Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

An Approach to Hide an Audio File in Image Using LSB Technique

Mohammed Majid Msallam[1]

Control and Systems Engineering Department, University of Technology, Baghdad, 10001, Iraq

[1]60190@uotechnology.edu.iq

https://dx.doi.org/10.46649/150920-01

Abstract— **Recently, the world is interested in moving data between various devices. When The data transfer over the internet, maybe it attacks and reads or modifies on containing it. So, Data transmission must be encrypted before sending it to read and interpret by the intended receiver. Thus, information security is more critical than it used to be. This paper reflects the implementation of the two Least Significant Bit (LSB) techniques is named sequential LSB and sorted LSB. It is done by embedding a secret audio file into a cover file of the image using the LSB techniques with an approach to choose the hiding index. The work proposed uses the conventional approach to the LBS techniques under the name sequential LSB as the basic steganography model to compare my algorithm which called sorted LSB. Based on results, the sorted LSB produces is the same sequential LSB in which the stego image is not recognized by human eyes, but the security more complex than the LSB sequential.**

Keywords— **Steganography, Cryptography, LSB, image hiding.**

I. INTRODUCTION

The encryption of secret information had found in the time of the Greeks [1]. The Greeks used it to send important messages at the time of the wars. Hidden information had been messy at begin. Messages were sent on foot before phones, before post, before horses. If you wanted to hide a letter, you had two choices: Memorize it by the messenger, or hide it on the messenger. In modern, data send over the internet so it prevents any sort of unauthorized by encrypting it. The different methods used to information hiding techniques can be categorized as shown in figure 1.

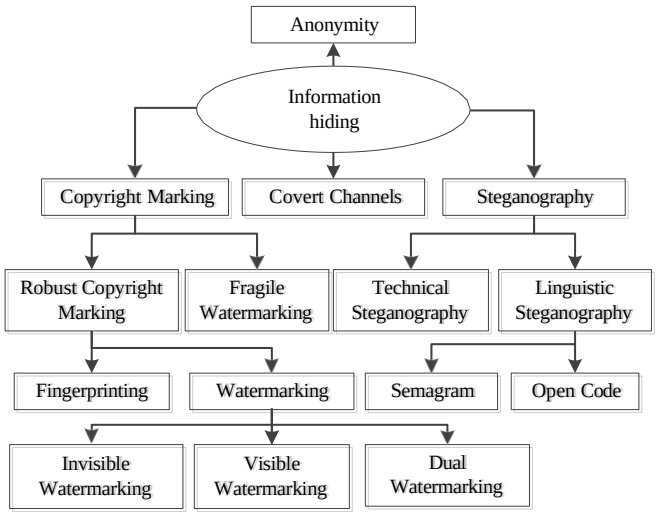

Fig. 1 Information Hiding Techniques [2].

In computer science, Steganography word means "Covered writing" that derived from the Greek language. Steganography is the science and art of communicating in a way that hides secret data inside other data called cover data. The merit of steganography is to hide a secret message inside cover data so that no anyone can even detect a second message at cover data. Steganography is composed of the two words Stegano and Graphy. Different types of covers media are shown in figure 2. Cryptography comes from the Greek language, meaning "Covered writing". Cryptography is a method of transmitting a message in a distinct form so that it can be read and interpreted by the intended recipient [3].

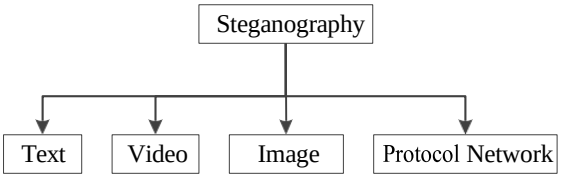

Fig. 2 Different Types of Covers Media.

Figure 3 illustrates the part of the steganographic system. The cover object or data is the name of the object or the data which is used to hide secret information. Stego data is referred to as data that is obtained by embedding secret data inside cover data. Cover data will send to the receiver over the network [4]. Steganography techniques can be categorized as spatial domain techniques and transform domain techniques [5].

ATU-FJIECE, Volume 2 – Issue 2 – Nov. 22, 2023, © 2020 FJIECE, All Rights Reserved

Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

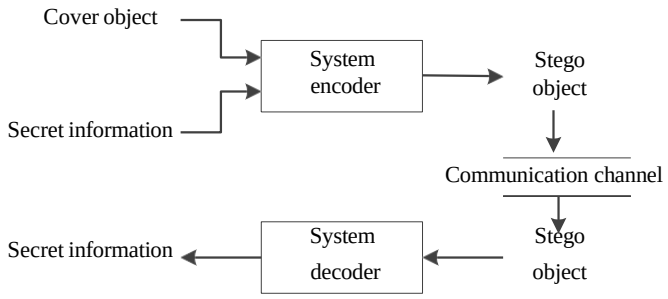

Fig. 3 Basic Steganographic System.

The advantages of LSB are less chance for distortion of the original image so it is not recognized by human eyes. An image can be contacted with more data to embed. The hidden data can be lost with image manipulation is the disadvantages of LSB. The image manipulation is image crop, compression, resize, etc.

This paper organized as section II study Least Significant Bit (LSB) at the literature review, section III presents the proposed steganography method, section IV presents the evaluation of implemented, while section V results, and section VI the conclusion has presented.

II. LITERATURE REVIEW

Least Significant Bit (LSB) Steganography is one technique in which the secret data bits replace the least significant bit of cover data. This method has the advantage that comprehension, quick implementation. The downside of LSB is that it is vulnerable to steganalysis [6].

A large number of hidden information techniques have been proposed in the literature. Sultana [7] used a technique that adds double-layer security to hide secret data in an image using LSB algorithm, AES-128 encryption and a method to choose an index of an image pixel. A method to choose an index of the image pixel is a protocol between the sender and receiver to return original secret data at the receiver. Verma [6] suggested the method does not collect the least important bits of pixels in a sequence but is combined with a midpoint circle method to select which pixels are used as cover pixels. The concept of the chaotic sequence was used as the security approach that selects an image pixel to hide a secret text into a video cover file technique introduced by Singh [8]. A proposed technique was introduced by Tappe [9] that read pixel of cover Image read bit number five and six, calculate the difference, and compare the difference with secret data bit, If the data bit is not equal to the difference then transverse bit number five. Juneja [10] provided a new algorithm to encrypt important messages in the edges and smooth areas of images in nonadjacent and random pixel positions. At first, the hidden message was to encrypt, then use an enhanced edge detection filter to detect edges in the cover-image, finally important massage hidden at the cover image. Audio steganography uses to hide secret data by the LSB technique was proposed by Tayel [11].

In hiding information systems, the enemy knows about the design and implementation details of the steganographic system and all details about LSB. So, all researchers are concerned with the complexity of the way to hide secret data.

In hiding information, the impact factor that improves encryption is the index for hiding so the literature review was the focus on methods for choosing index to hide sensitive data. Previous papers increase the robustness of encryption through were proposal method to hide the important data. But methods for choosing index was based on methods such as a midpoint circle method or equation such as the equation chaotic. This method is constant and with a long time increases the probability of breakthroughs sensitive data. So, my proposal to hide important data depend on the cover data. The cover data will be a dynamic key. In this work, LSB selects image pixels to hide important data from the cover data but this selection is not a sequence but it depends on proposal protocol to reduce the possibility of a secret message being recognized is provided. My proposal uses the aim of steganographic systems that is to obtain a reliable and stable way to conceal the high quantity of secret data. And my proposal combines the advantages of steganography and cryptography. One of the applications that could use this encryption is the Automated Teller Machine (ATM). When a particular user wants to deposit cash to or draw it from the ATM, the authentication data will be compromised to the internet. Therefore, hiding this information is necessary to ensure their security.

III. THE PROPOSED STEGANOGRAPHY METHOD

LSB embed a secret data bit into the least significant bit of cover image pixel. The change will be in the least significant bit and other bits do not change. The first step in this work is to find a hiding index to hide secret information depend on the hiding index. So, the cover image will duplicate into two copies. The first copy of the cover image will use to extract the hiding index. Every image pixel will be 255 for 8 bit and it will shift to right one bit that will be 127 for 7 bits, then sorts for all numbers. The hiding index will get depend on the sort numbers. The second copy of the cover image will use in the next step. The second step in this work is to use the LSB to substitute the least significant bit of all image pixels with important data based on the hiding index. For example, the secret data is 00101010 and image pixels are 4, 134, 42, 78, 200, 33, 76, and 57. The first step to obtaining a hiding index is shown in Table I.

Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

TABLE I
EXAMPLE OF MY PROPOSAL

Original index	Image pixels	Right shift	Sort pixels	Hiding index
1	4	2	2	1
2	134	67	16	6
3	42	21	21	3
4	78	39	28	8
5	200	100	38	7
6	33	16	39	4
7	76	38	67	2
8	57	28	100	5

The original index is to name for index of the cover image while the hiding index is to name for path that chooses to hide important data. Based Table I, the first bit of secret data that has value zero will be hiding at the first image pixel that has value four, then the first image pixel has become value four.

The first bit of important data that has value one will be hiding at the seventh image pixel that has value seventy- six, then the first image pixel has become value seventy- seven and so on such as in shown Table II.

TABLE III
PROCESS OF MY PROPOSAL

Original index	Image pixels	Hiding index	Secret data for the hiding index	Stego image pixels
1	4	1	0	4
2	134	6	1	135
3	42	3	0	42
4	78	8	0	78
5	200	7	0	200
6	33	4	1	33
7	76	2	1	77
8	57	5	0	56

Thus, my proposed technique is based on two algorithms that are embedded in the sender side and extraction in the receiver side.

A) Encoding Algorithm

The method suggested for data encoding procedure before transmitted secret data. The encoding steps for the secret data in the cover image are given in Algorithm 1.

Algorithm 1: embedding secret data in cover image

i. Read secret data bits.
ii. Read a cover image.
iii. Apply **Algorithm 3** to get on hiding index.
iv. Use the hiding index to embed secret data in the second cover image.
v. Send a stego image over a network.

B) Decoding Algorithm

The steps in Algorithm 2 are to extract the secret data from the stego image.

Algorithm 2: extracting secret data from the stego image

i. Receive the stego image from a network.
ii. Read the stego image.
iii. Apply **Algorithm 3** to get on hiding index.
iv. Use the hiding index to extract secret data from the second stego image.

One of the most important parts in the case of the LSB algorithm is finding the exact pixels of the cover image where the data would be hidden. **Algorithm 1** and **Algorithm 2** will find the index of cover image pixel that called hiding index by **Algorithm 3**.

Algorithm 3: Algorithm for finding index of pixel from image.

i. Get image.
ii. Duplicate the image.
iii. Convert the first image from matrix form into an array form.
iv. For every number of the array.
  a. Shift to right one bit.
  c. store in the new array.
v. Sort new the array.
vi. Get the hiding index from the sort.
vii. Return the hiding index.

The color image is a 3-dimensional matrix form that my proposal converts it into an array form. At first, it gets the first red pixel from layer red in the cover image and store in an array. Second, it gets the first green pixel from layer green in the cover image and store in an array. Third, it gets the first blue pixel from layer blue in the cover image and store in an array and so on such as in figure 4.

R1	G1	B1	R2	G2	B2	R3	G3	B3	……

Fig. 4 Three components of each pixel in the array

IV. EVALUATION OF IMPLEMENTED

There are many factors to determine the efficacy of steganography including Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Robustness, Imperceptibility, and Payload Capacity.

1) *Robustness:* This property means that the stego image stays unchanged during processing regardless of the type of transformation used. More robustness is not

 © 2020 FJIECE, All Rights Reserved

Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

possible to recognize the difference between the cover image and Stego image by a human eye.

2) *Payload Capacity:* This property refers to the number of secret data that can be hidden in the cover image. High payload capacity means a large amount bit of the secret data that had hidden in stego image.

3) Mean Square Error (MSE): MSE is determined by combining all the pixel squared differences and dividing them by the total number of pixels. The smaller the value means the better the technique. MSE is defined in equation 1 [12].

$$MSE = \frac{1}{N}\sum_{i}^{N}(I_i - D_i)^2 \qquad (1)$$

Where I_i is a color value of an i^{th} pixel in the cover image. D_i is a color value of the ith pixel in the stego image. N is the total number of pixels.

4) Peak Signal to Noise Ratio (PSNR): This Ratio signifies the difference in quality between the original image and the stego image, and is defined as the ratio between a signal's maximum available power and the noise power that affects the fidelity. The high value of the PSNR means the higher the conversion efficiency. PSNS is defined in equation 2 [13].

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE} \qquad (2)$$

Here MAX is the maximum intensity value color of a pixel so MAXI will be 255 for 8 bits.

V. RESULT

The proposed model was implemented in the MATLAB® 2019b version in order to obtain several criteria for determining steganography effectiveness. In this work, four images used to hide secret data that was an audio file. The size of the audio file is 42.1 kilobytes (KB) with 43,204 bytes or 345,632 bits. The audio file needs to cover image that has 345,632 pixels to hide in the cover image.

The number of color images uses in my work as a cover image is four to examine my algorithm. These images are Lenna, Baboon, Fruits, and Mohammed and all images have the size is 512 x 512 and type PNG which shown in figure 5. Every color image contains 786,432 pixels Which have been calculated by multiplying the width by the height and by three. The payload capacity for these images is a number bit of secret data which is 345,632. When dividing secret bits by pixels of the image, the ratio payload capacity is 0.4395 which means nearly half of the cover image will contain important data. The robustness and payload capacity of the stego image is medium because half of the cover image contains secret data.

The least significant bit for the pixel of the cover image and stego image is called a changeable bit. And the bit of secret data that will hide in a cover image is called an embedded bit.

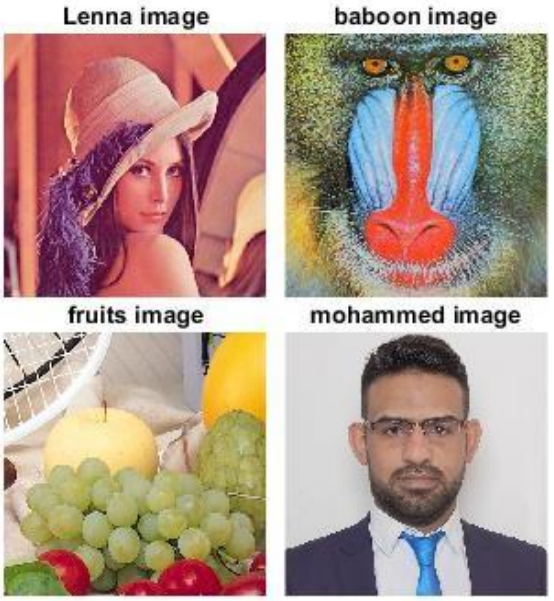

Fig. 5 Cover Image in my proposal.

On the sender side, the secret bit will be replaced with a changeable bit based on the hiding index of the sort depend on my algorithm shown in figure 6. And on another side, the secret bit will extract based on the hiding index of the sort, which means the same step on the sender but it read audio not replaced.

PNSR is the difference in quality a stego and an original image showing in Table III. When LSB used in encoding, nearly half of the stego image had contained sensitive data and the effect of changing then will not be recognized by human eyes which means my algorithm is robustness.

TABLE III
PSNR AND MSE FOR HIDING INFORMATION TECHNIQUE

Image	MSE		PSNR	
	sorted LSB	**sequential LSB**	**sorted LSB**	**sequential LSB**
Lena	0.2206	0.2197	54.6954	54.712
Baboon	0.2198	0.2201	54.7101	54.703
Fruits	0.2193	0.2214	54.71	54.67
Mohammed	0.2204	0.2168	54.6987	54.770

ATU-FJIECE, Volume 2 – Issue 2 – Nov. 22, 2023, © 2020 FJIECE, All Rights Reserved

Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

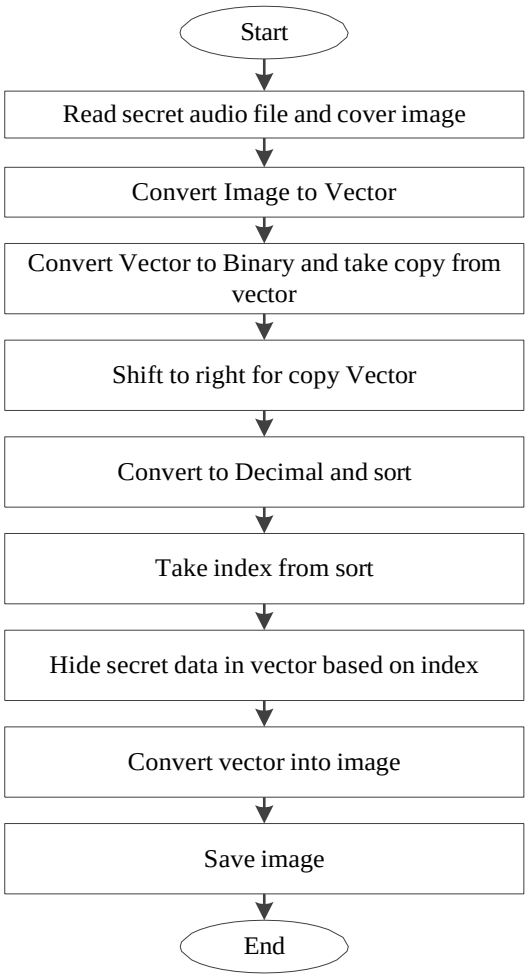

Fig. 6 Flow Chart of The Proposed Model.

The histogram in figure 7 figure 9, figure 11 and figure 13 illustrate the secret data had hidden in light colors. While figure 8, figure 10, figure 12 and figure 14 illustrate that the data is stored in random locations based on original data for my proposal, in contrast to the LSB technique in which the data is stored in a sequence.

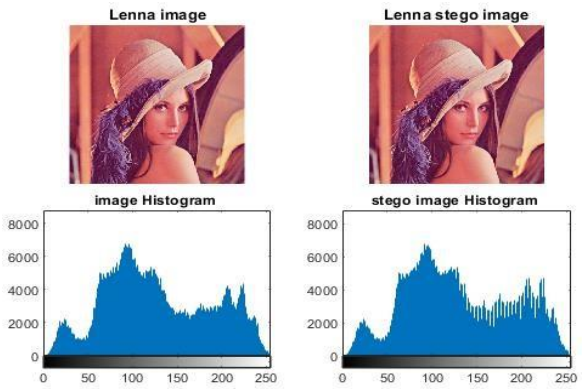

Fig. 7 Lenna Image.

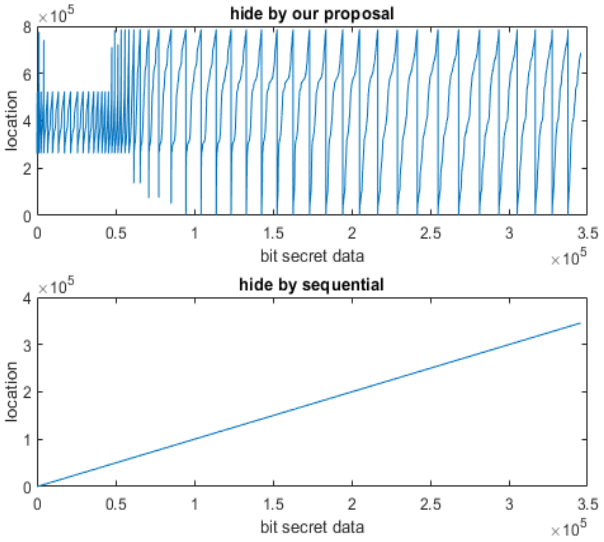

Fig. 8 Hidden Secret Data in Stego Image for Lenna Image.

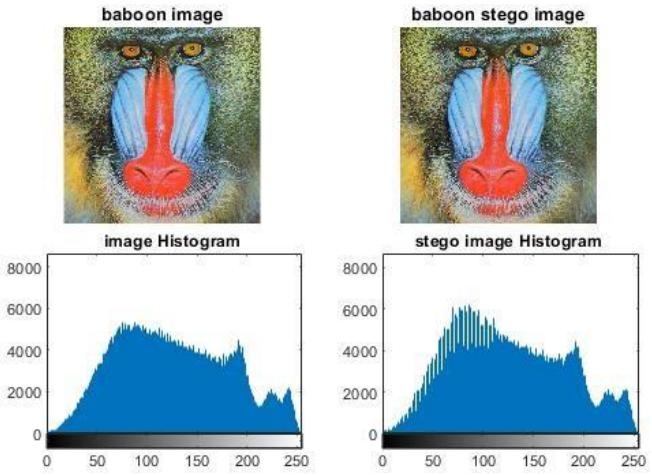

Fig. 9 Baboon Image.

ATU-FJIECE, Volume 2 – Issue 2 – Nov. 22, 2023, © 2020 FJIECE, All Rights Reserved

Al-Furat Journal of Innovation in Electronics and Computer Engineering (FJIECE) is an international, open access, interdisciplinary, quarterly, and double blind peer-reviewed journal published by Al-Furat Al-Awsat Technical University/Iraq. It is dedicated to the latest advancement in Electronic Engineering, Computer engineering, and their related and subfields.

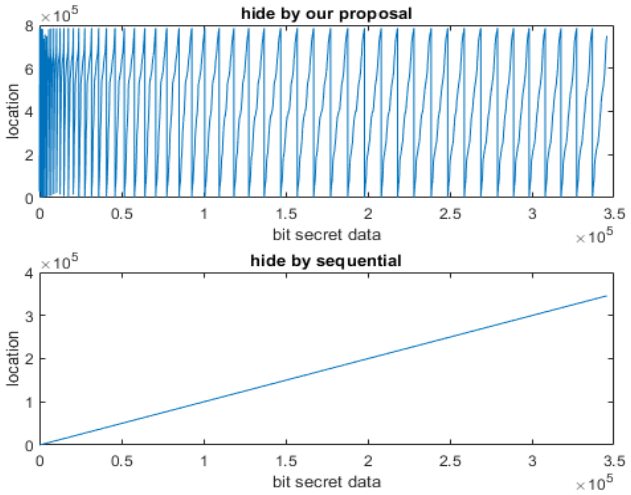

Fig. 10 Hidden Secret Data in Stego Image for Baboon Image.

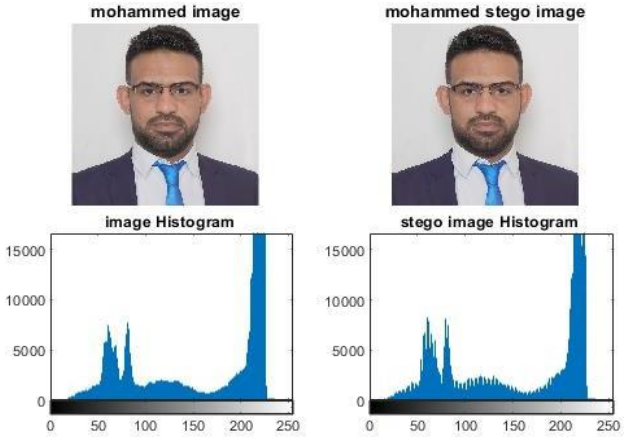

Fig. 13 Mohammed Image.

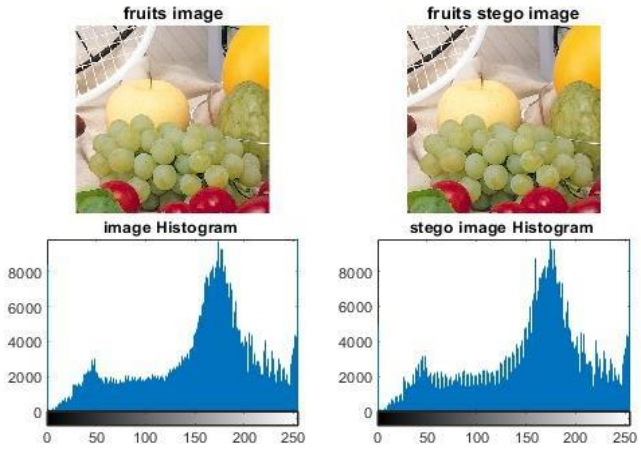

Fig. 11 Fruits Image.

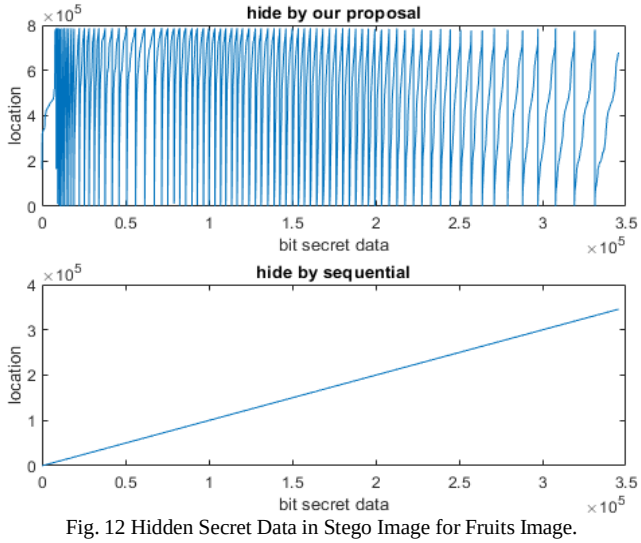

Fig. 12 Hidden Secret Data in Stego Image for Fruits Image.

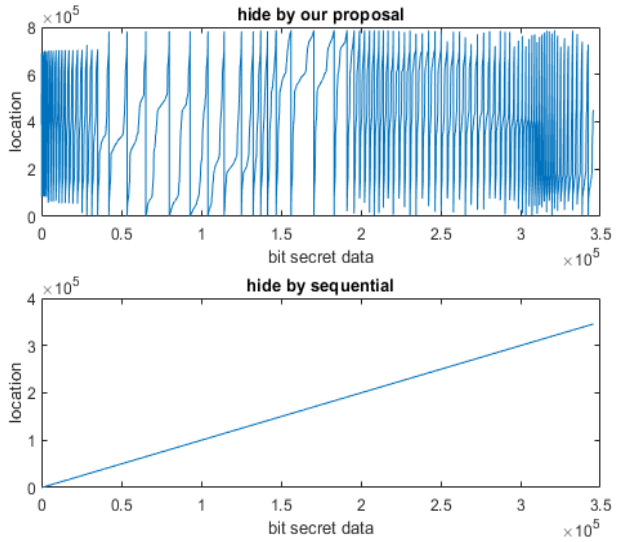

Fig. 14 Hidden Secret Data in Stego Image for Mohammed Image.

VI. CONCLUSION

This paper proposed a technique to combine the advantages of steganography and cryptography. At steganography, sorted LSB uses LSB techniques to hide the secret audio file in the cover image. and at cryptography, It uses a method for obtaining a non- sequential location to hide the secret audio file. the method depends on the cover image to get a hiding index that secret audio data will be embedded in the cover image

based on it that main difference between sorted LSB and sequential LSB.

The value of image pixel will change between ±1 on the color grade in both sequential LSB and sorted LSB. almost the value of the PSNR is fifty for each of them so no effect on the PSNR. Luckily, maybe the embedded bit may have been the same changeable bit so that there is no effect on the color grade. although nearly half of the stego image had contained sensitive data, sorted LSB is not affected on stego image by comparing it with sequential LSB because sorted LSB is no effect on the color grade.

ACKNOWLEDGMENT

I cannot express enough thanks to my mother for her continued support and encouragement. My completion of this project could not have been accomplished without the support of her.

REFERENCES

[1] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, and A. Gutub, "Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination," Journal of Information Security and Cybercrimes Research (JISCR), vol. 2, no. 1, 2019.

[2] S. M. Thampi, "Information Hiding Techniques : A Tutorial Review," ISTE-STTP on Network Security & Cryptography 2004.

[3] M. Hussain and M. Hussain, "A survey of image steganography," International Journal of Advanced Science and Technology, vol. 54, 2013.

[4] M. G.R and A. Danti, "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, 2015.

[5] S. Sharma1 and U. Kumar, "Review of Transform Domain Techniques for Image Steganography," International Journal of Science and Research (IJSR), vol. 4, no. 5, 2015.

[6] V. Verma, Poonam, and R. Chawla, "An enhanced Least Significant Bit steganography method using midpoint circle approach," International Conference on Communication and Signal Processing, 2014.

[7] Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta, and M. N. Islam, "A new approach to hide data in color image using LSB steganography technique," 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 2017.

[8] N. Singh and J. Bhardwaj, "Comparative Analysis for Steganographic LSB Variants," Computing, Communication and Signal Processing. Springer, Singapore, 2019.

[9] C. G. Tappe and A. V Deorankar, "An Improved Image Steganography Technique based on LSB," International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 4, 2017.

[10] M. Juneja and P. S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images," International Journal of Computer and Communication Engineering, vol. 2, no. 4, 2013.

[11] M. Tayel, A. Gamal, and H. Shawky, "A proposed implementation method of an audio steganography technique," 2016 18th International Conference on Advanced Communication Technology (ICACT), 2016.

[12] Mohit, "An Enhanced Least Significant Bit Steganography Technique," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 5, no. 6, 2016.

[13] Sheshadri, H. S., and W. I. A. Almazaydeh., "Image Steganography Using a Dynamic Symmetric Key," Proceedings of the 2nd International Conference on Inventive Computation Technologies (ICICT 2017), 2017.