VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELAGAVI-590018, KARNATAKA

MINI PROJECT REPORT

ON

"Audio encryption and decryption using python."

Submitted by

PRAJWAL N G
1CR21EC151

Under the guidance of

Dr. Imtiyaz Ahmed B K
Associate Professor, Dept. of ECE
Department Of Electronics and Communication Engineering
October – February 2023

Department Of Electronics and Communication Engineering

CMR INSTITUTE OF TECHNOLOGY

#132, AECS LAYOUT, IT PARK ROAD, KUNDALAHALLI,

BENGALURU-560037

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify the Mini Project Report entitled “**Audio encryption and decryption using python**”, prepared by **PRAJWAL N G**, bearing **USN 1CR21EC151**, a bona fide student of **CMR Institute of Technology, Bengaluru** in partial fulfillment of the requirements for the award of **Bachelor of Engineering in Electronics and Communication Engineering** of the V**isvesvaraya Technological University, Belagavi-590018** during the academic year 2022-23.

This is certified that all the corrections and suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Mini Project has been approved as it satisfies the academic requirements prescribed for the said degree.

Signature of Guide
Dr. Imtiyaz Ahmed B K
Associate Professor
Dept. of ECE, CMRIT

Signature of HOD
Dr. R Elumalai
Professor & HOD
Dept. of ECE, CMRIT

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people whose proper guidance and encouragement has served as a beacon and crowned my efforts with success. I take an opportunity to thank all the distinguished personalities for their enormous and precious support and encouragement throughout the duration of this seminar.

I take this opportunity to express my sincere gratitude and respect to **CMR Institute of Technology, Bengaluru** for providing me an opportunity to present my mini project.

I have a great pleasure in expressing my deep sense of gratitude to **Dr. Sanjay Jain,** Principal, CMRIT, Bangalore, for his constant encouragement.

I would like to thank D**r. R Elumalai,** HOD, Department of Electronics and Communication Engineering, CMRIT, Bangalore, who shared his opinion and experience through which I received the required information crucial for the mini project.

I consider it a privilege and honor to express my sincere gratitude to my guide **Dr. Imtiyaz Ahmed B K** Associate Professor, Department of Electronics and Communication Engineering, for the valuable guidance throughout the tenure of this review.

I also extend my thanks to the faculties of Electronics and Communication Engineering Department who directly or indirectly encouraged me.

Finally, I would like to thank my parents and friends for all their moral support they have given me during the completion of this work.

THANK YOU

Prajwal N G

(1CR21EC151)

ABSTRACT

Securing data encryption and decryption using Cryptography and Steganography techniques. Due to recent developments in stego analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using stego analysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for communication between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using RSA. In Steganography we are using Image Steganography for hiding the data. And we also use Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. Since we use algorithm for securing the data and again on this we perform Steganography to hide the data in an image. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

CONTENTS

LIST OF FIGURES

Chapter 1 INTRODUCTION

Speech to text conversion is the process of converting spoken words into written texts. Speech is one of the most important and basic tool for the communication between humans and his environment. A voice encryption system is developed as a real-time software application. Basically, the speech is taken as an input and is encoded to be decoded by authenticated users only The environment may include computers, mobile phones, etc. The human computer interaction is termed as human computer interface. In order to establish such an interface, keyboard and mouse forms the most common method for interaction. When the amount of data to be entered is large, then these devices become time consuming. For an efficient communication to take place, we tend to change the method of interaction.

According to human beings, the best way of communication between them is speech. If a system can understand what a human speaks, then it is the best method of interaction between a human and a computer. υ Speech control or widely known as Speech Recognition is the method to control something by human voices/speech. Speech recognition technology is one of the fastest growing engineering technologies. It has a number of applications in different areas and provides potential benefits. Nearly 20% people of the world are suffering from various disabilities; many of them are blind or unable to use their hands effectively. The speech recognition systems in those particular cases provide a significant help to them, so that they can share information with people by operating computer through voice input.In order to share some confidential data between people, secure communication must be ensured. This could be brought into picture by introducing encryption and decryption of the message to be delivered which in audio format i.e. speech. υ Encryption is considered one component of a successful security strategy. Successful encryption completely depends on robust passwords and pass phrases called “keys”.

1.1.1 Cryptography:

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like confidentiality, privacy, nonrepudiation, key exchange, and authentication.

1.1.2 Fernet:

Fernet is a recipe that provides symmetric encryption and authentication to data. It is a part of the cryptography library for Python, which is developed by the Python Cryptographic Authority (PYCA). There are a range of different use cases for Fernet.

Symmetric-key Encryption: In symmetric-key encryption, the data is encoded and decoded with the same key. This is the easiest way of encryption, but also less secure. The receiver needs the key for decryption, so a safe way need for transferring keys. Anyone with the key can read the data in the middle.

1.1.2.1 Steps

1. Import Fernet
2. Then generate an encryption key, that can be used for encryption and decryption.
3. Convert the string to a byte string, so that it can be encrypted.
4. Instance the Fernet class with the encryption key.
5. Then encrypt the string with the Fernet instance.
6. Then it can be decrypted with Fernet class instance and it should be instanced with the same key used for encryption.

1.1.3 Problem Statement:

The purpose of this project is to provide the correct data with security to the users. For some of the users the data might be lost during the transmission process in the network and for some, the data might be changed by the unauthorized person in the network and there are some other security problems in the network. Our application will give you more Security to the data present in the network and there will be able to reduce the loss of data in the network which will be transmitted from the sender to the receiver using the latest technologies.

Only the Authorized persons i.e., who are using our application will be 8 there in the Network. The proposed algorithm is to hide the audio data effectively in an image without any suspicion of the data being hidden in the image. It is to work against the attacks by using a distinct new image that isn’t possible to compare.

The aim of the project is to hide the data in an image using steganography and ensure that the quality of concealing data must not be lost. We used a method for hiding the data in a distinct image file in order to securely send over the network without any suspicion the data being hidden.

This algorithm, though requires a distinct image which we can use as a carrier and hide the data which is well within the limits of the threshold that the image can hide, that will secure the data.

At present there are many encryption and decryption, especially in the communication system provided in a variety of application.

Encryption and decryption is particularly impacted in the field of military communications and reliable security data to protection for transmitting.

Chapter 2 Encryption and Decryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.

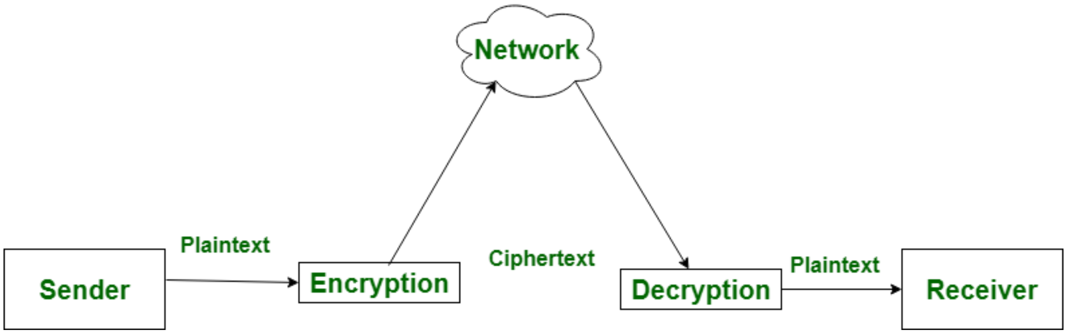


Fig 2. Encryption and Decrtption

2.1.1 The Public Key:

As asymmetric cryptosystem or public key cryptosystem, this technique use two keys which use separately for encrypting and decrypting the information. In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. The key used for encryption is stored public therefore it's called public key, and the decryption key is stored secret and called private key.

2.1.2 The Private Key: The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption of secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption.

Chapter 3 Methodology

So, this technique combines the features of cryptography and provides a high level of security. It is better than either of the technique used separately.

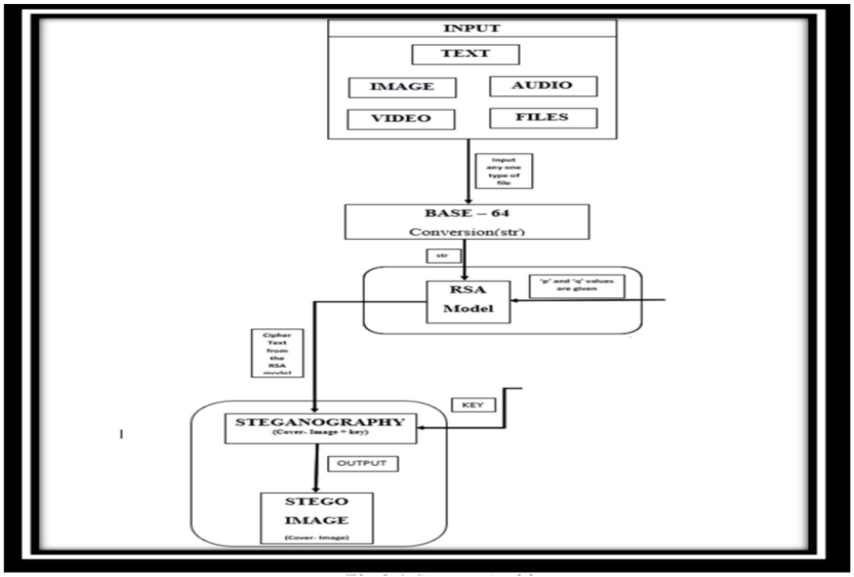


Fig 3. Methodology

There will be an agreement between the sender and the receiver about the key for the concealment algorithm as well as the key for the encryption algorithm or these keys may be exchanged by a secure communication method. Our method starts by encryption first then hide encrypted data.

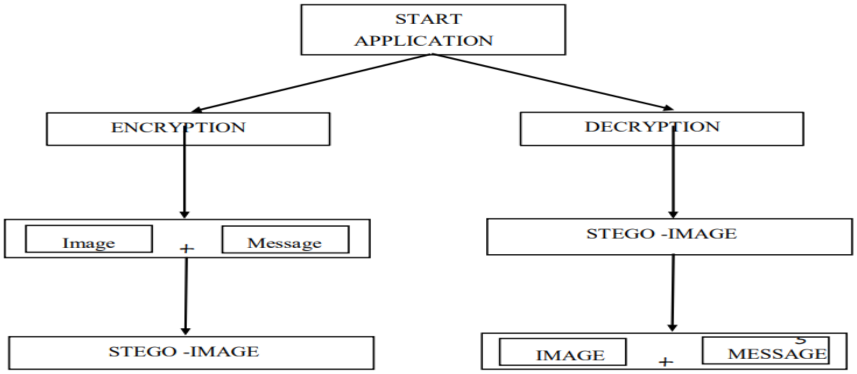


Fig 3.1 Flowchart for Encryption and Decryption

- The proposed methodology consists of two stages: encryption and decryption of the audio signal.
- Public and private keys are generated previously and then the public key is used to encrypt the acquired speech or audio samples at the transmitter.
- The ciphered or encrypted audio samples are sent to receiver sequentially through a communication channel who will decrypt each sample by employing the private key.
- For simplicity, it is assumed that the transmission or communication channel is ideal or free of noise.

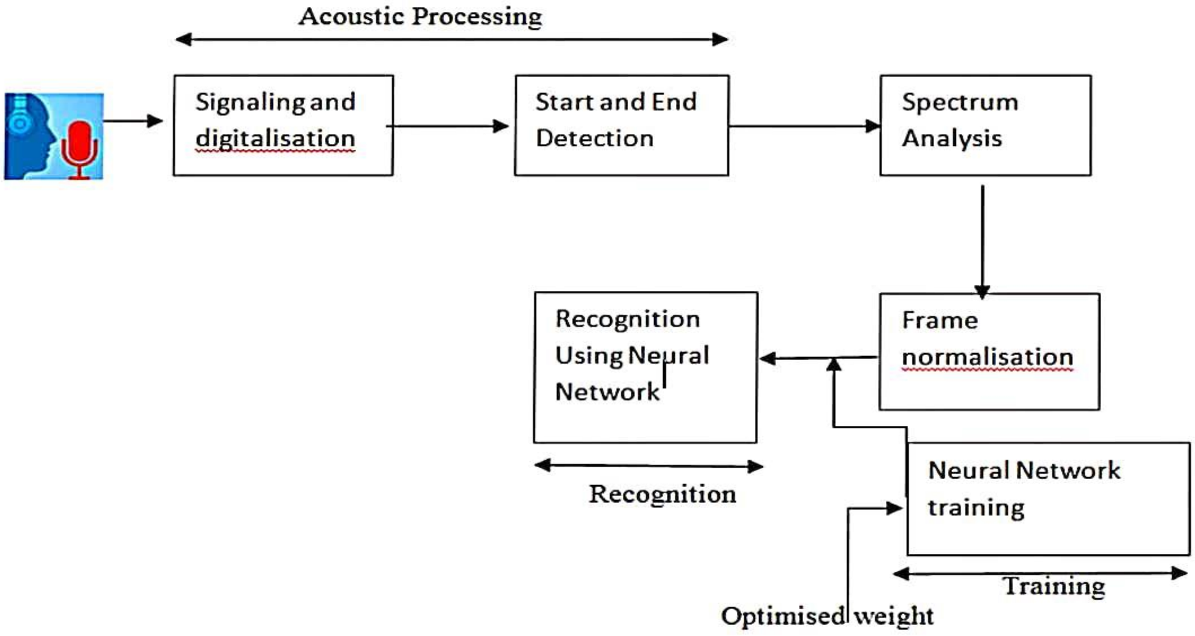


Fig 3.1 Process of audio Encryption and Decryption

the original key from fernet_ key:

Set fernet_ key to new _fernet _key, old_ fernet _key

Run airflow rotate-fernet-key to re-encrypt existing credentials with the new fernet key

Set fernet _key to new _fernet_ key

3.1.1 Implementation

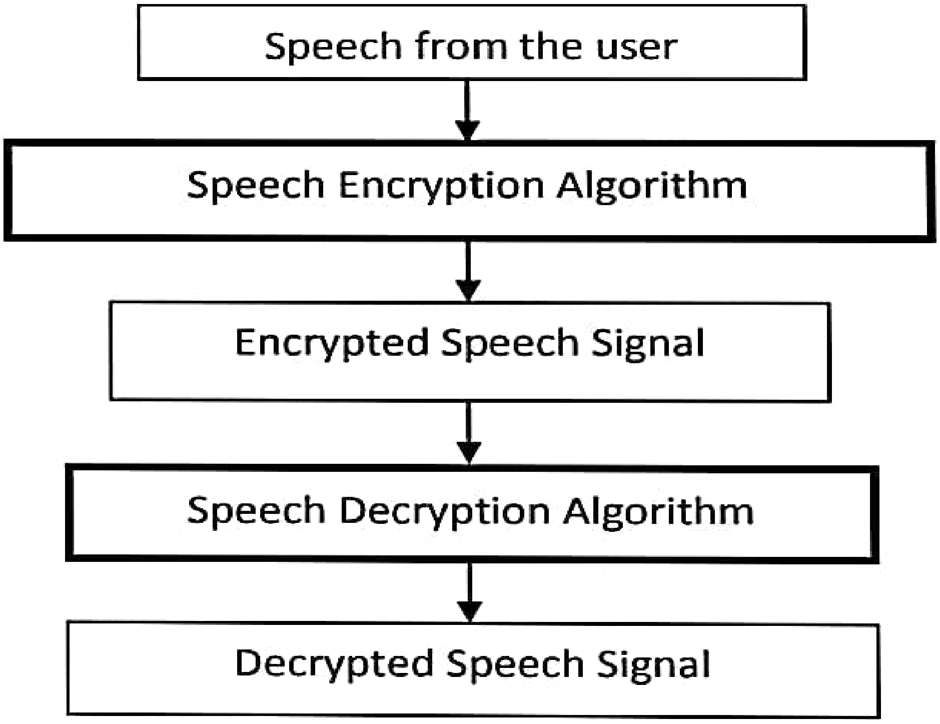


Fig 3.1.1.1 Flowchart for Implementation of Encryption and Decryption

```
From cryptography. fernet import Fernet
 # we will be encrypting the below string.

message = "hello geeks"

# generate a key for encryption and decryption

# You can use fernet to generate

# the key or use random key generator

# here I'm using fernet to generate key

key = Fernet. generate _key()

# Instance the Fernet class with the key
```

```
fernet = Fernet(key)
# then use the Fernet class instance
# to encrypt the string string must
# be encoded to byte string before encryption

incessive = fernet.  encrypt(message .encode())
print("original string: ", message)
print("encrypted string: ", enc Message)
 # decrypt the encrypted string with the
# Fernet instance of the key,
# that was used for encrypting the string
# encoded byte string is returned by decrypt method,
# so decode it to string with decode methods
dec Message = fernet. decrypt(enc Message).decode()
print("decrypted string: ", dec Message)
```

Chapter 4 Program

```
#import the module

from cryptography. fernet import Fernet

#key generation

Key _ enc = Fernet. generate_ key()

print (key _enc)

b'Em-c19-LnFMrTdEfeZ2JTFDlNu9O7B6houvv8YWnW9Q='

#encryption
fernet=Fernet(key _enc)

print(fernet)

audio file="C:/Users/Prajwal N G/Downloads/first.wav"

with open('keyfile.key','wb') as file key:

    file key .write(key_ enc)

with open('keyfile.key','rb') as file key:

    key_ dec = file key .read()

with open(audio file,'rb') as file:

    original audio = file. read()

encrypted=fernet. encrypt(original audio)

with open('voice encryption.wav','wb') as encrypted  _file:

    encrypted. file. write(encrypted)


#Decryption

fernet=Fernet(key _enc)

with open('voice encryption.wav', ‘rb') as enc _file:

    encrypted=enc _file. read()
```

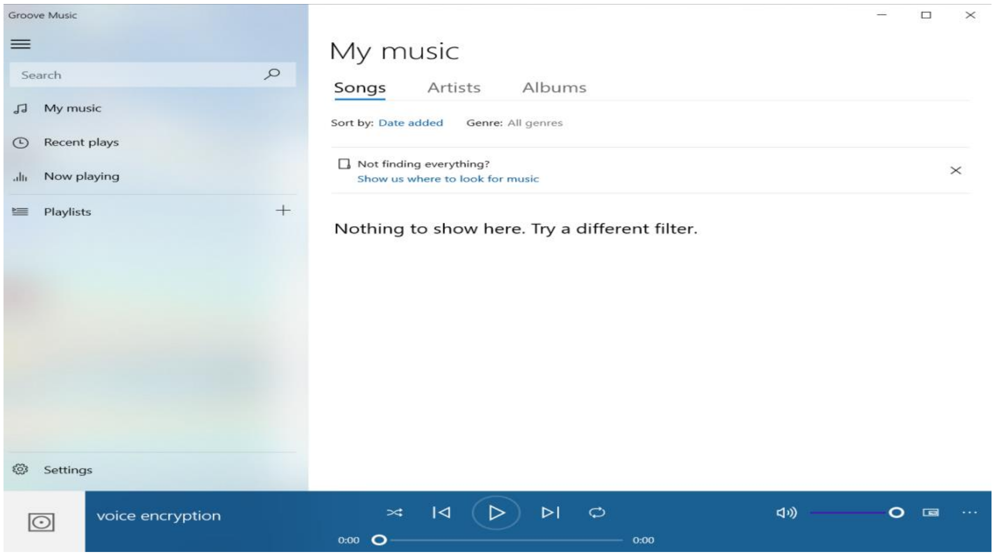
```
decrypted =fernet. decrypt (encrypted)

with open('voice decryption .wav', 'wb') as dec _file:

    dec _file. write(decrypted)
```

Chapter 5 Result

5.1.1 Encryption



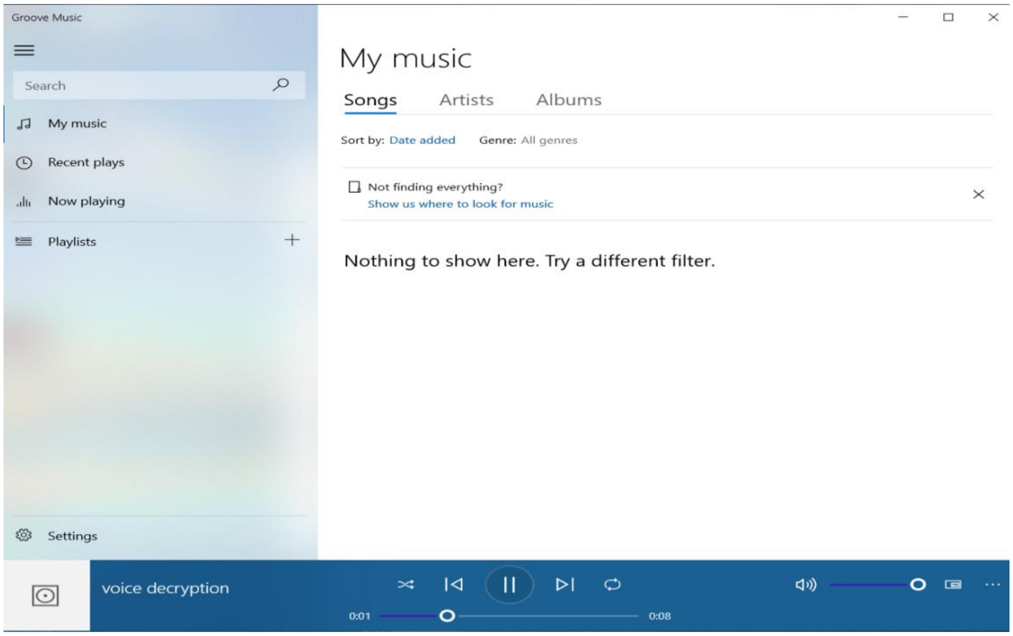
Sort by: Date added Genre: All genres

Not finding everything?
Show us where to look for music

Nothing to show here. Try a different filter.

Fig 5.1.1 Encryption

5.1.2 Decryption



Sort by: Date added Genre: All genres

Not finding everything?
Show us where to look for music

Nothing to show here. Try a different filter.

Fig 5.1.2 Decryption

Chapter 6 Conclusion

The proposed model introduced above is a combination of cryptography and Steganography. The goal of the technique is to put the unauthorized person in a difficult position to determine the presence of information. The dual security makes the information more secure. With this model any one can easily send multiple information to the receiver using public network. This model is very useful for defense, corporate, banking, communication and different government portals where information exchange is more crucial. The data hiding capacity in audio and video is more than image, so in future using audio or video steganography and cryptography huge amount of data will transmit in public network without security violence.

Reference

[1] M. M Amin, M. Salleh, S. Ibrahim, M.R.K at min, and M.Z.I. Shamsuddin, Information Hiding using Steganography, National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003 IEEE.

[2] S Ushll , G A Sathish Kumal, K Boopathy bagan ,A Secure Triple Level Encryption Method Using Cryptography and Steganography, 20 II International Conference on Computer Science and Network Technology, 978-1- 4577-1587-7/111$26.00 ©20111EEE, December 24-26, 2011

[3] X. Zhang and S. Wang, Steganography using multiple base notational system and human vision sensitivity, IEEE Signal Process. Lett., vol.12, no. I, pp. 67-70, Jan. 2005.

[4] Behrouz A. Forouan, Deb deep Mukhopadhyay, 2nd edition Cryptography and network security, McGraw Hill Education, pp.295-296

[5] S. M. Masud Karim, Md. Sai fur Rahman, Md. Ismail Hossain, A New Approach for LSB Based Image Steganography using Secret Key987-161284-908- 9/11/$26.00 2011 IEEE

[6] M. Hossain, S.A. Haque, F. Sharmin, Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information, Proceedings of 200912th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[7] Controlled NOT gate, From Wikipedia, http://en,wikipedia. org/wiki/Controlled _NOT _gate .

[8] Ivan W. Selesniek "Wavelet Transforms A Quick Study", Physies Today magazine, üetober, 2007.

[9] "Blum Blum Shub", From Wikipedia, http://en.wikipe dia.org/wiki/ Bluffi _Bluffi _ Shub

[10] R Praveen Kumar, V Hemanth, M Shareef, Securing Information Using Sterganoraphy, 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]