Al-Qadisiyah Journal of Pure Science

Volume 25 | Number 1 Article 16

1-7-2020

HIDING VOICE MESSAGE USING BOTH CRYPTOGRAPHY AND STEGANOGRAPHY

Huda Dheyauldeen Najeeb
University of Al Iraqia, Public Relations, huda_iraq81@yahoo.com

Recommended Citation
Najeeb, Huda Dheyauldeen (2020) "HIDING VOICE MESSAGE USING BOTH CRYPTOGRAPHY AND STEGANOGRAPHY," *Al-Qadisiyah Journal of Pure Science*: Vol. 25: No. 1, Article 16.
DOI: 10.29350/2411-3514.1221
Available at: https://qjps.researchcommons.org/home/vol25/iss1/16

Available online at http://qu.edu.iq/journalsc/index.php/JOPS

Al-Qadisiyah Journal Of Pure Science (QJPS)

Vol. 25, No. 1, pp Comp. 10 –17, Year2020

ISSN 2411-3514 ONLINE

ISSN 1997-2490PRINTED

Received : 23/1/2020 Accepted :19/2/2020

HIDING VOICE MESSAGE USING BOTH CRYPTOGRAPHY AND STEGANOGRAPHY

Huda Dheyauldeen Najeeb

…Email huda_iraq81@yahoo.com ,Iraq ,University of Al Iraqia, Public Relations

ABSTRACT:

The goal of voice encryption is to keep the private conversation and not allow anyone to access or view it except the authorized person. Steganography and cryptography together are used to strengthen the hiding and obscuring of information. Usually, one of the media is hidden inside the steganography technique and the audio message is hidden inside audio or video, but in this paper, we present a new algorithm for hiding two types of media (audio and text) inside the image. This algorithm contains three steps: record the speech as the input through a microphone, encrypt the voice message by using the Advanced Encryption Standard (AES) algorithm and hiding a secret voice with it key in the cover image without impacting the content and quality of the image by using the Least Signification Bit steganography (LSB). The proposed algorithm solves the problem of distributing and exchanging keys and can use as a real-time software application. Instead of sending the key in another message, it is included with the same message and is saved as a file text. Results (the stego-image) are evaluated through the mean square error (MSE) and the signal-to-noise ratio (PSNR). The stego-image cannot be distinguished by the naked eye from the original cover image when the voice message and key embedded at bit value 1 and 2 respectively, thus we reach the goal to cover the presence of a hidden sound inside the image with high accuracy and robust system against different kinds of attacks such as Median filtering, scaling, and blurring.

KEYWORDS: Voice encryption, Advanced Encryption Standard(AES), Image steganography ,Least Significant Bit embedding(LSB), Mean Square Error(MSE), Peak Signal to Noise Ratio(PNSR).

1. Introduction

During the past years, information security has become an interesting of many researchers who are trying their efforts to come up with solutions, techniques and new ideas to ensure a safe transfer of information through the network, especially the internet without any breakthrough revealed in that information. As a result, there are many techniques and methods that are currently used in information security [14].

The most common information security ways are steganography and cryptography. There is a big difference between them. In steganography , the message is being hidden in another median so that nobody will be aware of the existence of such information and the end result of this technique is called stego-media, while in the cryptography, anyone is aware that there is a hidden encrypted information but incomprehensible and the end result of this technique is called ciphertext. Therefore, the most appropriate way to build a strong protection system is to rely on two technologies to make the process of penetrating the system more complicated [1,20]. In this paper, We used both steganography and cryptography methods to take advantage of both methods for encrypting a voice message in an insecure channel through implemented Advanced Encryption Standard (AES) and the Least Signification Bit (LSB) algorithms.

2. Related Works

Over the past years, information security has become the focus of many researchers who are trying to find new solutions, technologies and ideas that ensure the safe transfer of information through the network, especially the Internet, without interference. As a result, there are many techniques and methods currently used in information security. In this article we will highlight some ways to protect information. Mahalakshmi., [13]proposed a new algorithm of steganographic for preventing unauthorized persons to become aware of the presence of a message. The system embedded secret data on audio steganography by generated the ciphertext through AES algorithm which will be embedded in the audio file through LSB algorithm. In the end, the researcher concluded that AES encrypted data is unbreakable and more secure than DES. Geetha, [8] presented a method for embedded the audio file with format mp3 in color image using Most Significant Bit (MSB). This method provided greater flexibility to the user for embedding the secret data in the first two bits of each byte of color image. Rasedur, [17] & Noor, [15] made a hybrid between steganography and cryptography in their proposed algorithm. Rasedur, and others have hidden text in audio steganography. Their algorithm contain two steps: encrypt secure message by using AES and embed the cipher message in wav audio file, while Noor and others have hidden text in image steganography and their algorithm contain five steps: generate key through Blowfish, create ciphertext through split plaintext in blocks each one is 64 bit which is the same size as the key then making XOR between them, apply edge detector on cover image through Sobel filter, and using bat algorithm to choose the random position which is used for embedding ciphertext in image steganography through LSB. Both methods achieved a strong system for hiding the text message with PSNR more than 60. Bhabesh, [5] presented a new system for hiding an audio file in image steganography and making the watermark by using Deep Learning Approach. The result achieved high accuracy and robust system against different kinds of attacks such as noise, cropping, rotation, and blurring. Aishwarya, [2] built a new system by using hardware and software to convert the input speech through a microphone to writing text. Then, through AES the text is encrypted to ciphertext which is sent over a channel to the receiver. The system is very safe and can use as a real-time software application.

3. Voice encryption

Voice is an electronic means of recording, transfer, and broadcasting of the audio file without visual images. Voice encryption is a process of converting sound signals in a secure form using an encryption algorithm. In cryptography, a secure voice is a term used to encrypt the audio file in the insecure communication medium such as the internet [10].

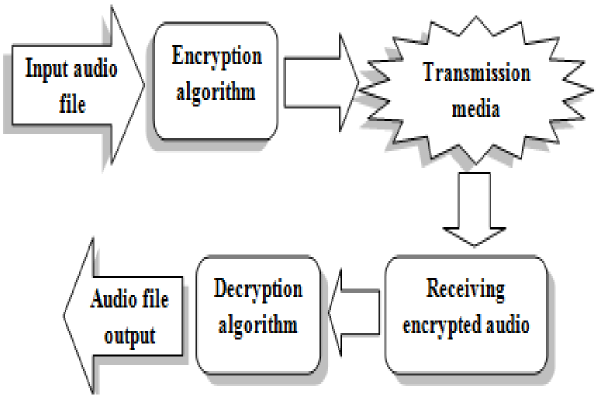


Figure 1. Operations in Voice Encryption[10].

4. Advanced Encryption Standard

AES is an international standard algorithm used for protecting electronic data. It is based on symmetric block cipher Rijndael that means the same key is used for both decryption and encryption. AES has a fixed block size of 128 bits (16 bytes) with a key size of 128,192, or 256 bits. Encrypted data that is returned by cipher block has an equal number of bits of data that were entered. A loop structure is used by iterative ciphers to carry out substitutions and permutations of input data, repeatedly[4,8].

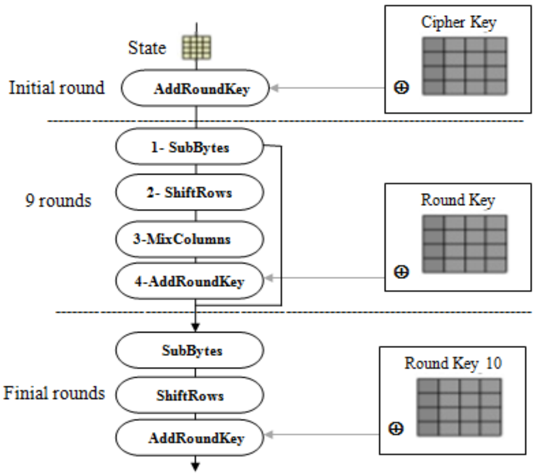


Figure 2. AES with 128 bit key

AES algorithm performs four steps these are 1) Sub Bytes. 2) Shift Rows. 3)Mix Columns. 4)AddRoundKey. AES algorithm has several amount of round depends on the size of the key [6,7]. Each round (except the final round includes only three steps) includes four steps:

1) Sub Bytes: In the state matrix[x,y], each byte state is replaced by the value of S-Box.
2) ShiftRows: we cyclically left shift every row *x* of the state matrix by *x*, $0 \leq x \leq 3$..
3) MixColumns: Each array column (four bytes) is combined with invertible linear transformation by arithmetic over GF(2^8)
4) AddRoundKey: Using simple bitwise XOR for adding roundkey with each byte of the state.

AES structure is very simple. In decryption and encryption, the algorithm starts with an AddRoundKey state, followed by 9 rounds which each includes (Sub Bytes, Shift Rows, Mix Columns, AddRoundKey) state while the tenth round includes only 3 states (Sub Bytes, Shift Rows, AddRoundKey)[12,16].

5. Image steganography

Embedding using images is the most common type because of the image characteristics which make it the ideal medium for inclusion,through existence evidence redundant bits which can be exploited and replacing the secret message.

5.1. LSB (Least Significant Bit embedding)

The most known steganography techniques and characterized by an easy implementation is LSB which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes that contains the hidden data. The image can be indicated by a set of colored pixels. The color image block is represented by 3 bytes (Red, Green, and Blue). When the first binary cell is changed, each point is changed in 3 bytes because each point is represented by 3 bytes. Therefore this change will not be noticed by the human eye [11].

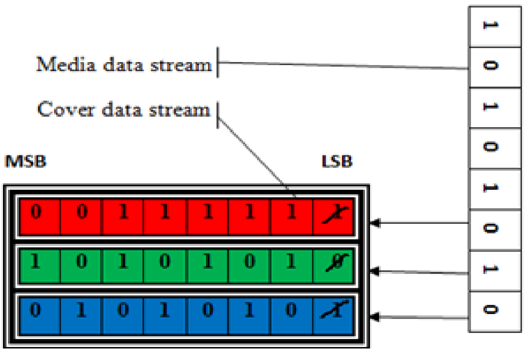


Figure 3. Least Significant bit in color image

5.2. Image quality measurements

There are several methods which are used for measuring the quality. Some of these are:

1) Mean Square Error and Peak Signal to Noise Ratio

PSNR is the most widely used objective image quality metric. It defines simply through MSE. [19] .MSE must be as small as possible between the reconstructed image and the original image with maintaining the quality of the reconstructed image which would be near to the original image. Given Image X which is n×m monochrome with noisy approximation Y, is defined as follows:

$$MSE = \frac{1}{nm}\sum_{i=o}^{n-1}\sum_{j=0}^{m-1}[X(i,j) - Y(i,j)]^2 \qquad (1)$$

$$PSNR = 10\, log_{10}\left(\frac{Max^2}{MES}\right) \qquad (2)$$

Where MAX is the maximum possible pixel value of the image. Get it from this equation 2^B-1 , where B is the value of bits.[3]

2) Relative Entropy (RE) between Stego and Cover Images

RE is one parameter uses for evaluating the performance of a security system. It must be smaller as possible in any steganography system. RE is calculated from the following equation: [6]

$$RE = \sum P_{CI} log\frac{P_{CI}}{P_{SI}} \qquad (3)$$

6. Quality Evaluation of Hiding Capacity and the Security of the Image Steganography System

There are many criteria for evaluating the performance of a security system that is based on the Image Steganography. The criteria we relied upon to evaluate the proposed work are: [18]

1) Embedding Efficiency: hiding information in a cover image changes the cover image entropy or the mean quantity of information. So it is predicted that the stego-image will have a different entropy value compared to the cover image. Therefore, one of the main goals of any steganography system is to minimize the difference in entropy between the stego and the cover object. By Equation (3), the entropy difference can be measured for images using the Relative Entropy (RE) between the stego and the cover images.

2) Imperceptibility or Fidelity: indicates the visual quality of the stego-image after the embedding process from the point of view of the hiding information. However, the higher fidelity includes better visual quality for the stego-image which is one of the basic requirements for any 'Image-Steganography system'. There are many of standard metrics used for determining the fidelity of for the stego-image. One common metric is MSE and PSNR which is measures the degree of distortion the stego-image creates compared with the original cover image. Ratnakirti, [18]built a table of rating scale for quality evaluation of image-steganography which is shown in Table(1).

Table 1. Scale for Visual Fidelity and Embedding Efficiency

Scale Value	**Criteria1**	**Criteria2**
High	PSNR≥60	0<RE≤0.1
Medium	40≤PSNR<60	0.1<RE≤0.5
Low	PSNR<40	RE>0.5

3) Resistance against various attacks: when designing a steganography algorithm, its performance must be tested by subjecting it to various kinds of attacks is required. The hidden information should be retrievable even if the stego-image is undergoing some attacks.Cropping,scaling, JPEG compression, median filtering, Gaussian noise etc. are common attacks that the stego-image may experience. [9]

4) Capacity: it means the amount of data that a steganography algorithm can effectively mask without causing visual impairment to the image within a chosen cover medium. The rate of embedding is expressed mostly in absolute measurement (like the size of the secret message). In our work, The size of the voice message must be not exceeding the allowed limit according to the following formula:

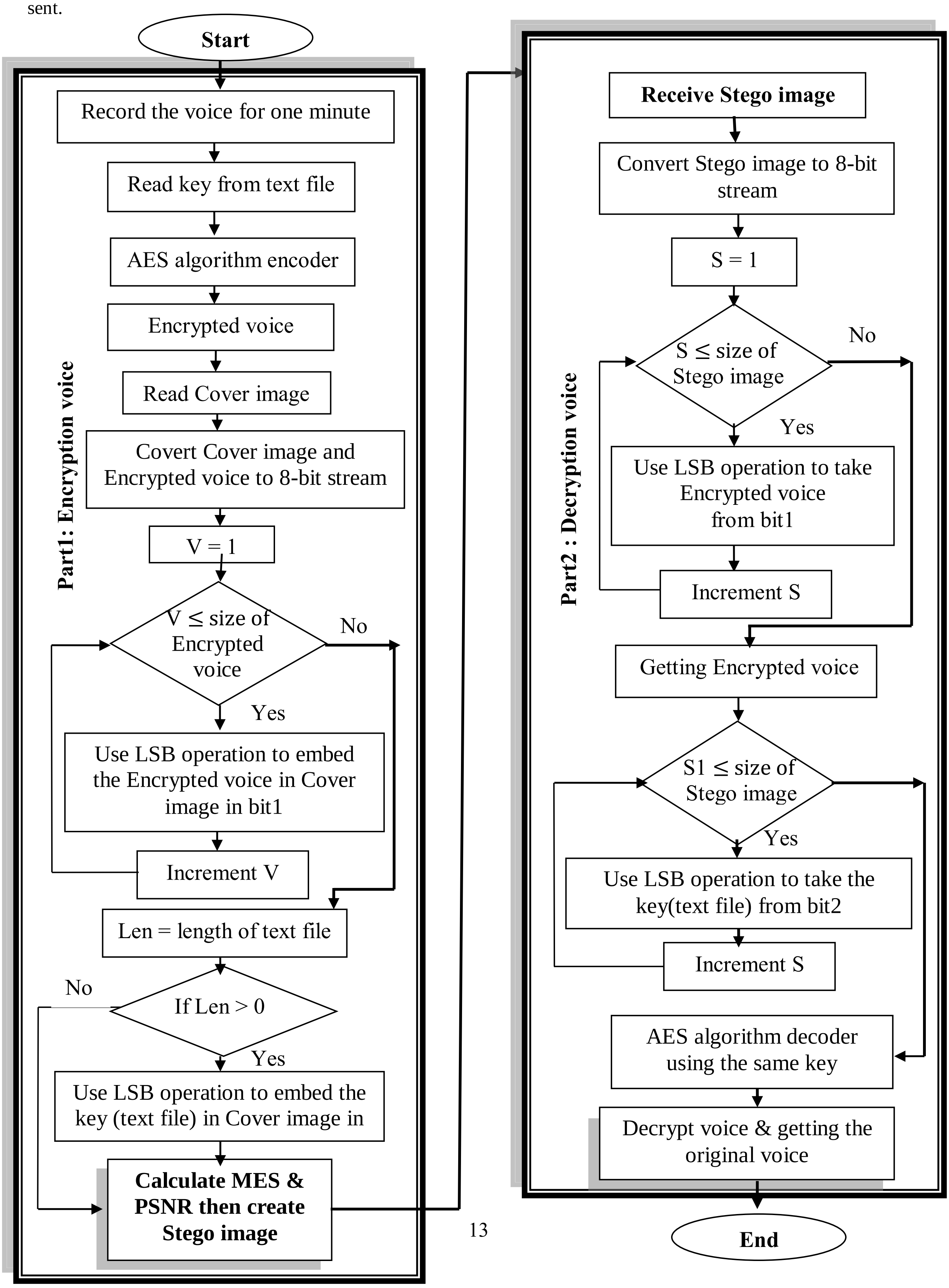
$$16 \times V\ 9\ \times W\ \times H \qquad (4)$$

Where V is the size of the voice message, W and H represent the width and height of the cover image. So the maximum size of voice message is: [8]

$$V\ = (9\ \times W\ \times H)/16 \qquad (5)$$

7. Proposed System Design

The proposed work is to build a strong system for encryption and decryption voice message. This system is combining both cryptography and steganography. First, we have recorded voice message for one minute which has been encrypted by AES algorithm with choosing one of the keys (select a random key) which are saved in a text file to get Encrypted voice then we have embedded the encrypted voice and its key inside a color image and generated Stego image which will be sent.


Start
Part1: Encryption voice
Record the voice for one minute
Read key from text file
AES algorithm encoder
Encrypted voice
Read Cover image
Covert Cover image and Encrypted voice to 8-bit stream
V = 1
V ≤ size of Encrypted voice
No
Yes
Use LSB operation to embed the Encrypted voice in Cover image in bit1
Increment V
Len = length of text file
No
If Len > 0
Yes
Use LSB operation to embed the key (text file) in Cover image in
Calculate MES & PSNR then create Stego image
Part2 : Decryption voice
Receive Stego image
Convert Stego image to 8-bit stream
S = 1
S ≤ size of Stego image
No
Yes
Use LSB operation to take Encrypted voice from bit1
Increment S
Getting Encrypted voice
S1 ≤ size of Stego image
Yes
Use LSB operation to take the key(text file) from bit2
Increment S
AES algorithm decoder using the same key
Decrypt voice & getting the original voice
End

Flowchart 1: Proposed system design

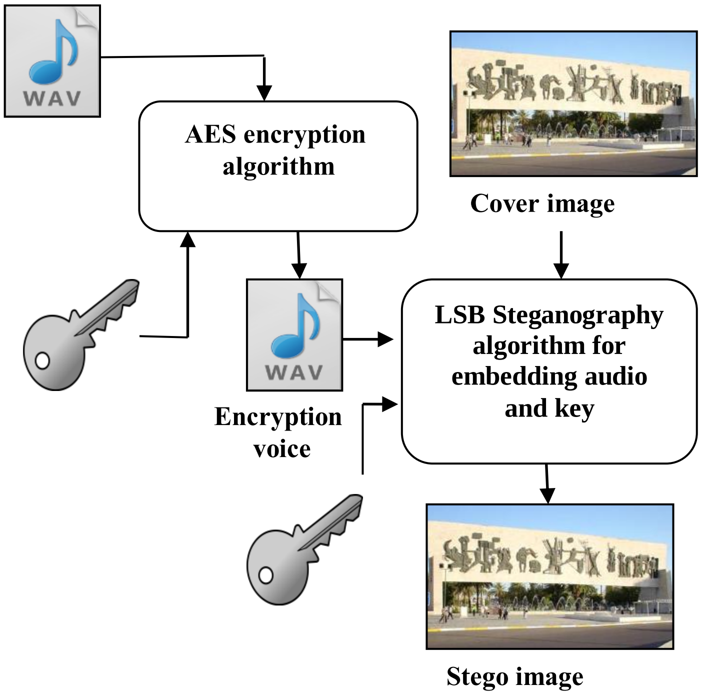


Figure 4. Encryption the vioce

(1) Algorithm

.**Input :** Voice, Key and Cover image
.**Output :** Stego1 image

.Step1 : Convert the voice file to 8-bit stream
Step2: Perform an AES encryption algorithm .using the input key
.Step 3 : Create an encryption voice
.Step 4: Covert Cover image to 8-bit stream
Step 5 : perform LSB operation on Cover image for each 8-bit stream until all the bits of encryption voice and key .were embedded
Step 6: Convert the result to the decimal value that will generate a stego1 .image
Step 7: Calculate MSE and PSNR between .Cover and Stego1 image

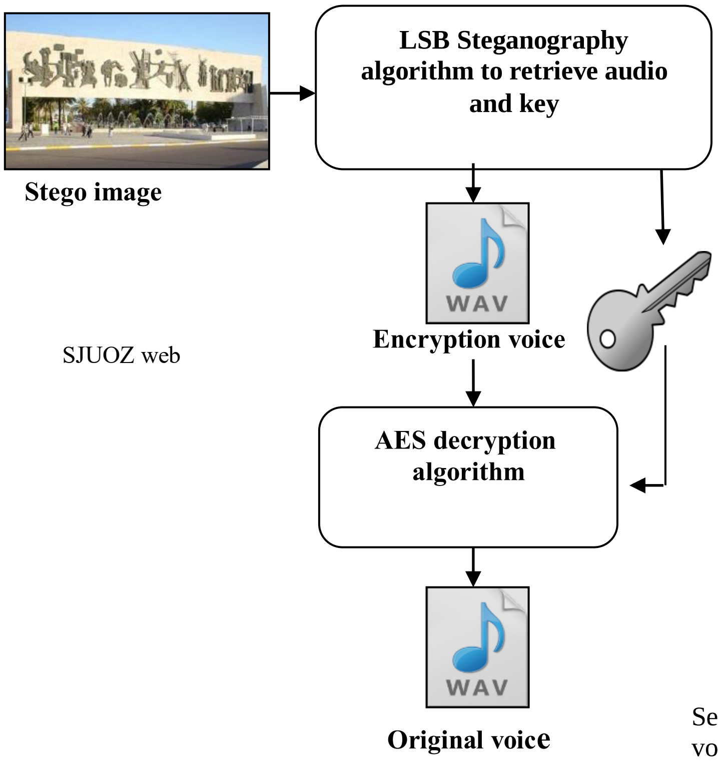


Figure 5. Retrieve the voice

Algorithm (2)

.**Input :** Stego1 image
.**Output :** Original voice

Step 1: Read Stego1 image then convert it .to 8-bit stream
Step 2 : Perform LSB operation on Stego1 image and retrieve bits of encryption voice from Bit "1" and key (text file) from Bit "2" which are hidden in.
Step3 : Perform an AES decryption algorithm using the same key.
Step4 : Convert the result to decimal value for getting the original voice.

Second, when the Stego image received, the encrypted voice and its key have been retrieved. The encrypted voice has been decrypted by using the AES algorithm with the same key to get the original voice message..

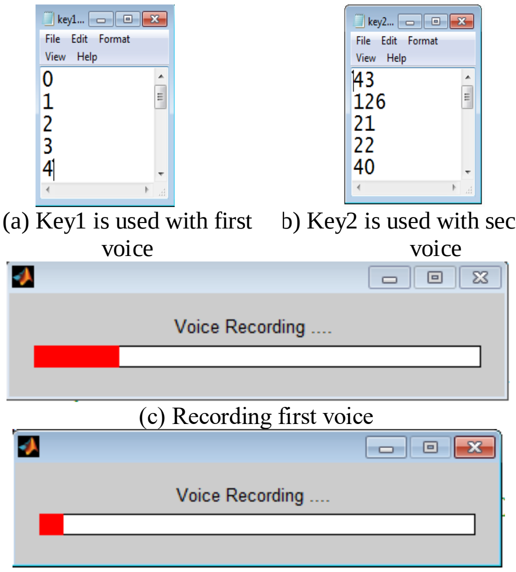
1) Encryption the vioce by AES algorithm and hiding the result inside Cover image, Algorithm (1)
2) Retrieve the voice from Stego image and decryption it by AES algorithm ,Algorithm(2)

8. Experimental Results

This model has been implemented in MATLAB 2013a using LSB Steganography technique. We used TIF images with 512*512 pixel as Cover image and encrypt voice message as Secret part to get TIF images which represent Stego image.

1) .Encryption voice message

We have recorded two voices and save them with formula "wav" which encrypted by using the AES algorithm with key 1 and key 2 respectively.



0
1
2
3
4

43
126
21
22
40

(a) Key1 is used with first voice b) Key2 is used with second voice

Voice Recording ....

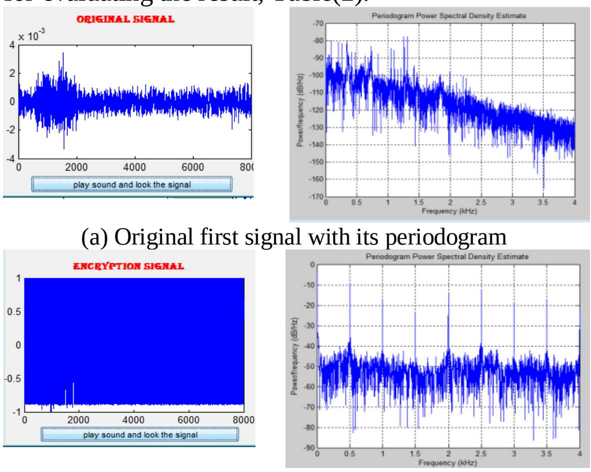
(c) Recording first voice

Voice Recording ....

(d) Recording second voice

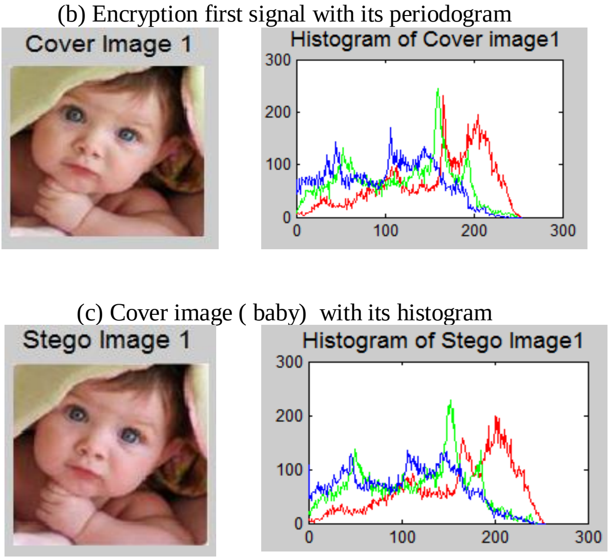
Figure 6. Created the voice and key

We have been hiding encrypt first voice inside image " Baby.TIF" which becomes "Cover image". This encrypt voice and its key have been embedded in Bit "1" and Bit "2" respectively by using LSB algorithm then creating" Stego.TIF", while encrypting second voice and its key have been hidden inside image " Elena.TIF" which becomes "Cover image" which are embedded by using the same algorithm to create" Stego.TIF" that will send. Finally, the Mean Square Error, Peak Signal to Noise Ratio must be calculated for evaluating the result, Table(2).



(a) Original first signal with its periodogram

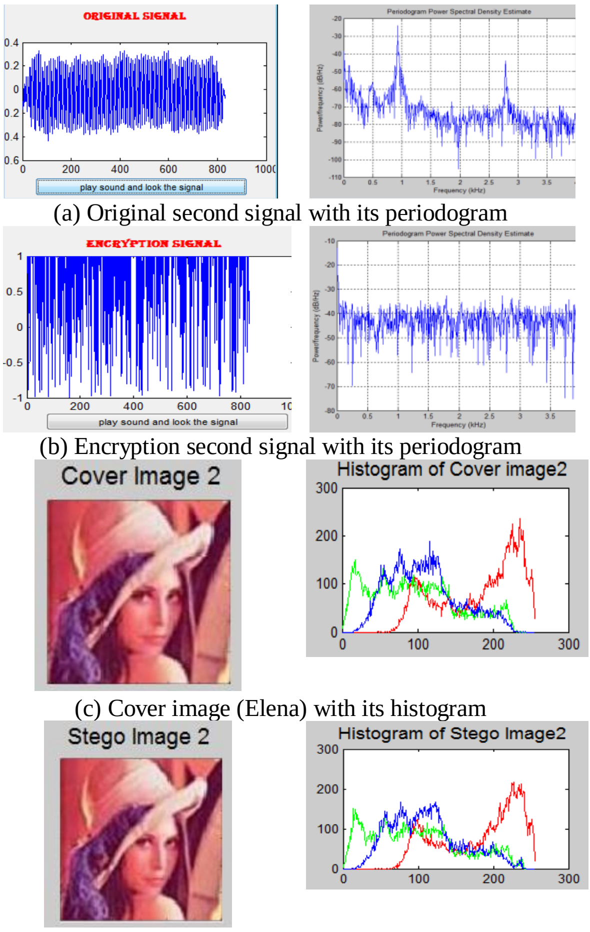
(b) Encryption first signal with its periodogram



(c) Cover image (baby) with its histogram

(d) Stego image (Baby) with its histogram

Figure 7. Encryption first voice and great Stego image



(a) Original second signal with its periodogram

(b) Encryption second signal with its periodogram

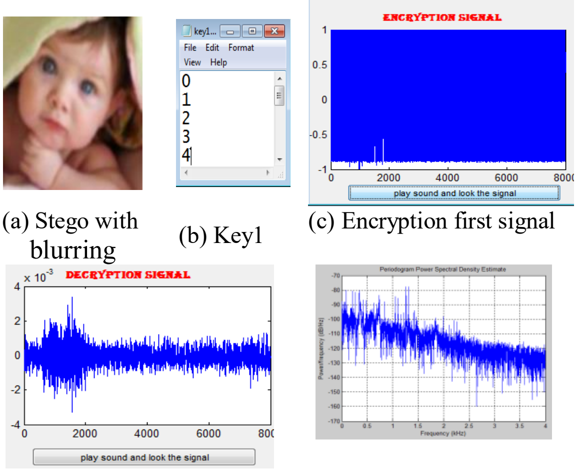
(c) Cover image (Elena) with its histogram

(d) Stego image (Elena) with its histogram

Figure 8. Encryption second voice and great Stego image

2) Retrieve the voice

The hidden data can get back easily from the received image "Stego". By using Steganography algorithm, encrypt voice has been retrieved from Bit "1" and retrieved key that is text file from the Bit "2" which was used to get the original voice by using the AES algorithm. The system has resistance against various attacks. The hidden information can be retrievable from stego-image even if the stego-image is exposed to Median filtering, scaling, and blurring attacks, Figure(9,10) from Stego image with blurring (Baby) can be retrieved Key1 and encrypt first voice while from Steg- image with Median filtering (Elena) can be retrieved Key2 and encrypt second voice then decrypt it to get the original voice.



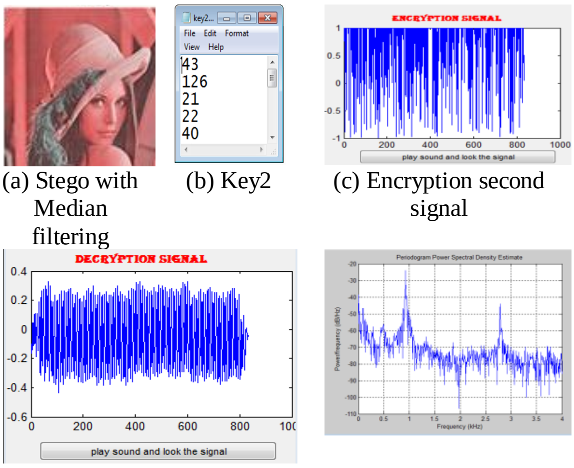
(a) Stego with blurring

(b) Key1

(c) Encryption first signal

(d) Deccryption first signal with its periodogram

Figure 9. Retrieve original first voice



(a) Stego with Median filtering

(b) Key2

(c) Encryption second signal

(d) Deccryption second signal with its periodogram

Figure 10. Retrieve original second voice

Table 2. Shows the results of PSNR and MES obtained for difference between Cover image and Stego image

Cover Image	**Image Format**	**Recorded voice size**	**PSNR**	**MES**	**RE**
Baby	TIF 512*512 pixel	15.6 KB	62.879	0.0335	0.349
Elena	TIF 512*512 pixel	Bytes 876	73.523	0.0028	0.467

9. Conclusion

Cryptography is a method of protecting information and communications through the use of codes while Steganography is the art of writing hidden messages. So this system enables to provide better security when combined both of them by performed the AES algorithm and combined it with a new steganography method. This work is implemented successfully when encrypted a recorded voice message by AES algorithm, then embedded it in color image through the Least Signification Bit steganography (LSB). Inside the color image, we embedded encrypted voice and its key (file text) in Bit "1" and Bit "2" respectively, therefore the receiver gets back both key and encrypted voice easily from image then retrieve the original voice even if the image is exposed to Median filtering, scaling, and blurring attacks by decryption algorithm using the AES algorithm. After performing the work, the results proved that the recorded voice could be hidden in an image but it becomes more secure when encrypting it before hiding it in the image If the unauthorized person is able to remove the cover, he will find confused voice (unclear) and he is not expected to create another voice.

10. Future work

- Though it is a well-built system, it has been limited size of voice message (voice is recorded for one minute). To develop our project, we can increase the size of voice message (voice can be recorded for a long time) then divide the original voice into smaller segments, each segment can be encrypted separately and embedded in a single image. So, in this case, prefers using video steganography instead of image steganography.
- We can get a higher level of security when we use two secret keys for encryption and decryption the voice message. Use the first key with AES algorithm and the second key with image steganography.

Reference

[1] Ahmed.A, Farida.R & Azni.A. (2017). A Hybrid Method for Data Communication Using Encrypted Audio Steganography. *Article in Advanced Science Letters*,1-6, DOI: 10.1166/asl.2017.8946.

[2] Aishwarya.A, Pratibha.R & Sandhya.K. (2019). Secured Audio Encryption using AES Algorithm. *International Journal of Computer Applications*, 178(22), 29 – 33.

[3] Arpita .A.(2016). Secure Digital Communication using LSB based Image Steganography Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(9), 17-21.

[4] Avi .K.(2017). AES: The Advanced Encryption Standard. *Lecture 8 Notes on Computer and Network Security, Purdue University*.

[5] Bhabesh.D, Pradipta.M, Sushmita.M, Dhruba.K, Prabin.K & Sankar.K. (2019). Pattern Recognition and Machine Intelligence Part II Springer, 1-622, ISBN 978-3-030-34871-7.

[6] Diego.R, Sebastian.M & Dora.M. (2019). Encrypted audio dataset based on the Collatz conjecture, *Article in Elsevier Inc.*1-4, DOI:org/10.1016/j.dib.2019.104537.

[7] Dhananjay .M & Nitin.J.(2014). Video Encryption Using AES Algorithm. *IEEE Conference on Current Trends in Engineering and Technology,* 332-337.

[8] Geetha.B, Sathya.L & Susmitha.S.(2016). Embedding Audio in Image for Hiding Information Using MSB Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(6), 444-449.

[9] Hemalatha.S, Dinesh.A & Renuka.A. (2015).Wavelet transform based steganography technique to hide audio signals in image. *Procedia Computer Science Elsevier,* 47 , 272 – 281, DOI: 10.1016/j.procs.2015.03.207.

[10] Himanshu .G & Vinod .K.(2013). Role of Multiple Encryption in Secure Voice Communication. *International Journal of Computer Science and* .316-319 ,)2(*Electronics Engineering (IJCSEE)*, 1

[11] Huda .D. (2019). New Techniques of Watermark Images using Bit Plane Slicing and Cubic-spline Interpolation. *Ibn AL-Haitham Journal for Pure and Applied Science*, 23(3),192-200, doi:10.30526/32 .3.2295.

[12] Liandeng .L, Jiarui. F, Jinlei. J, Lin. G, Weijie. Z, Haohuan. F & Guanwen .Y.(2017). SW-AES: Accelerating AES Algorithm on the Sunway TaihuLight. *IEEE International Conference on Ubiquitous Computing and Communications*, DOI: 10.1109/ISPA/IUCC.2017.00181.

[13] Mahalakshmi.S, Selvarani. R, Thilagam .J & Tharminie.N.(2015). Audio Steganography Using AES Algorithm. *International Journal of Innovative Research in Science*, Engineering and Technology,4(11), 22-27.

[14] Nithya.V & Jawagar.L. (2014). Audio Based Steganography for Hiding Secret Data. *International Journal of Innovative Research in Science, Engineering and Technology*, 3(3),667-680.

[15] Noor.H, Rajaa.A, Hazim.N &Adel.A. (2018). Multilevel hiding text security using hybrid technique steganography and cryptography. *International Journal of Engineering & Technology,* 7 (4), 3674-3677. DOI: 10.14419/ijet.v7i4.20951

[16] Prasada .P, Pinto. A, & Ranjith. H.(2019). FPGA Implementation of Parallel Transformative Approach in AES Algorithm. *Lecture Notes in Networks and Systems*, 333–340,doi:10.1007/978-981-13-0586-3_34.

[17] Rasedur.R, Partha.C, Zahidur.R & Golam.M. (2019). Hiding Confidential File using Audio Steganography. *International Journal of Computer Applications,* 178(50), 30 – 35, DOI: 10.5120/ijca2019919422.

[18] Ratnakirti.R & Suvamoy .C.(2016). Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach. *International Journal of Security and Its Applications,*10(4),179-196.DOI: 10.14257/ijsia. 2016. 10.4.18

[19] Ravi .T ,Gudipati. & Gowtham .P.(2016). Overview of digital audio steganography techniques. *International Journal of Emerging Technologies and Engineering (IJETE)*, 3(7), 62-66.

[20] Zainab. N. (2019). Transmission of an Encryption Audio Message Using Chaotic Map in a Noisy Channel. *Journal of Communications*,14(2),142-147.DOI: 10.12720/jcm.14.2 .142-147