Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 10, No. 3, pp. 54-62, September 2017

HIDING (1-8) MULTIMEDIA FILES IN ONE COLOR IMAGE

Jinan N. Shehab [1], Haraa Raheem Hatem [2], Omar Abdulkareem Mahmood [3]
[1, 2,3] *Assistant Lecturer, Department of Communication Engineering, University of Diyala*
jinanalazawi@.engineering.uodiyala.edu.iq [1], haraa@engineering.uodiyala.edu.iq [2]
(Received: 1/9/2016; Accepted: 23/10/2016)

ABSTRACT: - This paper presents hiding one to eight gray images or texts (secret information) inside color image (cover image) based on Least Significant Bits (LSB) algorithm.

The main idea is to insert the secret message (one to eight texts or one to eight gray images) in the three LSB of the cover image (color image). The color cover image RGB model (R channel, G channel and B channel) is separated into three cover images (the red cover, green cover, and blue cover). Each one of these three cover images is used to hide secret messages (gray image (two secret images in R channel, three secret images in G channel and three secret images in B channel) or text). The experiments and comparative studies show that the algorithms are characterized by many features of the ability of hiding huge data, and then the ability of extracting secret message without errors. Beside the reconstructed image, has efficacies (to human acquaintance) according to peak signal to noise ratio (PSNR) and mean square error (MSE), also retain both the explicitness and the characteristics of the both secret message and cover image.
Keywords: *LSB algorithm, image hiding, text hiding*

1. INTRODUCTION

In the digital world, the heart of computer communication and global economy is information. To ensure the security of the information, the concept of information hiding has attracted researchers to come up with creative solutions to protect information from falling into wrong hands [(1)].

Information hiding (Steganography) is the operation of writing hidden messages in such a manner that no one apart from the transmitter and receiver, suspects the existence of the hidden message. The process of information-hiding in a steganographic system starts by recognition the redundant bits in cover medium, that can be modified without damage the medium integrity. The embedding process creates a stego medium by replacing these redundant bits with information from the secret message to be transmitted [(2)].

Although, there are many different carrier file format (cover) can be used but digital image is the most popular because hold huge amount of information and their frequency on the network [(3)].

In this paper, we will take one of the methods of steganography it is LSB, to hide one to eight texts or gray images in a cover image. This paper includes two algorithms:

- Hiding one to eight texts in an image (color image).
- Hiding one to eight gray-images in an image (color image).

Using these algorithms, high quality of the extracted secret information (reconstructed message high quality) and the stego-image, compared with the original cover are obtained.

2. RELATED WORKS

In [4], an encryption algorithm with LSB method is used to embed text in image. It enables the user to provide the system with both cover and text, and obtain a final image which contains the hidden text inside. In [5], a hash based LSB method is proposed. The proposed method takes eight bits of secret information at a same time and put them in LSB of RGB pixel value of a cover image in 2,3,3 order respectively. Such that out of eight bits of message five bits are inserted in R and G pixel and remaining three bits are inserted in B pixel. In [6], a new Steganographic method was proposed, which provides high embedding capacity and PSNR. In addition, the security of the system has improved by using Pseudo Random Number Generator (PRNG).

3. LEAST SIGNIFICANT BIT (LSB) SUBSTITUTION METHOD

The LSB technique is a spatial domain technique since it embeds the secret bits directly in the cover file. Because LSB substitution technique is relatively quick and easy to use, it is the most popular technique used for digital steganography and especially with digital images [7].

A basic algorithm for LSB substitution is to take the first N cover pixels where N is the total length of the secret message for text and image where N=R×C (where R row and C column numbers in secret image) that is to be embedded in bits. After that every pixel's last bit in cover image will be replaced by one of the message bits [8].

4. THE STEGANOGRAPHY SYSTEMS PROCEDURE

First in these systems, the cover image should be selected carefully like choosing the cover with low details as shown in Figure.1. cover image with low details. Notice that the cover image has the size 512×512, so when the information in the pixels are replaced with another information, the cover image will not have a noticeable degradation. In this paper, the procedure of steganography divided in two sides:

4.1 Embedded Side

Figures.2.,3.,4. shows the stages involved in the sending process. Each stage is briefly discussed below:

Step (1) Preparation of the Cover Image: -

Transform 2-D color image (R×C) into three(1-D) image (red(N), green(N), blue(N)).

Step (2) Preparation of the Secret Message: -

In this algorithm, a secret text is being reading and then each character is transformed into equivalent number according to the **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange (**ASCII**) (1- 8 texts in one color image as shown in Figure.2.). The secret image transform from 2-D into 1-D (1- 8 secret images in one color image as shown in Figure.3.).

Step (3) Proposed Embedding Algorithms: -

A. Hiding (1-8) Texts in one color Image: -

In this algorithm, secret texts messages are embedded in a cover image, as shown in Figure.2. The algorithm steps represented by:

1. Divided color image into 3-channel (red, green, blue)
2. Texts hiding in three channels, two texts in R-channel, three texts in G-channel and three texts in B-channel.
3. Every pixel's last two or three bits in cover image will be replaced by one of the message bits and the steps of hiding texts are below: -

- Replace the value of eighth bit in every pixel (in cover image(R-channel)) by the value of bit from first secret text and seventh bit (in R-channel) by the value of bit from second text as shown in Figure.4.

- Replace the value of eighth bit in every pixel (in cover image (G-channel)) by the value of bit from third secret text, seventh bit (in G-channel) by the value of bit from fourth text and sixth bit (in G-channel) by the value of bit from fifth text.
- Replace the value of eighth bit in every pixel (in cover image (B-channel)) by the value of bit from sixth secret text, seventh bit (in B-channel) by the value of bit from seventh text and sixth bit (in B-channel) by the value of bit from eighth text.
- Transform results back from binary to decimal to get stego-image.

B. Hiding (1-8) Gray Image in a color Image: -

In this algorithm, a secret images will be hidden in a cover image as shown in Figure.3. The steps for this algorithms are:

1. Divided color image into 3-channel (RGB) and then secret image embedding in each channel.
2. Each pixel in secret image represented by (8-bits/pixel (gray-image)).
3. Hidden each bit from secret image in the bit from pixel in cover image according to LSB algorithm as indicated in the above section A. step 3.
4. Transform back from binary to decimal and then from 1-D to 2-D to get stego-image.

4.2 Reconstructed Side

The receiver need stego-image to extract the secret information. The extracting algorithm is the inverse of the embedding algorithms, as shown in Figure.5.

A. Extract Text from Color Image

As in extracting text (from 1-8) of color image as shown in Figure.5. A. The steps will be followed: -

1. Divided color stego-image into 3-channel (red, green, blue)
2. Convert each channel of color stego-image from 2-D into 1-D and then convert each pixel to binary number (8-bit/pixel).
3. Take two last bits from each pixel in R-channel and three last bits from each pixel in (G and B channels) to construct the (1-8) secret texts (binary)
4. Transform each texts from binary to decimal value.
5. Transform each decimal value into character according to ASCII.

B. Extracting Image from Color Image

As shown in Figure.5. B. This process will be done by these steps:

1. Divided color stego-image into 3-channel (red, green, blue)
2. Convert the each channel of color stego-image from 2-D into 1-D and then convert each pixel to binary number (8-bit/pixel).
3. Take two last bits from each pixel in R-channel and three last bits from each pixel in (G and B channels) to construct the (1-8) secret image (binary)
4. Transform from binary to decimal value.
5. Transform from 1-D into2-D to construct secret image.

5. NUMERICAL SIMULATION RESULTS

There are many tests that can be used to measure the quality of the image: -

5.1 Peak-Signal-to-Noise-Ratio (PSNR)

Depending on Human Visual System (HVS), some amount of distortion between the original image and the modified one is allowed. Steganography techniques are measured by objective measure, the Mean squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) between the stego-image and its corresponding cover image are observed [9]. PSNR is usually measured in dB. To compute the peak signal to noise ratio as: -

$$\mathrm{PSNR(dB)} = 10\log_{10}\frac{\mathrm{P}^2}{\mathrm{MSE}} \qquad (1)$$

Where P is the maximum pixel value. Also, the Mean Square Error (MSE) which measures the cumulative Mean Square Error between the original and the stego-image. The MSE is defined as: -

$$\mathrm{MSE} = \frac{1}{\mathrm{R}\times\mathrm{C}}\sum_{\mathrm{i}=0}^{\mathrm{R}-1}\sum_{\mathrm{j}=0}^{\mathrm{C}-1}[\mathrm{X(i.j)} - \widehat{\mathrm{X}}\,\mathrm{(i.j)}]^2 \qquad (2)$$

Where R: number of pixel in each rows, C: number of pixel in each columns, i and j: row and column numbers, X(i,j): original image and (i,j): stego image.

Using Matlab program, the simulation result for the proposed method are:-

1. Hiding texts into a color image. The implementation results to hide (1-8) different texts and result of PSNR (between original image and Stego-image) for color image are shown in Table (1).
2. Hiding gray images into a color image. The implementation results can be seen in Table (2).

The size of the color image is larger than the size of the gray image, therefore; color image is used as cover image in this paper to hide (1-8) texts or (1-8) gray images in the same time as shown in Tables (1&2). As a result of that, we can hide and transmit multi- texts or image in one cover image instead of hide and transmit multi- texts or image in multi-cover images and that lead to reduce time and capacity (means amount of secret information that can be inserted in a cover media) that we need it. Also we noted that PSNR is prospered to HVS from the result in Tables (1&2).

5.2 Histogram Analysis

The histogram of the stego-image and cover image are found to show that the statistical properties of the cover image are not affected by changing 3-bits in some pixels [(1)]. Therefore; if the histogram of the cover is nearly equal to the histogram of the stego-image, that means the proposed system is good enough to avoid the attackers. Figure.6. represented one example (red-channel) of the cover and stego-images histograms, we noted that histogram of image before hiding information (2-images) is the same that after hiding information because of the small change in some pixels don't effect on the histogram of the cove image as shown in Figure.6.

CONCLUSIONS

The simulation results show that, the proposed algorithm has high PSNR which means that: the stego-image (the image after hiding process) and the original image (the image before hiding process) cannot be distinguished by human eye and large hiding texts or images in one cover image instead of hiding text or image in cover image. As a result; reduction in time and capacity. Also; the stego-image is obtained with very close properties to the original cover image according to PSNR, MSE, and histogram tests, so it is so difficult to recognize between them and to detect secure message.

REFERENCES

1) Zaynab Najeeb Abdulhameed," High Capacity Steganography Based On Chaos and Contourlet Transform For Hiding Multimedia Data", M.Sc. Thesis, Department of Electronics & Communications Engineering, University of AL-Mustansiriy, 2014.
2) Malini Mohan & Anurenjan P.R," A New Algorithm for Data Hiding in Images using Contourlet Transform", IEEE, 2011.

3) Morkel, Eloff, Olivier, " An Overview of Image Steganography" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science, University of Pretoria, Pretoria, South Africa,2005.
4) Aishvary Goel, Anubhav Srivastava and Alok Kr. Mishra," Implementation of LSB Steganography with 12-bit Frame Format ", ICACEA,2014.
5) G.R.Manjula1 and AjitDanti " A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.
6) Marwa M. Emam, Abdelmgeid A. Aly and Fatma A. Omara," An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", (IJACSA), Vol. 7, No. 3, 2016.
7) Adel Almohammad," Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility",Ph.D.Thesis ,Brunel University,August, 2010.
8) Bhavana.S, and K.L.Sudha" Text Steganography Using Lsb Insertion Method Along With Chaos Theory", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.2, April 2012.
9) Juan José Roque and Jesús María Minguet" SLSB: Improving the Steganographic Algorithm LSB ", www.researchgate.net/profile/Jj_Roque,2010.

Figure (1) Cover Image jpg (512×512) pixels

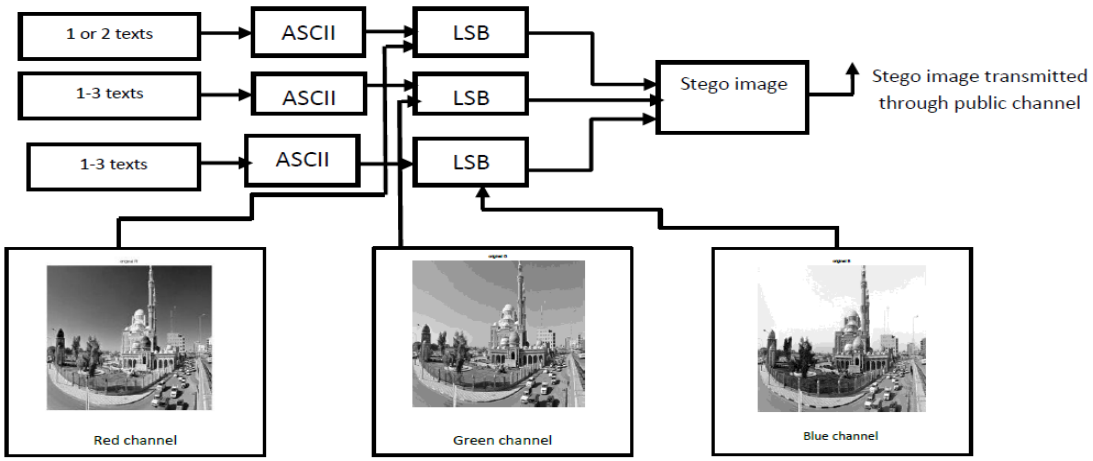


Figure (2) Embedded System for Text.

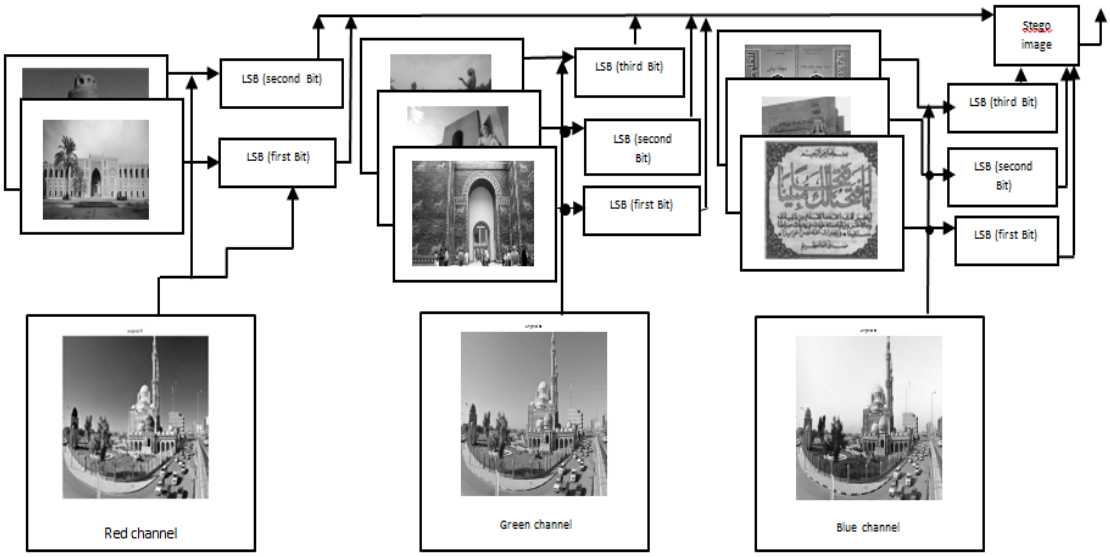


Figure (3) Embedded System for Gray Scale Images

secret text
Text1(Red)
Text2 (Green)

Character		Decimal	Binary							
Text-1		b-1	b-2	b-3	b-4	b-5	b-6	b-7	b-8
R	82	0	1	0	1	0	0	1	0
e	101	0	1	1	0	0	1	0	1
d	100	0	1	1	0	0	1	0	0

Text-2		b-1	b-2	b-3	b-4	b-5	b-6	b-7	b-8
G	71	0	1	0	0	0	1	1	1
r	114	0	1	1	1	0	0	1	0
e	101	0	1	1	0	0	1	0	1
e	101	0	1	1	0	0	1	0	1
n	110	0	1	1	0	1	1	1	0

Red Cover image
(only least 7 and 8 bits are using)

							Bit-7	Bit-8
Pixel-1	1	1	0	0	1	0	1	1
Pixel-2	1	1	0	0	0	1	1	1
Pixel-3	1	1	0	0	0	1	1	0
Pixel-4	1	1	0	0	1	0	1	1
Pixel-5	1	1	0	1	0	0	0	0
Pixel-6	1	1	0	1	0	0	1	1
Pixel-7	1	1	0	1	1	0	1	0
Pixel-8	1	1	1	0	0	0	0	0

Stego-red cover image
(for hiding R and G characters only in 8 and 7 bits)

							G	R
P1	1	1	0	0	1	0	1	0
P2	1	1	0	0	0	1	1	1
P3	1	1	0	0	0	1	1	0
P4	1	1	0	0	1	0	0	0
P5	1	1	0	1	0	0	0	1
P6	1	1	0	1	0	0	0	0
P7	1	1	0	1	1	0	1	1
P8	1	1	1	0	0	0	0	0

Figure (4) Hiding (2-Text) into R-Channel Cover Image

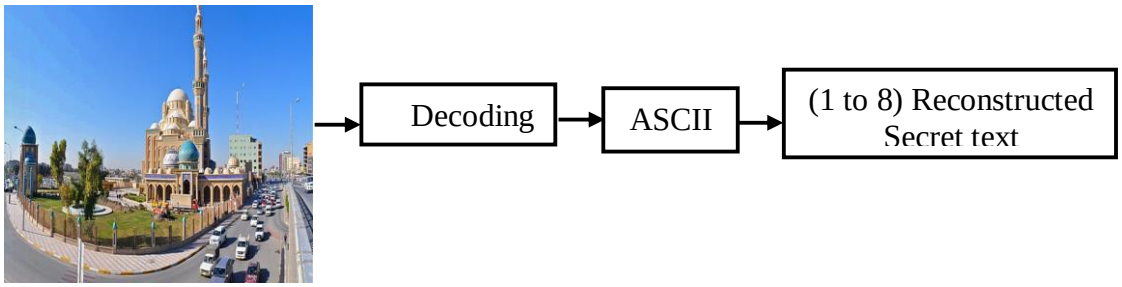


Figure (5.A) Reconstructed system for Texts

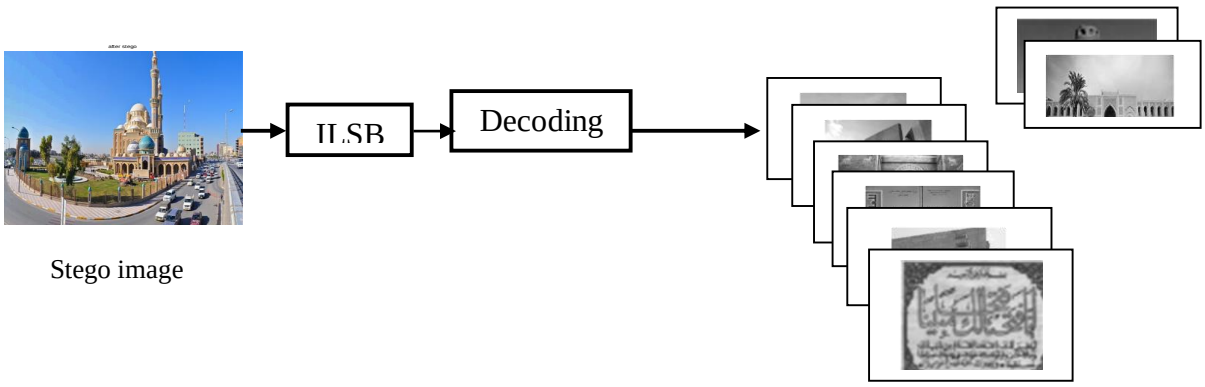


Figure (5.B) Reconstructed system for Images

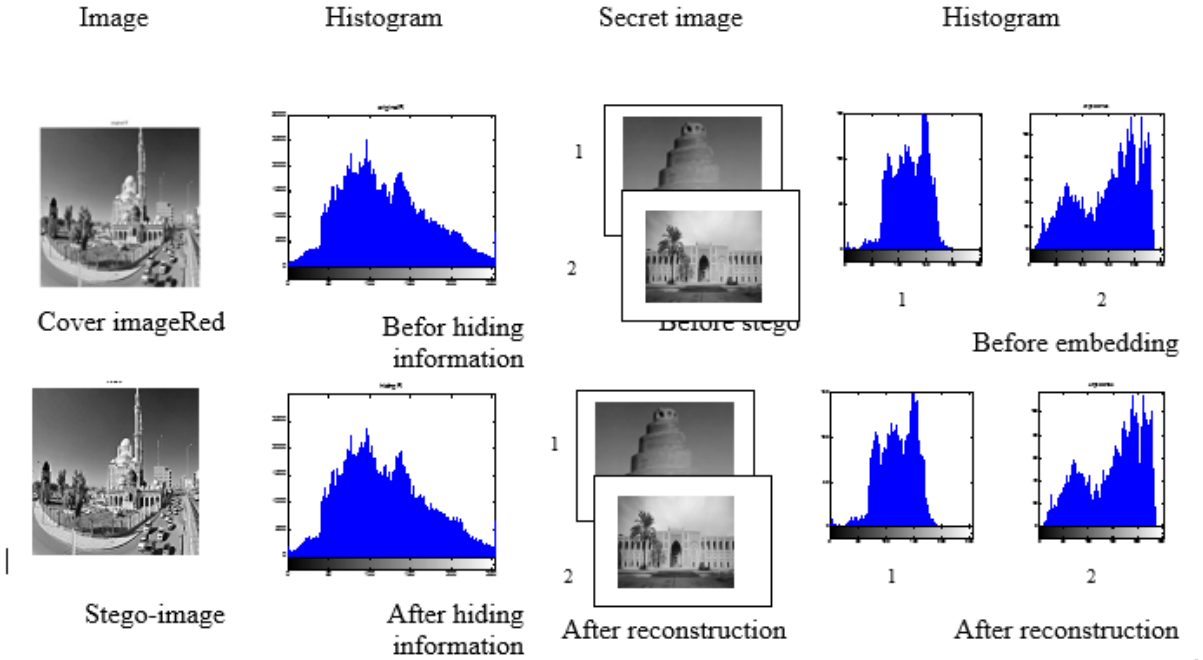
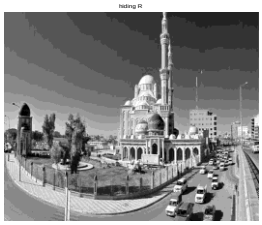
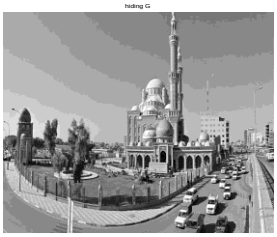
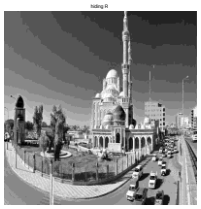
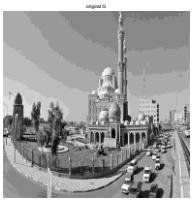
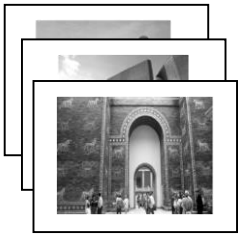
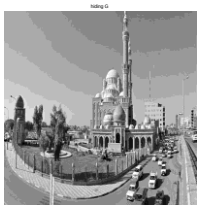
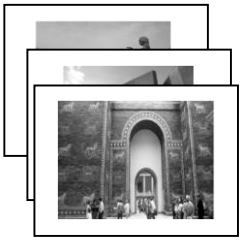
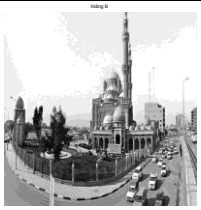
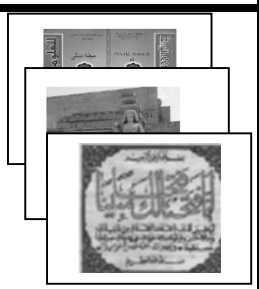


Figure (6): cover and stego – images Histogram

Table (1) Hiding Eight Texts in Image and PSNR to each State.

Red Stego- image	Green Stego- image	Blue Stego- image
		
Text 1=Red Text 2=Green	Text 1= Red Text 2= Green Text 3=Blue	Text 1= Red Text 2= Green Text 3= Blue
PSNR= 81.7432	**PSNR= 78.5120**	**PSNR= 75.8374**

Table(2) Results of Hiding eight Images into Color Image also PSNR for Each State.

Cover image	Secret image	Stego-image	Extraction Secret image	PSNR
 **Red channel**				**49.3615**
 **Green channel**				**43.0879**
 **Blue channel**				**43.1854**

اخفاء (8-1) ملفات وسائط متعددة في صورة ملونة واحدة

جنان نصيف شهاب ، حراء رحيم حاتم ، عمر عبد الكريم محمود
قسم هندسة الاتصالات، كلية الهندسة، جامعة ديالى

الخلاصة

يقدم هذا العمل اخفاء من 1 الى 8 صور رمادية او نصوص (تمثل المعلومات السرية) داخل صوره ملونة واحدة (صورة الغلاف) بالاعتماد على البت الاقل وزنا.

الفكره الاساسيه في هذا العمل هو ادخال النص او الصورة (من 1 الى 8 نصوص او صور رمادية) في البتات الاقل وزنا في الصورة الملونة الاصلية. الصورة الملونة تقسم الى الالوان الاساسية الثلاثة . كل لون يستخدم لا خفاء صور او نصوص (اللون الاحمريستخدم لإخفاء نصين او صورتين واللون الاخضر والازرق كل منهما لاخفاء3 نصوص او 3 صور) . لقد بينت التجارب والدراسات ان الخوارزميات المستخدمه تتحدد صفاتها عن طريق قابليتها في اخفاء عدد كبير من البيانات وعن طريق قدرتها في استرجاع الرسالة الأصلية بدون اخطاء. بالإضافة الى ان الصورة المسترجعة تمتلك كفاءات عالية (إلى التعارف البشري) بالاعتماد على نسبة الضوضاء ((PSNRومعدل مربع الخطأ ((MSE، كما تحتفظ كل من الوضوح وخصائص الرسالة السرية وصورة الغلاف على حد سواء.