Evaluation of using Steganography Technique to Hide a Text in Grayscale Digital Images

Sultana O Alsharkasi, Mohammed M Elsheh, Farij O Ehtiba

The Libyan Academy- Misurata

sulty87@gmail.com, m.elshah@lam.edu.ly, f.ehtiba@lam.edu.ly

Abstract**—***this paper presents a new approach to hide sensitive data inside grayscale digital image. It makes use of combining the RSA encryption algorithm with steganography technique. This approach based on searching for identical bits - two by two bits - between the sensitive data bits and image pixel bits values. In case the bits are non-identical, it hides the sensitive data bits at tow least scientific bits (LSB technique). Two types of images are used for implementing the steganography technique, one is light grayscale image and the other is dark grayscale image. The results of the grayscale are compared with resultant of RGB digital images. The results reveal that MSE, PSNR and correlation coefficient values were satisfactory.*

Keywords**: identical, Non-identical, steganography, LSB, RSA.**

I. INTRODUCTION

Over the last two decades, the growth of electronic documents which contain high volume of information has increased rapidly. So, it becomes very crucial to secure the information transmission between the sender and the receiver over the communication channels like the Internet[1]. This makes the researchers developing techniques to secure the information transmission. Cryptography and Steganography are techniques were developed to protect sensitive data from being stolen while transmitted. Cryptography is known as "the science of secrete writing", the data is encrypted by sender so it becomes unreadable by a third party and only the receiver who has the right key can decode the secrete message. Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from intended recipient knows the existence of the message. The secrete message is hidden inside a media carrier such as audio, video or digital image [2].

The terminologies used in the Steganography technique are: cover file, secrete message, stego file, secrete key and embedding algorithm. The cover file is the carrier, where the secrete message is hidden such as image, audio or video. The secrete message is information that needs to be sent safely to the receiver. The stego file is defined as the file after embedding the secrete message into it. The secrete key must be known by the receiver and it is depending on the embedding algorithm. The embedding algorithm is the algorithm used to hide the secrete message in the cover file [3].

Steganography techniques are classified into basic types namely, spatial domain techniques and transform domain techniques. In former type, the secret messages are embedded directly in the image. In this type of steganography, Least Significant Bits (LSB) is considered the most common and simplest insertion method, while in the later type of Steganography techniques the pixel values are transformed and then processing is applied on the transformed coefficients. The transformed coefficients are extracted by applying transforms, such as Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) to the image. In DCT, following transforming the image infrequency domain, the data is embedded in the LSB of the medium frequency components and is specified for loss compression, on the other hand, in DWT secret messages are embedded in the high frequency coefficients resulted from DWT and deliver maximum robustness [1, 4].

II. LITERATURE REVIEW

Rawat and Bhandari in [5] improved the least significant bit (LSB) substitution method which is used to hide text information into cover image. The characters of the secrete message are converted into ASCII code first then each value is converted into eight binary bits. Then separating the image into RGB plane and insert the bits in this order (RRGGGBBB). This means that the insertion of the first bit of the secrete message is in the last bit of the first pixel in red plane and the second bit in the last bit of red plane of the second pixel of the image and so on until the whole text is inserted. Douiri, Medeni, Elbernoussi and Souidi in [6] introduced a new steganography

Manuscript received March 3, 2021; revised March 29, 2021; accepted March 31, 2021, Published online April 4, 2021

method to hide information in a grayscale image based on graph coloring problem (GCP) in order to locate the optimal positions to hide secrete message, and be able to increase the capacity and imperceptibility of the image after embedding.

There are some researchers who combine the two methods, Steganography and Cryptography to increase the level of information security. Such as the method by Mathe, Atukuri, and Devireddy in [7] which demonstrates two phases of sending information in secure manner by utilizing public-key cryptography and Steganography depending on matching method in different regions of the image. The first step was converting the plain text message into cipher text utilizing Public-key Encryption algorithm. The following step was to find common Stego-key between the sender and receiver by Diff-Hellman key exchange protocol. The sender hides eight bits of information based on a matching method. Similarly, Chauhan, Kumar, and Doegar in [8] proposed approach that combines the steganography and cryptography using variable block size placed in fixed size. For encrypting data they used content based encryption algorithm and steganography techniques which are LSB and raster scan technique. Singh and Sharma in [9]explained an original approach for data communication over an unsecure channel and demonstrated steganography on gray and color images utilizing DCT enhancement and RSA Cryptosystem with LSB technique. Baek, Kim, Fisher and Chaoin in[10] basically used an Exclusive-OR (XOR) operation and a binary-to-gray code conversion. Recognizing that there are meaning patterns of the resultant XOR operation and its relationship against the binary and gray code. Utilizing some simple observed relationships between the binary representation of a pixel, the gray code representation, and the utilization of a simple XOR operation based upon N images available to the sender and the receiver. Mittal, Arora and Jain in[11] analyzed the degree of difference when steganography and cryptography are implemented together and separately, later they compared the.

Many studies concentrated on how to hide the information in the image, but Kaul and Chandra in [4] concentrated on how to increase the size of data hiding rather than how to hide it. They worked on bit level specifically embedding text in an image. Character pairing and mapping has been done in this research. Hence, the image will be like a search engine to search for the secrete key which will help out in how to trace the secrete message in the image.

Al-Shatnawi in [3] suggested a new algorithm to embed the secret information into image by enhancing the LSB. The secrete message is hidden in the image based on searching about the identical bits between the secrete message and the image pixels values. In each pixel it hides six bits of the secret message applied with two RGB images and the result was analyzed by calculating the ratio between the number of identical bits and the number of non-identical bits of the image color pixels values and the text message values.

Amjad Y. Hindi and his colleagues in [12] demonstrated a stego-method to hide sensitive data in any type of digital color image. Their work goes through several stages, staring by reshaping the original image from 2D matrix to 2D matrix with size n1*n3, n2 following by calculating the row and column indexes using a defined hash function. Then, LSB method is applied in order to hide a message using the indexes. Next, the holding image is reshaped back to a 3D matrix. On the following stage the second key (key2) is generated by using another hash function. Finally, the hidden data is extracted. The obtained results are acceptable when compared with the results of the LSB method; this is due to the fact that this method requires two keys to extract the secret message from the holding image, each of these keys consisting of eight decimal digits making the process of diffusion very complicated.

Dilpreet Kaur and his mates in[13] defined an approach to hide secret data in random LSB pixels. Their main goal was to maintain the quality of stego image while hiding more data per a single image. LZW compression technique is used to enlarge the text coverage in cover images, and for added security, it hides data in random pixels of the image which provides the strength of transposition cryptography. They argue that their approach is completely secured against the possibility of R-S detection attacks yet when having 2 times more data masking as compared to kekre's technique.

III. PROPOSED METHOD

This research combines Encryption and Steganography techniques based on spatial domain. The encryption process is implemented using RSA algorithm. Two types of grayscale images are used as a cover images to hide the secret message, one is dark and other is light of bmp format. Figure 1 shows the framework of the proposed approach.

A. EMBEDDING ALGORITHM:

Steganography method is proposed based on searching identical and non-identical bits between the secret message and cover image pixels which illustrated in Figure 2.

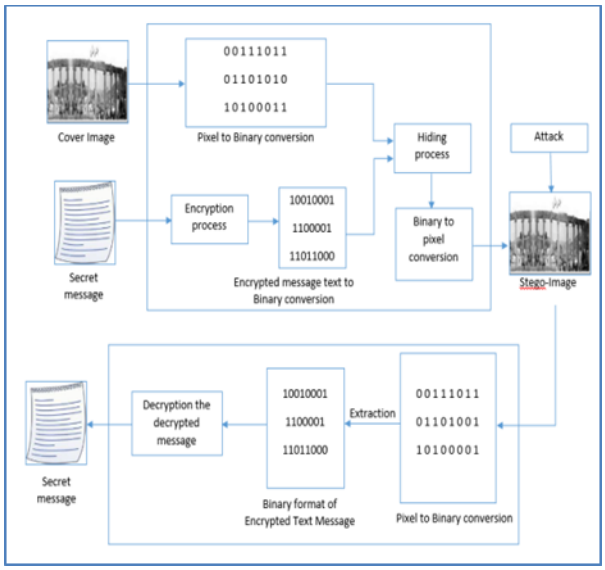


Figure 1. The framework of the proposed approach

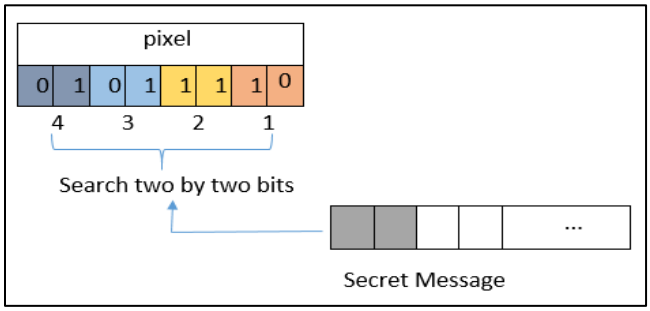


Figure 2. Proposed hiding algorithm

The proposed method is used to hide the secret message by using Algorithm 1.

B. Least Significant Bit Hiding (LSB):

If no identical bits were found, the two bits of secret message are hidden in the two least significant bits of the cover image as explained in Figure 3 and Algorithm 2.

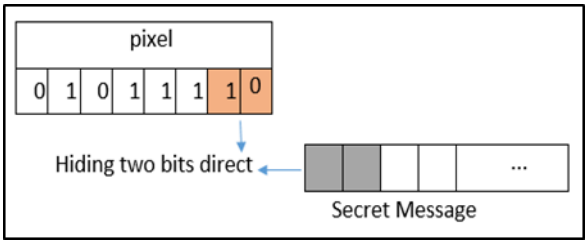
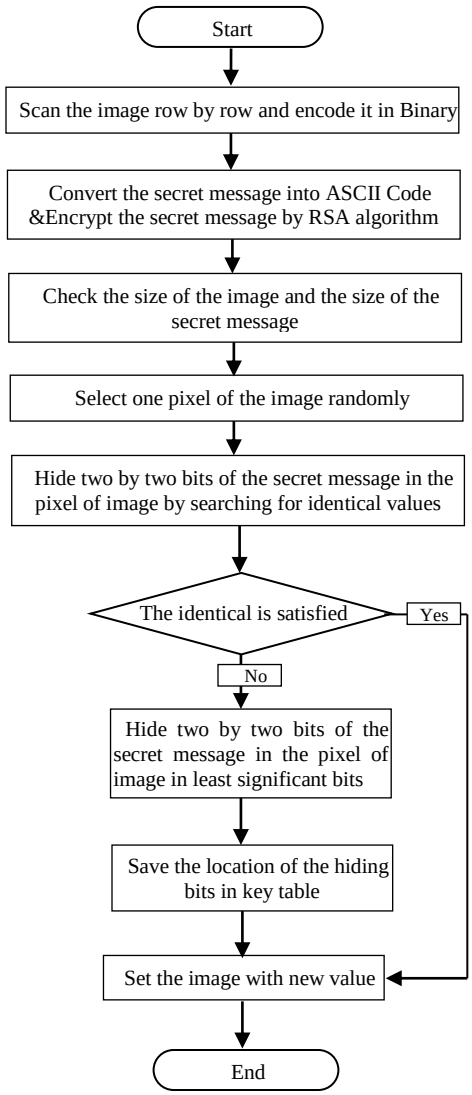


Figure 3. LSB hiding Technique

Algorithm (1): The Hiding Algorithm



Algorithm (2): The LSB hiding Technique

- Start
  - Scan the image row by row and encode it in Binary.
  - Convert the secret message into ASCII Code.
  - Encrypt the secret message by RSA algorithm, and then encode it in binary.
  - Check the size of the image and size of the secret message.
  - Start sub-iteration 1:
    - ✓ Hide two by two bits of the secret message in each pixel of image in least significant bits.
    - ✓ Set the image with new values.
  - End sub-iteration 1
  - Set the image with the new values and save it.
- End

C. *IDENTICAL AND NON-IDENTICAL BITS RATIO:*

Count the number of identical bits between the bits of the secret message and the image pixel bits, as well as the number of non-identical bits between them. The ratio of identical and non-identical bits is then calculated separately as in equations (1) (2):

$$Ratio_{Non-iden} = \left(\frac{number\ of\ non-identical\ bits}{Total\ number\ of\ bits\ hiddden}\right) * 100 \quad (1)$$

$$Ratio_{iden} = \left(\frac{number\ of\ identical\ bits}{Total\ number\ of\ bits\ hiddden}\right) * 100 \quad (2)$$

IV. RESULTS AND DISCUSSION

Several experiments were carried out to evaluate the proposed method. As shown in Figure 4 and Figure 5, two grayscale images with size 219X307 for dark image and 215X303 for light image are used as cover image and the secret message is: "The Libyan Academy".

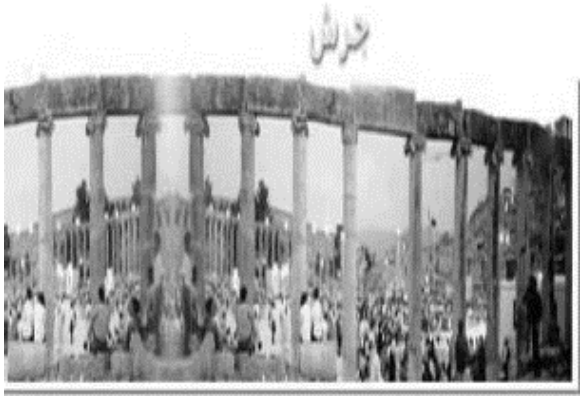


Figure 4: Light grayscale image

Figure 5: Dark grayscale image

Results of the proposed method and LSB hiding methods are analyzed based on the ratio between the number of the identical and the non-identical bits between the pixel of gray image values and the secret message values and compared it with a previous study in [3] .

Identical and Non-identical Bits Ratio by proposed hiding method is explained as follow:

Table (1) shows the ratio of identical bits and non-identical bits of light grayscale image and compares it with light color image in [3] , while Table (2) presents the identical bits and non-identical bits of dark grayscale image and compare it with results of dark color image of [3].

Table (1): A comparison between resultant of light images of the proposed method and in previous study in[3]

	Proposed method (Light gray image)		Exist study (Light RGB image)		
Identical bits	106	59.55 %	Red	35	64 %
			Green	46	
			Blue	31	
Non-identical bits	72	40.45 %	Red	23	36 %
			Green	12	
			Blue	27	
Sum (bits)	178	###		174	###

This means that light RGB image is better than the light gray image in hiding sensitive data

Table (2): A comparison between resultant of Dark images of the proposed method and previous study in [3]

	Proposed method (Dark Gray image)		Exist study (Dark RGB image)		
Identical bits	138	77.52 %	Red	46	80.5 %
			Green	49	
			Blue	45	
Non-identical bits	40	22.47 %	Red	12	19.5 %
			Green	13	
			Blue	9	
Sum (bits)	178	###		174	###

This means that dark RGB image is better than the dark gray image in hiding sensitive data.

Identical and Non-identical Bits Ratio by LSB hiding method is explained as follows:

. Here, we hide all bits of the secret message in two least significant bits of pixels of cover image and test bits of secret message to be hidden are identical with two values of least significant bits of pixel or not.

Tables (3, 4) explain the identical and non-identical bits when using LSB method for hiding the secret message in cover images that are RGB and grayscale.

Table (3): A comparison between resultant light images of the LSB method and previous study in [3]

	The Proposed Method		The LSB Method	
	Light Gray	Dark Gray	Light Gray	Dark Gray
Correlation Coefficient	0.999804	0.9999	0.999674	0.999678
MSE	5.8474	1.9495	10.6259	9.01652
PSNR	40.4612	45.2315	37.8671	38.5804

The shown results above tell that the light gray image is better than the light RGB image to hide sensitive data by LSB technique.

Table (4): A comparison between resultant dark images of the LSB method and previous study in [3]

	Light Gray image		Light RGB image		
Identical bits	112	62.92 %	Red	12	22 %
			Green	14	
			Blue	13	
Non-identical bits	66	37.07 %	Red	46	77 %
			Green	44	
			Blue	45	
Sum (bits)	178	###		174	###

LSB method gave the same result with color image and gray image.

V. STEGANOGRAPHY ATTACK:

To evaluate robustness of the proposed method, we used some attacks on stego-image. The attacks are: noise speckle, salt and pepper and rotate image clockwise. The results of the experiments that performed on a stego-images (light and dark) show that the robustness of the proposed algorithm is unsatisfied. The secret message is not protected and no strong safety against attack was achieved.

VI. CONCLUSION

The proposed method is concerned with hiding sensitive data within a grayscale image depending on the identical of the bits of the secret message with a cover image. In case of Non-identical bits, the LSB technology is used to hide data in the last two bits of image pixel. Pixels are randomly chosen. Two bits of sensitive data are hidden in each pixel chosen from the grayscale image, while six bits are hidden in one pixel of RGB image. Based on the obtained results using the principle of identical, it is found that hiding sensitive data in color digital images is more efficient than grayscale images. Random selection of pixels is the best way because the effect on the image quality is minimal, because the hiding based on search about the identical bits between the sensitive data bits and the cover image bits saves the values of some pixels of the cover image unchanged. When using LSB technology, it is clear that light grayscale image are more efficient than light RGB, and gave equal values in the case of dark images.

REFERENCES

[1] A. Abdelmged, A. Tarek, A.-H. Seddik, and M. Shaimaa, "Improving ZOH Image Steganography Method by using Braille Method," *International Journal of Computer Applications*, vol. 151, 2016.

[2] A. Abdelmgeid, A. Tarek, S. S. Al-Hussien, and M. Shaimaa, "New Image Steganography Method using Zero Order Hold Zooming," *International Journal of Computer Applications*, vol. 133, 2016.

[3] A. M. Al-Shatnawi, "A new method in image steganography with improved image quality," *Applied Mathematical Sciences,* vol. 6, pp. 3907-3915, 2012.

[4] N. Kaul and M. Chandra, "A Proposed Algorithm for Text in Image Steganography based on Character Pairing and Positioning," *International Journal of Computer Applications (0975–8887) Volume,* 2015.

[5] D. Rawat and V. Bhandari, "Steganography technique for hiding text information in color image using improved LSB method," *International Journal of Computer Applications*, vol. 67, 2013.

[6] S. M. Douiri, M. B. O. Medeni, S. Elbernoussi, and E. M. Souidi, "A new steganographic method for grayscale image using graph coloring problem," *Appl. Math*, vol. 7, pp. 521-527, 2013.

[7] R. Mathe, V. R. Atukuri, and S. K. Devireddy, "Securing information: cryptography and steganography," *International Journal of Computer Science and Information Technologies*, vol. 3, pp. 4251-4255, 2012.

[8] S. Chauhan, J. Kumar, and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," in *Computational Intelligence & Communication Technology*

(CICT), 2017 3rd International Conference on, 2017, pp. 1-7.

[9] Y. K. Singh and S. Sharma, "Image steganography on gray and color image using DCT enhancement and RSA with LSB method," in *Inventive Computation Technologies (ICICT), International Conference on*, 2016, pp. 1-5.

[10] J. Baek, C. Kim, P. S. Fisher, and H. Chao, "(N, 1) secret sharing approach based on steganography with gray digital images," in *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*, 2010, pp. 325-329.

[11] S. Mittal, S. Arora, and R. Jain, "PData security using RSA encryption combined with image steganography," in *Information Processing (IICIP), 2016 1st India International Conference on*, 2016, pp. 1-5.

[12] A. Y. Hindi, M. O. Dwairi, and Z. A. AlQadi, "A Novel Technique for Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 9, pp. 4942-4945, 2019.

[13] D. Kaur, H. K. Verma, and R. K. Singh, "Image Steganography: Hiding Secrets in Random LSB Pixels," in *Soft Computing: Theories and Applications*, ed: Springer, 2020, pp. 331-341.