Analysis of Affine and Hill Cipher method using Audio Steganography

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted by

Yashika Garg

(Roll No. 801533016)

Under the supervision of:

Dr. Rajiv Kumar

Assistant Professor

Dr. Anil Kumar Verma

Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147001

JULY 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Analysis of Affine and Hill Cipher method using Audio steganography ", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Information Security submitted in Computer Science and Engineering of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Rajeev Kumar & Dr. Anil Kumar Verma and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any degree of this or any other University.

Yashika

(Yashika Garg)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Rajeev Kumar)

Assistant Professor, CSED

(Dr. Anil Kumar Verma)

Associate Professor, CSED

ACKNOWLEDGEMENTS

I am truly thankful to my advisor Dr. Rajiv Kumar and Dr. Anil Kumar Verma whose encouragement and guidance at every step enabled me to develop an understanding of the subject. I am grateful for his patience, time and support that they showered on me throughout the length of my research.

I am equally thankful to the entire faculty members of CSED for their direct and indirect help and cooperation.

Last but not least, I would like to thank my parents and friends for their encouragement and support. They have always wanted the best for me and I admire their determination and sacrifice.

Above all, I would like to thank the Almighty for the kindness who blessed me during this journey.

(Yashika Garg)

ABSTRACT

As the internet growing day by day secure transmission of data is very crucial. Steganography and Cryptography together helps us to provide data confidentiality and helps to protect the data from day by day attacks. So, the communication must be secretive as well as secure. In the proposed work, a comparative analysis of Affine and Hill Cipher method for Audio steganography using LSB (Least Significant method). Affine and Hill cipher are compared to each other on the basis of various factors such as Time Taken to embed the information, Frequency representation, PSNR, MSE etc.

Keywords- Audio Steganography, LSB (Least Significant Bit), PSNR-Peak signal to noise ratio, MSE-Mean Square error, Affine cipher, Hill Cipher

TABLE OF CONTENTS

CERTIFICATE i

ACKNOWLEDGEMENTS ii

ABSTRACT iii

TABLE OF CONTENTS iv

LIST OF FIGURES vii

LIST OF TABLES ix

ABBREVIATIONS x

CHAPTER 1

INTRODUCTION 1

1.1 Overview 1

1.2 Motivation 2

1.3 Cryptography 2

1.3.1 Authentication 2

1.3.2 Confidentiality 3

1.3.3 Integrity 3

1.4 Cryptosystem 4

1.5 Types of cryptography 5

1.5.1 Symmetric key cryptography 5

1.5.2 Asymmetric key cryptography 5

1.6 Cryptographic techniques 6

1.6.1 Affine cipher 6

1.6.2 Hill cipher 7

1.7 Audio steganography 8
1.7.1 Least Significant Bit 8
1.7.2 Echo hiding 10
1.7.3 Parity coding 10
1.7.4 Phase coding 10
1.7.5 Spread spectrum method 11
1.7.5.1 Frequency hoping spread spectrum 11
1.7.5.2 Direct sequence spread spectrum 11

CHAPTER 2

LITERATURE SURVEY 12

2.1 Information hiding using LSB method 12
2.2 Combined strength of steganography and cryptography 14
2.3 Using genetic algorithms 17
2.4 Using discrete wavelength transform method 18
2.5 Using noise gate software logic 19
2.6 AVIS system 19
2.7 Hybrid spread spectrum method 19
2.8 Using cepstrum modification 20
2.9 Using modulo operator 20

CHAPTER 3

RESEARCH PROBLEM 21

3.1 Problem statement 21
3.2 Research gaps 21
3.3 Research objectives 22

3.4 Research methodology…….22

CHAPTER 4

AUDIO STEGANOGRAPHY USING CRYPTOGRAPHY 24

4.1 Encryption process 25

4.2 Embedding process using LSB method 26

4.3 Decoding process 27

4.4 Decryption process 27

CHAPTER 5

EXPERIMENTAL RESULTS 29

5.1 Experiment 1 29

5.2 Experiment 2 33

5.3 Experiment 3 35

CHAPTER 6

CONCLUSION AND FUTURE SCOPE 39

REFERENCES 40

APPENDIX A

PUBLICATION 44

APPENDIX B

VIDEO PRESENTATION LINK 45

APPENDIX C

PLAGIARISM REPORT 46

LIST OF FIGURES

Figure No.	Title of Figure	Page No.
Figure 1.1	Steganography system scenario	2
Figure 1.2	Absence of authentication	3
Figure 1.3	Loss of confidentiality	3
Figure 1.4	Loss of integrity	4
Figure 1.5	Cryptosystem	4
Figure 1.6	Symmetric key cryptography	5
Figure 1.7	Asymmetric key cryptography	6
Figure 1.8	Message is encoded using LSB	9
Figure 1.9	Parity coding method	10
Figure 1.10	Phase coding method	11
Figure 4.1	Proposed system design	25
Figure 4.2	Encryption process	26
Figure 4.3	Embedding ciphertext	27
Figure 4.4	Decoding process	27
Figure 4.5	Decryption process	28
Figure 5.1	Displaying the GUI of proposed work	30
Figure 5.2	Selecting the audio file for embedding process	30
Figure 5.3	Selecting the text file	31
Figure 5.4	Text is hidden confirmation using affine cipher	31
Figure 5.5	Cover signal representation	32
Figure 5.6	Encoded signal using affine method	32
Figure 5.7	PSNR and MSE values of cover signal	32
Figure 5.8	PSNR and MSE values of encoded signal using affine cipher	33
Figure 5.9	Hiding the text using hill cipher	33
Figure 5.10	Text is hidden confirmation using hill cipher	34
Figure 5.11	Encoded signal using hill cipher	34

Figure 5.12 PSNR and MSE values of encoded signal using hill cipher 35
Figure 5.13 Frequency representation of cover signal 36
Figure 5.14 Frequency representation of encoded signal using affine cipher 36
Figure 5.15 Frequency representation of encoded signal using hill cipher 37

LIST OF TABLES

Table No.	Title of Table	Page No.
Table 5.1	Shows PSNR, MSE, Time taken(secs) before and after embedding using affine cipher	37
Table 5.2	Shows PSNR, MSE, Time taken(secs) before and after embedding using hill cipher	37
Table 5.3	Comparison table	38

ABBREVIATIONS

DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest-Shamir-Adleman
VPN	Virtual Private Network
LSB	Least Significant Bit
SNR	Signal to Noise Ratio
TTP	Trusted Third Party
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
ST	Statistical Technique
EXE	Executable File Cover
GA	Genetic Algorithm
HAS	Human Auditory System
HVS	Human Visual System
VAMI	Value Based Multiple Insertion
DSSS	Direct Sequence Spread Spectrum
BPSK	Binary Phase Shift Keying
FFT	Fast Fourier Transform
SVM	Support Vector Machine

VADDI	Voice Activity Detection Dynamic Insertion
AVIS	Advanced VoIP Steganography System
HLLAS	Higher LSB Layer Based Audio Steganography

CHAPTER 1

INTRODUCTION

1.1 Overview

Internet communication is the essential part of the communication now a days. Data needs to be very secure when transferred over the network. So, we can secure the data by applying the various cryptographic techniques and can increase the confidentiality of the data and steganography is proposed to provide the more security to the information. The digital information can be edited. Further, when such digital information is to be transmitted on a network, the unauthorized access and the ownership of the document needs to be protected. This yields the biggest security concern from the past few years. The approach to minimize such attacks is to convert the digital information into some other format in which the output information be precise for those having right to access that information which is generally covered in cryptography. By combining steganography and cryptography we can add security to the information to be transmitted over the public network.

Steganography paves a way to handle such serious concerns. This idea has been increasingly used in the past few years. The word steganography means the hidden words. The information is transmitted securely and cannot be detected by any hacker. Steganography is a successive approach that provides a potential security and lawful information hiding. After the embedding of text is being done, the stego audio is obtained by various steganographic methods. At the receiver side, the hided text can be obtained from the audio signal used while hiding it using the reverse algorithm as that of used for embedding the information.

Communication is the exchange of messages or important information as by writing or speech. So, secure communication is needed and their exists a many tools for secure transmission of secret information. For secure transmission, if we send compressed form of messages this will result in secure and powerful system. Main objective is to make data so secure so that no one can decrypt it.

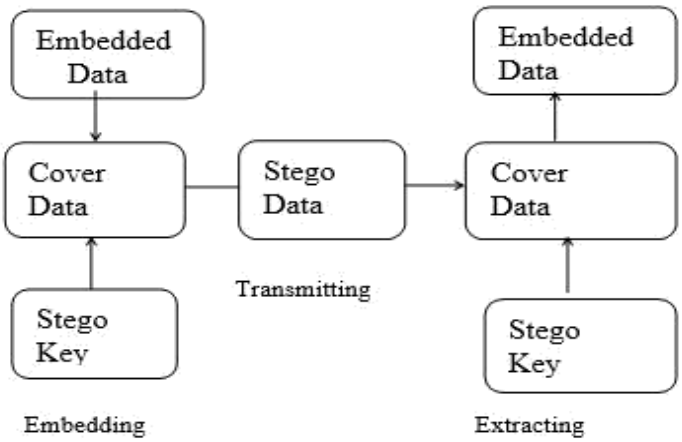


Fig 1.1: Steganography system scenario

1.2 Motivation

This topic was selected due to keen interest in security field. Security of information is taken as the base theme. Most of the researchers select one base theme and shrink their research into various sub topics. Integrity of secret information can be achieved by combining steganography and cryptography together.

1.3 Cryptography

Cryptography is the art of achieving the security to make the data secure by encoding to make it non – understandable form so that no third party can identify it. There are various goals of cryptography as follows-

1.3.1 Authentication

Authentication is the act of confirming the truth of a single piece of information claimed true by the entity. It is process of actually confirming the identity of person to whom the information is being communicated over the public network(Saurabh *et al.* [3]). For example- user C posing as user A, sending a request of funds transfer from A's account to C's account to be done by bank B, Bank will think that it's the A sending the request to transfer the funds and might transfer the funds happily as shown in Fig1.2 below

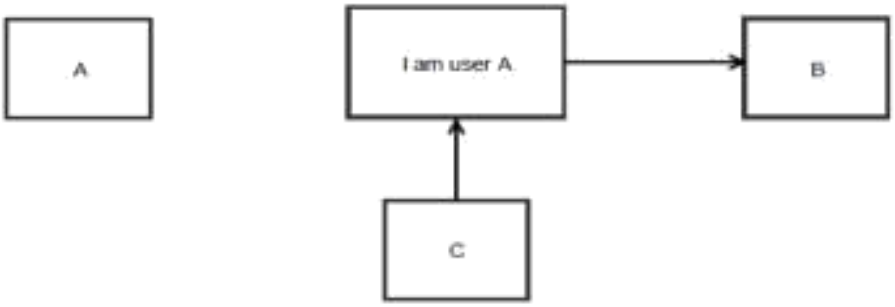


Fig 1.2: Absence of authentication

1.3.2 Confidentiality

It's about the protection of the information from the unauthorized access. So, to do so encryption of messages is used. Confidentiality gets generally compromised if the attacker is able to access the contents of the information. For example – Suppose some secret message is sent by A to B , but it is received by C without the permission of A and B shown as below-

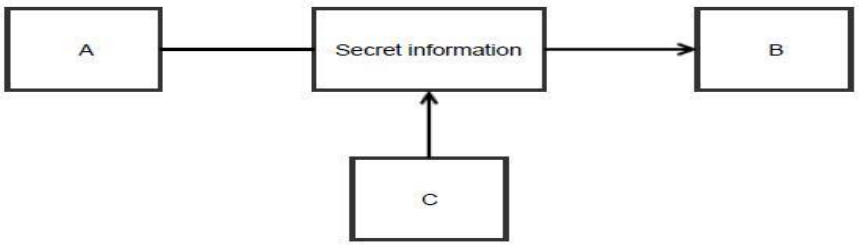


Fig 1.3: Loss of confidentiality

1.3.3 Integrity

The assurance that the information received is exactly as sent by the authorized entity so that it contains no modification, no data is inserted and no data is deleted from the information being sent(Fatima *et al.* [4]). Data integrity is achieved by the following some rules, by playing the check values. For example – Here user C tampers the message

originally sent by the user A and send the tampered message to user B shown in Fig1.4 below-

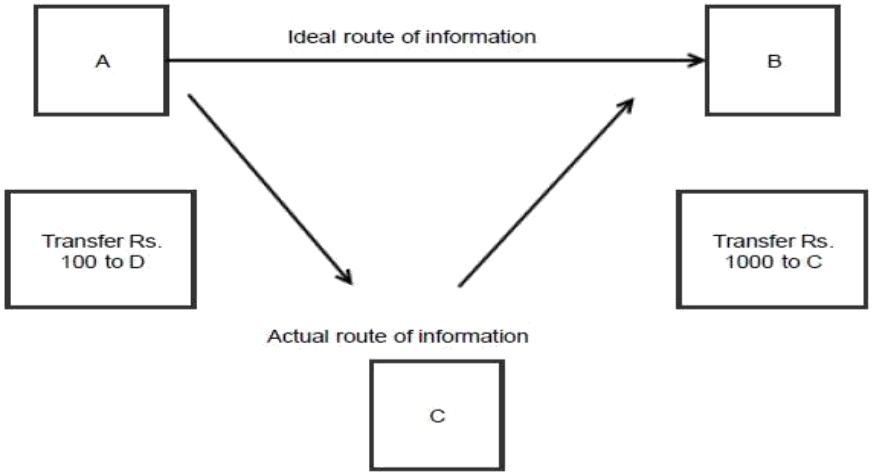


Fig 1.4: Loss of integrity

1.4 Cryptosystem

In cryptography, encryption is the process of changing the information using the algorithm in such a way it becomes difficult for the attacker to understand it except those possessing the secret information. The reverse process to get back to the original information is called decryption. The information transferred in the meaningless form is called Plain text. The unreadable or meaningless form is called cipher text. Algorithm which is used for transforming plain text to cipher text is called as key.

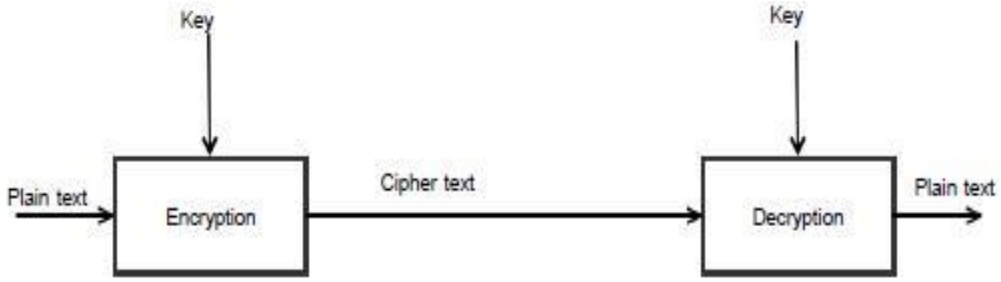


Fig 1.5: Cryptosystem

1.5 Types of Cryptography

There are mainly two types of cryptography: Symmetric key cryptography and Asymmetric key cryptography described as below-

1.5.1 Symmetric key cryptography

This is often called as Secret key cryptography or Private key cryptography. Symmetric key algorithms under cryptography use the same keys for encryption of plain text and decryption of cipher text (Fatima *et al.* [4]). These keys share the secret between the two parties. Symmetric-key encryption provides secrecy when two parties communicate with each other.

An adversary who interprets the information should not get any insignificant information about its content. If the same key is used for encryption and decryption process we call it symmetric key cryptography. For example – DES, AES.

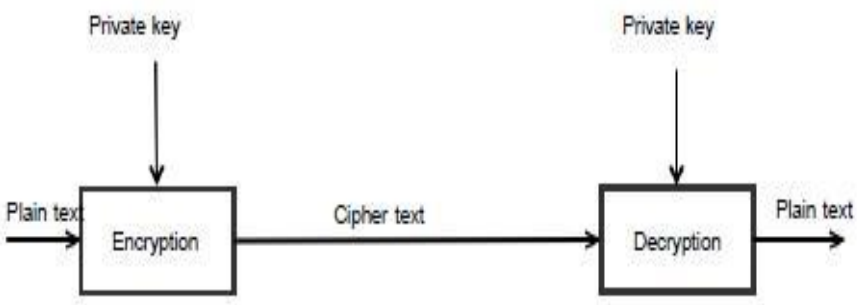


Fig 1.6: Symmetric key cryptography

1.5.2 Asymmetric key cryptography

This is known as Public key cryptography. It is cryptographic system requiring the two different keys one to encrypt the plain text and the other key to decrypt the cipher text. In the asymmetric (public key) sender makes use of the public key to transmit the information and receiver use the private key held secret by A to decrypt the information.

Asymmetric key cryptography solves the problem of key agreement and key exchange. If two different keys are used in a cryptographic mechanism, we call it asymmetric key cryptography. It can be used for encryption and decryption as well as for digital

signatures. The great advantage of asymmetric ciphers is that a shared secret key does not have to be exchanged over an insecure medium such as the public Internet. For example – RSA algorithm

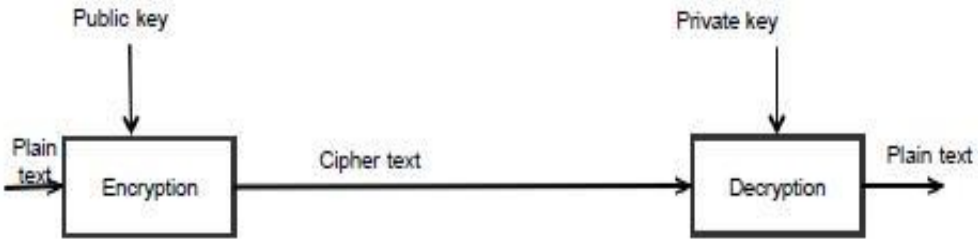


Fig 1.7: Asymmetric key cryptography

1.6 Cryptographic Techniques

Cryptography is one of the essential technologies used in building a secure VPN. Data confidentiality may be provided by one of two categories of encryption algorithm, namely symmetric cryptography and asymmetric cryptography. Different applications of the same basic algorithms can provide both encryption that keeps data secret and authentication. In order to encrypt and decrypt the information, some cryptographic techniques widely used are described as below-

1.6.1 Affine Cipher

Affine cipher is a type of substitution cipher. Affine ciphers are far secure and can be applied to the system to make more secure (Artz *et al.* [17]). To set up the affine cipher, generally we consider the two values x and y and then set €(m) = xm + y mod 26.

Decryption of the cipher text obtained while implementing the Affine cipher will be similar to the encryption process.

The decryption formula is as follows-

$$\delta(m) = x{-}1\ (m - y) \bmod 26 \qquad (1)$$

1.6.2 Hill Cipher

Hill cipher is poly-alphabetic cipher used to encrypt the information by making use of the matrices (Acharya *et al.* [27]). The cipher key consists of k*k square matrix, larger are the dimensions of matrix more secure the information will be.

The purpose of the Hill cipher is to put the letters of data into the k*k square matrix and each block of the information letters are converted into the column matrix of integers with respect to the alphabets being chosen and then multiplied by the k*k key matrix.

The result obtained is converted back to the alphabets and thus obtaining the cipher text.

Due to high complexity for working with the larger size matrices, we generally stick to the 2*2 key matrix

[w x]

[y z]

that is the invertible modulo 26 and where det(A) = (wz – xy)

To decrypt the information hided using Hill cipher-

The decryption formula is as below-

$A-1 = [\det(A)]-1*[z\ -x]\bmod m$

$[-y\ w]$

Then multiplying the cipher text matrix with the inverse of original key matrix, thus obtaining the original text.

1.7 Audio Steganography

It involves hiding the data in the audio files. This method hides the data in MP3 files. It is the technique used for transmitting the hidden information by modifying the audio signal in an imperceptible manner. The secret message before steganography and after applying steganography will have the same characteristics.

Different embedding techniques for Audio:

1.7.1 LSB (Least Significant Bit)

It is one of the data embedding method of the Audio steganography. Least significant bit is one of the easiest method to embed the data into the audio signal.

In LSB coding, the ideal transmission rate is 1 kbps per 1 kHz. In LSB, the particular bits of the audio signal is replaced with the two data bits. This eventually results in increasing the amount of information to be encoded into the audio signal. But by doing so, it increases the resultant noise in the audio signal(Roy *et al.* [26]). So, before we embed secret information into the audio signal one should consider the number of samples present in audio signal.

To extract the hidden text from an LSB encoded audio signal, one needs to have access to sample bits in which the text has been hided. Normally, while hiding the data into the audio signal the secret data to be encoded is smaller than the audio sample bits. The important part is to choose the sample bits in which the secret information is been hidden and communicated over the network so that it can reach the receiver safely.

LSB method provides a very high watermark channel bit rate, if only one LSB of cover signal is used giving the capacity of 44.1 kbps and very low complexity. The common drawback of this process is that it provides very low robustness while embedding data into the audio signal.

As the number of LSB's increases during LSB encoding process, the depth of LSB layer becomes larger, the chances of the secret information to be detectable by the attacker increases. So, there should be limit for the LSB layer to be used for data

embedding in each audio sample. To minimize this distortion, 16 bits per sample LSB layer is used for audio signal embedding.

LSB technique is one of the easiest methods to hide the crucial information in the digital audio signal. LSB method allows for a large amount of information to be embedded in the audio signal by replacing the least significant bits of the digital audio file with the binary information. In some of LSB implementations done so far, two LSB of the signal is replaced with the message bits. This technique results in increasing the amount of data to be encoded in the audio signal but increases the noise in audio signal. To recover the text information hidden in the LSB audio signal one needs to have access to the sequence of sample used for performing the embedding. (Roy *et al.* [26]).

This method has many advantages such as it is one of the easiest method for hiding information in the audio file. It allows the large amount of information to be embedded in the audio file, it gives the capacity equivalent to the sampling rate that could vary from 8 kbps to 44.1 kbps if only 1 lsb of the original audio signal is used, it provides low robustness against the attacks as the drawbacks.

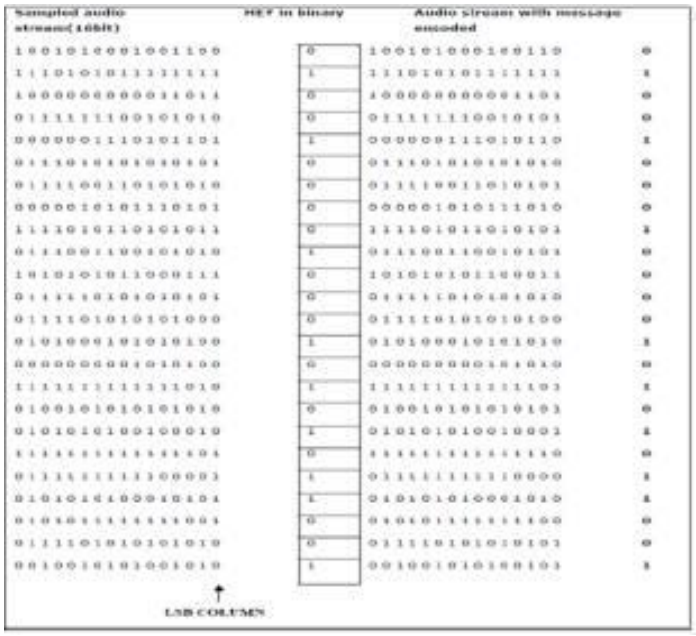


Fig 1.8: Message is encoded using LSB method

1.7.2 Echo Hiding

It inserts the secret data in a audio document by bringing the echo in the discrete audio signal(Othmani *et al*.[34]). In this technique a single bit of secret information could be encoded if just a single resound was created from the first signal.

This method having advantages as it is resilient to the lossy data compression algorithms used in this method. it provides low security and capacity as the drawbacks.

1.7.3 Parity Coding

It breaks the cover audio signal into many areas and then information is encoded in the parity bit. If the parity does not matches, LSB of one of the samples is adjusted to get the required parity(Othmani *et al*.[34]).

This method has advantages as in this, there are more choices for the sender to encode the secret bit. it provides no robustness as the drawbacks.

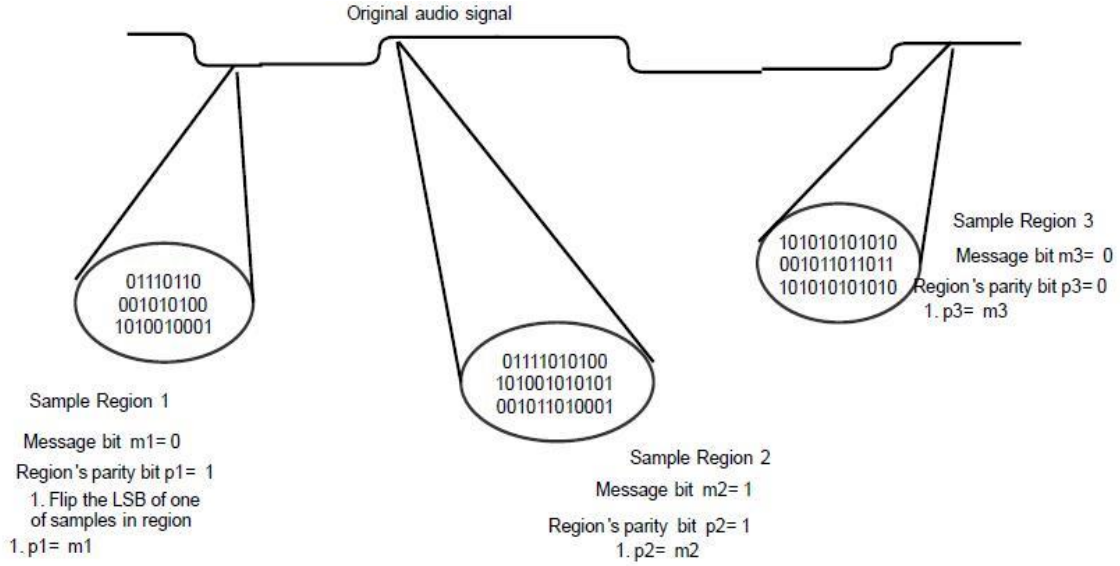


Fig 1.9: Parity coding method

1.7.4 Phase Coding

In this technique the initial audio segment phase is replaced with the phase which represents the secret information hided in it called as reference phase (Othmani *et al*.[34]). The phase of the remaining segments are adjusted to make relative phase

between the segments, Phase coding comes in category of best methods for information hiding using the audio steganography.

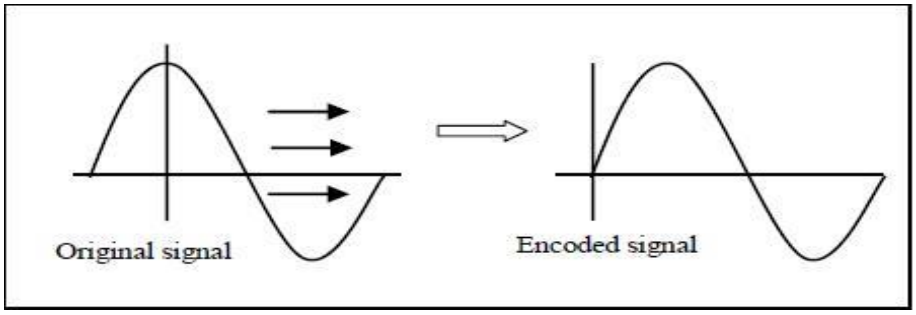


Fig1.10: Phase Coding

1.7.5 Spread Spectrum

The spread spectrum method tries to spread the data across the frequency spectrum of audio signal. Spread spectrum method provides the better performance in some areas compared to other methods such as LSB method, Parity coding, Phase coding(Othmani *et al*.[34]). It also provides the better robustness against the various removal techniques. There are two types of spread spectrum technique:

1.7.5.1 Frequency hoping spread spectrum

It is often called as FHS method. It is the method of transmitting the radio signals by rapidly switching the carrier among the various frequency channels using the known by both the sender and the receiver. It can minimize the effects of unintentional interference.

1.7.5.2 Direct sequence spread spectrum

It is often called as DSS method. It is the type of spread spectrum technique used to reduce the overall interference of signal. Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. The noise signal is pseudorandom sequence of 1 and - 1 values.

Spread spectrum method having advantages as it provides the high robustness against the removal techniques. it can introduce the noise in the audio signal, it is vulnerable to time scale modifications as the drawbacks.

CHAPTER 2

LITERATURE SURVEY

In this chapter, a brief literature survey on the topics included in this work is presented.

2.1 Information hiding using LSB method

Udham Singh [18] explained exactly how LSB embedding is done and the capacity of technique used in this work. To recover the hidden secret information hided in the audio signal, receiver follows the same approach used while embedding the secret information. The length of the information to be embedded in the audio signal should be generally smaller than the number of samples in audio signal. Before embedding the information one must decide on how to choose the number of sample bits in the audio signal that will contain the hidden information.

Cvejic *et al.* [31] proposed a enhanced LSB technique which was applied on .wav sample. In this, random bits were selected to embed the secret information into audio signal. This method resulted in more security and robustness. The basic idea of the proposed work is watermark embedding that results in minimal embedding distortion of cover audio signal. Using the two-step algorithm proposed in this work, watermark bits are embedded into higher LSB layers, which will result in increased robustness against the noise addition.

Bhasker *et al.* [21] proposed a new proposal of submission techniques related to audio steganography. While using genetic algorithms, secret information is embedded into higher (Least Significant Bit) values based on a algorithm that embeds the information into the deeper layers of LSB which results in more robustness. The increased robustness will be beneficial against the various attacks that tries to extract the secret information embedded into the audio signal. Integrity, robustness and security of system are maintained using this method as the information is not under the possibility of any security attacks.

Ballesteros L *et al.* [22] presented the technique in which consecutive LSB's of audio signal is replaced with the secret information. LSB is one of the easiest method for embedding data into the audio signal but only disadvantage of this method is that it does not provide more robustness for the system. It also provides the comparison of original audio signal spectra before embedding the information and after embedding the information and then compare the results by using the various audio samples having different specifications.

Basu *et al.* [6] presented a technique in which sampling of audio signal is done and then further alters the appropriate bit of each sample with the text information. The steganographic technique is to be applied in such a way so that the host audio signal quality is not degraded. A procedure for embedding the information is done in such a way, information field is first edited to embed information into the audio signal. Before proceeding with proposed work, audio signal header was checked because the small change in the header section can corrupt the whole audio signal.

Asad *et al.* [16] proposed a three layer model based on audio steganography based on least significant bit replacement. The secret information is first passed through the two layers before embedding the message in the third layer. The hidden message is recovered from the network and the secret information is recovered by applying the reverse operations. The main purpose of proposed work is to maintain the confidentiality of information. The first layer converts the characters of secret information into the bits to increase the capacity caused by the compression. The second layer encrypts the secret information, changes the secret information into some other form so that attackers cannot get easily access to the information. The third layer embeds the encrypted information into the cover message. And, then transmits the secret information over the public network. By changing the information into some other format increases the robustness of the system. The receiver extracts the stego data from the public network using the three layers in reverse order.

Sharma *et al.* [28] proposed the random key indexing method to replace the LSB's of the carrier audio signal with the secret information. Primary key performs the bit

replacement between the audio signal and the secret information which is provided by TTP and secondary key will be generated while the embedding process at the encoder side. Secondary key is transferred at the receiver side for extracting the secret information. This proposed work has been tested at the various 16 bit and 32 bit stereo wave files with the various different payloads.

M. Nasef *et al.* [24] proposed a technique for Embedding and Extraction process. In this, three random keys is been used to maximize the robustness of LSB method. The first key used is for embedding the type of secret information "audio or video or text", the second key embeds the secret information. The third key skips some bits resulting in increased robustness of LSB method. This method also provides the comparison for SNR ratio.

Mean square error, often called as MSE measures the distortion in the audio signal. It measures the square of the error between the original audio signal and the encoded audio signal

Peak signal to noise ratio, called as PSNR is the ratio between the maximum possible power of audio signal and power of noise in audio signal.

PSNR is most easily easily defined by the Mean Square Error(MSE). MSE and PSNR(in dB) is defined as follows, given a noise free m*n monochrome image I and its noisy compression K

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20 \cdot \log_{10}\left(\frac{MAX_I^2}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

2.2 Combined strength of steganography and cryptography

Gopalan [15] proposed a technique in which AES is been used for encryption. This encrypted information is further embedded into the audio signal. Then authors made use

of the Spread Spectrum method of audio steganography technique to embed the encrypted information before communicating it over the public network. In the proposed work, cryptography is combined with steganography to provide more security to information so that it can be transmitted safely without any risks of tampering attacks by the attackers in between the transmission phase. This results in providing more security to the system.

In this method, information bits are embedded into multiple LSB's. In this work, to improve the capacity of audio signal for embedding the information using two substitution techniques is been proposed. This method help to increase the capacity of audio signal so that more amount of information can be added to it. From the results found for this method, it improves the capacity of information hiding in the audio signals.

Bhowmick *et al.* [25] proposed a method providing information hiding using the encryption with audio steganography. They first encrypted the information using cipher techniques, the original plaintext is subjected to the classical Vigenere cipher followed by double column transposition., then audio file is also encrypted. Encryption is being carried out by the transposition which leads to scrambled audio file. This scrambling is carried out by BBS pseudo random generation algorithm. This process is repeated till the audio samples are exhausted.

Priyanka *et al.* [1] proposed a method to provide a more security to the information in which they first encrypted the text using the RSA encryption algorithm and then higher LSB layer of the audio signal is used for inserting the message bits. RSA algorithm is generally very difficult to break by the attackers. After the information is hided in the audio signal a new audio signal is generated containing the secret information. This way we get some new samples.

Fatima *et al.* [4] proposed a approach where DES is used for encrypting the information and then LSB method is used to embed the encrypted information into the audio signal. We used 16 sub keys in a row generated from the random key so that the information cannot be easily extracted. Before embedding the data into the audio signal, it is compressed so that more amount of information can be embedded into the audio signal Thus increasing the capacity for data hiding in audio samples.

Oluwakemi *et al.* [7] proposed a system for data hiding based on cryptography and audio steganography for the safe transmission of information between the source and destination. Audio wav file is used for steganography approach and data is embedded using LSB Method. For the cryptographic technique, Diffie-Hellman key exchange algorithm is been used. The presented work does the affect the size of the original audio signal after embedding of information. This method can be used with other audio formats as well. The encryption phase and decryption phase covered in this proposed work makes the system's security more robust.
This system can be recommended to the internet users for the secure transmission of the information over the public network.

Khan *et al.* [8] proposed a new approach for securing the crucial information from the attackers. To make the information more secure efficient algorithms is been used. Even if the attackers are able to trace the audio file containing the information but they will not be able to track the data present in the audio signal. AES algorithm is been used for encrypting the information before embedding it into the audio signal. After encrypting the information, it is embedded into the audio signal using spread spectrum technique of audio steganography method.

Verma *et al.* [11] As digital documents are very easy to copy so its becomes necessary to find a technique so maintain the accuracy and sensitivity of the information. Cryptography and steganography are considered as one of techniques for maintaining the integrity of the information. Authors proposed a technique using cryptography and steganography providing a double layer protection to the crucial information. First, the user enters the data followed by the sampling rate. Cipher is generated for encrypting the information and after the encryption process ASCII conversion of information takes place. Now, the input is been given by the user in the form of voice signal. Then Cipher generated and voice signal entered by the user are combined. This way, security of the system is increased.

Zaidan *et al.* [10] proposed a framework which makes use of both steganographic and cryptographic techniques for ensuring the security of the information. The approach

which makes use of AES and statistical technique computation. They further made use of EXE file as cover for the hidden information because it can more amount of information into it. As most of the antivirus systems now a days do not allow to directly write into the executable files. This results as the advantage to this system by not allowing the hidden information being disclosed by these systems. Executable files are not affected by the information hiding process and keeps on working normally.

Kanhe *et al.* [29] presented a new approach of audio steganography technique by randomly changing the embedding bits. Along with audio steganography technique AES algorithm is been used to provide the additional security to the system. To check the quality of the audio signals SNR and correlation coefficients is been calculated. Here, SNR is referred as the embedded information. SNR measures the noise present in the encoded cover signal. The proposed work has been tested over 10 people quality of speech and rated on a scale of 5. In the future, the proposed work will be tested for the lossy channels and according to that further modification will be done in the proposed technique.

2.3 Using genetic algorithms

Saurabh *et al.* [3] proposed a technique related to the problems of substitution technique of the audio steganography. They used the improved RSA encryption algorithm which is very difficult to break. And, then audio signal is used for embedding the encrypted information using the GA based LSB method. And, further the information is embedded into the random layers of LSB so that the attackers can not get access to the information so easily. The basic idea of this proposed approach is to maintain the robustness and providing the efficient and good method for hiding the information from the attackers.

Zamani *et al.*[5] proposed a novel approach for substitution techniques of audio steganography. Further genetic algorithm is used in which the information is embedded into the multiple, some higher LSB layers. Various problems of substitution technique and audio steganography has been solved using this proposed work. In the proposed

work, genetic algorithms are used for embedding the data into the higher and multiple LSB layers to provide the more robustness.

Bhowal *et al.* [9] In the internet world, secure transfer of information is very difficult due to the various attacks occurring now a days on information communication over the public network. So, the authors proposed the system based on the cryptography and steganography together for ensuring the secure transmission of the information safely without affecting the integrity of the data. In the first level of security, information is been encrypted using RSA algorithm which is difficult to break. In the next level of security, they used GA based LSB method (Genetic algorithm based Least Significant Based Method) for embedding the information into the audio signal before transmitting it over the public network. The encrypted bits of the information is embedded into the random bits of LSB layer to increase more robustness of system.

2.4 Using Discrete wavelet transform method

Shirali-Shahreza [19] proposed a Discrete wavelet transform method to embed the information in LSB's of the wavelet coefficients of the audio signal. To improve the inaudibility of the embedded information they employed a hearing threshold for hiding data in the integer wavelet coefficients, and avoided the information hiding in silent part of audio signal. In this work, robustness is been achieved, it is better than Human auditory system and provides security too.

Haj *et al.* [12] presented the new approach to audio watermarking algorithm based on discrete wavelength transform. In the past few years many watermarking algorithms have been proposed for digital videos, but only few algorithms have been implemented for audio watermarking technique. Therefore, HAS is more sensitive and complex in comparison to HVS. Performance of the proposed algorithm have been tested to reveal the robustness of system. The original cover signal was disintegrated to discover the various positions so that watermark bits can be embedded securely.

2.5 Using noise gate software logic

A. Ahmad *et al.* [2] proposed the technique that shifts the limit for transparent data hiding in audio signal from 4^{th} LSB layer to 8^{th} LSB layer thus results in increasing the capacity and robustness for information hiding in the audio signal by using the two steps. In the initial step of this work noise gate software logic was used to get the required signal to embed information into it. After the audio signal is been selected for embedding the information low bit encoding method of audio steganography approach is implemented. They proposed a method for audio steganographic technique using low bit encoding. Noise gate software logic is used to avoid embedding of information into the silent parts of the audio signal.

2.6 AVIS (Advanced VoIP steganography approach) system

Xu *et al.* [13] presented a framework AVIS, to embed the data within the network audio streams. AVIS system consists of mainly two parts – VAMI and VADDI. VAMI selects the multiple bits based on VoIP sector value and VADDI changes the intervals in which the embedding is done to avoid the detection of the information hided in the network streams by the attackers trying to get access to it.

2.7 Hybrid spread spectrum method for audio steganography

Nutzinger *et al.* [32] proposed a hybrid steganographic system for hiding the digital audio information. They added the DSSS system with the frequency for varying the frequency of BPSK signal carrying the secret information. Further, for per secret bit number of chips were adopted. This proposed work provides the secure steganographic system due to bit rate less feasible. This hybrid work is built for two enhancements of the DSSS system.

Zeng *et al*. [14] proposed a new approach for detecting the phase coding in audio signal. It takes FFT of segments of audio signal and unwraps the phases of audio samples and thus calculating the phase difference in the neighboring samples. For monitoring the phase difference five statistical features for phase difference in audio steganography is calculated. Then at the third stage, for detecting the phase difference in the signal SVM

classifier is used. This work provides the detecting rate of phase difference of up to 95%. It is one of the best embedding methods in audio steganography in terms of signal to noise ratio.

2.8 Audio steganography by cepstrum modification

Gopalan [20] proposed the method in which the data embedded into the cepstral domain of audio signal for audio steganography field. This work combines the auditory perception masking property of HAS with decorrelation property of speech spectrum so that information can be retrieved accurately. Hidden information is retrieved by using the threshold at the receiver side. Embedding may be moderately noticeable in the wave form or while hearing as it depends on the choice of frequencies used for cepstrum modification. This impact can be limited by choosing the frequencies based on their power levels in respect to masking thresholds. Changing cepstrum at higher covered frequencies has appeared to bring about unintelligible stego that is more robust to added substance commotion. It is robust for the additive noise occurring in the audio signal for secure transmission of the data over the public network.

2.9 Using modulo operator

Datta *et al.* [30] proposed the secure audio steganography technique. Modulo operator is been used for embedding the information inside the audio signal. First, the hexadecimal equivalent of the secret information is calculated by taking four bits at a time. Modulo operator is been used before the embedding process so that distortion can be less. The quality of the audio signal is analyzed by calculating the SNR and then compared with LSB and HLLAS technique. The proposed work is found 4 times better than LSB method and two times better than HLLAS method. So this proposed strategy is preferable in terms of imperceptibility, robustness and limit-the three difficult tasks of steganography

CHAPTER 3

RESEARCH PROBLEM

3.1 Problem Statement

As the internet is growing day by day secure transmission of the data is very crucial. So, secure transmission of information must be secretive as well as secure. Internet communication is essential part of communication now a days. So, we can increase the confidentiality of data by applying the security techniques and steganography to provide more security to the data. When digital information is transmitted over the internet, it can be edited or tampered by the attackers. This problem yields the biggest concern over the last few years. So, the unauthorized access of the transmitted information and ownership of the document needs to be protected.

The present work is focused on improving the security of the document while it is been transferred over the public network So, that no attacker can tamper it within the transmission. In this work, cryptographic and steganography technique has been employed to handle this concern. We have applied Affine and Hill cipher with Audio steganography technique using LSB Method and calculated their respective PSNR, MSE, Time taken to embed the information using both the ciphers independently and represented their Frequency representations for cover signal and encoded signal to differentiate between them. The concern of this research work is the audio steganography especially with the WAV files, thus not changing the size of the audio signals even after the embedding process.

3.2 Research Gaps

1. In some of the earlier work done in the field of audio steganography, when we embed the information into the wav files, the size of the wav files gets changed after the embedding the text information. If the size of .wav files will be larger, less amount of information it will be able to hide[5].

2. Huge record measure makes WAV's unfeasible for versatile gadgets and streaming.
3. In the earlier work done in audio steganography by combining the cryptographic techniques, authors didn't worked on more than one technique so that it can be differentiated which technique is better in terms of maintaining the integrity of the information[17].

3.3 Research Objectives

1. This proposed work won't be changing the measure of the sound record and is reasonable for .wav samples.
2. Integrity and confidentiality of information is maintained using secure audio steganography and cryptographic techniques.
3. PSNR, MSE and Time taken to embed the information into the audio signal using both ciphers is calculated so that we can compare the results with the other methods as well.

3.4 Research Methodology

In the proposed work, a sound signal with the ".wav" augmentation is been used for hiding the information. LSB method has been implemented in such a way that the least significant bits of the sound document ought to be adjusted in such a way that it does not influence the measure of the original sound signal without degrading its quality.

Steganography and Cryptography are executed together to improve the security of the system. Before, we embed information into the audio signal one has to know the record structure of the sound signal. WAV records have fundamentally two sections header is arranged in the initial 44 bytes of the sound file and rest of the bytes are for concealing the data. While embedding the data one cannot consider the header section of the audio signal. Header is mainly used to identify the audio signal. This is because the little change in the header segment can make harm the entire sound signal.

A program has been created in which first the data is encoded using Affine or Hill cipher. System then reads the audio signal file bit by bit and hides the encrypted

information. A new audio file is generated containing the hidden information. PSNR, MSE and time taken to embed the information are calculated. Representation of cover signal and encoded signal using particular cipher are drawn. Then the comparison is made between the two ciphers on the basis of the above factors.

CHAPTER 4

AUDIO STEGANOGRAPHY TECHNIQUE USING CRYPTOGRAPHY

In the present study, we have applied audio steganography technique using cryptography on the text information with the help of MATLAB. Development stages of this proposed work are shown in Figure 4.1. Section 4.1 illustrates the encryption process to change the information into unreadable manner before embedding it in the audio signal. Section 4.2 illustrates the embedding process of the information using LSB method, Section 4.3 discusses the decoding process for the information hidden in the stego audio signal to retrieve the hidden information and Section 4.4 discusses the decryption process in order to get the original information.

MATLAB – It is the short form is a programming bundle intended for quick and simple logical computations. It is the programming language developed by MathWorks[33] . It has actually several types of built in functions for a wide assortment of calculations and numerous tool compartments have been intended for different research disciplines, including the information analysis and statistics.

MATLAB help function help to find any additional functions we may need to use for our work. MATLAB allows matrix manipulations, plotting of functions and information, implementation of algorithms, making of UI's, and interfacing with programs written in other dialects such as Java, C, C++, Python.

MATLAB in a programming language, as well as a programming domain also[33]. You can perform operations from the command line, as a sophisticated calculator or we can make projects and capacities that perform repetitive tasks, similarly as whatever other language.

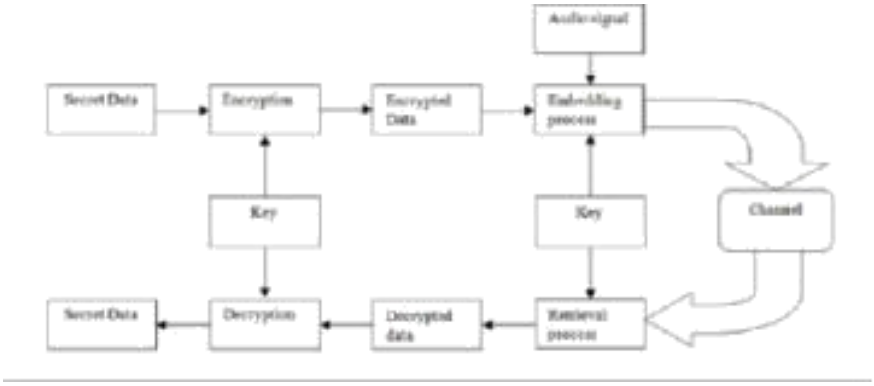


Fig 4.1: Proposed system design

The proposed system works in an optimized way without giving any problem. Figure 4.1 represents both receiver and transmitter side of the algorithm used. The secret information to be transmitted is encrypted using the proposed encryption algorithm.

The encrypted information is then further encoded into the audio signal using Steganographic method. At the receiver side, the audio signal containing the secret message is been received. From, this signal hided information is retrieved using the decryption algorithm. For decryption same cipher that was used while encrypting the text is used

4.1 Encryption Process

In the audio steganography technique using cryptography, encryption is the first and very important stage. The main role of encryption is to ensure the classification of computerized information put away on PC frameworks or transmitted by means of the Internet or other PC systems. As, we can't proceed further without completing this phase. In the proposed work, encryption and decryption process is handled by Affine and Hill cipher method.

Encryption of information is done when we are dealing with some important data. Important information is changed into the cipher text that cannot be easily understood by the unauthorized persons who are trying to get access to that information to tamper or destroy it (Bhowmick et al., 2015). After encryption is performed then only we can embed the data into the audio signal.

Fig 4.2: Encryption Process

Here,

Plain text – Any communication in the language we speak that is the human language

Cipher text – When plain text is codified using suitable scheme giving the codified message.

4.2 Embedding process using LSB

LSB strategy enables huge measure of secret data to be encoded in a sound record. Audio file contains set of bytes which can be used for encoding. Some audio files may contain several bytes depending on their sizes**.** The following steps are used during the encoding process:

1 Encrypt the information to be hided in the audio signal using the key so that it becomes difficult for the attackers to understand it.

2 Convert the audio signal into the bit stream. Audio signal bits are replaced with the message bits using LSB (Least Significant Bit) method.

3 Change over each character display in the message into the bit.

4 Substitute the LSB bits of the sound signal with the LSB bits of the secret data.

5 A new audio sample containing the secret information is generated.

Integrity of information is a maintained using secure audio steganography and cryptographic techniques. This combination of audio steganography and cryptography make sure that even if the attacker interpret the audio signal and will not be able to

discover the secret information as it has been embedded into the deep layers of LSB method using audio steganography. Hence, providing the double security to the system.

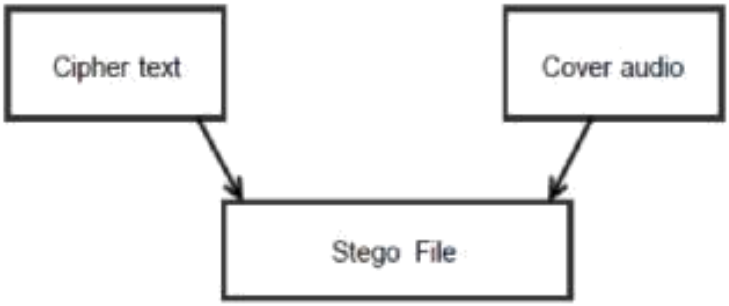


Fig 4.3: Embedding ciphertext

4.3 Decoding Process

At this phase, encoded file is decoded to get the hidden information stored in the new generated audio signal. The message is decoded first and afterward decrypted by public key that is known just by the approved collectors or clients of the proposed framework. Decrypting is the way toward changing over code into plain content or any configuration that is helpful for consequent procedures. Decrypting is the invert of encoding.

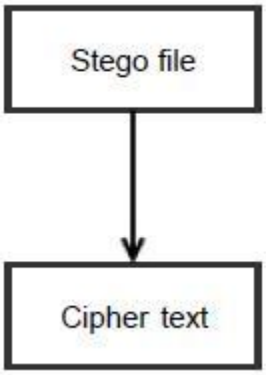


Fig 4.4: Decoding ciphertext

4.4 Decryption Process

Decryption is the way towards taking encoded or the encrypted text and converting back to the content which can be read and understood. This can be referred as the process of

un-encrypting the information by using the keys. The user's key/password is supplied to decrypt the encrypted message in order to get the original message. In the proposed work, the process of encryption and decryption is handled by Affine and Hill cipher method. It is the way toward unraveling the information which has been encoded into a secret arrange. An approved client can just decode information since unscrambling requires a secret key or password.

Fig 4.5: Decryption process

CHAPTER 5

EXPERIMENTAL RESULTS

As discussed in Chapter 4, we have used cryptographic techniques with the audio steganography for embedding the text information into the audio signal. Present study is focused on improving the integrity of information so that text information cannot be tampered by the attackers while transmitting it over the public network. Thus, improving the security of the system. We have applied affine and hill cipher method on the original text information then embedded it in the audio signal using LSB technique. After applying this technique we get representations of cover signal and audio signal as output. We have further implemented this work using various parameters such as time taken to embed the information using both cipher methods, PSNR, MSE etc. Frequency representation of original cover signal and encoded signal after applying cipher method with audio steganography technique are also shown. We have illustrated the results obtained using various audio .wav samples and made the comparison between both the cipher methods using above mentioned factors.

MATLAB has been used for hiding the text information in audio signal using cryptographic technique. This technique helps in improving the security of the cryptosystem. We have performed various experiments for implementing the above approach. Here, experiment 1 describes how text information is hided using affine cipher and audio steganography technique, experiment 2 describes the how text information is hided using hill cipher and audio steganography and experiment 3 discuss the results obtained using both methods. Experiments conducted in this work are discussed further in this chapter.

5.1 Experiment 1

Experiment 1 has been performed for embedding the text information using affine cipher followed by LSB method in the selected audio signal by the user displaying the

time taken to embed the text information using this cipher method. Also, representations of cover signal and encoded signal is displayed using above method.

First, we will select the task to be performed that is Hide text or Recover text from the task panel. Presently in experiment 1 we are working on hide text task using affine cipher method.

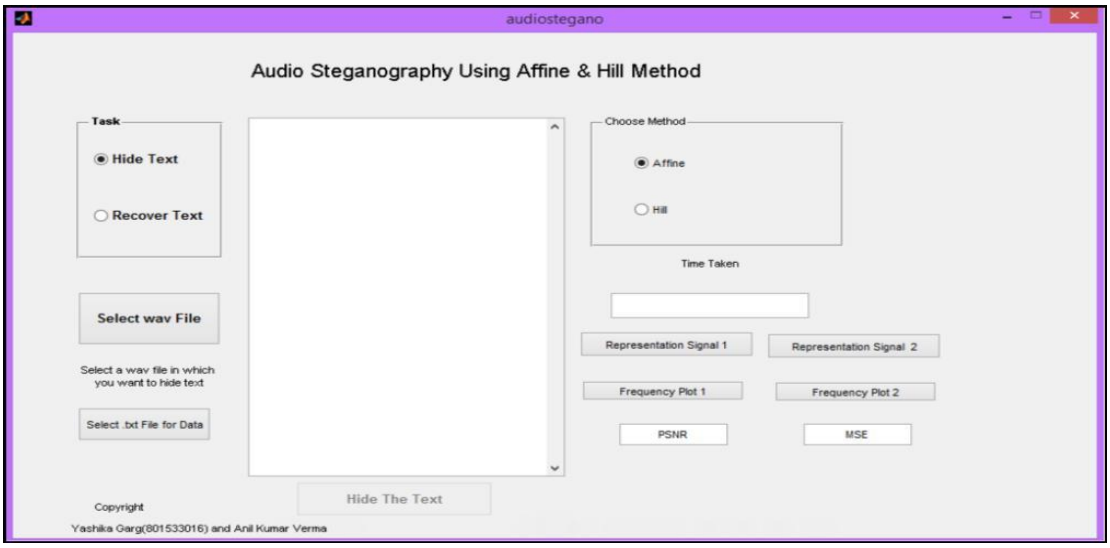


Fig 5.1: Displaying the GUI of proposed work

Then, we will choose the method as Affine cipher out of two methods defined in the choose method box and hide text as task to be performed from the task box. Now, we will be selecting the original audio signal to be used for embedding the text in it using selected cipher method shown as below-

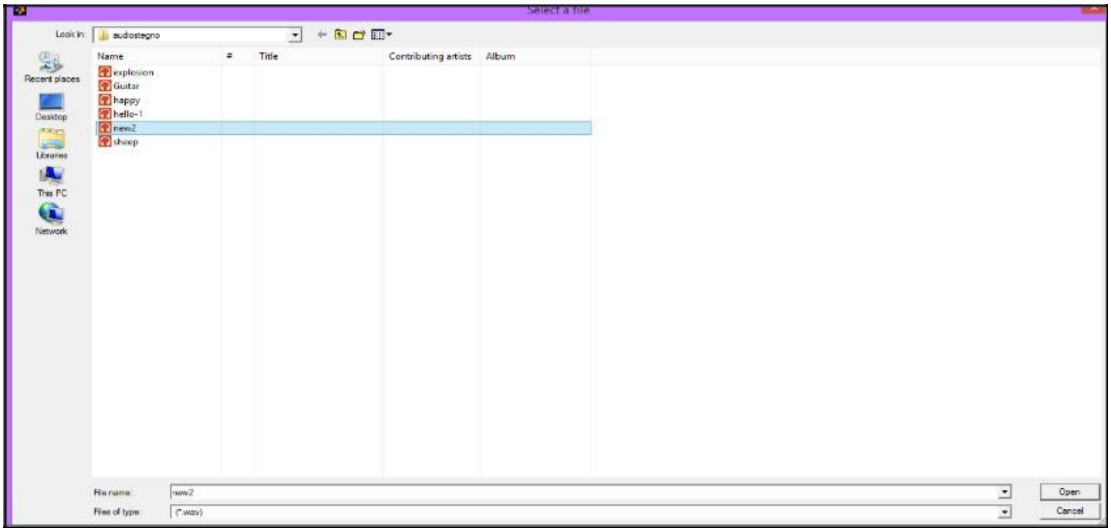


Fig 5.2: Selecting the audio file for embedding process

Now, we will select the text file containing the information to be embedded into the selected audio signal shown as below-

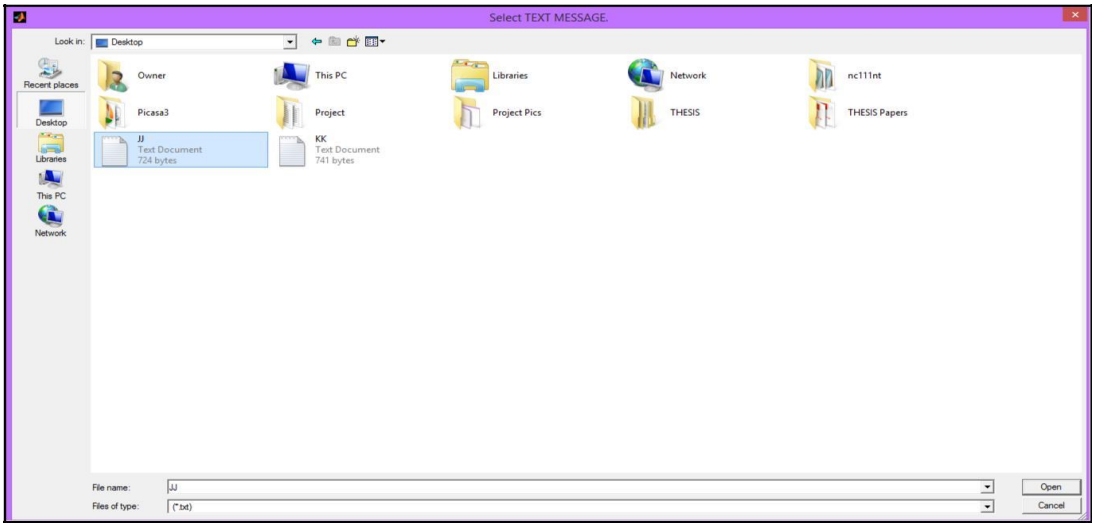


Fig 5.3: Selecting the text file

Now, we will click on Hide the txt button for hiding the text using affine cipher method in audio steganography. Here, a dialog box will open displaying that text information is been successfully embedded into the selected audio signal. Audio steganography technique here is implemented using LSB (Least Significant Method). Time taken to embed the text information into the selected audio signal is also displayed here. This phase of embedding process is shown in Fig 5.4 as below-

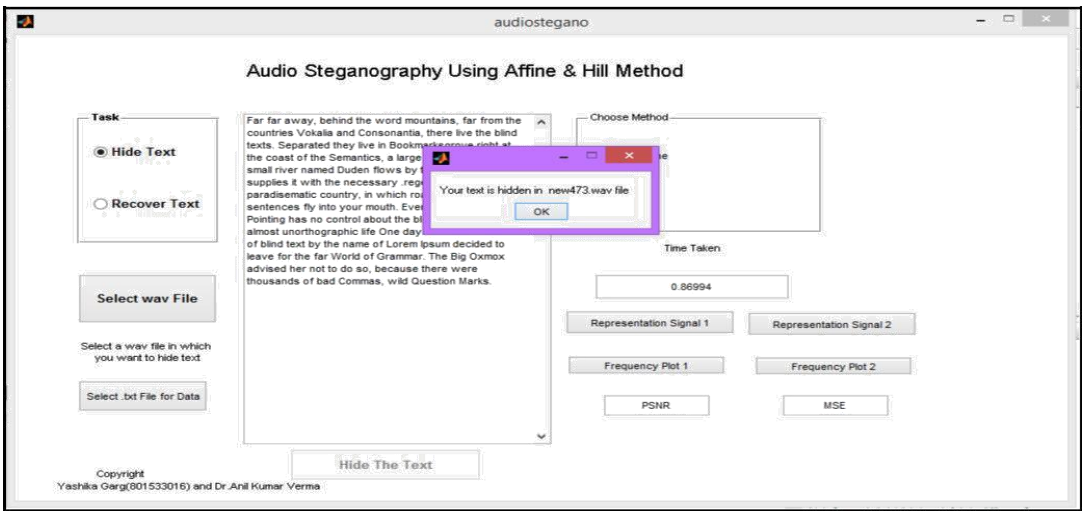


Fig 5.4: Text is hidden confirmation using affine cipher

Representation of cover signal and encoded signal using affine cipher method are shown as below-

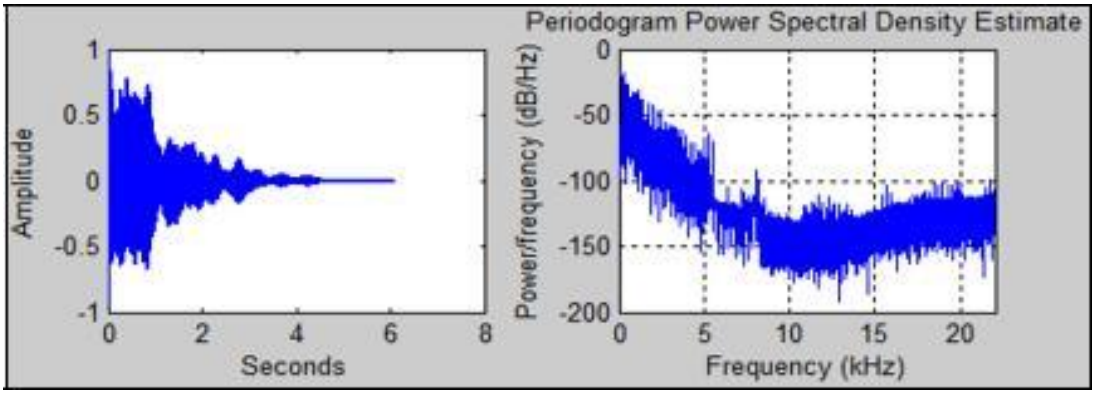


Fig 5.5: Cover signal representation

:

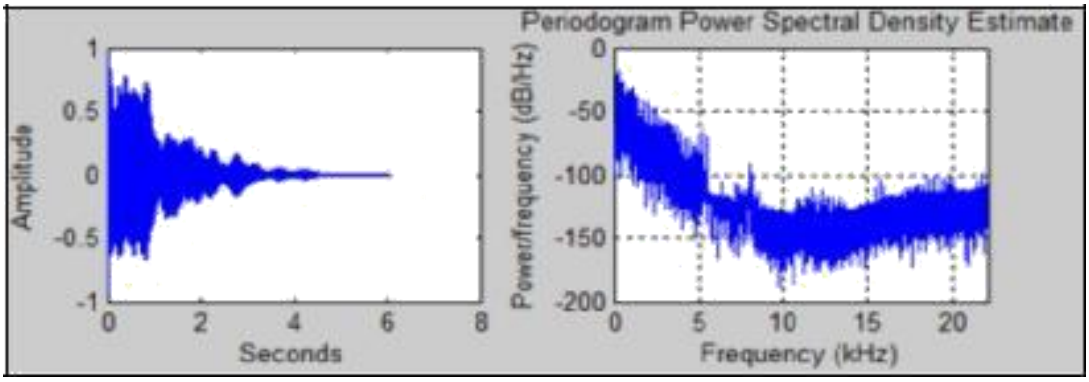


Fig 5.6: Encoded signal representation using affine cipher

Now, PSNR and MSE values of cover signal and encoded signal using affine cipher method is shown as below-

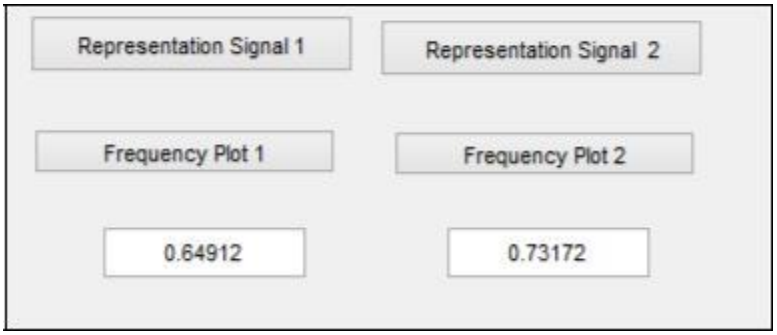


Fig 5.7: PSNR and MSE values of cover signal

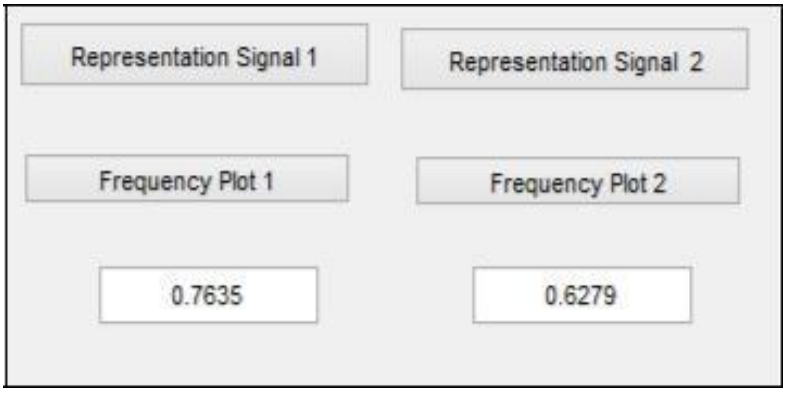


Fig 5.8: PSNR and MSE values of encoded signal using affine cipher

5.2 Experiment 2

Experiment 2 has been performed for embedding the text information using hill cipher followed by LSB method in the selected audio signal by the user displaying the time taken to embed the text information using this cipher method. Also, representations of cover signal and encoded signal is displayed using above method.

First, we will select the task to be performed that is Hide text or Recover text from the task panel. Presently in experiment 2 we are working on hide text task using hill cipher method.

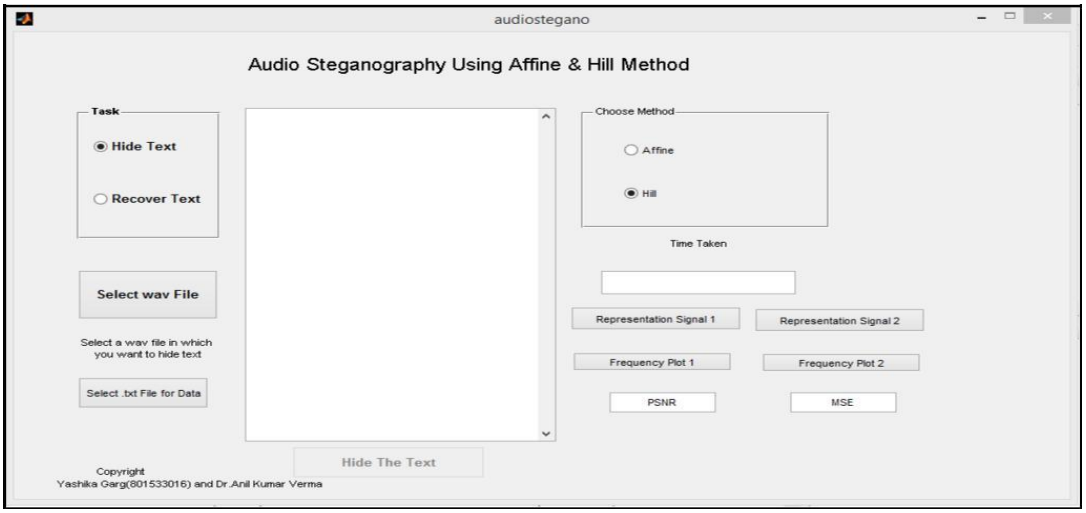


Fig 5.9: Hiding the text using hill cipher

Similarly, we will be selecting the original audio signal to be used for embedding the text in it using selected cipher method and the text file containing the text information as we did in affine cipher method.

Now, after selecting the audio signal and text file click on Hide the text button as shown below in Fig 5.10

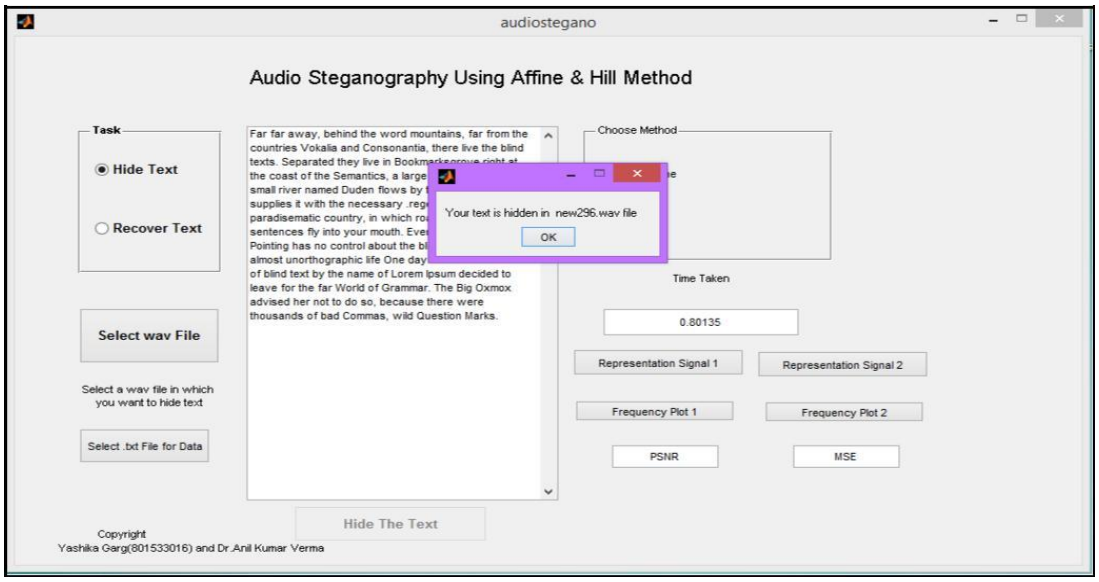


Fig 5.10: Text is hidden confirmation using hill cipher

Representation of encoded signal using hill cipher method are shown as below-

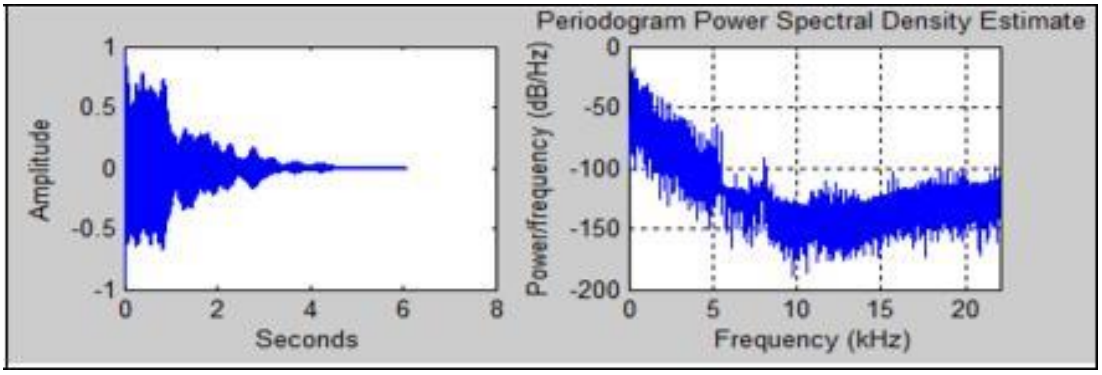


Fig 5.11: Encoded signal representation using hill cipher

Now, PSNR and MSE values of encoded signal using hill cipher are shown as below-

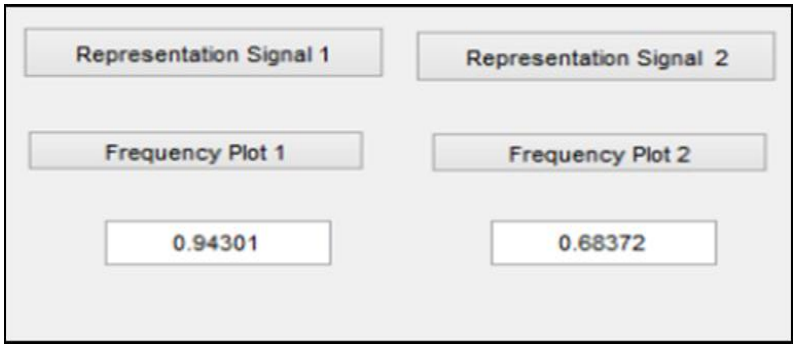


Fig 5.12: PSNR and MSE values of encoded signal using hill cipher

5.3 Experiment 3

Experiment 3 has been performed for making the comparison between the affine cipher method and hill cipher method on the basis of various factors such as Time taken to embed the information in audio signal, PSNR, MSE values, Frequency representation of cover signal and encoded signal using both the methods. This proposed work has been implemented on various audio samples.

The three most important aspects considered while information hiding are security, capacity and the robustness. In proposed work, we have implemented Audio steganography using LSB method with Cryptographic techniques. In this way, more security can be provided to the system. By comparing the two tables, we find out

1. Time taken for embedding in Hill cipher is less than the time taken for embedding in Affine cipher.
2. PSNR, MSE values are more in Hill cipher than that of Affine cipher.
3. Higher the PSNR estimate, better the nature of the audio signal.
4. Change in the cover signal and encoded signal graphs is very negligible which clearly demonstrates it is hard to locate the concealed content which fulfills the prerequisite of secret communication.

   Frequency representation of cover signal and encoded signal are shown as below-

- Affine cipher

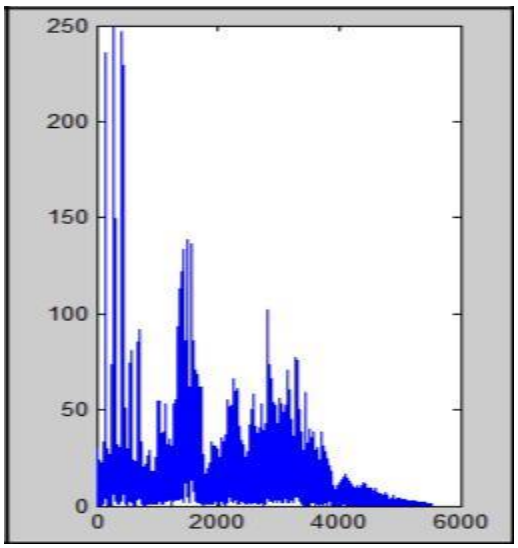


Fig 5.13: Frequency representation of cover signal

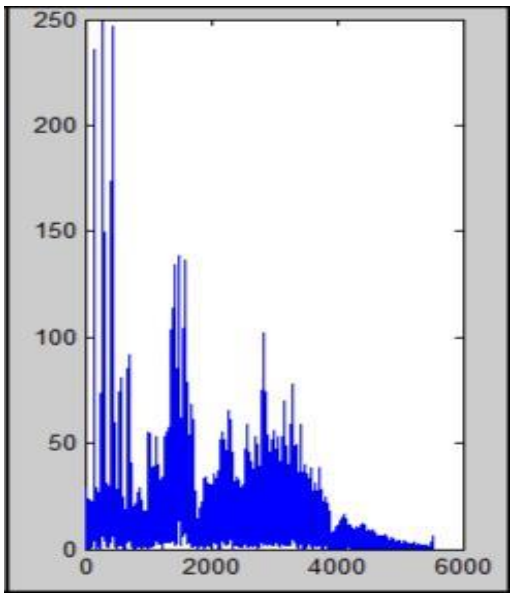


Fig 5.14: Frequency representation of encoded signal using affine cipher

- Hill cipher

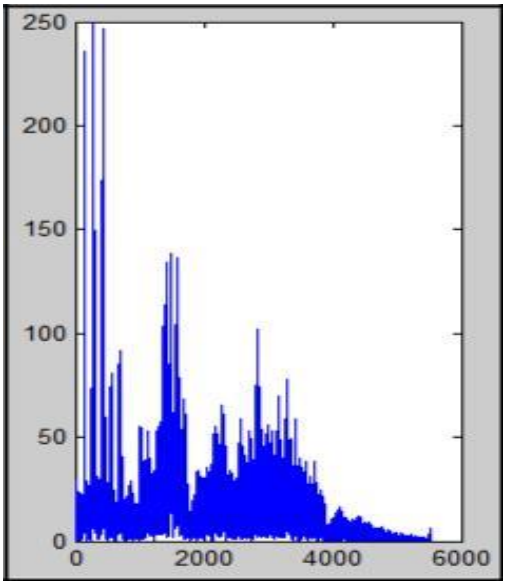


Fig 5.15: Frequency representation of encoded signal using hill cipher

Table 5.1 shows PSNR, MSE, Time taken(secs) before and after embedding using affine cipher

Table 1 : Using Affine Cipher				
Cover Signal		Encoded Signal		
PSNR	MSE	PSNR	MSE	Time Taken
0.649	0.732	0.7635	0.6279	0.86994

Table 5.2 shows PSNR, MSE, Time taken(secs) before and after embedding using hill cipher

Table 2 : Using Hill Cipher				
Cover Signal		Encoded Signal		
PSNR	MSE	PSNR	MSE	Time Taken
0.649	0.732	0.94301	0.6837	0.80135

Table 5.3 Comparison Table

Table 3 : Comparison between Affine and Hill Cipher Method							
Audio	Capacity	Encoded Signal Using Affine			Encoded Signal Using Hill		
		PSNR	MSE	Time Taken	PSNR	MSE	Time Taken
Input.wav	176 KB	0.7635	0.6279	0.86994	0.94301	0.6837	0.80135
Hello.wav	248 KB	0.667	0.844	0.5983	0.672	0.85	0.3411
Happy.wav	41 KB	0.89	0.196	0.6628	0.92	0.583	0.338
Explosion.wav	550 KB	0.092	0.0078	0.484	0.29	0.31	0.212
Sheep.wav	20 KB	0.808	0.755	0.932	0.89	0.98	0.789

The wav samples used for implementing this research work have been used from online source and then these wav samples were used for making comparison between both the ciphers on the basis of various parameters defined in this proposed work[35].

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

This thesis presents an implementation of audio steganography technique using cryptography for enhancing the security of text information embedded in the audio signal so that they can be transmitted safely on the public network. We have proposed a new approach for enhancing the security of information from the attackers. The approach used in this thesis and results obtained can be summarized as follows:

- Integrity of information is maintained using secure audio steganography and cryptographic techniques.
- The proposed work will not be changing the size of the audio signal and is suitable for .wav samples.
- This combination of audio steganography and cryptography make sure that even if the attacker interpret the audio signal and will not be able to discover the secret information as it has been embedded into the deep layers of LSB method using audio steganography.
- It provides the double security to the system.

6.2 Future Scope

An interested researcher may implement a few more things to this work:

- It is difficult to obtain a system that satisfies both criteria of high security and robustness therefore to find a new mechanism to satisfy our needs is yet to be investigated.
- Future work is focused on increasing the capacity of secret information and confidentiality of the system.

REFERENCES

[1] Priyanka, Bankar R., Katariya R. Vrushabh, Patil K. Komal, Shashikant M. Pingle, and Sanghavi R. Mahesh. "Audio Steganography using LSB." International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE) 2 (2012): 90.

[2] Ahmed, Mohamed A., Miss Laiha Mat Kiah, B. B. Zaidan, and A. A. Zaidan. "A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm." Journal of Applied Science 10, no. 1 (2010): 59-64.

[3] Saurabh, Juhi, and Asha Ambhaikar. "Audio steganography using RPrime RSA and GA based LSB algorithm to enhance security." International Journal of Science and Research 1, no. 2 (2012).

[4] Fatima, Zameer, and Tarun Khanna. "Audio steganography using DES algorithm." In Proceedings of the 5th National Conference, pp. 10-11. 2011.

[5] Zamani, Mazdak, Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki. "Robust audio steganography via genetic algorithm." In Information and Communication Technologies, 2009. ICICT'09. International Conference on, pp. 149-153. IEEE, 2009.

[6] Basu, Pramatha Nath, and Tanmay Bhowmik. "On embedding of text in audio a case of steganography." In Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on, pp. 203-206. IEEE, 2010.

[7] Abikoye Oluwakemi, C., S. Adewole Kayode, and J. Oladipupo Ayotunde. "Efficient data hiding system using cryptography and steganography." IJAIS 11, no. 4 (2012): 1-6.

[8] Khan, Md Shafakhatullah, MV Vijaya Bhaskar, and MV Shiva Nagaraju. "An optimized method for concealing data using audio steganography." International Journal of Computer Applications (0975–8887) Volume (2011): 25-30.

[9] Bhowal, Krishna, Debnath Bhattacharyya, Anindya Jyoti Pal, and Tai-Hoon Kim. "A GA based audio steganography with enhanced security." Telecommunication Systems 52, no. 4 (2013): 2197-2204.

[10] Zaidan, A. A., B. B. Zaidan, O. Hamdan Alanazi, Abdullah Gani, Omar Zakaria, and Gazi Mahabubul Alam. "Novel approach for high (secure and rate) data hidden within triplex space for executable file." Scientific Research and Essays 5, no. 15 (2010): 1965-1977.

[11] Verma, Tanmaiy G., Zohaib Hasan, and Dr Girish Verma. "A Unique Approach for Data Hiding Using Audio Steganography." International Journal of Modern Engineering Research (IJMER) www. ijmer. com 3, no. 4 (2013).

[12] Al-Haj, Ali, Ahmad A. Mohammad, and Lama Bata. "DWT-based audio watermarking." Int. Arab J. Inf. Technol. 8, no. 3 (2011): 326-333.

[13] Xu, Erchi, Bo Liu, Liyang Xu, Ziling Wei, Baokang Zhao, and Jinshu Su. "Adaptive VoIP steganography for information hiding within network audio streams." In Network-Based Information Systems (NBiS), 2011 14th International Conference on, pp. 612-617. IEEE, 2011.

[14] Zeng, Wei, Haojun Ai, and Ruimin Hu. "A novel steganalysis algorithm of phase coding in audio signal." In Advanced Language Processing and Web Information Technology, 2007. ALPIT 2007. Sixth International Conference on, pp. 261-264. IEEE, 2007.

[15] Gopalan, Kaliappan. "Audio steganography by cepstrum modification." In Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on, vol. 5, pp. v-481. IEEE, 2005.

[16] Asad, Muhammad, Junaid Gilani, and Adnan Khalid. "Three layered model for audio steganography." In Emerging Technologies (ICET), 2012 International Conference on, pp. 1-6. IEEE, 2012.

[17] Artz, D. (2001) 'Digital steganography: hiding data within data', IEEE Internet Computing, May–June, Vol. 36, No. 5, pp.75–80.

[18] Kamred Udham Singh, "A Survey on Audio Steganography Approaches," International Journal of Computer Applications (0975 – 8887), p. 9, 2014.

[19] M Shirali-Shahreza S Shirali-Shahreza, "Steganography in Silence Intervals of Speech," in , proceedings of the Fourth IEEE International Conference on Intelligent Information Hiding and Multimedia Signal (IIH-MSP 2008), Harbin , china, 2008.

[20] S Wenndt Gopalan, "Audio Steganography for Covert Data Transmission by Imperceptible Tone Insertion," in WOC, Banff , Canada, july 8-10,2004.

[21] V.Vijaya Bhasker, V. Shiva Md. Shafakhatullah Khan, "An Optimized Method for Concealing Data using Audio Steganography," International Journal of Computer Applications, pp. 0975-8887, 2011.

[22] D. M. Ballesteros L and J. M. Moreno, "Highly transparent steganography model of speech signals using Efficient Wavelet Masking," 2012.

[23] Katariya Vrushabh R, Patil Komal K Bankar Priyanka R., "Audio Steganography using LSB," nternational Journal of Electronics, pp. 90-92, 2012.

[24] Mohammed M. Nasef and Fatma T. Eid Ali M. Meligy, "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys," I. J. Computer Netwok and Information Security, pp. 24-29, 2015.

[25] Anirban Bhowmick, B. Kishore Nishith Sinha, "Encrypted Information Hiding using Audio Steganography and Audio Cryptography," International Journal of Computer Applications, pp. 0975-8123, 2015.

[26] Roy, S., Manasmita M., 2011. A novel approach to format based test stegonography, International conference on communication computing and security, ICCCS 2011,Proceedings by ACM with ISBN-978-1-4503- 0464-rourkela,Odisha,India.

[27] Acharya, Bibhudendra, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy. "Novel methods of generating self-invertible matrix for hill cipher algorithm." (2007).

[28] V. Sharma and R. Thakur, "LSB modification based Audio Steganography using Trusted Third Party Key Indexing method," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 403-406.

[29]A. Kanhe, G. Aghila, C. Y. S. Kiran, C. H. Ramesh, G. Jadav and M. G. Raj, "Robust Audio steganography based on Advanced Encryption standards in temporal domain," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015, pp. 1449-1453.

[30] B. Datta, S. Tat and S. K. Bandyopadhyay, "Robust high capacity audio steganography using modulo operator," Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, 2015, pp. 1-5.

[31] N. Cvejic and T. Seppanen, "Increasing robustness of LSB audio steganography using a novel embedding method," International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., 2004, pp. 533-537 Vol.2.

[32] Nutzinger, Marcus, Christian Fabian, and Marion Marschalek. "Secure hybrid spread spectrum system for steganography in auditive media." In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on, pp. 78-81. IEEE, 2010.

[33] https://in.mathworks.com/

[34]Al-Othmani, Abdulaleem Z., Azizah Abdul Manaf, and Akram M. Zeki. "A survey on steganography techniques in real time audio signals and evaluation." International Journal of Computer Science Issues (IJCSI) 9, no. 1 (2012).

[35] https://www.freesoundeffects.com/free-sounds/explosion-10070/

APPENDIX A

PUBLICATION

[1] Yashika Garg, R Kumar and Anil Kumar Verma, "Audio Steganography using Affine and Hill Cipher Method", in International Journal of Information and Computer security (**communicated**).

[2] Yashika Garg and Anil Kumar Verma, "A Review of Steganography and its methods", in 3rd DAV National Conference held at Jalandhar(STEHM-2016).

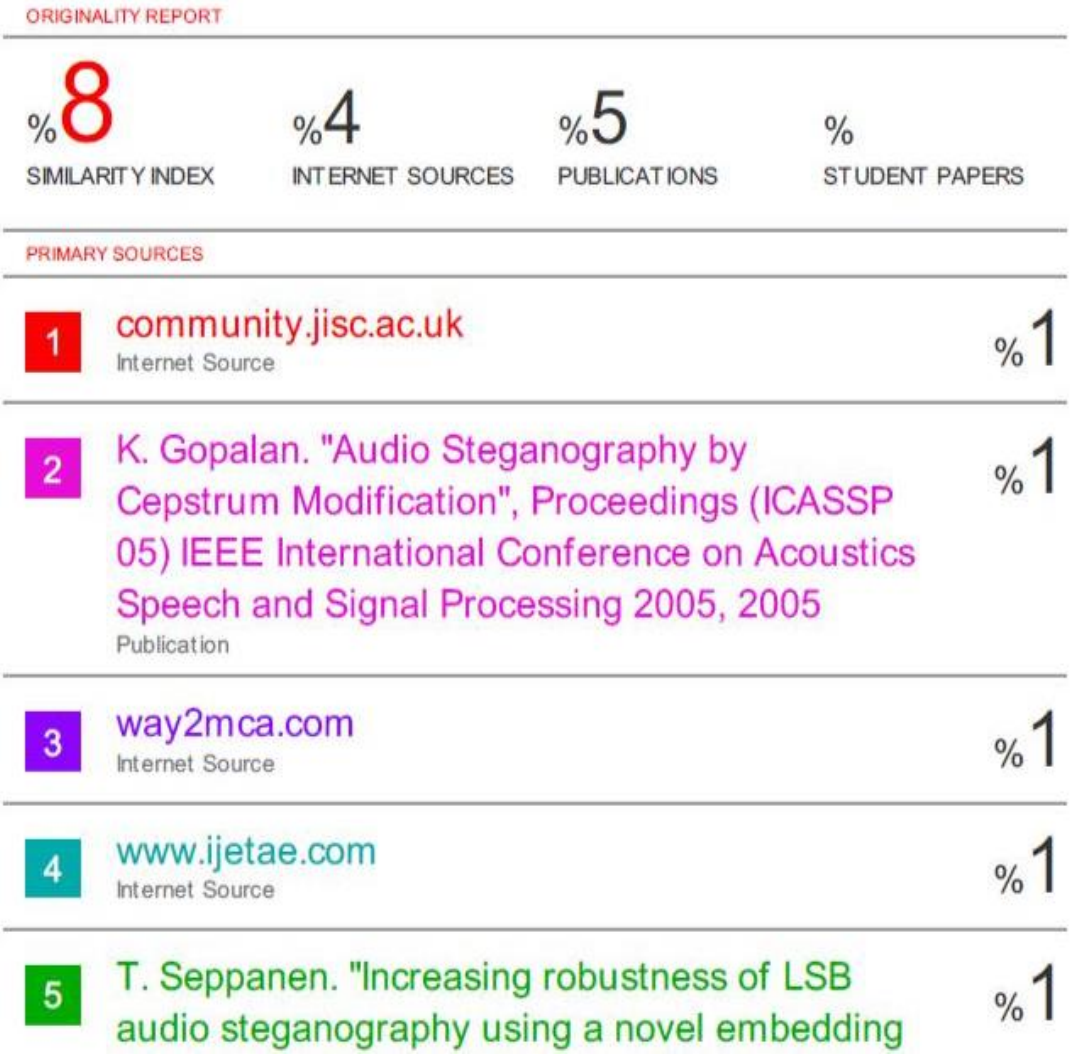
APPENDIX B

VIDEO PRESENTATION LINK

https://youtu.be/MrHYQEx4gUw

APPENDIX C

PLAGIARISM REPORT



ORIGINALITY REPORT

%8	%4	%5	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	community.jisc.ac.uk Internet Source	%1
2	K. Gopalan. "Audio Steganography by Cepstrum Modification", Proceedings (ICASSP 05) IEEE International Conference on Acoustics Speech and Signal Processing 2005, 2005 Publication	%1
3	way2mca.com Internet Source	%1
4	www.ijetae.com Internet Source	%1
5	T. Seppanen. "Increasing robustness of LSB audio steganography using a novel embedding	%1