# A NOVEL APPROACH OF IMAGE STEGANOGRAPHY FOR SECRET COMMUNICATION USING SPACING METHOD

Wa'el Ibrahim A. Almazaydeh[1] H. S. Sheshadri[2] and S. K. Padma[3]

[1]Research Scholar, PET Research Foundation, PESCE, Mandya, India
[2]PESCE, Mandya, India
[3]Sri Jayachamarajendra College of Engineering, Mysore, India

***ABSTRACT***

*Steganography is the art of hiding a digital media with another digital media, it is very important to transmit a secret data from place to another because if any one intercept the data during the transmission he can't know if there is a data a data or not. This paper shows a new method to hide a secret data in an image without any bit change of the stego image that means the PSNR value between the original image and stego image equal to Infinity. The size of the secret message that can be hidden in the image is infinity or unlimited. This method based on generating a dynamic symmetric key between the sender and the receiver, it is used for encoding and decoding process and it is derived from the image and the secret message together.*

***KEYWORDS***

*Least Significant Bit (LSB), ASCII code, PSNR, zigzag scanning*

## 1. INTRODUCTION

Steganography is an art of secret communication of data. i.e., the data which is being transmitted is hidden from a third person. In cryptography, the secret message is kept in an unreadable form to a third person, whereas in steganography, the existence of the message is kept as a secret from the third person. In this method, the secret message can be embedded inside a cover medium, which can be a text, an image, an audio or a video. Based on this, steganography can be classified as text steganography, image steganography, audio steganography and video steganography respectively. For embedding the secret message into the cover medium, a convenient algorithm is used by the sender and the same technique is used by the receiver to extract the message from the cover. After embedding the secret, the resulting file is called the 'stego' which is transmitted through the communication channel [1].

Steganography find their existence over a long time ago. In past ages Greek Historian Herodotus used to tattoo the secret message over the scalp of the slave and when the hairs were grown again the slave used to dispatched for the destination. During Second World War German discover a new technique called Microdots. In this technique Germans supposed to decrease the size a secret message or image unless and until it will become as the same size of the typed period. Later this technique was used to hide the secret message on a wooden piece and then it is covered by wax. In similar way a new technique were used as invisible ink. In this technique the secret message is written with the help of special kind of ink called invisible ink and the message can only be retrieved when the paper gets heated [2].

DOI: 10.5121/ijnsa.2018.10304 

This study is based on creating a Matlab program to test the results, it is called (Wa'el Steganography) program.

## 2. RELATED WORK

### 2.1. Previous Study

Wa'el Ibrahim A. Almazaydeh, H. S. Sheshadri and S.K. Padma proposed a novel method of image steganography, they used two techniques together: the dynamic symmetric key technique and Arithmetic coding technique (LSB+KEY+ARITH), the dynamic symmetric key is used to create a shared binary technique between the receiver and the sender to encoding and decoding process, it is also generated according to the binary value of image pixels and binary values of the secret message. The arithmetic coding is used to decrease the size of the secret message and to give the steganography process more security. They simulate their results using the Peak Signal to Noise Ratio (PSNR) algorithm to prove that the proposed method is better than the common method of steganography that is Least Significant Bit (LSB).

The authors Wa'el Ibrahim A. Almazaydeh, and H. S. Sheshadri proposed a new technique of image steganography, they used three methods: the common technique that is Least Significant Bit (LSB), the Huffman Coding technique to decrease the size of the secret message that it was called (LSB+HUFF) and the arithmetic coding technique to decrease the size of the secret message that was called (LSB+ARITH). They implement and simulate their results by using a Matlab program and Peak Signal to Noise Ratio (PSNR) to prove that the proposed two methods (LSB+HUFF) and (LSB+ARITH) is better than the common technique (LSB).

Wa'el Ibrahim A. Al-Mazaydeh proposed a novel technique of image steganography to hide a text in gray scale image using Huffman coding and zigzag scanning. The new technique is based on decrease the size of the secret message before start of the image steganography process. Zigzag scanning is used here to select the image pixels that wanted to embed the binary secret message in it and to give the steganography process more safety. The proposed was implemented by a Matlab program and using the Peak Signal to Noise Ratio (PSNR) to prove that the proposed method (LSB+HUFF) is better than (LSB) to hide a secret message in an image.

R Praveen Kumar, V Hemanth and M Shareef explaind that by using LSB technique, embedding larg amount of secret data is not possible. This paper depends on hidding huge amount of secret data using LSB common technique. To achieve this process, the size of the secret data is decreased using wavelet transforms. After compression, the results bits of the compression process are encoded using a reversible quantum gate. LSB is the best-known techniques when compared to the transformation techniques, because it reduces lots of noise distortion. In cryptography, the hacker can know the existence of the secret message transferring to the sender. Using this process huge amount of data can be communicated in the covert channel and even the existence of the secret message is hard to identify [7].

Dr. Saad Abdual azize AL_ani, Bilal Sadeq Obaid Obaid showed a new method to hide text in an image. This method depends on converting the character into six bits, by using the b-table to compress the data to four bits and it used similarly to value of image pixels. The receiver gets value of location encrypted by RSA method. There is no data hidden in the image data [8].

Amanjot Kaur, Dr. Bikrampal Kaur proposed a novel embedding approach based on k-Modulus Method for colored images. From experimental results it is clear that the proposed technique obtained high PSNR along with good image fidelity for various images which conform k-Modulus Method based image steganography can obtain better security [9].

Madhavi V.Kale , Prof. Swati A.Patil presented steganographic process system, the Compress ratio is computed using the Huffman Encoding compression technique. Then, the text is hidden in image, vedio and audio using the common technique of steganography that is Least Significant Bit (LSB) and encrypt by using advanced encryption standard algorithm. On another hand, when the receiver gets the receives the stego media that is will be image , audio or video appear as an original image. After that, receiver extracts the hidden data by using advanced encryption standard algorithm (AES) and getting the secret message which is hidden by sender in image, audio or video [10].

Amanjot Kaur, Dr. Bikrampal Kaur has proposed a new method to hidden approach based on k-Modulus Method for colored images. From their study results it is clear that the proposed method obtained a high PSNR along with good image fidelity for different images which conform k-Modulus Method based image steganography can obtain good security [9].

Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat presented a simple method to calculate the secret message data that is wanted to be hidden in the image. This method based on and used Connective Logical (CL) to calculate a binary number of the secret message while the most significant bit (MSB) the pixels were used as a key. MSB is a first bit of each pixel and it has a great significant value. Generally, the MSB of each pixel calculated with secret message using operator Negation, OR and XOR to get a new secret message. The new secret message will be hidden in the LSB of image pixels. The implementation of this model will produce a low computational complexity of steganography because of the simplicity of the proposed algorithm [11].

Yun-Te Lin, Chung-Ming Wang, Wei-Sung Chen, Fang-Pang Lin, and Woei Lin proposed a new method of hiding data for HDR images encoded by the OpenEXR format. The presented method hides data in the 10-bit mantissa field of each pixel, while the 1-bit sign and 5-bit exponent fields are kept intact. They recommend an optimal base allowing secret messages to be hidden with the least pixel distortion. An aggressive bit encoding and decomposition scheme is introduced herein, which offers the benefit for hiding an extra bit in a pixel group without incurring pixel distortion. The influence of the message probability is analysed and the embedding capacity is further increased by taking advantage of the recommended bit inversion hiding scheme [12].

Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain, and K. Raja Sekhar illustrated the various performance evaluation parameters of image steganography techniques. The performance of a steganographic technique can be rated by three parameters; (i) hiding capacity, (ii) distortion measure and (iii) security. The hiding capacity means the maximum amount of information that can be hidden in an image. It can also be represented as the number of bits per pixel. The distortion is measured by using various metrics like mean square error, root mean square error, PSNR, quality index, correlation, structural similarity index etc. Each of these metrics can be represented mathematically. The security can be evaluated by testing the steganography technique with the steganalysis schemes like pixel difference histogram analysis, RS analysis etc. All these metrics are illustrated with mathematical equations. Finally, some future directions are also highlighted at the end of the paper [13].

NIELS PROVOS AND PETER HONEYMAN discussed existing steganographic systems and presented recent research in detecting them via statistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking or else provide an overview of detection algorithms [14].

Dharmesh Mistry, Richa Desai, and Megh Jagad explained that the Steganography cannot take the place of the cryptography but it supports the cryptography. They showed that if the steganography and the cryptography is used together the result will be getting double layer of security and protection and decrease the probability to detect the hidden data [15].

## 2.2. Steganography

Figure 1 shows the Steganography technique [6]:

- Secret Message: the information that you want to embed inside the cover media.
- Stegokey: the key used in the Steganography process.
- Cover Media: the medium used in Steganography process such as: image, video, audio, etc.
- Encoding Algorithm: the method used in Steganography process.
- Stego-Media: the medium resulting from adding the secret message into a cover media using Stegokey and encoding algorithm.
- Decoding Algorithm: the method used to extract the secret message from Stego-media using Stegokey.

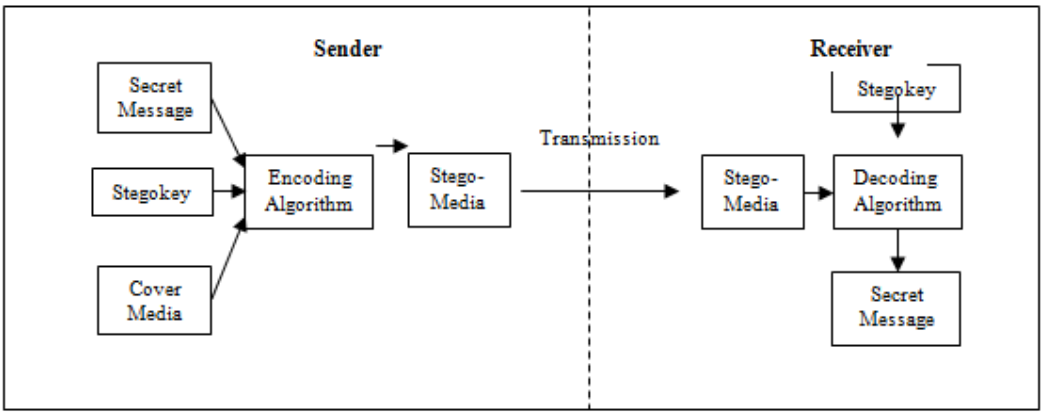


Figure 1. Steganography Technique

## 2.3. ASCII Code

American Standard Code for Information Interchange (ASCII) is the most common format for characters in the computer systems. In an ASCII code, each alphabetic, numeric, or special character is represented with a 7 bits binary number (a string of seven 0s or 1s). For example, the ASCII Code for (A, a, X, $, #) are (65, 97, 88, 36, 35) respectively. In this study, the ASCII code converts the secret message character to its corresponding value in the binary system [4].

## 2.4. Least Significant Bit (LSB)

The best common technique of image steganography the Least Significant Bit (LSB). This paper uses the LSB bit of the binary image pixel to compare it with the corresponding bit of the binary secret message data according to the proposed method that is shown in the figure 5. Figure 2 shows the LSB position in the one grayscale image pixel (8 bits).

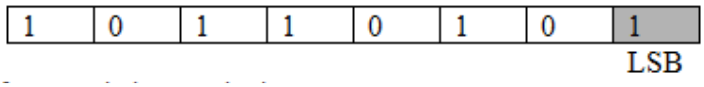


Figure 2. LSB of grayscale image pixel.

## 2.5. Zigzag Scanning

Zigzag scanning is the scanning process to the image to convert the image into one column of pixels. There is two procedures for the zigzag scanning: encoding zigzag scanning that converts the image to one column of the image pixels and decoding zigzag scanning that convert the column of the image pixels value to the original image (matrix). Figure 3 shows the encoding zigzag scanning process.

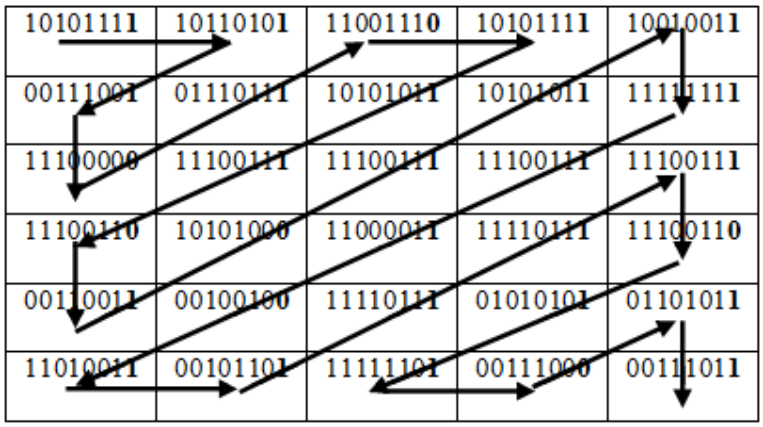


Figure 3. Encoding zigzag Scanning [4]

## 2.6. PSNR

Peak Signal to Noise Ratio (PSNR) (equation 1) is measured on a logarithmic scale. It depends on the mean squared error (MSE) between an original image and stego image, relative to (2n - 1)2 (the square of the highest-possible signal value in the image, where n is the number of bits per image sample) [16].

$$MSE = \frac{\sum_{M,N} [A(m,n) - B(m,n)]^2}{M \times N} \quad (1)$$

$$PSNR_{db} = 10 \log_{10} \frac{(2^n - 1)^2}{MSE} \quad (2)$$

"PSNR can be calculated easily and quickly and is therefore a very popular quality measure, widely used to compare the ‘quality’ of compressed and decompressed video images" [16].
If the PSNR value between the original image and the stego image is high, that means the change in the image resolution between the two images is low, if the PSNR value is low, that means the change in the image resolution between the two images is high and if the PSNR value equal to "infinity" that means no one bit change in the resolution between the original image and the stego image.

# 3. MEHODOLOGY

This paper shows two techniques to hide a secret message in an image: the traditional method Least Significant Bit (LSB) and a new method that is image Steganography using spacing based on a secret key between the sender and the receiver, it is called (LSB+SPACING Algorithm). This algorithm uses LSB and LSB-1 positions. The results between the two methods have been compared using Peak Signal to Noise Ratio (PSNR).

## 3.1. Steganography using LSB

LSB is the traditional method for the image Steganography. In this method, the original colored image is converted to a column of decimal values of all pixels of the image by using zigzag scanning with size equal to (M×N×3) where M is the number of rows in the original image, N is the number of columns in the original image and 3 is the number of planes of the image (Red plane, Green plane and Blue plane). The column of the decimal values after zigzag scanning is converted to the corresponding value in the binary value with size equal to (M×N×3×8) where 8 is the number of bits for each pixel in the plane. In a parallel process by using the ASCII code, the secret message is converted to a row of binary values with size equal (1×R) where R is the number of bits in the secret message. Each character in the secret message needs 7 bits to represent it in the ASCII code.

The size of data (Secret Message) that can be hidden in the image using this method is computed in the following way:

$$S1 = (M \times N \times 3) - 27 \tag{3}$$

Where S1 is the size of the binary secret message, M is the count number of rows in the image, N is the count number of columns in the image, and the number 27: the first 7 bits from 1 to 7 are reserved positions to the Steganography type that may be [1, 2, 3, …, 127], for example, if the Steganography type equals 1 that means the Steganography process is LSB, if the Steganography type equals 2 that means the Steganography process is another Steganography process and etc. The bits from 8 to 27 are reserved positions of bits to the length of the binary secret message.
Figure 4 shows the methodology of this study.

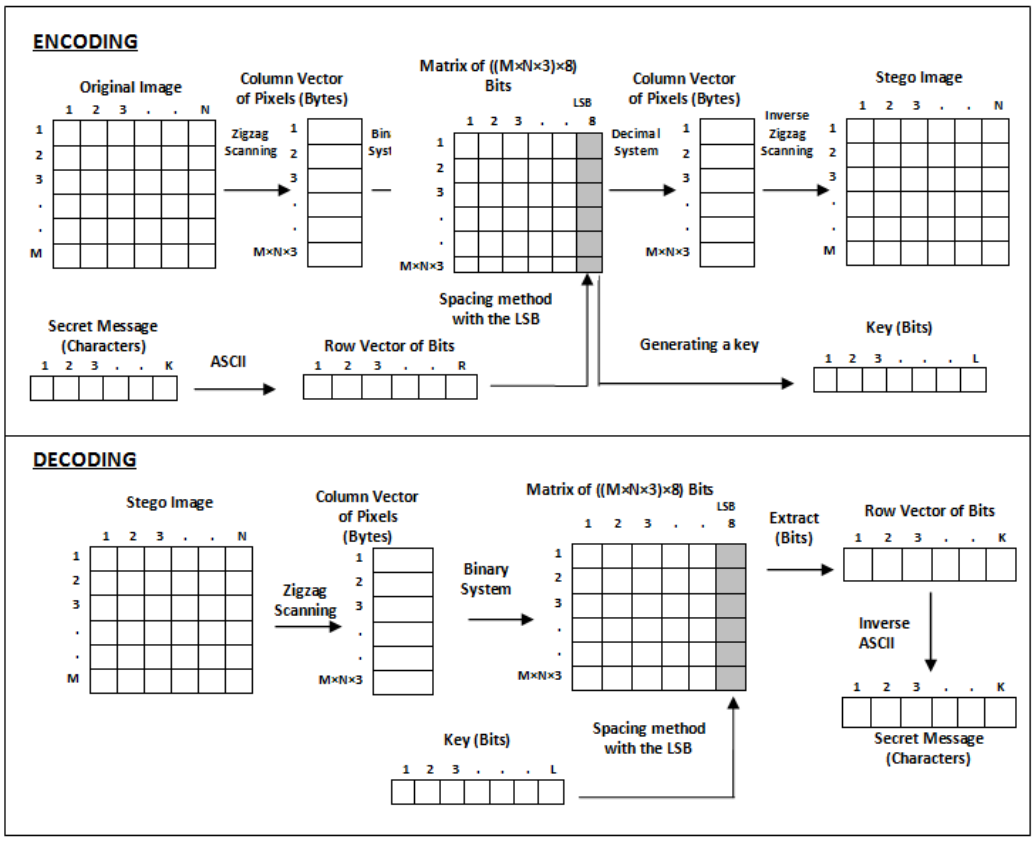


Figure 4. Encoding and Decoding of this study

## 3.2 Steganography using Spacing Method

LSB+SPACING method converts an original image to column of decimal values using zigzag scanning, after the converts the result values to the corresponding values in the binary system with size equal to (M×N×3×8) bits, where M is the count number of rows in the original image, N is the count number of columns in the original image, 3 is the count number of planes of the coloured image (Red, Green and Blue plane) and 8 is the number of bits of each pixel in the plane. In parallel process, the secret message is converted to the binary values using ASCII code. After that the method matches the first bit of the secret message with the bits in LSB and LSB-1 positions in the first row of the column of binary value, then it matches the second bit of the secret message with the bits in LSB and LSB-1 positions in the second row of the column of binary value, and it match the third bit of the secret message with the bits in LSB and LSB-1 positions in the third row of the column of binary value, etc. Figure 5 shows the Encoding and decoding of LSB+SPACING algorithm.

There are only three probabilities for the matching process in Spacing algorithm:

1. If the bit of the secret message matches with the position 0 of the (LSB), the key will be 0.
2. If the bit of the secret message matches with the position 1 of the (LSB), the key will be 1.

3. If the bit of the secret message doesn't match the first and the second position of the (LSB), the key will be empty character. In the decoding process to obtain the original bit we inverse (in logical process is not) the LSB bit across the empty character.

At the end of this process we will get row vector values of the keys that are called together the Key. This key is symmetric and shared key between the sender and the receiver, and without this key, the receiver will not be able to obtain the secret message.
This key is the base of this method and it is called dynamic symmetric key; because the key is changed depending on the image and on the secret message and symmetric because the key is shared between the sender and the receiver.

The word (Spacing) is used here because the key contains spaces.
The size of the data (Secret Message) that can hided into the image by using this method can be calculated by using the following formula: is computed as the following:

$$S2 = Infinity \quad (3)$$

Where S2 is the size of the secret message, and infinity because if we arrive to last row of the column of the binary value and we didn't finished from the embedding the secret message, Then we can start again from the first row of the column of the binary value.

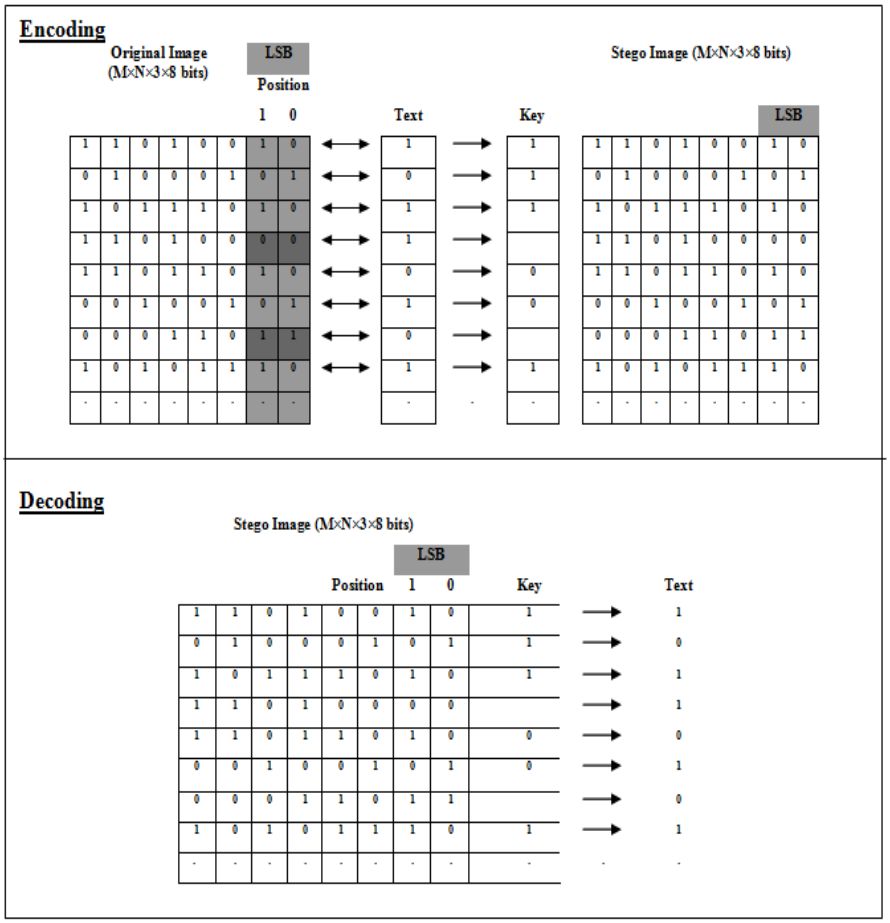


**Figure 5** The New Technique of Image Steganography (Spacing algorithm)

# 4. EXPERIMENTAL RESULTS

A MATLAB program has been created to simulate and develop this study. It called (Wa'el Steganography) according to the first author of this paper. Figure 6 shows the program window.
The used images in implementation process are coloured images (RGB images) of the type (JPEG, PNG and PMB) and grayscale images.

## 4.1. The Implementation

In implementation process, the colored image of Mysore-Palace has been used of size (800×600×3) pixels of type of (JPEG). The secret message that was used is shown in the figure 7. The number of characters of the secret message are (4054) and the number of bits are (28378) bits.

The first time of the implementation of the steganography process the secret message was one copy of the secret message, the second time of the steganography process the secret message was five copies of the secret message, the third time of the steganography process the secret message was ten copies of the secret message, the fourth time of the steganography process the secret message was fifteen copies of the secret message and the fifth time of the steganography process the secret message was twenty copies of the secret message.

### 4.1.1. Encoding

The following steps explain the encoding process of the (LSB+SPACING) algorithm using a Graphic User Interface (GUI) simulation program by Matlab:

- Press on the push button (open image) to select the Mysore-Palace image from the bath storage.
- Press on the push button (open text) to select the secret message from the bath storage that is saved as a .txt file. The secret message that we want to implement it on this study is shown in the figure 7, the text of the secret message will also appear in the text on the program window.
- Open the Steganography method list to choose the Steganography method (LSB+SPACING).
- At the end of the Steganography process, a dialog window will appear to ask the user to save the key in the bath storage. The key that has been generated according to the data of the secret message and the Mysore-Palace image using the (LSB+SPACING) method is shown in the figure 8.
- Then, the stego media will appear in the stego image area.
- The user can know the PSNR value between the original image and the stego image using the button PSNR.
- After that, the user can press on the push button (Save Stego Image) to save the stego image on the disk.


Figure 6. Simulation Results using Matlab GUI (Encoding)

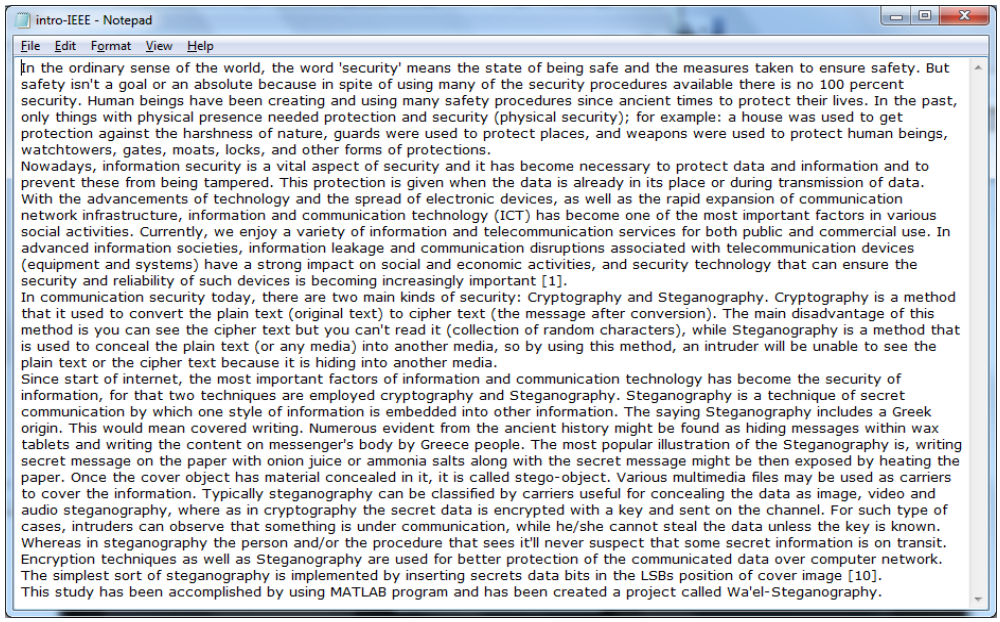


Figure 7. The secret message

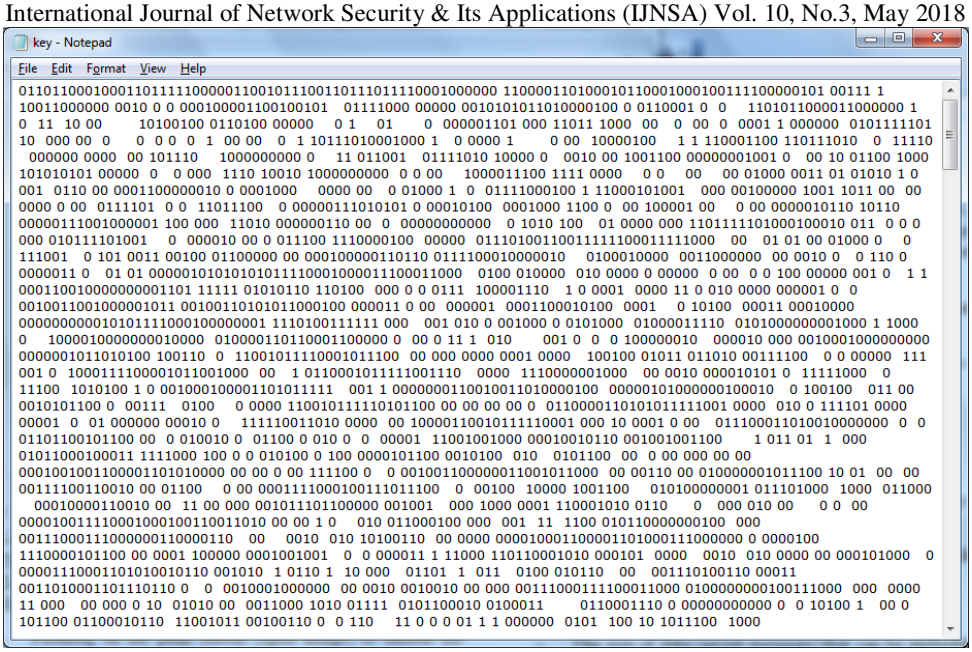


Figure 8. The key

### 4.1.2. Decoding

This process will be at the receiver, it extracts the secret message from the stego image based on the shared key between the sender and the receiver. the following steps show the dncoding process using the Matlab program that is shown in the figure 9:

- Press on the push button (Open Stego Image) to select the stego image from the bath storage.
- On pressing the push button (Show). The decoding process will start to extract the secret message from the stego image.
- A dialog window will appear to ask the user to choose the key from the disk storage.
- The user will choose the key from the disk storage as a text file.
- After that, the extracted secret message will appear in the text area on the program window.
- Finally, the user can save the secret message that is appeared in text on the program window by clicking on the push button (Save Text) to save it in the disk storage as a text file.

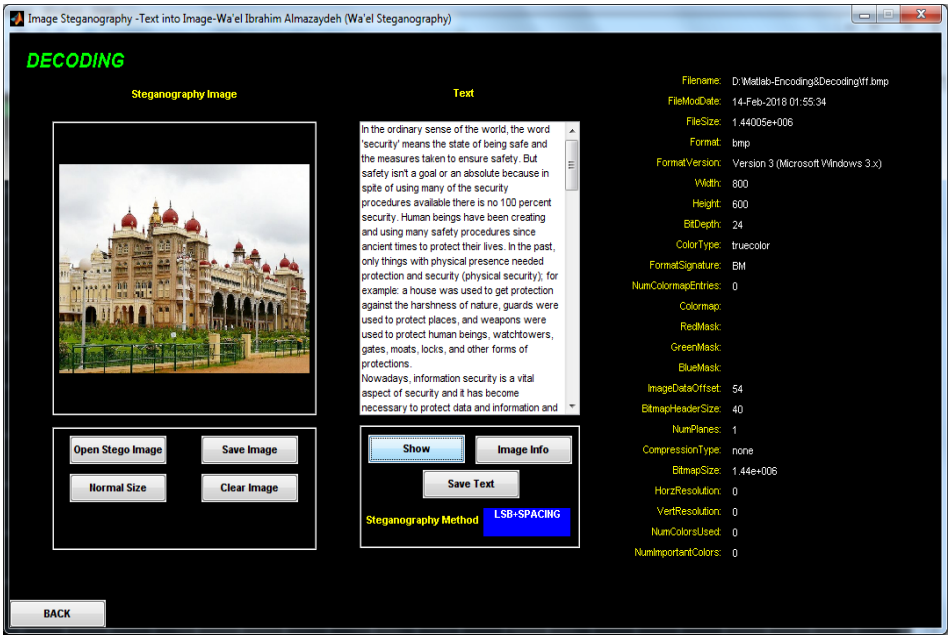


Figure 9. Simulation Results using Matlab GUI (Decoding)

## 4.2. The Results

The results of implementation of the steganography process according to the secret message that is shown in the figure 7 and Mysore-Palace image is shown in the Figure 7 by using the method: LSB and LSB+SPACING algorithms. Table 1 and Figure 10 show the results obtained after applying the algorithms.

Table 1. Comparison the PSNR between LSB and LSB+SPACING methods

| The Number of copies of the secret message | Number of characters | Number of bits | Steganography Method | |
|---|---|---|---|---|
| | | | LSB PSNR | LSB+SPACING PSNR |
| 1 | 4054 | 28378 | 68.2247 | Inf |
| 5 | 20270 | 141890 | 61.1791 | Inf |
| 10 | 40540 | 283780 | 58.1857 | Inf |
| 15 | 60810 | 425670 | 56.43 | Inf |
| 20 | 81080 | 567560 | 55.1794 | Inf |

According to the results obtained the PSNR values to the LSB+SPACING method are equal to the Infinity that is mean the no any bit change between the original image and the stego image and the size of data that can be hidden by the LSB+SPACING method is unlimited. While as the PSNR value to the LSB method is changed based the size of the secret message (if the size of the

secret message is increased the PSNR value is decreased) and the size of data that can be hidden by LSB is limited.
The maximum size of secret message bits that can be hidden in this Mysore-Palace image using the LSB algorithm is:

$$(800 \times 600 \times 3) - 27 = 1439973 \; Bits$$

The maximum size of the secret message bits that can be hidden in the Mysore-Palace image using image Steganography using SPACING algorithm is:

$$\inf \; Bits$$

Figure 10 shows the results obtained from the implementation process (as a diagram) for the same values in table 4.

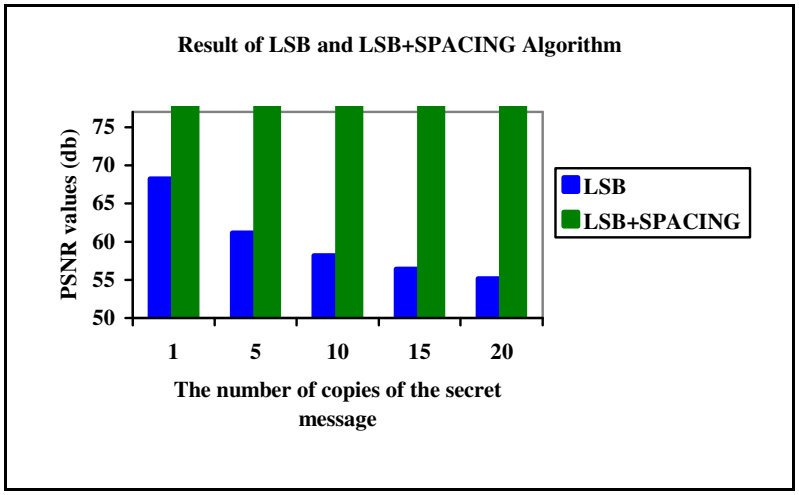


Figure 10. The SPNR Values of LSB and LSB+SPACING Algorithm.

## 5. CONCLUSIONS

This paper shows tow methods to hide a secret message in an image. The first one is the traditional method that is the Least Significant Bit (LSB) and the second one is the new method that is LSB+SPACING algorithm. However, the performance of the results has been compared using the PSNR values of individual algorithms; the results have proved that the new method (LSB+SPACING) is better than the Least Significant Bit (LSB) technique.

Table 1 and figure 10 show the results of the PSNR values of the LSB and LSB+SPACING method.

This is one of the experimental results in this research work and the work is under development to improve the algorithms and to reach to the best method of image Steganography to hide a secret message in an image. Also it is further intended to develop algorithms for secret sharing of patient data in medical images under telemedicine.

## REFERENCES


[1] Princymol Joseph, Vishnukumar S.. "A Study on Steganographic Techniques". Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015), IEEE.

[2] Rina Mishra, Praveen Bhanodiya. "A Review on Steganography and Cryptography". 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India, IEEE.

[3] Wa'el Ibrahim A. Almazaydeh, H. S. Sheshadri, S.K. Padma. "Enhancement of Image Steganography using a Dynamic Symmetric Key by Arithmetic Coding". International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), ISSN (Online) 2394-2320, Vol 4, Issue 12, December 2017.

[4] Prof. H. S. Sheshadri and Wa'el Ibrahim A. Almazaydeh, "Image Steganography using a Dynamic Symmetric Key", 2nd International Conference on Inventive Computation Technologies (ICICT – 2017), organized by RVS Technical campus during August 24-25 2017, IEEE, Coimbatore, India.

[5] Wa'el Ibrahim A. Almazaydeh, H. S. Sheshadri. "Image Steganography using LSB, LSB+Huffman Code, and LSB+Arithmetic Code". International Journal of Computer Applications, (0975 – 8887), Volume 155 – No 11, December 2016.

[6] Wa'el Ibrahim A. Al-Mazaydeh. "Image Steganography using LSB and LSB+Huffman Code". International Journal of Computer Applications, (0975 – 8887), Volume 99– No.5, August 2014.

[7] R Praveen Kumar, V Hemanth, M Shareef. "Securing Information Using Sterganoraphy". International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], IEEE.

[8] Dr. Saad Abdual azize AL_ani, Bilal Sadeq Obaid Obaid. "A Steganography Method to Embed Text in Image without Change Structure of Image". INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH, Volume 3 issue 1 January 2015 Page No.824-828 ISSN :2320-7167.

[9] Amanjot Kaur, Dr. Bikrampal Kaur. "Secure The Secret Information In An Image Using K-MM In Steganography". Journal of Multidisciplinary Engineering Science and Technology (JMEST), ISSN: 3159-0040, Vol. 2 Issue 8, August – 2015.

[10] Madhavi V.Kale, Prof. Swati A.Patil. "Text Hiding In Multimedia By Huffman Encoding Algorithm Using Steganography". International Journal of Advance Research in Science Management and Technology, Volume 2, Issue 1, January 2016.

[11] Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat. "A New Model for Hiding Text in an Image Using Logical Connective". International Journal of Multimedia and Ubiquitous Engineering, Vol.10, No.6 (2015), pp.195-202.

[12] Yun-Te Lin, Chung-Ming Wang, Wei-Sung Chen, Fang-Pang Lin, and Woei Lin. "A Novel Data Hiding Algorithm for High Dynamic Range Images". IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 19, NO. 1, JANUARY 2017.

[13] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain, K. Raja Sekhar. "Performance Evaluation Parameters of Image Steganography Techniques". International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016), April 06-07, 2016, R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India, 2016 IEEE.

[14] NELS PROVOS AND PETER HONEYMAN. "Hide and Seek: An Introduction to Steganography". IEEE Computer Society, Volume: 99, Issue: 3, May-June 2003.

[15] Dharmesh Mistry, Richa Desai, and Megh Jagad. "Hidden Data Transmission using Image Steganography". International Journal of Computer Applications, (0975 – 8887), Volume 130 – No.14, November 2015.

[16] Iain E. G. Richardson. H.264 and MPEG-4 Video Compression, The Robert Gordon University, Aberdeen, UK 2003.