Performance Evaluation of LSB Technique into visual Objects based on Steganography

Bashir M. Mujber [1*], Ali Ahmad Milad [1,2]
[1]mojbar_ca12@yahoo.com, [2]alimilad@elmergib.edu.ly
[1]Department of Computer, Faculty of Education, Elmergib University
[2]Faculty of Information Technology, Elmergib University
*Corresponding author email: mojbar_ca12@yahoo.com

ABSTRACT

Steganography is an important field of research in recent years to embed a range of data, it is the science that hide information in cover medium without being accompanied by any effect or distortion in that medium. Nevertheless, most of the modern researches focus on hiding information in image according to its popularity. This paper studies the Least Significant Bit (LSB) (1-LSB, 2-LSB and 3-LSB) with one or RGB color based Steganography, The LSB algorithm has experimented on Bitmap 24 bits format as cover image to generate a stego images. The aim of this paper is to carry out various types of image steganography technique for purpose of identifying various principles of image steganography in terms of visual effectiveness and efficiency. However, the algorithm that has been chosen for this purpose is discussed in details in this paper. The visual effectivity of the stego were measured by comparing the histograms of the stego and cover images. In this study we used Mean Squared Error MSE calculation and discussed the implementation of this algorithm in detail. The results from experiments prove that algorithm is not affected by different visual characteristics of the cover images in so doing, the perceptual distortion to the cover image is nearly negligible and unlikely to be detected by simple visual inspection.

Keywords: steganography, LSB, RGB

1 Introduction

Steganography means verbatim which covers the procedure of writing, and is studied as one of the most crucial communication arts [1]. It contains two words, the first word is Steganos means "coverage" and the other word graph in which means “writing” in Greek. The main idea of it is to conceal the communication procedure without using encryption algorithms that make the process of communication non-understandable except for those who have the right keys [2]. Steganography inside the image is the process of developing a hidden message within the same or given image so that nobody can know what the message is or should not be able to detect its presence.

The term Steganography means “cover writing” while Cryptography means “concealed writing” as showed in figure 1 and 2. Cryptography is the procedure of sending the message in distinctive forms so that only the involved people can demystify the message and then read it [3]. The message that is sent without encryption is called the plaintext whereas the

enciphered message is labeled as ciphertext. The procedure for changing the plaintext to a ciphertext is called encryption while the reverse operation (i.e., alteration of encrypted text to a plaintext) is called decryption. Encryption protects the contents of the message by encrypted it during transmission of data from the sender to the receiver. However, when the receiver receives the message he decrypts it and ensures from its integrity Steganography works to conceal the message in plain view inside the data instead of encrypting it and does not require sending confidentially [4].

At the present time, steganography works on digital media as cover image and embedding digital media as secret message, the example for the used digital media are .wav, .gif, .bmp, .jpeg, .txt, .mp3, and .doc. Steganography is thought to be one of the most essential techniques to the future of the Internet in terms of privacy and security. The importance of steganography is highlighted because of the weakness in the encryption process and the desire to get the secrecy in the open systems. Lots of governments have made laws in an effort to decrease the strength of encryption systems or completely prevented them; this may create unfortunately weak and breakable encryption algorithms in the Internet community [5]. Hence, the of steganography appears more than ever significant where the hidden message inside another file can be detected and read only by the involved entities or individuals and no one has the ability to read the message even with the knowledge of its existence. However, encryption and steganography do not provide the desired privacy and confidentiality, but that can be accomplished by utilizing both technologies to provide acceptable limits of privacy and confidentiality of anyone connected to the open systems [5].

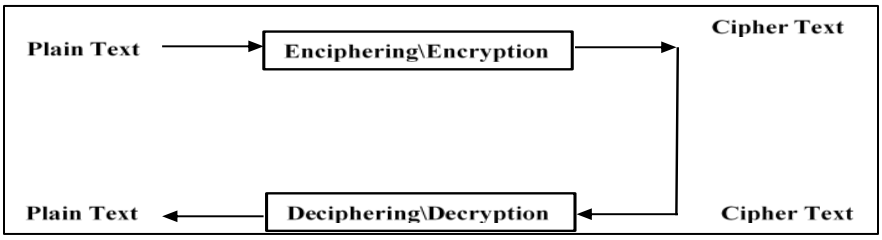


Figure 1: *Cryptography*

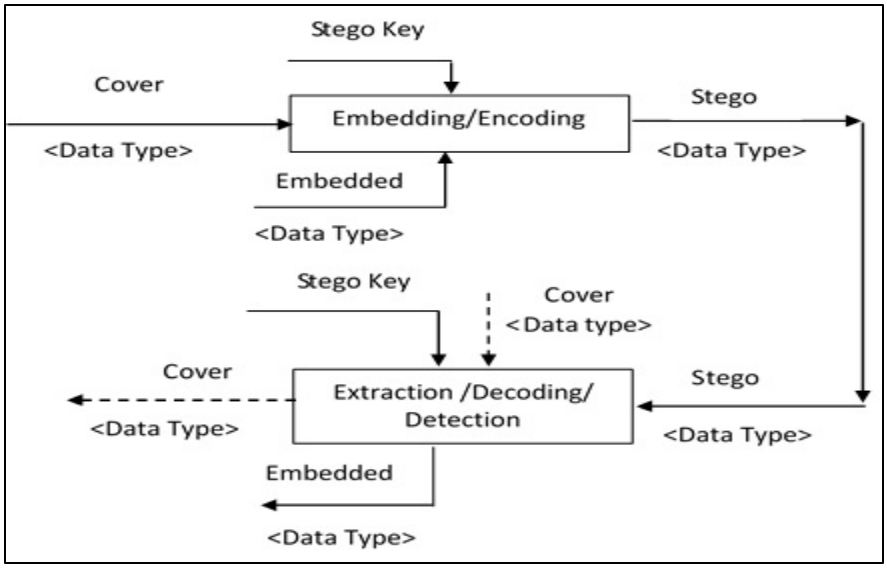


Figure 2*: Steganography*

There are many techniques which can be applied for concealing information within the multimedia objects, with audio files, image or video object cover depending on the object type given below. Here we will discuss various methods and techniques that are frequently applied in text, image, audio or video of steganography.

- Text: The procedure of hiding a text inside text can be accomplished by changing the text format or by changing certain properties in text elements such as letters. The goal of designing coding methods is to initiate changes that are unbreakable even if they contain noise [6], [7].
- Audio: The process of concealing information is computer-based audio steganography system, secret messages are embedded in digital sound [8]. Here a message is hidden in the mode of a simple change in the binary sequence of an audio file.
- Image: To embed specific messages or text inside an image that requires encrypting all message bits or inserting noisy areas which brings less attention so that we could hide our specific message within the region of huge natural colors variations. It is equally possible that the hidden message is randomly distributed to various sections of the image. There are numerous methods that are utilized for the reason of hiding information within the image [9].
- Video: The video file is a collection of concealed images with added voices to it, here the intended information is hidden in form of displayed images using image concealing techniques such as DCT [10].

There is a system applied to the colored image by using LSB method. The system compares the value for each ASCII character with palette location of the image if the value is equal to the palette value that is compensated in another location [11]. A system designed an efficient system to check the image as if to see it contains a secret message or not. Through the system

has extracted the secret message, which may be in the form of text or image, and when it fails to extract the hidden message or keep it from traffic, the system destroys the hidden text [12]. Fridrich J. and Goljan M. In 2003 described steganography where they took large loads of gray scale images and added a few amplitude of the noise to the image pixels with certain specifications. Susceptibility noise distribution is arbitrary so the parties related to it have the possibility to hide the noise in conformity with the output noise of the devices themselves [13].

2 System Design

Least significant bit insertion (LSB): LSB is substitution method that uses specific k LSBs in each pixel to hide a secret message. It is thought as one of the easiest ways to conceal a secret image in a specific image. Nevertheless, it is not difficult to disclose a stego-image that is related by using the LSB insertion technique [14].

We have selected the image carefully for that it is complicated and of multi characteristics, it is expected here that it has an effect in power and capacity, all images have the same size 300*200 on two formats BMP, JPEG, as given in the following: We examined if the characteristics of the cover image has impact on the concealment efficiency of stego.
In figure 3 (A) Group_of_student: here the dominant color is the blonde color regarding the hair, but the color of the jackets is black which makes it also a dominant color in this picture. (B) Living_room_home_house, it is obvious that the dominant color is green color of the trees and the field which has a light green color. (C) Spring_sunshine_may the dominant color is pink color, although it is complicated to tell the exact color.

Figure 3: *Cover Image Selection A, B and C*

In this paper the text file was chosen in making our experiment and the reason for that is the objective which is, to use the maximum insertion capacity of every method which is not expected in few of them and also depends on formats and scenes of chosen image, that leads to use a concealed message that is different in size for every experiment. We used a text message since it is not important for our study whether the message is text, voice or another image, it is just a data, a collection of 0's and 1's… Therefore, with regard to, 'Vocabulary as a reflection of life wisdom [15] we have chosen the below mentioned paragraph given in bold, as the concealed message for our experiment, and it is kept in a text file to be used with the suggested techniques. Emphasize the repetition of the same text to fill up the total capacity of the cover image which differs depending on the steganography technique used.
"Comprehend the environment in terms of discrete objects and events as a result we can say that the world consists of a multitude of uniquely defined objects and

events They can be further organized into classes as groupings based on the criterion of similarity or shared characteristics The mental construction which comprises the criterion of similarity and which subsequently enables the classification of objects is called the concept In other words it stands for or represents a common set of attributes of an object or event" [15].

The advantage of using LSB steganography is not needed to a complex calculation for the purpose of the data hiding in the image as well as it is considered one of the most prevalent methods to hide data in the spatial domain of the image. These methods are simple to implement, however, over time the tool Internet offers the possibility to identify and extract the information in any bit plane. Therefore there is a need to make a program which permits us to withhold information in an image using proper to the purpose of the research, so we develop program to adjust some variation of parameters and getting the final result of the application as stego image file. Based on the inherent characteristics of the human eye and images in this paper.

LSB in Single Color

- **One LSB**: Basically it consists of changing the least important bit of the color bands (R, G or B) of an image cell array in consideration to enter the message utilizing the space of one bit per pixel to store the message. Besides the already mentioned low computational cost that is characteristic of LSBs algorithms, specifically in this regard we can quote high fidelity between the original image and the stego-image. The change of just one bit ensures a great difficulty to note the "naked eye" the contrast between them in Figure 4. Here, one bit stored in accordance to the method described in this Section.

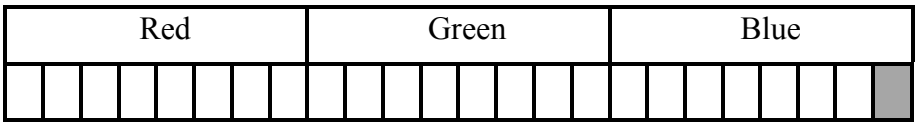
- 

Figure 4*: One bit in Blue Color*

- **Two LSBs**: A slight variation of the one LSB, the only difference, as its name suggests, is to use two least significant bits of the color bands (R, G or B) separately in the image. The subtle difference is in the ability to the hide message stored twice, and the change in the figure is also a bit sharper, but still generally imperceptible to the "naked eye", as we can observe in Figure 5, where two bits of message stored in it.

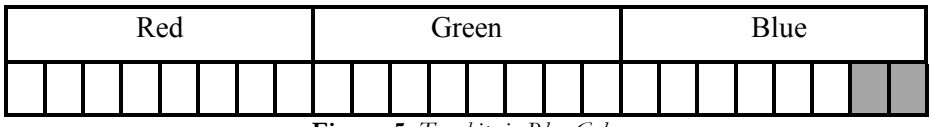


Figure 5*: Two bits in Blue Color*

- **Three LSBs**: In general, the three LSB bits boost the quantity of bits to be used. This causes a boost in storage capacity over a stego-image quite modified from the original. To illustrate, Figure 6 presents an example of inserted three bit in one color in pixel.

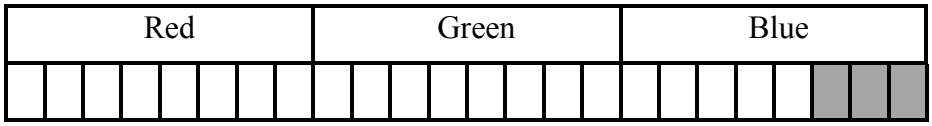


Figure 6*: Three bits in Blue Color*

- **LSB in Three Color (RGB):**

The least important bit to be modified is switched between bands cyclically. For example, a message to store only four bits in the image the algorithm record the first bit in the R band, the second bit in the G band, and B in the third quarter turn to band R in next pixel. Thus, a switchover is produced in order pixels to be modified to achieve thus imposing a difficulty more for steganalysis to detect and get the message correctly. Figure 7 shows the one, two and three bits of secret data using the cyclical LSB algorithm.

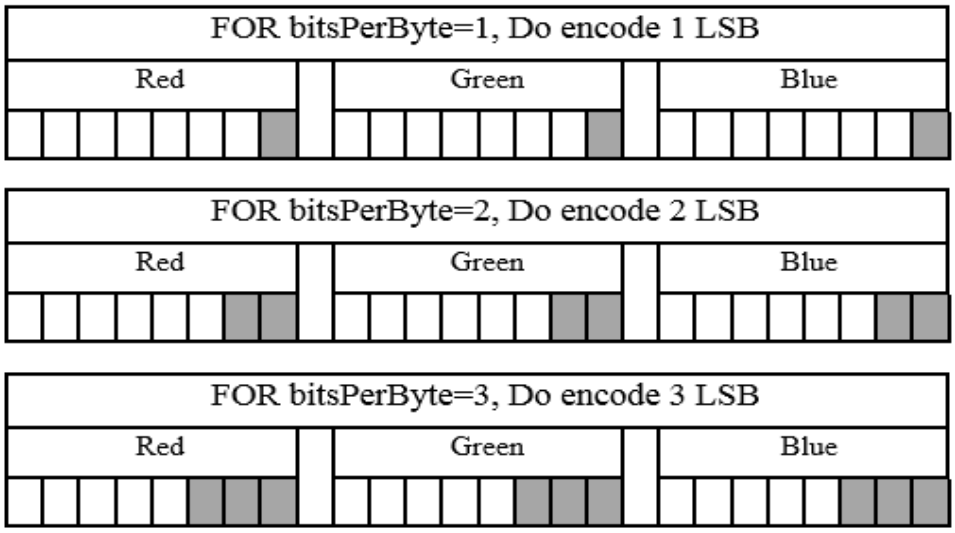


Figure 7*: LSB Three Colors Embedded*

The algorithm has been tested and validate using MATLAB and each allows the variation of Parameters such as number of bits or color component to modify. The techniques were developed initially in the shape of scripts, wherein each was implementing a method (LSB bit 1, etc.). Subsequently, aiming facilitating experimentation and obtaining the results, a graphical interface was created (GUI) using the guide Matlab. This interface provides a facility to choose the parameters of each experiment. In Figure 8 one can notice the GUI.

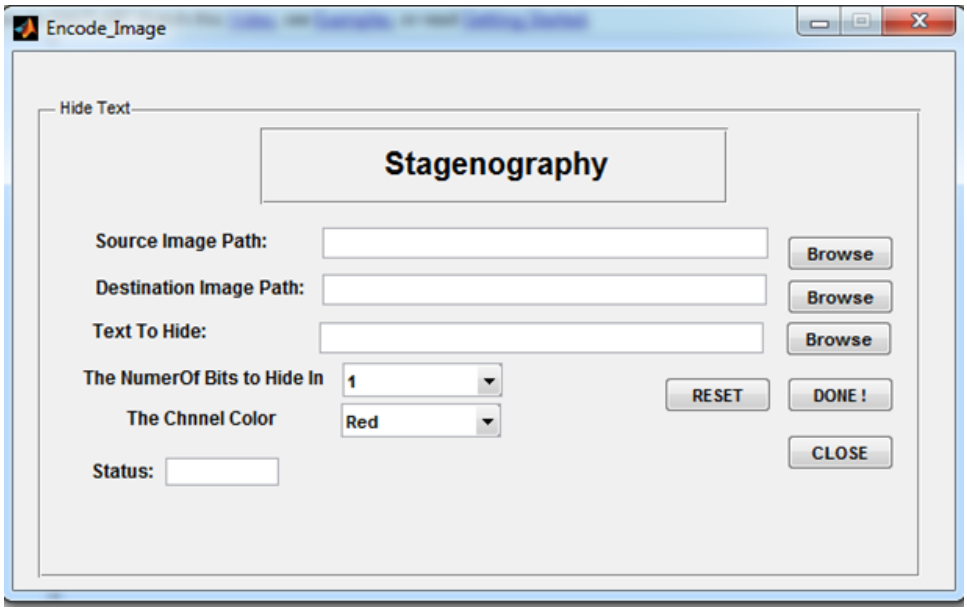


Figure 8*: LSB Method Interface*

With regard to the parameters of each algorithm, we varied the use of each one of them in regards to the number of LSB bits to be modified in the image in consideration to making it possible the analysis of the impact which this change does not only through use of the similarity indices, but also by our visual system. In choice of which color component (R, G or B) to modify we opted for, where possible, modify each of color separately and all of them because of the difficulty inherent to the human being to visualize this component. Therefore, we sought to make changes in the images less possibly noticeable to our eyes.

In this case, the quality criteria are either subjective (determined by the human eye), or based on image characteristics: shape and parameters of the brightness distribution, the width of the spatial spectrum, etc. Moreover, objective criteria used in assessing the quality of the images are criteria to get a computed image characteristic difference signal between two images: a real and some ideal, or it may be the original and transformed. They are called difference metric distortion. Using these criteria it allows to evaluate the quantitative changes of brightness levels of image distortion. When creating transformations (filtering, data compression, etc.) that is substantially the quality of the conversion means - algorithm or system. It is extremely necessary in the construction of algorithms and image processing systems and algorithms for evaluating quality.

The histogram is a significant statistical characteristic of data. In various image processing applications, the histogram is generally utilized as the basic characteristic to present the distribution of the intensity, color, and texture parameters of images. As a statistical feature, the histogram is equally not sensitive to translation and rotation of objects. Meanwhile, it is a standardized and compressed data storage type that can save much space. Because of these advantages and along with the same, the histogram is used mostly in image segmentation, registration, tracking, and especially in the image retrieval field that involves a large amount of

data. The following formula calculates the histogram measurement where its parameters are k is the maximum pixel value in an image, m is the pixel value.

$$n_i = \sum_{i=1}^{k} m_i$$

The most popular distance tools for analysis of the level of distortions that are introduced into the cover image at the time to hide the information, therefore, MSE can be utilized to examine the quality of the stego-images as well. MSE is the ratio of sum of the square of the differences in the pixel values between the corresponding pixels of the two images over total pixel number. MSE can be calculated if two images dimensions are equal. If two images are identical MSE value will be 0. Next formula shows how to calculate MSE value. X and Y are images with same dimensions. m and n are the dimensions of images [16].

$$MSE(X, Y) = \frac{1}{(m.n)} \sum_{i=1}^{i=m} \sum_{j=1}^{j=n} [X(i, j) - Y(i, j)]^2$$

3 Results and Discussion

Here, the results of the histograms were collected for the stego images that have one color modulation in one form, and RGB colors stego images. The one least significant bit result is shown in the figures 9 and 10, two least significant bit result in the figures 11 and 12, and three least significant bit result in the figures 13 and 14.

One LSB:

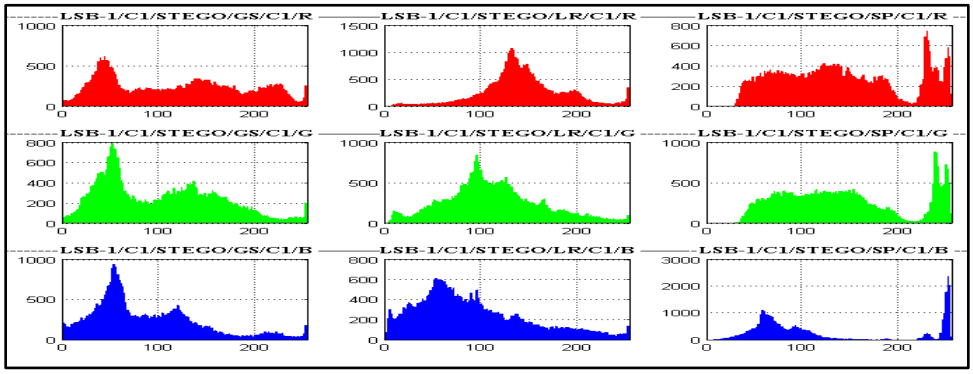


Figure 9: Histogram of One LSB One Color

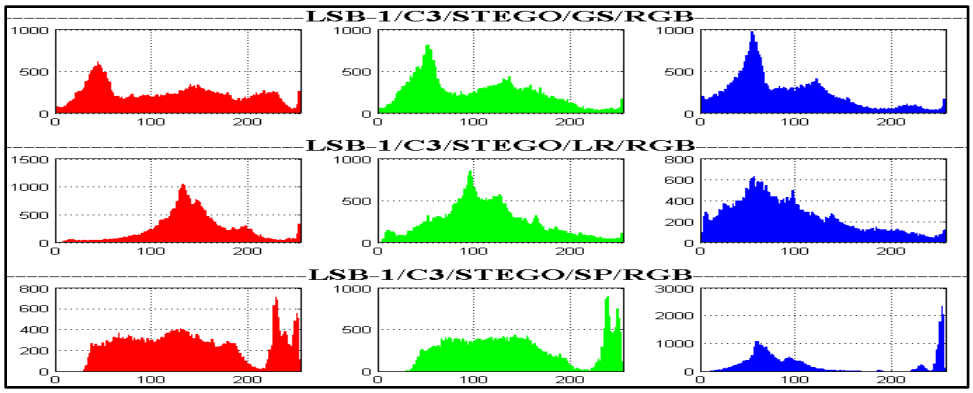


Figure 10: Histogram of One LSB RGB Color

Two LSBs:

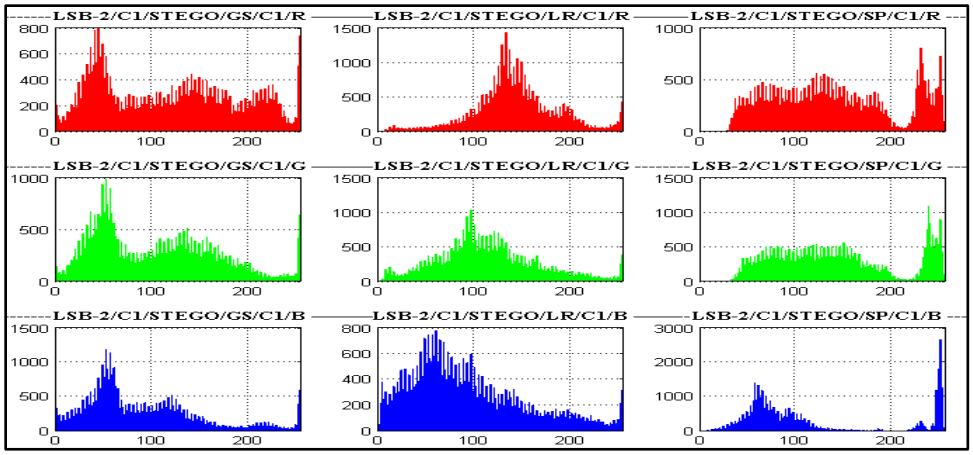


Figure 11: Histogram of Two LSB One Color

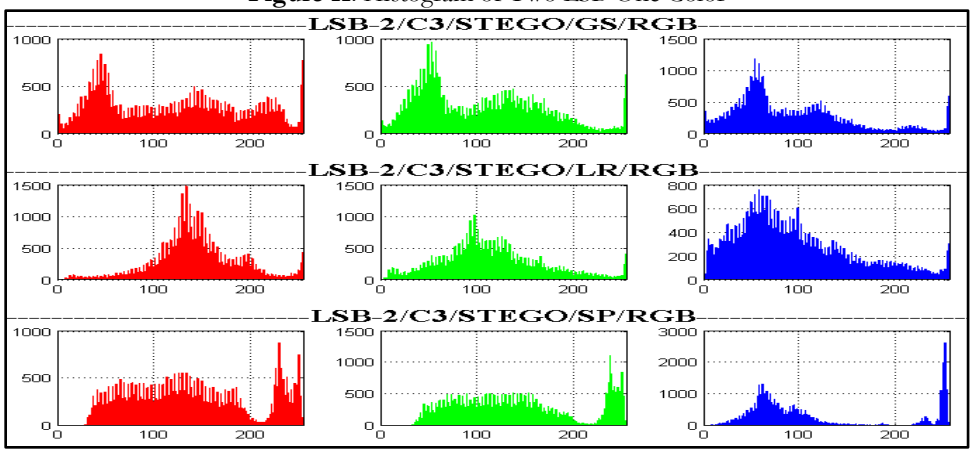


Figure 12: Histogram of Two LSB RGB color

Three LSBs:

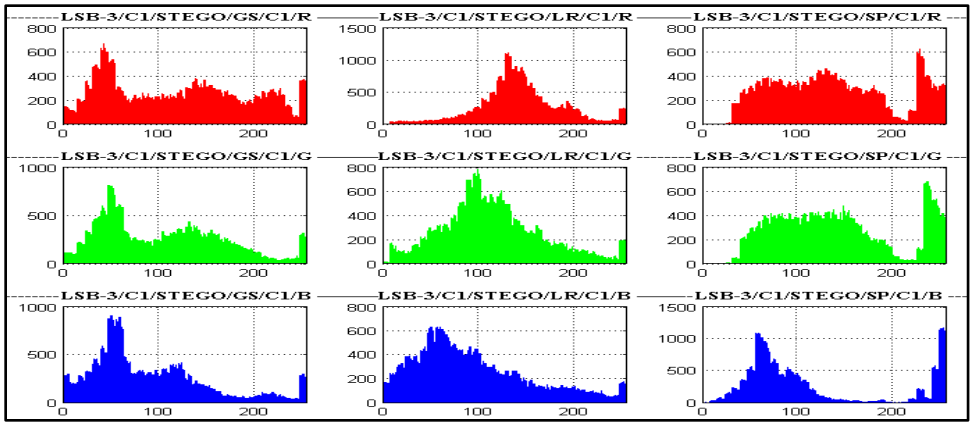


Figure 13: Histogram of Three LSB One Color

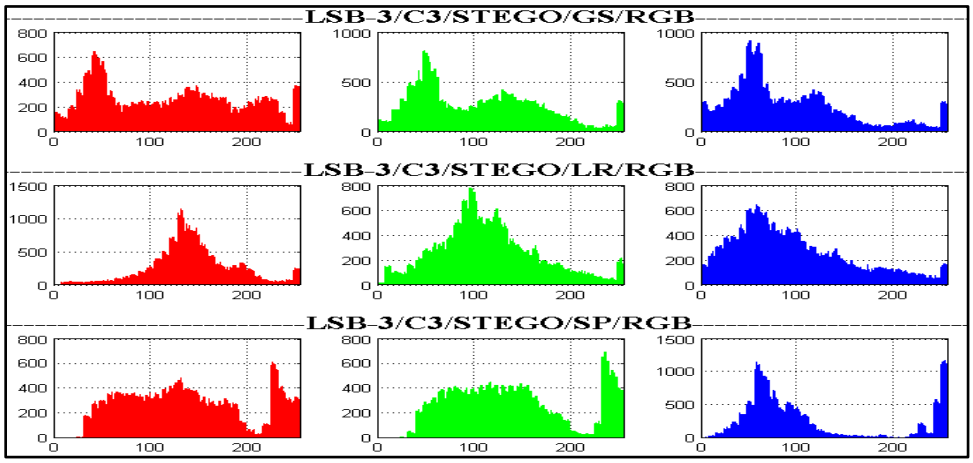


Figure 14: Histogram of Three LSB RGB color

In Table 1, we have presented the results of MSE parameter that have been obtained using LSB algorithm. Through this table, one can notice that the error values of a single color that is experimented on three images (as can be seen) are increasing with the increasing number of bits insertion, while, the increasing error values for all the stego-images are considered as slight which is between 0.0881% to 1.9801 in the average. However we found it imperceptible with the human eye. Nevertheless, the RGB error rate values as described in Table 2 are higher than the error rate for a single color and it is also considered as a small percentage and cannot be observed by the Human Visual System as well.

Table 1: *MSE Results of LSB Method with One Color*

LSB	Group_of_student			Living _room_home_house			Spring_sunshine_may		
Bits	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
One	0.0903%	0.0888%	0.0898%	0.0891%	0.0896%	0.0901%	0.0886%	0.0881%	0.0884%

Two	0.4447%	0.4459%	0.04437%	0.4346%	0.4458%	0.4431%	0.4454%	0.4356%	0.4345%
Three	1.9801%	1.9563%	1.9532%	1.9009%	1.938%	1.9334%	1.8638%	1.8985%	1.7408%

Table 2: *MSE Results of LSB Method with RGB Color*

LSB	Group_of_student	Living _room_home_house	Spring_sunshine_may
Bits	RGB	RGB	RGB
One	0.2686%	0.2679%	0.2650%
Two	1.3345%	1.3231%	1.3194%
Three	5.8868%	5.7983%	5.4970%

4 Conclusions

Steganography is an important tool in hiding the information either during transfer or in storage. It was discovered a long time ago as a cryptographic method. Since then, it has been used to hide large amounts of data securely and reliably to some extent. The technique which has been used in this research namely LSB, which is easy to use for concealments and extraction operations.

According to the results that were obtained in MSE analysis and by visual comparisons on histograms of the original and the stego-images, one can perceive the distinctive effects of different algorithms and also varying influence of the images with different visual characteristics. However, by looking to the results of MSE parameter that we have obtained, it is clear that the information hiding efficiency of LSB algorithm is not effected by different visual characteristics of the cover images which were in bitmap format if we use 1-LSB, 2-LSB and 3-LSB.

References

[1] N. F. Johnson, and S. Jajodia, *"Exploring steganography: Seeing the unseen,"* Computer, vol. 31, no. 2, pp. 26-34, 1998. https://ieeexplore.ieee.org/abstract/document/4655281/

[2] N. Johnson, "*Digital Watermarking and Steganography: Fundamentals and Techniques*," ACM Digital Library, 2007. https://dl.acm.org/doi/book/10.5555/1557373.

[3] A. A. Milad, Z. Muda, Z. A. B. M. Noh, and M. A. Algaet, "***Comparative study of performance in cryptography algorithms (Blowfish and Skipjack)***," Journal of Computer Science, vol. 8, no. 7, pp. 91, 2012. https://thescipub.com/abstract/jcssp.2012.1191.1197

[4] S. M. Thampi, "***Information hiding techniques: a tutorial review***," arXiv preprint arXiv:0802.3746, 2008. https://arxiv.org/abs/0802.3746.

[5] B. Dunbar, "***A detailed look at Steganographic Techniques and their use in an Open-Systems Environment***," Sans Institute, vol. 1, 2002. https://www.sans.org/webcasts/security-compliance-hypergrowth-startup-113570.

[6] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," IEEE Journal on Selected Areas in Communications, vol. 13, no. 8, pp. 1495-1504, 1995. https://ieeexplore.ieee.org/abstract/document/464718/.

[7] H. Singh, P. K. Singh, and K. Saroha, "***A survey on text based steganography***." Proceedings of the 3rd National Conference; INDIACom-2009 pp. 332-335. 2009.

[8] N. F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures:" Springer Science & Business Media, 2001. www.wakp.nl.

[9] A. Singh, and S. J. Singh, "***An overview of image steganography techniques***," International Journal of Engineering and Computer Science, vol. 3, no. 07, 2014. http://103.53.42.157/index.php/ijecs/article/view/1199

[10] N.-D. Hoang, and Q.-L. Nguyen, "***A novel method for asphalt pavement crack classification based on image processing and machine learning***," Engineering with Computers, vol. 35, no. 2, pp. 487-498, 2019. https://link.springer.com/article/10.1007/s00366-018-0611-9.

[11] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L. Xiang, "***Coverless real-time image information hiding based on image block matching and dense convolutional network***," Journal of Real-Time Image Processing, vol. 17, no. 1, pp. 125-135, 2020. https://link.springer.com/article/10.1007/s11554-019-00917-3.

[12] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, and G. M. Bhat, "***Information hiding in edges: A high capacity information hiding technique using hybrid edge detection,***" Multimedia Tools and Applications, vol. 77, no. 1, pp. 185-207, 2018. https://link.springer.com/article/10.1007/s11042-016-4253-x.

[13] A. Sharif, M. Mollaeefar, and M. Nazari, ***"A novel method for digital image steganography based on a new three-dimensional chaotic map,***" Multimedia Tools and Applications, vol. 76, no. 6, pp. 7849-7867, 2017. https://link.springer.com/content/pdf/10.1007/s11042-016-3398-y.pdf.

[14] A. K. Sahu, G. Swain, and E. S. Babu, "***Digital image steganography using bit flipping,***" Cybernetics and Information Technologies, vol. 18, no. 1, pp. 69-80, 2018. https://content.sciendo.com/view/journals/c`ait/18/1/article-p69.xml.

[15] E. H. Rachmawanto, and C. A. Sari, "***Secure image steganography algorithm based on dct with otp encryption***," Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1-11, 2017. http://publikasi.dinus.ac.id/index.php/jais/article/view/1330.

[16] Z. Wang, and A. C. Bovik, "***Mean squared error: Love it or leave it? A new look at signal fidelity measures***," IEEE signal processing magazine, vol. 26, no. 1, pp. 98-117, 2009. https://ieeexplore.ieee.org/abstract/document/4775883/.