

# Hiding Data in Color Image Using Least Significant Bits of Blue Sector

**Hussein L. Hussein**

Dept.of Computer Science/College of Education for Pure Science (Ibn AL-Haditha)/ University of Baghdad.

**Received in:19/November/2017, Accepted in:15/January/2018**

## **Abstract**

Concealing the existence of secret hidden message inside a cover object is known as steganography, which is a powerful technique. We can provide a secret communication between sender and receiver using Steganography. In this paper, the main goal is for hiding secret message into the pixels using Least Significant Bit (LSB) of blue sector of the cover image. Therefore, the objective is by mapping technique presenting a model for hiding text in an image. In the model for proposing the secret message, convert text to binary also the covering (image) is divided into its three original colors, Red, Green and Blue (RGB) , use the Blue sector convert it to binary, hide two bits from the message in two bits of the least significant bits of blue sector of the image.

**Keywords:** Steganography, Hiding, Image processing, Mapping.

## Introduction

The words of Greek steganos and graphia, which mean cover-up and writing respectively, is where Steganography derived from [1]. The main purpose is to intercept and modify the encrypted message by changing it cannot be easily read format the enemy can detect. Steganography main goal is to protect so that secrete message through hiding it in other object is called cover, so that the message will be invisible to anyone [2, 3]. Protect the data from unauthorized user is the main concerning of the transmission information through the communication network. Several information hide mechanisms exist to deal with this problem like, Cryptography, Steganography, Digital watermarking, etc [4].

Steganography system consists mainly of two processes: Embedding and Extracting processes. In embedding process, the produced image can be named as a stego-image or a cover image and is used to embed the secret data. For hiding data inside image pixels, all selected pixels must be chosen secretly by using a secret key, which is commonly known as a stegokey [5, 6].

Imperceptibility /security and capacity are the primary components that make steganography thoughtful for information concealing, which likewise postures challenges.

## Mapping Methodology.

ASCII Mapping Technology (AMT), which a text steganography is based on, uses ASCII map technique to map the binary sequence of the secret message to generate the Stego-text. Quantum logic technique to find the valid embedding position increases additional level of security. AMT produces stego-text with minimum degradation. This property enables the method to avoid the steganalysis. The proposed steganography technique with ASCII map made a new model for the English steganography [4].

The colored image will be returned at first to its base values of mixed colors (RGB). The system presents a method to enhance the AMT by using the last two LSB bits to each blue color of pixel and compare embeds secret data, which encrypted.

Because the selection of color is based on differences in color and values of pixels' colors, detecting message will be difficult. So that there is no need to insert additional information, changing will be small and quality of the image will be great. [9]

Vyas and Pal introduced an improved LSB method [10], by finding the exact matching between the two least significant bits in image pixels' values (red, green and blue) and the secret data. This system presents a novel system to hide secret messages/data inside the image. This work finds the exact matches between the Blue scale of RGB image decimal values and the secret message/data after converting them to binary.

The system generates a key to recover the secret data, which is randomly generated based on matched pixels and the secret text. As well as, a Random Key-Dependent Data (RKDD) is generated without performing any changes on the image's pixel values [11].

### The Proposed Technique

The proposed system operations are converting secret message into LSB of blue sector of covering RGB image that will be represented as a binary for each pixel, the binary code for both character of the secret message and pixel value of blue sector dividing in to four divisions of 2-bits for hiding the secret message in that cover image.

The matches are saved and sent to the receiver in separate encrypted channel.

Figure-1 shows the structure of the proposed algorithm that can be summarized in the three steps as follows: -

### Embedding algorithm, the secret message

Input: secret message and RGB covered image.

Output: RGB covered image, MSE and PSNR.

The proposed algorithm steps are summarized as follows:

**First step (Preprocessing):**

- Select the covered color RGB image.
- Extract the Blue sector values from this RGB image.
- Read the secret message
- Convert the Blue sector values and each character of secret message into binary codes.
- Separate each binary value from to four sections each section contains 2-bits.

**Second step (Mapping technique):**

- Take each section of 2-bits of the character, then search to find the similar 2-bits in the binary value of each character in first and second division of Blue sector.
  - If this division of 2-bits of secret message matches the first 2-bits of Blue scale image, then the LSB of this Blue scale will be changed into '01'.
  - If this division of 2-bits of secret message matches the second 2-bits of Blue scale image, then the LSB of this Blue scale will be changed into '10'.
  - If this division of 2-bits of secret message does not match the first or second 2-bits of Blue scale image, then the LSB of this Blue scale will be changed into '00'.
- At the end of secret message, the LSB of this Blue scale will be changed into '11'.

**Third step (Accumulation):**

- Finally, the Blue scale will be returned and accumulating with the other two colors (Red and Green scales) to regeneration of the covered image to be sent to the destination.
- The PSNR and MSE was calculated to refer to the difference between the original and covered image, this was shown in table-1, and the architecture of the system was shown in figure-1.

**Results and Discussion**

When testing the suggested system, which is used to hide message in a cover image, by taking different sizes of messages and images. Tables-1 illustrates the PSNR and MSE of each image with the same secrete text.

The MSE and Peak Signal-to-Noise Ratio (PSNR) are commonly used measures for evaluating the performance of the proposed algorithms from the perspective of image quality degradation according to equation 1 and 2.

The MSE refers to the error between two images: - cover and stego-image, where PSNR refers to a measure for peak error.

The lower the value of MSE shows the lower the error while higher value for PSNR shows better quality for that image [7, 8].

To compute the PSNR, we first calculate the MSE using the following equation:

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n [C(i,j) - S(i,j)]^2 \quad (1)$$

Where,  $m$  and  $n$  are the image dimensions and  $C(i,j)$  and  $S(i,j)$  are cover and stego-image respectively.

Then PSNR computing using the equation (2) bellows:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \quad (2)$$

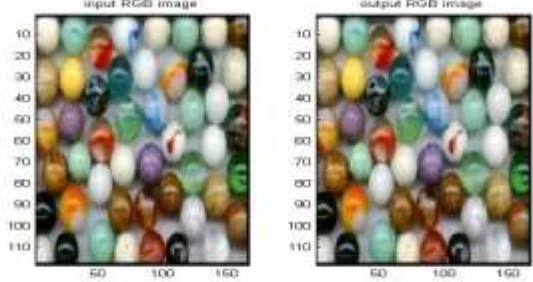

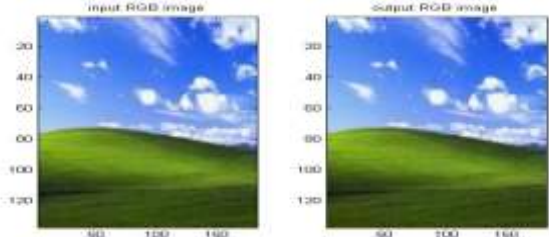

Where,  $R$  is the maximum possible value in the input image pixels?

For many important goals, the system was successful, which is, from the different experiments, system illustrates that the system successfully hides message in the cover image with minimum changes as show in table-1 above which is one of the important models for any steganography system.

## Conclusions

The proposed system used bits of the LSB of Blue scale of pixel for hiding characters of secrete message. When allocation each 2-bits from the character of the message overall same 2-bits of the blue sector of the image that will not change that image. The suggested system will use image to designate as a cover and a key for hiding and extracting secret message. Testing the proposed system for hiding the secret message, we recommend using it for protection from hackers.

**Table (1): Illustrates examples of RGB images with their PSNR and MSE for each example.**

Image	PSNR and MSE
	<p>PSNR = 63.3352 MSE = 0.0302</p>
	<p>PSNR = 65.6333 MSE = 0.0178</p>
	<p>PSNR = 56.9191 MSE = 0.1322</p>
	<p>PSNR = 77.5881 MSE = 0.0011</p>

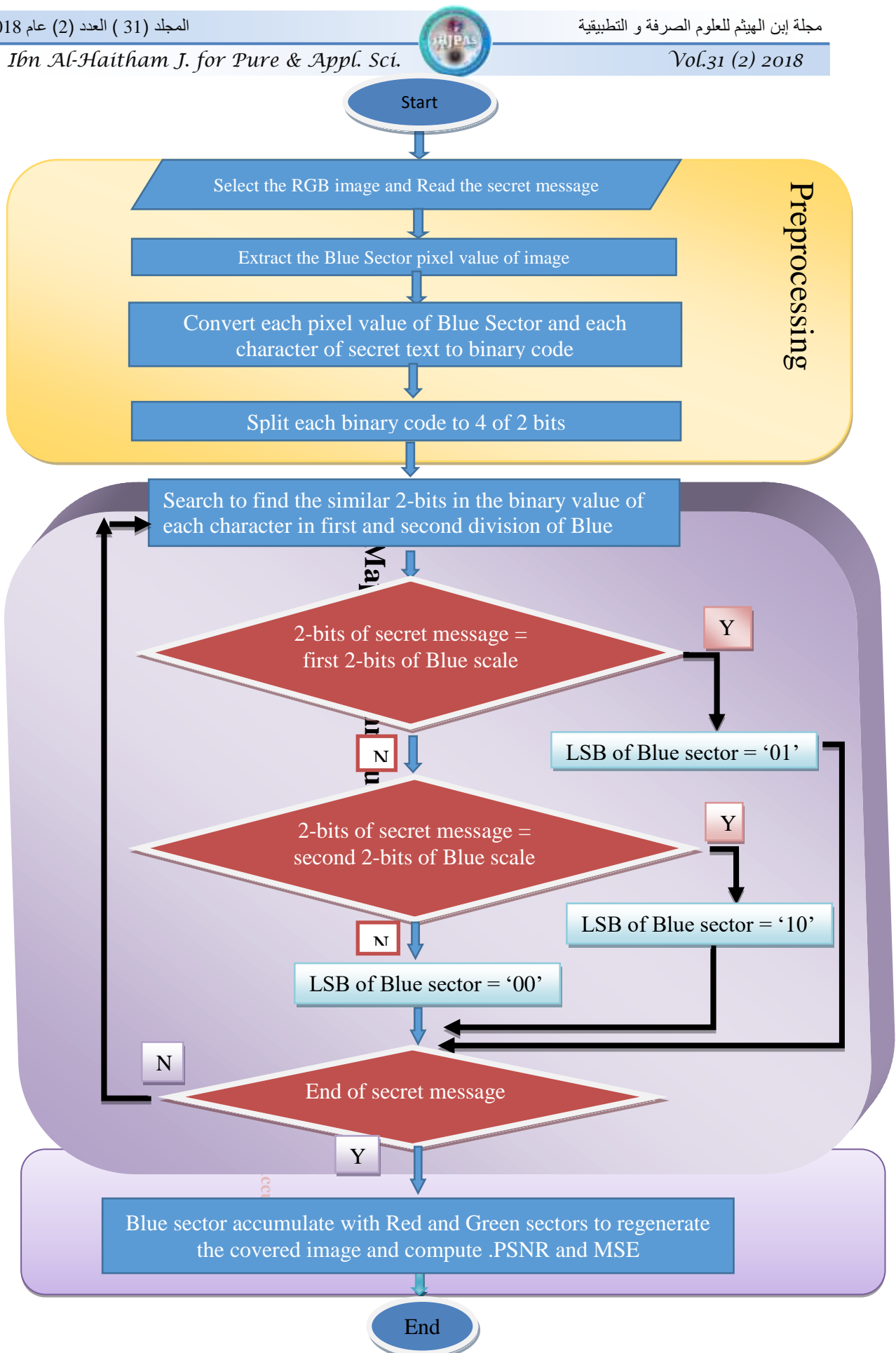


Figure (1): The architecture of the proposed system.

## References.

1. Ingemar J. Cox; Matthew, L and Miller, Jeffrey A.( 2009) ,( 2008). Bloom, Jessica ridrich and Ton Kalker, , " Digital Watermarking and Steganography" ,Second Edition, Morgan Kaufmann Publishers is an imprint of Elsevier, USA
2. Mohammed, A.F. Al-Husainy, " Image Steganography by Mapping Pixels to Letters", Journal of ComputerScience 5 (1),.33-38.
3. Al-Saffar Amna, (2011)"Proposed Steganography Method based on DCT coefficient", Education of Ibn Al- Haitham for pure since, Ibn al-haitham journal 24,. 311-319,.
4. Souvik Bhattacharyya, (2013) Pabak Indu and Gautam Sanyal, " Hiding Data in Text using ASCII Mapping Technology (AMT)", International Journal of Computer Applications, 70–18,.29-37,.
5. Randeepika Samagh and Shailja Rani,( 2015) "Data Hiding using Image Steganography", International Journal of Emerging Trends in Engineering and Development, ISSN 2249-6149, 123-124, 5,. 3..
6. Alaa A. Abdul Latef and Firas A. Abdul Latef,"Hiding Encrypted Color Image within MPEG-2 Video", Eng. and Tech. Journal , 30,.4 , 2012.
7. Rani, J. and Khan, T. A. (2014) "Performance Optimized DCT Domain Watermarking Technique with JPEG." International Journal of innovative Technology and Exploring Engineering, 4(2),.
8. Tuama, A. Y.; Mohamed, M. A.; Muhammed, A and Zurina, M. H. (2017) "Randomized Pixel Selection for Enhancing LSB Algorithm Security against Brute-Force Attack." Journal of Mathematics and Statistics13(2): 127-138,.
9. Vijaya Raghava Kukapalli, Tarakeswara Rao and Satyanarayana Reddy ( 2014) " Image Steganography byEnhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare", International Journal of puter Trends and Technology (IJCTT) –15, 3 ,.97-101,.
10. Krati vyas and B.L.Pal,( 2014)" A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering,. 3, 1,,: 5246-5251,.
11. Maher a. Alsarayreh, mohammad a. Alia and khulood abu maria,( 2017) ," a novel image Teganographic system based on exact matching algorithm and key-dependent data technique", Journal of Theoretical and Applied Information Technology,.95. 5,. 12.12-1224,