[1]Nora H. Sultan

Hiding Data using LSB in Combination with AES

Journal of Electrical Systems

Abstract: - In our increasingly digital age, steganography has emerged as one of the most trustworthy methods for the transmission of confidential information. This new research improves upon earlier LSB approaches by demonstrating how they may be utilized to efficiently encode secret data into a covert object without causing any obvious distortion. This opens the door for future applications of these methods. A safe data-hiding model will be produced by combining LSB-based steganography with AES; an LSB-based AES-256 encryption has been created and implemented in MATLAB.

First, encrypted picture data is produced by encrypting the original image using a 256-bit AES technique. This process takes place before the image is used. The subsequent step includes sending a LSB-based steganography picture to the objective, which additionally contains the scrambled information. Interpreting the steganography picture information and reestablishing the first picture have both been achieved through the work of a similar strategy at the less than desirable finish of the transmission. We have examined and assessed an expansive range of sources of info and results from a few emphasess of the procedure applied to an assortment of picture information types. It is feasible to involve it in numerous useful cryptography applications to go through with steganography picture exchanges in a safer way.

Keywords: Cryptography, Steganography, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Advanced Encryption Standard (AES), Least Significant Bit (LSB).

1. Introduction

The most common way of covering interchanges by the encoding of messages inside different information is alluded to as steganography [1]. Steganography utilizes a few unique kinds of covering material so data can be hidden. Video steganography, picture steganography, sound steganography, and text steganography are a few models [2,3]. Cryptography incorporates changing the data to a disjointed or confused text to guarantee that main the planned beneficiary, who knows the way to unscramble the code text, can understand it. This is achieved by encoding the message. Then again, steganography is utilized to conceal information on display with the end goal that it can't be found by anybody who is looking [5]. In this collection of work, we depict a way for making two-layered security that depends on the mix of cryptography and steganography as the fundamental security systems. Cover pictures are utilized to conceal data, though stego pictures are utilized to conceal pictures that have been scrambled. The need to safeguard data from other people who shouldn't approach it is normally the main thrust behind the secretive scattering of data.

2. Least Significant Bit

The method known as Least Significant Bit (LSB) addition is among the most widely recognized approaches used in the investigation of spatial spaces. The most common way of covering data inside a host picture should be possible in a simple and well-known way. Utilizing the LSB approach, you can cover data in the main bits of one picture by involving the least significant bits of every pixel in another picture [6]. In the event that you change the least significant bit (LSB) of a pixel, you will see minor variances in the brilliance of the pixel; by and by, the modifications will be excessively unobtrusive for the natural eye to identify [7]. During the stage assigned for getting, the data is recovered. It is important to initially decode the code message to peruse the message that has been covered up [8].

3. Advanced Encryption Standard (AES)

Software and hardware that supports the Advanced Encryption Standard (AES) is used all over the world to encrypt sensitive data. The Data Encryption Standard (DES) started showing indicators of being susceptible to

[1] Department of Computer Sciences, College of Education for Girls, Kufa University, Iraq

norah.mayali@uokufa.edu.iq

brute-force assaults in 1997. This prompted the National Institute of Standards and Technology (NIST) to bring attention to the necessity of finding an alternative [9]. According to the National Institute of Standards and Technology (NIST), the new, more complex encryption algorithm will be made available to the public and must be "capable of protecting important government information well into the [21st] century." Its design objectives included the simplification of implementation in both hardware and software, as well as in limited environments like as a smart card, while yet providing sufficient security against a variety of attack methods [10]. [Note: The Advanced Encryption Standard (AES) was initially commissioned for development by the United States government, and it is now widely utilized in both commercial and government settings [11,12]. In order to encrypt and decode data, the Advanced Encryption Standard (AES) uses keys that have either 128 bits, 192 bits, or 256 bits, as shown in Figure (1) [13]. The approach requires that the data in an array go through a certain amount of transformations before it can be encrypted using AES. First, the data are arranged in an array, and then, over the course of numerous encryption rounds, the cipher alterations are performed repeatedly each time. The first transformation that occurs while using AES as an encryption cipher is a data substitution based on a substitution table. This occurs during the beginning of the process. The second change is the relocation of information rows. The third column contains a combination of columns from all three categories. When performing the final transformation on each column, a specific portion of the encryption key is required in order to do so. It will take you more iterations to do the job if you use keys that are longer.

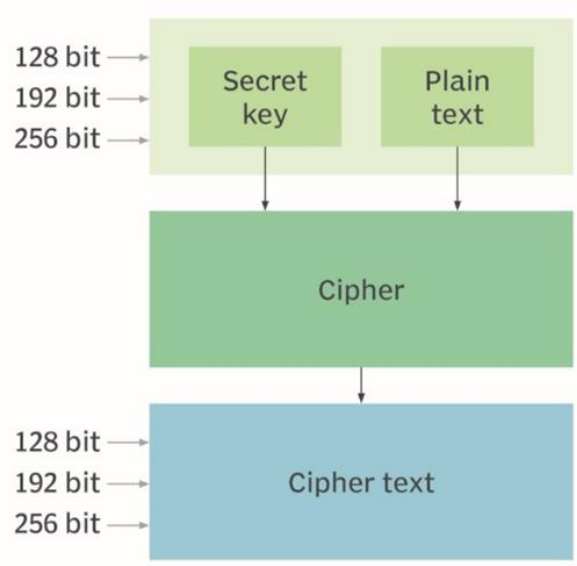


Figure 1.AES Design

4. Proposed Method

We present a method for secure data transmission that combines steganography and cryptography. In this case, we employed AES encryption and LSB image concealment. Before using the LSB approach to conceal sensitive information in a picture, the data must first be encrypted.

In Figure 2, we show how we propose combining the two methods:

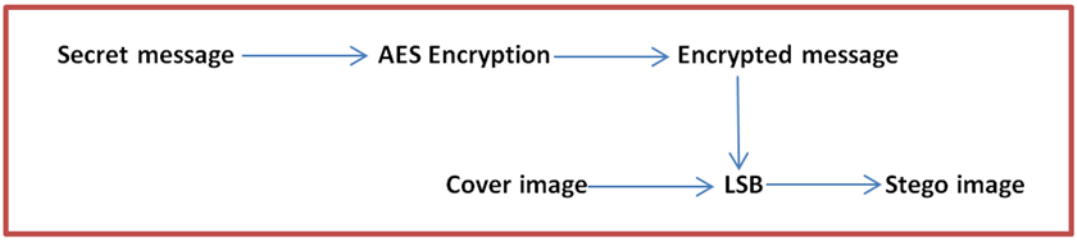


Figure 2. Encrypting System

After the secret message has been encrypted using AES and converted into a byte array, the next step is to enter the cover image and perform the least significant bit (LSB) transformation to obtain the stego image. The proposed system's decryption algorithm is described below (Figure 3):

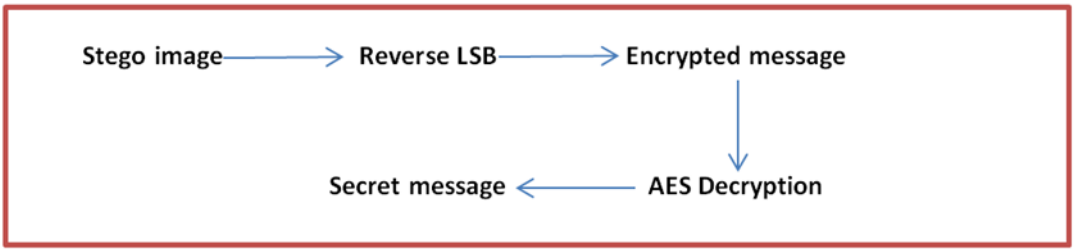


Figure 3. Decryption System

5. Result and Discussion

The experiment used a variety of images. With the LSB method, we can encrypt an image and combine it with a cover image to send a hidden message. Figures 4,5,6, and 7 depict a cover picture, a secret message encrypted image, and a steganographic image in a situation where the cover image's resolution must be higher than that of the secret image's resolution.

Figure 4. Cover image

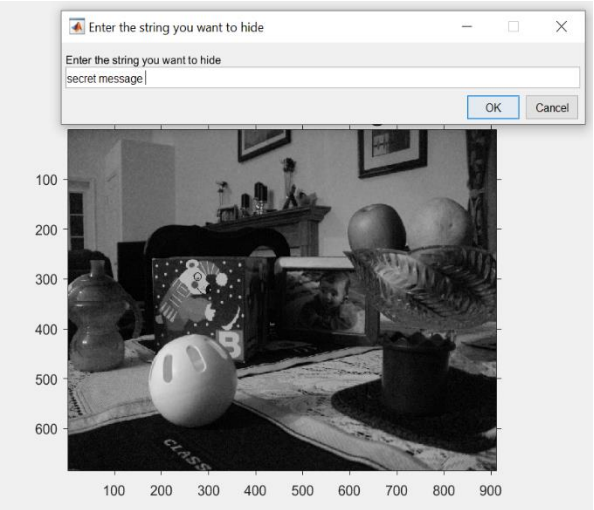


Figure 5. Encrypted image

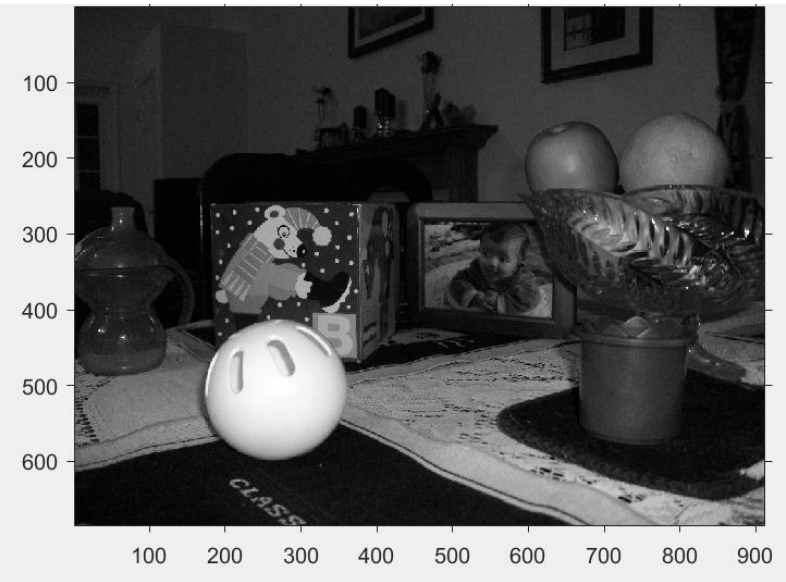
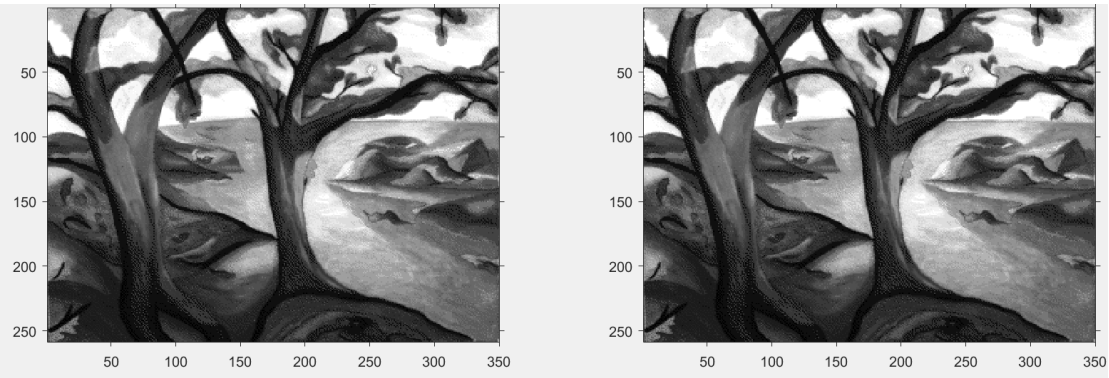


Figure 6. Encrypted image with secret message

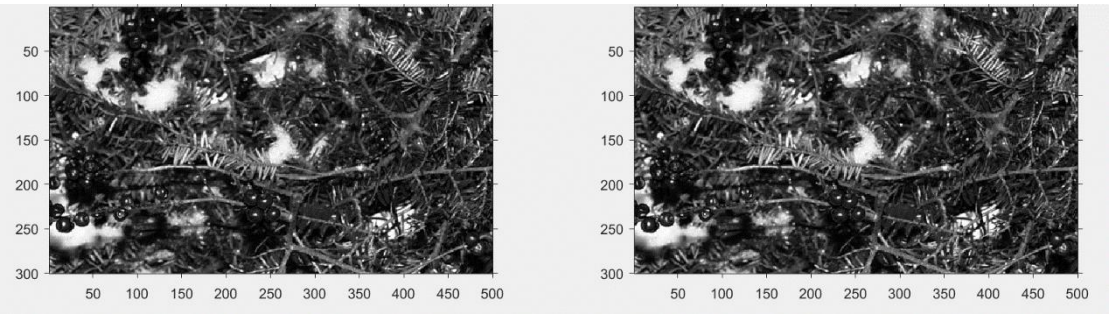
Figure 7. Stego image

Figure 8 show some image were used in proposed algorithm and the results show in table 1 and 2.



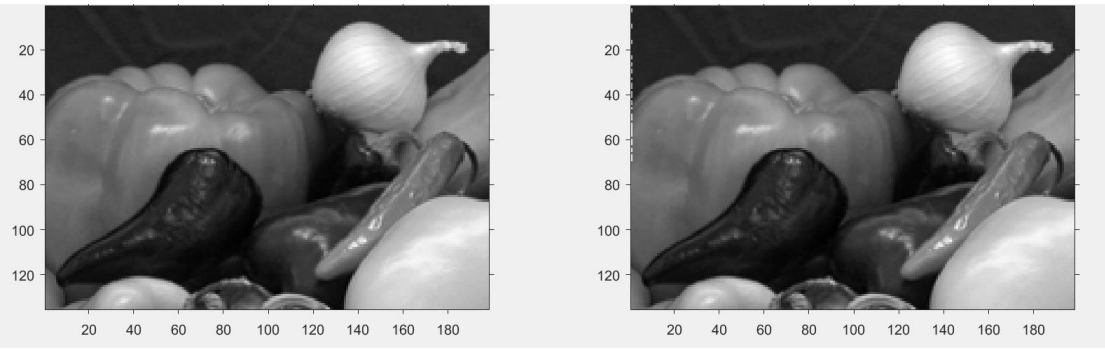
a. Cover image **b. stego image**

Image 1



a. Cover image **b. stego image**

Image 2



a. Cover image **b. stego image**

Image 3

Figure 8. cover images with stego images

Table 1: Entropy for cover images and stego-images

Images	Entropy of cover image	Entropy of stego image
cameraman	7.5237	7.5295
Image(1) in Fig.8	7.6322	7.6409
Image(2) in Fig.8	6.4498	6.5711
Image(3) in Fig.8	6.8446	6.9012

The images in Table 1 reveal that the stego-image possesses an entropy that is slightly greater than that of the cover image. This is the result of more secret data being added to the cover image without significantly affecting the pixel values in any significant way.

The results of the experiments make it abundantly evident that the strategy that has been described is effective in achieving the appropriate level of concealment while incurring only a little amount of distortion in the process. Table 2 contains estimations of the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) that occur when the suggested method is applied to image data.

Table 2: PSNR and MSE of Proposed Method for stego images

Images	**PSNR**	**MSE**
cameraman	**42.8412**	**0.0865**
Image(1) in Fig.8	**56.7531**	**0.0341**

Image(2) in Fig.8	**55.5431**	**0.0447**
Image(3) in Fig.8	**40.8911**	**0.0972**

6. Conclusion

When it comes to transmitting sensitive data, only a combination of steganography and encryption can guarantee the necessary privacy and security. Our method relies on the premise that it is possible to conceal information within a picture file. Experiments show that the cover media undergoes only slight modifications due to the secret data being contained within it, with no noticeable impact on its quality.

References

1. Lalitha Chinmayee and Tegashwini Gadag,"An Innovative Method of Text Steganograph", International Journal of Engineering Research and Technology (IJERT),ISSN:2278-0181, Vol.8,Issue06 , June 2019.
2. Ghazali Sulong and Rozniza Ali," The use of Least Significant Bit (LSB) and Knight Tour Algorithm for image steganography of cover image", International Journal of Electrical and Computer Engineering , 9(6):5218, 2019.
3. Rosziati Ibrahim and Teoh Suk Kuan," Steganography Algorithm to Hide Secret Message inside an Image",Computer Technology and Application, 102-108, 2011.
4. Ala Hamarsheh,"Exploiting Omega Networks to Hide Text in Text Message" IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.5, May 2015.
5. Ahmed Kadem Hamed," A method to hide text in image", Journal of Missan Researches, Vol (12), No (24), 2016.
6. T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005
7. Rusul Mohammed Neamah, Jinan Ali Abed and Elaf Ali Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm", (IJECE) Vol. 10, No. 1, pp. 809~815, February 2020.
8. Swati Bhargava and Manish Mukhija," HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE STEGANOGRAPHY", DOI: 10.21917/ijivp.2019.
9. Ali J. Mohammed , Ali A. Dawood and Fatin E. Muhy,"Text Hiding Technique in Digital image", Al- Mustansiriya J. S ci Vol. 18, No 4, 2007
10. Astuti, Y.P., E.H. Rachmawanto, and C.A. Sari. "Simple and secure image steganography using LSB and triple XOR operation on MSB". International Conference on Information and Communications Technology (ICOIACT). IEEE 2018.
11. J. Nechvatal, et al.,"report on the development of the advanced encryption standard (AES)",National institute of standard and technology, October 2,2000
12. Lawrie Brown's s slides supplied with William Stalling's book "Cryptography and Network Security: Principles and Practice," 5th Ed, 2011.
13. S. A. Laskar and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems (IJDMS), vol. 4, no. 6, pp. 57-68, 2012