# Implementation of Cryptographic Method for Secure Audio Data Hiding in Digital Image

**Pranjali Ihare[1], V. T. Gaikwad[2]**

[1]Electronics and Telecommunication, SIPNA C.O.E.T/ SGBAU University, Maharashtra, India

[2]Associate Professor, Information Technology, SIPNA C.O.E.T/ SGBAU University, Maharashtra, India

**Abstract:** ***Information security is a major obstacle in different areas like military, network application, are illegally access the information. So, it is very important to hide the secret data efficiently. By means of steganography we can hide information to be transmitted over network. In this project we have developed the technique to hide the secret short audio file into cover image to form a stego cover image in order to provide the robust security. The proposed system consists of the steganography using the wavelet based LSB technique and the cryptography which uses the BRA algorithm it takes the smallest amount of time and provides the more security. The performance analysis has been done by using the performance parameters like PSNR, MSE, SNR by using the matlab software.***

**Keywords:** Cover image, Cryptography, Encryption, Secret short audio file, Steganography

## 1. Introduction

Broadband Internet connections almost an errorless transmission of data helps people to distribute large multimedia files and make identical digital copies of them. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. It is very important to hide the secret data efficiently, as many attacks made on the data communication. In modern communication system data hiding is most essential for network security issue. As hackers have developed many types of software to attack on secret key, Password and ID can't provide the strong security. The Internet has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life.

So, encryption technique along with the data hiding can provide the perfect security. Encryption is used to encrypt the secret audio signal to be transmitted. There are basically two types of cryptographic algorithms, symmetric-key and public-key. In symmetric-key cryptographic algorithm sender as well as receiver uses the secret key. Whereas, in public-key cryptographic algorithm different keys are used for encryption and decryption Data hiding is another technique which totally denies the existence of information in an image or video so there is no knowledge of existence of any message in an image or video. By means of data hiding we are hiding the encrypted audio file to be transmitted inside the digital image. So that it will provide more secured audio data transmission. Cryptographic technique in support to the data hiding in order to provide more security is used. The purpose of our project is to provide cryptographic method for perfectly secured transmission of an audio file hiding in digital images.

## 2. Literature Review

In literature review we have summarize the proposed work that has been carried out by the different authors. Different authors have mentioned the different techniques as well as methods of steganography as well as cryptography. They have developed encryption, decryption as well as embedding algorithm where it was needed in order to provide strong security.

Punam V. Maitri and Dattatray S. Waghole [1] presented low latency in order to encrypt and decrypt file using BRA Algorithm in Network Security. Information security is very important in different areas like military, bank application, network application. Confidential data is forward from one location to another location in the network. Many hackers are illegally access the information. To provide solution to this problem many authors has introduced different algorithms and techniques. The different algorithms like AES, DES and triple DES achieve more security but it takes more time for encryption and decryption files. These algorithm increases the complexity of the algorithm. In their algorithm they have investigate parameters of network security. Their algorithm provides more security and takes smallest amount of time for file encryption and decryption. Their algorithm can apply on different types of files like text, image, audio, video files. In the Byte Rotation Algorithm involve two techniques. One is random key generation technique is used and second is parallel encryption and decryption is process using multithreading technique.

Parallel decryption technique decrypts the data and combine the divided block. The public key cryptosystem is used to detect the location of sensor node. This algorithm uses smaller key and liner block chipper algorithm for encryption and decryption. The RSA and diffie Hellman algorithm has combined to implement new hybrid algorithm. The hybrid algorithm provides more security by using Bitwise XOR operation. The asymmetric RSA algorithm has proposed by Ashraful Islam. The text message is encrypted by using shared secret key. The secret key should be shared among network before message transmission. The transmission of text message through different SNR level. Those send the message to receiver. At receiver side decryption is done by using secret key. Advantage of this algorithm is easily retrieving the data at receiver side. The AES algorithm has implemented using different techniques like rearrangement, substitution and transformation technique. The application can be used in different field telephony as well as in military. Communication In this paper performance analysis of BRA and AES Algorithm for file encryption and decryption process is done. After performance analysis results shows that compare to the AES algorithm, the performance of the Byte Rotational Algorithm is better. As compare to the AES algorithm BRA is taking 5 to 13% less time for text encryption. 5 to 17% less time take BRA for Image Decryption as compare to AES algorithm 6 to 14% less time require BRA for Image Encryption as compare to AES algorithm. BRA algorithm needs 4 to 16% less time for audio file encryption as compare to AES algorithm. For Audio file decryption BRA algorithm is require 5 to 18% less time as compare to AES algorithm. Finally they have conclude that for encryption and encryption process as compare to the AES algorithm the performance of the BRA algorithm takes very less time. In future work in order to reduce time and improve network security. they will be implementing a new Hybrid encryption and decryption algorithm.

Tawfiq S. Barhoom and Zakaria M. Abusilmiyeh [2] presented cryptography method based on image for key generation. They have proposed a method for encrypting the sender's messages using new algorithm with a secret key which is generated from this key will be used for encrypting and decrypting the messages which are transmitted between two sides. The length of the key varies according to the size of the message as it varies in every session according to the session type. It is a reliable and flexible way to generate the key to secure the information which is transferred through the networks and it is easy to implement. This method ensures the prevention of guesses or breaking the key and provides a more secure way for information encryption.

Their motto is the two sides need to communicate with each other securely through the local network or the internet. By using cryptography algorithm they need to ensure the confidentiality and authenticity of the messages transmitted between them. Finally they conclude that this method is more secure as compared to the traditional cryptographic processes. The alogorithm process provides advantage of key generation based on sessions and according to the message length the key length varies. Finally they conclude that this process is more flexible as compared to any RGB image that can be used for key generation. As the key generation is directly based on the image content.

Harshitha K M, Dr. P. A. Vijaya [3] presented algorithm for data hiding using encrypted secret message. In today's world in any communication, security is the most important issue. Lots of data hiding and data security algorithms have been developed in the last decade, which worked as motivation for the research. This project is a combination of cryptography and stegnography that provides a strong backbone for its security. Now a days information security system includes confidentiality, authenticity, integrity, non-repudiation. In their project they focus on enlightening the technique to secure data or message with authenticity and integrity.In their project work, before the actual embedding process starts the secret message is encrypted. The hidden message is encrypted using a simple encryption algorithm using secret key and hence it will be almost impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key. Only receiver and sender know the secret key. N-bit LSB substitution technique is used as embedding and extraction method. We propose that this method could be most appropriate for hiding any secret message (text, image, audio, video) in any standard cover media such as image, audio, video files.

Data hiding techniques have been widely used for transmission of hiding secret message for long time. For computer users data security is very important. Businessmen, professionals, and home users all have some important data that they want to secure from others. In their proposed system they have mentioned the software for data encryption and then embed the cipher text in a cover medium. This system combines the effect of these two methods to enhance the security of the data. The proposed system encrypts the data with a crypto algorithm and then embeds the encrypted data in a cover file. This system improves the security of the data by embedding the encrypted data and not the plain data in cover file. The block diagram of proposed system is as shown in fig. To embed a secret message file in the cover file used two distinct methods: Encrypt the secret message and the encrypted secret message is embed in the cover media by using LSB substitution technique. In this paper they have given an idea to enhance the security of system by combining the two techniques. It enhances confidentiality of information and provides a means of communicating privately.

Guangyong Gao and Yun-Qing Shi, Fellow, IEEE [4] presented data hiding with the help of controlled contrast enhancement and integer wavelet transform. The conventional reversible data hiding (RDH) algorithms pursue high Peak-Signal-to-Noise-Ratio (PSNR) at the certain amount of embedding bits. Recently, Wu et al. deemed that rather than keeping high PSNR, the improvement of image visual quality is more important. Based on this viewpoint, they presented a novel RDH scheme, utilizing contrast enhancement to replace the PSNR. However image contrast is over enhanced when a large number of bits are embedded, which introduces obvious distortion for human visual perception. Motivated by this issue, a new RDH scheme is proposed using the controlled contrast enhancement (CCE) and Haar integer wavelet transform (IWT). The proposed scheme has large embedding capacity while maintaining satisfactory visual perception. Experimental results have demonstrated the effectiveness of the proposed scheme enhancement and integer wavelet transform'.

There are two main parts in the message embedding process, including data embedding with CCE in spatial domain and more data embedding in Haar IWT domain. The data extraction and image recovery are the reverse procedure of data embedding process. Data hiding is applied extensively to the fields of owner- ship protection, authentication, finger printing and secret communication. The most classical data hiding leads to permanent distortions. Recently, a new data hiding technique, i.e., reversible data hiding (RDH), is proposed, which can not only extract the embedded bits, but also restore the original cover image without any error. It is observed that as more data needs to be embedded Wu et al.'s method needs to use more peak-pairs (for example 50 pairs), consequently the image contrast may be over-enhanced, which can introduce annoying perception distortion. So, finally they conclude that the proposed scheme performs better than Wu et al.'s scheme as well as some of state-of-the-art schemes with keeping image's PSNR high as criterion for RDH.

Minal Govind Avasare and Vishakha Vivek Kelkar presented [5] image encryption using Chaos theory. In open network, it is very important to keep sensitive information secure from becoming vulnerable to unauthorized access. Encryption is used to ensure high security for Images. Chaos has been widely used for image encryption for its different features. There are many chaos based encryption techniques. Most of the proposed discrete chaotic cryptographic approaches are based on stream or block cipher schemes. If these two schemes are combined the security level is improved. Novel image encryption is proposed based on combination of pixel shuffling. Chaos is used for expand diffusion & confusion in image. Chaotic maps gives advantages of large key space and high level security.

The initial value of chaotic map takes the original image as input sequence of bit provided by user mapped as control parameter. Output chaotic sequence produces the cipher image. Basic architecture of chaotic map represents that the small change in input bit stream produce a huge change in output bit stream after multiple round. Slight change of user key also produces totally different output sequence of bit stream. Usually a robust encryption scheme should have the fundamental characteristics such as mapping the plaintext to the random cipher text and it should be sensitive to the plaintext and Sensitive to the secret key.

The proposed algorithm will exhibit higher security as compared with the single chaotic map scheme. Due to the structure similar to the style of Feistel block cipher, the proposed algorithm can complete the encryption of two pixel blocks at one time, which is helpful for increasing data throughput. The security analysis shows that the method can resist many forms of cryptanalysis. An image encryption scheme is proposed based on chaotic standard map. Bit level permutation not only changes the locations of the image pixels, but also modifies their values. Due to features of bit level permutation, they have proposed a bit level confusion and dependent diffusion to enhance the security of cryptosystem. In this stage bit confusion operation reduces the computation redundancy. Finally they conclude that the new scheme has a satisfactory security level with a low computational complexity, which renders it a good candidate for real-time secure image transmission applications.

Rade Petrovic, Joseph M. Winograd, Kanaan Jemili and Eric Meto [6] presented data hiding within audio signals. In this paper they have presented the general principles of steganography, basic terminology, and an overview of applications and techniques. Particularly, they have consider data hiding within audio signals, basic requirements and the state of the art techniques. They wishes to propose a novel technique, the short-term autocorrelation modulation, with several variations. The proposed method is characterized by perfect transparency, high bit rate, robustness, low processing load and particularly high security.

A data message is hidden within a cover signal (object) in the block called embeddor using a stego key, which is a secret set of parameters of a known hiding algorithm. Stego signal (object) is the output of the embeddor. After transmission, recording and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor.The proposed approach is called the short-term autocorrelation modulation, and can be classified as a case of modulation of statistical properties of analog signals. The process is very simple, as inserting a delayed and/or advanced version of the signalitself can modify the autocorrelation.In order to optimize the process,it is require firstly to calculate natural autocorrelation, and then determine necessary modification.

Rade Petrovic, Joseph M. Winograd, Kanaan Jemili and Eric Meto [6] presented data hiding within audio signals. In this paper they have presented the general principles of steganography, basic terminology, and an overview of applications and techniques. Particularly, they have consider data hiding within audio signals, basic requirements and the state of the art techniques. They wishes to propose a novel technique, the short-term autocorrelation modulation, with several variations. The proposed method is characterized by perfect transparency, high bit rate, robustness, low processing load and particularly high security.

A data message is hidden within a cover signal (object) in the block called embeddor using a stego key, which is a secret set of parameters of a known hiding algorithm. Stego signal (object) is the output of the embeddor. After transmission, recording and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor.The proposed approach is called the short-term autocorrelation modulation, and can be classified as a case of modulation of statistical properties of analog signals. The process is very simple, as inserting a delayed and/or advanced version of the signalitself can modify the autocorrelation.In order to optimize the process,it is require firstly to calculate natural autocorrelation, and then determine necessary modification.

Mohamed Radoune and Taric Boujiha [7] presented a method of digital image watermarking using SVD Transform on DWT Coefficients with optimal block.In today's world the protection of data have become very important. To protect multimedia data against illegal copying and transferring, the insertion of a signal (digital signature, watermark) has become a duty without modifying quality of the original image.The goal of this operation is to identify the owner and protect his intellectual property. Digital watermarking has been proposed as a solution to solving the copyright problem by introducing invisible data (watermark) into original image. They have proposed the study of digital images watermarking. This study is achieved by inserting watermark in different coefficients of DWT (LH, HL, HH) using SVD transform by searching the optimal block that have the maximum entropy which can be used to insert the watermark in original image. Finally they have represented the different results of PSNR for each coefficient of DWT and the robustness against most attacks. They have presented a robust method of watermarking based on optimal block selected by the level value of entropy then have made modification in singular value decomposition (SVD) of this block after the application of DWT combined with DCT, to ensure the robustness and imperceptibility of their watermarking scheme.

The proposed algorithm combines the properties of SVD techniques,DWT, DCT to increase the robustness and capacity of the algorithm by selecting specific blocks which have the maximum entropy value. Finally they have proposed a robust watermarking method for copyright protection.This method based on combination of three transformations DCT, DWT, SVD using optimal block ensure the criteria of digital image watermarking, robustness, imperceptibility and capacity. The experimental results show that the best coefficients of DWT to insert watermark data is the HH and LH coefficients, so if we want increase the data capacity we can make the insertion of watermark data on both HH and LH simultaneously which will give the best results to ensure imperceptibility and robustness for this method against most attacks.

Deepthi S.,Renuka A. and Hemalatha S. [8] presented the technique of data hiding in audio signals using wavelet transform with enhanced security. For secure transmission of secret data with audio signal as the carrier, audio stegnography is used. In their proposed method, cover audio file is transformed from space domain to wavelet domain using lifting scheme, leading to secure data hiding. Using dynamic encryption algorithm text message is encrypted. Then, we have to hide cipher text is then in wavelet coefficients of cover audio signal. Signal to Noise Ratio (SNR) and Squared Pearson Correlation Coefficient (SPCC) values are computed to judge the quality of the stego audio signal. Results show that from the cover audio signal stego audio signal is perceptually indistinguishable.Even in presence of the external noise the stego audio signal is robust.So, with the help of the proposed method we can secure adta and can acieve the least error data extraction.

The wavelet transform (WT) has gained wide spread acceptance in image compression and in signal processing. Wavelet transform is the breaking up of a signal into shifted and scaled versions of the original (or mother) wavelet. A wavelet is a waveform of effectively limited duration that has an average value of zero. For signals the low-frequency component presents the identity of the signal. The high-frequency content only imparts savour or nuance. In human voice, if high- frequency components are removed, the voice sounds different, but still it can be understood. If low frequency components are removed, signal sounds gabble. On applying wavelet transformations on audio signal, approximation and detail components of audio can be obtained. The approximations are low-frequency components of the signal and details are high-frequency components. The first level detail coefficients have less importance in comparison with detail coefficients of next levels and approximation coefficients because of their low energy level. Figure shows the decomposition of audio signal on wavelet transform.

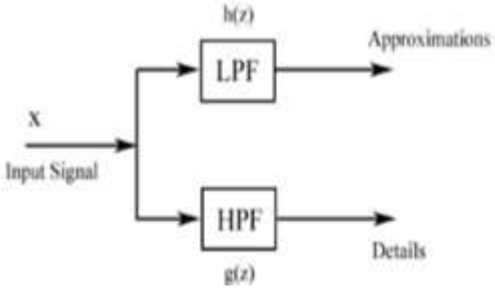


**Figure 2.1:** One stage signal decomposition

Finally we conclude that they have proposed method to hide encrypted text in cover audio using lifting wavelet transform. Number of bits used to hold secret data is chosen based on the values of coefficients. In the proposed method based on the message size text is encrypted and then hidden in cover audio. Results are then computed and observed. This algorithm yields good SNR and SPCC,zero error extraction. Similar technique is used by Sajad Shirali-Shahreza and M.T. Manzuri-Shalmani without encryption. There SPCC is not calculated, which is a good metric to test the audio quality based correlation. In their proposed method approximately same values of SNR and MSE are obtained as in even with encryption and noise added.

## 3. Proposed Work

Proposed system here with mainly consists of encryption algorithm as well as embedding algorithm. Encryption algorithm provides encryption technique to encrypt the secret audio file to be transmitted to the receiver. Embedding algorithm embeds the secret audio file into the cover image file with secret key in order to form steno cover image. Stego cover image get transmitted along the network towards the receiver. Receiver takes stego cover image as an input and gives it to the de-embedding algorithm. Receiver gets the secret audio file iff secret key get matched. In this way, encryption algorithm along with the data hiding technique provides perfect security to the audio file to be transmitted inside the digital cover image.

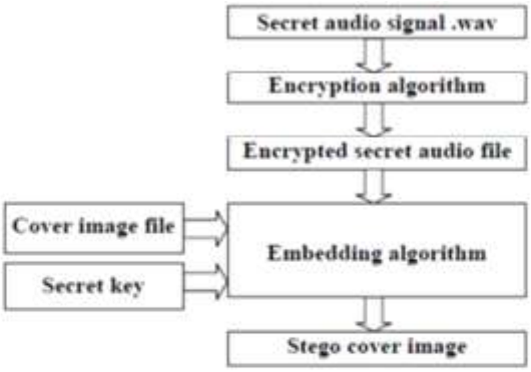


**Figure 3.1:** Transmitter Flow Diagram

Description of the transmitter flow diagram is as follows:

**1) Cover image file and secret key :**
Cover image is just like outer coverage provided to the audio file for security. Secret key is also provided for the same

purpose i.e., for the security. Cover image as well as secret key are provided to the embedding algorithm. Embedding algorithm embeds encrypted secret audio file into the cover image to form a stego cover image with secret key.

**2)Secret audio signal.wav :**
This is thesecret audio signal which we want to transfer from one location to the another location. In this case it is provided in the.wav form. First of all a secret audio signal in the.wav form is provided to encryption algorithm,

**3)Encryption algorithm :**
Encryption algorithm is basically provided toto encrypt secret audio signal in.wav form.

**4) Encrypted secret audio file:**
With the help of encryption algorithm after encrypting the secret audio signal in the.wav form we get the encrypted secret audio file.

**5) Embedding algorithms:**
Embedding algorithm embeds encrypted secret audio file into the cover image to form a stego cover image with secret key.

**6) Stego cover image:**
The output of the transmitter flow diagram is the stego cover image. The operation of hiding encrypted audio file into the digital image takes place at the transmitter side in order to provide perfect security in the form of stego cover image. In this way stego cover image get ready to transfer to the receiver side.

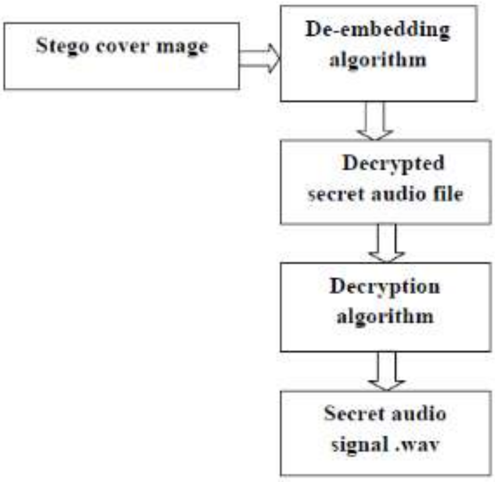


**Figure 3.2:** Receiver Flow Diagram

**Description of the transmitter flow diagram is as follows:**

**1)Stego cover image :**
The operation of hiding encrypted audio file into the digital image takes place at the transmitter side in order to provide perfect security in the form of stego cover image.To the receiver flow diagram we provide stego cover image as an input.

**2)De-embedding algorithm :**
Stego cover image transmitted by transmitter is provided as an input to the de-embedding algorithm. After applying de-embedding algorithm onto the stego cover image we will have cover image with secret key. Receiver will have a secret audio file if the secret key gets matched.

**3) Decrypted secret audio file:**
The decrypted secret audio file is given as an input to the decryption algorithm.

**4) Decryption algorithm:**
After applying decryption algorithm onto the decrypted secret audio file we will get desired secret audio signal as an output to the receiver side. In this way secret audio file reaches to the receiver side with highest security.

**5) Secret audio signal.wav:**
This is the output of the receiver flow diagram. The proposed technique of cryptography is the symmetric-key cryptography, in which sender as well as receiver uses the same key for encryption as well as decryption. For encrypting the secret audio file to be hide inside the digital image a secret key is used. Further the same secret audio file can be encrypted with the same cover image but, with different secret key. So, by doing this for the same secret audio file every time a new secret key is generated. Secret audio file encrypting procedure can be performed multiple times by using this technique.

## 4. Result and Discussion

### 4.1 System Design Flowchart

It is the system design flowchart which shows the flow of the system. When the project is started it first loads the secret short audio file. Then the secret short audio file is encrypted, so we get the encrypted secret audio file. It is then embedded on the cover image to form stego cover image. At the receiver, the stego cover image is first loaded and then we have to extract the encrypted audio from cover image. Then, there is authenticate data which is first checked and if it matches then only the secret audio will be decrypted otherwise error will occur. In this way the extracted encrypted audio is decrypted and we get our original secret audio

### 4.2 Transmitter block diagram

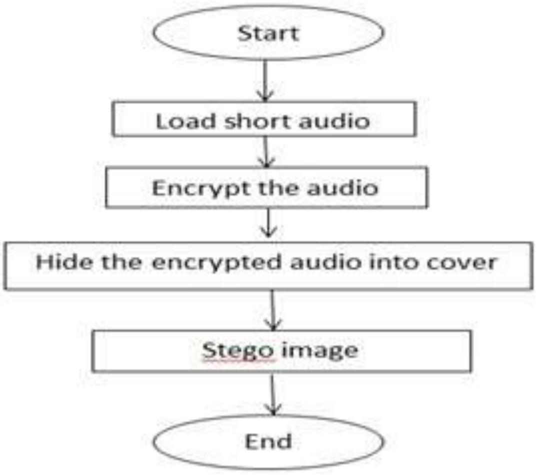


**Figure 4.2:** Transmitter block diagram

### 4.3 Receiver block diagram

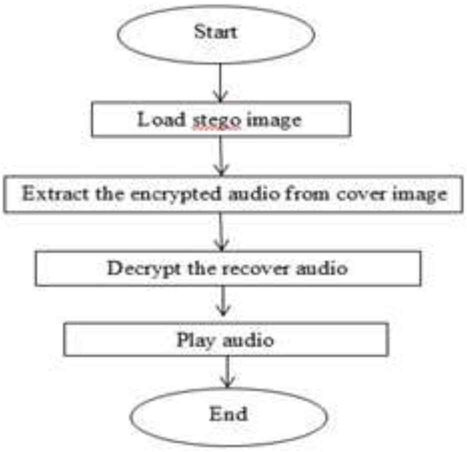
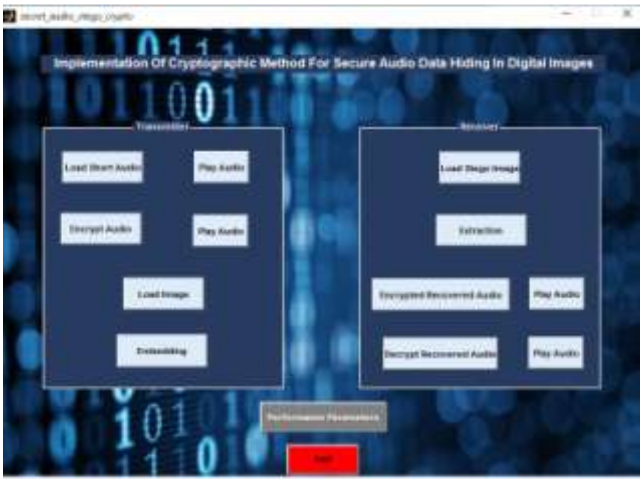

Start
Load stego image
Extract the encrypted audio from cover image
Decrypt the recover audio
Play audio
End

**Figure 4.3:** Receiver block diagram

### 4.4Screenshots

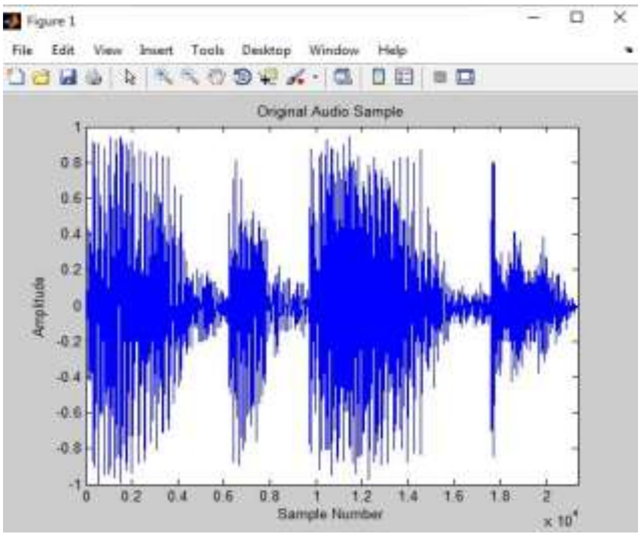
The proposed system is developed in the Matlab Software Tool and it is run as follows:



**Screenshot 4.4.1:** Home screen

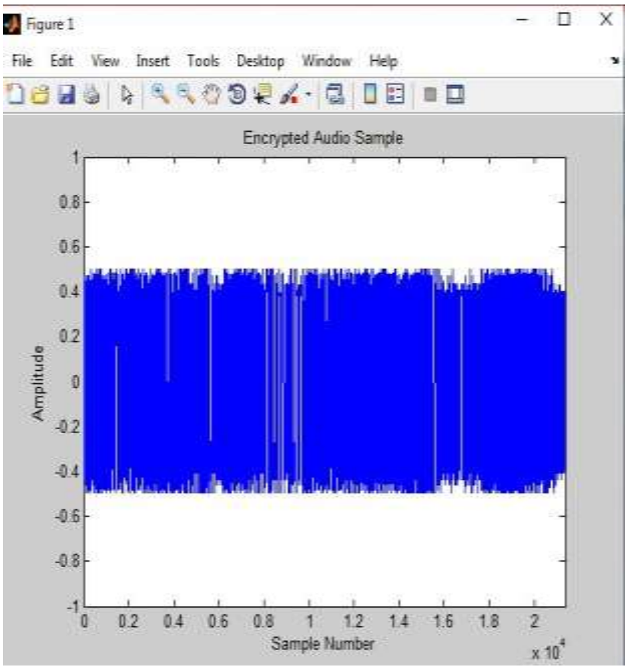
When the system is run, it is the first screen which appears. It contains all the operations to be performed on the system

### Case I



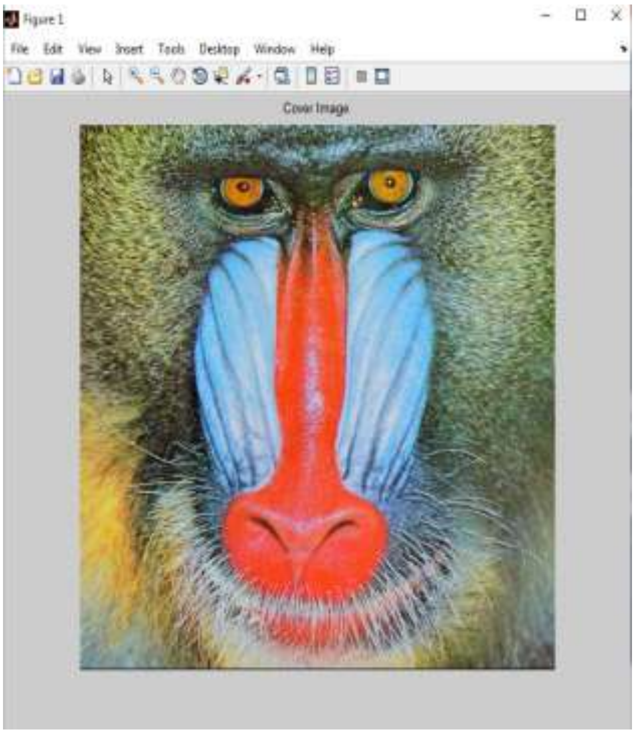
**Screenshot 4.4.2:** Load short audio

When we click on the load short audio file of size 20.9 kb, it selects the input short audio file and play it as shown below**.**



**Screenshot 4.4.3:** Encrypted Secret short audio

When we click on the encryption button, it performs the encryption on the secret short audio and displays the short audio as shown above.



**Screenshot 4.4.4:** Load Cover Image

When we click on the load cover image of size 1024x1024 button it selects the cover image and resize it and display in the figure.

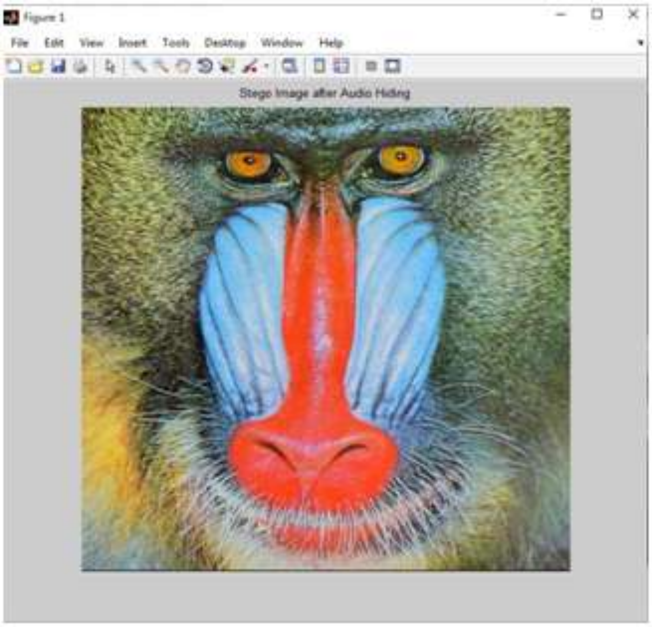


Figure 1
File Edit View Insert Tools Desktop Window Help
Stego Image after Audio Hiding

**Screenshot 4.4.5:** Embedded Image

When we click on the Embedding button it performs the integer wavelet transform and embeds the secret encrypted short audio file into the cover image to form the stego image.

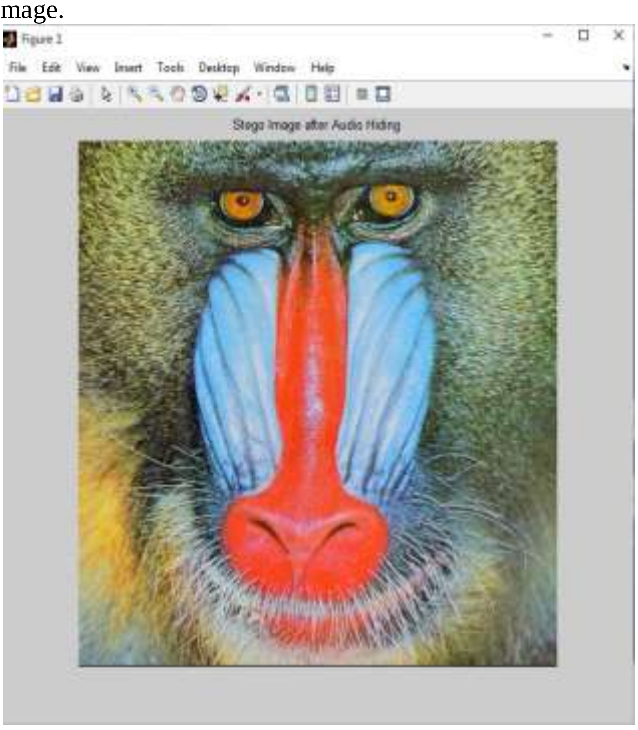
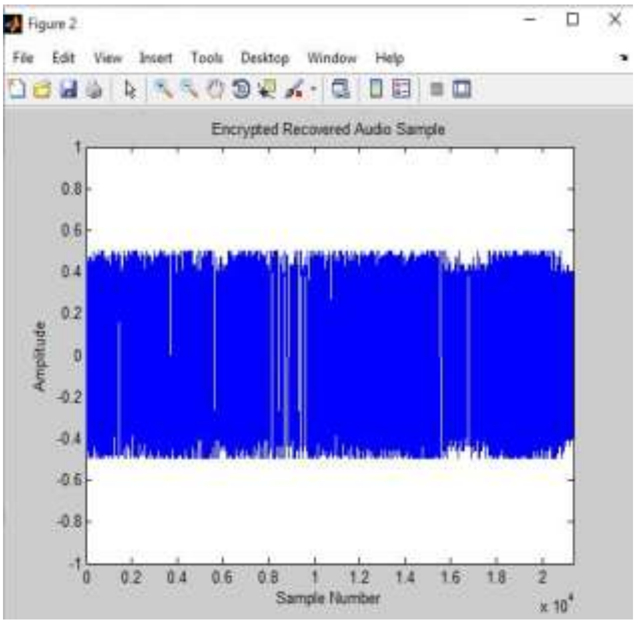


Figure 1
File Edit View Insert Tools Desktop Window Help
Stego Image after Audio Hiding

**Screenshot 4.4.6:** Load Stego Image

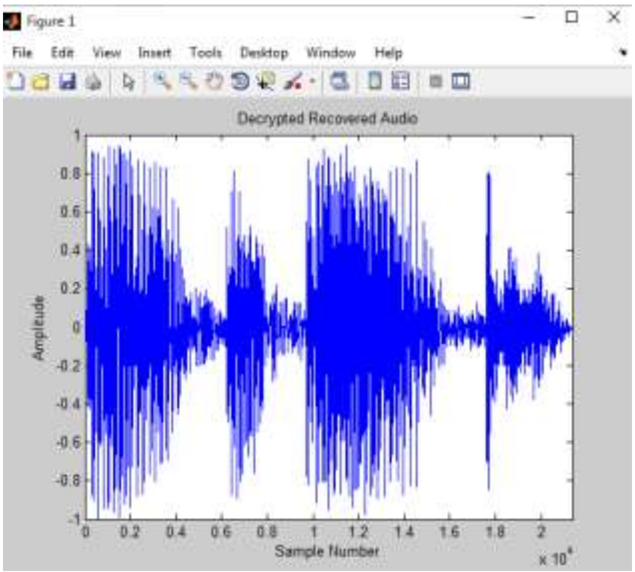
At the receiver when we click on the button Load Stego image it selects the Embedded Image from the output folder and displays it as shown in screenshot 6.6.

After the embedding of the image when we click on the Encryption to Stego Image button it performs the extraction and displays the encrypted secret short audio file and the cover image.



**Screenshot 4.4.7:** Encrypted recovered audio

When we click on the encrypted recovered audio button it play the encrypted short audio send by the transmitter.



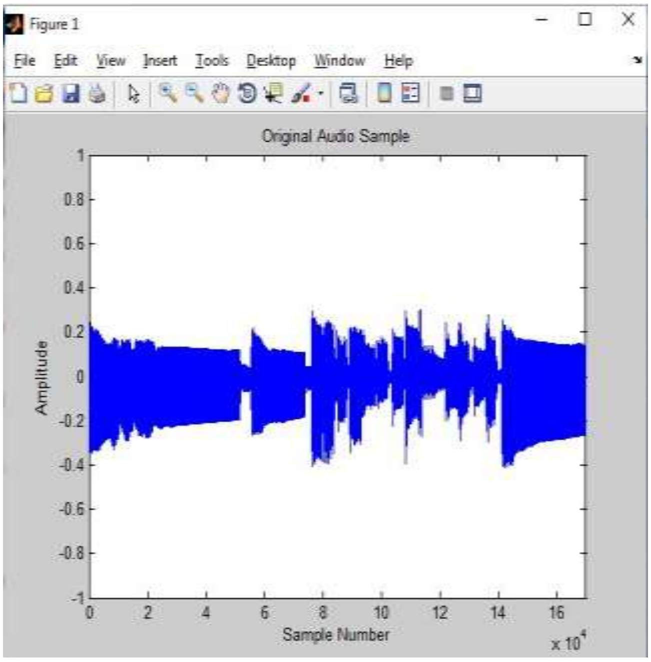
Screenshot 4.4.8: Decrypted recovered short audio

When we click on the decrypted recovered audio button it performs the decryption and play the decrypted secret short audio file. Hence, we get the original secret short audio back.

When we click on the Performance Parameters, it calculates and displays the values on command line.

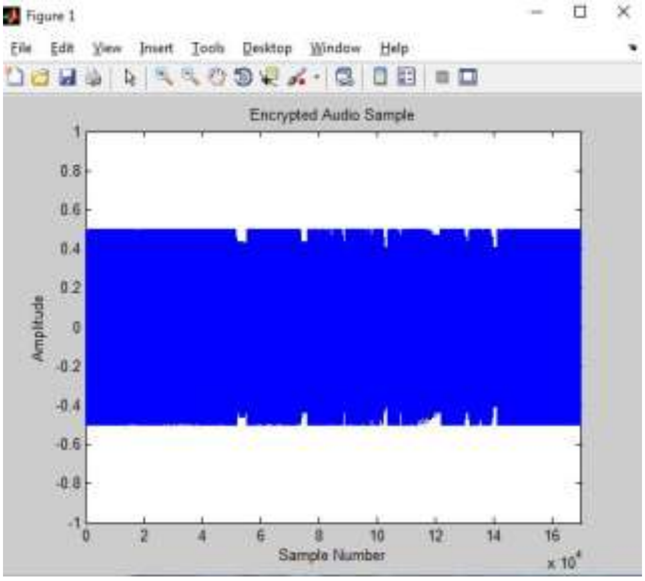
**CASE II**

Second case is that if audio file size is larger than capacity of image file size, then audio can't be hide. Let us see that case.



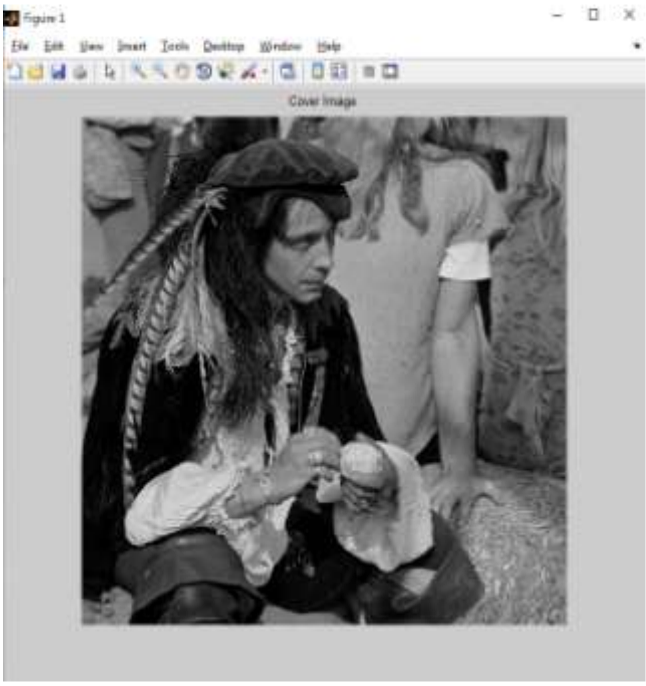
**Screenshot 4.4.9:** Load short audio

This is the original audio size of 331 kb of 169785 bytes of audio sample data.



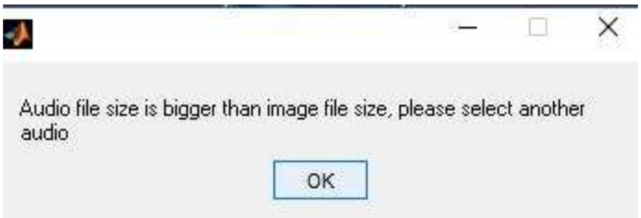
**Screenshot 4.4.10:** Encrypted Secret short audio

This is the encrypted audio sample



**Screenshot 4.4.11:** Load Cover Image

This is the cover image file size of 1024 x 1024 grayscale image, so total bit hiding capacity of size = 1024 x 1024 = 1048576 total bits of audio to hide = 169785 (bytes) * 8 = 1358280 so here hiding capacity is smaller than total audio capacity, so can't hide the audio and its respective message comes.



Audio file size is bigger than image file size, please select another audio

The proposed work is run for several short audio whose images and results are as follows:

### 4.5 Performance Parameters:

Encryptions and embedding of secret images are required to maintain original cover image statistics so that visual degradation is kept minimal low. Many performance measures are reported. To measure the imperceptibility of encryption and embedding several metrics are used. The metrics indicates how similar or different obtained recover image with original image is.

The following section explains the performance metrics used in this work.

**Mean Square Error (MSE):** MSE quantifies the difference between the cover image and the stego image. MSE is computed by performing byte by byte comparisons of the cover image and stego image. The Computation expressed as:

$$MSE = \frac{1}{NxM}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2$$

Where,
N,M=no of rows and column in the image
X(i,j)=pixel value at position (i,j) in the input image
Y(i,j)=pixel value at position (i,j) in the output image

**Peak Signal -To-Noise Ratio (PSNR):** PSNR is another widely used image quality metric that is expressed as the ratio of maximum gray scale intensity to MSE. It is expressed as shown in the equation below.

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

*R* is the maximum fluctuation in the input image data type. For example, if the input image has a double precision floating-point data type, then *R* is 1. If it has an 8bit unsigned integer data type, *R* is 255, etc.

The PSNR block computes the peak signal to noise ratio, in decibels (dB), between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image. Peak Signal-to-Noise Ratio (PSNR) assesses the quality of obtained image with respect to the original image.

**Root Mean Square Error (RMSE):**The root-mean-square error (RMSE) or root-mean-square deviation (RMSD) is a frequently used measure of the differences between values predicted by a model or an estimator and the values actually observed. The RMSE represents the sample standard deviation of the differences between predicted values and observed values. These individual differences are called residuals when the calculations are performed over the data sample that was used for estimation, and are called prediction errors when computed out-of-sample. Here RMSE is used to calculate error between the original ECG signal and the resulting newly constructed watermarked ECG signal. RMSE is calculated by using the equation: **RMSE** $=\sqrt{MSE}$

**Correlation Factor:** Correlation factor is one of the performance parameter. Correlation coefficient "r" is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related.

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

Where, xi - pixel intensity of original image
x- mean value of original image intensity
yi- pixel intensity of obtained image
y - mean value of obtained image intensity

**Signal to Noise Ratio (SNR):**Signal-to-noise ratio (SNR) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal. The formulae is

$$\mathrm{SNR_{dB}} = 10\log_{10}\left(\frac{P_{\mathrm{signal}}}{P_{\mathrm{noise}}}\right)$$

Where, SNR= Signal to noise ratio, Psignal is mean of original image's square and the Pnoise is mean of subtraction of original and modified image's square.

**Tabular Representation**

| Secret Audio (audio sample bytes) | Cover Image | MSE | RMSE | PSNR | Correlation | SNR |
|---|---|---|---|---|---|---|
| 20.9 kb (21371) | 1024*1024 | 0 | 0 | Inf | 1 | Inf |
| 331 kb (169785) | 1024*1024 | - | - | - | - | - |
| 31.5 kb (32240) | 1024*1024 | 0 | 0 | Inf | 1 | Inf |
| 15.8 kb (31000) | 1024*1024 | 0 | 0 | Inf | 1 | Inf |

**Figure 4.5:** Table of performance parameter's values for different images

## 5. Applications

Secured secret data transmission is required in many public places such as:

1) Banking sectors
2) Share markets
3) Educational sectors
4) IT industries

### 1) Banking sectors:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. With the wide-expansion of mobile telecommunication technology into the business world, mobile banking became the popular and promising banking method in bank industry recently. Mobile banking can provide customers with better quality and more cost-saving services. It refers to provision and availment of banking and financial services with the help of mobile telecommunication devices. The scope of provided services may include facilities to conduct bank and investment market transactions, to administer accounts and to access customized information. Most of the mobile banking researchers agreed that mobile banking consists of three parts: mobile accounting, mobile brokerage and mobile financial information services. But, now a days security in banking sectors carries a lots of importance. Many hackers hack the confidential data. So, in order to avoid this we can use the techniques such as cryptography as well as data hiding to secure the data.

**2) Share Markets**

A stock market, equity market or share market is the aggregation of buyers and sellers (a loose network of economic transactions, not a physical facility or discrete entity) of stocks (also called shares), which represent ownership claims on businesses; these may include *securities* listed on a public stock exchange as well as those only traded privately. Examples of the latter include shares of private companies which are sold to investors through equity crowd funding platforms. Stock exchanges list shares of common equity as well as other security types, e.g. corporate bonds and convertible bonds**.** As many attacks made on the data communication. In modern communication system data hiding is most essential for network security issue. So, with the help of encryption technique along with the data hiding we can provide more security.

**3) Educational Sectors**

The security in the education sector is incredibly important as the information collected by these institutes can be misused by hackers. The database comprise of students personal data such as: email id, home address, contact number, financial information, etc. Students educational data such as: projects, marks, etc. admission details, examination details, administration details, institute's employee details, financial data of the institute. The education sector, especially institutions of higher education has been the focus of information security professionals in recent times. It has been observed that the education sector ranks very high in the list of targets for cyber-attacks. The enormous amount of user information which can be easily comprised attracts the cyber criminals. These range from student's personal information, credit card data or financial aid records. Additionally, educational institutions also generate a lot of intellectual property through research, which is lucrative for cyber criminals. So, with the help of cryptographic technique we can develop robust system to provide more security.

**4) IT Industries:**

When a major company experiences a data breach, it's all over the news. It makes sense. These big companies have access to sensitive data for millions of people and a data breach makes them all potential victims of identity theft. But, these big security breaches are only part of the story. The fact is regardless of the size your company is at risk. If If you are dealing with the sensitive data. It's important to take measures to secure it properly for the safety of your customers and for your own liability. The amount of information that companies must keep secure is increasing. As a result of technological advances, companies are constantly gaining more data about their clients and customers. They must ensure that data security and privacy remain a priority to protect against costly breaches. We can protect data by using the cryptography as well as data hiding techniques.

## 6. Conclusion and Future Scope

### 6.1 Conclusion

Cryptography along with the steganography definitely provides the better security. Steganography helps us to hide information to be transmitted over network and cryptography makes the secret message not understood unless the decryption key is available. Many hackers bits-level to achieve greater strength of encryption which is hidden inside the cover image. Security can also be achieved by using the various algorithms such as AES, DES and triple DES but, the time required for encryption as well as decryption for this algorithm is more. However, the Bra algorithm used for file encryption and decryption takes smallest amount of time and provides more security. The encryption of this project is to provide a new technique which will provide better security for hiding the short audio data by using BRA algorithm along with embedding method forming a robust system for data hiding. Proposed system can hide the short secret audio file in an encrypted form into a cover image. So that it will be difficult for the hacker to hack it. Receiver gets the encrypted secret audio file by performing the extraction on the stego image. Later by performing decryption on the encrypted short audio file receiver will get the original secret audio file. We have taken the test on different short audio files by hiding it into cover image in order to obtain the desired results by using embedding, encryption, decryption, data hiding and extraction technique. Performance analysis of BRA algorithm for file encryption and decryption process is done in this project. After performance analysis results shows the performance of the Byte Rotational Algorithm is drastically better algorithm. Steganography using the wavelet based LSB technique has also given the better performance. Finally, we conclude that the proposed system provides the strong security.

### 6.2 Future scope

In future work, we can implement techniques which will reduce time and improve network security by using the combination of different steganography and cryptography techniques. In proposed system, we have used the secret short audio file so respectively used the short size of the image. However, if the sender wants to hide the large audio file then sender has to use the large size of the image. Also, project can be extended to use the different secret data such as text, image or video or can do the same for cover data file.

## References

[1] Punam V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande, "Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security", IEEE, P.P. 2015 International Conference on Pervasive Computing (IPCP).

[2] Tawfiq S. Barhoomand Zakaria M. Abusilmiyeh, "A Novel Cryptography Method Based on Image for Key Generatio",IEEE P.P. 2013 Palestinian International Conference on Information and Communication Technology.

[3] Harshitha K M, Dr. P. A. Vijaya "Secure Data Hiding Algorithm Using Encrypted Secret message", International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012

[4] Guangyong Gao and Yun-Qing Shi, Fellow, IEEE "Reversible Data Hiding Using Controlled Contrast Enhancement and Integer Wavelet Transform",IEEE, P.P. 2015

[5] MinalGovindAvasare, VishakhaVivekKelkar "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT),2015.

[6] RadePetrovic, Joseph M. Winograd, Kanaan Jemili and Eric Metois, "DATA HIDING WITHIN AUDIO SIGNAL", Series: Electronics and Energetics vol. 12, No.2 (1999).

[7] Mohamed RADOUANE, Rochdi MESSOUSSI, Raja, Tarik Bhoujiha. "Robust Method of Digital Image Watermarking using SVD Transform on DWT Coefficients with Optimal Block",IEEE 2014.

[8] Deepthi S. 1,Renuka A. 2 and Hemalatha S. 3, "DATA HIDING IN AUDIO SIGNALS USING WAVELET TRANSFORM WITH ENHANCED SECURITY", CS & IT-CSCP 2013

[9] Preeti Jain1, Vijay Kumar Trivedi 2, "A Novel Technique for Data Hiding in Audio by Using DWTS", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012

[10] Sheetal A. Kulkarni, Shubhangi B. Patil "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", 2015 International Conference on Pervasive Computing (ICPC)

[11] Rintu Jose, GincyAbraham,"A Separable Reversible Data Hiding in Encrypted Image with Improved Performance",International Conference on Microelectronics, Communication and Renewable Energy ( ICMiCR-2013)

[12] Chandra Prakash Shukla, Mr. Ramneet S Chadh, "International Journal of Advanced Research in Computer Science and Software Engineering", IJARCSSE 2014.

[13] Sheetal A. Kulkarni, Shubhangi B. Patil, "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", IEEE, P.P. 2015InternationalConference on Pervasive Computing (ICPC).

[14] Rupesh Gupta, Dr. TanuPreet Singh, "New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters", IEEE, p.p. 2014.

[15] Harshitha K M, Dr. P. A. Vijaya, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE, P.P.( ICMiCR-2013) International Conference on Microelectronics, Communication and Renewable Energy.

[16] N. Umate, ShubhangDhengre, "IMPLIMENTATION OF ADVANCED ENCRYPTION ALGORITHM", IORD, vol-1, Issue-5, ISSN 2348-0831, pp. 33-39, July-August 2014.

[17] M. Madhurya, B. A. Krishna, T. subhashini, "Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks", IJCNIS, Vol-2, pp.30-37, January 2014.

[18] Krishna Kumar Pandey, VikasRangari, Sitesh Kumar Sinha, "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security", International Journal of Computer Applications, Vol. 74, No. 29, PP. 29-33, July 2013.

[19] S. M. Elshoura, D. B. Megherbi, "A secure high capacity full-gray-scale-level Multi-image information hiding and secret image authentication scheme via Tchebichef moment," Journal of signal processing, Vol. 28, PP. 531-552, 2013.

[20] Sunil. K. Moon Rajshree D. Raut "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security" Proceedings Of the2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).