ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 6, Issue 10, October 2019

Image Steganography using Canny Magic LSB Substitution Method

[1] Aye Thu Hlaing, [2] Mya Thidar Myo Win

[1][2] Department of Computer Engineering and Information Technology, Mandalay Technological University, Mandalay

[1] ayethuhlaing@mtu.edu.mm, [2] myathidarmyowin@mtu.edu.mm

Abstract: Steganography is the art of concealing the communication existence by hiding the secret message in cover media. The major goals of steganography are undetectability, robustness and embedding capacity. This paper aims to study image steganography using Canny Magic LSB Substitution Method (CM-LSB-SM) for hiding secret bits in Least Significant Bits (LSBs) (1-LSB and 2-LSB). Firstly, cover image is separated into three components (Red-Green-Blue) images and is detected the edge pixels using Canny Edge Detection. Then, the secret message is embedded in the location of Magic Matrix sequence of the three edge images by applying LSB Substitution method. Their performance is measured using PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), EC (Embedding Capacity) and Histogram. The findings indicate that the CM-LSB-SM (2-2-2) method supplies a relatively high embedding capacity in the higher edge pixel image.

Index Terms – Canny Magic LSB Substitution Method, Embedding Capacity, Least Significant Bits, Steganography

1. INTRODUCTION

Steganography is the art of passing the information in the manner that the very existence of the message is unidentified. The goal of steganography is to avoid doubt to the transmission of hidden message, such that it is highly secured. Hiding a message with steganography methods decreases the chance of a message being discovered. The word steganography is originated from Greek words which mean “Hidden Writing”. It has been used in various forms for thousands of years [1]. In the 5th century, BC Histaiacus shaved a slave’s head, tattooed a message on his head and the slave was dispatched with the message after his hair grew back. The slave could travel freely as no one can detect the presence of the hidden message on his head.

There are five different types of steganography based on the carrier object that is applied for embedding the secret message. The carrier objects are images, text, videos, audios or network protocol packets. Image steganography is also a technique which is used to hide secret message within an image. The binary bit of the secret message is hidden in the binary of image and this slightly affects the intensities of color or brightness which is not detectable by naked human eyes. Image steganography techniques can be divided into two groups: Spatial Domain and Frequency Domain. Spatial domain techniques embed messages in the intensity of the pixels directly, while for frequency domain techniques, images are first transformed and then the message is embedded in the image [2].

Salleh, M. [3] presented an information hiding method that can be extended to copyright protection for digital media and data for confidentiality. The Internet as a whole does not use secure links, thus information in transit may be susceptible to interception as well. Previous work has discussed how to pass information in a manner that the very existence of the message is unknown to repel attention of the potential attacker. The system improved the LSB technique by randomly scattering the bits of the message in the image and thus making it harder for illegal people to remove the original message.

In 2014, Muhammad et al. studied a new Cyclic Steganographic Technique (CST), which embedded the secret data in the LSB of cover image pixels in a randomized cyclic manner [4]. The method improved its robustness and randomly dispersed the secret data inside the cover image pixels. The method was tested with histogram analysis, PSNR and MSE to prove its efficiency. The major weakness of the method was its vulnerability to different image processing and statistical attacks such as image cropping, scaling and noise attacks.

One of the major embedding strategies in the spatial domain is edge adaptive embedding technique. In the spatial domain, direct modification of pixels allows a visual distortion if these pixels belong to smooth areas in the image. Thus, the edge adaptive embedding schemes are developed to keep the minimum image distortion. Similarly, edge adaptive steganographic methods are favorite to provide high imperceptibility [5]. Shyla, S. I. [6] in 2016, used the Public key steganographic technique to improve the security of the copyright. The objective of this work is to compare the performance of the public key

Steganography in three different methods such as Edge Adaptive Scheme, Multibit Assignment Scheme, and Low Distortion Transform Scheme. The performance of these methods is compared by using the PSNR (Peak Signal-to-Noise Ratio), Embedding Capacity and Embedding time taken values. From the comparative study, the performance of the public key Steganography scheme in Low Distortion Transform is better than others.

In addition, several existing methods having good visual image quality suffer from the low embedding capacity. In this paper, it is firstly considered to provide high embedding capacity and better quality stego-image by combing Magic LSB Substitution method with Canny Edge Detection. The main contributions of this paper are:

1) Cover image is separated into three (R-G-B) images to improve the embedding capacity.
2) Canny Edge Detection method is used to search edge areas of the image.
3) Secret message is embedded in the edge regions of three images using Magic-LSB-Substitution Method which further makes the data extraction more challenging.

The rest of the paper is organized as follows. Section 2 discusses the background theories of proposed system. Section 3 explains the detail process of proposed work. The experimental results are discussed in Section 4. Section 5 presents the conclusion of the paper.

II. BACKGROUND THEORY

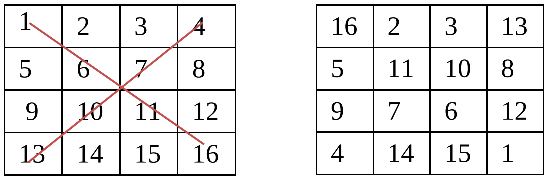
In this research, the proposed method is combined three existing algorithms such as Magic Square Matrix, Canny Edge Detection and LSB Steganography.

A. Magic Square Matrix

Magic Square Matrix (MGM) is employed to embed the secret message in this location series. This series makes its extraction more challenging for attackers. A n-by-n magic square is an array containing the integers from 1 to n^2, arranged so that each of the rows, each of the columns, and the two principal diagonals have the same sum. The sum is called magic constant (M) [7]. The magic sum has a constant dependent on the order n, is calculated by the Equation 1. The magic sum for order 4 is 34.

$$M = \frac{n*(n^2+1)}{2} \qquad (1)$$

A 4 by 4 MGM is a doubly even magic square which is a multiple of four. To make a 4 by 4 MGM, the numbers 1 through 16 is written from left to right. The numbers in the diagonals (the red lines) are turned over. The number 16 and 1, 6 and 11, 13 and 4, 10 and 7 are swapped so that the magic sum will be 34 [8]. The MGM of order 4 is demonstrated in Fig. 1.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Fig.1 MGM of order 4

The properties of MGM are as follows:

1. Magic matrix contains unique numbers (non-repeated).
2. The numbers inside a magic matrix are not greater than the product of rows and columns. (3*3 = 9)
3. The sum of all rows, columns and its diagonals are equal to the same number.

B. Final Stage Canny Edge Detection

Canny is one of the popular edge detection algorithms, which was invented by John Canny [9] in 1986. Canny edge detection has the advantage of being able to detect the edge of the original image with a small error tie so as to obtain the edge of the optimal image. This detector has been widely used in various image processing algorithms that require edge detection. Performance of edge detection is highly reliant on the threshold value used [10]. This makes it very popular and widely applied because it successfully supplied standardized localization solutions and complex mathematical calculations to collect smoothing filters. Canny can also reduce many inputs to a certain edge [11].

C. LSB Steganography

Steganography is a method used to hide data in a file with the intention to mislead the human vision system. LSB is a method in the highly popular spatial domain used in steganography. LSB is applied in an approach to alter the smallest bit value of image pixels by changing them directly [12]. LSB is traditionally done by changing the smallest bit values in a sequential order. When there is an image pixel value {255, 125, 200, 90} and there is a message with a value of 10, then the steps taken to insert the message are as follows:

1) First, convert the pixel values of images and messages into bit numbers
   Cover {255: 11111111 | 125: 01111101 | 200: 11001000 | 90: 01011010},

Message {10: 1010}.

2) Next, change the smallest bit of image pixel value with each bit value of the message.

Thus, the Stego’s bits becomes {11111111 | 01111100 | 11001001 | 01011010}.

3) Finally re-convert pixel image bit value into decimal number.
The decimal value of Stego-pixels becomes {255 | 124 | 201 | 90}.

A steganography research using LSB method is very easy, so this method is also very predictable and risky anymore. But until now this method is still being considered to increase the visual quality and safety. This is due to the benefit possessed by LSB in good imperceptibility quality, so the human sensory system cannot detect small changes that occur. For that reason, to improve the quality, payload, and security of message insertion, LSB is combined with several methods, such as insertion in edge areas [13], cryptographic techniques, adaptive and dynamic LSB [14], and so on.

III. PROPOSED WORK

In this section, the proposed method is presented in detail. Two embedding algorithms of Canny Magic LSB Substitution Method are firstly discussed. Then, two extraction algorithms of Canny Magic LSB Substitution Method are also described.

1) Embedding Algorithm: The step by step procedures of the embedding algorithms are explained below.

```
Embedding Algorithm 1: Canny M-LSB-SM (1-1-1)
Step 1: Read the Cover Red Green Blue (RGB) image
        and secret message
Step 2: Find the edge point location from the cover
        image using Canny Edge Detection
Step 3: Separate Each Colour Components from Cover
        Image such as R-Colour Image, G-Colour
        Image and B-Colour Image.
Step 4: Generate a magic matrix (MGM) of size equal
        to the size of the cover image
Step 5: Set magic_index = 1, i = 0
        While magic_index <= size of MGM and i <=
        size of message do
          a. Find the magic_index of a particular
             message bit in MGM (show the location)
          b. If this magic_index in the R-G-B images
             is the edge pixel location, then
               i.  Replace the 1LSB of the pixel at that
                   particular index in R-G-B images
               ii. i = i +1
          c. magic_index = magic_index +1
Step 6: Combine all Stego R-G-B images for
        display.
```

```
Embedding Algorithm 2: Canny M-LSB-SM (2-2-2)
Step 1: Read the Cover RGB image and secret
        message
Step 2: Find the edge point location from the cover
        image using Canny Edge Detection
Step 3: Separate Each Colour Components from Cover
        Image such as R-Colour Image, G-Colour
        Image and B-Colour Image.
Step 4: Generate a magic matrix (MGM) of size equal
        to the size of the cover image
Step 5: Set magic_index = 1, i = 0
        While magic_index <= size of MGM and i <=
        size of message do
          a. Find the magic_index of a particular
             message bit in MGM (show the location)
          b. If this magic_index in the R-G-B images
             is the edge pixel location, then
               i.  Replace the 2LSB of the pixel at that
                   particular index in R-G-B images
               ii. i = i +2
          c. magic_index = magic_index +1
Step 6: Combine all Stego R-G-B images for
        display.
```

The embedding procedure of the sender site is shown in Fig. 2.

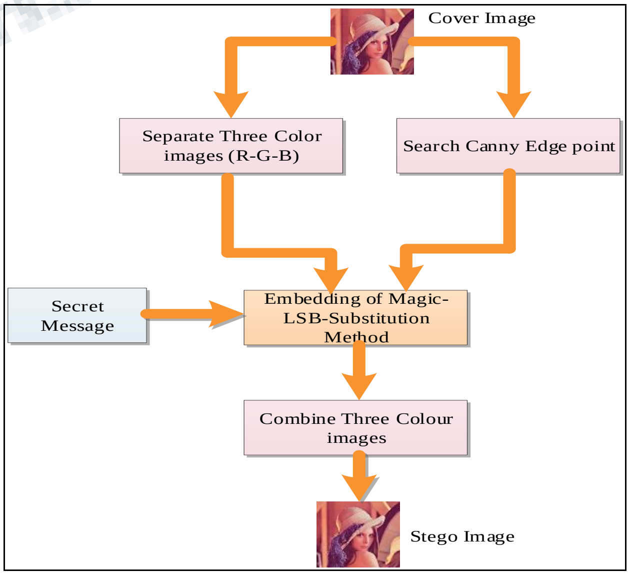

Cover Image
Separate Three Color images (R-G-B)
Search Canny Edge point
Secret Message
Embedding of Magic-LSB-Substitution Method
Combine Three Colour images
Stego Image

Fig. 2 Embedding Procedure of the sender site

2) *Extraction Algorithm:* The step by step procedure of the extraction algorithms are discussed below.

```
Extraction Algorithm 1: Canny M-LSB-SM (1-1-1)
  Step 1:  Read the Stego RGB image
  Step 2:  Find the edge point location from the Stego
           image using Canny Edge Detection
  Step 3:  Separate Each Colour Components from Stego
           Image such as R-Colour Image, G-Colour
           Image and B-Colour Image
  Step 4:  Generate a magic matrix (MGM) of size equal
           to the size of the stego image
  Step 5:  Set magic_index = 1, i = 0
           While magic_index <= size of MGM and i <=
           size of message do
           a.  Find the magic_index of a particular
               message bit in MGM (show the location)
           b.  If this magic_index in the R-G-B images
               is the edge pixel location, then
               i.   Extract the 1LSB of the pixel at that
                    particular index in R plane, G plane
                    and B plane
               ii.  i = i +1
           c.  magic_index = magic_index +1
  Step 6: Get the secret message
```

```
Extraction Algorithm 2: Canny M-LSB-SM (2-2-2)
  Step 1:  Read the Stego RGB image
  Step 2:  Find the edge point location from the Stego
           image using Canny Edge Detection
  Step 3: Separate Each Colour Components from Stego
           Image such as R-Colour Image, G-Colour
           Image and B-Colour Image
  Step 4:  Generate a magic matrix (MGM) of size equal
           to the size of the stego image
  Step 5:  Set magic_index = 1, i = 0
           While magic_index <= size of MGM and i <=
           size of message do
           a. Find the magic_index of a particular
              message bit in MGM (show the location)
           b. If this magic_index in the R-G-B images is
              the edge pixel location, then
               i.   Extract the 2LSB of the pixel at that
                    particular index in R plane, G plane
                    and B plane
              ii.   i = i +2
           c.  magic_index = magic_index +1
  Step 6: Get the secret message
```

The extraction procedure of the receiver site is shown in Fig. 3.

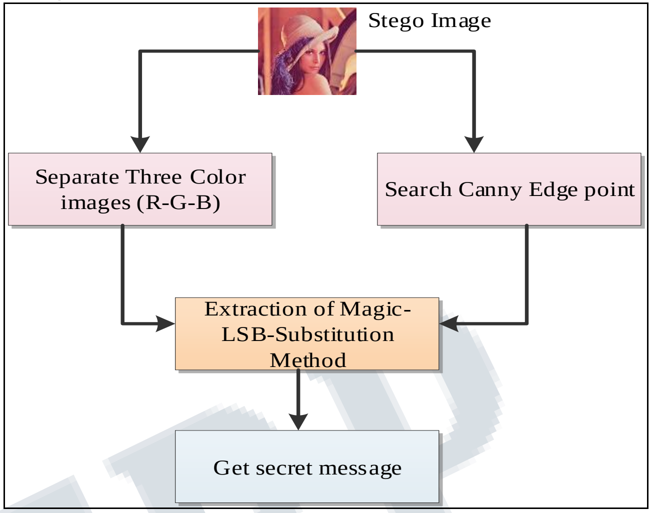

Stego Image
Separate Three Color images (R-G-B)
Search Canny Edge point
Extraction of Magic-LSB-Substitution Method
Get secret message

Fig. 3 Extraction Procedure of the receiver site

IV. RESULTS AND DISCUSSION

The image quality of the proposed technique has measured by using PSNR, MSE and Histogram. Five images of size 256 x 256 are used as test images in our experiments shown in Fig. 4.

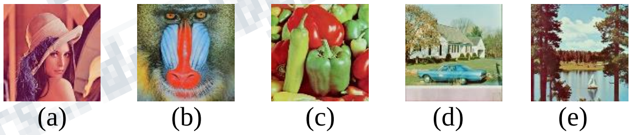


Fig. 4: Standard 256*256 cover images (a) Lenna (b) Baboon (c) Pepper (d) House (e) Sailboat

For implementation, NetBeans IDE 7.4 with Java has used on Windows. Secret message embedded on the LSB of pixels in three color (R-G-B) images and selection of pixels for hiding in cover image has done by using the Magic Matrix and the Canny Edge Detection. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the standard measures for finding the difference between the original cover image and the stego image. High PSNR value represents that the cover image has small distortion after embedding. Low PSNR value indicates the poor visual quality of the cover image.

TABLE I Results of PSNR and MSE Values of Five Images

Cover image (256*256)	Message size (bytes)	CM-LSB-SM (1-1-1)		CM-LSB-SM (2-2-2)	
		MSE	PSNR	MSE	PSNR
Lenna	474	0.009	68.336	0.020	65.008
	508	0.010	67.869	0.021	64.780
	633	0.012	67.184	0.027	63.803
	808	0.159	66.108	0.035	62.663
Average		0.048	67.374	0.026	64.064
Baboon	474	0.009	68.329	0.022	64.540
	508	0.010	67.964	0.023	64.450
	633	0.012	67.021	0.028	63.510
	808	0.016	66.018	0.036	62.493
Average		0.012	67.333	0.027	63.748
Pepper	474	0.008	68.609	0.022	64.699
	508	0.009	68.322	0.022	64.578
	633	0.012	67.237	0.028	63.563
	808	0.015	66.137	0.037	62.425
Average		0.011	67.576	0.027	63.816
House	474	0.009	68.241	0.020	64.928
	508	0.010	67.832	0.023	64.471
	633	0.131	66.971	0.029	63.455
	808	0.164	65.965	0.036	62.477
Average		0.079	67.252	0.027	63.833
Sailboat	474	0.009	68.274	0.021	64.906
	508	0.010	68.015	0.022	64.646
	633	0.130	66.986	0.029	63.449
	808	0.165	65.949	0.037	62.388
Average		0.079	67.306	0.027	63.847

PSNR is defined in the following Equation 2.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (2)$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2$$

where, ; C represents the original cover image; S represents the Stego image. If the MSE value increases, then the image degradation increases. When the MSE value reaches zero then the pixel by pixel matching of the images becomes perfect [15].

Embedding capacity (EC) is the maximum amount of information that can be concealed in the stego image, represented in bits. It can also be represented as bits per byte (BPB) that is calculated as in Equation 3 [16].

$$BPB = \frac{\text{Maximum embedding capacity in bits}}{\text{Image size in bytes}} \qquad (3)$$

The result of PSNR and MSE values of five images with different dimensions was shown in Table 1. In this table, 474 bytes to 808 bytes of secret message was embedded in 256*256 cover images. When the secret message size was increased to embed in the cover image, the PSNR value was decreased and the MSE value was increased. The CM-LSB-SM (2-2-2) method was used to improve the embedding capacity and good visual image quality based on the results of Table 1.

The comparison of the embedding capacity between the CM-LSB-SM (1-1-1) and CM-LSB-SM (2-2-2) was showed in Fig. 5. As a result, the CM-LSB-SM (2-2-2) method can embed two times higher than the CM-LSB-SM (1-1-1) method.

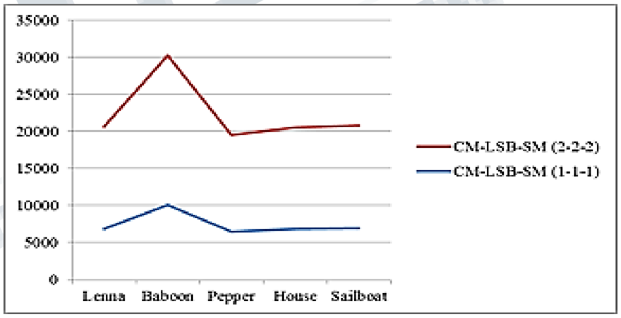


Fig. 5 Comparison of Embedding Capacity Value

The image size (256*256) and the message size (808 bytes) that were used to measure the histogram. The histogram analysis showed that it is very difficult to distinguish the difference between the cover image and stego image using the human eye as shown in Fig. 6 and 7.

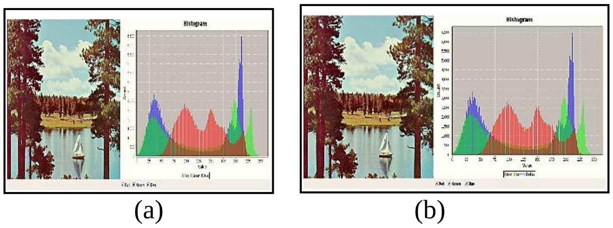
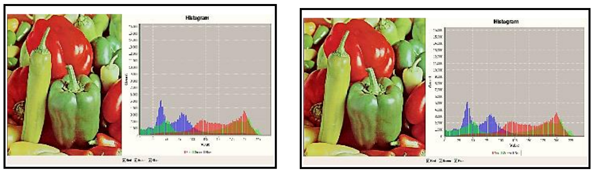


Fig. 6 Histogram of Sailboat image (a) Cover image (b) Stego image



(c) (d)

Fig. 7 Histogram of Pepper image
(c) Cover image (d) Stego image

From the experimental results, the proposed method embedding 1-LSB in the cover image found that it has high PSNR value and low embedding capacity. On the other hand, it has high embedding capacity by hiding 2-LSB. These tests highlighted that the embedding capacity of the image is increased by using the CM-LSB-SM (2-2-2). The good rate of PSNR in this method has been achieved because it is greater than standard PSNR value (35 decibel). However, the embedding capacity is low if the cover image contains the less number of edge-based objects.

CONCLUSION

In this study, the proposed image steganographic system has been developed by using a combination of Canny Edge Detection and Magic LSB Substitution Method (M-LSB-SM). Canny Edge Detection is used to find the location of edge point from the cover image. The secret data was embedded in edge point location to maintain the minimum visual distortion. Magic Matrix was used for choosing the pixel position of cover image for hiding the secret image.

The experimental results have been shown that the higher edge pixel points provided the higher embedding capacity. The evidence from this study suggests that the embedding capacity of CM-LSB-SM (2-2-2) method is higher than that of CM-LSB-SM (1-1-1) method. The minimum average PSNR value of 63.816 dB computed over five images is achieved with the CM-LSB-SM (2-2-2) method, which confirms the superiority of the proposed scheme.

REFRENCES

[1] T. Morkel, J.H.P. Eloff, M.S. Olivier, “An Overview of Image Steganography”, Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005

[2] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 147: 03, June 2000

[3] “Information hiding using steganography”, Conference Paper, · February 2003

[4] Muhammad K., Ahmad J., Rehman N. U., Jan Z., Qureshi R. J., "A Secure Cyclic Steganographic Technique for Color Images using Randomization," Technical Journal, University of Engineering and Technology Taxila, Pakistan, vol. 19, pp. 57-64, 2014.

[5] H. Al-Dmour, A. Al-Ani, “A steganography embedding method based on edge identification and XOR coding”, Expert systems with Applications, 46 (2016) 293-306.

[6] S. Immaculate Shyla, “Empirical Evaluation Of Image Steganography”, International Journal of Scientific Research and Engineering Studies (IJSRES), ISSN: 2349-8862, Volume 3 Issue 11, November 2016

[7] Sahar Mahdie Klim: Selected Least Significant Bit Approach for Hiding Information Inside Colour Image Steganography by Using Magic Square, Journal of Engineering and Sustainable Development, Vol. 21, No. 1, January, (2017).

[8] How to construct Doubly Even Magic Square, Copyright © 1999 – 2019, 2018, 1728 Software Systems.

[9] Canny, J. A Computational Approach to Edge Detection. – IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. **PAMI-8**, 1986, No 6, pp. 679-698.

[10] Nikolic, M., E. Tuba, M. Tuba. Edge Detection in Medical Ultrasound Images Using Adjusted Canny Edge Detection Algorithm. – In: Telecommunications Forum (TELFOR’16), Belgrade, 2016.

[11] Kaur, P., B. Kaur. 2-D Geometric Shape Recognition Using Canny Edge Detection Technique. – In: International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016 .

[12] Setiadi, D. R. I. M., H. A. Santoso, E. H. Rachmawanto, C. A. Sari. An Improved Message Capacity and Security Using Divide and Modulus Function in Spatial Domain Steganography. – In: International Conference on Information and Communications Technology (ICOIACT’18), Yogyakarta, 2018.

[13] Islam, S., M. R. Modi, P. Gupta. Edge-Based Image Steganography. – EURASIP Journal on Information Security, Vol. **2014**, 2014, No 1.

[14] Mohamed, M. H., N. M. AL-Aidroos, M. A. Bamatraf. A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB.

– International Journal of Engineering Research & Technology (IJERT), Vol. **1**, 2012, No 8, pp. 1-7.

[15] S. Rajkumar and G. Malathi, “A Comparative Analysis on Image Quality Assessment for Real Time Satellite Images,” Indian Journal of Science and Technology, vol. 9(34), Sept. 2016.

[16] M. H. Marghny and M. M. Loay, “High Capacity Image Steganography Technique based on LSB Substitution Method,” International Journal of Applied Mathematics & Information Sciences, Aug. 2015.