International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.06,Issue.31
October-2017,
Pages:6069-6079

www.ijsetr.com

# MATLAB Implementation of Audio Steganography for Secure Data Transmission

**L. V. R. CHAITANYA PRASAD[1], VADDE SEETHA RAMA RAO[2]**

[1]Assistant Professor, Dept of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, TS, India,
E-mail: lvrchaitanya@sreenidhi.edu.in.

[2]Assistant Professor, Dept of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, TS, India,
E-mail: seetharamaraovadde@gmail.com.

**Abstract:** Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, [6],which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Audio Steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. It not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. The basic model of Audio Steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.[3,4] In Steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with Steganography methods will not. In other word, Steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical Steganography system relies on secrecy of the data encoding system.

**Keywords:** Steganography, Security, Information, Eaves Dropper.

## I. INTRODUCTION

As the need of security increases encryption needs a more secure method to hide the confidential matters. So Steganography is the supplementary to encryption. It is not the replacement of encryption. But Steganography along with encryption gives more security to data. The word STEGANOGRAPHY [1,6] is Greek word which means "concealed writing" from the Greek words stegnos meaning "covered or protected", and graphy meaning "writing". Steganography is the technique to hide the information in audio, image or video so that others can't identify that information is hidden into that media.. That media can be an audio, text, image or video. The information that to be hidden is called stego and the media in which the information is hidden is called host. The stego object can be text, image, audio or video. When the information is hidden into the audio then it is called Audio Steganography. This process is described as selection of random samples to be used for embedding which may introduce low power additive white Gaussian noise (AWGN).

### A. Steganography

It is a technique of hiding information.[3,4] Hiding necessary information by applying this Steganography approach without causing any affect to the information is possible. Once the information is hidden, it cannot be identified easily.

### B. Cryptography

It is a technique of converting plain text into cipher text. It is possible to encrypt highly secure data by applying cryptography approach. This approach helps to convert data in such a way that it can't be understood. Only the authorized user can decrypt the encrypted data. An effective Steganography scheme should posses the following desired characteristics for a secured transmission of message signal: Secrecy: Disabling a person to extract the covert data from the host medium without the prior knowledge of the proper secret password or key which is used in the extracting procedure. Imperceptibility: The medium after being embedded with the covert data should be indiscernible from the original medium. One should not be so suspicious of the existence of the covert data within the medium. High capacity: Highest length of the covert message that can be embedded should be as long as possible case can handle. Resistance: The covert data should survive even when the host medium has been manipulated, for example by some lossy compression scheme .Accurate extraction: The retrieval of the covert data from the medium should be accurate and reliable It is said that the Steganography approach was first practiced during the Greece Empire. History of ancient Greece specifies that they practices melting wax off wax tablets and then they hides the message in the underlying wood.

As the message was hidden under the wax, hence no one can have any suspect about the hidden message. Later on a microdot technique has been introduced for hiding secret messages. Microdots were used to permit the transfer of large amount of data and drawings invisibly. After that the concept of invisible ink came into existence and was much popular till world war-II. Certain drawbacks have been identified in such techniques and new hiding techniques has put forward time to time. Since ancient ages, encryption is the popular approach for transferring important data securely. An encryption technique has been evolved since the Babylonian Era, and was evolving continuously as they were used in the military and political aspects. Hieroglyphics is the oldest encryption technique. Later, Scytale Cipher technique was used which involves use of cylinder and a parchment strip so that the text can be written on that strip. Caesar Cipher was another encryption technique which involved shifting of characters to encrypt the data. Substitution Cipher and Enigma are the most popular encryption techniques in the history of encryption. Every time an encryption technique introduced, someone finds out a decryption method for that. Hence considering drawbacks in existing techniques, newer techniques have been introduced day by day.

A best secure technique which can implement audio data hiding using LSB algorithm. Thus we need an audio data hiding technique that can be used for a number of purposes other than covert communication or data storage, data tracing and finger printing. The sky is not the limit so is the same for development. Man is now decreasing his own boundaries to make every possible thought. So various operations described can be further modified as it is in the world of Information Technology. Different information hiding techniques are proposed to embed secret information. Among them we choose with audio file, Least Significant Bit (LSB) coding method as it is the simplest way to embed secret data in a digital audio file by replacing the least significant bit of audio file with a digital converted secret message. Hence LSB technique allows huge amount of secret data to be encoded into an audio file. Steps to hide secret information using LSB are:

- Conversion of the audio file into bit stream that is digitalization.
- Convert each and every character in the secret message into digital bits.
- Replace every LSB bit of audio file with every LSB bit of character in the secret message.

This method which is proposed thus provides great security and it is the best method for hiding the secret data from hackers and sent to the destination in an undetectable manner. This proposed system ensures that the quality of the file is not changed even after such encoding and it is made suitable for all types of audio file formats. Steganography is the science of hiding secret data in a cover file so that only sender and receiver can be able to detect the existence of the secret data. The main aim of our Steganography technique is to communicate with full security with a completely undetectable manner and thus avoiding drawing suspicion to any intermediaries present transmission for a hidden data. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a Steganography method makes intermediaries to doubt suspicion that there is a some information in a carrier medium, then the method has failed. This technique Audio Steganography consists of Carrier signal(Audio file), Message(text) and Password(key). Carrier is the cover-file, which conceals the secret information. Basically, the technique for audio Steganography is shown in fig.1 below. Message is the data type which the sender wishes to remain it to be confidential. Message may be a plain text, image, audio or any type of file. Password is the key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file or else they cannot retrieve the file. The cover-file with the secret information is known as a stego-object in this audio Steganography technique.

For hiding data into a medium the requirements are:

- The cover audio signal(C) that will holds the hidden data
- The secret message data (M), may be plain text, cipher text or any other type of data
- The stego or covered technique(Fe) and its inverse(Fe-1)
- An optional stego-password (K) is used to hide and during retrival of the message.

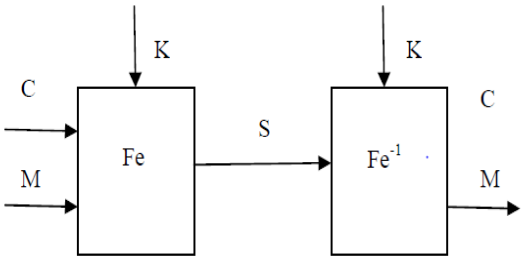


**Fig.1.The Steganography operation.**

### C. Related Work

The primary tool used in the research of Steganography and watermarking is the Internet. The first objective was to understand the various terminologies related to the field. The following points can be attributed to the renaissance of Steganography:

- Government ban on digital cryptography. Individuals and companies who seek confidentiality look to Steganography as an important complementary since combining cryptography and Steganography can help in avoiding suspicion and protect privacy.
- The increased need for protecting intellectual property rights by digital content owners, using efficient watermarking.
- The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, Steganography software is becoming effective in hiding information in image, audio or text files.

### D. Existing Approach

In an equal interval of time, several concepts has been brought forward in order to provide an optimum solution to ensure security, privacy and authentication of the information while carrying out data transfer over network. These concepts involved certain data hiding and data encryption techniques. Considering security and privacy as a major concern, initially the vital data is to be sent after hiding it behind some digital media such as audio, video, images etc. This technique was quite popular, later on hackers found a way out, now it is possible to extract the hidden data from the digital media. With the advent in the field of cryptography, encryption becomes a gossiping fact among all. Afterwards encryption was used for the data transfer. This technique was better option among other but, only encryption or data hiding cannot provide full assurance towards the data. Recently, the concept of double layer protection technique has been put forward to fill this gap. The double layer protection technique is simply cryptography cum Steganography approach which can definitely provide efficient security mechanism for transferring data among communicating parties. The main disadvantage of using the existing methods is that there is an introduction of noise and decrease in robustness of the system. The human ear is highly sensitive to noise and can detect even small disturbances introduced due to Steganography using the existing methods. In order to reduce noise introduction to a great extent we propose the following method of LSB modification.

### E. Modified Approach

The main goal of Steganography is to communicate securely in a completely undetectable manner. Considering security to be a major aspect, the most suggested implementation is of a double layer protection approach will helps user to send vital data without having any worry. We suggest an approach that constitutes both cryptography and Steganography. We are considering a situation where user wants to share some sort of vital information with another party located over some distance. The medium of communication may be wired or wireless. Now the information that is to be sent should be delivered securely. So in order to achieve this, we are suggesting a system that will implement the double layer protection approach.

### F. Proposed Method

The method we propose is to hide encrypted text in cover audio signal. This method consists of two parts – embedding (or encoding) at the transmitter end and extraction at the receiver end. In embedding phase, encrypted text is hidden inside the cover audio signal. There is no distortion in the cover audio by hiding the secret data since only the LSB is being modified while keeping all other parameters unaltered. In extraction phase, the secret text is retrieved from the stego-object that is the audio file containing the secret data. Secret data here is text, which can be encrypted before embedding into the audio. These transformed values of text are then hidden in LSB's of audio samples. This proposed method provides greater security and it is efficient method for hiding the secret data from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

## II. LSB TECHNIQUE IMPLEMENTATION

There have been many techniques for hiding information [3,5] or messages in audio in such a manner that the alterations made to the audio file are perceptually in dissemble.

### A. LSB Coding [2]

A very popular method is the LSB (Least Significant Bit) [2]modification algorithm in which the least significant bit in some bytes of the cover file is replaced to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation. In computing, the least significant bit (LSB) is the bit position (right most bit) in a binary integer giving the units value.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |

**Fig.2.Binary representation of decimal 147.**

The binary representation of decimal 147, with the LSB highlighted is shown above Fig.2. The MSB (1) in the 8-bit binary representation of the number represents a value of 128 decimal and the LSB (1) represents a value of 1. For example, to hide the letter "Z" (ASCII code 90, which is **01011010**) inside eight bytes of a cover, the LSB of each byte could be modified like this:

0 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1
0 0 0 0 0 0 1 0
1 0 0 0 1 0 1 1
1 1 0 1 0 0 1 1
1 0 0 1 1 0 1 0
0 1 0 1 0 0 1 1
1 0 0 1 0 0 1 0

During decoding the application reads the eight Least Significant Bits of the cover file bytes to recreate the hidden byte—that is 01011010—the letter "Z. In this method, each and every bit of the message byte is hidden into a cover byte. There is a fifty percent chance that the bit being replaced is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation. Fig.3 below illustrates how the message 'HAI' is encoded in a 16-bit sample of the cover file (audio file) using the LSB method. The secret information 'HAI' and the audio file are converted into bit streams and the least significant column of the audio file is replaced by the bit stream of secret information 'HAI'.

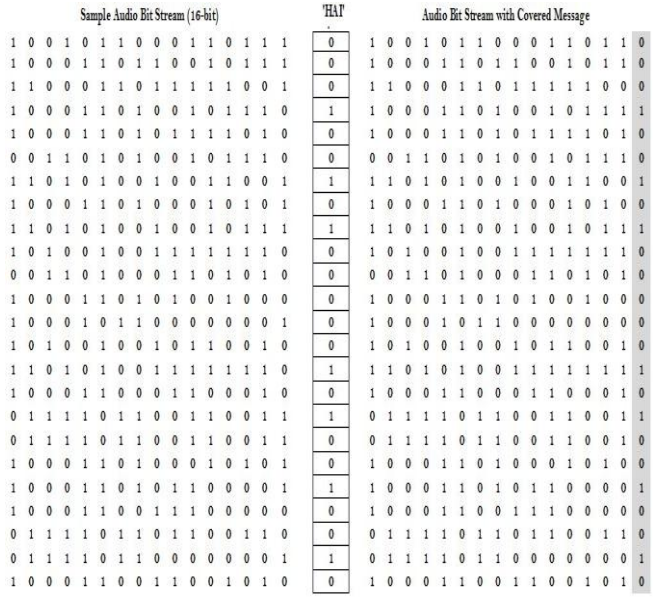


**Fig.3.LSB coding example.**

Steganography can also be implemented using the other approaches as given below, but LSB technique is the best way with minimum BER.

### B. Parity Coding

Parity coding is one of the robust audio Steganography techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more choice in encoding the secret bit. The parity coding procedure can be shown in Fig.4:

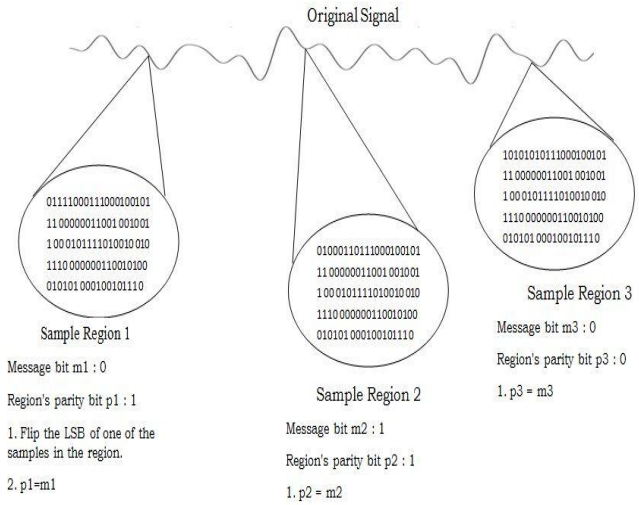


**Fig.4.Parity coding.**

### C. Phase Coding

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. Phase coding is one of the most effective coding methods in terms of signal to noise ratio. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved. This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Phase coding is explained in the following procedure:

- The original sound signal is divided into smaller segments such that length of each segment is same as the size of the message to be encoded.
- Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
- A phase difference between adjacent segments is calculated.
- Using the new phase of the first segment a new phase matrix is created while preserving the original phase differences.
- The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.

The receiver must know the segment length to extract the secret information from the sound file as shown in Fig.5. Then the receiver can use the DFT to get the phases and extract the secret.

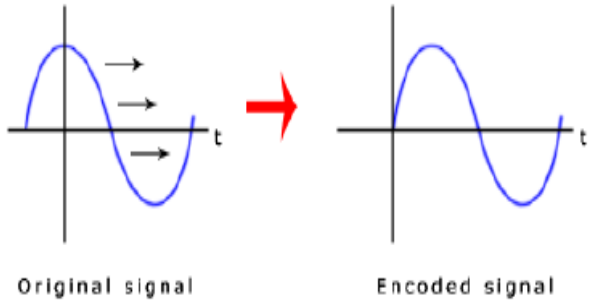


**Fig.5. Phase coding.**

### D. Spread Spectrum

In audio Steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal as shown in Fig.6. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission. The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding, phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. However, the Spread Spectrum method has one main

disadvantage that it can introduce noise into a sound file. The steps followed in Spread Spectrum are as follows:

- The secret message is encrypted using a symmetric key, k1.
- The encrypted message is encoded using a low rate error-correcting code. This step increases the overall robustness of the system.
- The encoded message is then modulated using a pseudo-random signal that was generated using a second symmetric key, k2.
- The resulting random signal that contains the message is interleaved with the cover-signal.
- The final signal is quantized to create a new digital audio file that contains the message.
- This process is reversed for message extraction.

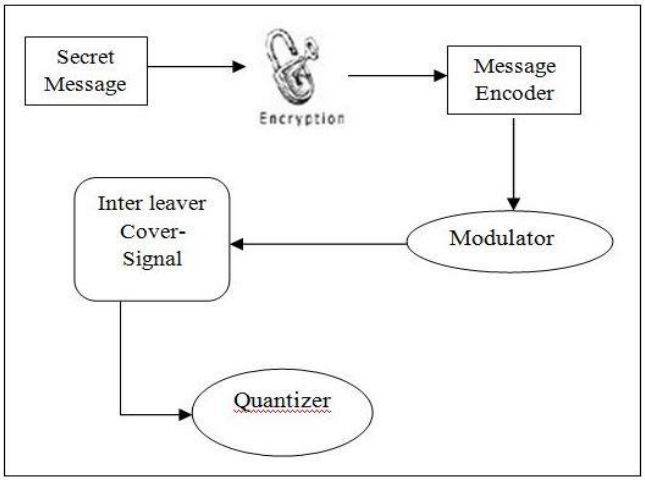


**Fig.6. Spread Spectrum (SS).**

### E. Echo Hiding

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal Echo Hiding is shown in Fig.7.

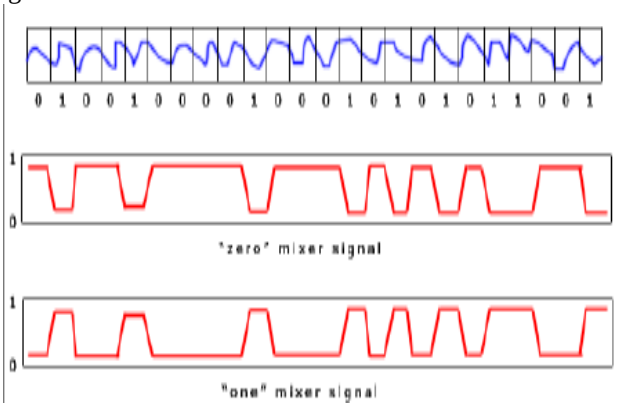


**Fig.7.Echo hiding.**

## III. IMPLEMENTATION DESIGN FOR AUDIO STEGANOGRAPHY

### A. Block Diagram

The block diagram depicting the proposed work is as shown in Fig.8: Here, the secret message file and the cover audio file are opened and sent into the Steganography encoder. The result of the encoder is the cover audio file with the LSBs of all its bytes modified using the message bits. This file known as the Stego-object is sent to the receiver through a communication channel.At the receiver end, the stego object is processed only if the exact key that was used at the encoder is given. Once the key is given by the user, the decoder extracts the message from the stego-object and gives back the secret message file with a minimum BER.

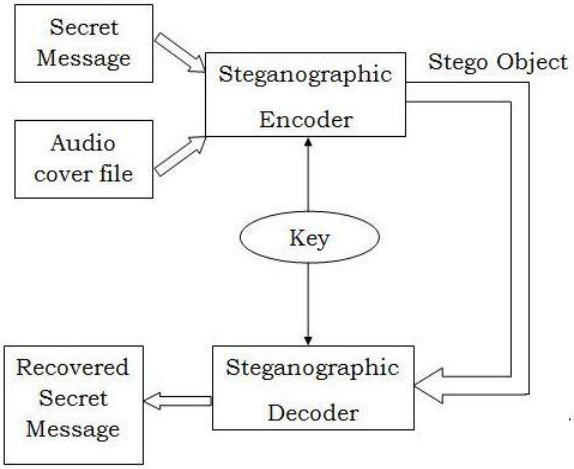


**Fig.8.Block Diagram.**

### B. Procedure

The algorithm used to implement the proposed method can be divided into four parts as mentioned below. The first two parts give the steps to embed the message into the cover audio file and the next two parts give the steps to detect the message from the received signal.

### C. Compatibility Check Algorithm

- Open the message file containing the secret text to be transmitted.
- Find the length of the message (number of bytes) and store it as L.
- Open the audio cover file.
- Convert the samples obtained into bytes of binary data and store them in an array.
- Find the length of the audio signal(number of bytes) and store it as N.
- Choose a key for Steganography of length K.
- Check if the length of message and key together is less than or equal to one-eighth of the audio length.
- If the above condition is satisfied, print a suitable message and start the Steganography process.
- If the above condition is not satisfied, print the suitable message and stop the execution.

The flowchart corresponding to the above compatibility check is shown below Fig.9. The lengths of message and cover files are to be chosen carefully to avoid errors.

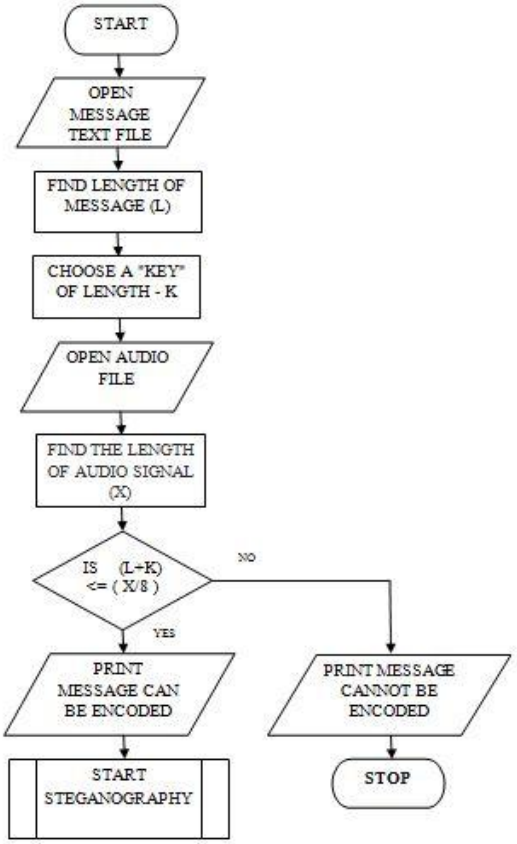


**Fig.9.Compatibility check Flowchart.**

**Encoding Algorithm:**

- Convert the chosen key into binary format.
- Extract one byte of the audio file at a time.
- Clear the LSB of the extracted byte.
- Choose one bit of the key and place it in the LSB of the extracted audio byte. Store the modified byte into another array.
- Continue the above steps(2-4) till all the bits of the key are embedded into the audio samples.
- Extract one byte of the message at a time.
- Repeat the steps from 2-4 for all the bits of the extracted message byte.
- Repeat steps 6-7 for all the message bytes.
- Copy all the remaining (unaltered) bytes of the audio signal array into the new array to avoid any modifications in the length of the audio signal.
- Convert the newly generated array of binary bytes into samples of the audio signal using the initial sampling frequency.
- Plot the initial audio samples and the newly generated audio samples in wave format. It can be observed that the two signal appear almost identical.
- In order to observe the difference created in the audio signal due to the message embedding, find the difference of the samples of the initial and newly generated arrays and store it in another array (difference array).
- Convert the binary difference array into samples of audio data using the same sampling frequency used above.
- Plot the difference of the two arrays. It can be observed that there are very minimal differences between the two signals.
- Generate the audio signal from the above samples and transmit it through the communication channel.

The complete encoding procedure can be depicted in a flowchart as shown in Fig.10:

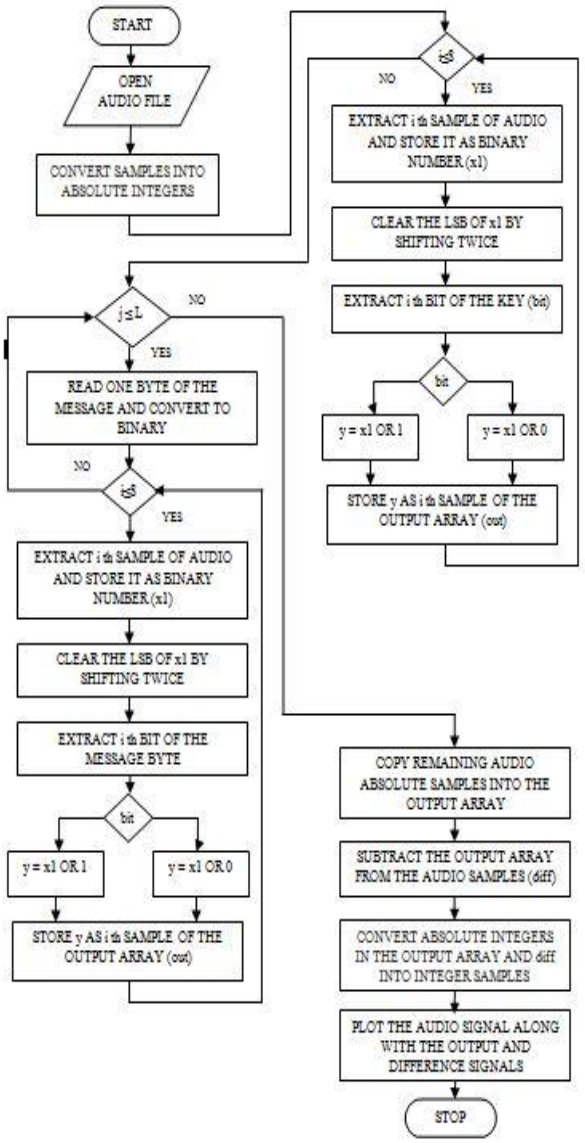


**Fig.10. flowchart.**

**Algorithm To Check Correctness Of The Key:**

- Prompt the user to enter a key.
- Extract eight bytes of the received signal and convert them into binary values.

- Extract LSBs of all the eight bytes and form the corresponding message byte which is the key used while encoding.
- Compare the extracted key with the key entered by the user.
- If the correct key is entered, display a suitable message and go to decoding algorithm.
- If the entered key is wrong, display a suitable message and abort the reception process.

The above algorithm can be depicted as shown in Fig.11:

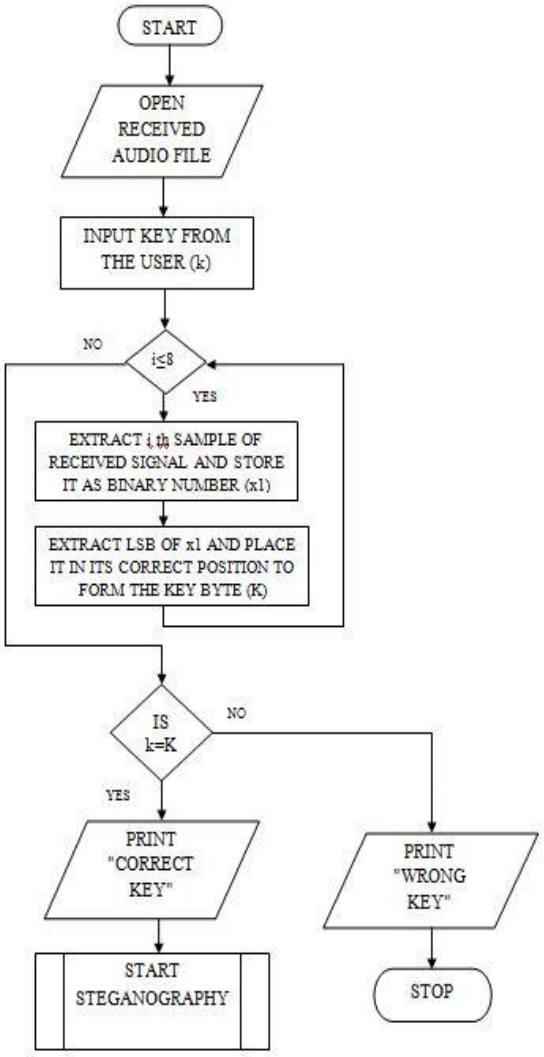


**Fig.11.**

**Decoding Algorithm:**

- Receive the stego-object from the communication channel.
- Convert the signal into samples using the sampling frequency.
- Convert the samples into absolute integers and subsequently into an array binary bytes.
- Send the first eight bytes to the checking algorithm (the above algorithm 6.2.2)and receive a control signal.
- If the control signal is positive, extract bytes of the stego array one at a time.
- Extract the LSB of each byte.
- Form eight bit groups of the extracted LSBs.
- Store such eight groups of bits in another array.
- Convert the newly generated array into characters and store it into a text file.

The above algorithm can be depicted as shown in Fig.12:

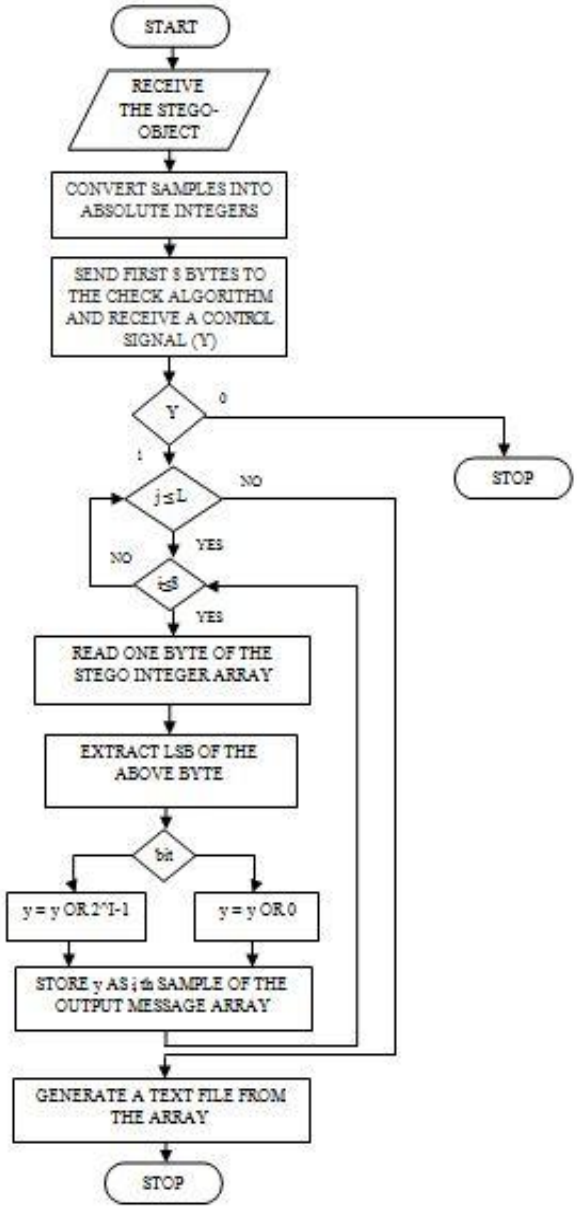


**Fig.12.**

## IV. SIMULATION RESULTS

In this project, the message chosen is a paragraph of text stored in a ".txt" file and the cover audio is an audio signal stored in a ".wav" file. The two files are opened through MATLAB using the "fopen" function. The message file is shown in the following fig.13:

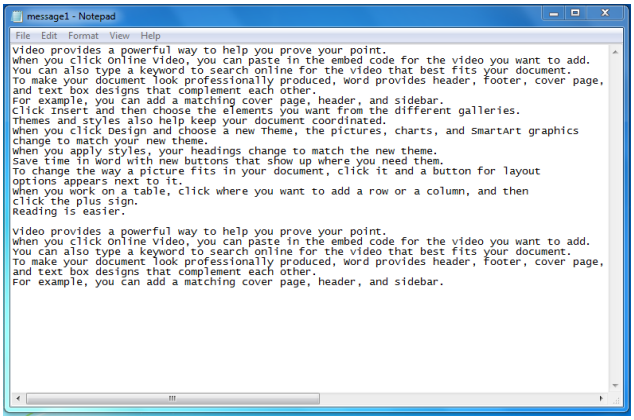


**Fig.13. Secret Message.**

The first step of the proposed method of Audio Steganography involves checking the lengths of the secret message and the cover audio file. The lengths need to satisfy certain conditions to be compatible with each other. The output generated after measuring and comparing the lengths is as following Fig.14:

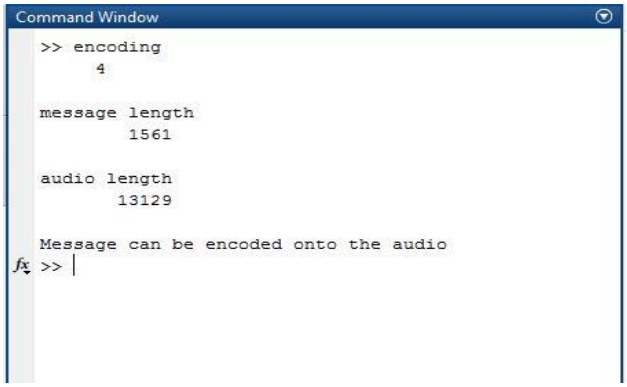


**Fig.14.Output when message and audio lengths are compatible.**

Once the "Message can be encoded onto the audio" message is displayed, the input audio file is sampled to obtain an array of sample values. The sample values are converted into integers and subsequently into absolute values while preserving the sign status in another array. The first few values of the samples before and after conversion into integers are shown in the following figs.15 to 18.

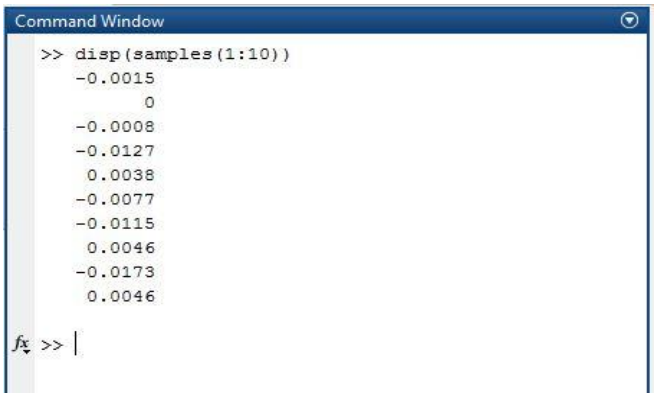


**Fig.15.First 10 samples of the considered audio signal.**

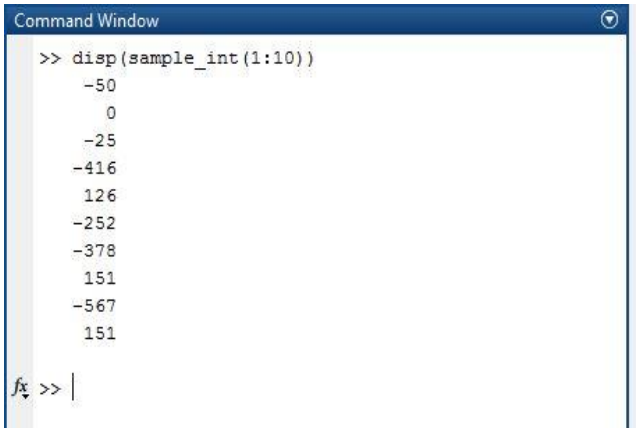


**Fig.16.First 10 samples of the audio signal after converting into integers.**

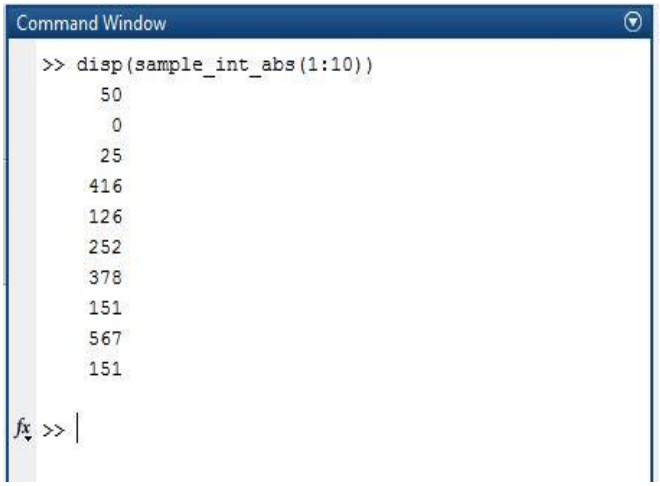


**Fig.17. Absolute values of the first 10 integer samples of the audio.**

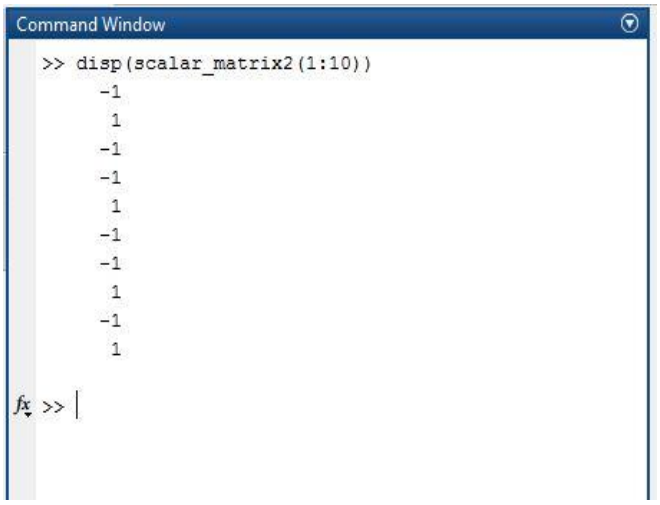


**Fig.18.Signs of the first 10 integer samples of the audio signal stored for reconstruction.**

In case the lengths of the message and the audio cover do not satisfy the required conditions, the execution of the code is halted with a suitable message. Such a situation is shown in the following fig.19.

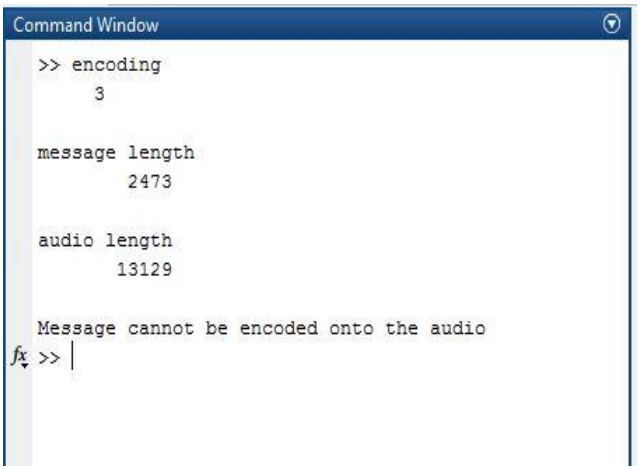


**Fig.19.**

After converting the samples array into absolute values array, the audio signal is plotted with the obtained samples. The obtained plot is as shown below Fig.20.

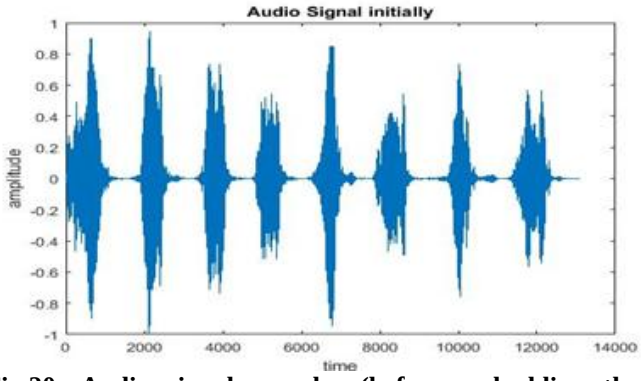


**Fig.20. Audio signal samples (before embedding the message) plotted against time.**

Embedding the message bytes onto the audio bytes is done as explained in the previous section. The process of embedding the first message byte into the audio samples is shown in the following fig.21.

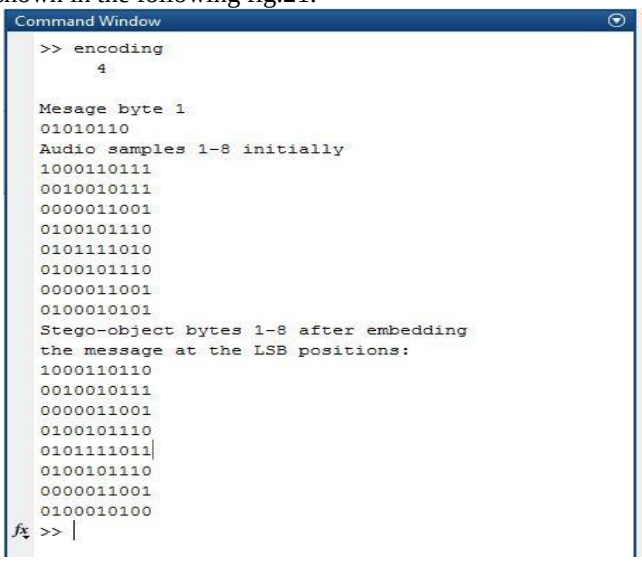


**Fig.21.Process of embedding message into audio samples shown for 1 message byte.**

After the embedding is done, the absolute samples are converted back into audio signal samples using the procedure opposite to that used in the beginning. The final audio samples obtained are plotted as follows shown in Fig.22..

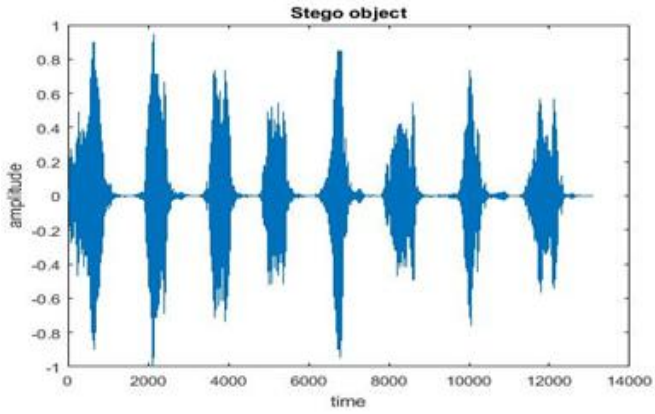


**Fig.22. Stego signal samples (after embedding the message) plotted against time.**

The difference between the audio signals before and after Steganography is calculated and is plotted. The following plot shows Fig.23 that there is hardly any difference between the two signals thus making this procedure highly feasible as the BER is very minimal.

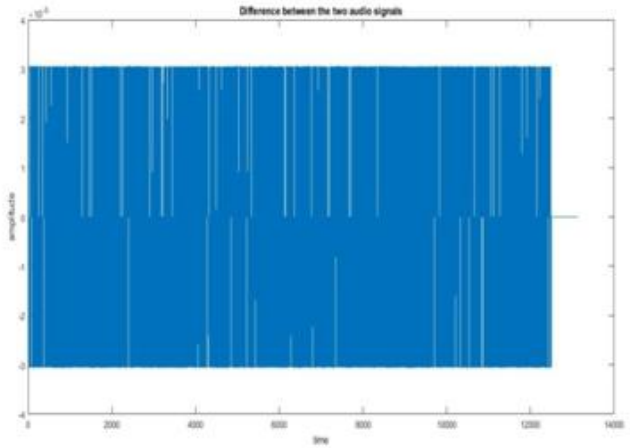


**Fig.23. Difference between the audio signals before and after steganography.**

Thus, the process of embedding a text message into a cover audio file has been accomplished. The obtained output file known as the "Stego-Object" is transmitted along a communication channel to the intended receiver. Even if an eavesdropper gets his hands on the stego-object, he will not be able to recognize the presence of a message in the audio. At the receiving end, the user is asked to enter the "Key" to ensure that he is the intended receiver. Upon receiving the entered key, the program checks the first eight incoming bytes and extracts the LSBs to form a byte. This newly formed byte was the key used during encoding. In case the keys match, the message can be recovered by the receiver. Such a case is shown below Figs.24 and 25.

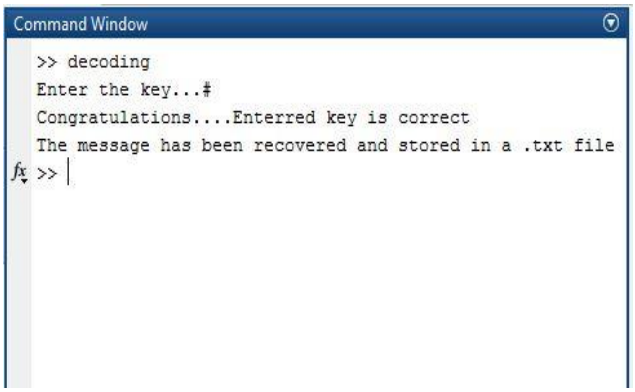


**Fig.24. Output When Entered Key Is Correct.**

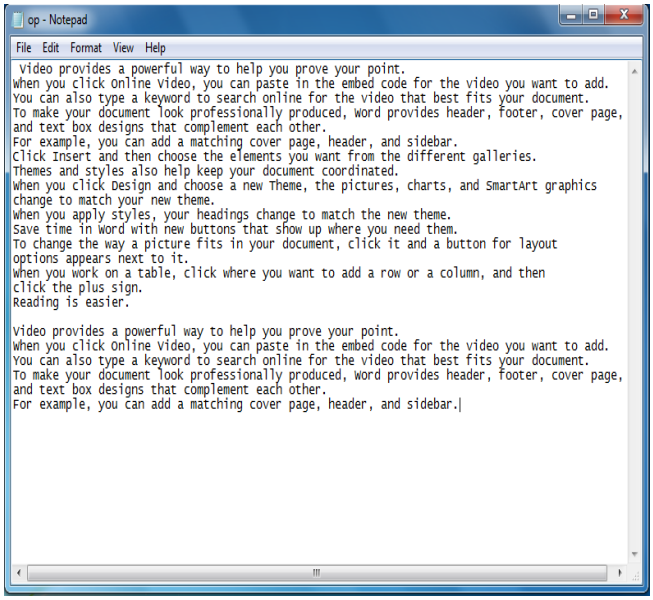


**Fig.25. Output Text File Obtained After Decoding the Stego-Object.**

If the entered key is wrong, a suitable message is displayed and the execution stops. the output shown in Fig.26 in this case is as follows

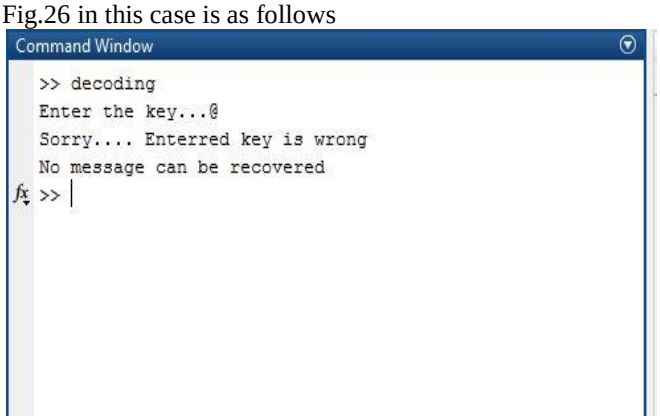


**Fig.26. Output When Entered Key is wrong.**

## V. CONCLUSION AND FUTURE SCOPE

### A. Advantages and Disadvantages

The main advantages are: It is easy to combine with existing cryptography techniques. Hiding of Higher data rates can be easily achieved. As emphasis placed on the areas of copyright protection, privacy protection, and surveillance increase. Limitations such as: Complexity increases for large Audio files.

### B. Applications

Audio data hiding is to be used whenever you want prevent unintended receivers from becoming aware of the existence of a secret message.

### C. Conclusion And Future Scope

Thus we can conclude that audio data hiding techniques can be used for a number of purposes other than information tracing, finger printing, tamper detection etc. Both Steganography and cryptography have certain limitations, yet these are the most familiar aspects of security and privacy. Either Steganography or cryptography cannot provide maximum trust towards security separately. Both combined Steganography and cryptography forms a double layer protection approach which can yield better secure solution for information sharing. As the sky is not limit so is not for the development. Man is now advancing his own boundaries to make every thought or idea possible. So these operations mentioned above can be further modified as it is the world of Information Technology. This method of data hiding can be further extended to hiding audio, video, images etc in the audio carrier or cover signal. A combination of encryption and Steganography can lead to high security of data while transmission. Other methods of audio Steganography like parity coding, phase coding, spread spectrum and echo hiding can be used either singly or as a combination depending on the requirement for different applications.

## VI. REFERENCES

[1] M. K. S. V. Shrivastav, "An Effective Approach to Information Hiding for Secure Message Transmission," International Journal of Computer Trends and Technology, 6-June 2013.

[2] D. A. S. Ambhaikar, "Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security," Research Gate, November2012.

[3] S. H. O. M. M. S. H. N. Youssouf Mahamat Koukou, "Comparative Study of AES, Blowfish, CAST-128 And DES Encryption Algorithm," IOSR Journal of Engineering, vol. 06, no. 06, June 2016.

[4] V. k. V. Sandip Thitme, "A Recent Study of Various Encryption and Decryption Techniques," International Research Journal of Advanced Engineering and Science.

[5] S.M. Thampi, "Information Hiding Techniques: A Tutorial Review".

[6] I. B. a. G. S. Souvik Bhattacharyya, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science, vol. 2, no. 4, April 2011.

[7] P. C. Mandal, "A Study of Steganography Technique using Discrete Wavelet Transform," Journal of Global Research in Computer Science.

[8] A. Takiedeen, "Design and Implementation of Hybrid Encryption Algorithm".

**Author's Profile:**

**Vadde SeethaRama Rao** is presently working as an Assistant Professor in the Department of Electronics and Communication Engineering, SNIST Hyderabad, Telangana, India. He is having 4Years of teaching experience. His areas of interest are VLSI and Analog IC Design.

**L.V.R Chaitanya Prasad** is presently working as an Assistant Professor in the Department of Electronics and Communication Engineering, SNIST Hyderabad, Telangana, India. He is having 8Years of teaching experience. His areas of interest are Advanced Communication System ,Network Security and Cryptography.