ENCRYPTION AND DECRYPTION OF SPEECH AND IMAGE SIGNALS

A PROJECT REPORT

Submitted by

Bhavesh Kasliwal (10BCE1026)

Shraey Bhatia (10BCE1094)

Shubham Saini (10BCE1097)

in partial fulfillment for the course

Discrete Time Systems and Processing

(ECE-104)

Computer Science and Engineering

School of Computing Science and Engineering

VIT UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
www.vit.ac.in
Vellore ▪ Chennai
CHENNAI CAMPUS
Vandalur - Kelambakkam Road, Chennai - 600127

November - 2013

ABSTRACT

- Data encryption has always been a very important part of military communications.
- Technically speaking, digital encryption of data is always the best approach, in which the original data x is first digitized into a sequence of bits, x (k) which are then encrypted digitally into a different sequence of bits, y (k) before transmission.
- Digital transmission is always much more efficient than analog transmission, and it is much easier for digital encryption techniques to achieve a very high degree of security.
- That is to convert the data into an unknown form and then the ciphered data is transmitted.
- The person who know, how the data is encrypted can decrypt (i.e. converting the ciphered data into original signal) the signal. Thus security of sending data is done.
- Encryption is a much stronger method of protecting speech communications than any form of scrambling.
- Eg: Voice encryptors work by digitizing the conversation at the telephone and applying a cryptographic technique to the resulting bit-stream.
- In order to decrypt the data, the correct encryption method and key must be used.

INTRODUCTION

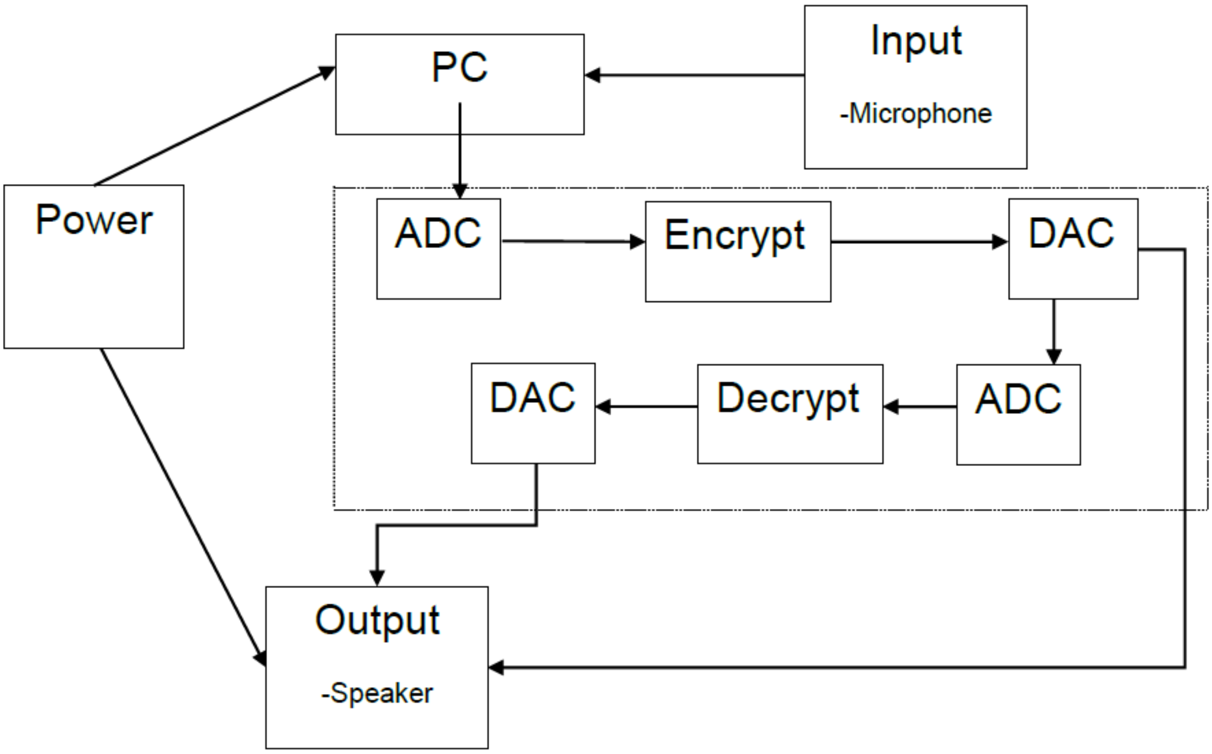
- In recent trends, cell phone, voice chat, Skype video calls etc., is the main topic of the communication. But it is not possible to speak secretly through them.
- Our objective is to speak secretly, i.e., to maintain security of certain important information.
- Also, the images to be transferred are encrypted into a secure form.
- Efficient speech and image encryption technique is required for recent communication, not only over digital but also analogue data transmission lines without invasion of privacy. So for that we are going for encryption and decryption of the signal and develop a software program in MATLAB.
- Here the voice and image signals is acquired and then digitally coded and stored in the memory. Then using the symmetric key cryptography it encrypts the data, again convert it to analogue signal and transmit it. Similarly at receiver end the signal is digitally coded, we decrypt the data using cipher key and converts it again in voice signal. This process is called cryptographic method.

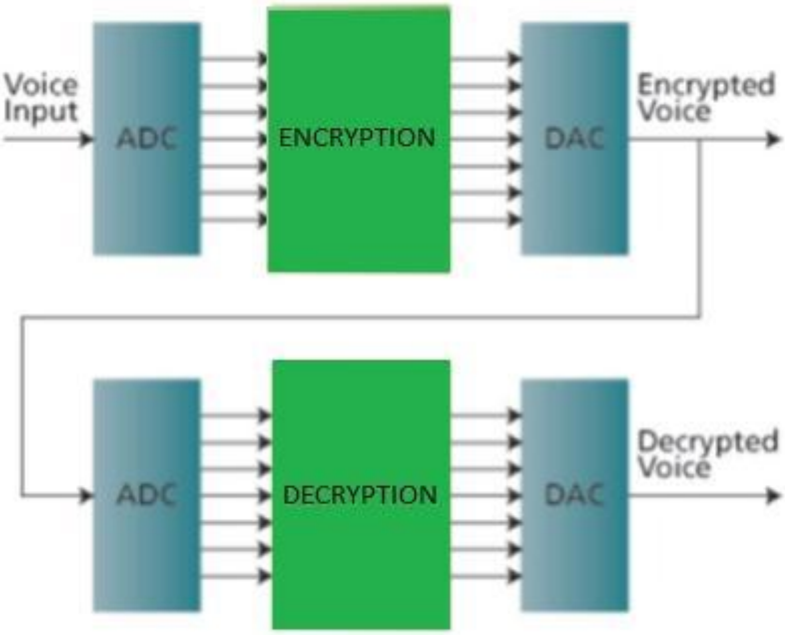
CORE IDEA

- To encrypt and decrypt the voice and image signal.
- Firstly convert analog input signal to digital and then take its XOR. And convert it into analog. This will be our encrypted signal.
- And then convert analog signal into digital and then take its XOR and convert this digital signal into analog and this will be our decrypted signal.

IMPLEMENTATION

Implementation block diagram:-





APPROACH

Encryption:-

- Give voice and image signal to the mat file.
- Convert analog to digital signal.
- Take XOR of the code and this will be my encrypted digital data.
- Convert it into analog encrypted signal.

Decryption:-

- Convert encrypted analog signal into digital.
- Take XOR of the code and then convert it into analog.
- This analog signal will be decrypted signal.

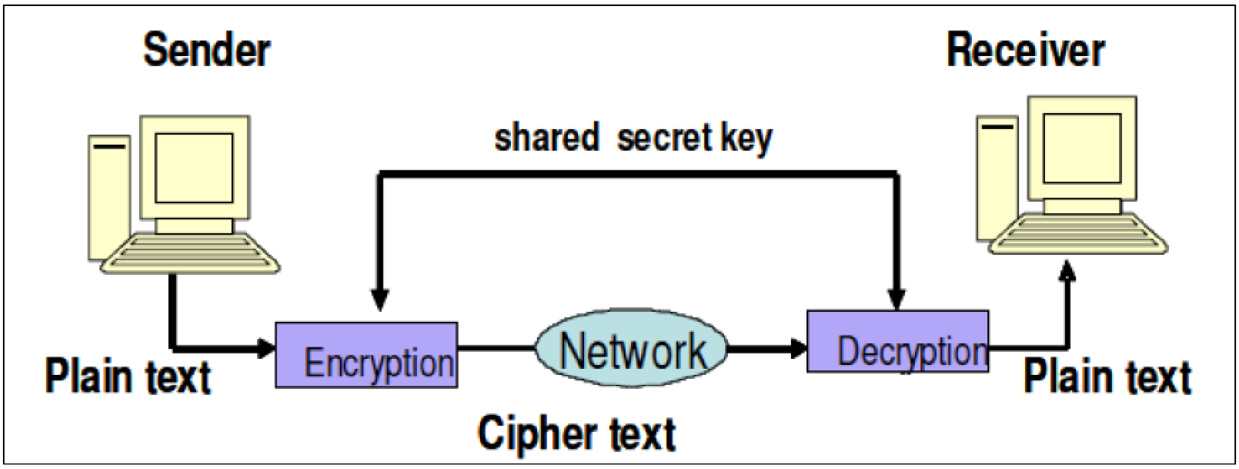
SOME DEFINITIONS

cryptography:-

- Cryptography refers to the science of transforming messages to make them secure and immune to attacks. It is the study of mathematical techniques for attempting to defeat cryptographic techniques and, more generally information security services so for the message to be secured and immune to attack we need to encrypt our message at the sender site and decrypt at receiver site.

The components involved in cryptography are –

a) Sender
b) Receiver
c) Plain text
d) Cipher text
e) Encryption and decryption algorithms
f) Network



- The original message before being transferred is called, plaintext.
- The message after being transferred is called, cipher text. This message contains all the information of the plaintext message but is not in a format readable by a human or computer without the proper mechanism to decrypt it.
- The Algorithm which transfers a plain text to cipher text is called Encryption algorithm.
- Encryption algorithm is used by sender.

- The algorithm which transfers cipher text to plain text is called Decryption algorithm.
- Decryption algorithm is used by receiver.
- A cipher is an algorithm for performing encryption and decryption. The sender-receiver pair in a network uses the cipher for a secure communication. A key is a number or a piece of information as an algorithm upon which the cipher operates. Hence for the encryption of a message we need an encryption algorithm, an encryption key, and plain text. Similarly to decrypt a message we need a decryption algorithm, a decryption key, and cipher text.

TYPES OF CIPHER

Modern ciphers can be classified according to how they operate and whether they use one or two keys. All the Encryption method of cryptography algorithms are divided into two groups:
1) symmetric-key cryptography algorithms (private key cryptography)
2) public-key cryptography algorithms
In this project we are using symmetric-key cryptography algorithm. In the cryptography the encryption and decryption algorithms are public but the key is secret. We have to protect only the key rather than the encryption and decryption algorithms.

SYMMETRIC-KEY CRYPTOGRAPHY:-

In symmetric-key cryptography, a common key is shared by both sender and receiver. The sender uses an encryption algorithm and the same key to encryption of data and the receiver uses a decryption algorithm and the same key for the decryption of data. In this process of cryptography the algorithm used for decryption is reverse of encryption algorithm. The shared key set up in advance and kept secret from all other parties.
Advantages of Symmetric key cryptography algorithm:-

- It takes a less time to encrypt a message using symmetric key algorithm than a message using public key algorithm.
- The key is usually smaller so symmetric key algorithms are used for to encrypt and decrypt long messages.

Disadvantage of Symmetric key cryptography algorithm:-

Each pair of user must have a unique key, so a large number of keys are required, hence distribution of keys between two parties can be difficult.

BENEFITS

We can use this technique in military for sending secret messages. We can use this technique wherever we want security.

Can be used for mobile services like blackberry which uses encrypted data for transmission.

CONCLUSION

We have successfully implemented encryption and decryption of speech and image signals using Private Key cryptography technique by the method of cumulative XOR operations.