MJRET
OPEN ACCESS
Multidisciplinary Journal of Research in Engineering and Technology
www.mjret.in
eISSN:2348-6953

Secrete Communication System Using Multi Image Steganography for Militart Application

Kokare Snehal, Mane Nikita,Wagh Mayuri,Kamthe Prasad,Prof..Sharad Adsure

Computer Departement, JSPM's BSIOTR, Wagholi,Pune, Maharashtra

Abstract : *Steganography is defined as the study of invisible communication .It usually deals with the way of hiding the information of the existence of the communicating data .It hides the facts of information. It is the process of hiding the data from one digital media to another digital media and recover the same information afterwards .This paper focuses on a process of hiding data to image by using the least significant bit(LSB) and the symmetric key between the sender and the receiver. Here we have to choose the bits that will get the minimum resolution between the original image and stego image. This paper further explains how the encryption and decryption processes are done.*

Keywords*: LSB, PSNR, Steganography and Dynamic Symmetric Key*

1. INTRODUCTION

Steganography is derived from the two Greek words Stego and Graphia, Stego means covering and graphia which means writing , thus the translation is covered writing or the hiding the data. The simplest way to do this process is by inserting the confidential data bits in LSB positions of original image.

Types of Steganography:

- Image to image
- Text to image
- Image to text
- Video to voice
- Voice to video

Image to Image :- In the image steganography the image is inserted within the another image by using the stego key.
Text to Image :- In this, the text is inserted within the image and sends the image with the help of the symmetric key.
Video to voice:- Hiding or embedding message in the video is like an art of hiding information because the sender is not only hiding but how that message is prevented open by anyone except receiver. Hiding message in the video is part of the art of hiding information, Video-based steganography techniques are same like image based.

In Today‘s world, Information security is the sensitive case of security and its getting necessary to protect the data from being tampered. For the data not being tampered, we are using this steganography technique. The protection should be required, when the data is already placed at the transmission.

2. STEGANOGRAPHY VS CRYPTOGRAPHY

Cryptography is the process used for the conversion of the plain text into cipher text by using the symmetric key and this process is known as the encryption. The main disadvantage of the cryptography is that the plaintext can be known and the cipher text is visible but we can‘t read it[4]. Steganography is a method that the plain text is concealed into the digital media .In this process the Trespasser can‘t be able to see the plaintext or the cipher text because it is concealing into the another media. The trespasser can‘t suspect if there is any confidential data that is existing. The steganography technique is used for the better security of the data over the computer network.

2.1 *Steganography Process*:

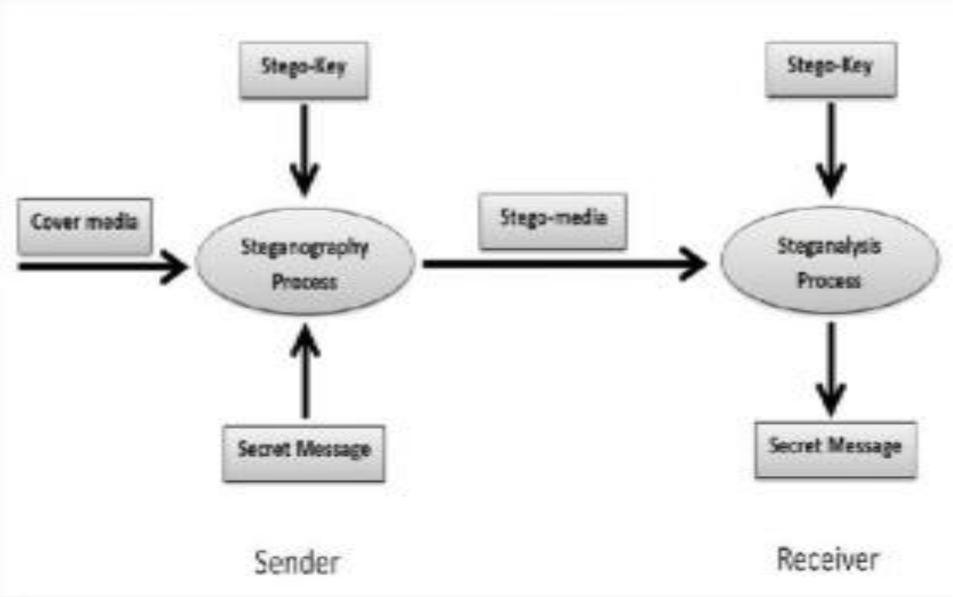


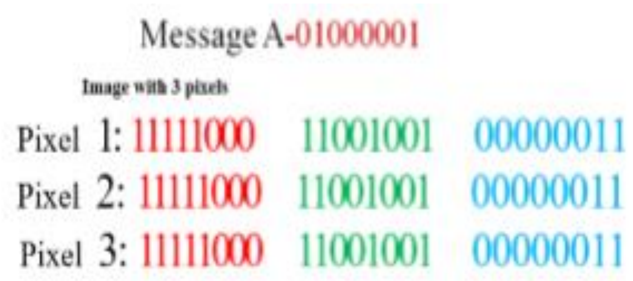
Fig. 1 Steganography Process

Secret Message: The data that you need to insert inside the digital media.. Stego-key: The key used in the Steganography process. Cover Media: The medium utilized in Steganography procedure, for example, picture, video and audio. Sender Algorithm: The technique utilized in this Steganography process. Stego-Media: The media coming about because of including the mystery message into a spread media utilizing Stego-key and encoding calculation. Receiver Algorithm: The technique used to extract the mystery message from Stego media utilizing Stego-key. symmetric key between the sender and receiver and by the Least Significant Bit. In this we will also see the how the encryption and decryption will be done.

3. IMPLEMENTATION

The well-known strategy that is utilized for steganography is the LSB. And additionally the prominent technique for present day, steganography is to utilize LSB of picture‘s pixel data. This investigation is utilized for one piece of the LSB. It inserts each piece of the double content piece with one piece of every pixel in the first picture. This strategy works when the record is longer than the message document and if picture is grayscale, when applying LSB strategies to every byte of a 24 bit picture, three bits can be encoded into every pixel[3] Example: We can use images to hide things if we replace the last bit of every color‘s byte with a bit from the message**.**

Image with 3 pixel



Message A-01000001

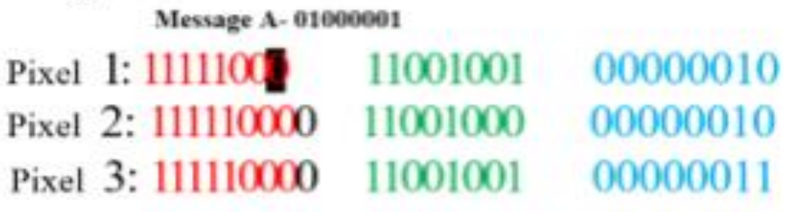
Image with 3 pixels

Pixel 1: 11111000 11001001 00000011
Pixel 2: 11111000 11001001 00000011
Pixel 3: 11111000 11001001 00000011

***Fig. 2** Message A before encryption*

Now we hide our message in the image.

Message A- 01000001



Message A- 01000001

Pixel 1: 11111001 11001001 00000010
Pixel 2: 111110000 11001000 00000010
Pixel 3: 111110000 11001001 00000011

***Fig. 3 Message** A after encryption*

3.1 ZIGZAG SCANNING:

For the purpose of more security we used Zigzag scanning method which is gained by Steganography technique. In this method the image pixels are used to hide the secret message by converting the secret message into bits. This Zigzag scanning uses patterns for hiding the secret message bits. This pattern will be only known to sender and receiver. By using this pattern, the receiver can retrieve his secret message.

3.2 PSNR:

PSNR means Peak Signal to Noise Ratio which can be calculated easily. It is used to compare the quality of compressed images and compressed videos. If the PSNR is high, the image resolution will be low. Our goal is to get high Peak Signal to Noise Ratio value so that our image resolution will not be affected. By getting this high PSNR value, there will not be much difference between primary image and the converted stego image.

4. METHODOLOGY

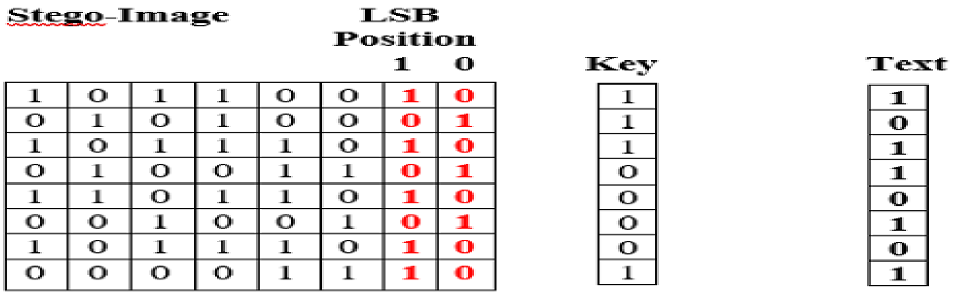
In this term paper we used the technique that is using the the data in an image. To rework the amusement with sure rational models, GUI has been made. Dull scale Petra picture (for example) which is of type jpeg, has been used in this program with size proportional to (1024×1024 pixels). The framework is addressed by going with advances: -The grayscale picture is to be converted into binary values by using the zigzag Scanning. - LSB technique is used to compute the degree of data (confidential message) that can be embedded in the image: (1024 × 1024) – 27 = 1048549 bits. - The degree of data (confidential message) that can be embedded in this image is computated by using the new system wa'el computation:

((1024 × 1024) – 27)/2 = 524261 bits. - for an example, the introduction to this paper has been picked in the spot of a secret message. The check of the bits of the introduction is given by: - 2136 characters × 7 bits = 14952 bits. - Choose the Steganography method (LSB). By comparing the results of both the methods using PSNR[6].Symmetric key between the sender and receiver and by the Least Significant Bit. In this we will also see the how the encryption and decryption will be done.

4.1 Steganography using LSB and Symmetric Key:

In this framework to the rejection of everything else we need to change over the picture pixels to Binary attributes by utilizing Zigzag Scanning by size=R*S*8 where R is the measure of lines in picture and S is count of sections and 8 is number of bits for each pixel. Eventually to get the last two bits of every pixel where LSB position is 0 and bit before the LSB is 1. While doing this method, meanwhile convert the riddle message(which you need to hide away) into coordinated qualities with size equivalent to1*N where N is count of bits in the mystery message. Coming about to changing over the picture pixels and secret message, straight forwardly we will encourage the mystery message two fold bits with the two bits of LSB. There are 3 steps in this process[5]. 1. If the confidential message bit equals with ―0‖th position of the LSB, then the key value will be "0". 2. In this process, if the confidential message bit equals with position ―1‖ of the LSB, then the key value will be "1". 3. In this process, if the confidential message bit doesn't equals with both position 1 of LSB and position 0 of LSB, by then the key value will be "0". After this strategy we will get the key. This key will be stegokey between the sender and receiver. Without having this stego-key, the receiver won't be able to interpret the confidential data. This stego-key will propose the Position of puzzle data in the stego-picture. This stego-key is basic for this framework. This key is called as Dynamic Symmetric key in light of how the key will be changed subject to the picture we will utilize the key for this in like manner, the extent of the secret message. By taking this model we will indicate how the encryption and the decryption methods are finished. In the below example I have taken the text as 181 and then I converted the text value 181 into binary value 10110101.Now using this text value I have calculated the key value. This key will be used for the both encoding and decoding processes**.**

4.2 Encoding:



Stego-Image						LSB Position		Key	Text
						1	0		
1	0	1	1	0	0	1	0	1	1
0	1	0	1	0	0	0	1	1	0
1	0	1	1	1	0	1	0	1	1
0	1	0	0	1	1	0	1	0	1
1	1	0	1	1	0	1	0	0	0
0	0	1	0	0	1	0	1	0	1
1	0	1	1	1	0	1	0	0	0
0	0	0	0	1	1	1	0	1	1

Fig 4 : Encoding Process

4.3 Experimental Results:

A MATLAB program that has been made by the makers for the computations check with suitable models like characters with the data in an image. To rework the amusement with sure rational models, GUI has been made. Dull scale Petra picture (for example) which is of type jpeg, has been used in this program with size proportional to (1024×1024 pixels). The framework is addressed by going with advances: -

The grayscale picture is to be converted into binary values by using the zigzag Scanning. - LSB technique is used to compute the degree of data (confidential message) that can be embedded in the image: (1024 × 1024) – 27 = 1048549 bits. - The degree of data (confidential message) that can be embedded in this image is computated by using the new system wa'el computation: ((1024 × 1024) – 27)/2 = 524261 bits. - for an example, the introduction to this paper has been picked in the spot of a secret message. The check of the bits of the introduction is given by: - 2136 characters × 7 bits = 14952 bits. - Choose the Steganography method (LSB). By comparing the results of both the methods using PSNR[6].

1. ENCODING

- The advancements will clarify the encoding procedure of the (LSB+SPACING) calculation utilizing a Graphic User Interface (GUI) reproduction program by Matlab:
- Press on the push catch (open picture) to choose the Mysore-Palace picture from the drive. Press on the push catch (open content) to choose the mystery message from the local drive that is spared as a .txt record.
- The confidential message that we need to execute it on this process is appeared in the figure, the content of the confidential message will likewise show up in the content on the program window. - Open the Steganography technique rundown to pick the Steganography strategy (LSB+SPACING).
- At the finish of the Steganography procedure, an exchange window will seem to request that the client spare the key in the shower stockpiling.
- The key that has been produced by the information of the confidential message and the Mysore-Palace picture utilizing the (LSB+SPACING) strategy is appeared in the figure 8. Then, the stego media will show up in the stego picture.
- The client can realize the PSNR esteem between the first picture and the stego picture utilizing the catch PSNR.
- After that, the client can push on the push catch (Save Stego Image) to spare the stego picture on the plate.

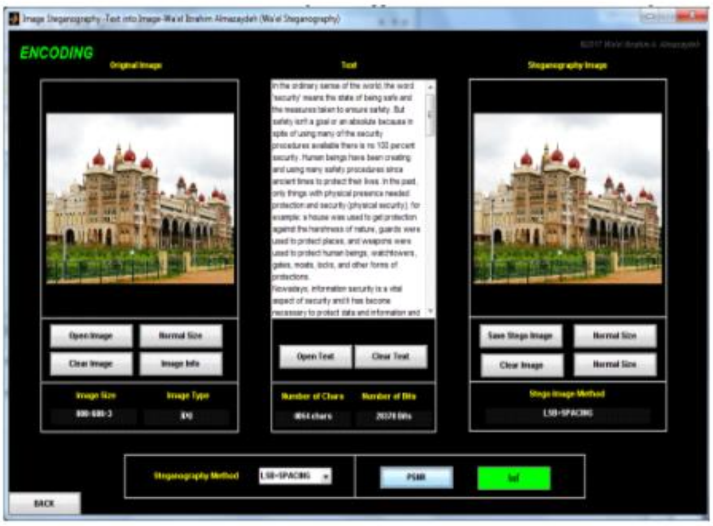


Image Steganography -Text into Image-Wa'el Ibrahim Almazaydeh (Wa'el Steganography)

ENCODING

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

Image Size: [illegible]
Image Type: jpg
Number of Chars: [illegible] chars
Number of Bits: [illegible] Bits
Stego Image Method: LSB+SPACING
Steganography Method: LSB+SPACING

Fig. 5 Encoding Process

Key:

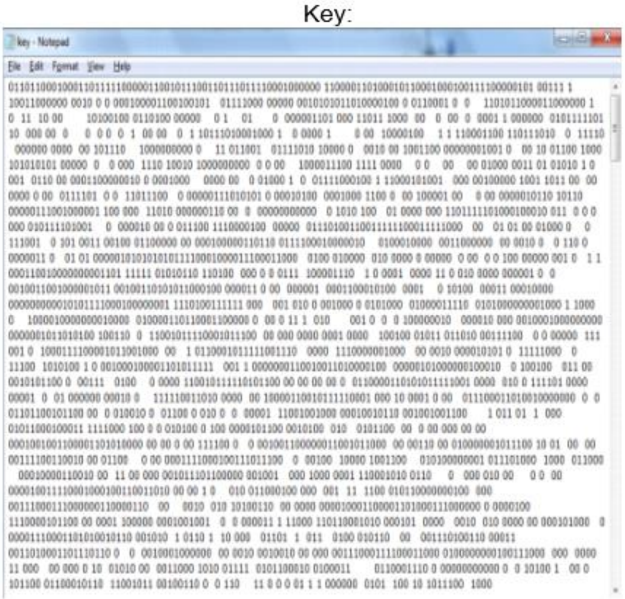
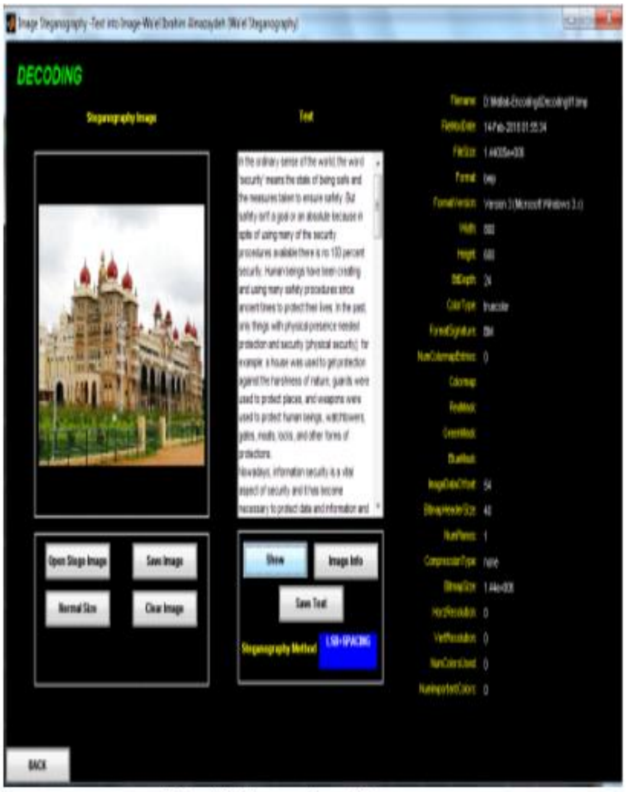


Fig. 6 *Key Value for the encryption process*

6. DECODING

This strategy will be at the recipient, it expels the confidential message from the stego picture subject to the common key between the sender and the receiver. Going with advancements we will show the decoding technique using the Matlab program that is showed up in the figure :

- Press on the push get (Open Stego Image) to pick the stego picture from the shower accumulating.
- On crushing the push get (Show). The unwinding system will start to remove the confidential message from the stego picture.
- A trade window will appear to demand that the customer pick the key from the circle amassing.
- The customer will pick the key from the plate storing as a substance report.



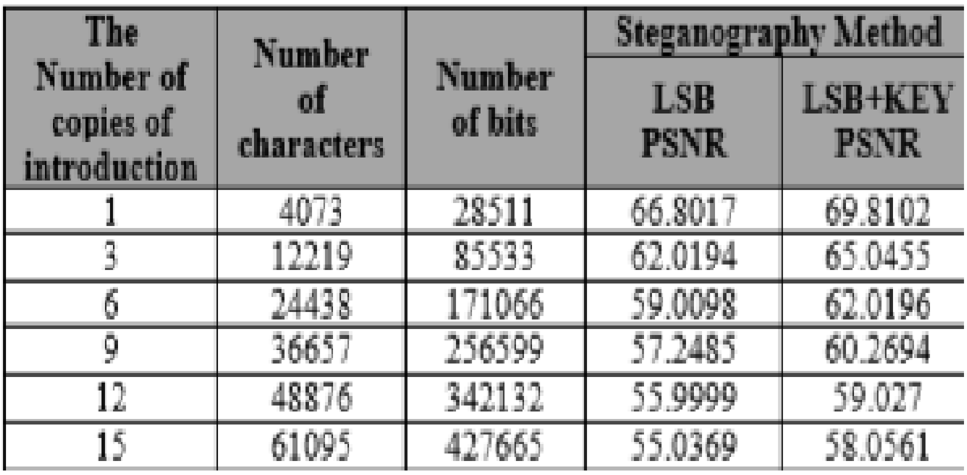
In the ordinary sense of the world, the word 'security' means the state of being safe and the measures taken to ensure safety. But safety isn't a goal or an absolute because in spite of using many of the security procedures available there is no 100 percent security. Human beings have been creating and 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

Filename	D:\Matlab-Encoding\Decoding\1.bmp
FileModDate	14-Feb-2018 01:55:34
FileSize	1.4405e+006
Format	bmp
FormatVersion	Version 3 (Microsoft Windows 3.x)
Width	800
Height	600
BitDepth	24
ColorType	truecolor
FormatSignature	BM
NumColormapEntries	0
Colormap	
RedMask	
GreenMask	
BlueMask	
ImageDataOffset	54
BitmapHeaderSize	40
NumPlanes	1
CompressionType	none
BitmapSize	1.44e+006
HorzResolution	0
VertResolution	0
NumColorsUsed	0
NumImportantColors	0

Fig. 7 *Decoding Process.*

7 . RESULTS

The values of PSNR for 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. 8 *Results*

8. CONCLUSION & FUTURE SCOPE

This paper demonstrates two structures for Steganography: Initially it is the striking rationality which is also known as Least Significant Bit(LSB), and the second one is the latest system with LSB+KEY. The results executions have been looked up for the estimations of PSNR with individual checks. It is seen that the [7] calculation of LSB+KEY gives better demands concerning the PSNR regards. This is one of the investigated results in this work and still the work is in its head-way to improve the computations for still better code unconventionality and time complexity nature. Also it is expected furthermore to make estimations in amaze sharing of patient data in healing pictures under telemedicine.

REFERENCES:

[1] J. Fridrich and M. Goljan, ―Digital image steganography using stochastic modulation‖, SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.

[2] T. Morkel, J. H. P. Elloff, M.S. Olivier, ―An Overview of Image Steganography‖.

[3] Provos, N. &Honeyman, P., ―Hide and Seek: An introduction to steganography‖, IEEE Security and Privacy Journal, 2003.

[4] Johnson, N.F. &Jajodia, S., ―Exploring Steganography: Seeing the Unseen‖, Computer Journal, February 1998.

[5] N. Provos and P. Honeyman, ―Detecting Steganographic Content on the Internet,‖ Proc. 2002 Network and Distributed System Security Symp., Internet Soc., 2002.

[6] D. McCullagh, ―Secret Messages Come in .Wavs,‖ Wired News, Feb. 2001, www.wired.com/news/politics/ 0,1283,41861,00.html.

[7] Trivedi M C Sharma S and Yadav V K 2016 Analysis of several image steganography techniques in spatial domain: a survey. In; Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS ‗16). ACM. Article 84.

[8] Wu D-A and Tsai W-H 2003 A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett. 24(9– 10):1613–1626

[9] Wu H-C, Wu N I, Tsai C S and Hwang M S 2005 Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings Vision, Image and Signal Processing 152: 611–615

[10] Anand J V and Dharaneetharan G D 2011 New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security. Proceedings of the 2011 In: International Conference on Communication, Computing 474–47[

[11] Jain M and Lenka S K 2016 A review of digital image steganography using LSB and LSB array. Int. J. Appl. Eng. Res. 11(3):1820–1824

[12] Luo W, Huang F and Huang J 2010 Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inf. Forensics Secur 5(2): 201–214

[13] X. Zhang and S. Wang, ―Vulnerability of pixel-value differencingsteganography to histogram analysis and modification for enhancedsecurity,‖ Pattern Recognit. Lett., vol. 25, pp. 331–339, 2004

[14] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, pp. 469-474, 2004