Combined Audio Steganography and AES Encryption to Hide the Text and Image into Audio using DCT

Siddalingesh Bandi, Manjunatha Reddy H S

Abstract*: Recently, security has become the prime concern for any organization and other civil and military applications. In this field of security, the data security during communication over an insecure wireless channel is the most important task which can be done by performing cryptography, watermarking and steganography. However, cryptography and watermarking schemes can be identified easily because of change in the data structure hence attackers can focus on that particular part to hack the secret information whereas steganography is a hiding mechanism in which secret message can be concealed into the cover and it can be retrieved at the receiver end. Several techniques have been introduced during last decade which are focused on image-image steganography and audio steganography. In the proposed work, we concentrate on audio steganography and develop a novel approach where secret message can be in the form of plain text or image, whereas cover message is in the form of audio. In order to provide additional security to this model we incorporate AES encryption scheme where secret message is encrypted and hidden in the cover audio. The proposed approach uses DCT coefficient computation and AES encryption scheme. An extensive experimental study is carried based on different test cases and evaluated against state-of-art techniques. The experimental study shows that the proposed approach achieves better performance for audio steganography.

***Index Terms*: Data Security, Discrete Cosine Transform, Multimedia Steganography, AES Encryption.**

I. INTRODUCTION

Demand of multimedia communication has increased drastically due to the immense growth of internet based applications. This growth in multimedia applications includes audio, video and image types of data which are widely adopted in the real-time communication systems such as wireless multimedia sensor networks, medical field, and military applications. The multimedia data is exchanged in an open environment which is considered prone to the security threats hence security is the prime concern in the multimedia and infotainment applications. Several researches have been carried out to enable the security, these techniques are based on the watermarking [1], cryptography [2] and steganography [3] concept. According to the digital watermarking, the information which need to be hide is known as watermark. This watermark is embedded into a multimedia data to maintain the no tampering on the original digital data. Similarly, according to the cryptography process, the data is encrypted to secure it from various attackers. In this process of cryptography, the encrypted data becomes meaningless until is reconstructed in its actual form. The cryptographic data can be identified by the attackers due to its deformed structure of data which can reveal that some sensitive information is being transmitted over the communication channel. On other hand, according to the steganography model, the secret data can be embedded in a cover message which can be transmitted to the desired destination. The Cover and secret data can be in the form of audio, video and image. The steganography is considered as the most promising technique for facilitating the secure communication without affecting the data quality. Several steganography models are presented which include the image, audio and video steganography. Recently, Jiang et al. [3] presented image-to-image steganography model using LSB (Least Significant Bit) technique. Hemalatha et al. [4] introduced a technique to hide the audio in the image using wavelet transform. Yao et al. [5] presented video steganography using motion-vector technique.

The conventional approach of image steganography suffer from various issues such as image quality, PSNR and extraction quality. In order to overcome these issue, recently, we have introduced scrambling based blind image steganography using wavelet transform [6] which shows a significant improvement in the image steganography. In this work, we focus on the audio steganography where we aim on combining the audio message into the cover audio signal. A general framework of audio signal steganography is depicted in figure 1.

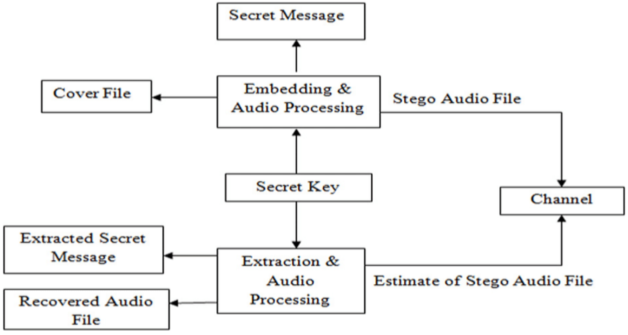

Figure 1: General architecture of audio steganography

Manuscript published on 30 September 2019
* Correspondence Author

Siddalingesh Bandi*, Department of ECE, Global Academy of Technology, Bengaluru. Email: siddubandi@gat.ac.in.

Manjunatha Reddy H S, Department of ECE, Global Academy of Technology, Bengaluru. Email: manjunatha reddy.hs@gat.ac.in.

According to the given architecture, the secret message can be in the form of audio, video or image but in this work we limit the proposed solution for audio file as secrete and cover files. Both audio files are processed through the embedding processing of steganography which generates the Stego audio which is generated with the help of a secret key. This file need to be transmitted over the insecure channel and received at the receiver end. After receiving at receiver end, the data extraction phase is performed which helps to extract the secret audio and cover audio files. Generally, steganography techniques are classified as temporal domain, frequency domain, and wavelet domain. The temporal domain techniques include several techniques such as LSB, parity coding and Echo hiding. Islam et al. [7] presented LSB image steganography technique along with the AES encryption technique. Zhou et al. [8] also presented a combined approach of watermarking and steganography where Arnold scrambling with LSB is implemented to improve the steganography. The techniques presented in [3, 7, 8] are implemented for image steganography. Thangadurai et al. [9] introduced LSB steganography for hiding text secret message into the audio cover data. Begum et al. [10] also presented LSB based audio steganography technique.

Similarly, the frequency domain techniques include the phase coding, spread spectrum and tone insertion techniques. Several researches have been carried out based on these techniques. Antony et al. [11] presented a literature review study and presented a brief review about phase coding based techniques. These techniques are also adopted in audio steganography. Rekik et al. [12] presented brief discussion about phase coding technique for audio steganography. On other hand, wavelet domain based techniques are also widely adopted for different types of steganography schemes. Ghasemi et al. [13] presented wavelet transform and genetic algorithm based approach for image steganography. These studies shows a noteworthy contribution in for steganography but in the case of audio steganography loss of the information can significantly degrade the performance and data may become unsuitable for analysis. Thus, the audio steganography is considered as more challenging task.

In order to deal with these issue, we present a novel solution to obtain the audio steganography which can perform the steganography for audio where cover and secret message are considered as text and image files. The main contribution of this work are as follows:

Rest of the manuscript is structured as follows: section II reviews the literature about existing techniques of steganography; the proposed solution is described in section III; section IV presents the experimental study and comparative performance analysis using proposed approach; and finally, section V presents the concluding remarks and future work direction.

II. LITERATURE SURVEY

This section presents a brief discussion about recent methods of steganography. In this discussion we include image, audio and video steganography schemes.

Bhowal et al. [14] discussed a novel approach for audio steganography. According to this method, authors presented a combined model of RSA encryption and genetic algorithm for audio steganography. This method uses LSB technique along with the Genetic algorithm to encode the message successfully into the audio. To improvise the robustness of the system, the message bits are encoded randomly into the higher LSB layers and GA operators helps to reduce the distortion.

Chadha et al. [15] presented image steganography technique in audio files using Least Significant Bit (LSB) technique. This work uses both, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) technique for data hiding in audio. This scheme provides higher capacity for watermarking which improves the robustness of the system.Nugrahaet. al. [16] presented steganography technique for hiding the audio data using direct spread spectrum sequence mechanism. This model requires a secret key to embed the data as data will be encoded as noisy signal which is modulated using the pseudo-noise. Tayel et al. [17] introduced LSB technique of audio steganography which is implemented using Arduino boards. In this method, the cover and secret both files are considered in the form of audio and LSB technique is implemented to obtain the embedded audio and final extracted audio.

Gambhir et al. [18] presented a new approach which provides multilayer security by combining the cryptography and steganography scheme. In order to mix the cryptography, the RSA algorithm is applied where ciphers are generated and these ciphers are processed through the LSB steganography scheme. Similar, approach is implemented at the receiver end where original data is recovered from ciphers and LSB extraction is applied to extract the complete data.

Kanhe et al. [19] also considered that the cryptography is an important part of any steganography scheme. Hence, authors introduced advance cryptography based methods to present the new method for steganography. According to this approach LSB based steganography is used for hiding the data and AES 128-bit encryption is applied for encrypting the data. Mohajon et al. [20] developed improved approach for audio steganography using LSB method where security key and genetic algorithm (GA) are considered as the important factor, the combined model of GA and security key is implemented to generate the embedded audio data. This study mainly focuses on the development of a robust approach where more number of data bits can be concealed into the audio files.

Das et al. [21] presented audio-text steganography model where the cover message is in the form of audio and the secret message is in the form of plain text. The DWT scheme is applied which generates the coefficients and encrypts these coefficients to generate the embedded audio file for secure transmission.

Yang et al. [22] discussed that audio steganography is likely to add the noise into the original signal and presented a new concept where a high-quality audio is generated automatically which can be useful for hiding the plain text message. This scheme is known as automatic audio generation-based steganography (AAG-Stega). This scheme shows a significant improvement in the performance of data hiding capacity.

Hemalatha et al. [4] developed image steganography technique where cover data is considered as image file and the secret message is in the audio form. The wavelet transform scheme is applied to achieve the embedded data. In this field of data security, the convolutional neural networks also have gained attraction from research community.

Recently, Chen et al. [23] presented CNN based approach for the audio steganography analysis. In this process, the $\pm 1\ LSB$ are analyzed to identify the steganography content. Moreover, convolution and max pooling to perform the data subsuming task which helps to reduce the overfitting error in the CNN learning.

Recently, Mustafa et al. [24] presented a new LSB algorithm which is known as LSB-block. In this process, the secret message is embedded in the audio file. A Binaries of Message Size Encoding model is presented to generate the key to secure the data before transmitting.

III. PROPOSED MODEL

This section presents the proposed solution for hiding text and image data in the audio i.e. the cover message is in the audio form and the secret message can be in the form of plain text or image. In order to make it more robust, we apply data cryptography schemes also where the secret data is divided into multiple blocks and these blocks are encrypted and then data embedding is applied. Similarly, during the extraction phase the data is decrypted and extracted using the extraction algorithms.

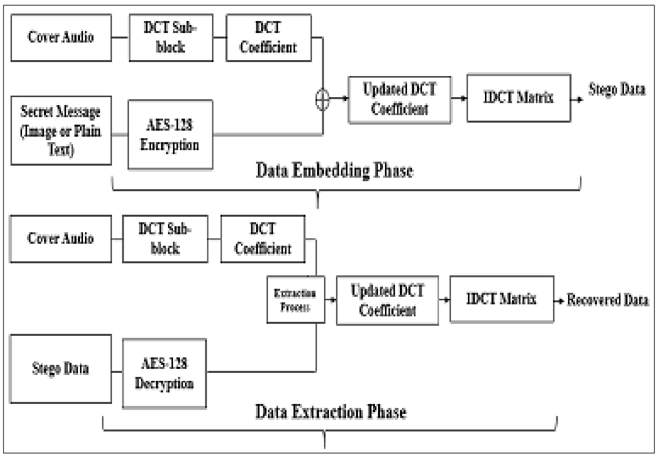

Figure 2: Proposed architecture

Figure 2 shows the complete architecture of proposed model where DCT scheme is implemented to divide the image into various blocks where DCT coefficients are computed for the given input image. At the same time the secret message is encrypted using AES-128 encryption scheme and these two data are combined together and the DCT matrix is updated. Finally, IDCT matrix is computed and the Stego data is obtained in the form of audio. Similarly, complete inverse process is performed to recover the hidden data from the Stego audio. Based on the quality of recovered data, the performance is computed and compared with the existing techniques.

A. AES Encryption Module

The first stage of proposed model is to present a cryptography scheme which can be useful for encrypting the image and plain text for better security. At this stage, we apply AES encryption which contains several operations such as sub-byte, shift-rows, mix-column, and add round key, similarly, for decryption, inverse sub-byte, inverse shift row, inverse mix column and inverse add round key operation are performed.

In this work, we consider that the input or output array is fixed which is considered as 128 bits. This is data is constructed into 4x4 matrix where every four bytes are arranged into the descending order of columns i.e. first four bytes into 1st column, and last four bytes into last columns. The input/output array is represented in the matrix form which is given as:

$$\begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix}$$

(a) Sub bytes

This is the first step of encryption phase. According to this step, the multiplicative inverse of given byte is computed using a polynomial function as $x^8 + x^4 + x^3 + x + 1$ in the GF (2^8) and this value is replaced in the considered input state matrix. In the next phase, affine transform is applied such as :

$$\beta_i = \beta_i \oplus \beta_{(i+4)\ mod\ 8} \oplus \beta_{(i+5)\ mod\ 8} \oplus \beta_{(i+6)\ mod\ 8} \oplus \beta_{(i+7)\ mod\ 8} \oplus c_i \qquad (1)$$

Where c_i is the i^{th} bit whose value is '63H'

(b) Shift rows

This is the second phase of the AES encryption model. In this step, the first row is kept fixed for the considered 4x4 matrix and other elements are shifted circularly i.e. elements of second row are shifted by one byte to the left, elements of third row are shifted by two bytes and fourth row elements are shifted by three bytes. This can be represented as given in (2)

$$\begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix} \begin{matrix} \rightarrow \\ \rightarrow \\ \rightarrow \\ \rightarrow \end{matrix} \begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,1} & D_{1,2} & D_{1,3} & D_{1,0} \\ D_{2,2} & D_{2,3} & D_{2,0} & D_{2,1} \\ D_{3,3} & D_{3,0} & D_{3,1} & D_{3,3} \end{bmatrix}$$

(c) Mix-Columns operation

According to this step, the each column of this matrix is processed separately and the each bye is replaced with the value which is dependent on the data present in the columns. In order to perform this task, a matrix multiplication is performed in GF (2^8) with the help of prime polynomial as $m(x) = x^8 + x^4 + x^3 + x + 1$. This can be expressed as:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix} = \begin{bmatrix} D'_{0,0} & D'_{0,1} & D'_{0,2} & D'_{0,3} \\ D'_{1,0} & D'_{1,1} & D'_{1,2} & D'_{1,3} \\ D'_{2,0} & D'_{2,1} & D'_{2,2} & D'_{2,3} \\ D'_{3,0} & D'_{3,1} & D'_{3,2} & D'_{3,3} \end{bmatrix} \qquad (3)$$

(d) Add-round key operation

In this process, the input 128-bit input state is mapped into 128-bit output state by performing the XOR operation between input states with 128-bit round key. This is given as:

$$\begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix} \oplus [W_i W_{i+1} W_{i+2} W_{i+3}] = \begin{bmatrix} D'_{0,0} & D'_{0,1} & D'_{0,2} & D'_{0,3} \\ D'_{1,0} & D'_{1,1} & D'_{1,2} & D'_{1,3} \\ D'_{2,0} & D'_{2,1} & D'_{2,2} & D'_{2,3} \\ D'_{3,0} & D'_{3,1} & D'_{3,2} & D'_{3,3} \end{bmatrix} \quad (4)$$

(e) Key Expansion

In the key expansion phase, the key used for cipher generation is expanded into a 44 words array. The cipher key is initialized by copying a cipher key into 4 words and then a loop is initialized to create the words.

B. AES Decryption Module

The previous section presents the data encryption process using AES algorithm. In this sub-section we discuss about the data decryption process.

(a) Inverse shift rows operation

Similar to the shift row operation, in this step also, the first row is kept fixed and other rows are shifted circularly. The second row is shifted in to the right by one byte, third and fourth rows are also shifted by two and three bytes respectively. This is represented as follows:

$$\begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix} \begin{matrix} \rightarrow \\ \rightarrow \\ \rightarrow \\ \rightarrow \end{matrix} \begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,1} & D_{1,2} & D_{1,3} & D_{1,0} \\ D_{2,2} & D_{2,3} & D_{2,0} & D_{2,1} \\ D_{3,3} & D_{3,0} & D_{3,1} & D_{3,2} \end{bmatrix} \quad (5)$$

(b) Inverse sub-byte operation

In this step the affine transform is applied in each input byte of the considered input matrix. The affine transform is given as:

$$\beta_i = \beta_i \oplus \beta_{(i+2)\ mod\ 8} \oplus \beta_{(i+5)\ mod\ 8} \oplus \beta_{(i+7)\ mod\ 8} \oplus d_i \quad (6)$$

$d_i$is the data bit whose value is ‘05H’

(c) Inverse Add-round operation

In this step, modulo 2 addition is performed to expand the key during expansion. This can be performed as given below:

$$\begin{bmatrix} D_{0,0} & D_{0,1} & D_{0,2} & D_{0,3} \\ D_{1,0} & D_{1,1} & D_{1,2} & D_{1,3} \\ D_{2,0} & D_{2,1} & D_{2,2} & D_{2,3} \\ D_{3,0} & D_{3,1} & D_{3,2} & D_{3,3} \end{bmatrix} \oplus [W_i W_{i+1} W_{i+2} W_{i+3}] = \begin{bmatrix} D'_{0,0} & D'_{0,1} & D'_{0,2} & D'_{0,3} \\ D'_{1,0} & D'_{1,1} & D'_{1,2} & D'_{1,3} \\ D'_{2,0} & D'_{2,1} & D'_{2,2} & D'_{2,3} \\ D'_{3,0} & D'_{3,1} & D'_{3,2} & D'_{3,3} \end{bmatrix} \quad (7)$$

(d) Inverse Add-round operation

In this step, the each column of the matrix is processed separately and a matrix multiplication is performed in GF 2^8 using a prime polynomial which is given as: $m(x) = x^8 + x^4 + x^3 + x + 1$. At this phase, the module arithmetic is used during matrix multiplication.

This complete process is used for encrypting and decrypting the data to provide more security to the steganography model. In the next phase we discuss about DCT coefficient computation.

C. Discrete Cosine Transform (DCT)

This method is adopted for transforming the data from spatial domain to frequency domain. Let us consider the scenario where we are aimed at hiding the image into the audio. The input imageis divided into 8x8 block size and the original image size is considered as $M \times N$. The DCT coefficient for given image can be computed as:

$$F(u,v) = \frac{1}{4} C(u) C(v) \sum_{i=1}^{8} \sum_{i=1}^{8} f(x,y) \times Z \quad (8)$$

Where $C(i) = f(x) = \begin{cases} 1/\sqrt{2}, & if\ i = 0 \\ 1, & else \end{cases}$ and $Z = \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{x(2y+1)v}{16}\right]$

After applying the DCT on input image, the DCT coefficient matrix K is obtained. This matrix data is arranged in such a way that its higher values are accumulated at the top left side. The higher value represents the lower frequency and higher signal energies.

After achieving the coefficient matrix, we apply the quantization using a standard quantization matrix (Q)can be taken from [25]. With the help of quantization, we obtain a matrix $P(i,j)$ as:

$$P(i,j) = \frac{K(i,j)}{Q(i,j)} \quad (9)$$

On this matrix P, the zigzag scanning is applied to arrange the metrices as low frequency to higher frequency. Now this data need to be embeded in to the audio data hence we cosnider LSB based method which can provide the stego data and inverse zigzag is applied on this obtiained array to reconstruct the stego image.

D. Extraction Process

In this section we present the discussion about data extraticon process. According to this appraoch, the quantized DCT coefficients and middle band coefficents are identified. The quantized coefficents can be identifeid by applying entropy coding.

In the next phase, the bit sequence of encrypted message is extracted from the DCT quantized coefficents and these coefficnets are arranged accrding to the quantization table. After receiving the array of encrypted message, the message is decrypted with the secret key and the decrypted array is arranged.

IV. Results and Discussion

In this section, we present the experimental study where we have considered two types of scenario. The first experiment scenario is focused on the hiding the text into the audio and the next phase focused on the hiding the image data in the audio cover data.

A. Performance Measurement Parameters

In order to measure the performance of proposed steganography model, we consider several performance measurement parameters such as: SNR (signal to noise ratio), PSNR (Peak Signal to noise ratio), embedding capacity and Structural Similarity Index and Normalized Cross-Correlation (NCC).

SNR can be computed as:

$$SNR = 10\log 10\left(\sum \frac{X^2(n)}{\sum X^2(n) - \sum Y^2(n)}\right) \qquad (10)$$

Where X and Y denotes the original and recovered signal. Similarly, the PSNR value can be computed as:

$$PSNR = 10\log 10\left(\sum \frac{R^2}{MSE}\right) \qquad (11)$$

where $MSE = 10\log 10 \sum_{i=1}^{n} \frac{(X-y)^2}{M*N}$, M and N represents the row and columns of the image data. $R$is the maximum signal value.

Hiding capacity is computed by taking the ratio of size of hidden data and cover data. It can be computed as:

$$Capacity = \frac{hidden\ data\ size}{Cover\ data\ size} \times 100 \qquad (12)$$

Similarly, we compute the structural similarity which is computed using luminance, structural difference and contrast between two images. This is computed as:

$$SSIM(S,E) = \frac{(2\varphi_s\varphi_E + c_1)(2\sigma_{SE} + c_2)}{(\varphi_S^2 + \varphi_E^2 + c_1)(\sigma_S^2 + \sigma_E^2 + c_2)} \times 100 \qquad (13)$$

Where φ_s and φ_E are the mean of secret and extracted image. σ_S and σ_E represents the standard deviation of secret and extracted image.

B. Hiding Text Data in the Audio

In order to perform the audio steganography we consider the publically available dataset which can be obtained from [26]. Generally, this dataset is used for genre classification where total 120 tracks are present in the data and each track has a length of 30 seconds. In this work, we use some sample audios to perform the steganography where we hide the text message in to the audio. For first experiment, we consider "voices.wav", "jazz.wav", "opera.wav", "pop.wav" and "rock.wav" as cover audio and "Hello world" as secret message.

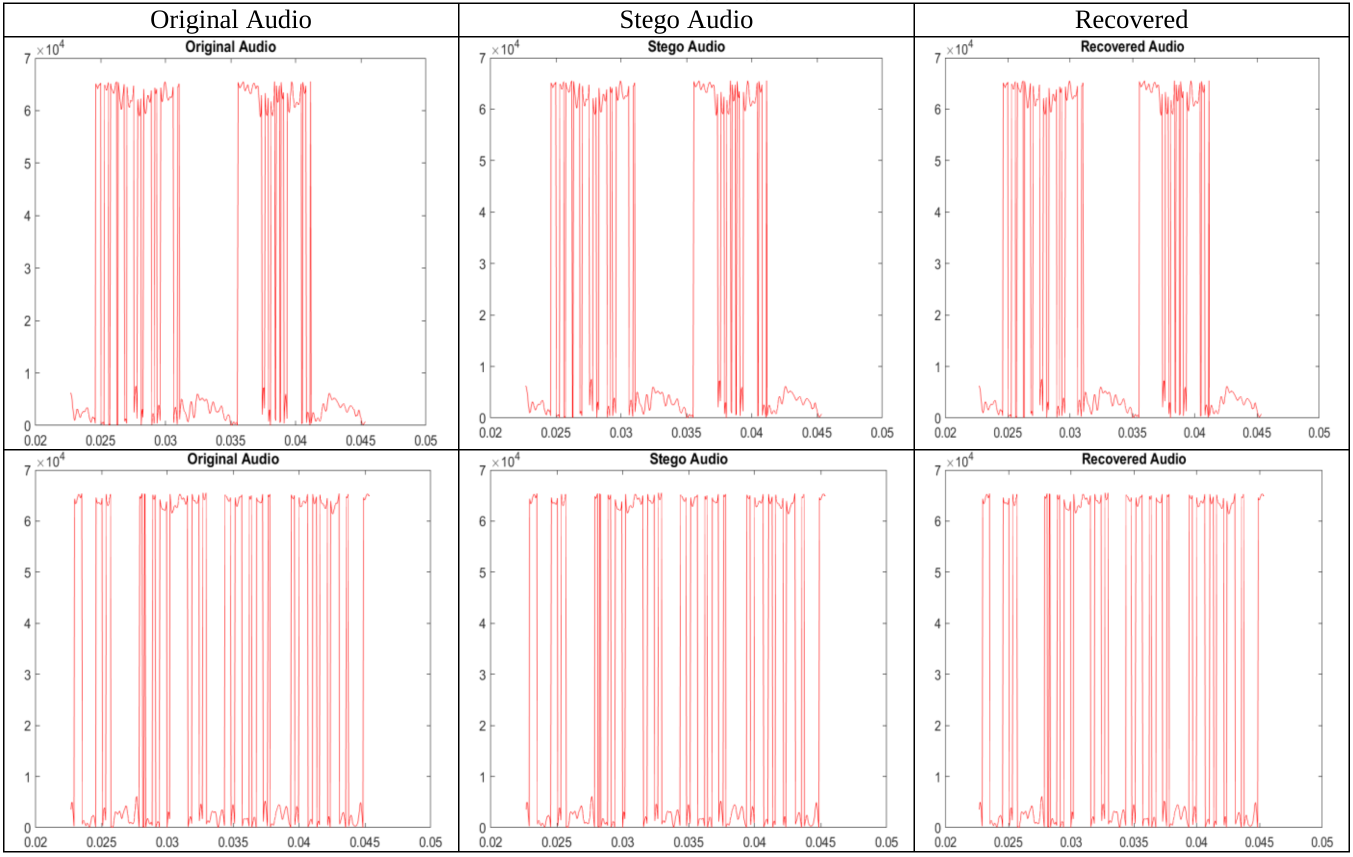

Figure 3: Experimental analysis of two cover audios

The above given figure shows the experimental analysis for two cover audios. First row of this experiment shows the Stego and recovery effect on the "voice.wav" signal and second row shows the experiment for "jazz.wav". Similarly, we have evaluated the performance for all audio and experiments reported successful recovery of the secrete message. The obtained PSNR values are compared with the state-of-art techniques as given in table 1.

Table 1: PSNR comparison for audio steganography

Audio Sample	LSB	Echo Hiding	Spread Spectrum	Wavelet
"voices.wav"	32.22	36.28	39.48	47.02
"jazz.wav"	36.95	42.30	43.65	46.85
"opera.wav"	38.21	41.20	42.09	44.68
"pop.wav"	35.29	39.66	40.29	45.28
"rock.wav"	37.22	39.89	42.33	49.28

C. Hiding Image Data in the Audio

In this section we present the experimental analysis to hide the image data into audio using proposed approach. In this experiment also, we consider that same dataset as discussed in previous experiment. The secret image is considered as "Lena" image. Below given figure shows the outcome of proposed approach.

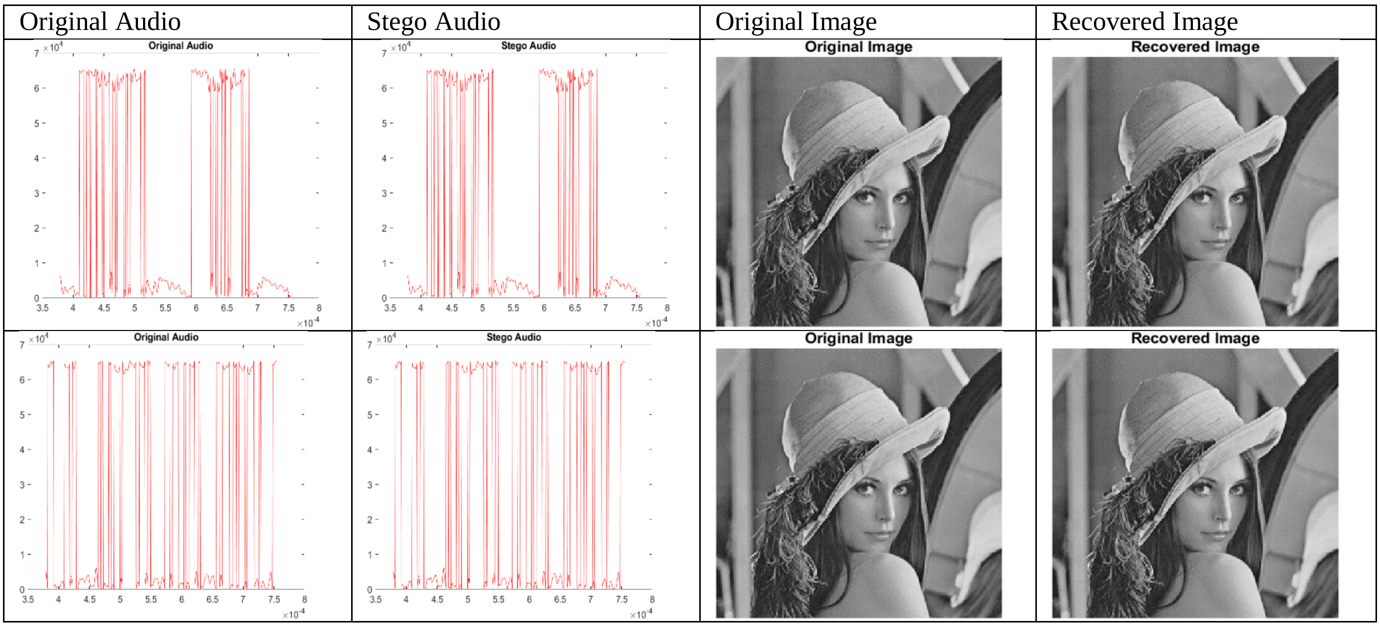

Figure 4: Proposed outcome

Similarly, we have considered different audio samples and evaluated the performance of proposed approach and compared it with the existing techniques. A comparative study in terms of PSNR, SSIM and hiding capacity is presented in table 2.

Table 2 PSNR comparison for audio steganography for 50% hiding capacity

Audio Sample	LSB	Echo Hiding	Spread Spectrum	Wavelet
"voices.wav"	36.22	39.22	42.36	45.21
"jazz.wav"	35.69	40.20	41.20	44.59
"opera.wav"	34.25	42.30	42.88	45.20
"pop.wav"	33.20	36.33	38.69	42.39
"rock.wav"	32.56	39.22	40.39	43.28

The table 2 shows the comparative performance for 50% hiding capacity for "Lena" image, similarly, we consider 100% hiding capacity and evaluated the performance and the comparative performance for this case is presented in table 3.

Table 3 PSNR comparison for audio steganography for 100% hiding capacity

Audio Sample	LSB	Echo Hiding	Spread Spectrum	Wavelet
"voices.wav"	30.25	33.25	36.28	41.28
"jazz.wav"	31.28	34.28	38.08	40.28
"opera.wav"	33.22	35.02	39.88	41.39
"pop.wav"	32.69	33.55	36.55	42.18
"rock.wav"	34.28	34.81	41.28	43.33

The comparative study shows that the proposed approach achieves better performance when compared with the state-of-art techniques of audio steganography.

V. CONCLUSION

In this article, we have focused on audio steganography and studied about the several existing techniques. The literature review shows that the performance of audio steganography techniques still can be improved by developing the robust algorithm for data embedding. Moreover, to improve the security, we incorporate data encryption and decryption process which provides additional security to the steganography module. The proposed approach is a combination of DCT coefficient and AES encryption to provide the data security. A comparative performance is carried out which shows that the proposed approach achieves better performance.

REFERENCES

1. Zong, T., Xiang, Y., &Natgunanathan, I. (2014). Histogram shape-based robust image watermarking method. 2014 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2014.6883430
2. Abood, M. H. (2017). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT). doi:10.1109/ntict.2017.7976154.
3. Jiang, N., Zhao, N., & Wang, L. (2016). LSB based quantum image steganography algorithm. International Journal of Theoretical Physics, 55(1), 107-123.
4. Hemalatha, S., Acharya, U. D., &Renuka, A. (2015). Wavelet transform based steganography technique to hide audio signals in image. Procedia Computer Science, 47, 272-281.
5. Yao, Y., Zhang, W., Yu, N., & Zhao, X. (2015). Defining embedding distortion for motion vector-based video steganography. Multimedia tools and Applications, 74(24), 11163-11186.
6. SiddalingeshBandi and H.S. Manjunatha Reddy, (2019) "SSAWS: Secure Scrambling and Adaptive Wavelet based Blind Image Steganography" Journal of Advanced Research in Dynamical and Control Systems, 11(7), 60-72.
7. Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014, May). An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. In 2014 International Conference on Informatics, Electronics & Vision (ICIEV) (pp. 1-6). IEEE.
8. Zhou, R. G., Hu, W., & Fan, P. (2017). Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Information Processing, 16(9), 212.
9. Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In 2014 International Conference on Computer Communication and Informatics (pp. 1-4). IEEE.
10. Begum, M. B., &Venkataramani, Y. (2012). LSB based audio steganography based on text compression. Procedia Engineering, 30, 703-710.

11. Antony, J., Sobin, C. C., &Sherly, A. P. (2012). Audio steganography in wavelet domain-A survey. International Journal of Computer Applications, 52(13).
12. Rekik, S., Guerchi, D., Selouani, S. A., &Hamam, H. (2012). Speech steganography using wavelet and Fourier transforms. EURASIP Journal on Audio, Speech, and Music Processing, 2012(1), 20.
13. Ghasemi, E., Shanbehzadeh, J., &Fassihi, N. (2012). High capacity image steganography based on genetic algorithm and wavelet transform. In Intelligent Control and Innovative Computing (pp. 395-404). Springer, Boston, MA.
14. Bhowal, K., Pal, A. J., Tomar, G. S., & Sarkar, P. P. (2010, November). Audio steganography using GA. In 2010 International Conference on Computational Intelligence and Communication Networks (pp. 449-453). IEEE.
15. Chadha, A., &Satam, N. (2013). An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution. arXiv preprint arXiv:1311.1083.
16. Nugraha, R. M. (2011, July). Implementation of direct sequence spread spectrum steganography on audio data. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics (pp. 1-6). IEEE.
17. Tayel, M., Gamal, A., &Shawky, H. (2016). A proposed implementation method of an audio steganography technique. 2016 18th International Conference on Advanced Communication Technology (ICACT). doi:10.1109/icact.2016.7423320.
18. Gambhir, A., &Khara, S. (2016, April). Integrating RSA cryptography & audio steganography. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 481-484). IEEE.
19. Kanhe, A., Aghila, G., Kiran, C. Y. S., Ramesh, C. H., Jadav, G., & Raj, M. G. (2015, August). Robust audio steganography based on advanced encryption standards in temporal domain. In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1449-1453). IEEE.
20. Mohajon, J., Ahammed, Z., &Talukder, K. H. (2018, December). An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key. In 2018 21st International Conference of Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.
21. Das, R., Mukherjee, D., Singh, R. S., Godara, S., & Kumar, S. (2017, August). DWTAS: A robust discrete wavelet transform approach towards audio steganography. In 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) (pp. 198-204). IEEE.
22. Yang, Z., Du, X., Tan, Y., Huang, Y., & Zhang, Y. J. (2018). AAG-Stega: Automatic Audio Generation-based Steganography. arXiv preprint arXiv:1809.03463.
23. Chen, B., Luo, W., & Li, H. (2017, June). Audio steganalysis with convolutional neural network. In Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security (pp. 85-90). ACM.
24. Mustafa, M., Mahmoud, M., Tagelsir, H., &Elshoush, I. (2018, September). A Novel Enhanced LSB Algorithm for High Secure Audio Steganography. In 2018 10th Computer Science and Electronic Engineering (CEEC) (pp. 125-130). IEEE.
25. Andrew B. Watson, “Image Compression Using the Discrete CosineTransform,” Mathematica Journal, 4(1), 1994.
26. http://marsyas.info/downloads/datasets.html

AUTHORS PROFILE

Siddalingesh Bandi, completed M.Tech in Digital Electronics from VTU. He is currently working in Department of ECE, Global Academy of Technology, Bengaluru. He is pursuing PhD. In the field of Image processing. His area of interest is digital security and computer vision.

Dr. Manjunatha Reddy HS, completed PhD in the domain of Image Processing from VTU, Belgaum. He is currently working as Professor and Head of ECE Dept.., Global Academy of Technology, Bengaluru. He has over 27 years of experience in the field of teaching and research.