DOI: 10.24996/ ijs.2017.58.4B.22

Iraqi Journal of Science

ISSN: 0067-2904

A proposal of Multimedia Steganography Algorithm based on Improved Least Significant Bit (LSB) Method

Huda Dheyauldeen Najeeb[*1]**, Israa Tahseen Ali**[2]

[1]Department of Public Relations, University of Al Iraqia, Baghdad, Iraq.

[2]Departmentof Computer Science, University of Technology, Baghdad, Iraq.

Abstract

Because of the rapid development and use of the Internet as a communication media emerged to need a high level of security during data transmission and one of these ways is "Steganography". This paper reviews the Least Signification Bit steganography used for embedding text file with related image in gray-scale image. As well as we discuss the bit plane which is divided into eight different images when combination them we get the actual image**.** The findings of the research was the stego-image is indistinguishable to the naked eye from the original cover image when the value of bit less than four Thus we get to the goal is to cover up the existence of a connection or hidden data. The Peak to Signal Noise Ratio(PSNR) and Mean Square Error (MSE) value is calculated so that the quality of the cover image before and after the data hiding is evaluated.

Keywords: Steganography, Least Significant bit embedding, Bit plane, Mean Square Error, Peak Signal to Noise Ratio.

خوارزمية إخفاء وسائط متعددة المقترحة بالاعتماد على طريقة البت الاقل اهمية المطورة

هدى ضياء الدين نجيب[*1]**، إسراء تحسين علي**[2]

[1]قسم العلاقات العامة، كلية الإعلام، الجامعة العراقية ، بغداد، العراق.

[2]قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة

بسبب التطور السريع واستخدام شبكة الإنترنت بوصفها وسائل الاتصال ظهرت الحاجة إلى مستوى عال من الأمن أثناء نقل البيانات و أن "إخفاء المعلومات "واحد من هذه الطرق. وتستعرض هذه الورقة لأقل اهمية الذي يستخدم لتضمين ملف نصي مع صورة ذات الصلة به في داخل صورة رمادية وكذلك قمنا بمناقشة مستوي البت والتي تتقسم على ثمانية صور مختلفة فعند الجمع بينها نحصل على الصورة الفعلية .والنتيجة التي توصل اليها البحث هي ان الصورةالتي تحوي الوسائط المتعددةلا يمكن تمييزها بالعين المجردة من قبل صورة الغلاف الأصلي عندما تكون قيمة مستوي البت أقل من أربعة وبالتالي نصل إلى الهدف من ذلك هو التغطية على وجود اتصال أو بيانات مخفية.تم احتساب متوسط مربع الخطأونسبة الإشارة إلى الضجيج لقياس جودة الصورة المرسلة التي تحتوي على ملفات الوسائط المتعددة واثبات جودتها قبل و بعد الاخفاء.

*Email: huda_iraq81@yahoo.com

1. Introduction

There are many ways which play an important role with regard to information security, including the most common and well-known encryption method (Cryptography) which is change the basic data in accordance with the particular method to become illegible.

Another art aims to hide the data completely is known as hiding of information (Steganography) which is a method or technique to hide data within a digital medium , so as to hide the existence of any contact or exchange of information into a cover media and is not aware of this contact only the persons concerned [1].

The basic difference between encryption and steganography is that when you encrypt the information, the third party can know that there is a contact between the two parties or two destinations but he cannot understand the information because it is encrypted. In the case of hiding of information (Steganography), the third party does not know that there is something hidden or that is a contact between the two parties because it was used as an intermediary to hide this contact completely [2].

2. Related Works

Over the past years, information security has become the focus of many researchers who are trying to find new solutions, technologies and ideas that ensure the safe transfer of information through the network, especially the Internet, without interference. As a result, there are many techniques and methods currently used in information security. In this article we will highlight some ways to protect information.Vijay kumar [3] proposed a new algorithm of steganographic which is based on logical process for embedding MSB of secret image in to LSB of cover image which resulted in a significant improvement with lower computational complexity. A.S.Mahdi et al. [4]. designed proposed system is to hide image in image by using discrete cosine transformation method (DCT) and discrete wavelet transformation method (DWT) and Least Significant Bit (LSB). The system will embed the (input) secret image color inside a cover image color the secret image apply it discrete cosine transformation method (DCT) and the cover image is decomposing into four parts (LL, LH, HL, HH) by using discrete wavelet transformation method (DWT) and the secret image hidden in the part (HH) in segment Least Significant Bit (LSB) of cover image, and produce (output) stego image. And uses the stego key for extraction the data hidden (secret image) from stego cover through use the process embedding inverse. Divya.E [5] presented hiding text message inside grayscale image using two approaches which are : Particle Swarm Optimization algorithm (PSO) and Discrete Wavelet Transform (DWT) . In the end, the researcher concluded that both these approaches gives excellent peak-signal-to-noise-ratio. Nikita Sharma [6] proposed a new approach that combined Discrete Wavelet Transform (DWT) Technique and RSA algorithm with Hash-LSB Technique for getting image steganography. First the secret message be encrypted by RSA algorithm then embedded by Discrete Wavelet Transform for obtaining cover image Which will be sent.Wejdan A. Amer [7] is proposed an improved text hiding with the image that have a high confidentiality by implementing a strong password method so as to ensure no change will be made in the pixel values of the cover image after text hiding

Most of the offered works that are relevant to our research did not embed different types of data, it was embedded either image or text message inside another image, but in this paper both of them are successfully embedded inside a single image.

3. Steganographic System

The word steganography basically derived from a Greek word meaning "hidden writing". Steganography includes four different types are: text files steganography, image steganography, video steganography and audio steganography [8].

The structure of a steganography, as shown in Figure-1, composed of a cover image, secret data and stego image. The cover can be a video, image or audio while the secret data can be an image, text message, video or audio and resulting from the process of concealment is stego [5].

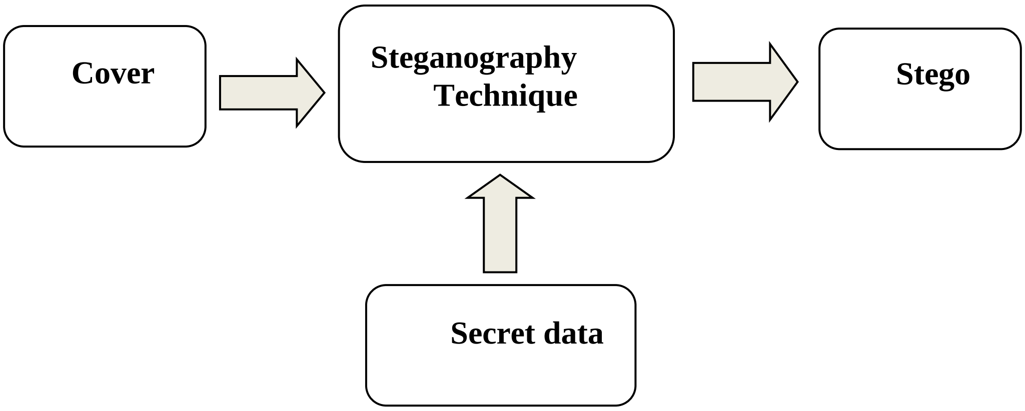


Figure 1-Steganographicsystem

4. Steganography Techniques

There are several techniques of steganography, the most common techniques will be explained as below:

A. LSB (Least Significant bit embedding)

The grayscale images consist of number of values called pixels which are represented as 8-bit binary strings (2^8 = 256) between 0 and 255 represent gradient gray values between black and white. Secret data are hidden in the LSBs of the 8-bit binary strings; this method is called "LSB steganography."[9]

The LSB is a simple and common method which used with steganography for embedding secret data in to the least significant bits of the pixel values in a Cover image [8, 9].

Suppose the first eight pixels of the Cover image are:

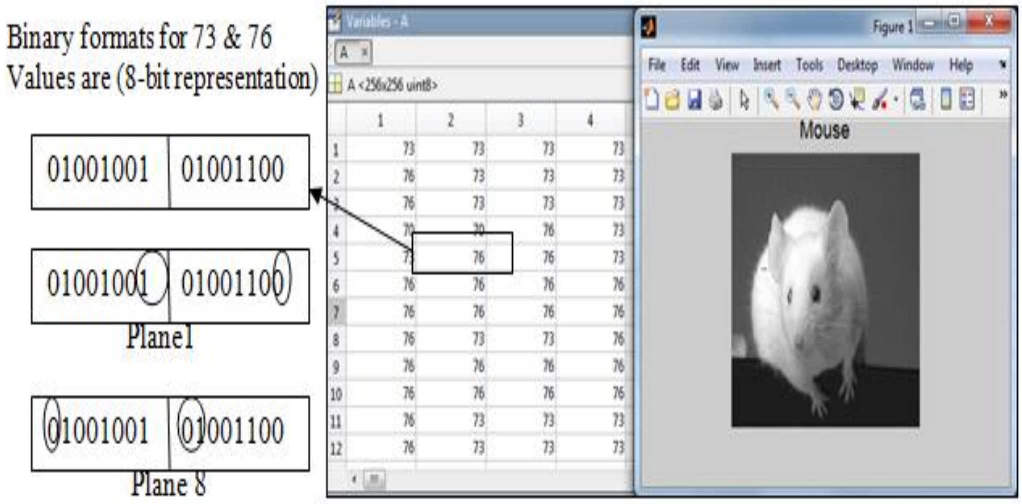
11010010 00100111 11101001 11101000 10000001 01010111 11101001 01000011
11001000 01001010 10010111 11101001 00100110 00010101 00100110 00100111

After hiding the message "Hi" whose binary value is 01001000 01101001, by LSB the values of these pixels become:

11010010 00100111 11101000 11101000 10000001 01010110 11101000 01000010
11001000 01001011 10010111 11101000 00100111 00010100 00100110 00100111

B. Bit Plane Slicing

Digitally, an image is represented in terms of pixels. These pixels can be expressed in bits. The grayscale image contains eight bit binary value; hence an image can be sliced up into 8 bit planes which give a sequence of binary images. In Figure-2 we can see that a grayscale image "mouse" is considered as a combination of eight bit-planes where each bit-plane can be represented by a binary matrix. Plane 1 contains the lowest order bit of all the pixels in the image. And plane 8 contains the highest order bit of all the pixels in the image [10].



	1	2	3	4
1	73	73	73	73
2	76	73	73	73
3	76	73	73	73
4	76	76	76	73
5	73	76	76	73
6	76	76	76	76
7	76	76	76	76
8	76	73	73	76
9	76	76	76	76
10	76	76	76	76
11	76	73	73	73
12	76	73	73	73

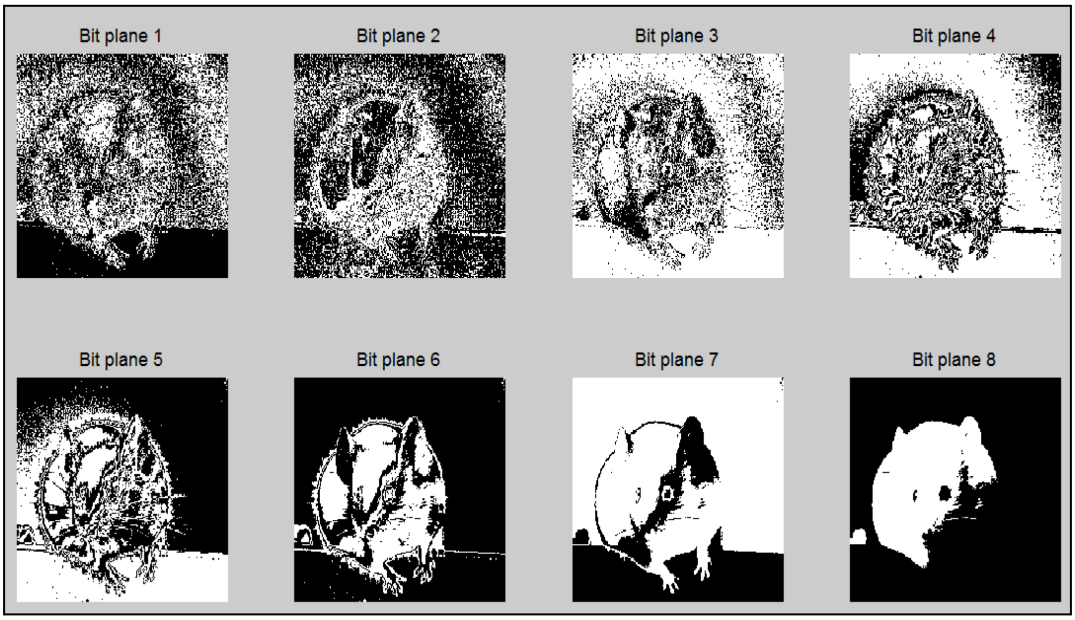


Figure 2-Bit plane slicing of a grayscale image

C. Mean Square Error and Peak Signal to Noise Ratio

MES is the measurement of mean square error between cover image and stego image. Its value should be minimization while PSNR used for measure the quality of stego image. Its value should be high. Both of them are standard measurement used in steganography technique for the sake of test the quality of the stego images. MSE is computed as follows: [11, 12]

$$\mathrm{MSE} = \frac{1}{\mathrm{nm}} \sum_{\mathrm{i=o}}^{\mathrm{n-1}} \sum_{\mathrm{j=0}}^{\mathrm{m-1}} [\mathrm{X(i,j)} - \mathrm{Y(i,j)}]^2 \qquad \ldots\ldots \qquad (1)$$

Image X which is n×m monochrome with noisy approximation Y.

Where

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MES}} \qquad \ldots\ldots \qquad (2)$$

5. Proposed System Design

The proposed work is to combine two types of steganography (text files steganography and image steganography) which is based on LSB and Bit plane to make image is not appeared what is inside it. In this work we are first hiding text file with image related to it inside the grayscale cover image and send the generation image is "Stego2". Then when the Stego2 image received, the text file with image had been retrieved.

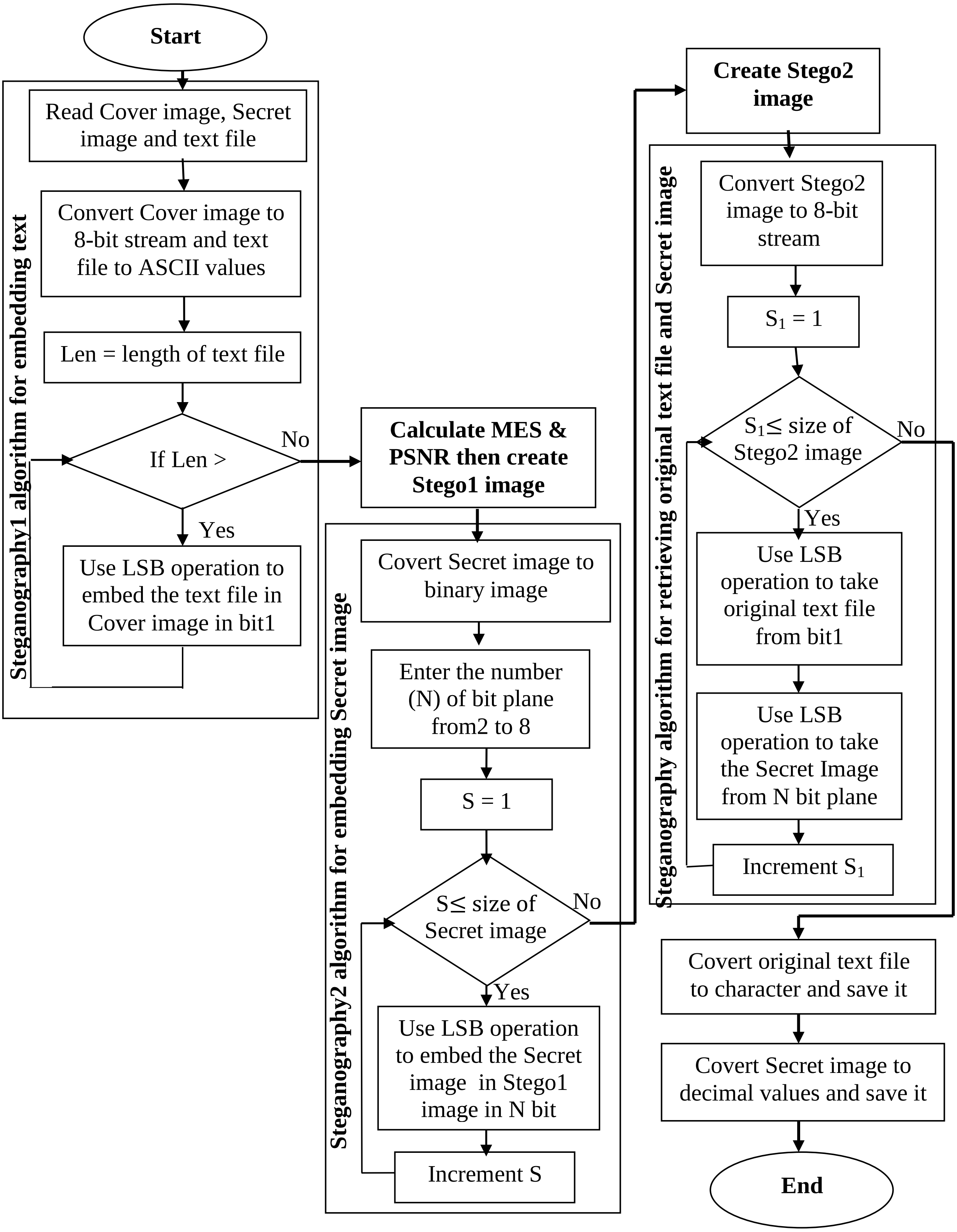
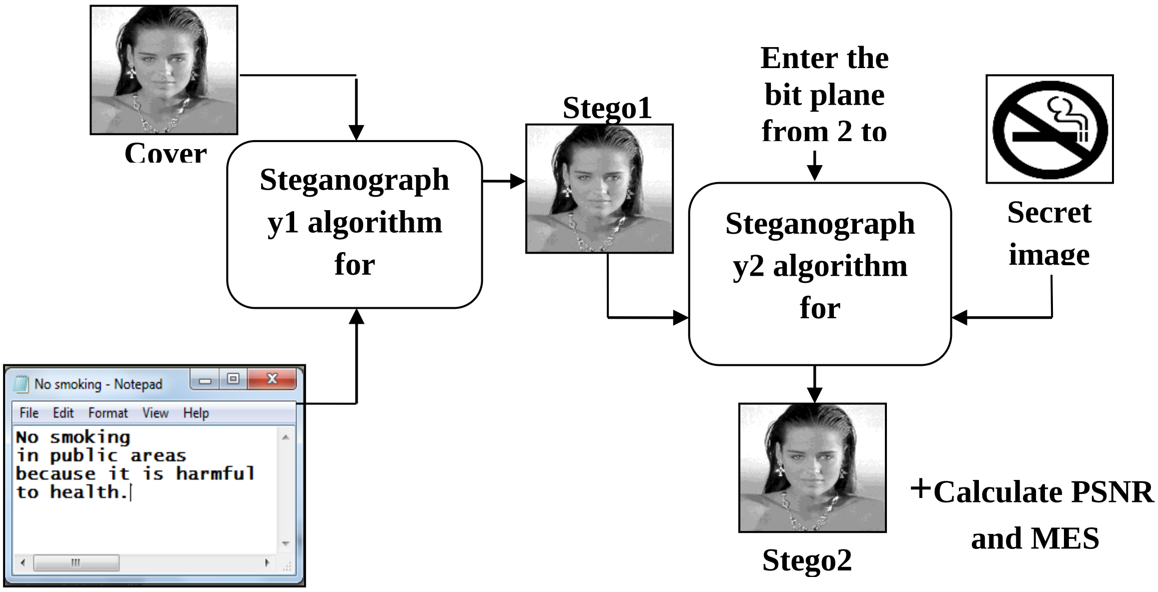

Start
Steganography1 algorithm for embedding text
Read Cover image, Secret image and text file
Convert Cover image to 8-bit stream and text file to ASCII values
Len = length of text file
If Len >
No
Yes
Use LSB operation to embed the text file in Cover image in bit1
Calculate MES & PSNR then create Stego1 image
Steganography2 algorithm for embedding Secret image
Covert Secret image to binary image
Enter the number (N) of bit plane from2 to 8
S = 1
S≤ size of Secret image
No
Yes
Use LSB operation to embed the Secret image in Stego1 image in N bit
Increment S
Create Stego2 image
Steganography algorithm for retrieving original text file and Secret image
Convert Stego2 image to 8-bit stream
S1 = 1
S1≤ size of Stego2 image
No
Yes
Use LSB operation to take original text file from bit1
Use LSB operation to take the Secret Image from N bit plane
Increment S1
Covert original text file to character and save it
Covert Secret image to decimal values and save it
End

Figure 3 -The flowchart of the Proposed Method

A. Steganography model for embedding text file and Secret image inside Cover image.


Cover
Steganograph y1 algorithm for
Stego1
Enter the bit plane from 2 to
Steganograph y2 algorithm for
Secret image
No smoking - Notepad
File Edit Format View Help
Stego2
+Calculate PSNR and MES

No smoking
in public areas
because it is harmful
to health.

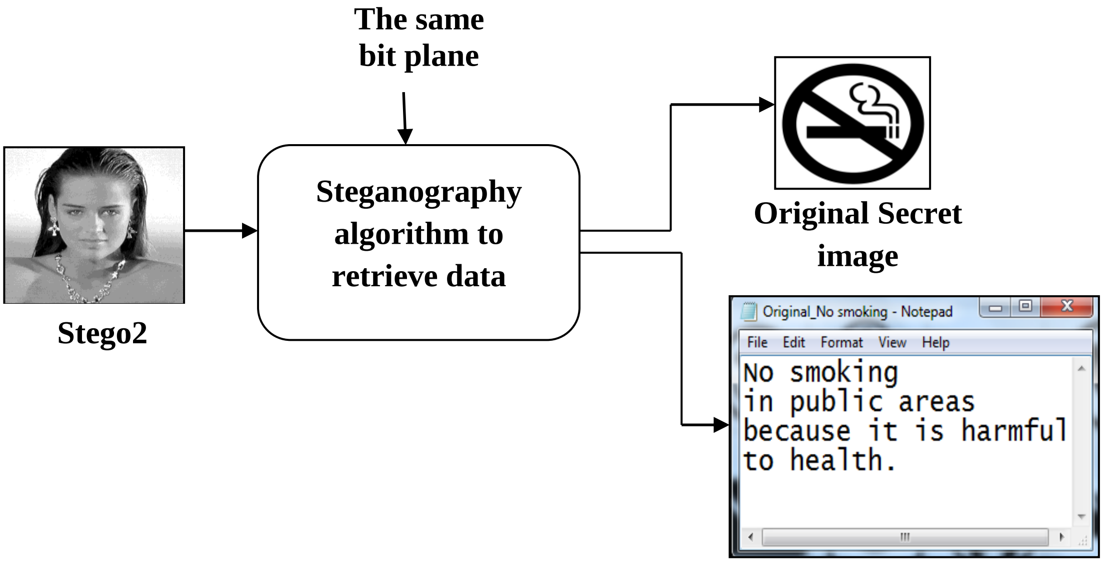
Figure 4-Steganography model for embedding.

Procedure 1:(proposed steganography Procedure)

Input : Cover and Secret image , Bit plane and Text file.
Output : Stego2 image.

Step 1 :Convert the text file to ASCII values and Cover image to 8-bit stream.
Step 2 :Perform LSB operation on Cover image for each pixels until all the bits of text file embedded.
Step 3 : Create Stego1 image.
Step 4 : Covert Secret image to binary image.
Step 5 :Get the bit plane to hide the Secret image in. The lowest bit is numbered 2, and the highest allowable bit plane is 8. Then perform LSB operation on Stego1 image for each 8-bit stream until all the bits of Secret image embedded.
Step 6: Convert the result to decimal value that will generate stego2 image.
Step 7 :Calculate MSE and PSNR between Cover and Stego2 image.

B. Steganography model for retrieving original text file and Secret image from Stego2 image



No smoking
in public areas
because it is harmful
to health.

Figure 5-Steganography model for retrieving

Procedure 2: (Multimedia Extraction Procedure)

Input : Stego2 image.
Output : Text file and Secret image.

Step 1: Read Stego2 image then convert it to 8-bit stream.
Step2 :Perform LSB operation on Stego2 image and retrieve bits of text file from Bit "1" as well as retrieve Secret image by using the same bit plane which the Secret image is hidden in.
Step3 :Convert the result to decimal value for getting Secret image and to character for getting text file.
Step4 :Write original hidden text file and Secret image.

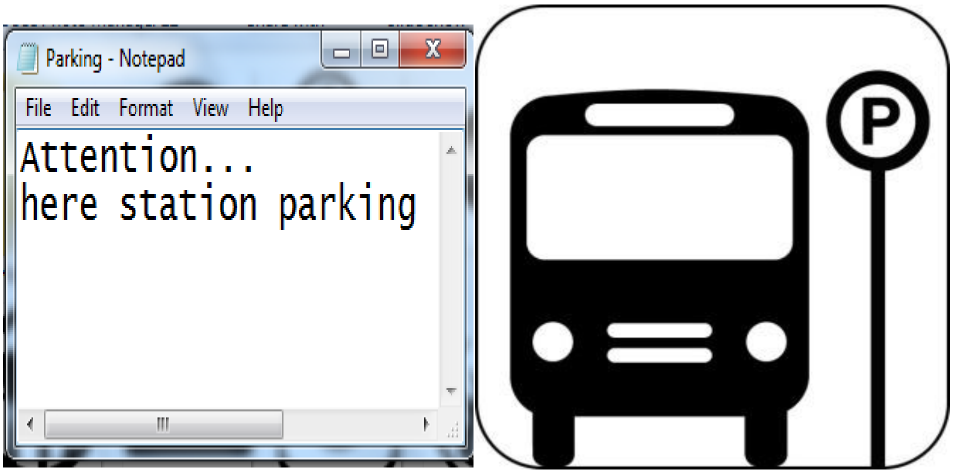
6. Experimental Results

6. Results

This model has implemented in MATLAB 2013a using LSB Steganography technique. We used TIF images as Cover image and JPG images as Secret image to get TIF images which represent Stego image.

6.1. Embed secret data

The text file "Parking.TXT" have been hidden inside grayscale image "Socha .TIF" which is became "Cover image". This text have been embedded in Bit "1" by using Steganography1 algorithm and create" Stego1.TIF", then hide "Bus .JPG" which is "Secret image" inside Stego1 image by using Steganography2 algorithm, here we must determine the value of Bit plane to hide the Secret image in which is from 2 to 8.In the end it will create a final image "Stego2.TIF" that will send and calculate both of MES and PSNR to know the quality of image sent"Stego2"by compared it with the original image "Cover image".



Attention...
here station parking

Figure 6-Text file and Secret image which they will be hidden.

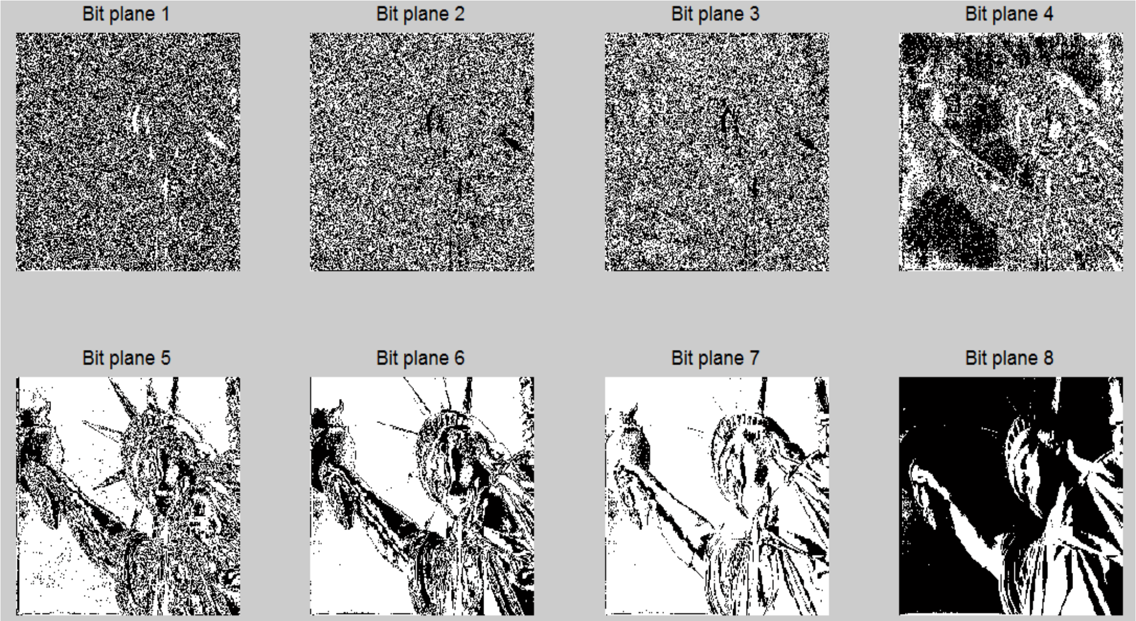


Figure 7-Bit plane slicing of a Cover image.

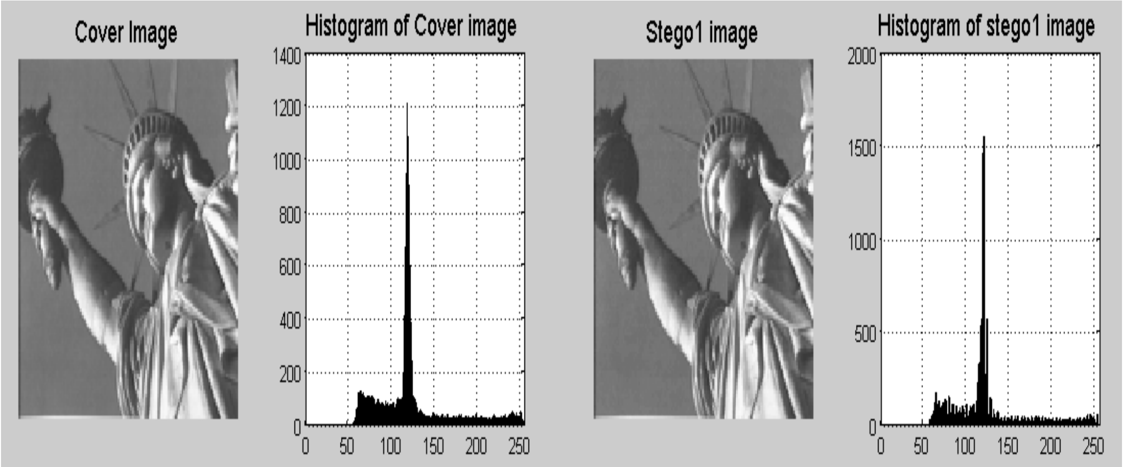
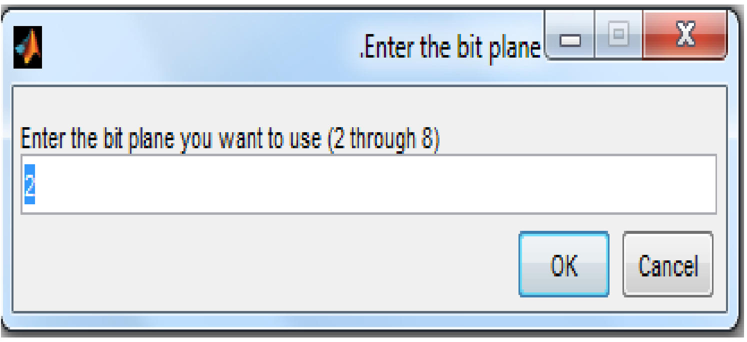
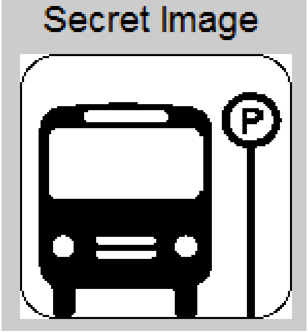


Figure 8- Steganography1 algorithm shows cover image with its histogram and Stego1 image with its histogram where text file was been hidden in



Enter the bit plane you want to use (2 through 8)

2



.

Figure 9-Dialog box ask to enter the value of Bit plane

Figure 10- Binary Secret

image

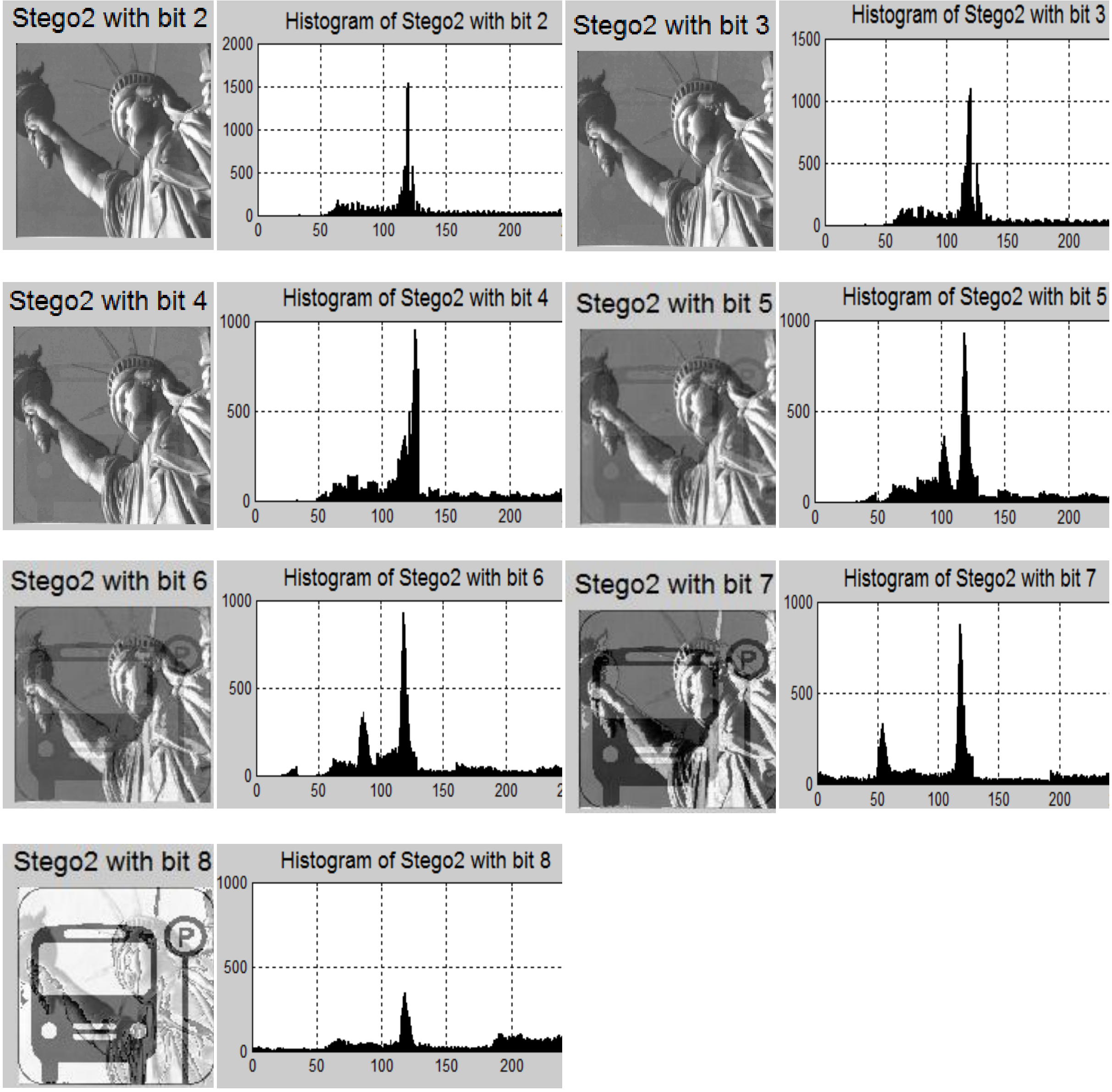


Figure 11-Steganography2 algorithmshowsStego2 image with its histogram where text file and Secret image were been hidden in, where shows all possibilities of Stego2 image when the value of Bit plane from 2 to 8.

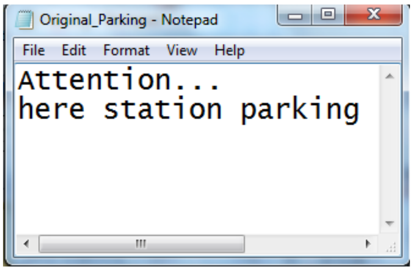
Table 1: shows the results of MSE and PSNR obtained for different between Cover image andStego2 image

The number of bit plane which will be hide in	**MSE**	**PSNR**
2	2.2756	44.5599
3	7.5534	39.3494
4	34.585	32.742
5	109.81	27.7242
6	425.32	21.8436
7	1578.7	16.123
8	9668.1	8.2774

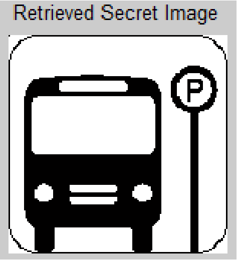
6.2. Retrieve secret data

The hidden data can be retrieved easily from the received image "Stego2". By using Steganography algorithm, "Original_Parking.TXT" has been retrieved from Bit "1" and retrieved Secret image from the same Bit plane which was entered in the Embed secret data part.

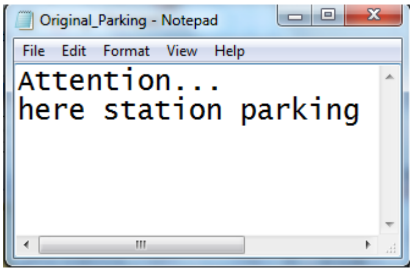
When the value of Bit plane that entered is 2



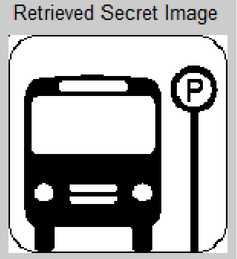
Attention...
here station parking



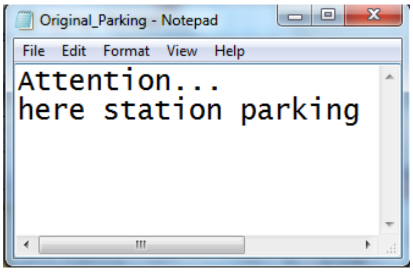
When the value of Bit plane that entered is 3



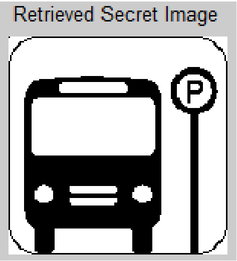
Attention...
here station parking

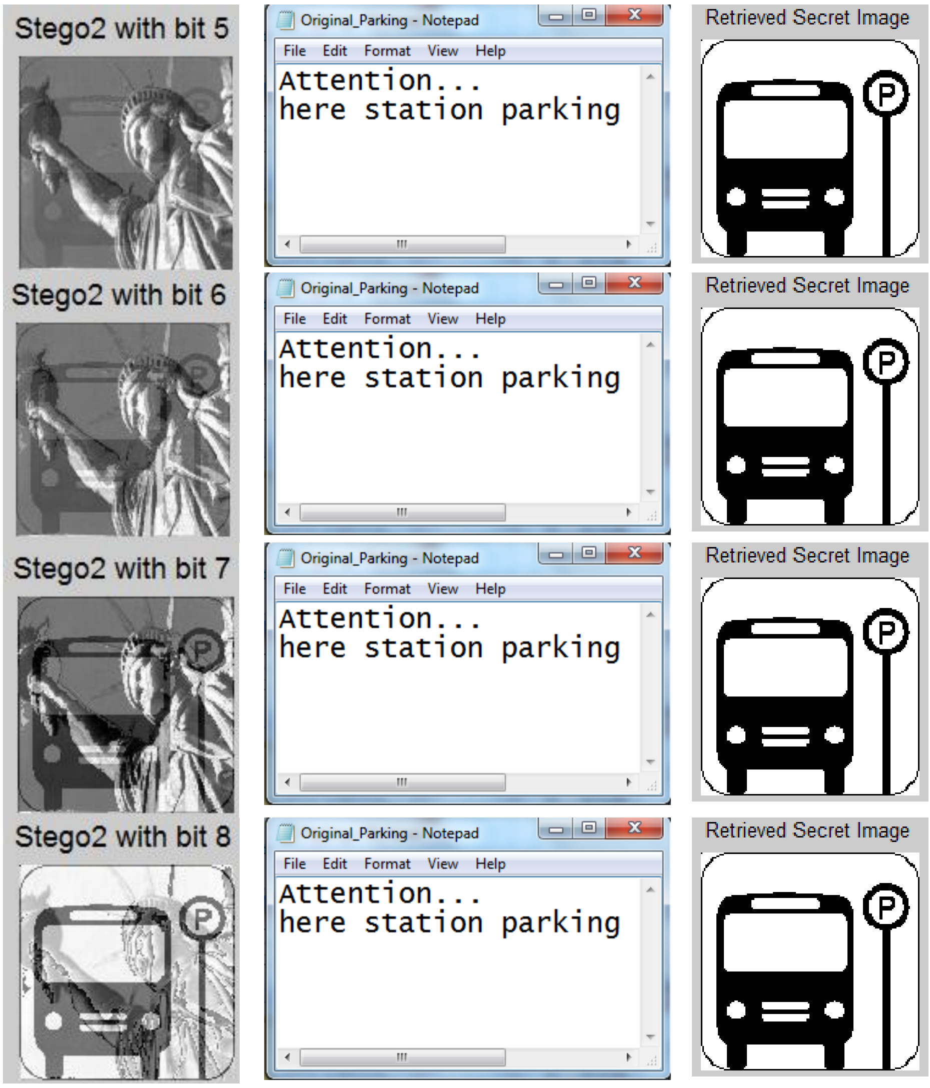


When the value of Bit plane that entered is 4



Attention...
here station parking





When the value of Bit plane that entered is 5

Stego2 with bit 5
Original_Parking - Notepad
File Edit Format View Help
Retrieved Secret Image

```
Attention...
here station parking
```

When the value of Bit plane that entered is 6

Stego2 with bit 6
Original_Parking - Notepad
File Edit Format View Help
Retrieved Secret Image

```
Attention...
here station parking
```

When the value of Bit plane that entered is 7

Stego2 with bit 7
Original_Parking - Notepad
File Edit Format View Help
Retrieved Secret Image

```
Attention...
here station parking
```

When the value of Bit plane that entered is 8

Stego2 with bit 8
Original_Parking - Notepad
File Edit Format View Help
Retrieved Secret Image

```
Attention...
here station parking
```

Figure 12-Steganography1 algorithm shows retrieved text file and Secret image from all possibilities of Stego2 image when entered value of Bit plane from 2 to 8.

7. Conclusion.

Steganography is the art of writing hidden messages which have four types. But often it is using only one type of steganographic techniques. So in this proposed work combined two types of it. Inside image we embedded file text and related image in by using bit plane where Sometimes called "LSB Watermarking".

This work is implemented successfully when we used JPG and TIF images with various sizes where file text embedded in bit 1 and the Secret image embedded in any bit from 2 to 8, but when the values of bit equal 4 or more may allow the presence of a Secret image be noticeable in the Stego2 image and MSE become bigger while PNSR become smaller, therefore there is really no reason to use any other bit plane than the lowest bit. Finally we conclude that proposed approach gives good quality of Stego2 image when the Secret image hides in bit 2 or 3.

References

1. Dipalee, B. **2015.** New Robust LSB Steganographic Technique for Increased Security. *International Journal of Engineering Research and General Science*, **3**(2): 113-112.

2. Abhay, D. and Sanjay, B. **2015**. A Review on Image Steganography Techniques. *International Journal of Advanced Research in Computer and Communication Engineering*, **4**(7): 24-26.

3. Vijay, K.S. and Vishal, S. **2012.** A Steganography Algorithm for Hiding Image In Image By Improved Lsb Substitution By Minimize Detection. *International Journal of Advanced Research in Computer Science and Software Engineering*. **36**(1): 1-12.

4. Mahdi, A.S, Khidhir, A.H. and Hussein, M.A. **2014**. Image in Image Steganography based on DCT. *Iraqi Journal of Science*, **55**(4A): 1675-1684

5. Divya, E. and Rajkumar, P. **2015.** Steganographic Data Hiding Using DWT and Particle Swarm Optimization. *International Journal of Computer Applications*, **117**(14): 31-34.

6. Sharma, N. and Khera, M. **2015.** A Novel Approach to Image Steganography Using Hash-LSB and DWT Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*, **5**(6): 1448-1454.

7. Wejdan, A. and Amer. **2016**. Efficient Text in Image Hiding Method based on LSB Method Principle. *Iraqi Journal of Science*, **57**(2C): 1539-1547

8. Vanitha, T., Anjalin, D. S., Rashmi, B. and Sweeta, D.S. **2014.** A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, **2**(5): 89-95.

9. Ahmed, F. H. and Rizwan, **2013.** Embedding Multiple Images in an Image Using Bit Plane Slicing. *International Journal of Advanced Research in Computer Science and Software Engineering*, **3**(1): 327-335.

10. Mayukh, D. **2015.** An Effective Method to Hide Texts Using Bit Plane Extraction. *IOSR Journal of Computer Engineering*, **17**(2): 17-23.

11. Deepesh, R. and Vijaya, B. **2013.** A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. *International Journal of Computer Applications*, **64**(20): 15-19.

12. Arpita, A. H. **2016.** Secure Digital Communication using LSB based Image Steganography Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*, **6**(9): 17-21.