Improving Data Security in Audio Steganography With Padding LSB Techniques And Audio Files

[1]G.Srikanth, [2]K.Ganesh Kumar,[3]K.Shivangini Reddy, [4]Rambabu M
[1]B.Tech, Student, [2]B.Tech, Student, [3]B.Tech, Student, [4]Assistant Professor,
[1]KGRCET JNTUH, RR District, Telangana, India, [2]KGRCET JNTUH, RR District, Telangana, India, [3]KGRCET JNTUH, RR District, Telangana, India, [4]KGRCET JNTUH, RR District, Telangana, India,

ABSTRACT: The project entitled **Audio Steganography** is the application developed to embed an audio file in another audio signal. It is concerned with embedding information in an innocuous cover Speech in a secure and robust manner. This system makes the Files more secure by using the concepts Steganography and Cryptography. Steganography, poor cousin of Cryptography is the art of hiding messages inside other messages such that the very existence of the message is unknown to third party. The goal of cryptography is to make data unreadable by a third party, the goal of stenography is to hide the data from a third party Through the use of advanced computer software, authors of images and software can place a hidden trademark in their product, allowing them to keep a check on piracy. This is commonly known as **watermarking**. Hiding serial numbers or a set of characters that distinguishes an object from a similar object is known as **finger printing**. Together, these two are intended to fight piracy. The latter is used to detect copyright violators and the former is used to prosecute them. But these are only examples of the much wider field of stenography.The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible. The embedded data should be as immune as possible to modifications from intelligent attacks or anticipated manipulations .Thus it is necessary that the hidden message should be encrypted.

1. INTRODUCTION

In 1986 BOOCH developed the Object Oriented Design concept is called as BOOCH METHOD. It covers both analysis and Design phases of the Object Oriented System, The BOOCH METHOD consists of following diagrams:

- Class diagrams
- Object diagrams
- State transition diagram
- Module diagram
- Process diagram
- Interaction diagram

BOOCH used the large set of symbols. Even though BOOCH defines a lot of symbols to document almost every design decision, if we work with his method, you will notice that you never use all these symbols and diagrams; this is this main draw back of the BOOCH METHOD.In 1991 Jim Raumbaugh develop the OMT (Object Modeling Technique) with the help of his team It covers analysis, Design and implementation of the system.

OMT separates Modeling into three different parts:

- Object Model

Presented by the Object Model and the data dictionary.

- Dynamic model

Presented by the State diagrams and Event flow diagrams.

- Functional Model

Presented by Data flow and constraints.

There is no traceability in the different phases, both forward and back ward; this is the main disadvantage of the OMT.

In order to avoid the problems faced in the above two models JACOBSON invented the one model called as the JACOBSON METHDOLOGIES (Object Oriented Software Engineering). It will cover the entire life cycle and stress tractability between different phases, 0both forward and back ward, Additionally he invented the Use case diagrams, these diagrams are necessary to understanding system requirement. It captures the goal of the system. It is used to identify the Use cases and External users (external users are the users who interact with our system to complete the task) .

Features

2. **Audio Steganography is a one of hidden messaging system, user can and hidden and important messages in a wave (.wav) file.**
3. **The message will be encrypted with a code number and send to the receiver, and then he can decrypt the message giving same code number.**
4. **Authors of books, manufacturers kept their emblem in hidden place to restrict the piracy like water marking, in this also sender will keep the message in .wav file.**
5. **The .wav file will be saved automatically in another name when encryption is completed.**
6. **If receiver has given the Key or Code number the original file will be opened automatically.**

The Jacobson ET Al. Methodologies

JACOBSON METHDOLOGIES (Object Oriented Software Engineering) OOSE cover the Entire life cycle and stress trace ability between the different phases, both forward and backward. And Use case diagrams, these diagrams are necessary to understanding system requirement. It captures the goal of the system. It is used to identify the USE CASES and External users (external users are the users who interact with our system to complete the task)

The Use case Description must contain

- HOW and WHEN the use case begins and ends.
- The interaction between the use case and its actors, including WHEN the interaction occurs and WHAT is exchanged.
- HOW and WHEN the use case will need data stored in the system or will store data in the system.
- EXCEPTION TO THE flow of events.
- HOW and WHEN concepts of the problem domain are handled.

By using the use case model we will find the External users, External users are the users who will interact with our system to complete the task. Every single use case should describe one main flow of events. An exceptional additional flow of events could be added.

OBJECT ORIENTED SOFTEWARE ENGINEERING

Object oriented software engineering also called, as the objectory. It is build around several models:

- USE CASE MODEL: The use-case model defines the outside (actor) and inside (use case) of the systems behavior.
- DOMAIN OBJECT MODEL: The objects of the “real” world are mapped in to the main object model.
- ANALYSS OBJECT MODEL: The analysis object model presents how the source code (implementation) is carried out and written. IMPLIMENTATON MODEL: The implementation model represents the implementation of the system.
- TEST MODEL: The test model constitutes the test plan, specification and reports.

JACOBSON METHDOLOGY consists of following diagrams:

- Use case Diagrams
- UML activity diagram
- UML use Case Diagram
- Sequence diagrams
- Class diagrams
- Business class diagrams

USE CASE DIAGRAMS:

A use case describes a sequence of actions that provide something of measurable value to an actor and is drawn as a horizontal ellipse an actor is a person, organization, or external system that plays a role in one or more interactions with your system.

UML ACTIVITY DIAGRAM:

Activity diagrams are used to document workflows in a system, from the business level down to the operational level. When looking at an Activity diagram, you'll notice elements from state diagram, the Activity diagram is a variation of the state diagram where the "states" represent operations, and the transitions represent the activities that happen when the operation is complete. The general purpose of Activity diagrams is to focus on flows driven by internal processing vs. external events.

SEQUENCE DIAGRAMS:

UML sequence diagrams model the flow of logic within your system in a visual manner, enabling you both to document and validate your logic, and are commonly used for both analysis and design purposes. Sequence diagrams are the most popular UML artifacts for dynamic modeling, which focuses on identifying the behavior within your system.

CLASSDIAGRAMS:

A class diagram describes the static structure of the symbols in your new system. It is a graphic presentation of the static view that shows a collection of declarative (static) model elements, such as classes, types, and their contents and relationships. Classes are arranged in hierarchies sharing common structure and behavior, and are associated with other classes.

II. RELATED WORKS

Steganography, coming from the Greek words *stegos*, meaning roof or covered and *graphia* which means writing.It is the art and science of hiding the fact that communication is taking place. Using the steganography, we can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an invisible message will not do so. There are many papers proposed in this audio steganography with most of the papers embed secret audio file in a carrier audio file. Some of them used cryptography for additional security. The author are mainly concerned with the security of the embedded message. To achieve high robustness and capacity of our steganalysis various methodologies have been implemented and verified their approach. In [1] kaliappan gopalan proposed a steganalysis in audio file with an encryption key for the embedded secret audio file. In [2] M Asad,J Gilani & A Khalid proposed a audio steganography with an encrypted audio file using Advanced Encryption Standard(AES).
In [3] Mazdak Zaman, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki proposed a genetic algorithm for the embedding secret audio files for achieving higher robustness and capacity. In [4] kaliappan gopalan embed the information of secret message in spectral domain of a cover audio or image files. In [5] K.B.Raja, C.R.Chowdary, Venugopal K R,& L.M.Patnaik proposed a work on image steganography where a LSB embedding is used and then DCT is performed followed by a compression technique to provide high security in the hidden data. In [6] Hossein Malekmohamadi and Shahrokh Ghaemmaghami proposed an enhancement in image steganalysis of LSB matching by reducing the complexity using gober filter co-officients. In [7] R Balagi & G Naveen extended their work towards video steganography by embedding the secret information in some particular frames. In [8] Andrew D. Ker derived a mathematical analysis for the steganlysis in last two LSB bits.
In this paper, a secret message of an audio file or a text file is first encrypted and then it is embedded into a carrier audio file. Our assumptions are the audio files are strictly in .wav format and the carrier audio file should be eight times greater than the secret audio message file. The paper is organized as follows: In section 2 the existing audio steganography methods are discussed. Section 3 deals with the overall system model with the proposed audio steganography technique. In section 4 and 5, the experimental results and conclusion are discussed

III. THE PROPOSED SYSTEM

To provide secure communication between sender and receiver we are going to provide security using Audio Steganography. In this the plain text (Message) will be encrypted that means we are going concatenation message and audio file using ASCII values. To overcome problem of symmetric cryptography message is encrypted with a key.

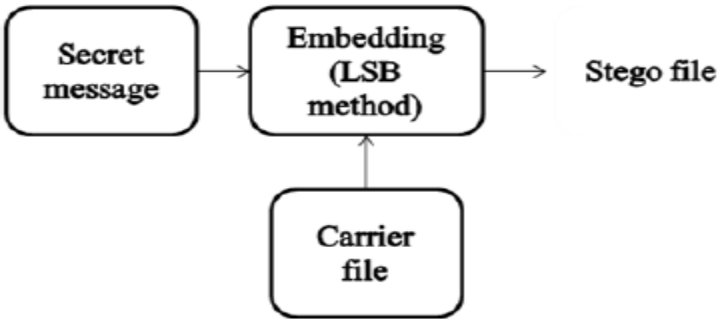

Figure 1 basic steganographic process at transmitter

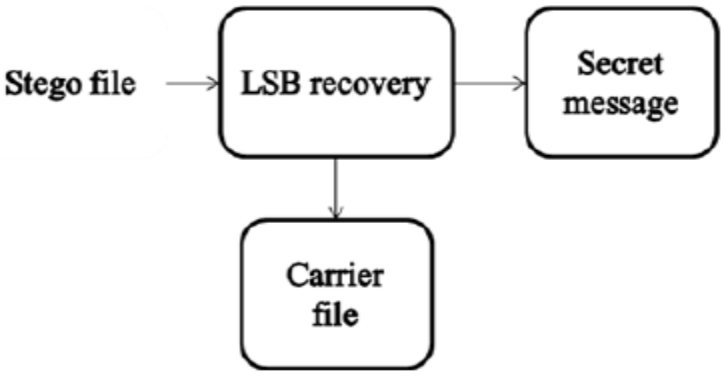

Figure 2 de-steganographic process at receiver

The same key should transmitted to receiver, here actual problem rises in the transmission of key through transmission message, call etc. we are using asymmetric cryptography this algorithm consists two keys public and private key the user can encrypt the message with the help of his own private key (or) public key of receiver then the receiver can decrypt with the help of public key of sender or private his respectively. Here there is no need of key transmission. In [1] the secret message and carrier files are taken as audio files. Before performing the embedding process the secret message is encrypted using a private key cryptography. Then the stego object is created. Thus using the key

the secret information is retrieved at the receiver side. In [2] audio files are taken and the AES of 256 bits key length is used for the encryption of secret audio file to ensure the security.

IV.PERFORMANCE DISCUSSION

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Here a key is taken at the transmitter with that a pseudo sequence is generated and this sequence is performed a logical operation with the secret message. Then the embedding process is carried out with the carrier audio file and is transmitted at the transmitter side as in figure 3.
In the receiver side with the audio stego file the LSB are recovered first and with the known key generated at the transmitter the decryption process is carried out and the secret message is recovered from the stego file. The entire proposed de-steganographic process is shown in figure 4.
The algorithm for our proposed method is followed,
Step 1: Get the carrier file and message file such as the length of carrier file is a1, and message file is a2.
y=wavread(a1,'native');
s=dec2bin(y(i),8);
Step 2: The key is obtained from the user and thus we generate the PN sequence based on the key value. Let the **key value be denoted as r and thus the output will be b.**
n=input('enter the key for encryption:');
r=dec2bin(n,8);
Step 3: Now encrypt the message signal with the generated PN sequence so that it will be difficult for the hacker **to trace the original bits even if they had tracked the transmitted signal**
d=(s~=w);
Where "d" has the encrypted value.
Step 4: Embed the encrypted message with the carrier signal
s=dec2bin(z1(i),8);
s(7)=p1(i);
LSB bits in carrier have been replaced with message bits.
Step 5: Transmit the embedded carrier audio file at the transmitter. In the receiver side the reverse operation is carried out for recovering the secret message.
The main assumptions in the proposed method are,

- The secret and carrier audio files taken are strictly in .wav format.
- The carrier file should be eight times greater than the secret audio file.

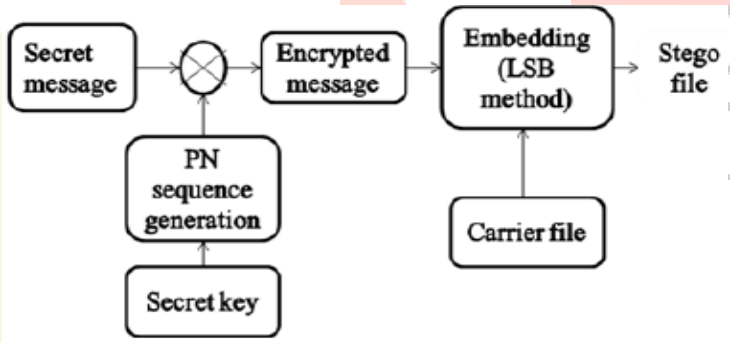

Figure 3 proposed steganographic approach at transmitter

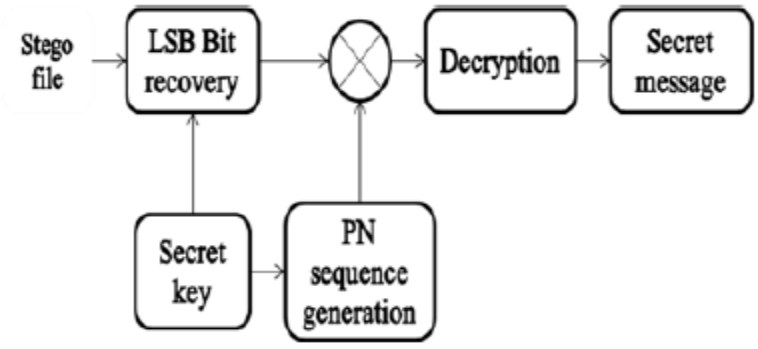

Figure 4 proposed de-steganographic approach at receiver

V. RESULTS

The carrier file should be strictly audio (.wav) file format and the secret message may be of audio (.wav) or text file. And here for our experimental scenario the carrier audio file is „*one.wav'* of 27.5 KB size and the secret audio file is „*hi.wav'* of 1.57 KB size. Thus the carrier file is eight times greater than the secret message file ensuring the assumptions made. The full details about the audio files. The secret text file chosen is „*rajeswari V'*. As per the proposed method a text file can also be embedded in the carrier audio file. Thus the chosen secret messages of audio or text files are embedded in transmitter side and are recovered at the receiver side as shown in the following figures. The simulation is carried out in MATLAB R2010a software.

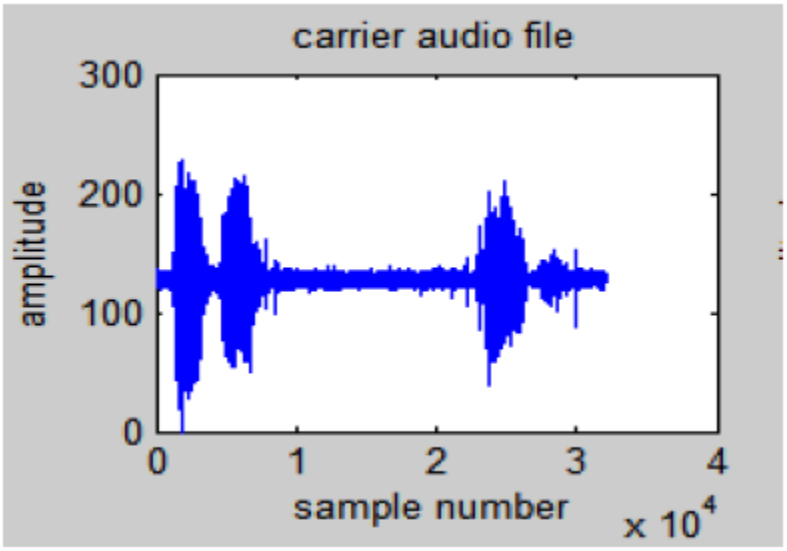

Figure 5: carrier audio file

Figure 5 shows the carrier audio file „bond.wav" representation. Figure 7 & 8 shows the secret audio and text file to be embedded in the carrier audio file. Figure 9 shows the stego audio file after embedding the secret audio file. Figure 10 shows the comparison of the carrier audio file and stego file. We can infer that there is no major difference in the

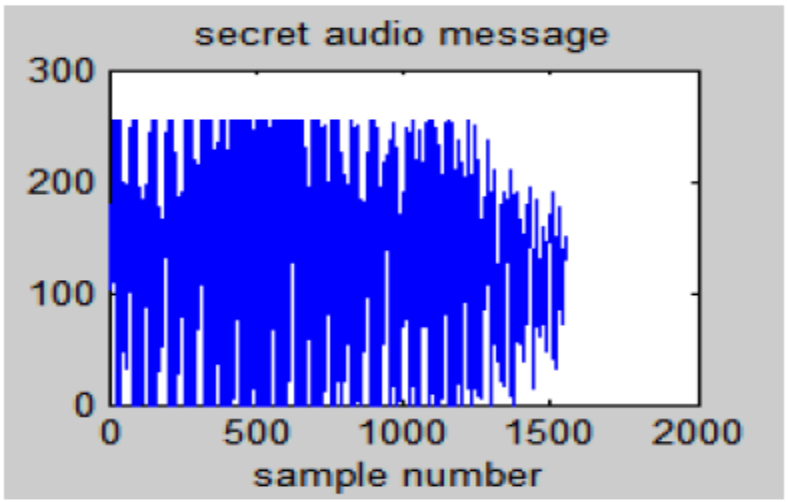

Figure 6: Secret audio file

VI.CONCLUSION

In this study, an audio steganalysis technique is proposed and tested. The objective audio quality measures, giving clues to the presence of hidden messages, are searched thoroughly. With the analysis of variance (ANOVA) method, we have determined the best individual features, and with sequential floating search (SFS) technique, we have selected features taking into account their intercorrelation. We have comparatively evaluated two classifiers, namely, linear regression and support vector machines. The SFS feature selection coupled with SVM classifier gave the best results. The output of the classifier is the decision whether the tested document carries any hidden information or not. The proposed method has been tested on four different watermarking and two steganographic data hiding techniques, first individually, and then in combinations. Experimental results show that the proposed scheme achieves satisfactory results, in that, in individual tests we achieve almost perfect detection except for the DCTwHAS watermarking method. In combination tests, the results are promising, but need to be improved. In this respect, we are investigating new ways of obtaining segment averages of quality measures, for example, using the power mean or the maximum. We will also consider a combination of classifiers; each specialized on a subset of data hiding methods.

VII. ACKNOWLEDGEMENTS

We authored this paper on secuirty transfer meaasges, with the support of my external guide, Mr.Rambabu M Assistant Professor, KG Reddy College of Engineering & Technology. We thank full to our HOD Mr. M Saidi REddy, We are thankful to my chairman sir, K..Krishna Reddy garu for his support and Director Dr. Vahini Reddy, for their support and inputs.

BIBLIOGRAPHY

[1]. < http://technofriends.in/2009/07/13/steganography-how-to-hide-data-in-images-and-audio-files/>

[2]. “Steganography FAQ” - Aelphaeis Mangarae [Zone-H.Org] March 18th 2006 , http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

[3]. “Steganography : Reversible Data Hiding Methods for Digital Media “ – Andrew Tilley <http://www.comp.leeds.ac.uk/fyproj/previous-titles/bsc2002.html>

[4]. < http://www.snotmonkey.com/work/school/405/methods.html>

[5] Raja K B, Chowdary C R, Venugopal K R, Patnaik L M “A Secure Image Steganography using LSB DCT and Compression Techniques on Raw Images” 2005 IEEE International conference on session B-image signal processing.

[6] Hossein Malekmohamadi and Shahrokh Ghaemmaghami Reduced Complexity Enhancement Of Steganalysis Of LSB-matching Image Steganography” 2009 IEEE/ACS International conference on computer system and applications.

[7] Balagi R, Naveen G“Secure Data Transmission Using Video Steganography”, 2011 IEEE International conference on electro/information technology (EIT).

[8] Andrew D. Ker, “Steganalysis of Embedding in Two Least-Significant Bits” 2007 IEEE transactions on information forensics and security, vol. 2, no. 1, march 2007. [9] W. Mazurczyk and Jozef Lubacz, “LACK– a VoIP Steganographic Method”, Journal of Telecommunication System, Springer Netherlands, Dec., 2009.