ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Information Hiding Using Audio Steganography with Encrypted Data

R.Valarmathi., M.Sc.,M.Phil [1], G.M.Kadhar Nawaz M.C.A., Ph.D [2]

Research Scholar, Bharathiar University, Coimbatore[1]

Research Supervisor, Director& Professor, Department of MCA, Sona College of Technology, Salem[2]

Abstract: Steganography is an art of hiding messages inside an image/Audio file or a video file such that the very existence of the message is unknown to third party. Cryptography is used to encrypt the data so that it is unreadable by a third party. This system combines both the above techniques. To make the system more secured this system uses most powerful algorithm in the first level of security which encrypts the data. In the second level the encrypted data is embedded in to the Audio file using modified LSB algorithm. This system ensures more security.

Keywords: Audio Steganography, Cryptography, Embedding, Encryption, Information Hiding.

I. INTRODUCTION

Information hiding has recently gained importance in various applications. Steganography has become one of the popular approaches for information hiding. A recent breakthrough in this field is hiding information in Audio files. The embedded data should be as immune as possible to modifications from intelligent attacks or anticipated manipulations [1]. Thus the hidden messages are encrypted before hiding behind Audio files.

This system hides encrypted information in Audio files. The text to be embedded is first encrypted and then embedded into the Audio file to allow maximum performance and robustness. This allows the users to easily and securely carry the data. The major task of the Audio Steganography is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and algorithms proposed and store the information in a form that is undetectable.

This system has a reversal process, which is used to de-embed the data from Audio file and decrypt the data to its original format upon the proper request by the user. While the Encryption and Decryption is done the application should satisfy the standards of authentication and authorization of the user [1].

II. REVIEW OF LITERATURE

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message [2].

A. Categories of Steganography

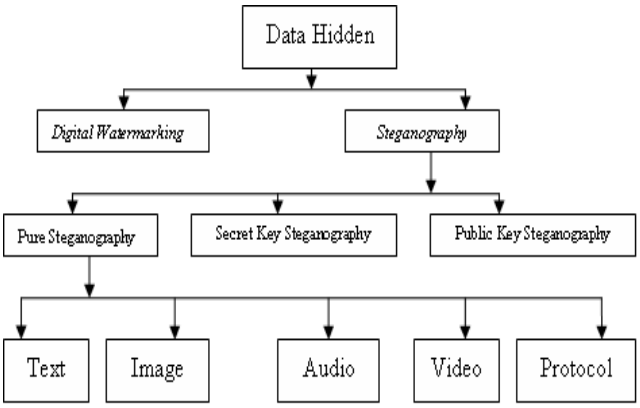

Figure 1. Categories of Steganography

There are basically three main categories in Steganography:

- Pure Steganography.
- Secret key Steganography.
- Public key Steganography

Pure Steganography

In pure steganography, the secret lies in the embedding and extracting algorithms that only the message sender and intended receiver should know [3].

Secret Key Steganography

Secret key steganography is similar to a symmetric cipher. It is assumed that a party other than the sender and intended receiver knows the embedding and extraction algorithms. The sender embeds a message in a cover-object using a

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

secret key known as a stego-key. Therefore, even if a third party intercepts the stego-object and extracts the information, the result will appear to be a random, garbled mess. Only the intended receiver who possesses the same key can extract the original message [3].

Public Key Steganography

Public key steganography is based on principles of public key cryptography. In a public key steganography system, two keys are used: a **private key** and a **public key**. The public key is used in the embedding process, and the private key is used in the extraction process. Public key steganography allows the sender and receiver to avoid exchanging a secret key that might be compromised. However, as with public key cryptography, public key steganography is susceptible to a man-in-the-middle attack [3].

B. Audio Steganography

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files [3]. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the exploit sophisticated signal processing techniques to hide information [3]. Signals are processed either on LSB, Parity, Phase, spread spectrum methods. Audio has been taken as the carrier to send the encoded messages using the above said methods. In this paper, the main algorithm used to hide the data is Least Significant Bit (LSB). The list of methods that are commonly used for audio steganography are listed and discussed below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

C. Cryptography

Cryptography is the process of conversion of data into scrambled code that can be deciphered and sent across a public or private network. The two main forms of encrypting data in cryptography are symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they for decryption [4]. Other names for this type of encryption are secret-key, shared-key, and private-key. Symmetric cryptography is at times simple to decode [1]. Asymmetric cryptography uses different encryption keys for encryption and decryption.

D.Combination of Steganogrpahy and Cryptography

Steganography is not the same as cryptography data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users [5]. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptograpgy and steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded [5][6]. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

III. RELATED WORK

Relevant work has been done on this subject. Many have designed system which increase the capacity of the steganography approach and few has increased security. In recent years, tools for audio steganography such a H4PGP, S-Tools, Steghide has been designed which increases the steganographic features like security and capacity. The most easy and commonly used algorithm for any steganographic application is LSB(Least Significant Bit) it has been used by many designers and in many applications. Concept of Genetic algorithm has also been applied on audio steganography by Mazdak Zamani et al. R.sridevi has created the four layered system which combines the steganographic approach with strong encryption. G.padmashree has proposed the process of embedding the encrypted secret message into the 4^{th} and 5^{th} layers of the Audio file. The steganographic applications are also extended to be used as watermarking schemes to make the copyright issues and areas where legal issues are concerned. Approaches like spread spectrum of audio data hiding method which hides data throughout an audio file at different frequencies of the file. There are other methods like parity coding, phase coding, echo hiding, which is also used in the audio steganography.

IV.PROPOSED WORK

In the Audiography, the process of embedding secret message using Symmetric-Key algorithm, Blowfish into the Audio file. The following gives the complete working of the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Audio Steganogrpahy. This system contains Sender Side and Receiver Side. Both are connected with Trustcenter. Both sides the user has to register their name. The system will generate secret key for the user. Using the login name and secret key both the users can enter into their area. Trustcenter is waiting for a sender and receiver request then it will generate the Quantum Key. Both Sender and Receiver have the same quantum key to connect with each other through Trustcenter to make the system more secured.

In the sender side, the text which has to be embedded into an audio file is encrypted using Symmetric Key cryptographic algorithm, Blowfish. The cipher text obtained is then embedded using Steganographic algorithm. The resultant audio file contains the secrete message embedded into it. In the receiver side, the embedded audio file is selected to extract the secret message. The secret message is decrypted using Blowfish decryption method.

Steganographic algorithms can be characterized by a number of defining properties. Three of them, which are most important for audio steganographic algorithms, are Transparency, Capacity and Robustness [7][8]. In the Proposed system, all these properties are taken into consideration and care is taken for not having too much error, which makes steganogrphy more secure.

The following gives the proposed methodology of this system:

A. Algorithm for Embedding Text file content into Audio file at the Sender Side:

Step 1: Select the Text file containing the secret message.

Step 2: Encrypt the text file contents using Blowfish Algorithm.

Step 3: Select the Audio file for embedding the secret message.

Step 4: Play the audio file so that it sounds clear to the end user.

Step 5: Compare the text file and audio file size. If text file size > audio file size then display the message indicating cannot embed secret message. Else embed the encrypted message into the Audio file using modified LSB algorithm.

B. Algorithm for Extracting the Embedded text from Audio file at the Receiver Side:

Step 1: Select the Embedded Audio file for extracting the secret message.

Step 2: Extract the secret message from Audio file using modified LSB algorithm.

Step 3: If secret message present in audio file then display the message to the end user after extracting message. Else display that no hidden data is present.

Step 4: Decrypt the secret message using Blowfish Algorithm.

Step 5: Display the secret message to the end user.

V.ANALYSIS OF THE PROPOSED WORK

With reference to literature survey LSB technique gives best results hence considered for implementation. The proposed steganography techniques take help of well known cryptography algorithm to increase the security level. In order to evaluate the sound quality after embedding the secret message into Audio files, test is carried out. The following figure gives signals of the original audio file and embedded audio file in various ways of analysis which shows that there is no much more deviation.

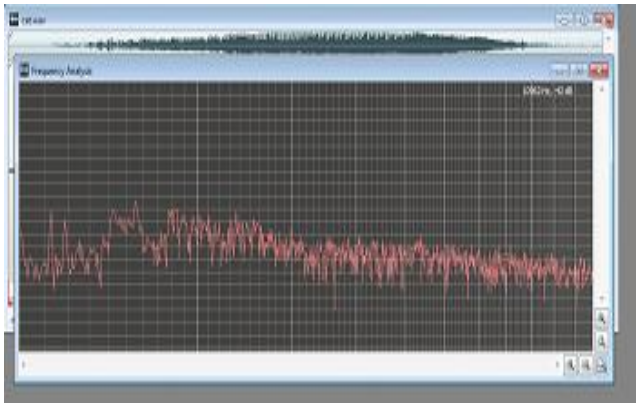

Fig 2 Original Audio File (Frequency Analysis-cat)

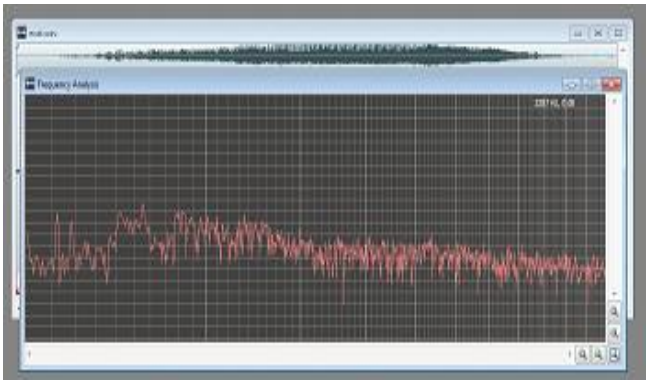

Fig 3 Embedded Audio File(Frequency Analysis-ecat)

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

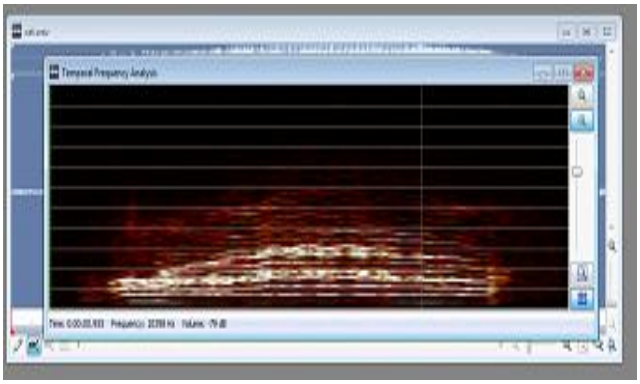

Fig 4 Original Audio File (Temporal Frequency Analysis-cat)

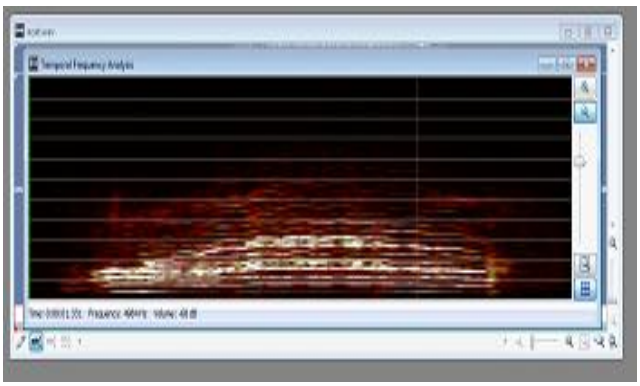

Fig 5 Embedded Audio File (Temporal Frequency Analysis-ecat)

VI. CONCLUSION

Data security has been a great importance since last few decades. The proposed system has been designed for hiding information using Audio steganography with encrypted data which increases the security of the audio steganography and a key management is also used in both the sender and receiver to make the system more secured.

VII. FUTURE WORK

With reference to future work, it can be extended to communicate over network by sending a file from one to the other by emailing the file to a particular account when the email is provided.

ACKNOWLEDGEMENT

My sincere thanks to Dr.G.M.Kadhar Nawaz M.C.A., Ph.D,. Director& Professor, Department of MCA, Sona College of Technology,Salem-5 for supporting and encouraging to do this research work and I extend my thanks to my friends who are in this circle and also the peer review committee members.

REFERENCES

[1] Keeping Secrets Secret - Implementation Of Steganography With Audio File And Encrypted Document -Vijaya Lakshmi Chittimalli.
[2] Steganography- Wikipedia, the free encyclopedia.
[3] Methods of Audio Steganography, Internet publication on www.Snotmonkey.com.
[4] Cryptography – Barcodeslnc.
[5] Secure Data Communication using Steganography and Cryptography by Suresh Babu.P.
[6] A Methodology on cryptography and Stegnography Applicant to Mobile Adhoc Network & Wireless Sensor Network -Pawiterjit kaur, Sanjeev Dhiman, Kawaljeet Kaur.
[7] Audio steganography – Hide the text into the Audio.
[8]Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers - Padmashree G, Venugopala P S.

BIOGRAPHIES

R.Valarmathi is a Research Scholar of Bharathiar University, Coimbatore, Tamil Nadu, India. She has presented papers in various national and international Conferences. She is guiding M.Sc and M.Phil Students of Various Universities. Her area of Interest includes Cryptography and Steganography, Artificial Intelligence, Design of Algorithms.

Dr.G.M.Kadhar Nawaz is presently working as Director in the Department of Computer Applications, Sona College of Technology, Salem, Tamil Nadu, India. He has presented and published papers in various national and international Conferences and journals. He has also organized national conferences. He completed Ph.D in Computer Science from Periyar University and his area of research includes Digital image Processing and Steganography.