www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Sep 2015, Page No. 14098-14104

An Audio Multiple Shuffle Encryption Algorithm

Mansi[1],Mrs Raman Chawla[2]

[1]M.Tech, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India

[2]Assistant Professor, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India

Abstract: The growth rate of the internet exceeds day by day. With the fast growth of internet, there is need to protect the sensitive data from unauthorized access. Cryptography plays a major role in the field of network security. There are many encryption techniques available currently to secure the data. Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. The strength of this cryptographic technique comes from the fact that no one can read (or steal) the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. Audio cryptography can be employed in audio distribution for the purpose of guaranteeing the confidentiality. Electronic commerce in audio products would be facilitated by the development of solutions which can ensure security/privacy, efficiency in compressed domain to reduce the bandwidth requirements, flexibility of implementing progressive audio quality control and computationally inexpensive to be used in real-time systems. Audio cryptography aims to minimize the residual intelligibility of the original audio and control the access to only authorized users. It is similar to but not a direct application of normal cryptographic techniques. The main advantage is that scrambled audio are still validly formatted which can be played by the corresponding players. In this research work, a novel method for audio encryption is proposed using random permutation with multiple key applications. The proposed method would not only provide highly secure audio but also efficient for audio file having higher frequency band. MATLAB R2013a has been used as an implementation platform using signal processing tool box.

Keywords: Audio Cryptography; Cryptography; Audio Steganography; Encryption; Decryption.

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 [5]. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message [2].

A. Fundamentals of Encryption

Encryption is a technique which maintains confidentiality while sending and receiving data or storing the information. The principle of Kerckoffs' on the encryption states that the security must not rely on the obfuscation of code, but only on the secrecy of the decryption key. In general, encryption techniques are classified into two broad categories: symmetric and asymmetric [3].

II AUDIO ENCRYPTION

Encryption is a technique used to transmit secure information. Over the years several encryption techniques have been implemented. But most of the techniques encrypt only text data, a very few technique are proposed for multimedia data such as audio data. The techniques which encrypt text data can also applied to audio data but have not achieved satisfactory results. Various encryption techniques are implemented for audio data. Some of which are inefficient to meet real time requirements and some are naive to meet the security requirements. Encryption of an audio data is difficult and complex process than the techniques used for text data. Audio encryption ensures secure audio transmission. With the fast growth of communication technology, protection of audio from the hackers became a critical task for the technologist. So there is always a need of a more secure and faster audio encryption technique [6].

A. Audio Cryptography

Audio cryptography encryption is the method of including the noise (key) to the plain text audio and while decryption is the process of taking out the original plain text back by using the same key.

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data cryptography; it is

widely used today due to the great security advantages of it. Here are the various goals of cryptography [8].

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity [8].

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control: Only the authorized parties are able to access the given information.

III CRYPTOGRAPHIC ALGORITHMS

There are lots of encryption algorithms (encryption standards) in the field of cryptography. These are symmetric and asymmetric encryption algorithm. Some basic symmetric encryption algorithms are studied and detailed below:-

A. **DES-**The DES (Data Encryption Standard) was created by IBM in 1975.It was the first encryption standard and remained a worldwide standard for a long time and was replaced by the new Advanced Encryption Standard (AES) [2].It provides a basis for comparison for new algorithms .DES is a block cipher based symmetric algorithm, same keys are used for both encryption and decryption. It makes use of 56 bits key.DES encrypts the data in 64 bits data blocks. Triple DES (TDES) is a block cipher formed from the DES cipher by using it three times [6].DES is not strong enough. Many attacks recorded against it.

B. **Triple DES-**It is a block cipher formed from the DES cipher by using it three times[6].This standard was created by IBM in 1978.When it was found that a 56-bit key of DES is not strong enough against brute force attacks and many other attacks, TDES was made as a same algorithm with long key size. In 3DES, DES is performed three times to increase security. It is also a block cipher technology having key size of 168 bits and block size of 64 bits. DES is performed three times, so it is slower algorithm. Triple DES has low performance in terms of power consumption and throughput when compared with DES. It always requires more time than DES because DES is repeated three times [6].

C. **Blowfish**-It is Block cipher based encryption algorithm provided by Bruce Schneider in 1993. It has variable length key ranging from 32 bits to 448 bits and block size of 64 bits. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays to taling 4168 bytes. All operations are EX-ORs and additions on 32-bit words. Blowfish is successor to Twofish. It suffers from week key problems. So some attacks are possible against it [6].

D. **RC4-**It is a stream cipher designed in 1987 by Ron Rivest for RSA Security. It is having key size of 40 or 2048 bits. It works with byte-oriented operations. The algorithm is based on the use of a random permutation. It is used in the two security schemes defined for IEEE 802.11 wireless LANs: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). RC4 was kept as a trade secret by RSA Security. In September 1994, the RC4 algorithm was anonymously posted on the Internet on the Cypherpunks anonymous remailer‟s list [7].The RC4 algorithm is remarkably simply and quite easy to explain [1].RC4 is suitable for text data [6].

E. **RC2-** It is a symmetric block cipher based technology developed by RSA Data security. It works on block size of 64 bit and make use of variable size keys ranging from 8-128 bits[5].RC2 has disadvantage over other algorithms in terms of time consumption. RC2 is vulnerable to differential attacks [6].

F. **RC6-** It is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes [4]. RC6 uses a block size of 128 bits and having key sizes of 128, 192 and 256 bits. It is similar to RC5 in structure. It is symmetric cipher algorithm.RC6 is vulnerable to bruite force attacks [6].

G. **AES-**It is most widely adopted encryption standard.AES was originally called rijndael. This standard was created by Joan Daemen and Vincent Rijmen in 1998.The Advanced Encryption Standard (AES) algorithm is a symmetric block. AES algorithm can encrypt and decrypt the plaintext and cipher text of 128-bits. It uses variable length key of size 128,192,256 bits [6]. Number of rounds in the encryption or decryption processes depends on the key size. Overall operation is thus similar to the Data

Encryption Standard (DES). The algorithm was created by Carlisle Adams and Stafford Tavares. .It requires very low RAM space and is very fast. It can be used for encryption of Text, Audio, and Image dta.AES provides excellent Data Security.

IV. PROPOSED METHODOLOGY

MATLAB R2013a has been used as an implementation platform using signal processing tool box. Six audio files 'audio 0.wav', 'audio 1.wav', 'audio 2.wav', 'audio 3.wav', 'audio 4.wav' and 'audio 5.wav'. The size of files are 32KB, 151KB,404KB,497KB, 647KB and 1360KB respectively. A new encryption algorithm for audio files is propose and presented in this research work. This new algorithm performs encryption using a advance random procedure. Audio is first encrypted using advanced random permutation method and then decrypted using reverse process. The steps for implementation of proposed method are as follows:

A. Encryption Part

1. Inputting and reading of secret audio data.
2. Checking of length and sampling frequency of audio data
3. If sampling frequency > 44100 than cut down the length and sampling frequency of secret audio.
4. Conversion of row vector audio to column vector audio.
5. Calculation of size of column vector.
6. Generation of 1st random row vector of a fixed length and seed value.
7. Generation of 2nd random row vector according to number of elements of audio column vector.
8. Generation of 3rd random row vector according to number of elements of audio column vector.
9. Random permutation of audio or rearrangement of elements of audio matrix according to 3rd random row vector.
10. Updation and modification of 1st random row vector.
11. Generation of empty row cell according to the seed value.
12. Allotment and division of random permuted audio into empty cells with fast Fourier transform of each elements.
13. Allotment of rest of the audio part into last cell.
14. Conversion of cell into matrix.
15. Again application of random permutation on updated audio matrix according to 2nd random row vector.
16. Normalization of updated and permuted audio matrix elements (real and imaginary separately).
17. Saving of all 3 random vector and maximum value of real and imaginary parts as key for decryption.
18. Joining of both part (real and imaginary) of normalized audio.
19. Saving of the new encrypted audio.

B. Decryption Part

20. Reading of encrypted audio file.
21. Conversion of row vector audio to column vector audio.
22. Calculation of size of column vector audio.
23. Loading of key matrix.
24. Estimation of all 3 random vectors and maximum values of real and imaginary parts
25. Estimation of seed value.
26. Combining of real and imaginary parts of encrypted audio with their maximum values.
27. Rearranging of encrypted audio according to 2nd random vector.
28. Generation of empty row cell according to the seed value.
29. Allotment and division of encrypted audio into empty cells with inverse fast Fourier transform of each elements.
30. Conversion of cell into matrix.
31. Rearranging of encrypted audio according to 3rd random vector.
32. Saving of new decrypted audio.

V. EXPERIMENTAL RESULTS

In this research work, a novel method for audio encryption is proposed using advanced random permutation with multiple key applications. The proposed method would not only provide highly secure audio but also efficient for audio file having higher frequency band. MATLAB R2013a has been used as an implementation platform using signal processing tool box. Six audio files 'audio 0.wav', 'audio 1.wav', 'audio 2.wav', 'audio 3.wav', 'audio 4.wav' and 'audio 5.wav'. The size of files are 32KB, 151KB,404KB,497KB, 647KB and 1360KB respectively. Audio is first encrypted using advanced random permutation method and then decrypted using reverse process. Figure 1 is the snapshot of original input audio waveform and encrypted audio waveform for 'audio 0.wav'. It is clearly seen from figure 1 that original signal is converted into a high frequency noise signal. It would be impossible for intruder to reconvert encrypted signal into original signal. Figure 2 is the snapshot of waveform of encrypted audio and decrypted audio. Figure 3 is the snapshot of waveform of original audio and decrypted audio. Both waveforms are

DOI: 10.18535/ijecs/v4i9.06

looking almost similar. To prove these analytical results we have given some output parameters i.e. MSE, PSNR, normalized correlation value, entropy of original signal, entropy of encrypted signal and entropy of decrypted signal. The values of these signal is given in table 1. Figure 4 is the snapshot of graph for MSE vs. size. Figure 5 is the snapshot of graph for PSNR vs. size. Figure 6 is the snapshot of graph for NC vs. size. Figure 7 is the snapshot of graph for entropy vs. size for original and encrypted signal.

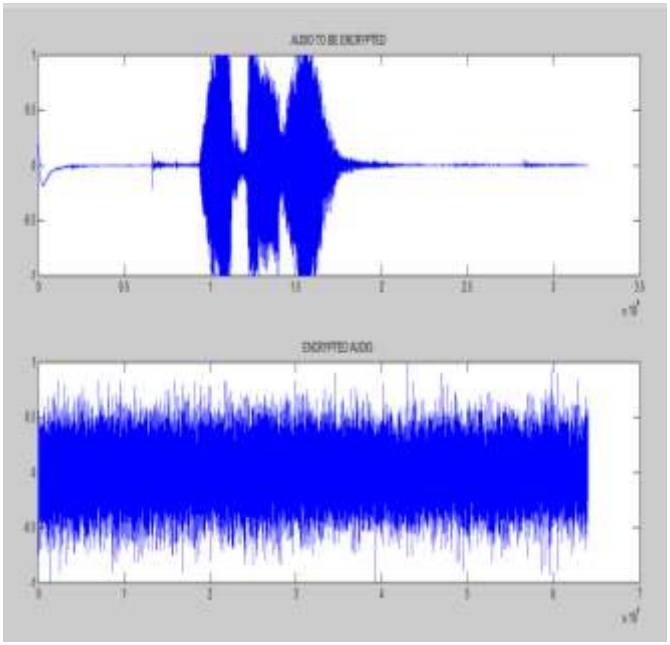


Figure 1 Snapshot of original input audio waveform and encrypted audio waveform for 'audio 0.wav'

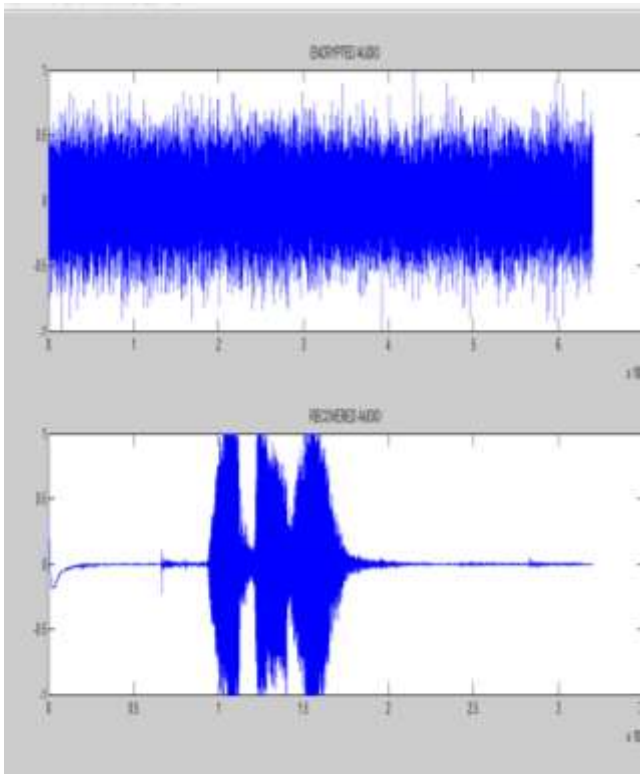
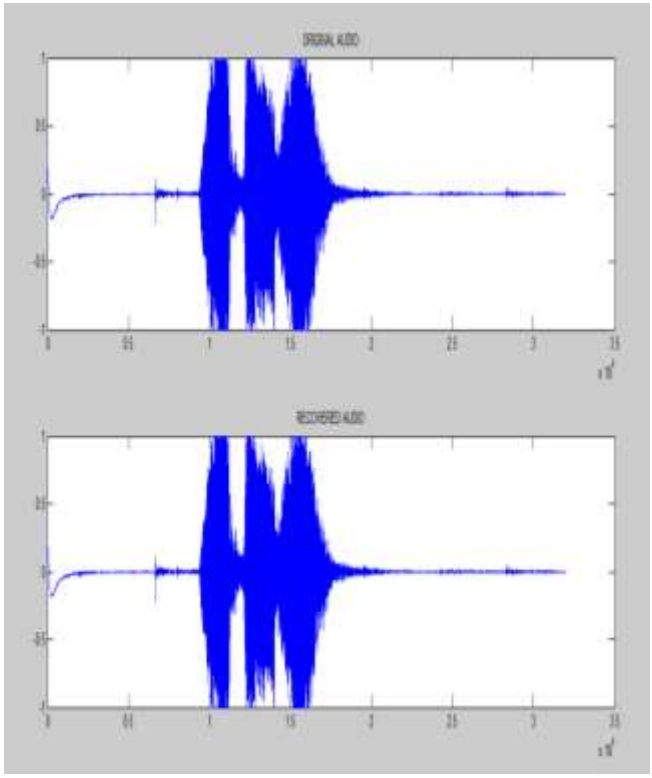


Figure 2 Snapshot of waveform of encrypted audio and decrypted audio



DOI: 10.18535/ijecs/v4i9.06

Figure 3 Snapshot of waveform of original audio and decrypted audio

Table 1 comparison of different parameters for different files

File name	MSE (decrypted audio)	PSNR (decrypted audio)	NC (decrypted audio)	Entropy of original audio file	Entropy of encrypted audio file	Entropy of decrypted audio file
Audio 0	5.2445e-11	102.7351	1.0000	2.0392	4.3394	2.0392
Audio 1	5.3218e-13	113.4271	1.0000	2.6555	4.3174	2.6555
Audio 2	2.7508e-11	105.5349	1.0000	3.6904	4.2555	3.6904
Audio 3	4.6920e-10	93.2186	1.0000	3.9514	4.1553	3.9530
Audio 4	2.9723e-10	92.6796	1.0000	3.0281	3.9390	3.0281
Audio 5	1.0054e-10	98.3980	1.0000	4.2722	4.2882	4.2722

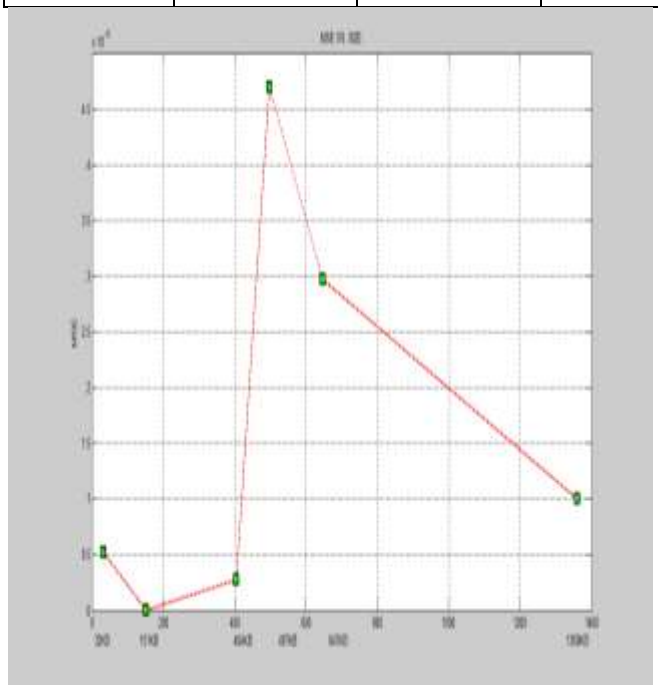


Figure 4 Snapshot of graph for MSE vs. size

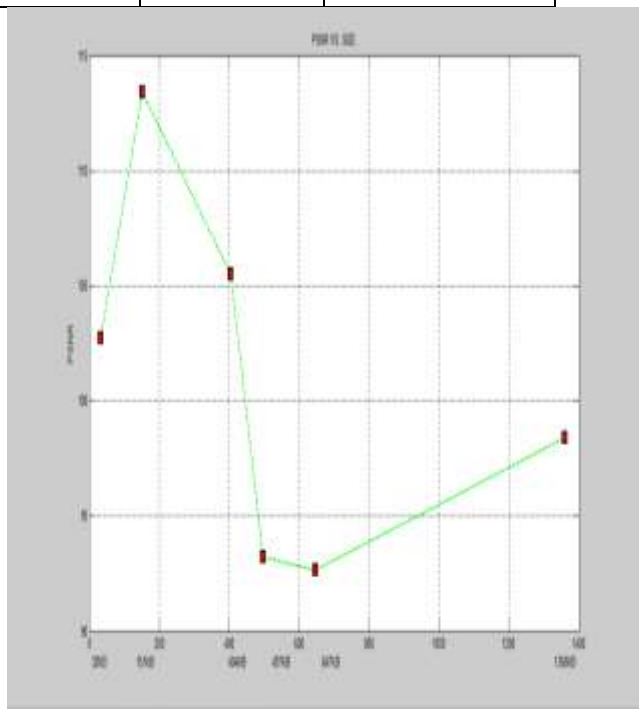


Figure 5 Snapshot of graph for PSNR vs. size

DOI: 10.18535/ijecs/v4i9.06

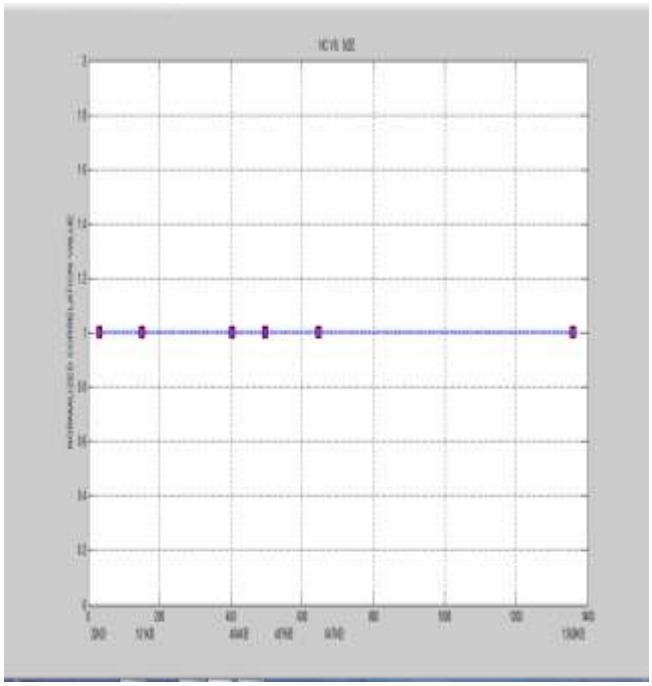


Figure 6 Snapshot of graph for NC vs. size

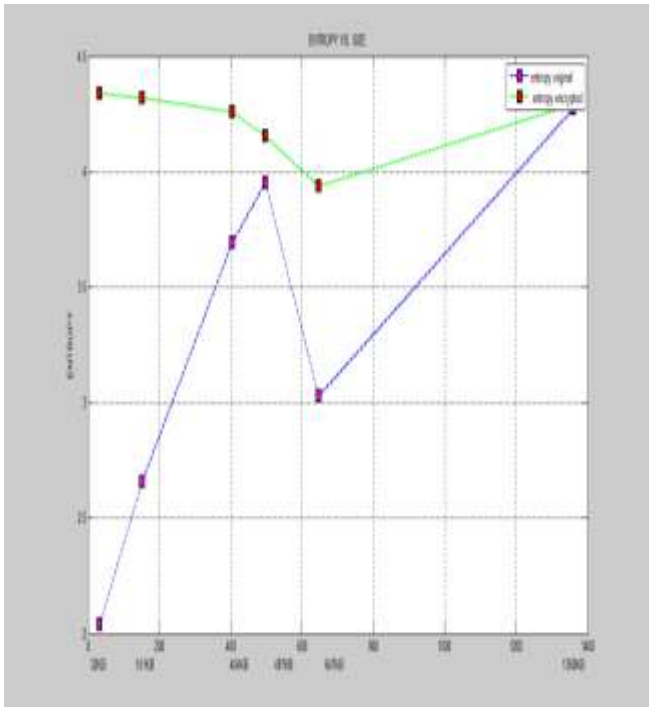


Figure 7 Snapshot of graph for entropy vs. size for original and encrypted signal

VI. CONCLUSION AND FUTURE SCOPE

With the fast growth of internet, there is need to protect the sensitive data from unauthorized access. Cryptography plays a major role in the field of network security. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. The strength of this cryptographic technique comes from the fact that no one can read (or steal) the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. In this research work, we have discussed various cryptographic algorithms (encryption standards), encryption techniques for audio data and some of encryption standards that have been used for encryption on audio data which are used for Network security purpose. With the help of these algorithms, one can generate its own algorithm by making modifications into existing algorithms to make audio data more secure. A new encryption algorithm for audio files is propose and presented in this research work. This new algorithm performs encryption using an advance random procedure. Statistical analysis using MSE, PSNR, correlation, and entropy showed that the algorithm is not vulnerable to statistical attacks. In addition, the huge number of possible keys makes a brute-force attack on the algorithm impossible. Our experiments show that the effectiveness of the proposal. It is a fast and simple solution, yet it can provide sufficient security for audio files. In future, the proposed method for audio cryptography can be combined with audio steganography. The combined method will not only provide security to the audio but also to the image hided in audio.

REFERENCES

[1] Abdelfatah A. Tamimi and Ayman M. Abdalla "An Audio Shuffle-Encryption Algorithm" Proceedings of the World Congress on Engineering and Computer Science 2014 Vol I WCECS 2014, 22-24 October, 2014, San Francisco, USA.

[2] Jayaram P, Ranganatha H R, Anupama H S "Information Hiding Using Audio Steganography – A Survey" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011. PP. 86-96.

[3]S.Rajanarayanan and A. Pushparaghavan "Recent Developments in Signal Encryption –A Critical Survey" International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012. Pp. 1-7.

[4] Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar, Neeraj Vishwakarma " Audio Steganography And Security Using Cryptography" International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 2, February 2014. PP. 317-318.

[5] Sheetal Sharma , Lucknesh Kumar and Himanshu Sharma "Encryption of an Audio File on Lower Frequency Band for Secure Communication" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013 . Pp. 79-84.

[6] Manpreet Kaur (12012134) and Ms. Sukhpreet Kaur "Survey of Various Encryption Techniques for Audio Data" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 5, May 2014. Pp. 1314-1317.

[7] Ms. Vishakha B. Pawar, Prof. Pritish A. Tijare, Prof. Swapnil N. Sawalkar "A Review Paper on Audio Encryption" International Journal of Research in Advent Technology, Vol.2, No.12, December2014. Pp. 45-48.

[8] Raghunandhan K R, Radhakrishna Dodmane, Sudeepa K B,Ganesh Aithal" Efficient Audio Encryption Algorithm For Online Applications Using Transposition And Multiplicative Non-Binary System." International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 6, June – 2013.pp. 472-477.