Security of Audio File based on Partial Encryption

Sushant Jillawar
Department of Information Technology
Pimpri Chinchwad College of Engineering, Pune, India

Trishala Sawant
Department of Information Technology
Pimpri Chinchwad College of Engineering, Pune, India

Ajinkya Khurud
Department of Information Technology
Pimpri Chinchwad College of Engineering, Pune, India

Jayashree Katti
Department of Information Technology
Pimpri Chinchwad College of Engineering, Pune, India

ABSTRACT
The use of multimedia data such as compressed audio urge for the need of secure transmission without compromising the audio quality. As there is a tremendous growth of digital data, the issue of security raises, which demands for developing of more advance cryptography techniques. Cryptography is a process that disarranges the information by rearranging and topping the content which makes the original content unreadable except the only person who knows the process of rearranging it. Encryption is a process of converting some data from its original form to encrypted form, practically that cannot understandable by unauthorized user. Decryption is a process of obtaining back the original data from encrypted form. In this paper more secure and fewer complex methods are studied which reduces the time complexity of encrypting and decrypting the audio file and a technique based on partial encryption is proposed where only the header of the audio file is encrypted which results in low time complexity. The techniques used are based on selective encryption, LSFR, Fast Fourier Transform, chaotic system.

General Terms
Security, Cryptography.

Keywords
Audio encryption, High dimensional chaos, -Linear feedback shift register, Division modulo circuit, Key stream generator

1. INTRODUCTION
In today's digital world everything such as data, files, payments are digitized. Therefore, there is high concern for security. The growing demand of transferring data over internet and storing it on cloud raises this concern. This digital world seeks new applications which must be efficient, faster and secure. The advancement in technologies and internet raises the concern of information and network security. Here the cryptography technique plays an important role in providing the network security. Cryptography is a process of converting plain text into unintelligible text form and vice versa. In laymen's language, an original message in the form of plain text is converted into unreadable message (cipher text) by applying some substitution techniques. The message that need to be protected (original message) is called as plain text. The technique used to make it unreadable is called encryption, the result of encryption led to formation of cipher text. The technique used to get the plain text back from the cipher text sis called as decryption. The main idea of this paper is to divide the audio file in two parts, one part consists of header and another part consists of the remaining portion of the file. The header part is encrypted and remaining part is left unprotected. On the other hand, it can be said that it encrypts only 10 to 12% of the whole data. In this paper the phase values of the frequencies of an audio signal is considered. Selective encryption is sometimes known as the partial encryption. Particularly, partial encryption can be implemented not only to achieve the same intuitive effect of full encryption but also to maintain the original quality with controlled disturbance. In this technique, partial encryption of the audio signal on phase values is done 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.

2. RELATED WORK
2.1. Method for encrypting and decrypting wave files by Mohamad M. Al-laham1, Mohamad a. Mai'iteh2, Hasan Rashaideh3, Ziad Al-Qadi4 [1] aims at presenting method for encrypting and decrypting wave files. The proposed method first, fetches the audio file, then a two-dimensional matrix is created to maintain the values that corresponds to the sample range, the values are placed in the 2-d matrix which is created. Now the matrix is multiplied with a private double matrix key to encrypt it. After encryption the data will be sent and it get decrypted using the same 2D matrix which was previously used for encryption. The proposed technique consists of two phases which are encryption and decryption.

The first phase is encryption phase in which the original file is captured. Then the captured wave file size is calculated, if the size of file is not a square number then it is converted into the nearest square number by padding zeros at the end. Then the wave file is converted into a 2D matrix. A new private matrix (secret key matrix) Is created which is used for multiplication with the matrix having the actual values of wave file. This results in an encrypted matrix. The encrypted 2-D matrix is then converted into 1-D matrix to get an encrypted file. The second phase is decryption. In this phase the encrypted wave file is obtained. The size of encrypted file is calculated, resize the file if needed, if the size is not a perfect square number the pad zeros to, make it a square number. Convert the 1-D matrix file to 2-D matrix. The inverse of secret key matrix is taken and multiplied which the matrix which is converted into 2-D from 1-D. this results in decrypted matrix. Again, resize the file and change it form 2-D to 1-D matrix to get the original wave file. The proposed theory is accurate, has high efficiency and it provides high security.

Table 1: Sample Values of the Wave File

Wave File Size (MB)	Encryption\Decryption Time (Millisecond)
0.022051	15
0.589824	168
18.690480	6194
1.214400	294
5.400000	854
10.00000	1281
20.00000	7105
30.00000	11237

Table 2: Encryption Time Comparisons

File Size (MB)	Proposed Technique	DES (1)	Blowfish (2)
10	1281	7566	34010
20	7105	10424	64195
30	11237	15211	82230

2.2. Secure Selective Encryption of Compressed Audio by, Shine P James, Sudhish George, Deepthi.P. **[2]** aims at the concept used is of selective encryption where only specific data is selected and encrypted rather than encrypting the whole file. Here only a part of Huffman coded data is selected and encrypted. Then the selected data is EX-ORed with a pseudorandom key, which is generated by a secure method. The size of file generated will vary, depending upon the amount of data taken for encryption. The factor of security depends not the key steam generator using LFSR algorithm. Applying Brute force algorithm, the file can be decrypted so LFSR algorithm is modified by adding a modular division circuit which helps to increase the throughput. To increase the security, the output is passed through a non-linear filter which introduces nonlinearity.

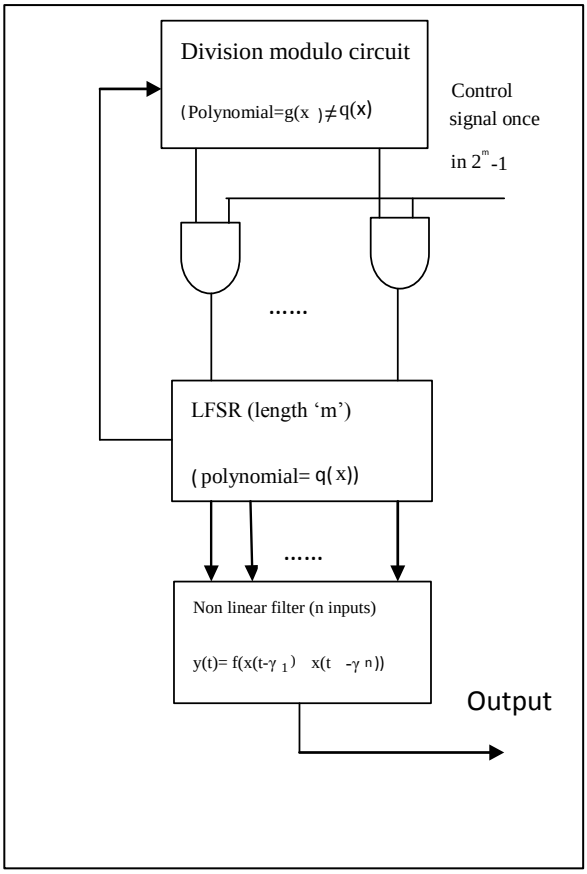

Figure 1: Block diagram of secure key stream cipher

The different keys obtained from the key model are EX-ORed with each frame of Huffman coded main data. The consecutive bits in the secure key stream are used to encrypt the main data of the consecutive frames of the audio, which results in encrypted frames with different keys. The audios are of varying quality because it depends upon the number of bits encrypted in each frame. Depending upon the total number of frames and the number of bits encrypted in each frame the keys can be generated of sufficient length by adding an initial seed for LSFR.

2.3. High dimensional chaos for Audio encryption by Ganesh Babu. S, Ilango. P [3] has proposed, a chaos- based audio encryption system, in the framework of cipher block architecture is proposed. An analog audio input is sampled at a frequency well above the Nyquist frequency of the signal. Then a 16-bit quantization is used to convert the analog signals into its equivalent decimal value. By masking these data with a random key stream generated by a chaos-based pseudorandom key stream generator, the corresponding encrypted audio is formed. Chaos - based look-up tables are used for encrypting audio files.

In chaos there are manly maps it is found that Arnold's Cat map is a good candidate for permutation thus it is extended to a higher dimensional version called Nth D map. The higher dimensional cat map is used as our pre-processing unit for generating Look-up tables. On the encryption block one uniform distributed random number is generated that sequence will select the tables for encryption. After selecting the table, the digital value of the audio signal is mapped to the iteration number of the chaotic sequence for encrypting the nth digit, the n-1th cipher digit value with nth plain value that resultant value will be mapped with the table value.

2.4. Encryption of an Audio File on Lower Frequency Band for Secure Communication. [4] In this paper, to perform encryption and decryption a frequency domain of wav audio signal is used. DFT i.e. Discrete Fourier Transform is used to convert the time domain audio signal to frequency domain audio signal. By applying DFT, an audio signal can be separated on the basis of phase and magnitude values into different frequency bins. For encryption and decryption, the algorithm used is this paper is RSA. Encryption is done only on the lower frequency bands as all frequency region does not participate equally in the communication. The encryption and decryption flow are as follows.

In encryption, the original audio file is obtained and transform function DFT is applied, selection of useful frequency is done, the selected frequency band is encrypted using RSA. The encrypted data then combined with non- encrypted data and Inverse Transformation Function (IDFT) is applied resulting into an encrypted audio file.

In decryption, the encrypted audio file is obtained and DFT is applied on it thus converting it into frequency domain. The encrypted frequency band is selected and only selected band is decrypted using RSA technique. The decrypted frequencies then combine with the non-encrypted frequencies and Inverse Transformation Function (IDFT) is applied resulting into original audio file.

3. PROPOSED METHOD

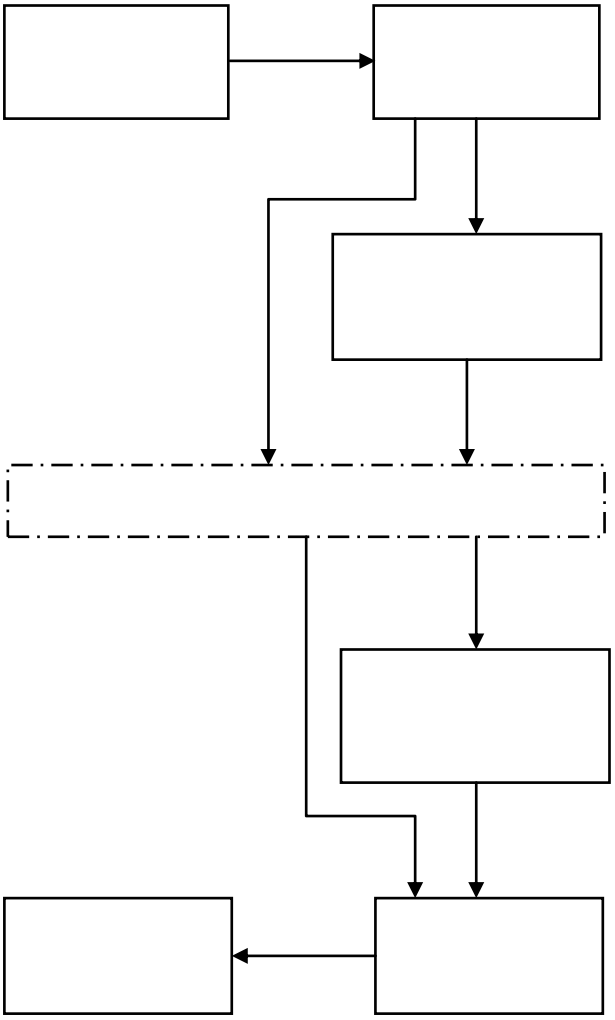

Figure 2: Architectural diagram of proposed method

The proposed approach is by using header selection to encrypt the header of the file which accounts partial encryption technique. Encrypting the header makes the whole file unplayable unless the header is decrypted. The encryption algorithm applied over the header is AES. Once the header is decrypted the header is attached to the file and the audio is playable again for use. The steps involved are as following: -

1. Selection an audio file(.wav/.mp3)
2. Conversion of the audio file into Byte Array format.
3. Reading the entire file to memory buffer & moving the header bytes to a new file.
4. Writing the data from memory buffer to a file with no header and a file with just the header.
5. Encrypting the file with header using AES encryption.
6. Similarly, for decryption the encrypted header file is decrypted.

The decrypted header file is then appended with the original data file.

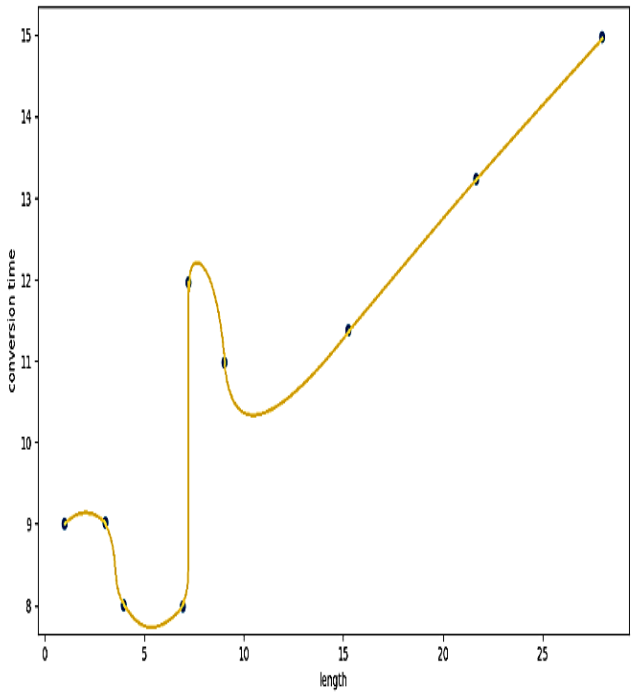

Figure 3: Graph of file length(sec) vs conversion time(sec)

4. CONCLUSION

In this paper, the analysis is based on the partial encryption technique at the time of audio compression. A selected quantized value is taken and AES encryption technique is chosen to apply based upon the comparison of various encryption algorithms. Utilizing this procedure, the computational time for the encryption procedure diminishes with regards to the encoding the full sound information. The bit rate is also reduced during partial encryption. This reduces the risk of slowing down the system to a great extent when the encryption process is applied to a large amount of data. This process is fast and provides more security for music ecommerce applications.

5. REFERENCES

[1] A method for encrypting and decrypting wave files. Mohamad M. Al-laham1, Mohamad a. Mai'iteh2, Hasan Rashaideh3, Ziad Al-Qadi4 1&2Department of MIS, Al-Balqa Applied University, Jordan 3&4Department of computer science, Al-Balqa Applied University, Jordan International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.4, July 2018

[2] Secure Selective Encryption of Compressed Audio by, Shine P James, Sudhish N George, Deepthi P P Department of Electronics and Communication National Institute of Technology, Calicut, Kerala, India -673601

[3] High dimensional chaos for Audio encryption by Ganesh Babu. S, Ilango. P.

[4] Encryption of an Audio File on Lower Frequency Band for Secure Communication. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)

[5] Sayyad, S. N., Sutar, P. S., Pise, R. S., Raut, V. H. and Nalawade, C.V. Dual-layer Video Encryption & Decryption using RSA Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2017, 7661-7668.

[6] Sharma, Er. J. and Rani, J. An Efficient Hybrid Approach for Secure Speech Cryptography, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.1, January, 2017, 23-29.

[7] Dastoor, Sarosh. "Comparative Analysis of Steganographic Algorithms Intacting the Information in the Speech Signal for Enhancing the Message Security in Next Generation Mobile Devices", IEEE Xplore Digital Library, in proceedings of The World Congress on Information and Communication Technologies. Mumbai, India, 11-14 Dec.2011: pp. 279-284.

[8] Dey, Sandipan, Ajith Abraham, and SugataSanyal. "An LSB Data Hiding Technique Using Natural Numbers", in proceedings of IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IIHMSP, Nov. 26-28, 2007, Kaohsiung City, Taiwan, vol.2: pp. 473-476.

[9] Antonio Servetti et al., 2003, "Frequency – selective Partial Encryption of Compressed Audio'', Proceedings of IEEE International conference on Acoustics, Speech, and signal Processing (ICASSP'03), Vol.5, April 610, pp.68-71.

[10] Nosrati,Masoud, RonakKarimi, HamedNosrati and Ali Nosrati, "Taking a Brief Look at Steganography: Methods and Approaches", Journal of American Science, vol.7, no. 6, 2011: pp. 8488.