

Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference

Marghny H. Mohamed¹, Naziha M. Al-Aidroos², and Mohamed A. Bamatraf³

¹Department of Computer Science, Faculty of Computers and Information,
Assiut University, Egypt.
marghny@aun.edu.eg

²Department of Computer Engineering, Faculty of Engineering and Petroleum,
Hadhramout University, Yemen.
Nazsa16@yahoo.com

³Department of Computer Science, Faculty of Science, Hadhramout University,
Yemen.
mbamatraf1@yahoo.com

ABSTRACT

Steganography is one of the branches of information security field, it aims to hide information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. The secret message is hidden in such a way that no significant degradation can be detected in the quality of the original image. The aim of this paper is to introduce an efficient steganographic scheme to hide data over gray scale images. This scheme is based on the property of the human eye, which is more sensitive to the change in the smooth area than the edge area using pixel value difference, besides employing the LSB substitution technique as a fundamental stage. The experimental results show that the proposed method could successfully achieve the goals of the high embedding capacity and maintaining the visual quality, in addition, provides more secure data hiding using selective pixel positions determined by a secret image (i.e. key). Moreover, based on that, the secret message is replaced with dynamic LSBs, our scheme can effectively resist several image steganalysis techniques.

KEYWORDS

Data Security, Steganography, Data Hiding, Least-Significant Bit (LSB), Pixel Value Difference (PVD).

1. INTRODUCTION

The development in technology and networking has posed serious threats to obtain secured data communication. In order to keep the unauthorized user away, variety of techniques have been proposed. Information hiding and cryptography are two main ways to secured communication. Steganography is one of the branches of information hiding, it is the art of hiding information by conceal its existence, unlike cryptography technique which about protecting the content of message by transform it to be meaningless and unintelligible to unauthorized users.

An information hiding system is characterized by having three different aspects that contend with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of data bits that can be hidden in the cover medium, security relates to the ability of an eavesdropper to detect the hidden information easily, and robustness is concerned about the

amount of modification the stego medium can resist before an adversary can modify or destroy the hidden information [21].

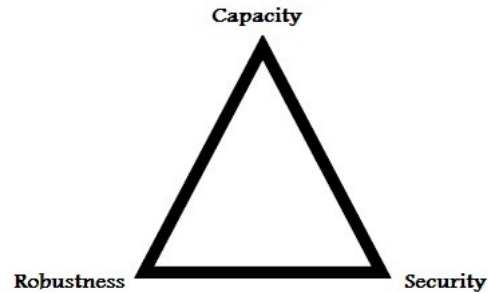


Figure 1. Information-hiding system features.

Steganography is the art and science of communicating in such a way which hides the existence of the message, as defined by Cachin [5]. It includes a variety number of methods for hiding data in media. These media were invisible inks, microdots, etc. Nowadays, steganography uses text, images, audio, and video media.

Image steganography is the most widely used, compared with the other types of steganography, this popularity because the large amount of redundant information present in the images that can be easily altered to hide secret messages inside them, and because it can take advantage of the limited power of the human visual system (HVS) [2].

In Image steganography, the term cover image is used to describe the image used to hold secret information inside, while the resulting image which obtained by embedding secret data into cover image is called the stego image.

An image in a computer is an array of numbers that represent light intensities at various pixels, these pixels make up the image's raster data. Digital images are stored in either 24-bit (true color images) or 8-bit per pixel files. Hence 8-bit color images, like GIF files, can be used to hide information. Here, each pixel is represented as a single byte, and the pixel's value is between 0 and 255. Grey scale images are preferred because the shades are changed very gradually between palette entries, this increases the image's ability to hide information [13].

A lot of ways are used to hide information inside the images. Least significant bit (LSB) substitution, and masking & filtering techniques are the most well known techniques using in image steganography. LSB technique is a simple approach to hide information in an image, but any image manipulation can destroy the hidden information in this image easily.

The steganography domain is growing up very quickly, several of practical trials and mathematical papers are published constantly, some of these papers are used LSB-based method in an attempt to get a new data hiding techniques or to develop an existing techniques, such as: [4], [6], [7], [14], [15], [16], [17], [22], [25].

The LSB-based techniques, directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is higher than that of a smooth area, this meaning that, an edge area can conceal more secret data than a smooth area. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more

sensitive to change in the smooth areas. So, new embedding techniques using the advantage of edge detection technique are introduced, such as, [8], [10], [19] which evaluate the correlation between neighboring pixels to determine whether a pixel is located in an edge area or a smooth area, and how many bits should be embedded in that pixel accordingly, using method named “Side Match”. Another technique proposed by Wu et al. [26], using the pixel-value differencing (PVD) method to distinguish edge and smooth areas. Based on this technique, several researches are suggested in order to provide data hiding methods achieve a high embedding capacity as possible, such as, [9], [23], [24], [30].

Because the PVD method does not utilize the smooth area to hide large amount of secret data, the capacity is still low. In order to achieve higher capacity, another researchers used a combination of PVD and LSB. These techniques are based on the idea of using PVD when the difference between a pair of pixels is large (edge area), and using LSB method when the difference is small (smooth area), such in [3], [18], [20], [27], [28], [29].

The proposed approach introduces a new hybrid method integrating both a dynamic classical LSB data hiding technique and the pixel value difference technique. Our primary target here is to increase the capacity of embedded data without much distortion, in addition to increase the security of the proposed scheme, key image is introduced as the secret key, then find the edges of both cover and key images, these edge pixels positions are used in the embedding process consecutively as discussed later.

The paper is organized as follows; briefly background about the techniques used in the proposed method is introduced in Section 2. Our scheme is presented in Section 3. The experimental results with some analyses and discussions are shown in Section 4. Finally, the conclusions are provided in Section 5.

2. BACKGROUND

2.1 Least Significant Bit Hiding (LSB) Scheme:

This method is one of the earliest proposed steganographic techniques. The idea is to store a fixed number of bits of the secret data directly into the least significant bits of the pixels of the cover image. Because LSB is extremely simple to implement and incurs less processing time, it is commonly used. However, the insertion of fixed-length bits in least significant bits may cause noticeable distortion in the image because not all pixels can tolerate large changes in its data. Furthermore, it is easy to attack. Hence, there is a trade-off between the amount of secret data that can be embedded, the image distortion, and the security of the stego-image [3].

To understand the operation of LSB replacement method, suppose we have the following pixels, $P_1 = [11001011]$, $P_2 = [00011010]$, $P_3 = [01001100]$, and the bits want to embed it in the LSBs positions of them are $M = [010]$, the resulted pixels after embedding are, $P_1 = [1100101\mathbf{\underline{0}}]$, $P_2 = [0001101\mathbf{\underline{1}}]$, $P_3 = [0100110\mathbf{\underline{0}}]$.

So we can say that the LSB method has the following limitations [3]:

- a) Since LSB is simple and well known, it becomes vulnerable to security attacks.
- b) Increasing the amount of embedded data in each pixel results in more visual degradation in the image quality.
- c) Due to the uniform distribution of the embedded data over the whole cover image, the disruption of the image histogram becomes noticeable.

2.2. Pixel-Value Differencing (PVD) Scheme:

In the human visual system, the alteration of edge areas cannot be distinguished well, unlike the alteration of smooth areas. With this concept, a novel steganography technique was proposed by Wu and Tasi [26] using the pixel-value differencing (PVD) method to distinguish edge and smooth areas. This method relies on the idea that not all pixels can store the same number of bits of the secret data. Instead of inserting the secret bits directly to the end of each byte of the cover image (which is the way in which LSB works), they determine the number of bits to be embedded based on the differences between pairs of adjacent pixels. This allows the method to embed more data in the edge area of the cover image without too much reduction in the stego image quality.

An edge is characterized by significant dissimilarity in gray levels being used to indicate the boundary between two regions in an image fragment. Edge detection is a significant area of the image processing and machine vision due to the fact that edges are considered to be the important features for analyzing the most essential information contained in images [11].

In the proposed method, we employed the PVD idea to generate the edges of the cover image and key image as well, while embedding the secret data.

3. THE PROPOSED SCHEME

In this section, the proposed scheme will be introduced in detail, it consists of two procedures, the embedding procedure and the extracting procedure.

3.1 The Embedding Procedure:

Suppose we have 2 images, the cover image I_C and the secret key image I_K , with the same size. Any image I consists of set of pixels:

$$I = \{P_1, \dots, P_N\},$$

$$|P_i| = 8 \text{ bits}, P_i = \{b_1, \dots, b_8\}, b_j \in \{1, 0\}. \quad (1)$$

The image size is computed as:

$$N = W \times H. \quad (2)$$

Where W, H is the image width and height respectively. Suppose M is the secret data bits, with length n ,

$$M = \{m_1, m_2, \dots, m_n\}, \text{ where } m_i \in \{1, 0\}. \quad (3)$$

The proposed method takes the dependency advantage of pixels on its surrounding neighbors. The correlation between a pixel and its neighbors decides whether it is located in a smooth area or in an edge area. The data embedding algorithm's steps are as follows.

Step 1: Obtain the edge images of the cover I_C and key I_K grayscale images, by dividing the images into overlapping blocks, each block consists of 4 neighboring pixels (Figure 2).

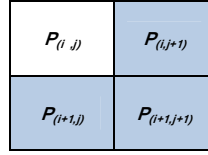


Figure 2. A target pixel and three neighboring pixels.

Where the target pixel $P_{(i,j)}$ with gray value $g_{(i,j)}$, let $g_{(i,j+1)}$, $g_{(i+1,j+1)}$ and $g_{(i+1,j)}$ be the gray value of the neighboring pixels, right pixel as $P_{(i,j+1)}$, down-right pixel as $P_{(i+1,j+1)}$ and down pixel as $P_{(i+1,j)}$, respectively.

Step 2: Calculate the difference value d of each block which is used to categorize the smooth and edge regions, then select the maximum difference among them as following:

$$d1 = |g_{(i,j+1)} - g_{(i,j)}|,$$

$$d2 = |g_{(i+1,j)} - g_{(i,j)}|,$$

$$d3 = |g_{(i+1,j+1)} - g_{(i,j)}|,$$

$$d = \max (d1, d2, d3). \quad (4)$$

Step 3: Using Equation (4), we can decide whether the target pixel is included in an edge area, if d value is more or equal to a certain threshold, otherwise it is included in a smooth area, after this step we will obtain two sets of pixels in each image, the first called edge pixels denoted as E , and the other called smooth pixels denoted as S ,

$$E = \{E_1, \dots, E_e\},$$

$$S = \{S_1, \dots, S_s\}. \quad (5)$$

Where e , s is the size of the edge pixels set and the smooth pixels set respectively, where $N = e + s$.

Step 4: Unselect all the intersected pixels between the key edge pixels set E_K and the cover edge pixels set E_C (.i.e. $E_K \cap E_C$), meaning the new E_K will be $(\overline{E_K \cap E_C})$ pixels, then determine the key edge pixel's position in the cover smooth pixel set S_C to obtain the smooth positions for embedding.

Step 5: Using the key edge pixel positions E_K , select the corresponding pixels in the smooth area of the cover image S_C for embedding.

Step 6: For embedding bits stream M , initially set a variable called a switch number (s_num) indicates to number of switches in the embedding process between the edge and smooth regions.

Step 7: To embed the secret data bits, we have two categories of pixels corresponding to edge pixels category and smooth pixels category. In each cover pixel belongs to the first category embeds 'x' secret data bits using the LSBs substitution technique, otherwise embeds 'y' secret data bits using the LSBs substitution technique in the second category pixels.

$$\begin{aligned}
 & \text{if } (P_i \in E_C) \\
 & \quad \text{embed } x \text{ bits} \\
 & \text{else embed } y \text{ bits.}
 \end{aligned} \tag{6}$$

Where P_i is the cover pixel, E_C is the edge pixels set of the cover image.

Step 8: The embedding process is done mutually (not consecutive) between the selected pixels of the edge E_C and smooth S_C areas. The switching between them is determined according to the switch number (s_num) as defined previously.

The block diagram of the embedding process steps is shown in Figure 3.

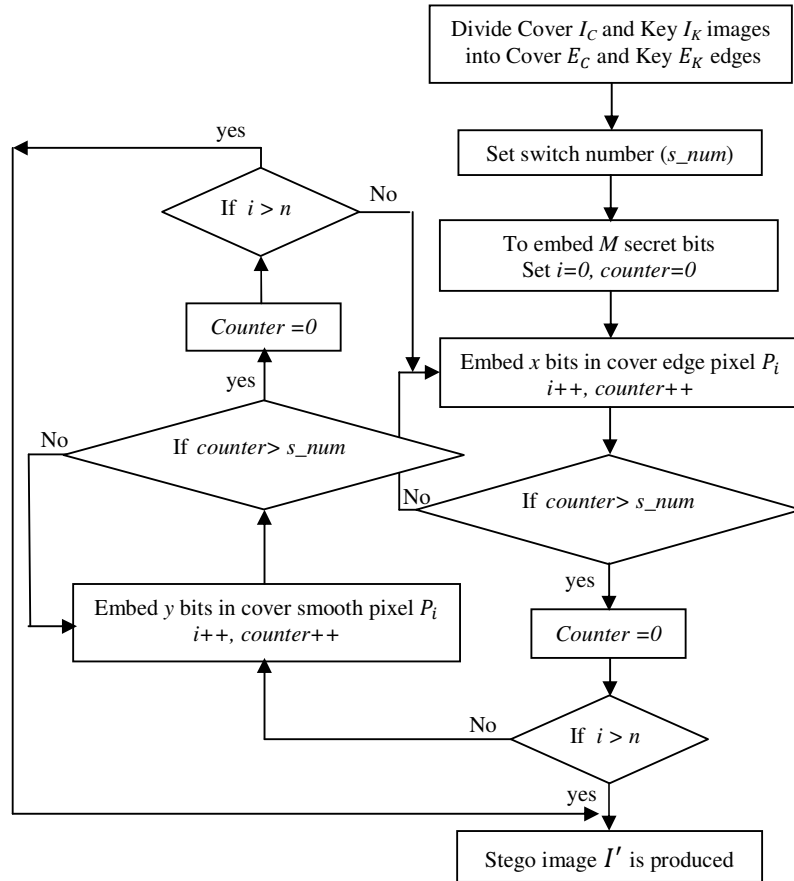


Figure 3. A block diagram of embedding steps.

3.2 The Extraction Procedure:

To recover the original secret data at the receiving side, the original image I must be known to determine the original edge E and smooth S areas before embedding, then the following steps are done.

Step 1: Find the edge and smooth areas of the cover and key images, as the same way described in the previous section.

Step 2: Using the position of the original smooth and edge areas, we can determine which pixels belong to the edge area E' , and which are belong to the smooth area S' in the stego image I' easily.

Step 3: Depending on switch number value we can know the position of the certain pixel, if it belongs to an edge area or to smooth area, according to that the extracting of the embedded data bits is done, as follows:

if ($P_i \in E'$)
extract x bits

else extract y bits. (7)

Step 4: At this stage, the retrieving algorithm finishes and the embedded data has been retrieved completely. These steps are described in the block diagram in Figure 4.

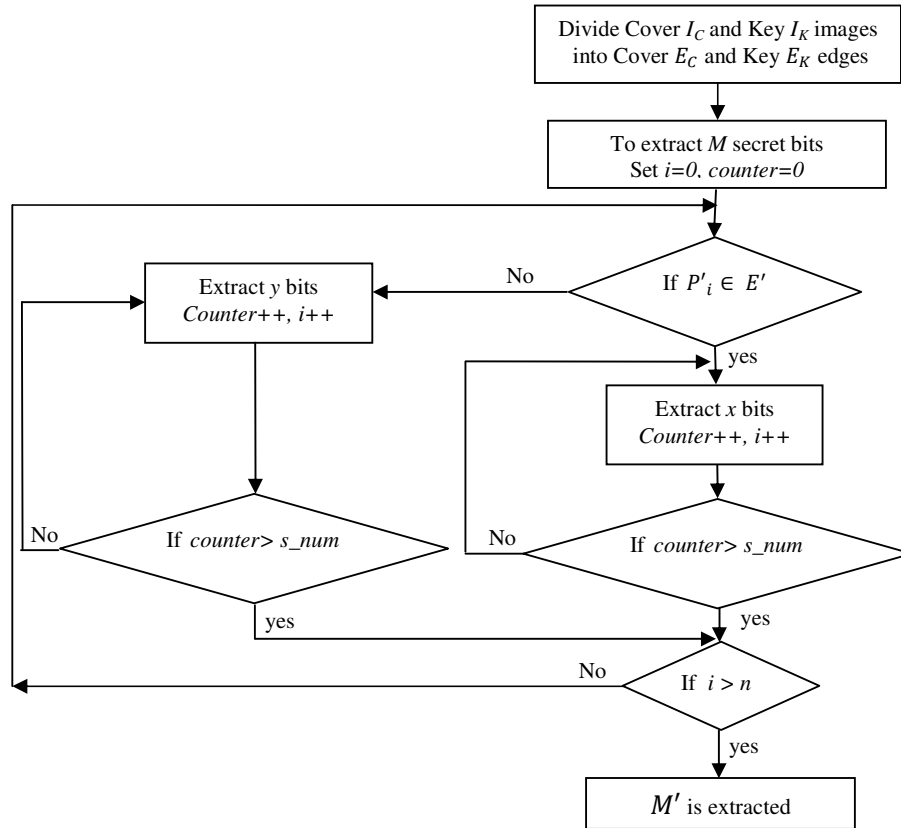


Figure 4. A block diagram of extracting steps.

4. EXPERIMENTAL RESULTS

The experimental results presented in this section demonstrate the performance of our proposed scheme. To conduct our experiments; we used four 128×128 standard grayscale images, “Baboon”, “Pepper” and “Cameraman” as the cover images and “Lena” as the key image,

which are commonly used in image processing, compression and steganography. These images are shown in Figure 5.

A series of pseudo random binary numbers are used as the secret data to be embedded into the cover images.

The performance of the proposed scheme is considered from two viewpoints, the visual quality of the stego image and the data capacity.



Figure 5. Four 128×128 grayscale images.

To evaluate the stego image quality, we used the peak signal-to-noise ratio (*PSNR*) measurement, which is used to evaluate the difference between the stego and cover images. The *PSNR* formula is defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} (dB). \quad (8)$$

Where *MSE* is the mean square error between the cover and stego images. For a cover image whose width and height are *W* and *H*, *MSE* is defined as:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H (I_{ij} - I'_{ij})^2. \quad (9)$$

Where I_{ij} and I'_{ij} are the pixel values of the cover and stego images, respectively.

Note that, a large *PSNR* value means that the stego image is most similar to the original image and vice versa. Generally, if the *PSNR* value is larger than 30 *dB*, then the distortion on the stego image is hard to be detected by human eyes [12]. Our experimental results show that the proposed scheme can embed a large amount of information while keeping an acceptable visual quality.

Second metric for performance evaluation is the data payload (capacity). Data payload can be defined as the amount of information it can hide within the cover media, this can be expressed as number of bits, which indicates the max message size that might be inserted into an image. It can be calculated as a percentage from the full image size [1].

$$Capacity = \left(\frac{\text{Total number of bits embedded into image}}{\text{Total number of pixels on image}} \right) (\text{bits/pixel}). \quad (10)$$









$$\text{Total number of bits embedded into image} = x \times no_c + y \times no_k \text{ (in bits)}. \quad (11)$$

Where: no_c = number of cover edge pixels, no_k = number of key edge pixels - intersected pixels.

Usually, the high payload requirement will conflict with the high *PSNR* requirement. Generally speaking, when the payload increases, the *MSE* will increase, and this will affect the *PSNR* inversely. So, a trade-off should be made between capacity and *PSNR* requirements [1]. Thus, innovative data embedding method presented here to improve the embedding payload and to maintain the visual quality as good as possible preserving the security requirement.

Table 1 shows the visual quality of the edge images and the number of edge pixels in each of them, which are generated by our proposed scheme at a certain threshold (*i. e.* $d \geq 15$).

Table 1. The edge images are generated by our scheme.

	Cover images			Key image
Greyscale images				
Edge images				
Number of edge pixels	8676 Pixel	7401 Pixel	7097 Pixel	2803 Pixel
Number of smooth pixels used for embedding *	1312 Pixel	1591 Pixel	1586 Pixel	

Note: *Number of smooth pixels used for embedding = Number of key edge pixels – (key edge pixels \cap cover edge pixels).











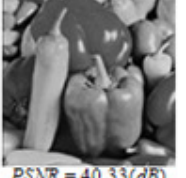

To facilitate the computation we fixed the length of the message to 1000 bits, Lena image was used as the key image. The performance of the proposed scheme is shown in Table 2. Note that x and y correspond to the number of LSBs in each edge and smooth pixels which are replaced by secret message bits. To maintain the quality of the stego image, the value of y is set 1 or 2. The experimental results show that we can choose the value of x as 3 or 4 without causing any perceptible distortion.

Obviously, the advantage of the proposed scheme depends on the two parameters x and y . To prove that our scheme can achieve better stego image quality and obtain a high embedding payload, we perform the proposed algorithm with various x and y values. Table 2 presents the relationship between these parameters and the stego image quality. It also show that the larger

values of parameters x and y will yield to a higher embedding payload but lower stego image quality. However, based on the experimental results, we clearly notice that the stego image quality is preserved based on the HVS. This is because the change in the edge pixel does not significantly affect the quality of the stego image.

Furthermore, from Table 2, the quality of the stego image is still acceptable even when the values of the parameters x and y are high. At this level, the changes in the original cover image due to embedding of secret data are hard to be recognized by human eyes. The proposed scheme preserves high embedding payload reaching 2.28 *bpp* while the quality of the stego image remains good.

Table 2. The performance of our scheme.

Stego images	$y=1$		$y=2$	
	$x=3$	$x=4$	$x=3$	$x=4$
Baboon	 PSNR = 41.41(dB) Capacity = 1.67 <i>bpp</i> Total no. of bits=27,340	 PSNR = 38(dB) Capacity = 2.2 <i>bpp</i> Total no. of bits=36,016	 PSNR = 40.72(dB) Capacity = 1.75 <i>bpp</i> Total no. of bits=28,652	 PSNR = 37.44(dB) Capacity = 2.28 <i>bpp</i> Total no. of bits=37,328
Camerman	 PSNR = 40.04(dB) Capacity = 1.4 <i>bpp</i> Total no. of bits=22,877	 PSNR = 37.84(dB) Capacity = 1.83 <i>bpp</i> Total no. of bits=29,974	 PSNR = 39.82(dB) Capacity = 1.5 <i>bpp</i> Total no. of bits=24,463	 PSNR = 37.6(dB) Capacity = 1.93 <i>bpp</i> Total no. of bits=31,560
Pepper	 PSNR = 41.02(dB) Capacity = 1.5 <i>bpp</i> Total no. of bits=23,794	 PSNR = 37.38(dB) Capacity = 1.9 <i>bpp</i> Total no. of bits=31,195	 PSNR = 40.33(dB) Capacity = 1.55 <i>bpp</i> Total no. of bits=25,385	 PSNR = 37.09(dB) Capacity = 2 <i>bpp</i> Total no. of bits=32,786

In addition to the generation high quality of the stego image and high embedding payload, the proposed scheme is robust against some steganalysis techniques. Indeed, by taking this approach, we can obtain:

1- The secret message is inserted into various numbers of LSBs in different cover pixels. In other words; there are x secret message bits replaced with x LSBs of each edge pixel and y secret message bits are inserted into each non-edge pixel.

2- The secret message is embedded into part of the cover image. In our proposed scheme, because the embedding is done only on edge pixels, and on smooth pixels chosen from key image. Therefore, the LSBs of every stego pixel doesn't contain the secret message.

Based on the above two properties, the scheme can resist some statistical analysis attacks.

Security factor is taking into consideration also, where it is an important issue to prevent extraction of hidden information by unauthorized party. Our proposed scheme provides levels of security, as following:

- 1- Determine the edge pixels by making the difference between pixels based on certain threshold.
- 2- Determine which pixels in smooth area will be used for embedding, using the edge pixels of key image, then based on these edge pixels positions we can determine which pixels in the smooth area of the cover will be used.
- 3- Number of the embedded secret bits in the edge pixels is different from those in the smooth pixels, where the pixels in an edge area will have large differences whereas the pixels at the smooth area will have small differences. The larger the difference, the more bits to be hidden.
- 4- To increase the security of the proposed scheme, we used switch variable (may be a fixed or a random number) to make the data extraction more difficult, as distribution of the secret data between the edge and smooth pixels is not sequential.

5. CONCLUSION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Imperceptibility, capacity and security are three aspects for a good steganographic approach. In this paper, we proposed a new scheme using combination between LSB and PVD methods. Our method increased the capacity of hidden data by embedding more data bits in the edge pixels, and to reduce the stego image degradation we embed a less data bits in the smooth pixels. Furthermore, we embed the secret data on the smooth region using pixels selected by the position of the edge pixels of the key image, in addition to using switch number, which makes the extracted process by anyone who doesn't know the switch number and key image more difficultly. Experimental results confirm that the proposed scheme is successful in obtaining a stego image of satisfactory quality and capacity. Moreover, it can resist some of steganalysis systems which are based on statistical analysis.

REFERENCES

- [1] Al-Ataby A. and Al-Naima F. (2010) "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, vol. 7, no. 4, pp. 358-364.
- [2] Al-Husainy M. (2011) "A New Image Steganography Based on Decimal-Digits Representation", Computer and Information Science, vol. 4, no. 6, pp. 38-47.
- [3] Al-Sadi A. and El-Alfy E. (2011) "An Adaptive Steganographic Method for Color Images Based on LSB Substitution and Pixel Value Differencing", ACC 2011, Part II, CCIS 191, pp. 535-544.
- [4] Battisti F., Carli M., Neri A., and Egiazarian K. (2006) "A Generalized Fibonacci LSB Data Hiding Technique", 3rd International Conference on Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta.
- [5] Cachin C. (2004) "An Information-Theoretic Model for Steganography", Information and Computation, vol. 192, no. 1, pp. 41-56. Parts of this paper appear in Proc. 2nd Workshop on Information Hiding, 1998.
- [6] Chan C. and Cheng L. (2004) "Hiding Data in Images by Simple LSB Substitution", Pattern recognition, vol. 37, pp. 469-474.
- [7] Chang C., Hsiao J., and Chan C. (2003) "Finding Optimal Least-Significant-Bit Substitution in Image Hiding by Dynamic Programming Strategy", Pattern Recognition, vol. 36, pp. 1583- 1595.

- [8] Chang C. and Tseng H. (2004) "A Steganographic method for digital images using side match", *Pattern Recognition Letters*, vol. 25, pp. 1431-1437.
- [9] Chang K., Chang C., Huang P., and Tu T. (2008) "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing", *Journal of Multimedia*, vol. 3, no. 2, pp. 37-44.
- [10] Chen P. and Wu W. (2009) "A Modified Side Match Scheme for Image Steganography", *International Journal of Applied Science and Engineering*, vol. 7, no.1, pp: 53-60.
- [11] Chen W., Chang C., and Le T. (2010) "High payload steganography mechanism using hybrid edge detector", *Expert Systems with Applications*, vol. 37, pp. 3292-3301.
- [12] Chou Y., Chang C. and Li K. (2008) "A Large Payload Data Embedding Technique for Color Images", *Fundamenta Informaticae*, vol. 88, pp. 47-61.
- [13] Franz E., Jerichow A., Moller S., Pftizmann A., and Stierland I. (1996) "Computer Based Steganography", in *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174 pp 7-21.
- [14] Huang W., Zhao Y., and Ni R. (2011) "Block-Based Adaptive Image Steganography Using LSB Matching Revisited", *Journal of Electronic Science and Technology*, vol. 9, no. 4, pp. 291-296.
- [15] Kekre H., Athawale A., and Halarankar P. (2008) "Increased Capacity of Information Hiding in LSB's Method for Text and Image", *International Journal of Electrical, Computer, and Systems Engineering*, vol. 2, no.4, pp. 246-249.
- [16] Ker A. (2005) "Improved Detection of LSB Steganography in Grayscale Images", in: J. Fridrich (Ed.), *Information Hiding, Sixth International Workshop, Lecture Notes in Computer Science*, Springer, New York, vol. 3200, pp. 97-115.
- [17] Khalaf E. and Sulaiman N. (2011) "A Robust Data Hiding Technique based on LSB Matching", *World Academy of Science, Engineering and Technology*, vol. 58, pp. 117-121.
- [18] Kim K., Jung K., and Yoo Y. (2008) "A High Capacity Data Hiding Method using PVD and LSB", *International Conference on Computer Science and Software Engineering*, pp. 876-879.
- [19] Li S., Leung K., Cheng L., and Chan C. (2006) "Performance Evaluation of a Steganographic Method for Digital Images Using Side Match", *First International Conference on Innovative Computing, Information and Control - Volume III (ICICIC'06)*, vol. 3, pp. 54-57.
- [20] Li S., Leung K., Cheng L., and Chan C. (2006) "Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing", *Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06)*.
- [21] Lin E. and Delp E. (1999) "A Review of Data Hiding in Digital Images", in *Conference on Image Processing, Image Quality, and Image Capture Systems, PICS*, pp. 274-278.
- [22] Mohamed M., Al-Afari F., and Bamatraf M. (2011) "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation", *International Arab Journal of e-Technology*, vol. 2, pp.11-17.
- [23] Padmaa M., and Venkataramani Y. (2010) "Zig-Zag PVD – A Nontraditional Approach", *International Journal of Computer Applications*, vol. 5, no. 7, pp. 5-10.
- [24] Wang C., Wu N., Tsai C., and Hwang M. (2008) "A high quality steganographic method with pixel-value differencing and modulus function", *The Journal of Systems and Software*, vol. 81, no. 1, pp. 150-158.
- [25] Wang R., Lin C., Lin J. (2001) "Image Hiding by Optimal LSB Substitution and Genetic Algorithm", *Pattern Recognition*, vol. 34, no. 3, pp. 671-683.
- [26] Wu D. and Tsai W. (2003) "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters*, vol. 24, pp. 1613-1626.
- [27] Wu H., Tsai C., Wu N., and Hwang M. (2005) "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", In: *IEE Proceedings Vision, Image and Signal Processing*, vol. 152, pp. 611-615.
- [28] Yang C., Wang S., Weng C. (2007) "Analyses of Pixel-Value-Differencing Schemes with LSB Replacement in Stegonagraphy", In: *Proc. of the 3rd Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, vol. 1, pp. 445-448.
- [29] Yang C., Weng C., Wang S., and Sun H. (2008) "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488-497.
- [30] Zhang H., Geng G., and Xiong C. (2009) "Image Steganography using Pixel-Value Differencing", *Second International Symposium on Electronic Commerce and Security*, pp. 109-112.

Authors:

Marghny H. Mohamed: Received his Ph.D. degree in computer science from the University of Kyushu, Japan, in 2001, his MSc and BSc From Asyut university, Asyut, Egypt, in 1993 and 1988, respectively. He is currently an associate professor in the Department of Computer Science, and Vice-President for Student Affairs and Education of the Faculty of Computers and Information Systems, University of Asyut, Egypt. His research interests include Data Mining, Text Mining, Information Retrieval, Web Mining, Machine Learning, Pattern Recognition, Neural Networks, Evolutionary Computation, Fuzzy Systems, and Information Security. Dr. Marghny is a member of the Egyptian mathematical society and Egyptian syndicate of scientific professions. He is a manager of some advanced research projects in Faculty of Computers and Information Systems, University of Asyut, Egypt.

Naziha M. AL-Aidroos: Received her Bachelor Science degree in computer science in 2003 from Hadramout University for Science and Technology, Yemen, got here M.Sc. degree in 2009 from Asyut University, Egypt, in computer science. She has worked teacher in Computer Engineering department in faculty of Engineering and Petroleum in Hadramout University, Yemen, and she is currently a Ph.D. student in Faculty of Science, Asyut University, Egypt. Her interest subjects are Networks, Data Security, Data Mining, Neural Networks, and Image Processing.

Mohammed A. Bamatraf: Is an assistant professor in Hadhramout University of Science and technology, Yemen, Faculty of Science, Department of Computer Science. He received his BS degrees in computer Science from Poona University, India, and got his M.Sc in computer Science from Osmania University, India, and received his Ph.D. from Asyut University, Egypt. His Doctoral thesis was about modified data mining techniques and its application in medical diagnosis and intrusion detection. His research areas of interest includes: data and network security, medical informatics, data mining, machine learning, and bioinformatics. His research activities are currently focused on the application of Bioinformatics, Machine Learning, and data security.