Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 2507-2520

Climatizing the Detection of Secret Data and Sterling Data Transmission in Steganography

Alaknanda S. Patil[1], Dr. G. Sundari[2]

[1]Research Scholar, Department of ECE, Sathyabama Institute of science and technology, Chennai, India, patilalaknanda@yahoo.com

[2] Professor, Department of ECE, Sathyabama Institute of science and technology, Chennai, India, sundariece16@gmail.com

Abstract

In the last decades, information security has become a crucial issue, as the data innovation field is growing rapidly. In military applications, there is a possibility of breaking the security message. Hence there is a need for secrete message communication technology to prevent message breaching. Steganography is the process of embedding any secret message or information like image, text, audio, and video with the original cover file. Today, most secret information hiding systems use multimedia objects. This paper proposes two-stage multimedia steganography. In the first stage, the secrete message is embedded in the extracted audio from a multimedia video file. In the second stage, stego audio is again embedded with the video frames. The audio steganography uses the Least Significant Bit (LSB) substitution algorithm to embed the secrete audio, called stego audio. This is then embedded with the video frames. The processed video is transmitted to the receiver side. In the receiver section, the audio is extracted from the video stream. The 4-bit LSB decryption algorithm separates a secrete message from stego audio. The evaluating performance parameters of the proposed algorithm are PSNR, SSIM, and MSE metrics. This proposed algorithm is achieved promising results.

Keywords: Audio; Information Security; LSB; video Steganography.

Introduction

The speedy progress of the internet and e-communication has led to the introduction of advanced security technologies like cryptography, watermarking, and steganography [1]. Cryptography (Crypt means hidden, and Graphy means writing) is a method of defensive information through programming so that only authorized persons can read and process it. But the information on the message becomes distorted after cryptography. In watermarking, data are hidden behind the other image to convey some information such as copyright. The watermarking has many similarities with steganography in terms of data embedding. The

embedding watermark in an image is easy, but it is more difficult to extract the embedded image's secret information.

Steganography is a way to transmit confidential information via secure transmission. Steganography was derived from the Greek word 'steganos' meaning 'covered,' and 'graphy' meaning 'writing' [2]. Unlike cryptography, the message is unaltered in steganography. Using steganography, the secrete message can be embedded inside the other information and send to anyone without knowing the secret message's existence. Hiding audio data is less doubtful than communicating encrypted files [3]. Steganography's main purpose is to transmit knowledge quite secretly through other media such as image, audio or video. These mediums are called cover objects or carrier objects of the steganography. The secret message can be text, image, audio, or video. The hidden object is called a message object in steganography. The embedding message object and cover object forms the stego-object.

There are four types of steganography according to the cover object used is as shown in Figure1.

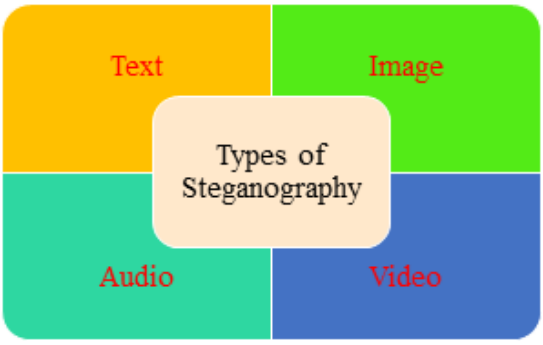


Figure 1. Types of Steganography

In this approach, initially, the audio from the video (.avi, .mpeg, or .ogg format) file is extracted, called original audio [4]. The secrete audio (of format .wav, .mp3, .aiff etc) is embedded into the original audio using Least Significant Bit (LSB) method. The stego audio is again embedded with the video file. This embedded video is transmitted over a secure communication channel. At the receiver side, stego audio is extracted from the embed video file and decrypts the secrete audio from the stego audio with the 4-bit LSB method. This method provides two-stage security.

This paper is assembled as follows; Module 2 gives an overview of multimedia steganography's current development with different algorithms with their pros and cons. Module 3 presents the architecture of the prospective methodology for the two-stage steganography perspective. Module 4 describes the experimental results with qualitative and quantitative analysis. Finally, the proposed method concludes in Module 5.

Literature Survey

There are various approaches implemented for steganography. Enhancement can be done after reviewing existing development in the steganography.

Moresh et al. [5] proposed a grouping of image encryption approach to give high security to the data/message to communicate over the communication channel. This method aims to provide high-level security, which is achieved using a fast and highly accurate Blowfish algorithm and LSB technique for encryption. The performance assessment of the system is done with PSNR and MSE.

S. M. Masud Karimet al. [6] introduce an LSB-based steganography approach where the confidential message is embedded in the cover image in random order with an encrypted key for advanced security. The secret keyword is converted into an ASCII stream and then into a binary stream. The binary bits stream then XORed with the binary bits of red color plane of an image. The PSNR value for Lena, Baboon, and peppers images is 53.7618, 53.7558, and 53.7869, respectively. The high PSNR value of the approach proved that the method is more accurate.

Nadeem et al. [7] presented the steganography approach using LSB. The bit inversion technique enhanced this approach to improve the stego-image quality. Instead of traditional sequential embedding, randomization in hiding the LSB data bits has been introduced in this approach. After embedding, stego image LSBs are inverted to reduce the number of changed LSBs. This process disperses the bit in the cover-image, making it difficult for an intruder to extract the original message. This approach shows good PSNR as well as image quality. The author suggested that this work can be extended by combining other bits of cover image pixels.

Murugan et al. [8] presented the steganography approach for jpeg and AVI format video by utilizing the swap method. This approach provides a simple algorithm with complex encryption. They suggested that UTF-32 encoding, combined with swapping algorithms, can improve steganography's strength with lower distortion and capacity. The experimental results show that the enhanced output of the AVI steganography without loss of data, quality, and size of the original video.

Hanafy et al. [9] present the steganography model using the cover video to cover sensitive data despite format. The approach in the framework is based on pixel-wise embedding hidden data in the video file. Before embedding the cover video, the hidden message is inserted in the block. Subsequently, the blocks are embedded in the random position using a pseudo-random sequence, which is mutually agreed-upon. Device efficiency was assessed using two performance measures, PSNR and MSE. Results indicate limited degradation for all data types and secret message sizes in the steganographic video format.

M. K. Khan et al. [10] proposed the LSB algorithm's data security approach, also called a Distributed LSB algorithm. In this approach, the data is hidden plane by plane in a non-sequential manner. The amount of the data to be hidden depends on the grayscale pixels' intensity. This makes the algorithm vigorous and adequate in data masking capacity and the cover image's degradation.

To merge audio and image steganography, Yugeshwari Kakde et al. [11] suggested an audio-video steganographic approach. This approach uses Singular Value Decomposition, Discrete Wavelet Transform, and random LSB audio steganography method to conceal the text in the audio.

Radha S. Phadte et al. [12] present the color image hybrid method by combining steganography and cryptography. The image hiding is done by randomized LSB-based method to form a stego image, the stego image being encrypted using chaotic theory. Investigational results show that the embedding ability of the color image is improved compared to conventional LSB process.

Xuehu Yan et al. [13] suggested two separate image sharing approaches based on least significant bits matching (LSBM). This approach aims to enhance the consistency and accessibility of shadow images. It is done by combining Boolean and MLE instead of error diffusion. The proposed schemes have many advantages, including fast generation and recovery computation, meaningful shadow images, alternative order of recovery of shadow images, pixel expansion and lossless recovery of hidden binary images.

Ahmed A. Abd El-Latif et al. [14] present a novel method to encode the secret binary shadow image. Includes random grids, ED and chaotic permutation. The confidential image is encrypted first with chaotic permutation, then exchanged by error diffusion with n halftone Shadow images RGs. Hidden images recovered from k or more shadow images. This scheme benefits from easy computation, alternative order Shadow images in recovery avoid complex codebook architecture and pixel expansion problem.

From the survey of current work, it is noticed that most of the techniques of steganography are developed for images. It is also observed that the LSB based approaches are simple, secure, and more effective with adequate data hiding capacity.

Prospective System

The prospective system consists of two modules: Encryption and Decryption. Each module is elaborated in detail below.

Encryption

The block diagram of the encryption section of the prospective multimedia steganography is as shown in Figure 2.

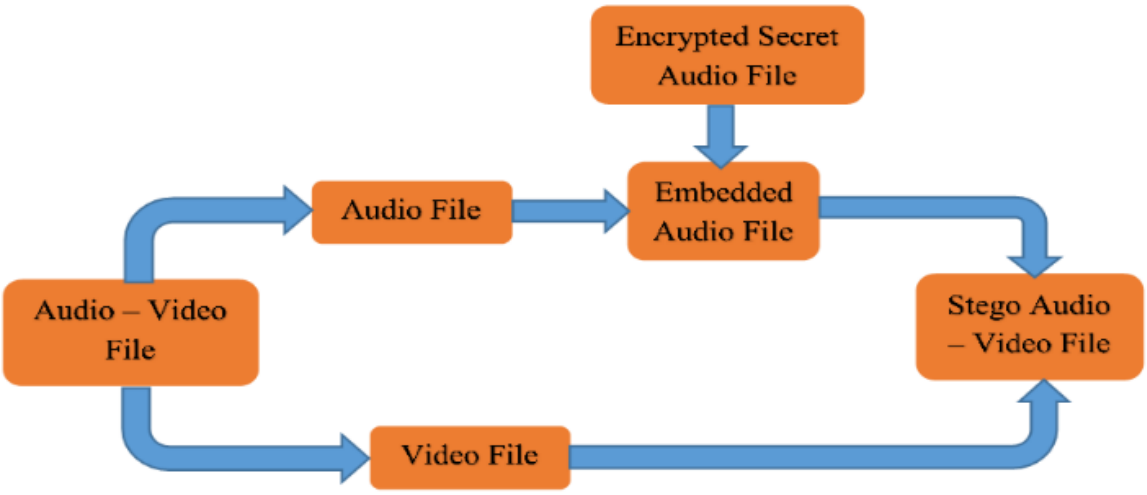


Figure 2. Block diagram for embedding

The audio-video file (.avi) is the input for the proposed system. Firstly, the audio from the video multimedia (audio-video) file is extracted. The secret audio in the .wav format is then embedded with the original audio file using the LSB method. The converted audio file is labeled a stego-audio file. The stego audio is again embedded into a video file and transmit over the secure communication channel. The LSB algorithm is explained in detail below.

Encryption Algorithm can be explained as:

1) Accepting the audio-video multimedia file
2) Extracting the original audio from audio-video multimedia file
3) Embedding secret audio in the extracted audio using the 4-bit LSB algorithm
4) Converting original audio and secret audio in the binary notation in length 'k' and secret audio of length 'm'.
5) If k>m, if yes, then execute the embedding process.
6) Embedding the binary code of secret audio (m bit) in the original audio (k-bit) in the LSB bit.
7) Repeat (c) till entire secret audio is embedded in the original audio to form stego-audio
8) Embedding the stego audio into video extracted in step (2)
9) The stego-audio-video file is then transmitted through multiple channels.

Decryption

The block diagram of the Decryption process is shown in Figure 3.

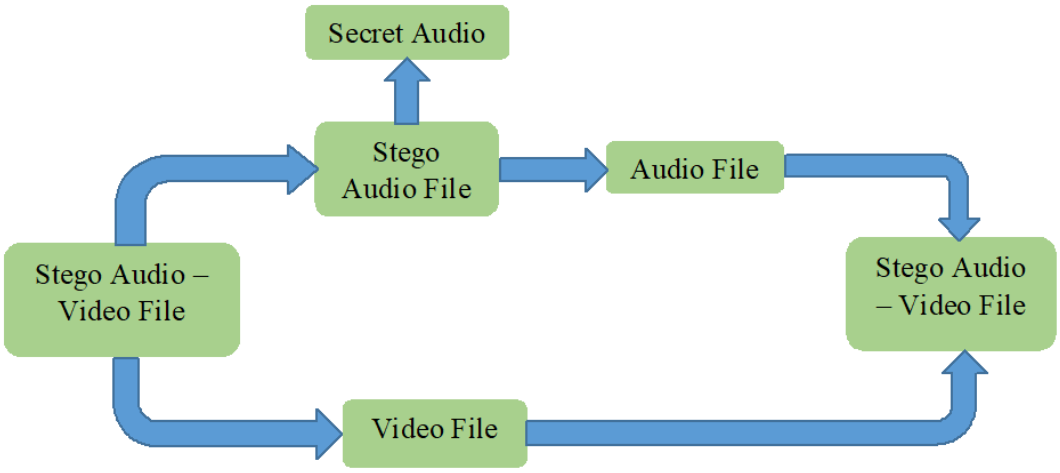


Figure 3. Block diagram for retrieval

The receiver section received the video transmitted by the transmitter. The stego audio is again extracted from the audio-video file. The crucial process of this algorithm is to extract the original confidential audio from stego-audio. It is executed with the LSB method. The decryption algorithm is as explained below.

Decryption Algorithm can be explained as:

1) Receiving the stego-audio-video multimedia file
2) Extracting the stego-audio from video multimedia file
3) Extracting secret audio from the stego-audio using Least Significant Bit (LSB)algorithm
4) Extracting original audio and secret audio in the binary notation in length 'k' and secret audio of length 'm'.
5) Convert the binary code of secret audio in the respective format
6) Extracting the binary code of secret audio (m bit) in the original audio (k-bit) in the LSB bit.
7) Repeat (c) till entire secret audio is extracted from the original audio to form stego-audio
8) Output secret audio

The flowchart of the prospective system is, as shown in Figure 4.

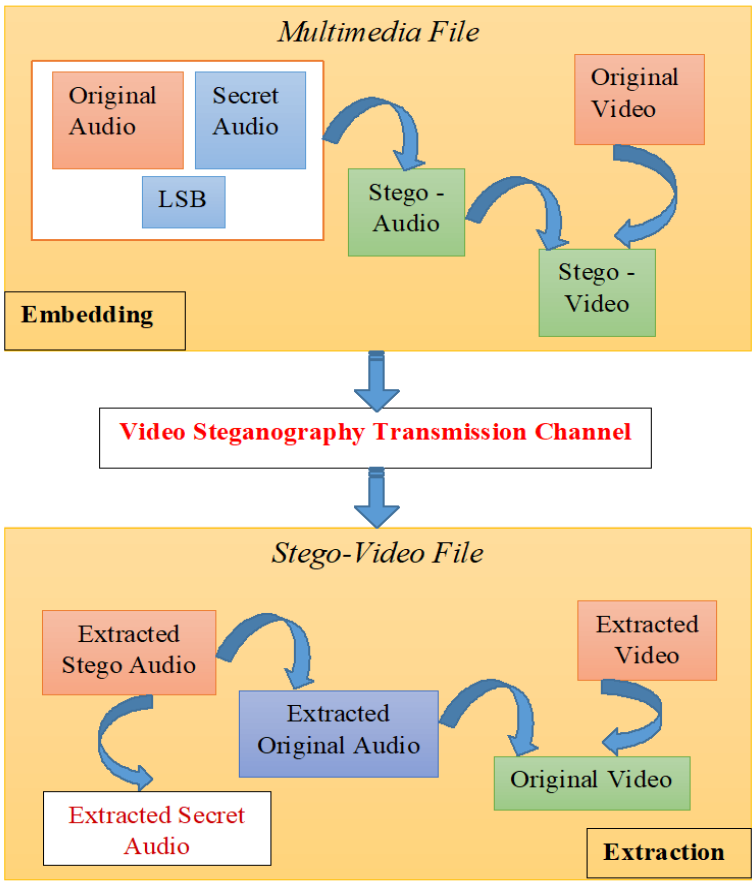


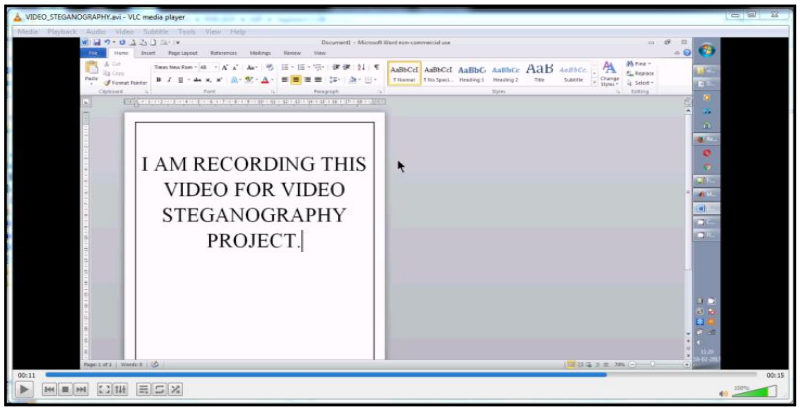
Figure 4. Flowchart of the prospective system

Result

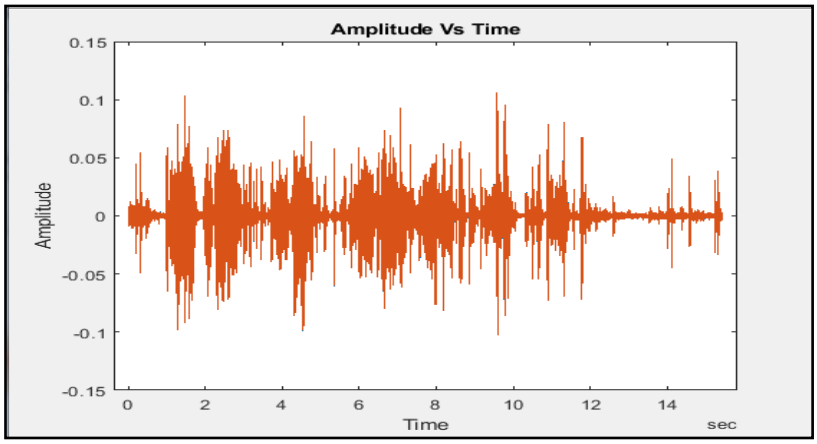
The prospective approach is implemented using MATLAB 2018aX64 bit version. The results of this method are explained using qualitative and quantitative analysis.

Qualitative Analysis

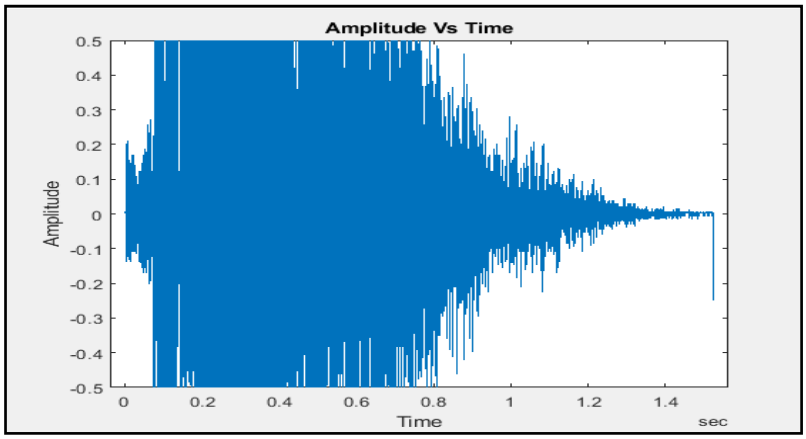
In this module, a visual analysis of the audio steganography is explained. Figure 5 (a-d) shows the qualitative analysis of the prospective system. The original audio-video multimedia file (VIDEO_STEGANOGRAPHY.avi) is the system's input, as shown in Figure 5(a). The audio file is extracted from the multimedia file called an original audio file or cover audio file. The waveform of the original audio file is, as shown in Figure 5(b). The secrete file (orig_secret.wav) is embedded in the original audio file using the LSB algorithm. The resultant audio file is labeled a stego-audio file. The secrete audio file's waveform is shown in Figure 5(c) and 5(d), respectively.


I AM RECORDING THIS
VIDEO FOR VIDEO
STEGANOGRAPHY
PROJECT.

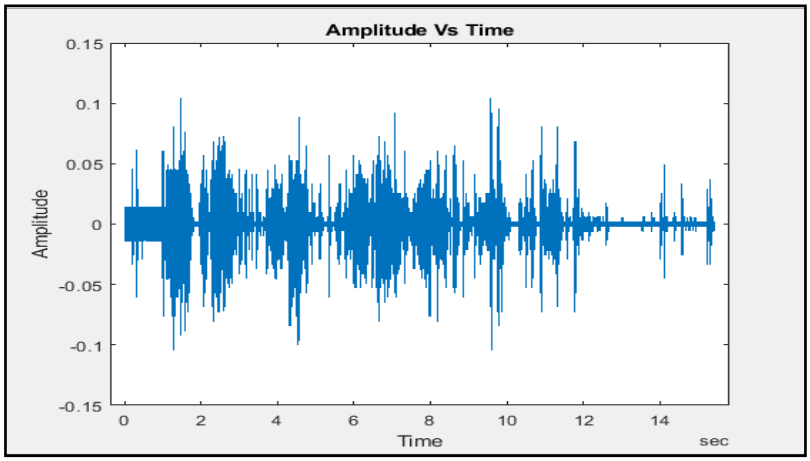
(a)


Amplitude Vs Time
Amplitude
Time
sec
0.15
0.1
0.05
0
-0.05
-0.1
-0.15
0
2
4
6
8
10
12
14

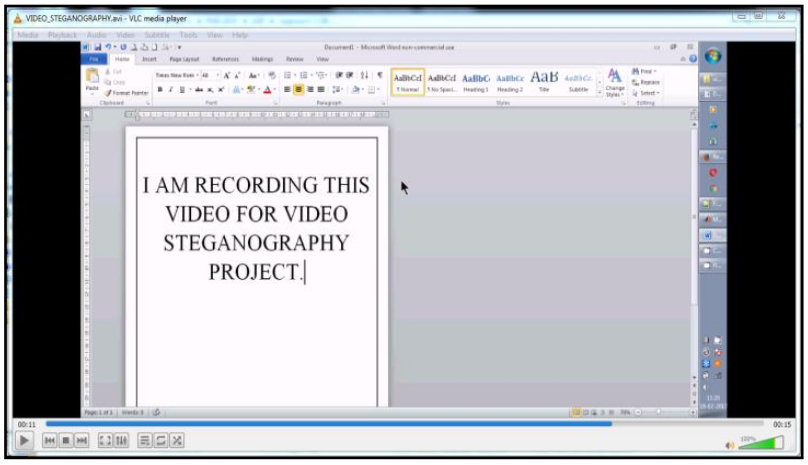
(b)


Amplitude Vs Time
Amplitude
Time
sec
0.5
0.4
0.3
0.2
0.1
0
-0.1
-0.2
-0.3
-0.4
-0.5
0
0.2
0.4
0.6
0.8
1
1.2
1.4

(c)



(d)

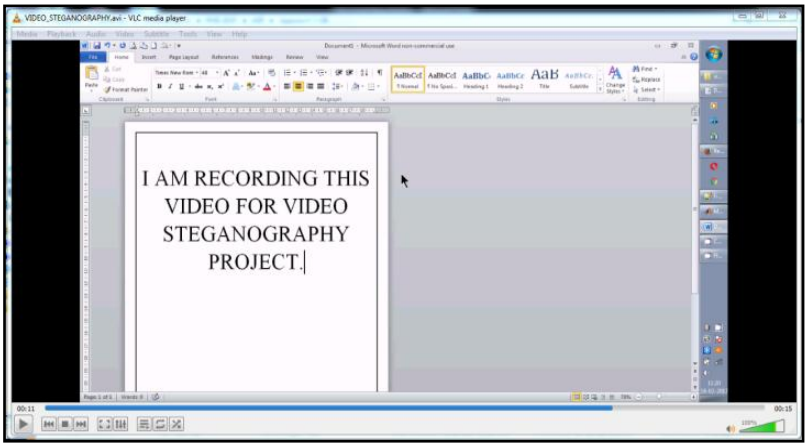


(e)

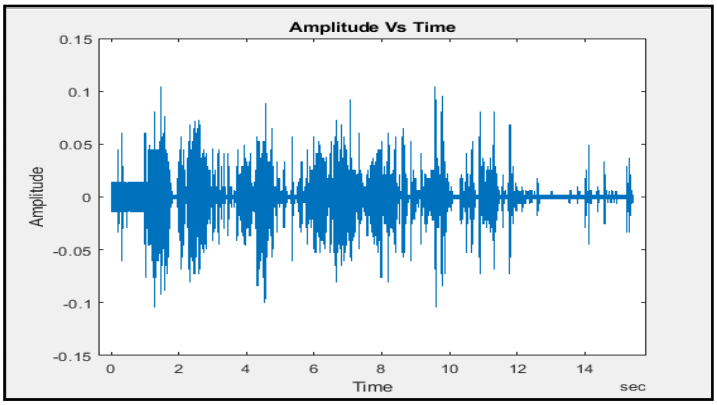
Figure 5. Qualitative analysis of the proposed audio-video steganography approach at the transmitter side (a) Input audio-video multimedia file sample (b) original or cover audio file waveform (c) secret audio waveform (d) stego audio waveform to form transmit (e) stegoaudio-video multimedia file sample

According to the graph of cover audio as shown in Figure 5(b) and the stego audio file as shown in Figure 5(d), it is noticed that the cover file and encrypted stego-audio files are visually as well as audibly same. There is no way to find out the existence of the secrete audio in the cover file. Finally, the stego audio is embedded in the original video file and transmitted over the communication channel.

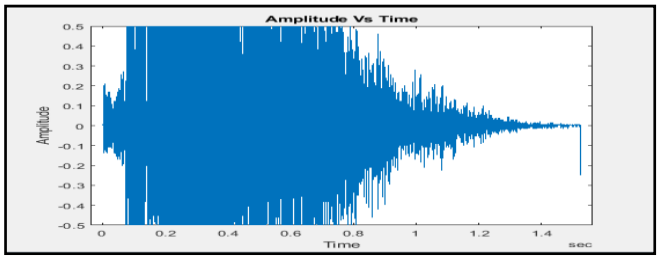
At the receiver side, the stego-audio-video file, as shown in Figure 6(a), the stego-audio is brought out from the stego-audio-video file, as shown in Figure 6(b). Further, the extraction of the secret audio from the stego-audio is performed. The extracted secrete audio and original cover audio are shown in Figure 6(c) and Figure 6(d).


I AM RECORDING THIS
VIDEO FOR VIDEO
STEGANOGRAPHY
PROJECT.

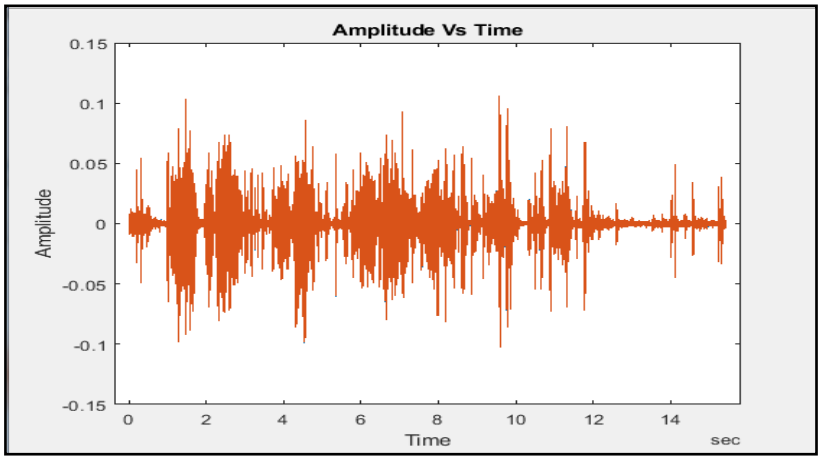
(a)


Amplitude Vs Time
Amplitude
Time
sec
0.15
0.1
0.05
0
-0.05
-0.1
-0.15
0
2
4
6
8
10
12
14

(b)


Amplitude Vs Time
Amplitude
Time
sec
0.5
0.4
0.3
0.2
0.1
0
-0.1
-0.2
-0.3
-0.4
-0.5
0
0.2
0.4
0.6
0.8
1
1.2
1.4

(c)



(d)

Figure 6. Qualitative analysis of the proposed audio-video steganography approach at the receiver side (a) stego-audio-video multimedia file (b) Extractedstego audio waveform (c) Extracted secret audio waveform (d) original or cover audio file waveform

From the qualitative analysis, it is noticed that the extracted cover waveform (as shown in Figure 6(b)) and original shield waveform (as shown in Figure 5(b)) is visually similar as well as audible same. In the same manner, the extracted secrete audio (as shown in Figure 6(c)) and original secrete audio (as shown in Figure 5(c)) are audibly and visually the same.

Quantitative Analysis

The Results of the systems are assessed using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), structural Similarity Index (SSIM), and Root Mean Square Error (RMSE). The detailed description of this parameter is described as follows.

- **MSE**

MSE is nothing but Mean Squared Error, and it is calculated by comparing the original audio file and extracted audio file with each of the bytes. We have the following equation to calculate the MSE value [15].

$$\text{MSE} = \frac{1}{[\text{N}\times\text{M}]^2}\sum_{\text{i}=1}^{\text{N}}\sum_{\text{j}=1}^{\text{M}}\left(\text{X}_{\text{ij}} - \text{Y}_{\text{ij}}\right)^2 (1)$$

Where $\text{N} \times \text{M}$ is the bits of the number in an audio sample, X_{ij} is the vector of observed value and Y_{ij} is the vector of the predicted value.

The MSE is the mean $\left(\frac{1}{[\text{N}\times\text{M}]^2}\sum_{\text{i}=1}^{\text{N}}\right)$ of the squares of the errors $\left(\text{X}_{\text{ij}} - \text{Y}_{\text{ij}}\right)^2$. It is a computable quantity for a particular sample; hence it is sample dependent.

- **PSNR**

PSNR is the specification of the audio file, which stands for Peak Signal to Noise Ratio. It is calculated between the original audio file and the extracted audio file. MSE and PSNR both are oppositely symmetrical to each other, and the PSNR can be computed with below equation [16].

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{I^2}{\mathrm{MSE}}\right] \quad (2)$$

Where Iis the maximum possible value of audio.

- **RMSE**

RMSE is a specification that stands for Root Means Square Error, computed as the square root of MSE.

$$\mathrm{RMSE} = \sqrt{\frac{1}{[N\times M]^2}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X_{ij} - Y_{ij}\right)^2} \quad (3)$$

- **SSIM**

SSIM is the estimation of the quality degradation because of the modification and loss in the data transmission. The SSIM is computed in this perspective is between the extracted audio and original audio [17].

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy}\,C + 2)}{(\mu_x + \mu_y + C_1)(\sigma_x + \sigma_y + C_2)} \quad (4)$$

where μ_x, μ_y stands for the local mean; σ_x, σ_y stands for the standard deviation and σ_{xy} stands for the cross-covariance of data x, y.

The mean, standard deviation, and cross variance is given by

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (5)$$

$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)^2\right)^{\frac{1}{2}} \quad (6)$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)\left(y_i - \mu_y\right) \quad (7)$$

The Qualitative analysis of the proposed audio-video steganography approach is tabulated in TABLE I.

Table 1

Quantitative Analysis

Audio Sample	MSE	RMSE	PSNR	SSIM
a.wav	0.0034	0.0585	24.6598	0.9495
cow.wav	0.0168	0.1297	17.7444	0.8601

Dog.wav	0.000017	0.0042	47.5863	0.9963
Duck.wav	0.00000590	0.0024	52.2901	0.9963
Lion.wav	0.00095467	0.0309	30.2015	0.9866

This system is tested on different audio samples. The qualitative and quantitative analysis of this system shows that the system is robust and accurate. From qualitative research, it is observed that the input and recovered audio samples are precisely the same audibly. The embedded video frame is visually similar to the original frame and challenging to identify for the intruder. The quantitative analysis shows that the PSNR and SSIM values of each tested sample are high. In contrast, the MSE and RMSE values are lower, which means the presented LSB algorithm is highly accurate for the steganography approach.

Conclusion and Future Scope

An audio-video steganography approach using the 4-bit Least Significant Bit (LSB) approach has been presented in this approach. The proposed method detects stego audio precisely and extracts the original audio and video frames accurately. On average, the technique embeds a secret audio bit per sample of cover audio. It is a way to implant the message in the digital hearing file. It allows a plenty of data to embed within the hearing file using a single LSB of the cover audio sample gives the capacity equals the sampling rate varies from 8 kbps to 44.1 kbps. This method could widely be used to modify LSB's except changing the audible attributes of the sound. The prospective system accomplished with improved performance in terms of PSNR and SSIM with lower MSE and RMSE. This method is safe, secure, and convenient for high secrecy communication between the two parties.

The system can be extended by considering more bits of cover audio samples that will provide the eight different bit pattern and improve the security. It can be implemented by using authorize user face embedding at video transmission and recognition techniques for authentic data receiver. The different embedding techniques can also be used as PVD method to increase the security.

References

1. Umair Khadam, Muhammad Munwar Iqbal, MeshrifAlruily, Mohammed A. Al Ghamdi, Muhammad Ramzan, and Sultan H. Almotiri, "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions," Wireless Communications and Mobile Computing, Volume 2020, Feb 2020, pp.1-15.
2. Sheelu, Babita Ahuja, "An Overview of Steganography," IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 1 (May. - Jun. 2013), pp. 15-19.
3. Rupali Patil, Prof. Dipak Pawar, "Secure Audio Steganography by LSB for Hiding Information," Novateur Publications, International Journal of Innovations in Engineering Research and Technology (IJIERT), June 2015, PP.1-6.

4. Vaishali Sarangpure, Prof. RoshaniTalmale, Prof. G. Rajesh babu, "Implementation on Hiding Data and Image in Audio- Video Using Anti Forensics Technique," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2015. pp. 8159-8164.
5. M. Mukhedkar, P. Powar and P. Gaikwad, "Secure non real time image encryption algorithm development using cryptography & steganography," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6
6. S. M. Masud Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka, 2011, pp. 286-291.
7. N. Akhtar, P. Johri and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," 5th International Conference and Computational Intelligence and Communication Networks, Mathura, 2013, pp. 385-390.

A. Murugan and R. Kavitha," Lossless Steganography on AVI File Using Swapping Algorithm, International Conference on Computational Intelligence and Multimedia Applications 2007, pp.83-88.

8. A. Hanafy, G. I. Salama and Y. Z. Mohasseb, "A secure covert communication model based on video steganography," MILCOM 2008, IEEE Military Communications Conference, San Diego, CA, 2008, pp. 1-6.
9. M. K. Khan, M. Naseem, I. M. Hussain, and A. Ajmal, "Distributed Least Significant Bit technique for data hiding in images," IEEE 14th International Multitopic Conference, Karachi, 2011, pp. 149-154.
10. Y. Kakde, P. Gonnade, and P. Dahiwale, "Audio-video steganography," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-6.
11. R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 230-235.
12. Yan X, Wang S, Abd El-Latif, "New approaches for efficient information hiding-based secret image sharing schemes" SIViP 9, 2015, 499–510.
13. Ahmed A. Abd El-Latif, Xuehu Yan, Li Li, Ning Wang, Jia-Liang Peng, XiamuNiu, "A new meaningful secret sharing scheme based on random grids, error diffusion, and chaotic encryption," Optics & Laser Technology, vol. 54, 2013, pp. 389-400.
14. Cemkasapbaşi, M., Elmasry, W. New "LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sadhana, 2018, pp. 43-68.
15. Jyoti, Er. Shilpa Jain, "Efficient Implementation of Watermarking to Reduce Bit Error Rate," International Journal of Engineering Sciences & Research Technology, 4. (9): September 2015, 281-290.
16. S. Hemalatha, U. Dinesh Acharya, A. Renuka, "Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image," Procedia Computer Science, vol 47, 2015, pp. 272-281.