Proceedings of the 2nd International Conference on Inventive Computation Technologies (ICICT 2017)
IEEE Xplore Compliant - Part Number:CFP17K52-ART, ISBN:978-1-5090-6697-1

Image Steganography using a Dynamic Symmetric Key

Prof. H. S. Sheshadri
PESCE, Mandya
hssheshadri@gmail.com

Wa'el Ibrahim A. Almazaydeh
Research Scholar
PET Research Foundation , PESCE, Mandya
Wael_mazaydeh@yahoo.com

Abstract

Steganography is the art of concealing one digital media within another digital media and retrieving the information afterwards. There are many examples of usage: image into image, text into image, video into voice, voice into video, etc. This paper concentrates on a method used for hiding text into image using Least Significant Bit (LSB), and using a symmetric key between sender and receiver to choose which bits are needed to be embeded the text to minimize the resolution between the original image and the stego-image. Further this paper also explains about the security issues to the stego-image. Also the comparision of the performance of the algorithms (PSNR) have been discussed.

KEY WORDS: Encryption, LSB and Zigzag sacking, Symmetric key, Stegonography.

1. INTRODUCTION

In the ordinary sense of the world, the word 'security' means the state of being safe and the measures taken to ensure safety. But safety isn't a goal or an absolute because in spite of using many of the security procedures available there is no 100 percent security. Human beings have been creating and using many safety procedures since ancient times to protect their lives. In the past, only things with physical presence needed protection and security (physical security); for example: a house was used to get protection against the harshness of nature, guards were used to protect places, and weapons were used to protect human beings, watchtowers, gates, moats, locks, and other forms of protections.

Nowadays, information security is a vital aspect of security and it has become necessary to protect data and information and to prevent these from being tampered. This protection is given when the data is already in its place or during transmission of data.

With the advancements of technology and the spread of electronic devices, as well as the rapid expansion of communication network infrastructure, information and communication technology (ICT) has become one of the most important factors in various social activities. Currently, we enjoy a variety of information and telecommunication services for both public and commercial use. In advanced information societies, information leakage and communication disruptions associated with telecommunication devices (equipment and systems) have a strong impact on social and economic activities, and security technology that can ensure the security and reliability of such devices is becoming increasingly important [1].

In communication security today, there are two main kinds of security: Cryptography and Steganography. Cryptography is a method that it used to convert the plain text (original text) to cipher text (the message after conversion). The main disadvantage of this method is you can see the cipher text but you can't read it (collection of random characters), while Steganography is a method that is used to conceal the plain text (or any media) into another media, so by using this method, an intruder will be unable to see the plain text or the cipher text because it is hiding into another media.

Since start of internet, the most important factors of information and communication technology has become the security of information, for that two techniques are employed cryptography and Steganography. Steganography is a technique of secret communication by which one style of information is embedded into other information. The saying Steganography includes a Greek origin. This would mean covered writing. Numerous evident from the ancient history might be found as hiding messages within wax tablets and writing the content on messenger's body by Greece people. The most popular illustration of the Steganography is, writing secret message on the paper with onion juice or ammonia salts along with the secret message might be then exposed by heating the paper. Once the cover object has material concealed in it, it is called stego-object. Various multimedia files may be used as carriers to cover the information. Typically steganography can be classified by carriers useful for concealing the data as image, video and audio steganography, where as in cryptography the secret data is encrypted with a key and sent on the channel. For such type of cases, intruders can observe that something is under communication, while he/she cannot steal the data unless the key is known. Whereas in steganography the person and/or the procedure that sees

it'll never suspect that some secret information is on transit. Encryption techniques as well as Steganography are used for better protection of the communicated data over computer network. The simplest sort of steganography is implemented by inserting secrets data bits in the LSBs position of cover image [10].

This study has been accomplished by using MATLAB program and has been created a project called Wa'el-Steganography.

2. RELATED WORK

The authors Wa'el Ibrahim A. Almazaydeh, and H. S. Sheshadri presented how to conceal information into an image by using three methods that concentrate on the compression of the data before hiding it into the image and then compare the results using Peak Signal to Noise Ratio (PSNR). The three methods that have been used here are Least Significant Bit (LSB), Huffman Code, and Arithmetic Coding.The performance analysis have been compared [12].

Sandeep Panghal, Sachin Kumar, Naveen Kumar presented LSB based Image Steganography. LSB based image Steganography is a good method of embedding sensitive information behind some cover media. LSB based Steganography in combination with AES will provide a good security model for hiding data. AES is preferred over DES due to its simplicity and its speed [2].

Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or indefectibility, capacity, and robustness) [3].

In paperref[4] the authors Wa'el Ibrahim A. Al-Mazaydeh explained the Steganography technique in the digital image, and it offers new technique for Steganography using (Least Significant Bit, Zigzag Scanning, and Huffman code). It contains two techniques for Steganography: The first is Least Significant bit, and the second is Least Significant bit and Huffman code. By comparing the results between the two techniques it concludes the LSB+HUFF method is better than LSB method to hide text into image

Pramendra Kumar, and Vijay Kumar Sharma presented the investigation of two security approaches, namely cryptography and steganography. Where the cryptography only change the format of the information that cannot be understood by any unauthorized user, the steganography hide the complete information in the cover media, so no one can easily identify that any message is hidden in the presented content. However both of these techniques provide the security to information but the standalone approach based of either of these techniques is not so good for practice. Therefore to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed [5].

Dr. Saad Abdual azize AL_ani, Bilal Sadeq Obaid Obaid proposed a new method of hiding data in the cover image. This algorithm is based on converting character to 6 bit, by using b-table compressed to 4 bit and from another side used similarly to value of cover pixel. The receiver gets value of location encrypted by RSA algorithm. There is no data embedded in the cover image [6].

Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat proposed a simple and an efficient model for calculating secret message that can be embed in an image. This proposed model used Connective Logical (CL) as an algorithm to calculate a new binary number of secret messages while the most significant bit (MSB) of each pixel was used as a key. MSB was 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 produce a new secret message. This new secret message would be embedded in the LSB of pixel. The implementation of this model can produce a low computational complexity of steganography because of the simplicity of the proposed algorithm [7].

Madhavi V.Kale , Prof. Swati A.Patil proposed steganographic system, Compress ratio is calculated by Huffman Encoding Algorithm. after that Text is hide in image, audio and Video by Least Substitution Method (LSB) and Encrypt by Using Advanced Encryption Standard Algorithm. On the another Hand Receiver receive that that hiding image, audio as well as Video as appear Original Image. After that Receiver Decrypt that Text by using Advanced Encryption Standard Algorithm (AES) and getting Text which is hide by Sender in image, audio as well as video [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].

NIELS PROVOS AND PETER HONEYMAN discusses existing steganographic systems and presents 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 [13].

Dharmesh Mistry, Richa Desai, and Megh Jagad showed that Steganography does not intend to take the

place of cryptography but rather support and supplement it. Consider that a message is initially encrypted and then hidden with a steganographic method, it provides a double layer of protection and reduces the chances of the hidden message getting detected [14].

Yun-Te Lin, Chung-Ming Wang, Wei-Sung Chen, Fang-Pang Lin, and Woei Lin presented a novel data hiding algorithm for HDR images encoded by the OpenEXR format. The proposed algorithm conceals secret messages in the 10-bit mantissa field in 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 concealed with the least pixel distortion. An aggressive bit encoding and decomposition scheme is introduced herein, which offers the benefit for concealing an extra bit in a pixel group without incurring pixel distortion. The influence of the message probability is analyzed, and the embedding capacity is further increased by taking advantage of the recommended bit inversion embedding scheme [15].

This study relies on the Least Significant Bit (LSB) because it is one of the most convenient and well known techniques that is being used for evolving image Steganography. In this paper, two techniques have been explained on how to hide a secret message within an image. The three methods are: Least Significant Bit (LSB), and a new method for Steganography based on LSB I called it wa'el algorithm. PSNR is used here to compare the results among the three techniques.

2.1 Steganography

Figure 1 shows the Steganography technique [4]:

- 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.

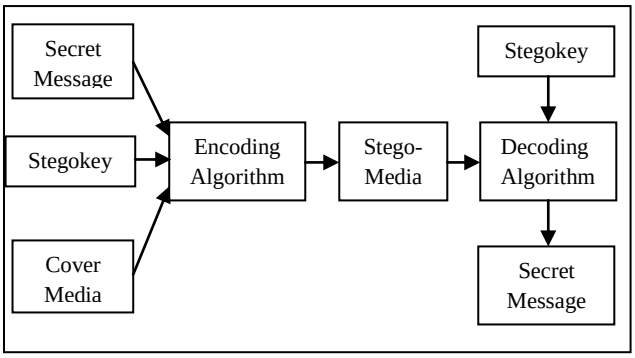

Fig 1: Steganography Technique [4]

2.2 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 paper, the ASCII code is used to convert each character of the secret message to the value of ASCII code.

2.3 Least Significant Bit (LSB)

The most common technique used for Steganography is the Least Significant Bit (LSB). This study used one bit of Least Significant Bit. It substitutes each bit of the binary text bit with one bit of each pixel in the original image. For example: if we have 8 bytes of data and we want to hide the number 195 which is represented in ASCII code as 11000011, we can use Least Significant Bit (LSB) technique. Figure 2 shows how the LSB technique can be used.

We shall Hide 195 which is represented as 11000011 in ASCII code by using one bit substitute:

Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
1000010**0** 1	1000011**0** 1	1000100**1** 0	1000110**1** 0
10000101	10000111	10001000	10001100
Byte 5	**Byte 6**	**Byte 7**	**Byte 8**
0111100**1** 0	0110010**1** 0	0100101**0** 1	0010011**0** 1
01111000	01100100	01001011	00100111

Fig 2: Least Significant Bit (LSB) Technique.

2.4 Zigzag Scanning

This study uses a zigzag scanning method to increase the security that can be achieved by using the Steganography technique. The pixels which will be used to embed the secret message bits are chosen through a method of zigzag scanning. The method of zigzag scanning is elaborated in figure 3 [4].

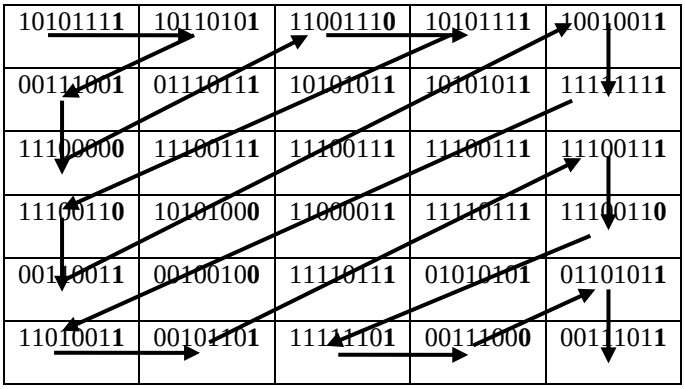

Fig 3: Zigzag Scanning

2.5 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 $(2^n - 1)^2$ (the square of the highest-possible signal value in the image, where n is the number of bits per image sample) [11].

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

"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" [11].

When the PSNR value is high, the change in the image resolution is low; and when the PSNR is low the change in the image resolution is high. So my goal is to get the high PSNR value.

3. METHODOLOGY

This paper shows two techniques: the first one is Least Significant Bit (LSB), and the second one is a new method for Steganography based on a secret key between the sender and the receiver. Here the authors have employed a method that uses a LSB to hide the data of specific bits. The results between the two methods have been compared with respect to the Peak Signal to Noise Ratio (PSNR) between the original and the encrypted data.

Steganography using LSB

In this method, the original image has been converted to a column of binary values for all pixels by using zigzag scanning with size equal to (M×8) where M is the number of pixels in the original image. In a parallel process, the secret message is converted to a row of binary values with size equal (1×K) where K is the number of bits in the secret message. We know that for each character in the secret message we need 7 bits.

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

$$S1 = (M \times N) - 27 \quad (2)$$

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

Figure 4 shows the methodology:

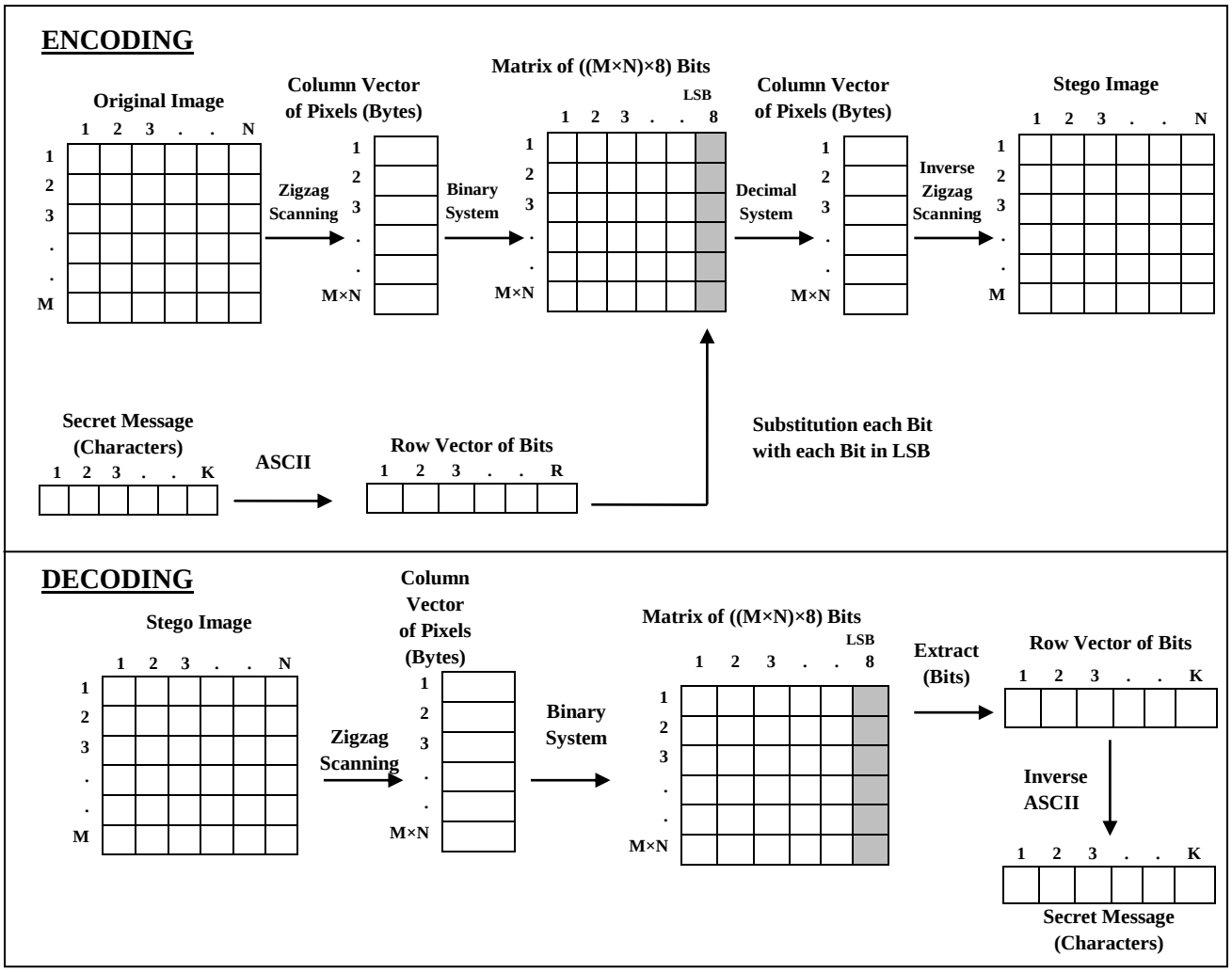

Fig 4: The Encoding and Decoding of this study.

3.1 Steganography using a new method

3.2 This is a new method of Steganography. It converts the image pixels to binary values using zigzag scanning with size equal to (M×8) where M is the number of pixels in the original image and 8 is the number of bits per pixel. Then, gets the two least significant bit of each pixel value according to the position, where the (LSB) position equal to 0 and the bit before (LSB) position equal 1. In a parallel process, the secret message is converted to a row of binary values with size equal (1×K) where K is the number of bits in the secret message. After this, each bit of the secret message is compared with the two bits of the (LSB) Figure 5 shows the encoding and decoding that has been done. There are three instances of matching process**:**

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), we will change the position 0 of the (LSB) to the value of that bit of the secret message and the key will be 0.At the end of this process, we get a vector of the key. The key refers to the position of the secret message in the stego-image. This key, is a shared secret key, between the sender and the receiver; and without this key, the receiver will not be able to get the secret message.This key is the base of this method and I have called it a 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 size of the data (Secret Message) that can imbed into the image by using this method can be calculated by using the following formula: is computed as the following:

$$S2 = (M \times N) - 27 \quad (2)$$

Where S2 is the size of the secret message, M is the number of rows in the image, N is the number of columns in the image, and the number 27 is: the first 7 bits from 1 to 7 are reserved to the Steganography type may be [1, 2, 3, …, 127], for example, when the

Steganography type equals 1 means that Steganography process is LSB, when the Steganography type 2 mens LSB-2 etc…

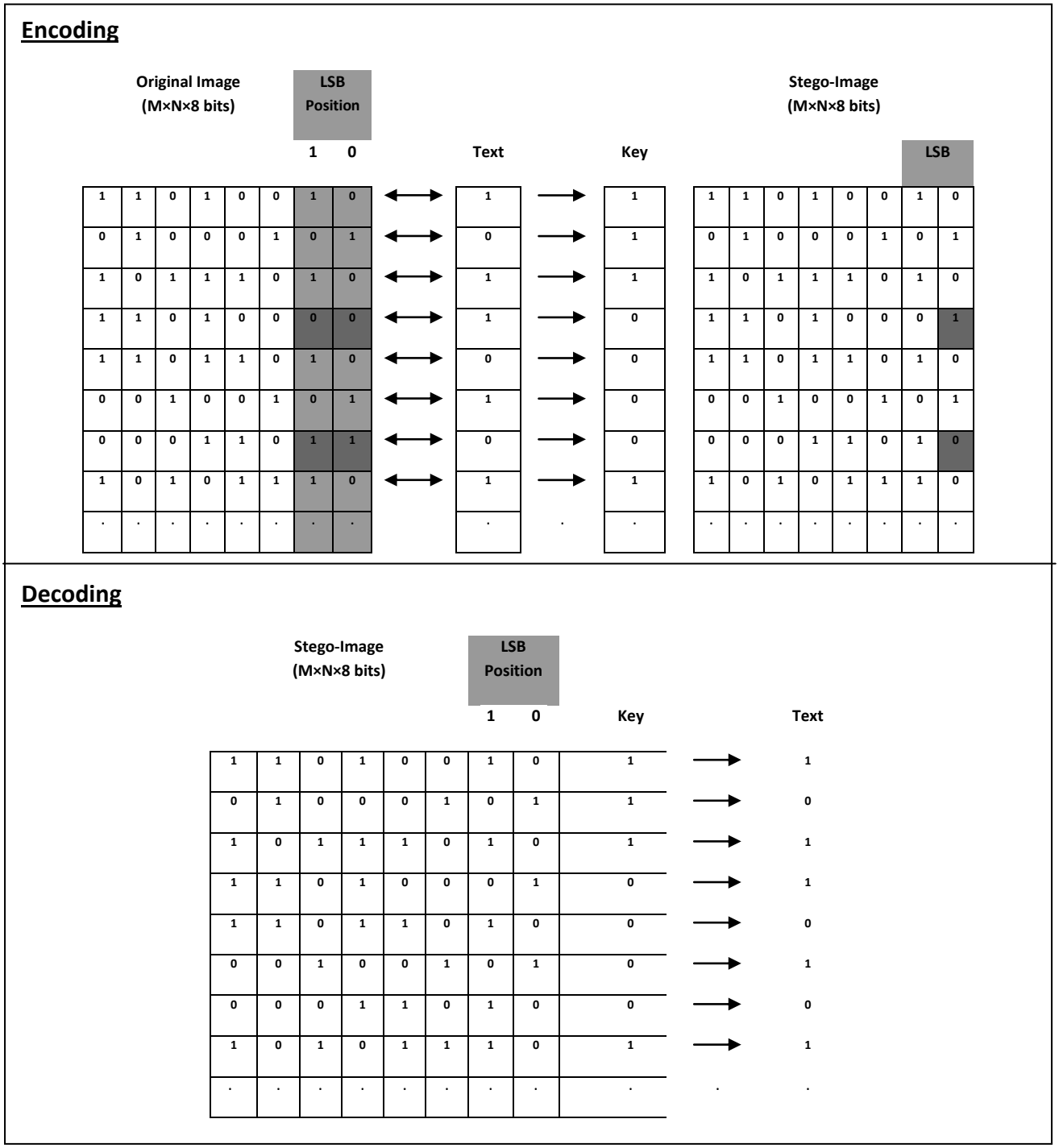

Fig 5: The New Technique for Image Steganography

4. Experimental Results

4.1 The Implementation

A MATLAB program has been developed by the authors for the verification of the algorithms with suitable examples like characters with an image data. A GUI has been created to simplify the simulation with certain practical examples.

Gray scale Petra image (as an example) has been used in this program with size equal to (1024×1024 pixels), and its type is jpeg. The technique is represented by the following steps:

- Convert the grayscale Petra image to binary values with zigzag scanning implementation.
- The size of data (secret message) that can be embedded in the image is calculated by using LSB method:

  (1024 × 1024) – 27 = 1048549 bits.
- The size of data (secret message) that can be embedded in this image is calculated by using the new method wa'el algorithm:

  ((1024 × 1024) – 27) / 2 = 524261 bits.
- As an example, the introduction to this paper has been selected in the place of a secret message. The count of the bits of the introduction is given by:
- 2136 characters × 7 bits = 14952 bits.
- Choose the Steganography method (LSB) or the new method Wa'el algorithm.
- Compare the results of the two methods using the PSNR.

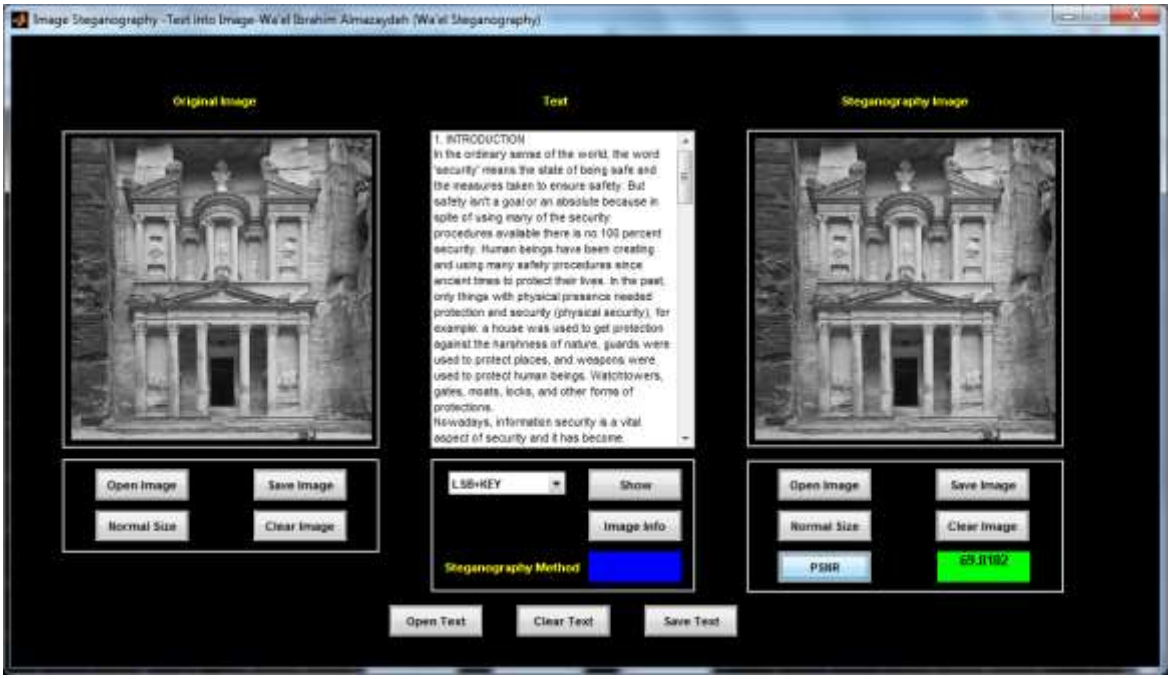

Fig 6:Simulation results using Matlab GUI

4.2 The Results

Table 1 shows the results after implementation of the two methods: LSB, LSB+KEY; the introduction to this paper has been selected in the place of a secret message to combare the results between the two methods.

Table 4: PSNR values of LSB and LSB+KEY methods

The Number of copies of introduction	Number of characters	Number of bits	Steganography Method	
			LSB PSNR	LSB+KEY PSNR
1	4073	28511	66.8017	69.8102
3	12219	85533	62.0194	65.0455
6	24438	171066	59.0098	62.0196
9	36657	256599	57.2485	60.2694
12	48876	342132	55.9999	59.027
15	61095	427665	55.0369	58.0561

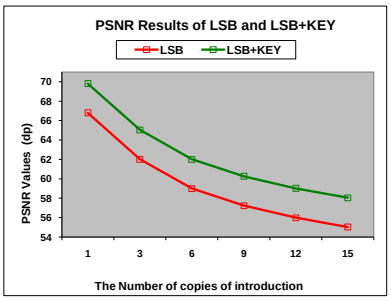

Fig 7: The PSNR of LSB and LSB+KEY

5. Conclusion

Figure 7 shows the results (as a diagram) for the same values in table 4.

This paper shows two techniques for Steganography: the first one is the well known technique which is known as Least Significant Bit, and the second one is the new technique with LSB +KEY.The performance of the results have been compared using the PSNR values of individual algorithms. It is noted that the LSB +KEY algorithm gives better output with respect to the PSNR values

This is one of the experimental results in this research work and the work is under development to improve the algorithms for still better code complexity and time complexity .Also it is further intended to develop algorithms for secret sharing of patient data in medical images under telemedicine.

Acknowledgement: The authors would like to thank the support extended by the VGST(Vision Group of science and Technology, Govt of Karnataka) for development of Medical Image Analysis Laboratory at the Dept of ECE of PESCE, Mandya during 2016-17. This laboratory is being used extensively for the research activities by PG and Research students.

6. REFERENCES

[1] Yu-Ichi Hayashi, Member, IEEE, Naofumi Homma, Member, IEEE, Takashi Watanabe, Member, IEEE, William O. Price, Member, IEEE, and William A. Radasky, Life Fellow, IEEE. Introduction to the Special Section on Electromagnetic Information Security. IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY, VOL. 55, NO. 3, JUNE 2013.

[2] Sandeep Panghal, Sachin Kumar, Naveen Kumar. Enhanced Security of Data using Image Steganography and AES Encryption Technique. International Journal of Computer Applications, (0975 – 8887) Recent Trends in Future Prospective in Engineering & Management Technology 2016.

[3] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi. Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012.

[4] 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.

[5] Pramendra Kumar, Vijay Kumar Sharma. Information Security Based on Steganography & Cryptography Techniques: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014.

[6] 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.

[7] 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.

[8] 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.

[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] Mamta Jain, Saroj Kumar Lenka. A Review of Digital Image Steganography using LSB and LSB Array. International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 11, Number 3 (2016) pp 1820-1824.

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

[12] 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.

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

[14] 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.

[15] 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.