A Novel Approach for Embedding Text in Audio to Ensure Secrecy

NAGASESHU.K, SRINIVASA RAO.V , HIMA DEEPTHI.V
Department of Computer Science and Engineering,V R Siddhartha Engineering College,Vijayawada--522007

Abstract-
Steganography is the art of hiding one medium of information in another medium. There are many approaches in hiding textual information in audio and hiding textual information in Audio method provides the most effective way to guard privacy. Key aspect of embedding text file in audio is that, after embedding text in audio the size of the audio remains same. The existing system can't provide more security and lack of user interface. The message length is restricted to few characters only. The audio file used for the embedding process can't be reused and it is also difficult for receiver to detect which audio file contains the secret message send by the sender. In the proposed technique we alter the data of lower bit in a cover object to embed textual information. The main goal of this paper is to embed textual information into audio without affecting the file structure of audio file and we encrypt text message to get advantage of cryptography also.

Keywords- **Steganography, Data hiding, Embedding, Extraction, Cover object.**

I. INTRODUCTION

The main goal of steganography [6] is to hide a secret message within a cover-media in such a way that others cannot detect the presence of the hidden message. The term steganography originated from Greek roots that literally mean "covered writing". Cryptography conceals about content or meaning of a message, while steganography conceals about the very existence of a message. There exist many steganographic techniques for hiding information in different carriers.

In early days the secret messages hiding was done in documents [7].The use of Steganography in documents works by simply adding white space and tabs to the ends of the lines of a document. This type of Steganography is extremely effective, because the use white spaces and tabs are not visible to the human eye at all, at least in most text/document editors. White space and tabs occur naturally in documents, so there isn't really any possible way using this method of Steganography would cause someone to be suspicious. It is used in initial decade of internet era. But it is not used frequently because documents have a small redundant data.

Later hiding secret message in images becomes more popular technique for Steganography [5] especially on internet. Least Significant Bit (LSB) coding is used to embed secret data in images. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. But this technique lacks in payload capacity and robustness.

At present hiding data in audio files becomes more popular. Audio data hiding [1] method provide most effective way to provide privacy. Embedding the secret messages in digital sound is usually a very difficult process. There are many techniques available for hiding text in audio signal.

II. RELATED WORK

1. Phase Encoding:

Phase encoding [5] is complex when compared to lsb. Instead of converting entire audio into bits, we convert it into phase. The length phase is equal the secret message. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments".

One disadvantage associated with phase coding is a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only. This might be addressed by increasing the length of the signal segment. However, this would change phase relations between each frequency component of the segment more drastically, making the encoding easier to detect. As a result, the phase coding method is used when only a small amount of data, such as a Watermark, needs to be concealed.

2. Spread Spectrum:

Spread spectrum [6] spreads entire message in the signal. The text is modulated using pseudorandom noise sequence which then becomes the key. Then the modulated data is attenuated and added to the original file as additive random noise.

Due to the wide spread of the noise, it is possible that it will be almost inaudible to a human ear. However due to the complexity of implementing this method, it was beyond the scope of this paper. Normally spread spectrum is used for small amount of data (holograms).

3. Echo Data Hiding:

In this technique we embed secret message by introducing in echo. The data is then hidden by varying three parameters of the echo [2]: initial amplitude, decay rate, and offset. It is possible to time the echo in such a way that a human ear will not be able to distinguish between the two signals, and registers the echo as some added resonance. However, doing so is not trivial. There is any rule for introducing echo. According to IBM research the best delay for the coded echo is 1/1000 of a second for most listeners.

III. PROPOSED SYSTEM

The proposed system provides a basic view of audio steganographic process in sender and receiver side. At the sender side the text message is encrypted by symmetric encryption (we choose one of the two AES, DES) algorithm using a key shared both sender and receiver as shown in Figure 1. Symmetric encryption is an efficient process for providing security to the message. The encrypted text is passed to embedding phase. In embedding phase encrypted text will embedded into the cover signal which is in audio format *.wav resulting a stego signal. The embedded audio or stego signal contains the encrypted text message which is extracted at the receiver side. When embedding secret message in audio one thing we must follow is size of the message is lower than audio signal.

At the receiver side stego signal is passed to extractor phase as shown in Figure 2. In extraction process encrypted text will be extracted from embedded audio signal and encrypted text is decrypted using decryption module.

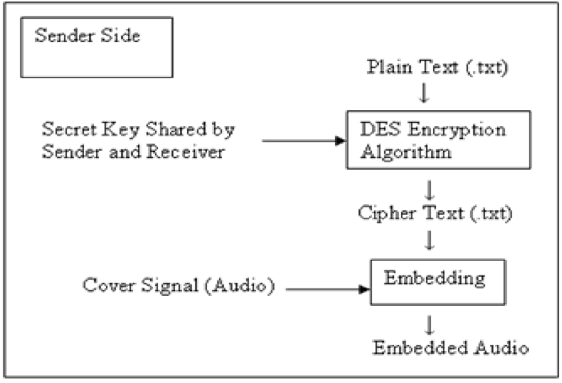

Fig 1: Steganographic System at sender side

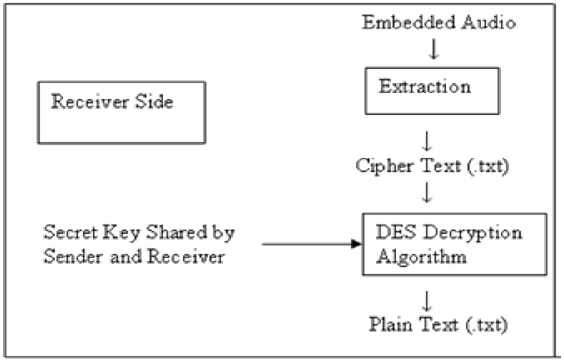

Fig 2: Steganographic System at receiver side

In decrypter, encrypted text will be decrypted using shared secret key. In symmetric encryption we use either DES or AES. AES provide more security than DES and also choose key size and block size for both encryption and decryption rest of embedding and extraction process is same for both AES and DES are same. In the propose system we can reuse audio which is embedded in past and we can also detect whether embedded audio contain secret message or not by uploading embedded audio in extraction process.

IV. OBJECTIVE

The main objective of the paper "A Novel Approach for embedding text in audio to ensure secrecy" is to embed the text message in cover object (audio file), using the Least Significant Bit (LSB) coding. The receiver extracts the message from carrier audio file. Before we embed the text message in audio, we encrypt the message using available cryptographic algorithms. To provide a security tool based on steganographic techniques for sending message secretly.

V. METHODOLOGY

Least significant bit (LSB) [1] coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In this paper we embed encrypted message in audio and extract encrypted message from audio. During embedding and extraction process the content of the message not to be damaged, if any damage occurs problem may arises during decryption process at receiver side.

Embedding:

First select a wav file and load it into steganographic system and steganographic system converts it into bits. As well as text file will also converted into bits. The first bit of the text will be inserted into the least significant bit of the audio file. The process will run until the entire text message will be inserted into audio file as show in Figure 3. If the text message will greater than the audio file then display the error message.

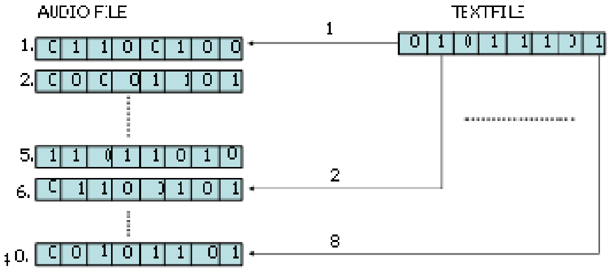

Fig 3: Encoding text file in to the audio file

Algorithm for Embedding Text in Audio:

Input: Audio file (.wav), Original message (.txt) and Shared Secret key.

Output: Embedded Audio file (.wav)

```
Step1: Convert the text message into cipher text by
       Using secrete key shared by sender and
       receiver.
Step2: Load the audio file (.wav).
Step3: IF size text file >= size of no of sample of audio
        Stop the process choose another audio
        Else
        Embedding can be done as explained below.
Step4: Convert the audio file in the form of bits.
Step5: Convert the encrypted text message into bits
Step6: Leave first 55 bytes it stores header section of audio file
```

Step7: Split converted audio into combination of 8 bits and substitute least significant bit of audio with text message.
Step8: Continue the process until the message fully embedded into audio file.

Extraction:
The output of embedding process is input for extraction. If the audio file cannot contain the any message then print the error message as shown in Figure 4.

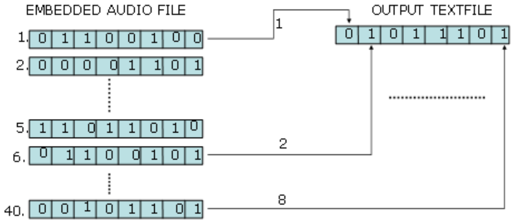

Fig 4: Extraction of text file from the audio file

Algorithm for Extracting Text from Audio:

Input: Embedded Audio file, Shared Secret Key
Output: Original message (.txt)

```
Step1: Load the embedded audio file (.wav).
Step2: Load an empty text file (.txt).
Step3: if audio file does not any message contain message
        Print error
        else
        Extract hidden message from embedded audio
Step4: for extraction reverse the process done in embedding algorithm in step7.
Step5: save the secret message in new text file (.txt)
Step6: using shared key decrypt message to get original data.
```

VI. EXPERIMENTAL RESULTS

In the existing system the size of the text file to embed in audio is limited to 15% of that cover object and it may damage the header section of audio file which may result degradation quality of audio file as shown in Figure 5.

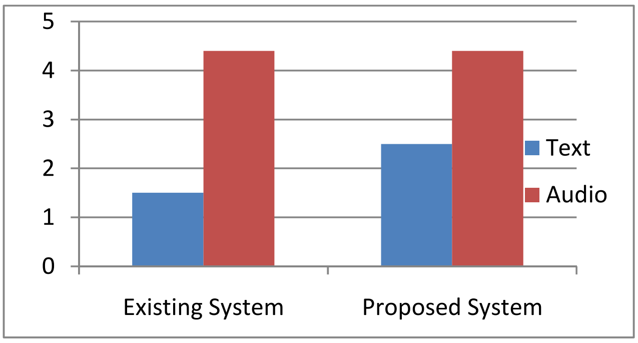

Fig 5: Comparison of text Embedded in audio file

In proposed system size of text file to embed in audio is raised up to 75% of that audio and it is not introduce any noise in audio file, because we are leaving header section and inserting data part of the audio. The Figure 5 shows difference in embedding capacity of text file in audio. The size of audio file is same in both system but difference in their embedding capacity. The size of the text file after encryption does increase it size little bit because of permutation in Des algorithm but does not make vast changes of its size**.**

VII. CONCLUSION

When we embed secret information (text) in audio using lsb technique it may raises enough noise in the resultant audio. The Proposed system finds a way to embed secret information in audio without introducing noise. To proceed with this the header section of the audio not modified because it stores sensitive information like sample rate, frame size etc. We encrypt text file to get advantage of cryptography also. The combinations of cryptography and steganography result secure steganography.
The proposed system embeds the text file in audio file successfully and retrieves text from cover object. In this system we encrypt text by using available encryption algorithm before embedding at the receiver side text will be decrypted, it provide security system robust. Future scope of the paper is to increase capacity of embedding secret message in the carrier as well as secrecy of the message.

VIII. REFERENCES

[1] Pramatha Nath Basu and Tanmay Bhowmik "On Embedding of Text in Audio-A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and Computing. 2010.

[2] K.Geetha and P.Vanitha Muthu "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy" International Journal on Computer Science and Engineering Vol.02, No. 04, 2010, 1308-1313.

[3] Masahiro Wakiyamat, Yasunobu hidakat, Koichit "An audio steganography by a low bit coding method with wave files, 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[4] Poluami dutta, Debnath Bhattacharya and Tai-hoon, "Data Hiding in audio signal: A Review", International Jouranal of Database theory and application, VO; .2, No.2, June2009.

[5] W.Bender, W.Butera, D.Gruhl, F.J.Paiz,S.Pogreb "Techniques for data hiding", IBM Systems Journal, volume 39, Issue 3-4, July 2000, pp 547-568.

[6] Soum.yendu Das, Bijoy Bandyopadhyay and sugata sanyal, "Steganography and steganalysis: Different Approaches", an article.

[7] Data Hiding in Images Part 1-Fundamental Issues and Solutions, IEEE Transaction on Image Processing, Vol. 12, No.6, June 2003.

[8] Aelphaesis Mangare [www. Zone-H. Org]