IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

An Enhanced Approach of Encrypting Audio Segments Using OFDM

Miss. Ashwini A. Varhekar[1], Prof. A. B. Gadicha[2]

M.E. II[nd] year student, CSE, PRPCET, Amravati, Maharashtra, India [1].

HOD, Dept of IT, PRPCET, Amravati, Maharashtra, India [2].

Abstract: The encrypted techniques present knowledge of encryption. A study of a new secure audio encryption and decryption technique is proposed here. A multidimensional key is generated then the selected audio samples are converted to binary format then in this technique, audio is sampled using orthogonal frequency division multiplexing (OFDM). Then the sample bits are swapped and the regenerated samples are filled into the orthogonal matrix. Thus a resultant encrypted audio wave is created. At the receiver and the same procedure is used to perform the decryption. The new technique is employing more security to the audio data file. Therefore, a more encrypted audio wave is obtained using this proposed technique.

Keywords: OFDM, encryption, orthogonal matrix, multidimensional key etc.

I. INTRODUCTION

Cryptography is art or science of sterilizing information, so that the important information is tough to extract throughout transfer over any unsecured channel. Latest growing technology and new opinion like quantum cryptography have superimposed an entire new dimension to information security. The idea of this cryptographic technique comes from the very fact that nobody will steal the data without sterilizing its content. This modification alerts the communicators to relate the chance of a hacker and so promising an extremely secure information transfer. [1]

As a result of this advantage, quantum cryptography has grasped a good deal of attention and large quantity of analysis is being disbursed thereon for safeguarding of business data. Throughout the course of your time, numerous cryptography algorithms are developed to realize the final aim of safe atmosphere for information transmission. The basic objective to manage the planning of associate cryptography rule should be security against all capable unauthorized attacks. However, for all sensible applications, performance and therefore the price of implementation are necessary issues.

The simple cryptographic rule is that the one that attacking on decent balance between security and performance. [1]

A. **Objectives**

To perform the Encryption on audio confidential message with help of OFDM i.e. orthogonal frequency division multiplexing.

B. **Scope**

The major advantage of this approach to full encryption of all the data to its lower complexity because efficient samples need to be encrypted.

II. LITERATURE REVIEW

There are many coding algorithms within the field of cryptography. These are symmetric and asymmetric encryption algorithm. Some basic symmetric encryption algorithms are studied and given below:-

The Data coding Standard (DES) was produced by IBM in 1975. It was the basic coding remained a worldwide for a continue time and was replaced by the new advanced coding (AES). [5] It provides a basis for comparison for new algorithms. DES could be a block cipher primarily based symmetric rule, same keys are used for each coding and confidential writing. [2]

Sheetal Sharma (2013) says DES isn't robust enough. Many attacks recorded against it. Triple DES is a block cipher formed from the DES cipher by using it three times. This commonplace was created by IBM in 1978.When it had been found that a 56-bit key of DES is not robust enough against brute force attacks and lots of another attacks; Triple DES was created as a same algorithmic rule with long key size. In triple DES, DES is performed thrice to extend the security. It's conjointly a block cipher technology having key size of 168 bits and block size of 64 bits. DES is slower algorithmic rule because it performed thrice. [9]

Blowfish is successor to two fish. It suffers from week key issues. So some attacks are probable against it. RC4 is a stream cipher designed in 1987 by Ron Rivets for RSA Security. It is having key size of 40 or 2048 bits. This works with the help of byte-oriented operations. The algorithm relies on the utilization of a alternate permutation.

This used in to the two security schemes defined for IEEE 802.11 wireless LANs:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). G. Ramesh (2012) says that RC4 was kept as a trade secret by RSA Security algorithm. In September 1994, the RC4 algorithm was anonymously transforming on the Internet on the Cypherpunks anonymous remailer's list. The RC4 algorithm is quite easy to explain. RC4 is proper for text data. RC2 is a symmetric block cipher based technology developed by RSA Data security. It works on block size of 64 bit and makes use of variable size keys ranging from 8-128 bits. RC2 has major drawback over further algorithms in terms of time consumption. [8]

Existing System

The selective AES encryption technique is better than the other two encryption techniques. Ms. Vishakha pawar and prof. pritish Tijare in has proposed a new encryption technique, which provides good security to the audio data. The encryption technique for the audio wave message is applied at the time of compression. The AES encryption technique to raise the cryptographic security of the audio wave content [1].

The all segmented audio samples are joined and binary sampling is done. Then multidimensional key is generated so as to send at the receiver side to decrypt the audio file. Thus resultant audio file contains the encrypted audio. On the receiver side, the encrypted confidential audio file is received to get the original audio. The encrypted carrier audio is decrypted using the same encryption process. The binary bits are sampled using OFDM. [7]

III. PROPOSED WORK

Figure 1 represents the complete working of the audio encryption process of the carrier audio using OFDM. In the sender side, the audio wave which has to be encrypted is selected. Then the audio file is converted into binary format depending on the samples in the file. Then the binary bits are sampled into 8bits. The sampled bits are filled into the OFDM matrix. The all segmented audio samples are joined and binary sampling is done. Then a multidimensional key is generated so as to send at the receiver side to decrypt the audio file. Thus resultant audio file contains the encrypted audio. On the receiver side, the encrypted embedded audio file is received to extract the original audio. The encrypted carrier audio is decrypted using the same encryption process. The carrier audio is first converted to binary format. Then the key used for encrypting the audio file is to be selected so as to obtain the original audio file. The binary bits are sampled using OFDM. After binary resampling, the effective bits are read and thus the encrypted audio is decrypted and the original audio is obtained.

A. Encryption Technique:

1. Select audio file.
2. Convert audio to binary format.
3. Sample audio with OFDM (Binary bits).
4. Create OFDM null matrix.
5. Join all segmented audio samples.
6. Binary Sampling
7. Generate key.
8. Create encrypted audio wave from orthogonal matrix.
9. Save audio

DFD (encryption):

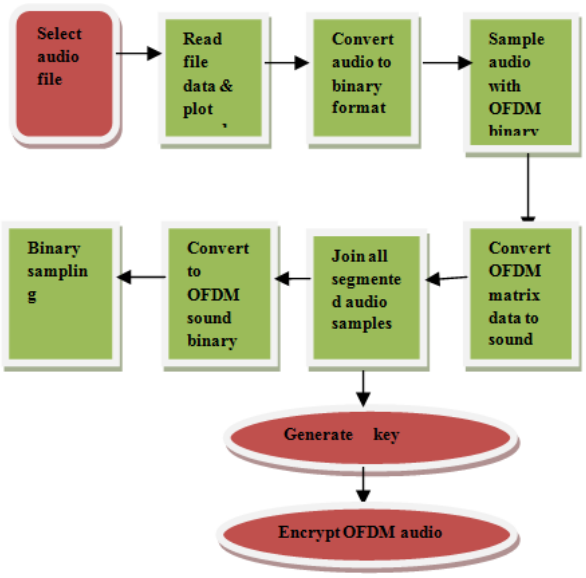


Fig 1 DFD for Encryption

B. Decryption Technique:

1. Select encrypted audio file.
2. Convert the samples to binary format.
3. Generate a multidimensional key.
4. Select sample from orthogonal matrix.
5. Convert selected samples to binary.
6. Then swap sample bits and separate samples.
7. Fill resultant orthogonal matrix with resample value.
8. Create decrypted audio wave from orthogonal matrix.
9. Original audio.

DFD (decryption):

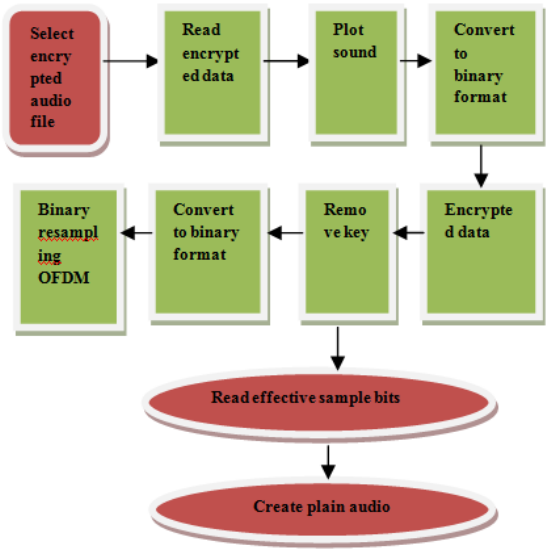


Fig 2 DFD for Decryption

DOI 10.17148/IJARCCE.2016.54210

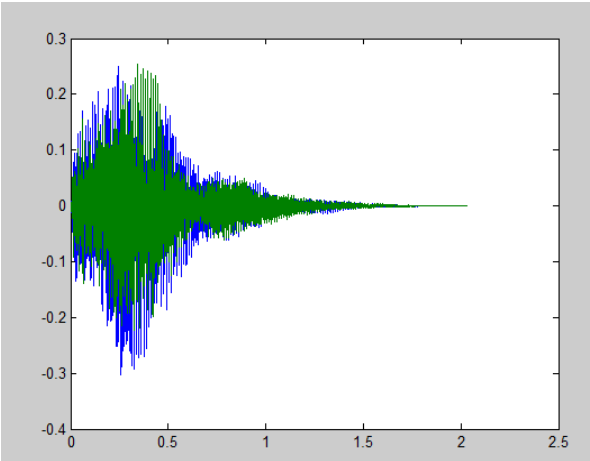
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

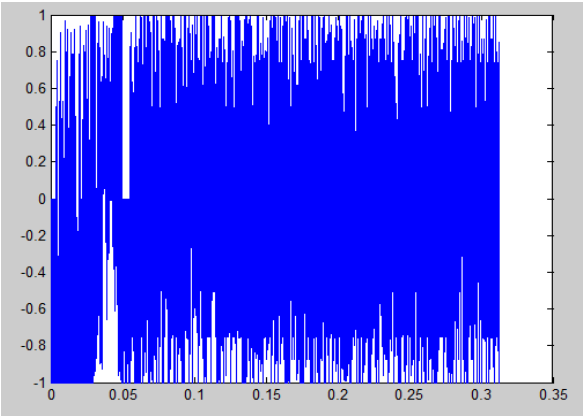
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Experimental Results:

Parameters	Selective encryption	Full encryption
Input audio name	New 196.wav	New 196.wav
Size of input audio(kb)	175 (kb)	175 (kb)
Start sample bit	4	4
End sample bit	5000	5000
Total samples	179660	79200
Total bits	1437280	79200
Size of encrypted audio (kb)	9.72(kb)	9.72(kb)
Size of decrypted audio(kb	5 (kb)	5(kb)



X axis: Pixel count
Y axis: pixel intensity
Fig 4 Plot sound without OFDM



X axis: pixel count
Y axis: pixel intensity
Fig 5 plot sound with OFDM

From the above two figure 4 and figure5 we compare graphical analysis of wave sound. Figure 4 is a plot of simple wave audio file that is without using of OFDM. And from figure 5 we clearly see the difference between these two figures. Figure 5 is the plot of sound with the help of OFDM. From these we say that there is very much difference in their frequencies of audio.

IV. CONCLUSION

1) This system is to provide a good, efficient method for hiding the information from hackers and sent to the destination in a safe manner
2) This proposed system will not change the size of the file even after encryption and suitable for wave type of audio file format
3) The audio encryption techniques can be used for a number of purposes other than convert communication or deniable data storage and it convert audio in to encrypted format with the help of OFDM.

REFERENCES

[1] Ms. Vishakha B. Pawar, prof.Pritish A. Tijare, Prof. Swapnil N. Sawalkar "OFDM based audio carrier sampling for an audio Encryption by efficient sample bit swapping with Random key generation" vol 2, pp 2529-2533, In 11 July 2015
[2] Naveen Jacob, U. Sripati "Bit Error Rate Analysis of Coded OFDM for Digital Audio Broadcasting System, Employing Parallel Concatenated Convolutional Turbo Codes" IEEE,PP 1-5,2015.
[3] R. Gnanajeyaraman, K.Prasadh 2, Dr.Ramar3, Research scholar, Vinayaka Missions University, Salem, Tamilnadu, India, "Audio encryption using higher Dimensional chaotic map" In May 2009.
[4] R.W Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmission" In Bell System Technical Journal, PP.1796-1966.
[5] Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad "Superior Security Data Encryption Algorithm (NTRU)" International Journal for Technological Research in Engineering Volume 2, PP.2347 - 4718, Issue 11, July-2015
[6] M. Anand Kumar, Dr.S.Karthikeyan "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" I. J. Computer Network and Information Security, vol.2, issue22, 2012.
[7] G. Ramesh, Dr. R Umarani "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, No.2.March-April2012.
[8] G Ramesh, Dr R Umarani "A New Symmetrical Encryption Algorithm with High Security and Data Rate for WLAN and width Line" International Journal of Information Technology, Vol.2, Isssue4, April2012.
[9] Sheetal Sharma, Lucknesh Kumar, 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, Vol.3, Issue7.Julyl2013
[10] Milind mathur, ayush kesarwan "COMPARISON BETWEEN DES, 3DES, RC2 , RC6 , BLOWFISH AND AES Proceedings of National Conference on New Horizons in IT - NCNHIT 2013
[11] Roshan Jain, Sandhya Sharma "Simulation and performance analysis of OFDM with different modulation techniques" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-1, Issue-1, March 2013