Encrypted Text into Wav File

[1*]V.P.Sridhar, [1]N.Chandru, [1]P.Chandhru, [1]R.B.Kannan, [2]Dr.K.Ramesh

[1] UG scholars, Dept of IT, Nandha Engineering College

[2] Professor, Dept of IT, Nandha Engineering College

[*]Email: ponsridharponnuswamy@gmail.com

Abstract

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information. It also enables verifiability of every component in a communication. In this paper a frequency domain of the wav audio signal is taken for the encryption and decryption. Here, we use the DFT (Discrete Fourier Transform) for transforming the time domain audio signal to frequency domain audio signal. An audio signal can be separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. Here, we apply RSA technique for the encryption and decryption on the lower frequency bands because all the frequency regions do not participate equally in the communication. After applying the encryption on different frequency bands, we observe that, the encryption on the lower frequency band is more effective than the higher one. So, we would apply encryption on lower frequencies with higher phase values. Here we are applying our technique on phase values.

Keywords

Steganography, Hiding, Cryptography, Data Encryption Standard, Time Domain, Frequency Domain.

1. Introduction

Steganography entails the art of writing concealed messages in such a manner that only the sender and the intended receiver are aware of the presence of the message. After the unprecedented technological advancement that has taken place over the years and in particular with the era of internet technology that is now commonly used for communication, it can be explained that there is a need to ensure that measures are put in place so that information that is sent from one party to another is secure. Indeed, such an approach would entail encryption and concealing of messages inside an image file, audio file or both types of files.

Concealing information can be discussed as an approach of restricting private information in an image file or audio, video and executable files in order to ensure that it becomes impossible for a person to have access to the message unless he/she is either the sender or the receiver. The program can modify the shape of the data indoctrination as well as the delivery of content format and not raise any suspicions.

The key benefit of concealing information through the use of various approaches is that it does not give any hints of there been a hidden message in case the message is accessed by a third party. Unlike encoded message, the message in this case will be used as a technique of inviting the focus of the third party.

Even though the steganography method has different applications that are useful, it can at times be applied for other illegal activities. For instance, drug dealers, terrorists and other criminals can use the technique in order to ensure that their communication is not accessed by third parties thus implying that it can help enhance the activities that are carried out by the criminals.

All of the above are some of the main reasons as to why development wider writing concealed compared techniques of encryption, since writing is encoded or distorted resulting to the administrator been required to implement different strategies in order to ensure that they get access to the original information and attempt to break the code, while writing concealed does not raise doubt when regular viewer, might pass by undetected with no suggestion of any information been concealed in the file that is included.

The suggested method integrates the cryptography and steganography concepts and as a result establishes a high level security which thwarts attackers from discovering the existence of the concealed message. In the initial level, the concealed message is encoded by application of Huffman coding Algorithm. In the succeeding level, the encoded text is concealed in the audio file through the use of least significant Bit.

2. Related works

Several researches in the field of data hiding are developed. Mohammed Majeed proposed a system for hiding audio in audio using Discrete Cosine Transform (DCT). The research is designed and implemented steganography system that provides six hiding methods with different hiding rates for hiding data into audio signal by using DCT. These methods could be classified according to the accuracy of secret data reconstruction (lossy and lossless), and to the domain for both secret and cover data during the hiding process (time and frequency) . Poulami Dutta et al. proposed efficient method for hiding the data from hackers and sent to the destination in a safe manner. The proposed system does not change the size of the file even after encoding and also suitable for any type of audio file format. Kriti Saroha and Pradeep Kumar Singh presented a new steganographic using Least Significant Bit (LSB) method for embedding an image in an audio file. Pushpa Aigal and Pramod Vasambekar proposed an efficient audio steganography system, in which the LSB technique is used to get high data hiding capacity and low perceptibility

3. Proposed System

The proposed system provides a basic view of audio steganography 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.

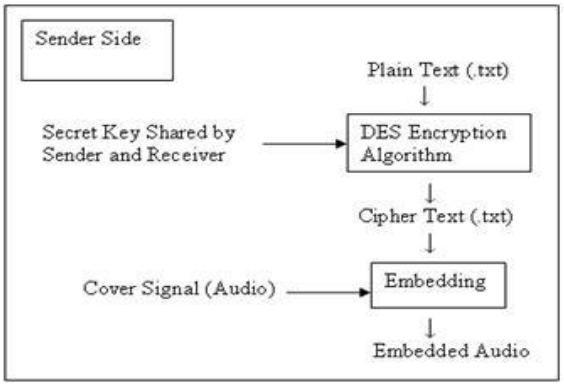

Fig 1: Steganographic System at sender side

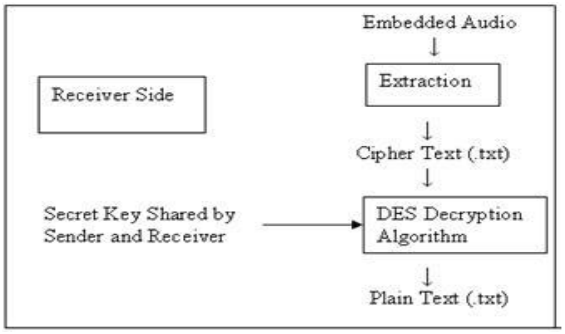

Fig 2: Steganographic System at receiver side

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.

4. Results and Analysis

A. Time Domain Analysis

1) The original wav signal is

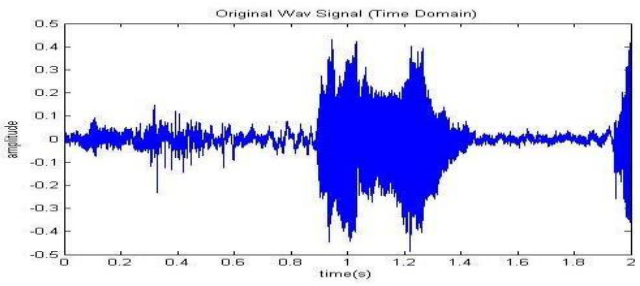

Fig-3: Original Wav Signal

2) The encrypted wav signal [1] is

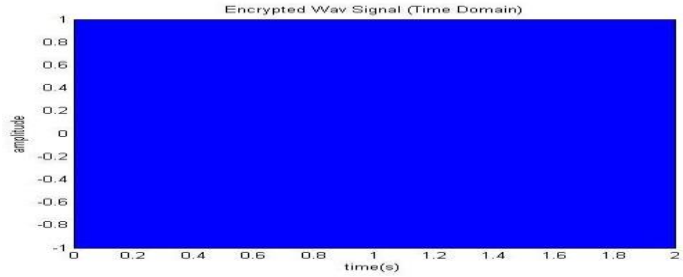

Fig-4: Encrypted Wav Signal

3) The decrypted wav signal is

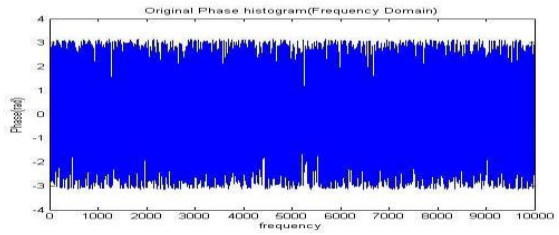

Fig-6: Original Wav Signal decrypted

B.FREQUENCY DOMAIN ANALYSIS:

1) The original power spectrum in frequency domain is:

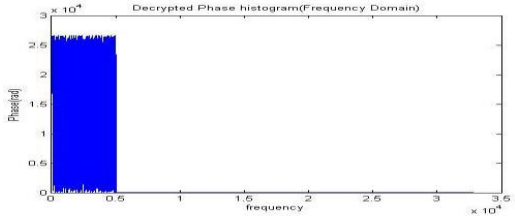

Fig-6: Original Power Spectrum (Higher Phase values)

2) The encrypted power spectrum is

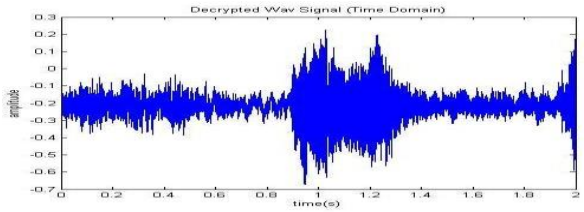

Fig-7: Encrypted Power Spectrum (Higher Phase values)

3) The decrypted power spectrum is

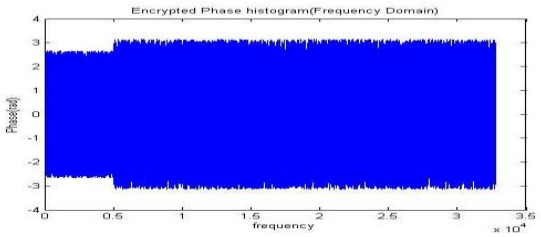

Fig-8: Decrypted Power Spectrum (Higher Phase values)

5. Conclusion

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Audio file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly.

Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic steganographic algorithms that do not use keys. By using this algorithm, two parties can be communicated with a fairly high level of confidence about the communication not being detected.

In designing the “Steganography” utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts. And principles so as to maintain good quality in the developed system as per the user requirements.

References

[1] M. Majeed, "Hiding Audio in Audio Using DCT", M.Sc. Thesis, Computer Science Dept., College of Science, Al-Nahrain University, Baghdad, Iraq, 2004.

[2] P. Dutta, D. Bhattacharyya and T. Kim, "Data Hiding in Audio Signal: A Review", International Journal of Database Theory and Application, Vol. 2, No. 2, June, 2009.

[3] K. Saroha and P. K. Singh, "A Variant of LSB Steganography for Hiding Images in Audio", International Journal of Computer Applications, Vol. 11, No. 6, December, 2010.

[4] P. Aigal and P. Vasambekar, "Hiding Data in Wave Files", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS), 2012.

[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]