ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Providing Security To Audio With Increased Hiding Capacity Using Cryptography & Steganography

Mr. Sanket. N. Wawale[#1], Prof. Arindam Dasgupta[*2]
[#]*Department of Information Technology, Amrutvahini College of Engg, Pune University*

Abstract— Due to research and new technologies it is possible to store and exchange information in different formats. Secret Information is a very important resource for any organization or individual person. Audio or sound medium is found to be used in many applications for providing security, voice commands, voice synthesis and entertainment. This project is an approach for providing security to audio information. This concept is based on Cryptography and Steganography. With the help of these two techniques, two levels of security is provided. Cryptography will convert the original audio in different form and Steganography will hide one audio file into other audio file. Generally LSB algorithm is used for steganography with single LSB. In this project for increasing the storage capacity the operation of Hiding are performed on 2 , 3 and 4 LSB bits.

Keywords— Cryptography, Information Hiding, Steganography and LSB

I. INTRODUCTION

Any person consists of information that can be used for identification or other personal use. Data which is related to individual or other available information, e.g. name, address, telephone numbers, personal email addresses, date of birth, bank and payroll details, passport particulars, images, etc. Personal Data and Commercial data both can be in Audio form due to advanced technology and multimedia. Personal data that may be related to any system or individual such as audio Password, audio commands, etc. Commercial data, such as audio sound tracks for entertainment purpose. Only allowing access to intended user and avoiding unintended access is a very difficult task. This Project is an approach for providing security for audio information. Unauthorized users may be harmful because they may try to reduce the effectiveness or take control of valuable resources by taking advantage of loop holes or drawbacks of these resources. For hiding secret information, there are number of different steganography techniques [6][9]. Users of computer and internet want to exchange their confidential information or data , but they want to achieve this in a secure manner so that unauthorized person should not gain access to their data or even if someone gets that data, it will be difficult for that person to recognize and fetch out information. One of the possible solutions as cryptography to encrypt or decrypt data and steganography to hide data in different carrier media files like image, audio, video, etc.

II. LITERATURE SURVEY

Steganography consist of study and science of hiding communication and important data. A steganography system puts secret content in some part of cover media so that an unauthorized user should not be able to track or identify that their is secret data. Today technology provide efficient and easy to use communication channels and storage for steganography [1]. There are different techniques used for hiding secret data. One of the popular technique is Least Significant Bit algorithm. In this technique the LSB bit is used to hide the secret contents. The information hiding is done in a steganography system by identifying a cover medium's data bits that are repeated (those that can be modified without affecting that medium or distorting it). The embedding process creates a stego medium by replacing these bits with data or message [7]. The objective of steganography system is to keep the presence of the message undetectable from an unauthorized access.

A. Information-Hiding System Features

Any information hiding system is based on three aspects capacity, security, and robustness. *Capacity* is concern about the amount of information that can be hidden in the cover medium, *Security* refers to an unauthorized users inability to detect hidden information, and *robustness* refers to the amount of modification the stego medium can handle before showing any negative effects or destroy secret information [5].

B. Related Work

1) *Audio Cryptography:*- In this method the audio data is divided into two or more parts called as shares. Each single part does not convey any meaningful information, but when all parts or shares are combined together they will reveal the original audio data [2]. Pros- If any unauthorized user plays one part in an audio player, he or she will only hear meaningless hiss sound, or irritating noise sound. But when all parts are mixed and played together, i.e. using an audio editor, the original audio comes back.

2) *Echo Hiding:*-An echo is generated and added in a signal by manipulating the parameters (initial amplitude, decay and offset) such that the echo is not audible. If we consider a signal f(t), an echo f(t-dt), with some delay can be added to produce the stego signal s(t)=f(t) + f(t-dt) [3].

III. TWO LEVELS OF SECURITY

This system uses Two levels for providing security, so that it should not be easy to detect or access the sensitive data.

A. Cryptography

Cryptography is the process of making or converting sensible data into a different form.

B. Steganography

Steganography is the process of Hiding the data into another media file.
Steganography and Cryptography are two different techniques. Cryptography involves converting the message so as to make it meaningless to unauthorized people who had tracked or received it. In cryptography, the system is not broken unless the unauthorized user can read the secret message. Breaking a steganographic system needs the unauthorized user to detect that steganography has been used and he is able to read the embedded message. Steganography provides a means of secret communication, which cannot be removed without changing the data in which it is hidden [10]. The security of steganography system depends on the strength of the data encoding system. Using Cryptography and Steganography together provides an approach for adding multiple layers of security. By combining, the data encryption can be done by using certain technique and then hide the cipher text in an audio media. Using these two methods will increase the security of the secret data. The requirements such as capacity, security and robustness for secure data transmission and storage can be fulfilled by using these two techniques together [8].

IV. PROPOSED SYSTEM

This system uses XOR operation for cryptography. And Modified Least Significant Bit(LSB) algorithm for Steganography.

A. Least Significant Bit (LSB)

This system uses Multiple least significant bits(i.e 2, 3 or 4 LSB bits) in every sample of the cover file to hide a sequence of bytes containing the secret data . LSB coding is the simple way to hide information in a digital audio file by replacing the least significant bits of each sample with a secret message. The least significant bit (LSB) is the bit position in a binary integer giving the unit value similar to unit value in decimal. The LSB is also referred to as the right-most bit.

B. System Architecture And Modules

These systems consist of two main modules hiding and unhiding which contains sub modules. These submodules perform the task of hiding the MP3 audio file into a Wave file and extracting the original MP3 from the Wave file as shown in figure 1 and 6.

C. Hiding Section

1) Byte Extraction: This module provides the data from both the files (MP3 and Wave) in byte form (8 bits). The entire operation is performed at the bit level, so this module provides the data in bits form to other modules for processing.

2) Codeword Generation: The key entered by user is not used as it is for encryption. The key is converted to codeword. The codeword generator takes the key from user , performs operation on it and generates the codeword. The generated CODEWORD is given to Encryption module.

3) Encryption: This module converts the binary MP3 data into un-meaningful binary data. This is achieved with the help of CODEWORD. The Encryption module performs an XOR operation between original MP3 data and the CODEWORD generated as shown in figure 2.

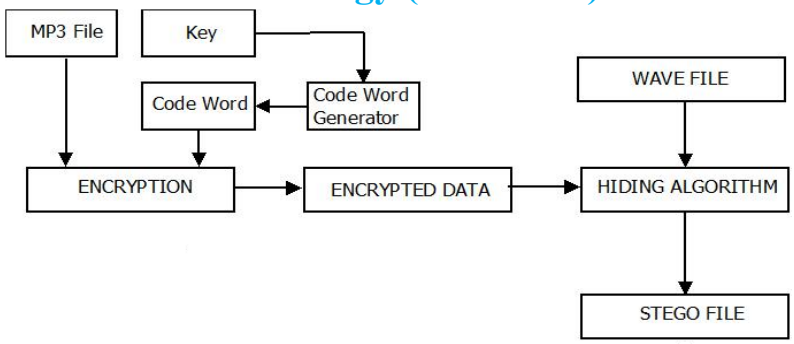

Figure 1: Hiding Process

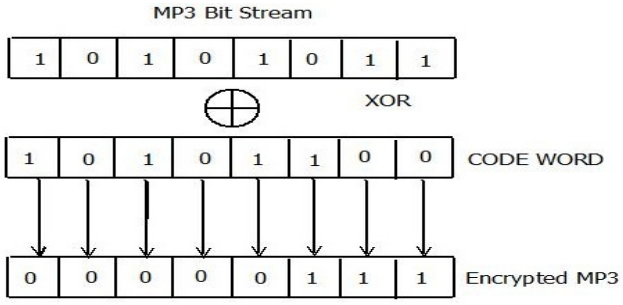

Figure 2: Encryption Using XOR Operation

4) Hiding: The function of this module is to hide the data. After the data is encrypted the hiding module hides the encrypted MP3 data in a Wave file. For this purpose a different versions of LSB algorithm is used. In this project different modes are defined as hiding in 2 LSB, 3LSB and 4 LSB. According to the mode being used, number of bits of encrypted MP3 will be hidden in every sample at LSB position's of the cover Wave file. After hiding all the Encrypted MP3 bits the hiding module generates a single Wave File but MP3 file is hidden in it.

a) *Hiding in 2 LSB of 16 bit file:-* In this mode two bits of secret MP3 data is made hidden in 2 LSB positions of every sample of Cover wave file as shown in figure 3.

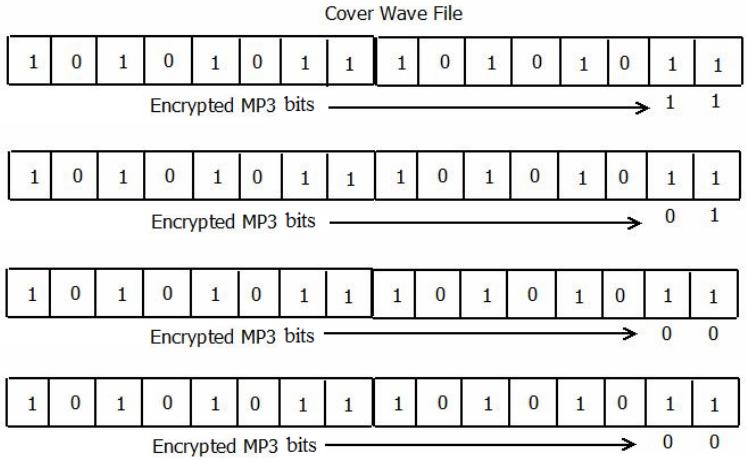

Figure 3: Hiding in 2 LSB bits of 16 bit file

b) *Hiding in 3 LSB of 16 bit file:-* In this mode three bits of secret MP3 data is made hidden in 3 LSB positions of every sample of Cover wave file as shown in figure 4.

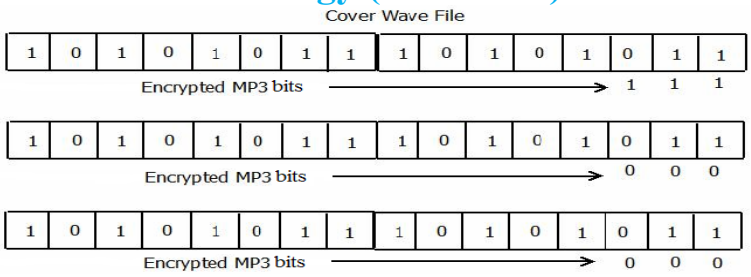

Figure 4: Hiding in 3 LSB bits of 16 bit file

c) Hiding in 4 LSB of 16 bit file:- In this mode four bits of secret MP3 data is made hidden in 4 LSB positions of every sample of Cover wave file as shown in figure 5.

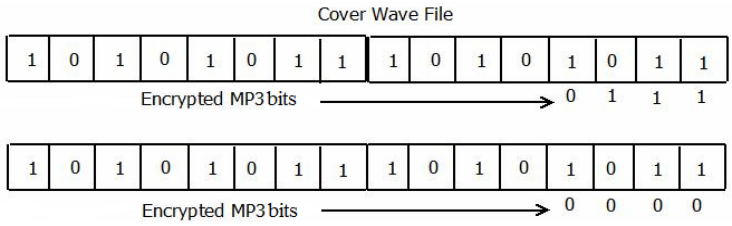

Figure 5: Hiding in 4 LSB bits of 16 bit file

D. Un-Hiding Section

1) Codeword Generation: For Decryption process also user needs to enter the key. Again key entered by user is not used as it is for decryption. The key is converted to codeword. The codeword generator takes the key from user , performs operation on it and generates the codeword.

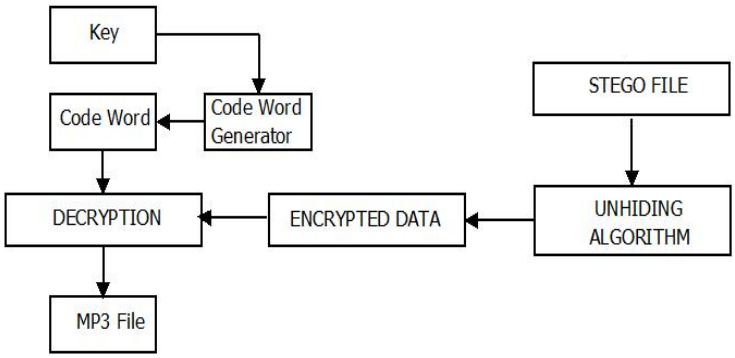

Figure 6: Un-hiding Process

2) Extraction Of Mp3: The function of this module is to extract the encrypted MP3 data from a WAVE file. This module uses a Reverse LSB algorithm to fetch out the MP3 Bits from a Wave File (Stego File). The extraction is based on the mode in which the data is hided i.e 2, 3 or 4 LSB.

3) Decryption: The function of this module is to construct the original MP3 data again from the encrypted MP3 data which has been extracted from the Stego Wave file. For this purpose generated CODEWORD is used. The algorithm performs XOR operation between the encrypted MP3 data and the CODEWORD generated. And the original MP3 file will be generated.

V. ALGORITHM

A. Hiding Algorithm

1. Start

2. Select the Mp3 file which you want to hide

3. Convert the Mp3 into its binary form

4. Get the key from user.

5. Convert key into CODEWORD.

6. Take byte of Mp3 and CODEWORD perform XOR operation between these two bytes.

7. Repeat Step 6 till the end of file.

8. Select the Wave file as cover File

9. Check wether mp3 file can be hidden into wave file.

10. If no then go to Step 8.

11. Else Convert the Wave file into Binary form

12. Replace LSB bits from byte of Wave file with bits of encrypted Mp3.

13. Repeat Step 12 till the end of Mp3 file.

14. Stop

B. Un-hiding Algorithm:

1. Start

2. Select the Stego file which you want to Un-hide.

3. Get the key from user.

4. Convert key into CODEWORD.

5. if CODEWORD is wrong then give Error " Cannot Proceed" and Go to step 12.

6. Extract LSB bits from byte of stego file and save them in memory.

7. increment the Byte pointer of Stego file.

8. Repeat Step 6 and 7 till the size of mp3 file has reached.

9. Take byte of encrypted Mp3 data and perfom XOR operation with the CODEWORD.

10. Repeat Step 9 till the end of Mp3 file.

11. Generate MP3 file.

12. STOP

TABLE I: TEST RESULTS : HIDING PROCESS

Sr. No	Cover Media (Input)	Cover Media Size	Cover Media Sample rate	Secret Message (Input)	Secret Message Size	StegoFile (Output)	Stego File Size
Test1 Hiding in 2 LSB	NFS1.wav	3,099 KB	44,100 Hz	Secret1.mp3	361 KB	Stego1.wav	3099 KB
Test2 Hiding in 3 LSB	NFS1.wav	3,099 KB	44,100 Hz	Secret1.mp3	361 KB	Stego1.wav	3099 KB
Test3 Hiding in 4 LSB	NFS1.wav	3,099 KB	44,100 Hz	Secret1.mp3	361 KB	Stego1.wav	3099 KB

TABLE II: TEST RESULTS : UN- HIDING PROCESS

Sr. No	StegoFile (Iutput)	Stego File Size	Stego File Sample rate	Recovered Mp3 file after Un-hiding	Recovered Mp3 file size
Test 4 Un-Hiding from 2 LSB	Stego1.wav	3099 KB	44,100 Hz	Decoded1.mp3	361 KB
Test 5 Un-Hiding from 3 LSB	Stego1.wav	3099 KB	44,100 Hz	Decoded2.mp3	361 KB
Test 6 Un-Hiding from 4 LSB	Stego1.wav	3099 KB	44,100 Hz	Decoded3.mp3	361

VI. RESULTS AND DISCUSSION

A. *Increase in Capacity*

The original Wave file before hiding the MP3 content and the Wave file after hiding the MP3 content (stego file) are having same size. The secret MP3 file was hided in Cover Wave file using different modes. (i.e 2, 3 and 4 LSB).

TABLE III: % INCREASE IN CAPACITY COMPARED TO SINGLE LSB

Sr. No	Cover Media (Input)	Data can be Hided	% Per Increase in Capacity
Hiding in 1 LSB	NFS1.wav 100 Samples	**100 bits**	-
Hiding in 2 LSB	NFS1.wav 100 Samples	200 bits	100 %
Hiding in 3 LSB	NFS1.wav 100 Samples	300 bits	200 %
Hiding in 4 LSB	NFS1.wav 100 Samples	400 bits	300 %

As shown by data in table and figure 7 if we take a wave file with 100 samples, by using traditional Single LSB algorithm we can hide only 100 bits. But by using our modified LSB algorithm the capacity of hiding is 200 bits(increased by 100%) in 2 LSB mode. The capacity is 300 bits (increased by 200%) in 3LSB mode and the capacity is 400 bits (increased by 300%) in 4 LSB mode. In all the three modes the stego wave file was played smoothly without any negative effects.

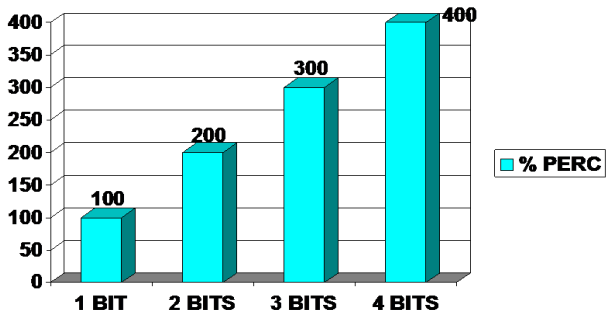

Figure 7: Increase in Capacity

B. *Signal to Noise Ratio*

TABLE IV: SIGNAL TO NOISE RATIO

Sr. No	Stego Media	Signal to Noise ratio (db)
Hiding in 1 LSB	Stego1.wav	96.32
Hiding in 2 LSB	Stego1.wav	86.78
Hiding in 3 LSB	Stego1.wav	79.42
Hiding in 4 LSB	Stego1.wav	72.8

As shown in table IV and figure 8 the Signal to Noise ratio decreases as we hide the data in different modes i.e 2 , 3 and 4 LSB. The Signal to Noise ratio is maximum i.e. 96.32 db while hiding in Single LSB. As we move forward to hide in 2, 3 and 4 LSB, the Signal to Noise ratio decreases. But it is important to note that even if the Signal to Noise ratio decreases with 2, 3 and 4 LSB , the stego file when played does not show any negative effects or distortion and is played smoothly. The Stego file that is

generated is having the same quality as that of original Cover wave file. The MP3 file generated after un-hiding process is having the same quality and same size as that of an original MP3 file before hiding.

The Cover wave file with different sample rates were used for testing purpose. But their were no any adverse effects due to change in sample rate. Increase in sample rate further increases the capacity of hiding secret data. The original MP3 can be securely and properly extracted from the stego file.

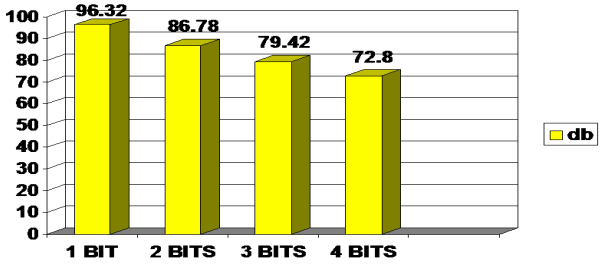

Figure 8: Signal to Noise Ratio in db

VII. CONCLUSION

A different approach is introduced through this project for securing audio data. This technique has been used to meet information hiding system features like robustness to attacks, the data-capacity of the cover media and the inability of un-authorized user to detect the secret data which can be used in various applications. More data can be hided using multiple LSB bits of a wave file without any negative effects.

ACKNOWLEDGEMENT

This work is implemented under the guidance of Prof. Arindam Dasgupta. His active guidance and valuable suggestion at every time encouraged me to carry out the same.

REFERENCES

[1] Abikoye Oluwakemi C, Adewole Kayode S. , Oladipupo Ayotunde J. December 2012 – "*Efficient Data Hiding System using Cryptography and Steganography"* International Journal of Applied Information Systems (IJAIS) ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4 No.11.

[2] Amresh Nikam, Poonam Kapade, Sonali Patil. 2010-*" Audio Cryptography: A (2, 2) Secret Sharing for Wave File"*. International Journal of Computer Science and Application ISSN 0974-0767.

[3] Dr D Mukhopadhyay, Fellow A Mukherjee, S Ghosh, S Biswas, P Chakraborty. November 2005. *" An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography"*- IE(I) Journal-CP-Vol 86.

[4] Jayaram P, Ranganatha H. R, and Anupama H. S. 2011. " *Information Hiding Using Audio Steganography – A Survey"*. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[5] Lin T. and Delp J, "*A Review of Data Hiding in Digital Images,"* Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278, 1999.

[6] Mohammad A. A, and Abdelfatah A. Y. 2010. " *Public-Key Steganography Based on Matching Method*". European Journal of Scientific Research, 40(2). ISSN: 1450-216X. Euro Journals Publishing, Inc., pp. 223-231.

[7] Niels P, and Peter H, 2003," *Hide and Seek: An Introduction to Steganography"*. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.

[8] Raphael A. J, and Sundaram V. 2011. " *Cryptography and Steganography - A Survey"*. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[9] Sujay. N, and Gaurav P. 2010. *" Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions"*. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.

[10] Vivek. J, Lokesh. K, Madhur. M. S, Mohd. S, and Kshitiz Rastogi 2012. " *Public-Key Steganography Based on Modified LSB Method*". Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.