Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Encryption of an Audio File on Lower Frequency Band for Secure Communication

Sheetal Sharma*, Lucknesh Kumar
Dep. Of CSE, GCET,
Greater Noida , India

Himanshu Sharma
Dep. Of ECE, M.U.
Aligarh, India

Abstract: Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information. It also enables verifiability of every component in a communication. In this paper a frequency domain of the wav audio signal is taken for the encryption and decryption. Here, we use the DFT (Discrete Fourier Transform) for transforming the time domain audio signal to frequency domain audio signal. An audio signal can be separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. Here, we apply RSA technique for the encryption and decryption on the lower frequency bands because all the frequency regions do not participate equally in the communication. After applying the encryption on different frequency bands, we observe that, the encryption on the lower frequency band is more effective than the higher one. So, we would apply encryption on lower frequencies with higher phase values. Here we are applying our technique on phase values.

Keyword--- Histogram, Wav Signal, DFT, Frequency Domain, Power Spectrum.

I. INTRODUCTION

Among human beings, there have always been a need of security and privacy of data. Therefore, the concept of encryption is as old as the fact that secret data have been interchange between the people. Over the decades from Caesar cipher to RC4, a number of different encryption techniques have been purposed and implemented. However, most of the proposed techniques encrypt only text data, a very few technique are proposed for image, audio and video data. The techniques which are for text message encryption also applied to other multimedia data but satisfactory results have not been achieved. Encryption of an audio signal is more difficult than text message, due to its complex nature. U.S., Defense Department, began the work on audio encryption in late 1940's. Initially the research was used in World War II for secured communication. For providing the security so that enemies could not understand the conversation among military people, the idea first was introduced by simply adding some noise to a voice signal. The main concept was, a noise signal is added by playing a recorded noise in synch with the voice signal and at the receiving point, the noise signal was subtracted out in order to get original voice signal. But there was a need of same noise signal at both the ends, so the noise signal were made in pairs , one for sender and one for receiver . Therefore, the idea was very robust as by using only two copies of the signal, it was very difficult to decrypt the encoded signal [2]. U.S. defense department had given this project to Bell laboratories, to implement this concept. The implemented system is called Sigsaly [2]. So the Sigsaly was the first implemented idea of most secure voice encryption system. Selective encryption is a modern approach to reduce the computational requirements for huge volumes of multimedia data in distribution networks with diverse client device capabilities.

Cryptography is the most important characteristic of communications security. Cryptography is becoming more and more important as a fundamental building block for data security. Cryptography systems can be generally classified into private-key cryptography (symmetric-key systems) and public-key cryptography (asymmetric–key systems). Symmetric-key systems are the systems that use a single key that both the sender and recipient have and Asymmetric-key or public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Four common goals in cryptography are as follows, *first* is message confidentiality: Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information, *second* is message Integrity: The recipient should be able to determine if the message has been altered, *third* is sender authentication: The assurance that the communicating entity is the one that it claims to be, and *fourth* is sender Non-repudiation: It prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was received by the alleged receiver.

The main idea presented in this paper is that the audio data can be subdivided in two parts: a more relevant fraction to be encrypted, and a remaining part that is less significative and can be left unprotected. On the other hand, we can say that our approach encrypts only10 to 12% of the whole data. In this paper we consider only the phase values of the frequencies of an audio signal. The main advantage of this approach to full encryption of the whole data (bit stream) is its lower complexity because less bits need to be encrypted.

Selective encryption is sometimes known as the partial encryption. Particularly, selective encryption can be employed not only to achieve the same perceptual effect of full encryption (that means of complete content protection) but also to preserve the original quality with limited and controlled disturbance. In our technique, we partially encrypt the audio signal on phase values because in that case (in the case of speech or audio signal) only loss of intelligibility may be sufficient, instead of complete loss of all perceptual information.

II. HISTOGRAM

A histogram is a graphical representation of the distribution of data. It is an approximate of the probability distribution of a continuous variable. A histogram is a representation of tabulated frequencies, shown as adjacent rectangles, erected over discrete intervals (bins), with an area equal to the frequency of the observations in the interval. The height of a rectangle is also equal to the frequency density of the interval, i.e., the frequency [9] divided by the width of the interval. The total area of the histogram is equal to the number of data. The density of data can be plotted by using the histograms, and often for density estimation: estimating the probability density function of the underlying variable. The total area of a histogram used for probability density is always normalized to 1. If the length of the intervals on the x-axis is all 1, then a histogram is identical to a relative frequency plot.

III. WAVE FILE

A standard waveform audio format, called a wav file, has given by Microsoft and IBM. This format is Windows' custom file format for representing digital audio data. Due to the popularity of Windows and the a number of computer programs written for the platform, the wav file has become one of the most widely supported digital audio file formats on the computers. Most of the program that can open and/or save digital audio supports this file format, making it both extremely useful and a virtual requirement for software developers to understand. This format takes more space than other formats because it stores uncompressed audio data. But wav file contain more information about the data and provide high quality of audio. The SINE WAVE is the simplest waveform, since it has only one FREQUENCY associated with it. These AUDIO waveforms are often termed fixed waveforms because of their lack of variation, whereas acoustic waveforms are constantly varying. The waveform represents the behaviour of the sound in the time domain. Waveform is sometimes used synonymously with TIMBRE, because of its shape is indicative of the frequency content of the sound, although all contributing factors to timbre cannot be understood simply in terms of the waveform.

IV. DISCRETE FOURIER TRANSFORM (DFT)

The frequency analysis of discrete time signal is usually and conveniently performed on a Digital signal processor.To convert time-domain discrete signal into frequency domain discrete spectrum, DFT is useful transformation. A continuous time signal links into discrete-frequency domain by using Fourier series. The periodicity of time-domain signal forces the spectrum to be discrete. The N-point discrete Fourier transform of a discrete- time signal g[n] or discrete time sequence is given as

$$\mathrm{G}[k] = \sum_{n=0}^{N-1} g[n] \exp(-j2\pi nk/N), \quad k = 0,1,2 \ldots. N-1$$

And the corresponding Inverse Discrete Fourier Transform (IDFT) is given as

$$\mathrm{G}[k] = \sum_{n=0}^{N-1} g[n] \exp(j2\pi nk/N), \quad k = 0,1,2 \ldots. N-1$$

Where

N is the number of time sequence values of g[n]. It is also the total number of frequency sequence values in G[k]; T is the time interval between two consecutive samples of the input sequence g[n]; F is the frequency interval between two consecutive samples of output sequence G[k].

N, *T* and *F* are related by the expression

$NT = 1 / F$

NT is also equal to the record length. The time interval, T, between samples should be chosen between the Shannon's sampling theorem is satisfied. This means that should be less than the reciprocal of $2f_H$ *where* f_H is the highest significant frequency component in the continuous time signal g*[t]* from which the sequence g[n] was obtained. Several fast DFT algorithms require N to be an integer power of 2. So, we can say that the DFT of a discrete-time sequence g(n) is obtained by performing the sampling operation in both the time domain and frequency domain. Here, g(n) be a finite duration sequence.

A discrete-time function will have a periodic spectrum. The time function and frequency functions are periodic in DFT. Because of the periodicity of DFT, it is common to regard points n=1 through n=N/2 as positive, and points from n=N/2 through n=N-1 as negative frequencies. In addition, since both the time and frequency sequences are periodic, DFT values at points n=N/2 through n=N-1 are equal to the DFT values at points n=N/2 through n=1.

Properties of Discrete Fourier Transform (DFT):In the practical techniques for processing signals, the properties of DFT are quite useful. These properties of DFT are as – Periodicity, Linearity, Shifting property, Time reversal of a sequence, Circular time shift, Circular frequency shift, Circular convolution, circular correlation, Complex conjugate property, Multiplication of two sequences, Parseval's Theorem.

V. SAMPLE FLOW DIAGRAM OF OUR APPROACH

A. Flow diagram of Encryption process

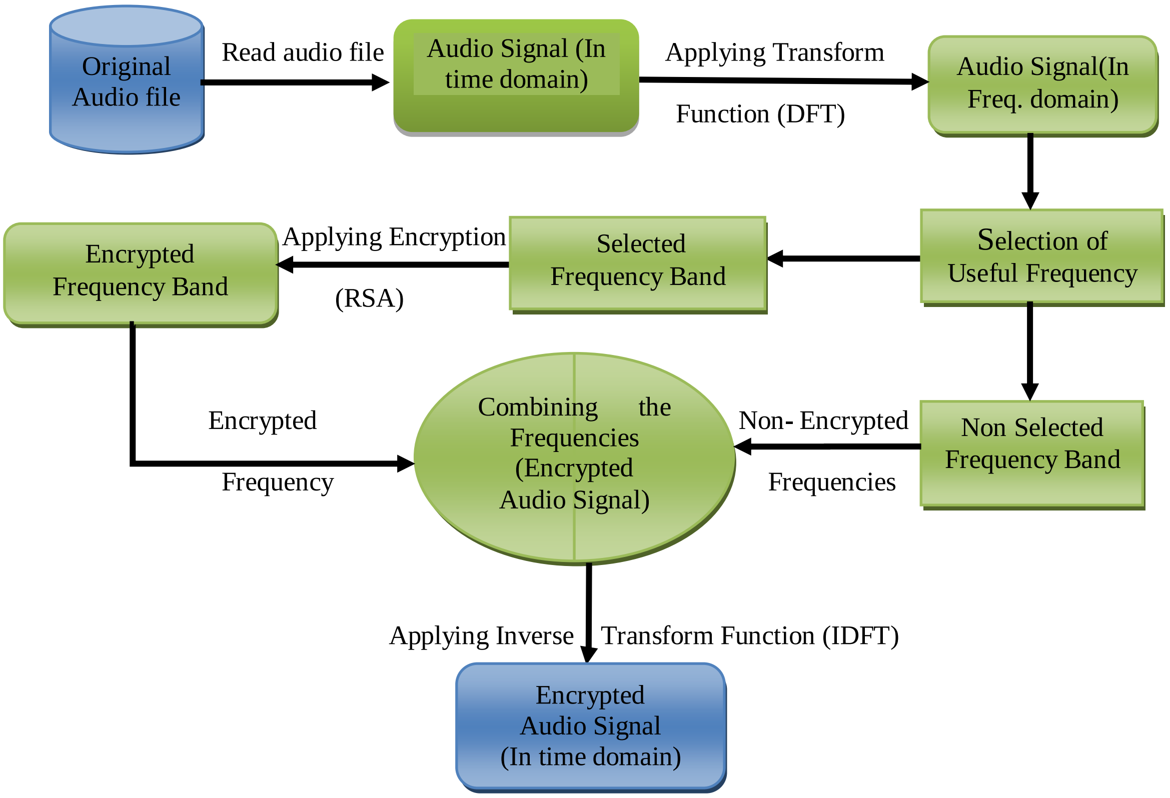
Original Audio file
Read audio file
Audio Signal (In time domain)
Applying Transform
Function (DFT)
Audio Signal(In Freq. domain)
Selection of Useful Frequency
Selected Frequency Band
Applying Encryption
(RSA)
Encrypted Frequency Band
Encrypted
Frequency
Combining the Frequencies (Encrypted Audio Signal)
Non- Encrypted
Frequencies
Non Selected Frequency Band
Applying Inverse
Transform Function (IDFT)
Encrypted Audio Signal (In time domain)

Figure-1: DFD for Encryption

B. Flow diagram of Decryption process

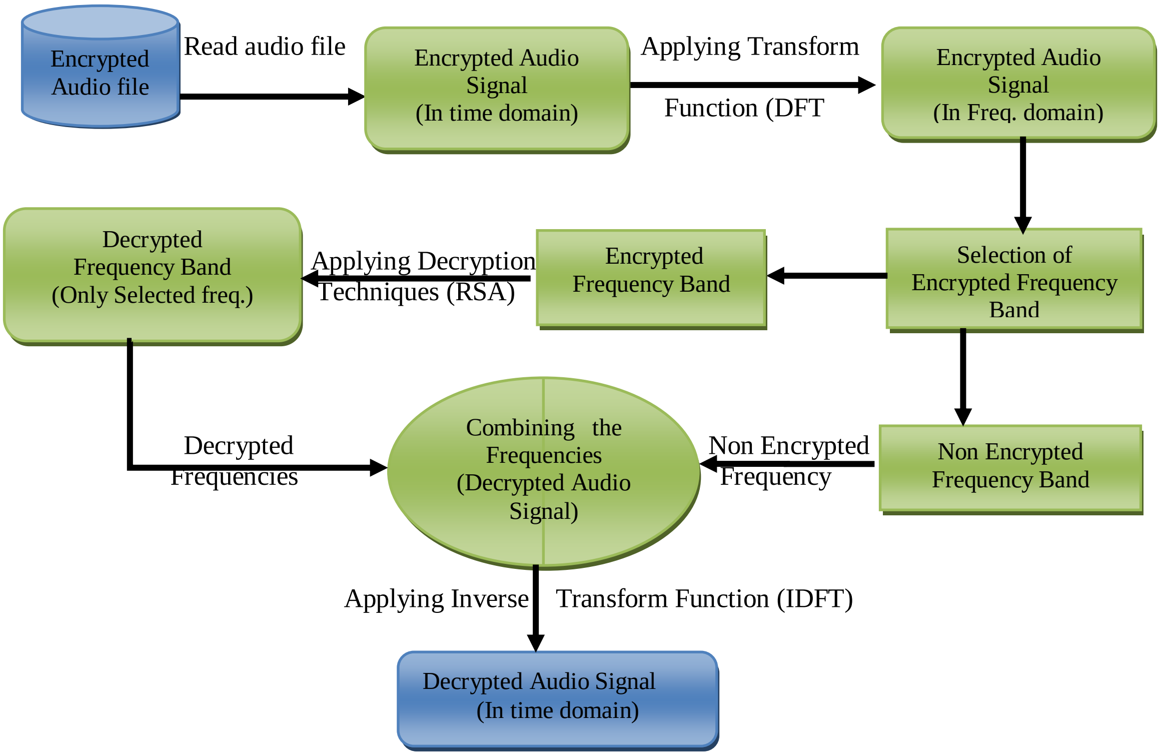
Encrypted Audio file
Read audio file
Encrypted Audio Signal (In time domain)
Applying Transform
Function (DFT
Encrypted Audio Signal (In Freq. domain)
Selection of Encrypted Frequency Band
Encrypted Frequency Band
Applying Decryption
Techniques (RSA)
Decrypted Frequency Band (Only Selected freq.)
Decrypted
Frequencies
Combining the Frequencies (Decrypted Audio Signal)
Non Encrypted
Frequency
Non Encrypted Frequency Band
Applying Inverse
Transform Function (IDFT)
Decrypted Audio Signal (In time domain)

Figure-2: DFD for Decryption

VIII. OBSERVATIONS

A. TIME DOMAIN ANALYSIS

1) The original wav signal is

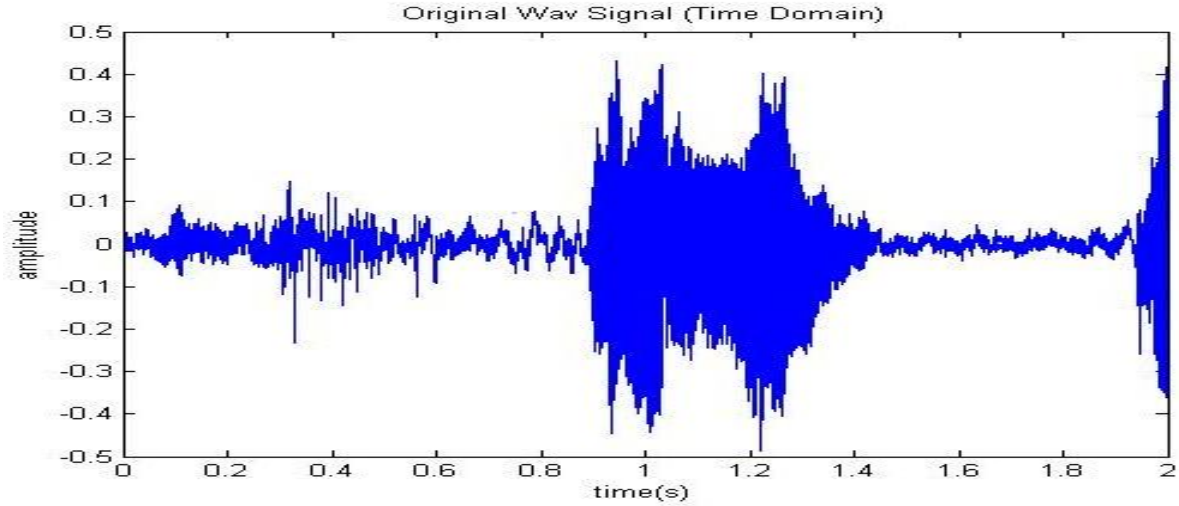

Fig-3: Original Wav Signal

2) The encrypted wav signal [1] is

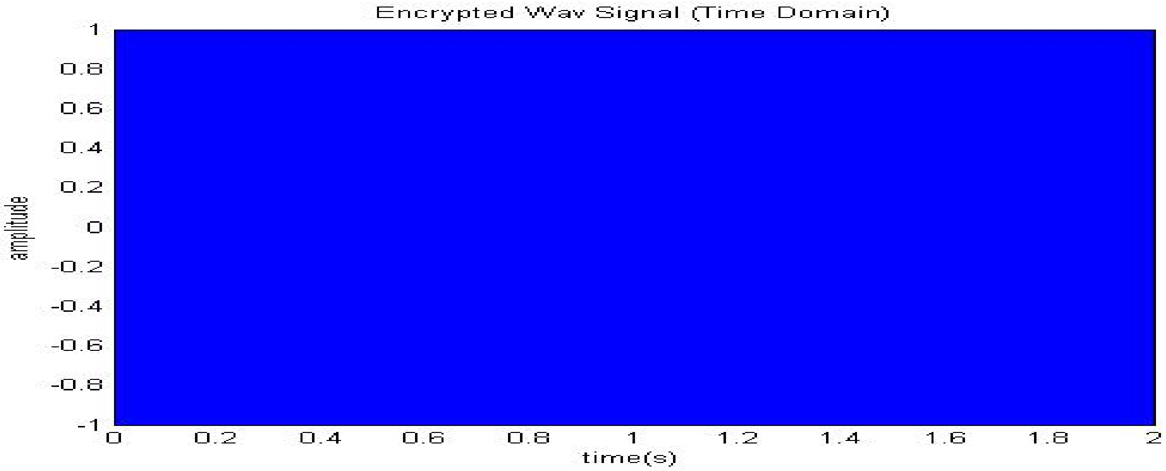

Fig-4: Encrypted Wav Signal

3) The decrypted wav signal is

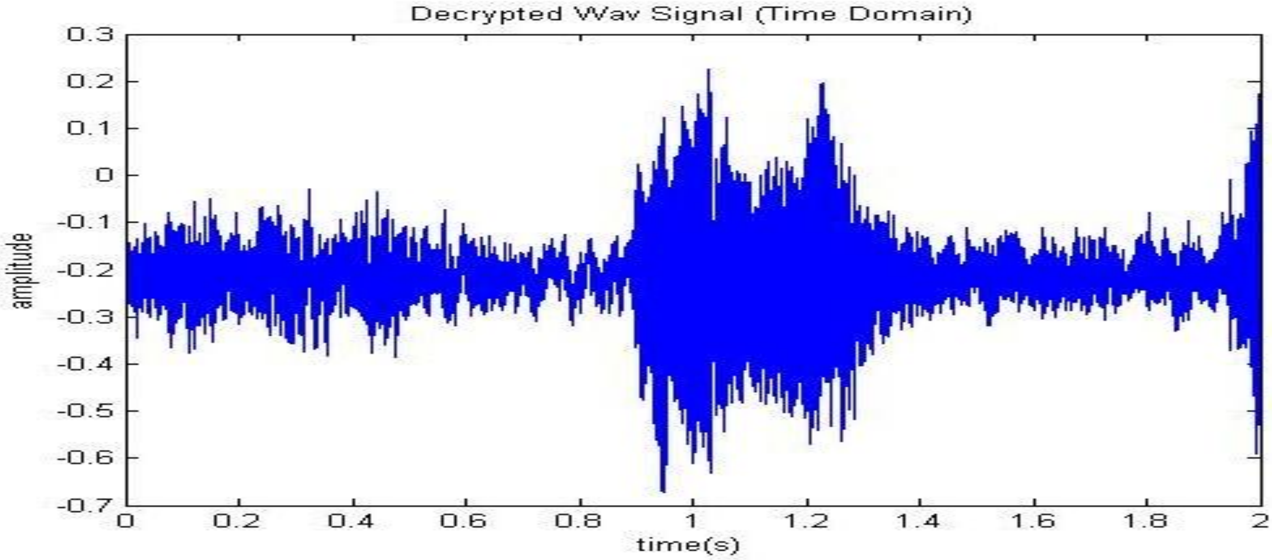

Fig-5: Decrypted Wav Signal

C. FREQUENCY DOMAIN ANALYSIS:

1) The original power spectrum in frequency domain is:

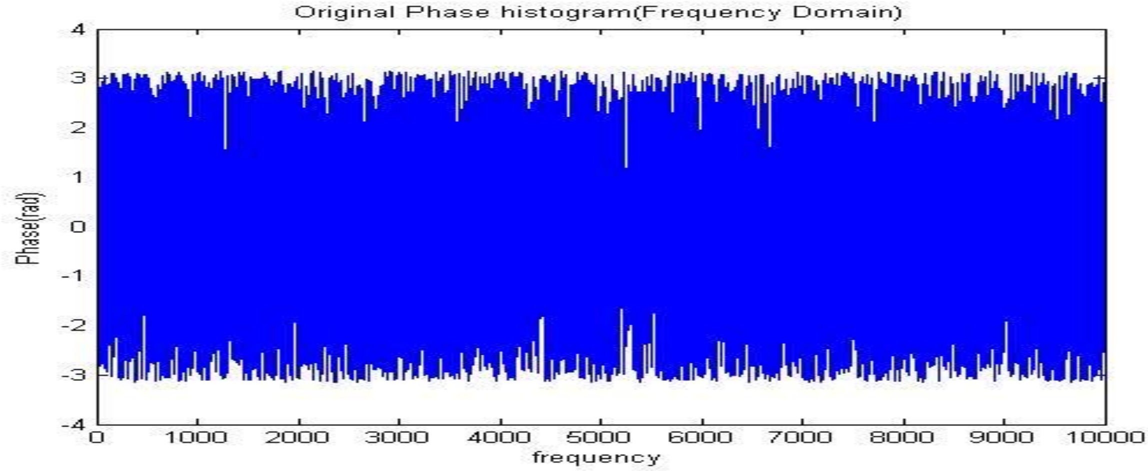

Fig-6: Original Power Spectrum (Higher Phase values)

2) The encrypted power spectrum is

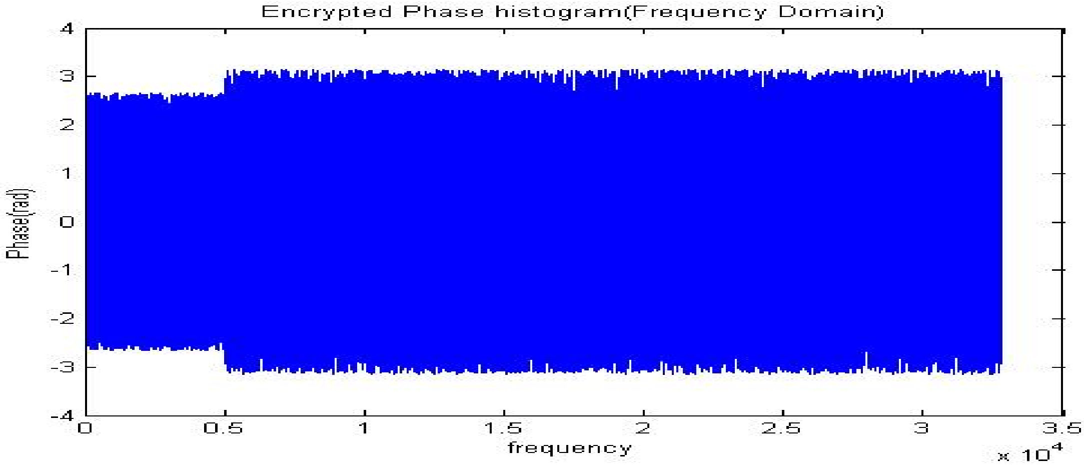

Fig-7: Encrypted Power Spectrum (Higher Phase values)

3) The decrypted power spectrum is

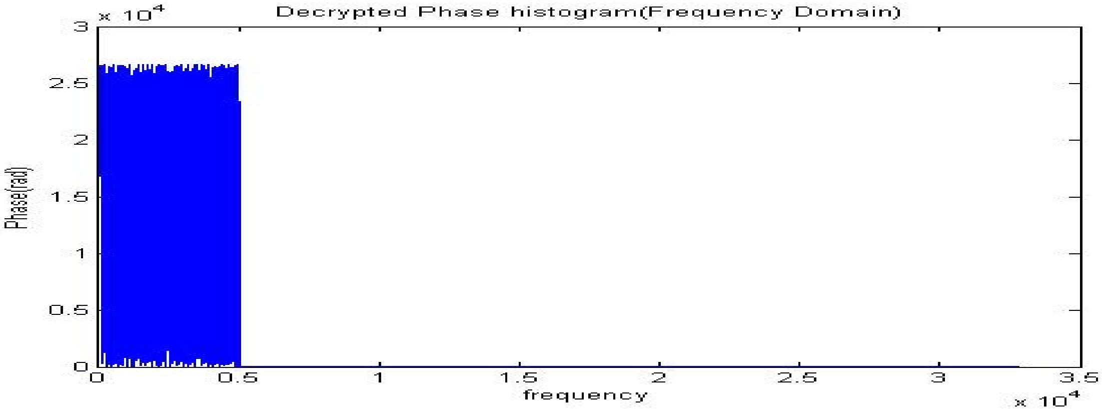

Fig-8: Decrypted Power Spectrum (Higher Phase values)

9. CONCLUSION AND FUTURE WORK

In this paper, we proposed a partial encryption approach. The proposed approach identifies and then encrypts important portions of the DFT coefficient (phase values). The proposed partial encryption scheme differentiates important audio information from less significant audio information. The important portion is encrypted so that the audio security is protected against interceptors or eavesdroppers in the network. To improve the performance of this technique, we can use another more secure encryption algorithms like modified RSA and DES etc. in future.

Acknowledgments

I am thankful to my head of the department Mrs. Bhawna Mallick and co-ordinator Mr. Ajit Bharti whose continues guidance help me to complete this work. I am also thankful to my family and friends to allow and to work with me for the completion of this project.

References

[1] In May 2009 “Audio encryption using higher dimensional chaotic map” R. Gnanajeyaraman , K.Prasadh 2, Dr.Ramar3, Research scholar, Vinayaka Missions University, Salem, Tamilnadu, India.

[2] History of Secure Voice Coding: Insights Drawn from the Career of One of the Earliest practitioners of the Art of Speech Coding, JOSEPH P.CAMPBELL, JR., and RICHARD A. DEAN.

[3] In 2003 “Frequency –selective partial encryption of compressed audio”_Servetti, A.; Testa, C.; De Martin, J.C.

[4] *www.mathworks.in/products/matlab/*.

[5] Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings.

[6] A. Nadeem , "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[7] Rivest, R.; Shamir, A.; and Adleman, L. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." Communications of the ACM, February 1978.

[8] “Index-Based Selective Audio Encryption for Wireless Multimedia Sensor Networks”,H. Wang, Member, IEEE, M.Hempel, Member, IEEE, D.Peng, Member, IEEE, W. Wang, Member, IEEE, H. Sharif, Senior Member, IEEE, and H.-Hwa Chen, Fellow, IEEE,2010 IEEE.

[9] Meyer, J. and Gadegast, F., “Security Mechanisms for Multimedia Data with the Example MPEG-1 Video,”*Project Description of SECMPEG*, Technical University of Berlin, Germany, May 1995.

[10] Spanos, G. A. and Maples, T. B., “Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video,” *Proceedings of 4th International Conference on Computer Communications and Networks*, Las Vegas, NV, September 20-23, 1995.

[11] Tang, L., “Methods for Encrypting and Decrypting MPEG Video Data Efficiently,” *Proceedings of the 4th ACM International Multimedia Conference*, Boston, MA, November 18-22, 1996, pp. 219-230.

[12] “Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions”, X. Liu, Ahmet M. Eskicioglu,2003.