ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

A Secure Image Steganography for Speech Data Hiding

[1] G.Sudha, [2]N. Shilpa, [3] H. Vidhya, [4] Mufshira Parvin. S
[1] Associate Professor, Department of Electronics and Communication,Sri Sai Ram Engineering College, Chennai, India
[2][3][4] Department of Electronics and Communication, Sri Sairam Engineering College, Chennai, India

***Abstract* – In today's internet world the data transmission should be fast and secured. The need for security in data communication is as long as mankind; since eavesdroppers often intercept such communication for malicious purposes. The secured signal may get hacked by breaking the password assigned to the system. Thus it is very important for designing a robust encrypted method for perfect data security. The objective of this project is to transmit an audio signal using digital image steganography technique to ensure security, integrity, robustness, ease of transmission. Audio file and cover image are encrypted using AES encryption algorithm. The encrypted file is converted into a stego file using steganography embedding algorithm. The encrypted and embedded audio file is de-embedded and decrypted at the receiver. The secret speech signal is obtained as it is at the receiver. While cryptography only encrypts the data, steganography ensures secured transmission of input by hiding the existence of data. Applications of steganography include government, military, banking, educational sectors, share market etc.**

Keywords: Segmentation, Encryption, Extraction, Decryption, Steganography

1. INTRODUCTION

The objective of this paper is to transmit an audio signal using digital image steganography technique to ensure security, integrity, robustness, ease of transmission. Audio file and cover image are encrypted using AES encryption algorithm. The encrypted file is converted into a stego file using steganography embedding algorithm. The encrypted and embedded audio file is de-embedded and decrypted at the receiver. The secret speech signal is obtained as it is at the receiver.

II. STEGANOGRAPHY BASICS

Steganography is an art and science of information hiding and invisible communication. It's unlike cryptography, where the goal is to secure communications from an eavesdropper by making the data not understood ; steganography techniques strive to hide the very presence of the message itself from an observer so there is no knowledge of the existence of the message in the first place. In some situations, sending encrypted information will arouse suspicion while invisible information will not do so. Both sciences can be combined to produce better protection of the information. In this case, when the steganography fails and the message cannot be detected if a cryptography technique is used. Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in a news groups.

To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modification. The most common methods to make these alterations involve the usage of the least-significant (LSB). The next interesting application of steganography, in which the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information.

When using a 24 bit colour image, each bit of red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. Thus, 800 × 600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes) of secret data. But using just 3 bit from this huge size of bytes is wasting in size. So the main objective of the present work is how to insert more than one bit at each byte in one pixel of the cover-image and give us results like the LSB (message to be imperceptible).This objective is satisfied by building new steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel.

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction

Though steganography is most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include:

1. Capacity (how much data can be hidden)
2. Invisibility (inability for humans to detect a distortion in the stego-object)
3. Undetectability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects)
4. Robustness (message's ability to persist despite compression or other common modifications)
5. Tamper resistance (message's ability to persist despite active measures to destroy it)
6. Signal to noise ratio (how much data is encoded versus how much unrelated data is encoded).

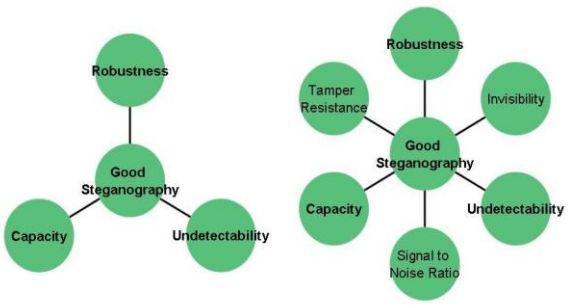

Fig. 1 Characteristics of steganography algorithm

A. Different kinds of steganography

The four main categories of file formats that can be used for steganography are:

1. Text
2. Images
3. Audio
4. Protocol

1)Text steganography: Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

2) Image steganography: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

3) Audio steganography: Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound. This property allows to select the channel in which to hide information.

4)Protocol steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

B. Applications of Steganography

- Copy protection: E-commerce, copy control(DVD),multimedia information distribution(video on demand)
- Documents secret annotation: Medical images, cartography, multimedia databases
- Authentication: Systems of video surveillance, e-commerce, voice mail, electronical confidential paperwork
- Concealed communication: Military applications

III. LITERATURE REVIEW

Niharika Ramacharla et al. (2018) performed steganographic embedding of speech signal into digital images. Adaptive segmentation was used on the cover image and pixel selection was done based on main cases and sub cases. AES algorithm was used for encryption and decryption. Signal to Noise ratio (SNR) was found to have improved to 97.7 from 56.73 [1].

Altaay et al. (2012) presented the important steganography measurements such as capacity, imperceptibility, robustness etc. CIA triangle metrics such

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

as Compression ratio, multiple watermarks, success rate, embedding complexity, and detection complexity were also discussed. Steganography is classified as fragile amd robust steganography. Features and restrictions that an embedding algorithm should meet are also presented. [2].

Divya Sharma (2012) described a cryptography technique for audio to increases the security of audio data meant to be transferred on an insecure medium. The audio is recorded in real time using microphone which is applied with five level of encryption which creates a cipher signal which is routed through an insecure line for the recipient who on receiving that signal decrypts the cipher signal in order to retrieve the signal back. The signal achieved in the proposed technique after decryption at the recipient end is a replica of the original signal which was meant for encryption. The proposed technique hides the audio data such that even if one level of encryption is broken the rest of the levels will still be there to prevent the actual audio data getting discovered by a third party. It guarantees a highly accurate communication between the sender and receiver [3].

Harjinder Kaur et al. (2012) described a four level encryption mechanism for speech signals using time domain scrambling, frequency domain scrambling, amplitude scrambling and two-dimensional scrambling combining frequency and time domain scrambling. The Output or encrypted signal of one level becomes the input for next level and so on .at last the encrypted signal of fourth level becomes the final output or encrypted signal for transmission. Last encrypted signal is a constant beep. The first advantage is that it makes the encrypted speech sound a constant beep. The second advantage is that it does not impose any restriction on the decoding of the specific signal because with every new signal it produces a new hash accordingly. PSNR values are calculated at the end of each stage [4].

Nath et al. (2012) proposed a new steganography method to hide any encrypted secret message in multiple steps. For encrypting secret message the authors have used new algorithm namely TTJSA developed by Nath et al. For hiding encrypted message the authors have used substitution of bits in 4-th bit from LSB of the cover file. Due to multiple time encryption and multiple time data hiding it is almost impossible for any intruder to extract secret message from embedded cover file [5].

Rawashdeh et al.(2014) presented a novel approach integrating image steganography and encryption techniques to achieve higher security. The approach uses primitive roots of prime numbers in selecting the secret key to encrypt a text message and to scatter the encrypted message across the cover PNG colored image. This technique provides higher security because without any knowledge about the used stego key it is very difficult to extract the sensitive text data on just knowing the algorithm. The technique also presents an acceptable level of image quality since the produced quality results are similar to the results of LSB technique, but with more robustness and security. The performance of the proposed approach is compared with the normal LSB technique [6].

Atee .H et al. (2015) proposed the dynamic encryption scheme combined and tested along with two steganographic methods separately to show its performance and effectiveness. The secret message was encrypted and then embedded in one of the two steganographic methods which are LSB and CIBDH. The Peak Signal to Noise Ratio and the Mean Square Error is calculated to measure performance. Satisfactory results are obtained by the two proposed algorithms, which achieved high level of capacity, higher PSNR for security and lower MSE for robustness against attacks [7].

Bin Li et al. (2011) discussed the basic model of steganography and steganalysis and their evaluation criteria. The authors have reviewed major image steganography techniques in spatial domain and in JPEG format. The latest effective and commonly used techniques in steganography and steganalysis are discussed. The paper also provides future scope of steganography in applications such as forensics and watermarking [8].

Vikas Tyagi et al. (2012) presented a work on the use of Least Significant Bit (LSB) algorithm in steganography. The paper discusses the implementation of LSB algorithm in the spatial domain and also the encryption process for hiding the input message through a secret key. The paper also discusses the applications of steganography in fields such as watermarking and fingerprinting [9].

Shikha Dubey et al. (2012) discuss how the edges of the images can be used to hide text message in steganography .It gives the depth view of image steganography and edge detection filter techniques. The LSB algorithm is used for embedding the input message into cover message. Edge detection is performed using zero crossing filter. The input messages are the extracted using the same LSB algorithm and PSNR and MSE values are calculated for different images and tabulated [10].

IV. METHODOLOGY

A. Introduction

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in a news groups. To hide a message inside an image

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modification. The most common methods to make these alterations involve the usage of the least-significant (LSB). The next interesting application of steganography, in which the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information. When using a 24 bit colour image, each bit of red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. Thus, 800 × 600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes) of secret data. But using just 3 bit from this huge size of bytes is wasting in size. So the main objective of the present work is how to insert more than one bit at each byte in one pixel of the cover-image and give us results like the LSB (message to be imperceptible).This objective is satisfied by building new steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel.

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data.

B. Block diagram

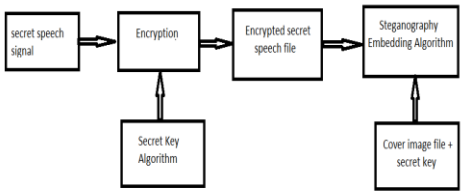

Fig. 2 Transmitter section

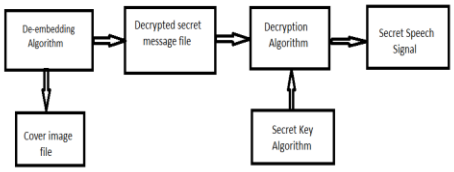

Fig. 3 Receiver section

C. Generation of cover image

- A 3x3 image is chosen as the carrier image.
- Image is converted into gray scale.
- Noise is added to the image.
- Noise is filtered from the image.

The noise filtered image is known as cover image.

1) Adaptive Segmentation : The image taken as the cover image is the JPG image. The cover image is segmented randomly of irregular segments based on the password given. Non uniform segmentation gives more security for giving the input. Lossless compression technique is applied for the JPG image for sending large files. To reconstruct the original imageexactly this lossless compression technique is used.

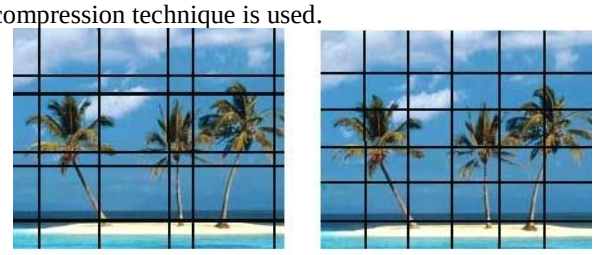

Fig. 4 Image Segmentation

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

```
//password for segmentation
pw_input=input('Enter Password for Segmentation.....: ','s');
L=length(pw_input);
for i=1:L
   Aw(i)=str2num(pw_input(i));
end
N=(round(L/2));

Sv=0;
for i=1:N
   Sv=i^2*Aw(i)+Sv;
end
Sh=0;
for i=(N+1):L
   Sh=i*Aw(i)+Sh;
end
```

2) Adaptive Filtering: An adaptive filter is a filter that self-adjusts its transfer function according to an optimization algorithm driven by an error signal. Because of the complexity of the optimization algorithms, most adaptive filters are digital filters.

3) Lossless Compression : Lossless data compression is a class of data compression algorithms that allows the original data to be perfectly reconstructed from the compressed data. By contrast, lossy data compression, permits reconstruction only of an approximation of the original data, though this usually allows for improved compression rates (and therefore smaller sized files).Lossless audio formats are most often used for archiving or production purposes, while smaller lossy audio files are typically used on portable players and in other cases where storage space is limited or exact replication of the audio is unnecessary.

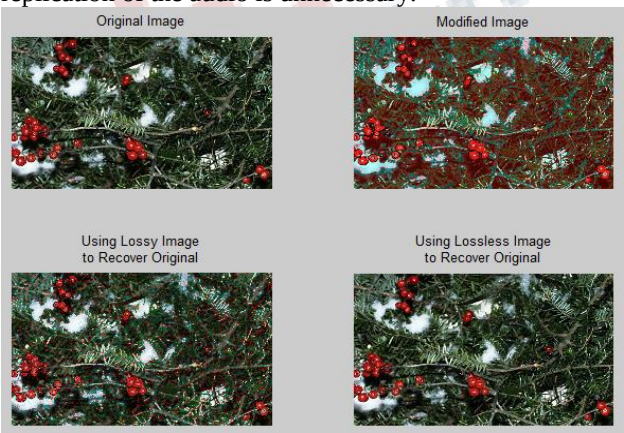

Fig. 5 Lossy and lossless compression

4) Cover Image : Cover image is "filtering the noise" from the original image. The noise removed image is called cover image.

a) Original image b) cover image

Fig. 6 Generation of cover image

D. Encryption using AES

The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round. All of the phases use the same sub-operations in different combinations as follows:

Initial round

- AddRoundKey

Main Rounds

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

Final Round

- SubBytes
- ShiftRows
- AddRoundKey

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

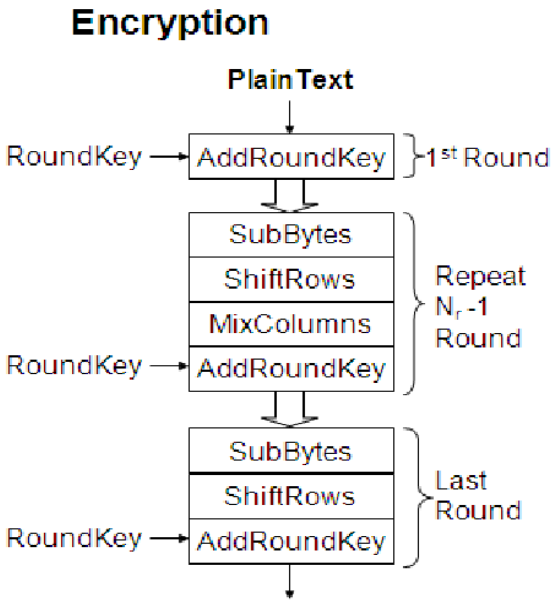

Fig. 7 Encryption in AES

1) AddRoundKey: The AddRoundKey operation is the only phase of AES encryption that directly operates on the AES round key. In this operation, the input to the round is exclusive-ored with the round key.

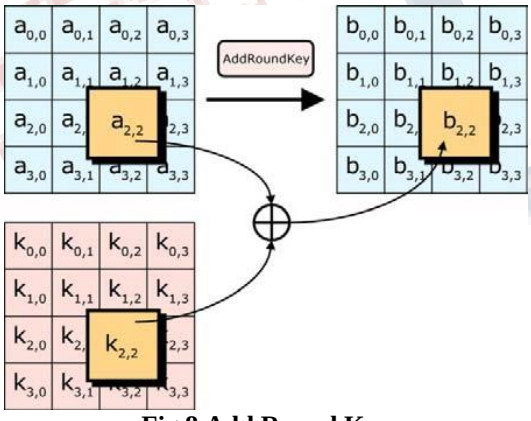

Fig 8 Add Round Key

2) SubBytes: The SubBytes phase of AES involves splitting the input into bytes and passing each through a Substitution Box or S-Box. Unlike DES, AES uses the same S-Box for all bytes. The AES S-Box implements inverse multiplication in Galois Field 28.

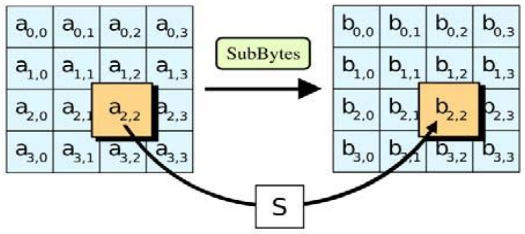

Fig. 9 Sub bytes

The AES S-Box is shown in the Table below.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 10 Lookup table for encryption

To read this table, the byte input is broken into two 4-bit halves. The first half determines the row and the second half determines the column. For example, the S-Box transformation of 35 or 0x23 can be found in the cell at the intersection of the row labeled 20 and the column labeled 03. Therefore decimal 35 becomes 0x26 or decimal 38.

3) ShiftRows: In the ShiftRows phase of AES, each row of the 128-bit internal state of the cipher is shifted. The rows in this stage refer to the standard representation of the internal state in AES, which is a 4x4 matrix where each cell contains a byte. Bytes of the internal state are placed in the matrix across rows from left to right and down columns. In the ShiftRows operation, each of these rows is shifted to the left by a set amount: their row number starting with zero. The top row is not shifted at all, the next row is shifted by one and so on.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

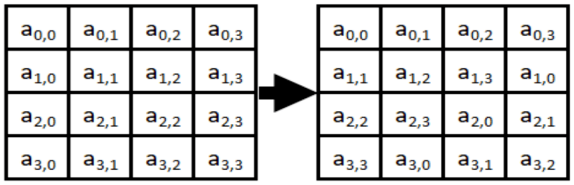

Fig. 11 Shift Rows

In the figure, the first number in each cell refers to the row number and the second refers to the column. The topmost row (row 0) does not shift at all, row 1 shifts left by one, and so on.

4) MixColumns: Like the ShiftRows phase of AES, the MixColumns phase provides diffusion by mixing the input around. Unlike ShiftRows, MixColumns performs operations splitting the matrix by columns instead of rows.

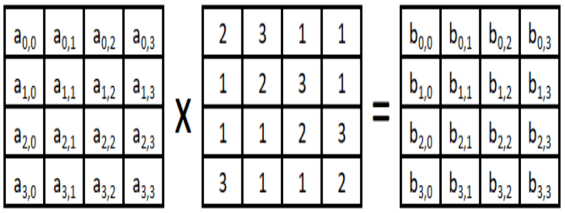

Fig. 12 Mix Columns

E. Steganography Embedding

The leftmost bit is the most significant bit. If we change the leftmost bit it will have a large impact on the final value. For example, if we change the leftmost bit from 1 to 0 (11111111 to 01111111) it will change the decimal value from 255 to 127. On the other hand, the rightmost bit is the less significant bit. If we change the rightmost bit it will have less impact on the final value. For example, if we change the leftmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254. Note that the rightmost bit will change only 1 in a range of 256 (it represents less than 1%). Summarizing: each pixel has three values (RGB), each RGB value is 8-bit (it means we can store 8 binary values) and the rightmost bits are less significant. So, if we change the rightmost bits it will have a small visual impact on the final image. This is the steganography key to hide an image inside another. Change the less significant bits from an image and include the most significant bits from the other image.

LSB works by replacing the least significant bit of the Pixel value of the cover image (in most of the cases 8 bit is replaced).

Example: Consider a 3- pixel grid in a 24- bit image:

00110011 01100011 01101111
01101110 01101100 00110100
01101101 01100101 01101011

Suppose we want to hide a character 'y' in the image. The ASCII code of 'y' is 121 whose binary value is 01111001. Now pixels after embedding the message in the image are as shown

00110010 01100011 01101111
01101111 01101101 00110100
01101100 01100101 01101011

8 bits were to be embedded in the image however only 4 bits were changed. Thus on an average only half of the bits are changed in the embedding process. In LSB process we use BMP (bitmap) images because they are lossless compression images. In lossless compression size of file is reduced but it does not affect the quality of file. The original data in the file is restored when the file is uncompressed.

Embedding the text inside the image:

- Calculate the Pixels of the image.
- Make a loop through the pixels.
- In each pass get the red, green and blue value of pixels.
- Make the LSB of each RGB pixel to zero.
- Get the character to be hidden in binary form and hide the 8-bit binary code in the lsb of pixels.
- Repeat the process until all the characters of the image are hidden inside the image.

F. Extraction of audio from image

The password is given for extraction of the audio file from the cover image. The pixels are scanned based on password. If the right password is given, audio is extracted and process moves to decryption. If a wrong password is given, an error message is shown on the screen.

G. Decryption using AES

To decrypt an AES-encrypted cipher text, it is necessary to undo each stage of the encryption operation in the reverse order in which they were applied. The three stage of decryption are as follows:

Inverse Final Round

- AddRoundKey
- ShiftRows
- SubBytes

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

Inverse Main Round
- AddRoundKey
- MixColumns
- ShiftRows
- SubBytes

Inverse Initial Round
- AddRoundKey

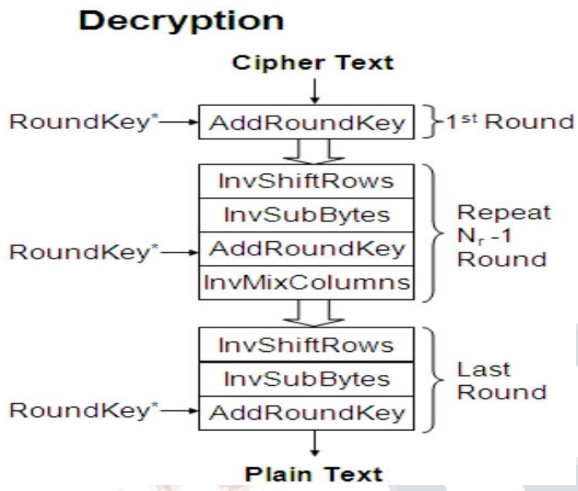

Fig. 13 Decryption in AES

Of the four operations in AES encryption, only the AddRoundKey operation is its own inverse (since it is an exclusive-or). To undo AddRoundKey, it is only necessary to expand the entire AES key schedule (identically to encryption) and then use the appropriate key in the exclusive-or.
The other three operations require an inverse operation to be defined and used. The first operation to be undone is ShiftRows. The Inverse ShiftRows operation is identical to the ShiftRows operation except that rotations are made to the right instead of to the left.

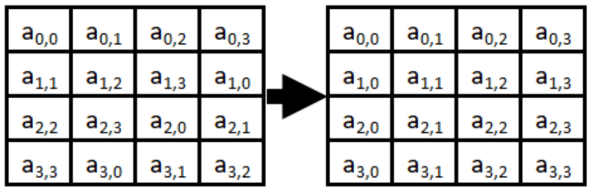

Fig. 14 Inverse Shift Rows

The next operation to be undone is the SubBytes operation. The Inverse S-Box is shown in the Table below. It is read identically to the S-Box matrix.

	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f	
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
70	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Fig. 15 Lookup table for decryption

The last inverse operation to define is MixColumns.

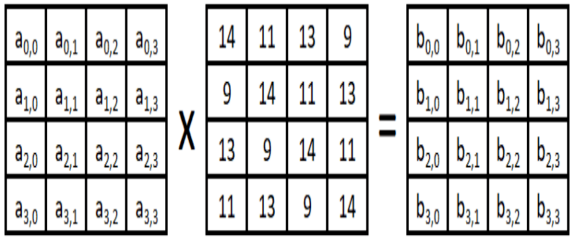

Fig. 16 Inverse Mix Columns

V. RESULTS AND DISCUSSIONS

The waveforms of the audio signal are obtained as follows. In this signal waveform, the audio signal which is a .wav file is displayed in time domain. The peak to peak value is inferred to be approximately 1.6. From the amplitude spectrum of the signal, -40db peak magnitude is obtained at 1000Hz. The strength of autocorrelation is sufficient for the signal to be transmitted without any distortion to the receiver.

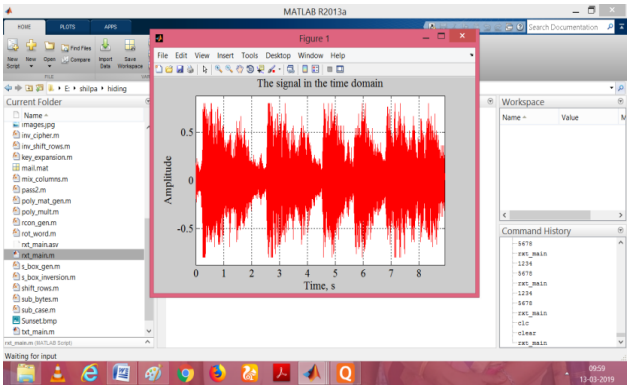

Fig. 17 Signal in the time domain

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

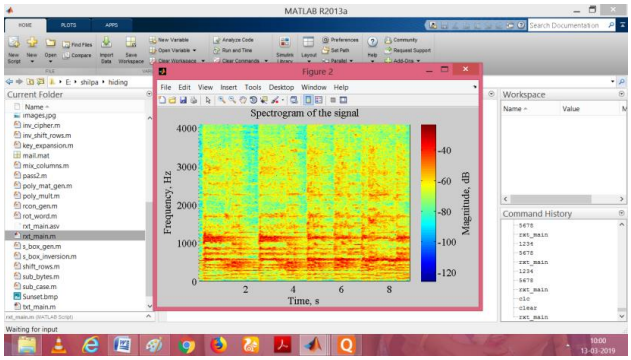

Fig. 18 Spectrogram

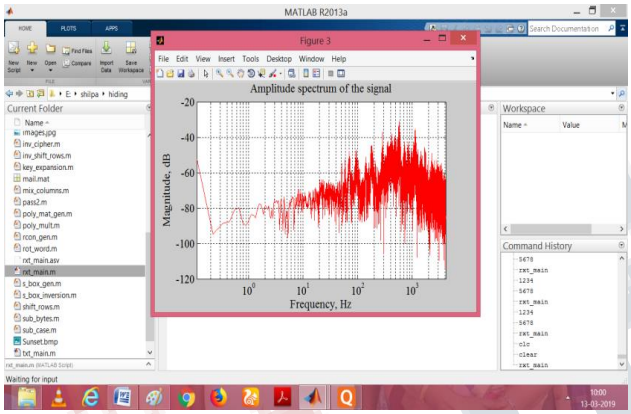

Fig. 19 Amplitude Spectrum

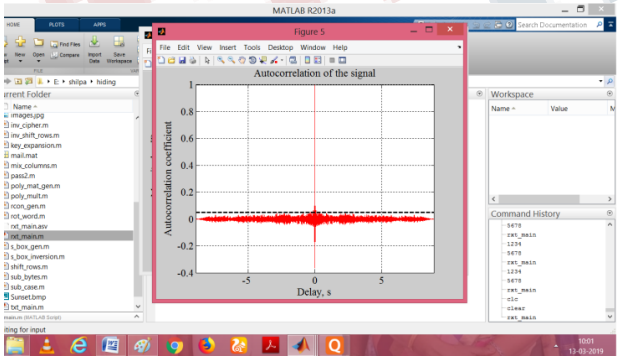

Fig. 20 Autocorrelation

Input and output parameters such as minimum value, maximum value, mean value, rms value, dynamic range, crest factor and autocorrelation time are measured and found to be equal.

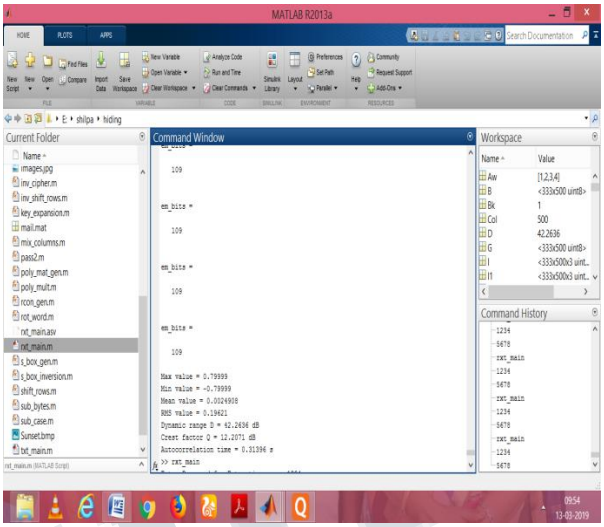

Fig. 21 Transmitter parameters

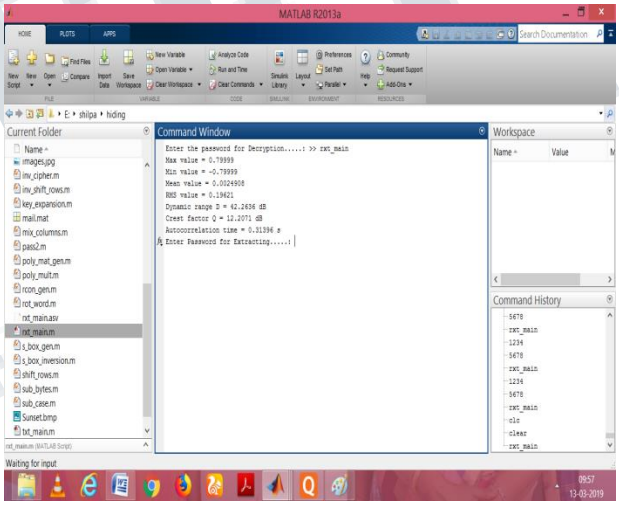

Fig. 22 Receiver Parameters

VI. CONCLUSION

The proposed method uses AES encryption standard to provide maximum security. Steganography ensures that the existence of the message is not known to any malicious person. Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

VII. FUTURE SCOPE

The experiment shows that our method is secure, imperceptible and can be used for hiding data in the image file. In the future, more powerful encryption standards can be used along with steganography to improve security. Critical applications of steganography such as digital watermarking and fingerprinting can be analyzed in the future. In summary, if implemented correctly and in conjunction with cryptographic methods to secure the embedded data before insertion to a cover medium, many of the data hiding methods described above could become powerful tools for the transmission of undetectable and secure communication.

VIII. REFERENCES

[1] Niharika Ramacharla, Sindhu Priya and Dr.E. Logashanmugam, A Secure Image Steganography for speech data hiding in digital images, International Journal of Pure and Applied Mathematics, Volume 118 No. 17 2018, 509-522.

[2] Altaay,J.S.Sahib and Mazdak Zamani, An Introduction to Image Steganography Techniques, International Conference on Advanced Computer Science Applications and Technologies, 2012, pp.122-126.

[3] Divya Sharma, Five level cryptography in speech processing using Multi hash and repositioning of speech elements, International Journal of Engineering Technology and Advanced Engineering, Vol. 2, No. 5, PP. 21- 26, 2012

[4] Harjinder Kaur, Gianetan Singh Sekhon, A four level speech signal encryption algorithm, IJCSC, Vol. 3, No. 1, PP. 151-153, January 2012.

[5] Joyshree Nath, Saima Ghosh, Asoke Nath, Advanced digital steganography using encrypted secret message and encrypted embedded cover file, International Journal of Computer Applications, Vol. 46,No.14, PP. 1- 7,May 2012

[6] Obaidah A. Rawashdeh and Dr. Nedhal A. M. Al-Saiyed, A Novel Approach for Integrating Image Steganography and Encryption, Int.J.Computer Technology & Applications,Vol 5 (6),1917-1923.

[7] Atee H., Ahmad R., and Noor N., Cryptography and Image Steganography using Dynamic Encryption on LSB and Color Image Based Data Hiding, Middle-East Journal of Scientific Research, vol. 23, no. 7, pp. 1450-1460, 2015.

[8] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi. A survey on Image steganography and steganalysis, Volume 2, Number 2, April 2011.

[9] Mr . Vikas Tyagi, Mr. Atul kumar, Image Steganography Using Least Significant Bit With Cryptography, Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012.

[10] Jain, Nitin, Sachin Mesh ram, and Shikha Dubey, Image Steganography Using LSB and Edge–Detection Technique, International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.