Journal of Education for Pure Science- University of Thi-Qar
Vol.12, No2 (December, 2022)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.12.02.20

Embedding Secret Data in Color Image Using LSB

Taleb A. S. Obaid

AlKunooze University College Al Basra, Iraq

Received 6/07/2022 Accepted 27/9/2022 Published 01/12/2022

Abstract:
Currently, steganography is considered the most powerful technique among other procedures to obscure the presence of buried information within a cover body. The Greek word steganographic means covered writing. This term may be considered the most appropriate to bury confidential secret data via internet correspondence. Steganography technique can be defined as the science of safe electronics transmitting. So, the aims of the steganography technique are to hide the presence of conveying data from un unwilling party. Various carrier object formats can be implemented, but color images become the more common among the other digital object. Currently, a lot of works adopted the image steganography as a cover object. The contemporary secure image steganography technique offerings a transferring the embedded confidential information task to the intended end point without being perceived or even suspicious by the attackers. There exists a large variability of steganographic techniques for fixed secret data in color images. Some of these techniques are more complicated than others, and each of these methods has positive and negative considered points. The objective of this work is to give a brief overview of steganography techniques using color images as a cover object by implementing MATLAB software using the LSB algorithm. We found that the carrier image keeps the original feature without any distortion caused by embedded secret information. The performance measured by PSNR and MSE technique and shown satisfied results.

Keywords: Image Hiding, Steganography, Cryptography, Least Significant Bits (LSB).

Introduction:

Most of the data around the world is stored digitally nowadays. The distribution of information has widely increased since the expansion of the Internet application and a lot of data is portable over the Internet application every day. The most substantial factor of the transmitted information through Internet communication is the safekeeping of information. Cryptography techniques were created as algorithms for camouflage writing data sending. Nowadays, there are many diverse methods established to encrypt / decrypt data to keep the safe data transmitted, Shind [1] and Obaid [2]. Unfortunately, sometimes the protection is not strictly enough to keep the message contents secured. Blur is required to rewrite the confidential data, in addition to, hiding any trace of it in the cover object been sent. The technique used to hide these data is called steganography, Al-Shatnawi [3] and Obaid [4].

Nowadays, the hiding data and cryptography techniques become two concurrent peers to conceal secret data that travels over various unsecured networks and the Internet. In order to remedy the problem of secured data travels, the cryptography technique is implemented besides hiding the secret data. Cryptography alone cannot provide total security since it is still available to perform cryptanalysis. Hiding the existence of secret data using steganography is most reliable technique to protect transmitted secret data. The individuals and enterprises aim to improve communication security using cryptography or steganography. But in practice, a mixture of both the techniques may offer better security in general, Lokhande [5].

One of the reasons that hackers can be efficacious discover secret data because most information can read and realized without difficulty. Hackers may make known information to others and intentionally alter the meaning to distort personality or organization and use it to upgrade an attack. To resolve this problem, we may use either cryptography or steganography. Cryptography is a technique to alter the body or formulation of a secret data. In contrast, steganography keeps the intruder to think about the existence of the hidden information Lokhande [5].

Steganography and cryptography are quite different procedures to keep secret data transmitted safely. Cryptography technique concentrates on keeping the secret data unreadable by rewriting it in the unexpected formula, while, steganography focuses on far from even thinking about the existence of secret data hidden by inserting this within the cover object. Both steganography and cryptography are methods to prevent unwanted parties from snooping on other people's messages to reveal their content. But neither of those ways alone is completely faultless. The steganography method used can be considered defeated by suspecting hidden information in the sent stego image. We may enhance the steganography technique by combining it with cryptography, Tiwari [6].

Steganography can be considered a branching of cryptography that tries to hide messages totally within other objects without the existence of any trace of a message. Information to hide can be anything: text, image, video, sound, … etc., see Roque [7]. To apply steganographic techniques a cover object, such as image, sound, video or audio is the most used today.

Literature Review:

Al-Shatnawi employed and analyzed the steganography technique. This proposed technique performed confidential information transition based on the similarity bits of the confidential information and the pixel image bits values. The proposed technique was implemented to hide the following secret information: "I will come to see you on the first of June" using two different BMP images. The size of the first one is "(24 x 502 x 333) and the second one is (24 x 646 x 165)". The results examined with a conventional LSB hiding technique. The investigated based on the ratio between the number of the matching and the non-matching bits between the pixel color values and the secret information values. The proposed method has proven efficient, fast, robust, and penetration resistance [3].

A work adaptive by Rogue, presented an innovative steganographic algorithm grounded on the spatial domain: "Selected Least Significant Bits (SLSB)". It runs with the LSB of one pixel of image color components and alters unsimilar bits according to the transmitted information bits to be hidden. The rest of the pixels are kept as they are without change in order to get the image color like the original one, [8], [9], and [10].

The image with confidential information inside it is called stego image. Transmitting stego images between two parties through network channels suffering from hacking detecting. Therefore, the process

of protecting the transmission of confidential information has become an essential task in today's world, Fkirin [11]. Recently, several techniques have been established to protect such transmitting. The main task is based on inserting confidential information in multimedia cover object.

Protect sensitive data against the malicious attack is the main objectives of the two publications by Varalaksshmi [12] and Nabi [13]. They implemented steganography technique to embedded confidential information in an image cover object. They encoded text in an image and the modified image that be send to the intended authorized person. This technique prevents the cybercriminals from even trying to think of a messaging hack. Once the authorized person received the stego image can be decode the confidential data that embedded in the sent image. The authors achieved the proposed algorithm using MATLAB using different types of image file, [14], [15], and [16].

Least Significant Bit Technique:

An effective technique to hide the presence of secret data inside a digital object carrier is steganography. The images are most covered objects in steganography applications. Intensive computations and high skill in application programming are required for embedding secret information inside image. As it is known the rightest bit has a lowest bit value of a binary code and is called "The Least Significant Bit (LSB)". LSB is one of the main techniques used in image steganography, see Moerland [17] and Wang [18].

The level of resolution in the image format is far from the possibility of human eyesight. Making a slight change in lowest bit (LSB) value in color components of an image will not be distinguishable by a human being eye. This slight change in the values of the bits of the color image compounds can be done using an LSB technique. The idea of LSB process is not complicated to perform such change bit values.

Tests have also proven that the LSB technique is a suitable style to insert secret information in a carrier object, such as image, video and audio files. In this method, the lowest bit value of the carrier file object is replaced with the bits value of secret data to be embedded. The most familiar carrier object is the images. The image that carries embedded secret data is called stego image. The steganography aims to make stego image look like the original image and has no distortion happened by insertion secret data. Computer image file shows diverse colors and concentrations of light on different zones of an image. The 24 Bit BMP image is best type of image file to cover secret data inside. When an image is of high quality and resolution it is more suitable to conceal more information within image, Choudary [19] and Kelvin [20].

In general, the right most (eighth) bit of a color byte is considered as the lowest value bit among other bits and called the Least Significant Bit. Therefore, the eighth bit of each color byte can be used to insert one bit of confidential information. When you use a 24-bit image, you can store three bits of confidential information in each pixel of image by replacing the least significant bits of each color component (Red, Green, and Blue), Champakamala [21].

Proposed Work:

In this work, we will need three pixels of the image to hide one byte of confidential information, as we modify the least valuable bit value of the image's color components with the corresponding bit of confidential information. The rest of the bits in the three pixels are leftovers without any changes. Let the three successive pixels are "pixel (i), pixel (i+1), and pixel (i+2)", with the three RGB components. Suppose that the binary pixel representation of three successive pixels in a color image is given as follows:

	Blue	Green	Red
pixel (i)	10101001	01001010	11001001
pixel (i+1)	11001010	10010101	10001000
pixel (i+2)	10101000	11001101	01001001

Fig. 3: Bits of three successive pixels.

Suppose that the number 270 represents our confidential information to be embedded in a cover image. The binary representation of 142 is 10001110. Now our mission is to embed these bits of confidential information in the least significant bit of each component's byte of the cover image. If we overlay these 8 bits of confidential information in a right location of the LSB of the three-consecutive pixel as in Fig. 4. In fact, we need only three pixels (8 bytes) to hide on byte of the confidential information. We may notice that the bits in underline bold font have been changed only among the rest of the bits of the image. So, the updating of these a few bits do not make any distortion on the original image itself.

Fig. 5, tries to illustrate the process of inserting one byte of confidential information into the cover image. As mentioned previously a number 142 or 10001110 in binary form is to be hidden in the color image with the least affected on the carrier color image.

Fig. 4, Three successive pixels beside secret data byte

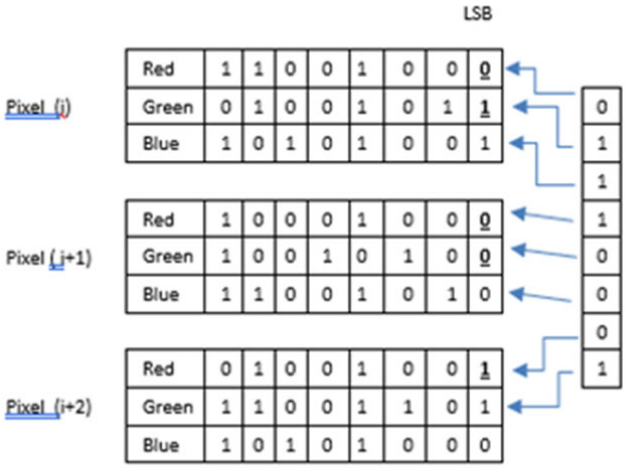

Fig. 5: Proposed LSB Algorithm

Figure 5, embedded number 142 ≡ (10001110) into the LSB of carrier image bytes. Notify that only the five bits really changed to embedded number 270 In general, the average number of bits that have changed out of the sum of the least significant bits value in the image, which are the same as the number of bits of confidential information, are usually less than half, and the values of the other bits of the image remain unchanged, Arya [22] and Odat [23]. To illustrate the process of inserting confidential information into the image carrier follow the algorithm:

Algorithm of LSB
Inputs: RGB image and confidential information
Output: Store the Result in Stego image
if cover image is not greater than confidential information Display message and stop
else
    Convert secret data into binary code
    Convert cover image into binary code
    Compute N as number of secret data bits
 for r = 1 to end binary cover image rows
    show the image component RGB
    hide all bits of the secret data in each LSB pixel
    if r greater than N
      stop
end
    save stego image with new values

Results And Discussion:

Steganography technique is the science of writing hidden confidential information in a carrier object, such as an image. We aspire from this technique to hide the confidential information features buried in the object that carrying this information to those people who are not authorized to see it. A conventional LSB algorithm is implied on the 24 bits color image. The algorithm mentioned above was applied to insert binary code of confidential information in the LSB of each color component of the

carrier image. This technique is implemented using MATLAB R2013a software. Two cover images carrier were used, the first one is light "flower image" RGB color BMP 225x225 pixels in size (24 bits/pixel), the second one is dark "galaxy image". The visualization results are shown in the below Fig. 6.

The method is practical to hide the secret data "embedded binary code of text in to LSB " on two different images. The first one is a "Flower" with dimension (1000x665) BMP which is a light image see Fig. 6 (a), whereas the second image with dimension (500x560), size 4.76 KB and called "Galaxy image" JPG as a dark image, see Fig. 6 (b). The secret data of 30 characters length "240 bits", size 1.90 MB have been used.

Fig. 6 (a): Light "Flower image".

Fig. 6 (b): Dark "Galaxy image".

1. Launch the matlab-13 to conceal secret data in an image cover object. The steganography process is shown in Fig. 7. The first window, Fig. 7 (a), asks you to Enter the Secret Data to be hidden in a cover image. We the Secret Data as in Fig. 7 (b). let the Secret Data is "embedded binary code of text in to LSB" have been Entered as in Fig. 7 (b). The original image used is shown in Fig. 7, (c) before hiding

the secret data. Finally, Fig. 7 (d) shows the image after the secret data has been hidden called *"stego image"*. Fig. 7 (e) shows the end process. Fig. 7 (f) show the extracted embedded message as a text file. The human eyes couldn't notice any distinctions between the two images, "the original image and a stego image", i.e., before and after the hiding process.

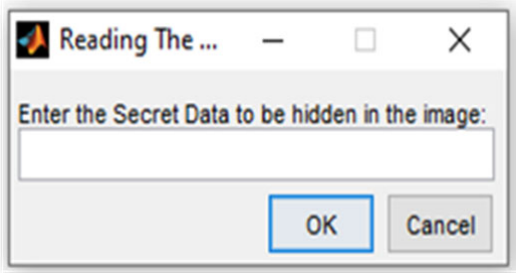

Fig. 7 (a): Once the MATLAB been launched.

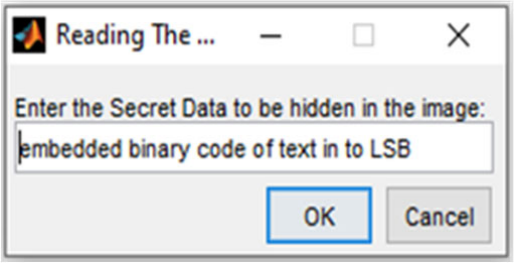

Fig. 7 (b): The secret data has been entered.

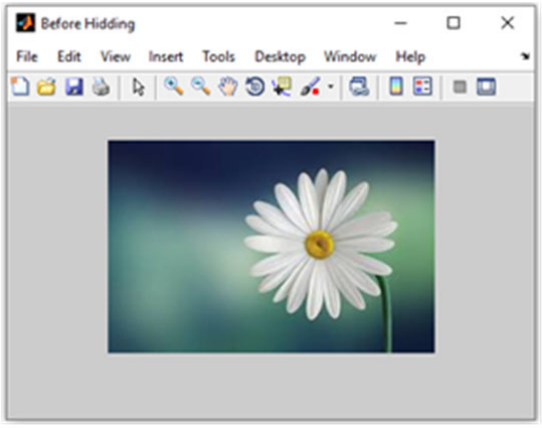

Fig. 7 (c): The original image before any process.

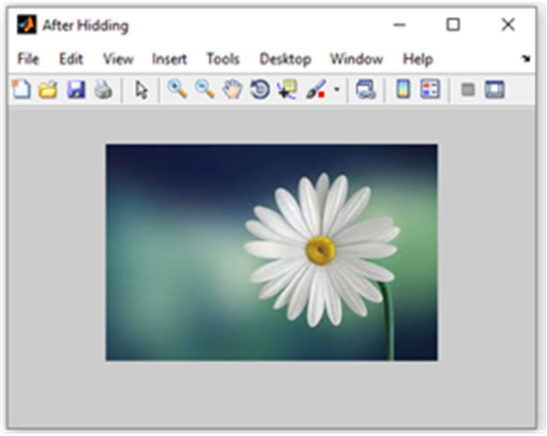

Fig. 7 (d): The image after been process.

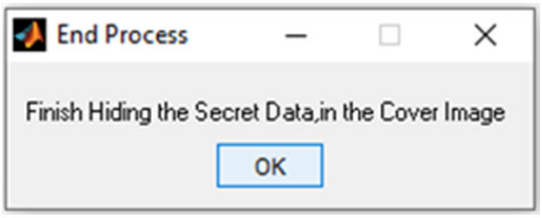

Fig. 7 (e):The end process message.

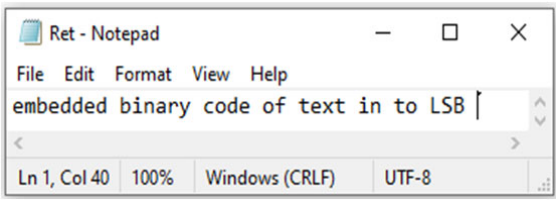

Fig. 7 (f): Saved the Embedded Message.

Performance Criteria:

In order to evaluate the embedded image, the following performance criteria are used, [12].

Peak Signal to Noise Ratio (PSNR)

The correctness of the steganography algorithm can be measured in the process of embedding confidential data in digital image files. Use the PSNR standard to measure the noise ratio between the embed image and the original image based on the PSNR criterion value, the image quality will be better when the criterion value is higher.

Mean Square Error (MSE)

The MSN standard measures the cumulative squared error between the embedded image of the information and the original image. The smaller the value of this measure, the more effective and efficient the method of concealing information within the coverage period.

To compute the PSNR, the block firs calculates the mean-squared error using the following equation

$$MSE = \frac{\sum_{m,n}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Where M and N are the number of rows and columns of the input images. (I1) and (I2) are the original image and stego image, respectively.

Then the block computes the PSNR using the following equation:

$$\text{PSNR} = 10\ log_{10}\frac{R^2}{(MSN)}$$

Where R is the maximum fluctuation in the input image data type.

Table 2. Comparison of Original Image Vs Embedded Image

Image Name	MSN	PSNR
Tropical Image	6.34043	60.1436
Flower Image	3.1702	43.3718

Table 2 shows the effectiveness of the applied algorithm in hiding confidential information in the images of coverage used and achieving the criteria referred to in the above.

A MATLAB program is developed to embed the data onto the image and to retrieve the hidden text from the embedded image by Decoding.

Conclusion And Future Work:

The Steganography technique has the ability to hide embedded confidential information in test format in an image carrier object. This technique with any message tracing when transmitted through the harmless network. The proposed LSB algorithm given in this work helps to fruitfully hide the confidential information within an image cover object without any distortion of the original image using MATLAB 2013a software. Because this method does not seriously affect the all pixel values of the image, so there is no loss of valuable resolution in the image. The transmitted confidential information can be retrieved back from the stego image without any loss.

R-G-B plane is separated and the proposal LSB algorithm is implemented for data embedding process. The retrieval of confidential information is precise and reliable. After extracting the secret message from stego image, the stego image remains preserved in its form and the confidential information in which it was planted within it. Zooming in and increasing its resolution can accommodate more confidential data. High resolution image can increase data hiding capacity and diminishes image quality distortion.

Future work can accommodate more random methods of hiding messages, in addition to, integrating cryptography with steganography to provide much more security to the confidential information. Moreover, we may adapt different technique to develop selecting certain region of color image to get better security. In addition, we can resort to random selection of image pixels and the scattering of confidential information to be transmitted.

References:

[1] H. N. Shinde, A. S. Raut, S. R. Vidhale, R. V. Sawant, V. A. J. I. J. o. E. Kotkar, and C. Science, "A Review of Various Encryption Techniques," *International Journal Of Engineering And Computer Science,* vol. 3, no. 09, 2014.

[2] T. A. Obaid, M. J. Khami, and L. G. Shehab, "A classical approach for hiding encryption key in the same encrypted text document," *Journal of Kufa for Mathematics and Computer,* vol. 5, no. 1, pp. 25-38, 2018.

[3] A. M. J. A. M. S. Al-Shatnawi, "A new method in image steganography with improved image quality," *Applied Mathematical Sciences,* vol. 6, no. 79, pp. 3907-3915, 2012.

[4] T. A. Obaid, "Enhanced Least Significant Bit Technique for Hiding a Text Message in an Image Cover Object," vol. 10, no. 1, 2019.

[5] U. Lokhande, "An Effective Way of using LSB Steganography in images along with Cryptography," *International Journal of Computer Applications* vol. 88, no. 12, 2014.

[6] A. Tiwari, P. Vashistha, "Information Hiding using Steganography and LSB Technique," *International Journal of Advanced Science and Technology,* vol. 29, no. 5, pp. 6, 2020.

[7] J. Roque, and J. M. Minguet, "SLSB: Improving the Steganographic Algorithm LSB." pp. 57-66.

[8] S. Singh, and A. Singh, "A review on the various recent steganography techniques," 2013.

[9] W. Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check," *Sādhanā,* vol. 43, no. 5, pp. 68, 2018.

[10] P. A. K. Maganbhai, and K. Chouhan, "A study and literature review on image steganography," *International Journal of Computer Science and Information Technologies,* vol. 6, no. 1, pp. 685-688, 2015.

[11] A. Fkirin, G. Attiya, and A. J. C. o. A. E. El-Sayed, "Steganography Literature Survey, Classification and Comparative Study," *Communications on Applied Electronics* vol. 5, no. 10, pp. 13-22, 2016.

[12] R. J. J. o. C. R. Varalakshmi, "Digital Steganography for Preventing Cybercrime Using Artificial Intelligence Technology " *Journal of Critical Reviews* vol. 7, no. 6, pp. 2020, 2019.

[13] F. Nabi, and M. M. Afzal, "Image Steganography: Critical Findings through Some Novel Techniques," *International Journal of Innovative Technology and Exploring Engineering*.

[14] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey." p. 052003.

[15] S. Gupta, A. Goyal, and B. Bhushan, "Information hiding using least significant bit steganography and cryptography," *International Journal of Modern Education and Computer Science,* vol. 4, no. 6, pp. 27, 2012.

[16] M. A. A. Pujari, and M. S. S. Shinde, "Cryptography And Encryption Algorithms For Information Security," *International Journal of Advance Engineering and Research Development*.

[17] T. Moerland, "Steganography and steganalysis," *Leiden Institute of Advanced Computing Science*, 2003.

[18] H. Wang, and S. J. C. o. t. A. Wang, "Cyber warfare: steganography vs. steganalysis," *Communications of the ACM,* vol. 47, no. 10, pp. 76-82, 2004.

[19] A. Choudary, "Steganography Tutorial – A Complete Guide For Beginners," *online website*, 2020.

[20] K. S., "Steganography: Hiding an image inside another," 2018.

[21] B. Champakamala, K. Padmini, and D. Radhika, "Least Significant Bit algorithm for image steganography," *Int. J. Adv. Comput. Technol,* vol. 3, no. 4, pp. 5, 2014.

[22] A. Arya, S. J. I. J. o. F. R. i. C. S. Soni, and C. Engineering, "A literature review on various recent steganography techniques," *International Journal on Future Revolution in Computer Science & Communication Engineering,* vol. 4, no. 1, pp. 143-149, 2018.

[23] A. M. Odat, M. A. J. I. J. o. S. Otair, and Technology, "Image steganography using modified least significant bit," *Indian Journal of Science and Technology,* vol. 9, no. 39, 2016.