ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Audio Cryptography System

Shaik Abdul Muneer
Assosiate Professor,
Department of Physics,
Osmania College (Autonomous), Kurnool.

G.Mahaboob Basha
Assosiate Professor,
Department of Physics,
Osmania College (Autonomous), Kurnool.

ABSTRACT:

Security often requires that data be kept safe from unauthorized access. And the best line of defense is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option (due to cost and/or efficiency considerations). Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use. Cryptography secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Stronger cryptographic techniques are needed to ensure the integrity of data stored on a machine that may be infected or under attack. So far Cryptography is used in many forms but using it with Audio files is another Stronger Techniques. The process of Cryptography happens with Audio File for transferring more secure sensitive data. The Sensitive Data is Encoded with an Audio File and Passed over Insecure Channels to other end of Systems. Here we are using .wav file Format for Encryption and Decryption of Message. The given message will be encrypted with a given audio file using a secret key. The System will then embed the secret message into the audio file. The result will be a new audio file, which has the secret message in it. While decrypting the same key should be given for encrypted audio file to get the secret message from it.

INTRODUCTION:

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. Due to this advantage, quantum cryptography has grasped a great deal of attention and huge amount of research is being carried out on it for safeguarding of business data. During the course of time, various encryption algorithms have been developed to achieve the ultimate aim of safe environment for information transmission. However, the principal objective guiding the design of an encryption algorithm must be security against all possible unauthorized attacks. However, for all practical applications, performance and the cost of implementation are also important concerns. The best cryptographic algorithm is the one that strikes a good balance between security and performance.

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.

Overview of Cryptography:

Cryptography is the science of information security. The word is derived from the Greek words kryptos, meaning “hidden” and graphia meaning “writing or study”. Cryptography is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. In other words a given message is coded into a secure message (ciphertext) by applying some substitution techniques, to make the input message unreadable by anyone during its transmission. Only the intended recipient is able to decode it. With the vast growth of data transmission over internet, its security became a great concern. Since no cryptographic scheme is foolproof, the idea is to make the cost of acquiring information more than the information itself.

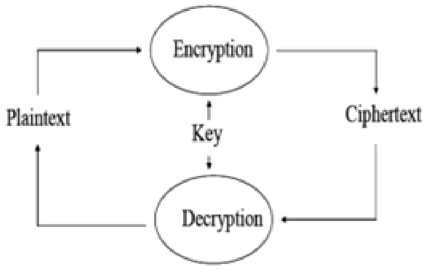

Fig:1 A General Model of Cryptography

Related work on Audio Encryption Keeping the volume of audio files in mind researchers in paper have discussed that all encryption techniques can be classified into three broad categories like: Complete encryption, Selective encryption and combined compression encryption approach. The complete encryption approach is the traditional way to accomplish content confidentiality which encrypt the whole file with the help of traditional ciphers like DES, AES, 3DES, RC$, or RSA. This leads to high processing and computational complexity. The selective encryption approach encrypts the parts of a multimedia file to reduce the computational requirements of the client side in real time applications. The major issue in this approach is to select the important data that need to be encrypted. The Combined compression encryption approach combines the compression process and the encryption process in a single step. In their work, researchers of paper had taken full encryption approach for real time multimedia data like image, audio, and video communication applications. A complete Binary tree performs substitution and a two dimensional array performs the linear diffusion. The experimental results prove the algorithm a success with some start-up delay. Researchers are trying to implement their work in embedded/mobile applications. To concentrate on the work of Audio Encryption, all types of cryptographic algorithms are analyzed. In the present work media type as well as wired and wireless media is of great concern.

While analyzing all the algorithms, factors like throughput, speed, and security are important but the need of computing resources like CPU time, memory and battery power is of utmost concern. These resources are limited in wireless environment. So while considering symmetric or asymmetric encryption algorithm it can be observed that public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [17]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques due to the high amount of computations. Again with Symmetric ciphers, block ciphers and stream ciphers play important role. A block cipher processes one block of data at a time while a stream cipher processes input elements continuously one element at a time. While encrypting an offline file and sending it over networks block cipher will give good result whereas encrypting real time data on a network in a continuous basis stream cipher will be a better solution.

Since the present work is focusing on stored audio files all the algorithms discussed in the previous section are symmetric block ciphers.

Existing System:

If a person sends sensitive information over the insecure channels of the system then there may be a chance of hacking it, they can alter the information and sends it over the net. (Example is military persons sending sensitive information over the net.) This problem has been solved by the proposed system.

Proposed System:

In the proposed system the above problem has been solved by embedding the data into the audio file. Before embedding it into the file, encryption operation will be performed by using the encryption key which is provided by the source. Then this audio file will be passed over the net, even if hacker hacks it, can be able to see only an audio file. At the destination side this data will be encrypted from audio file and performs decryption to get original message.

Module Description

Modules:

GUI Module:

This module generates the user interface through which a user browses the audio file and can play and stop the audio file. This GUI contains different fields such as text area for entering message and buttons for encryption and decryption.

Encryption and Decryption Module:

During encryption, audio file will be created and in this audio file. In this audio file LSB of the each byte will be replaced by the encrypted data which is generated by the combination of the encryption key and the plain text i.e., the original message. Then this audio file will be sent to the recipient. At recipient side this encrypted data will be extracted from each LSB and performs decryption operation on it and gives original information.

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:

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).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 DES is not strong enough. Many attacks recorded against it.

Triple DES:

It is a block cipher formed from the DES cipher by using it three times.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 cypher 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 .

CONCLUSION:

Cryptography with Audio is a desktop application. The purpose of this application is to provide the security for the confidential information. This application doest allow the hackers to view the data, can view only audio file when it is being passed over the internet.

Then at the recipient side the original information i.e., plain text will be extracted from the audio by performing decryption operations. This Project has been developed successfully. I learned java 2 standard edition and swings which are very use full to develop this application.

REFERENCES:

[1] Akash Kumar Mondal, Chandra Prakash, and Mrs Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES",IEEE Students' Conference on Electrical, Electronics and Computer Science, 2011.

[2] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, "Performance Analysis Of Data Encryption Algorithms", IEEE, 2011.

[3] Sruthi B. Asok, P.Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai, "A Secure cryptographic scheme for Audio Signals", International Conference on communication and Signal Processing, April 3-5, 2013, India.

[4] Sheetal Sharma, Lucknesh Kumar Himanshu Sharma, "Encryption of an Audio File on Lower Frequency Band for Secure Communication", International Journal of Computer Science and Software engineering, volume 3, Issue 7, July -2013.

[5] Rashmi A. Gandhi, Dr. Atul M. Gosai, "Steganography – A Sin qua non for Diguised Communication", International Journal of Innovative Research in Advanced Engineering", Vol 1, Issue 8, 2014.

[6] Shine P James, Sudish N George, Deepthi P P , "Secure Selective Encryption of Compressed Audio", International Conference on Microelectronics, communication and Renewable Energy, IEEE-2013.

[7] Ganesh Babu S, Ilango. P, " Higher Dimensional Chaos for Audio Encryption " IEEE, 2013.

[8] N. Radha Aathithan, Venkatesulu. M, "A Complete Binary Tree Structure Block Cipher for real-time multimedia", Science and Information Conference 2013, October 7-9, London, UK.

[9] S. Pavithra, E.Ramadevi, "Throughput Analysis of Symmetric Algorithms", International Journal of Advanced Networking and Applications, Volume-4, Issue-2, Pages:1574-1577, 2012.

[10] Diaa Salama1, Hatem Abdual Kader, and Mohiy Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, Page.213-219, May 2010.

[11] Nidhi Singhal, J.P.S Raina, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, July-August, 2011.

[12] Saurabh Sharma, Pushpendra Kumar Pateriya, "A Study on Different Approaches of Selective Encryption Technique", International Journal of Computer Science and Communication Networks, Vol.2(6),658-662.

[13] Majdi Al-qdah, Lin Yi Hui, "Simple Encryption/Decryption Application", International Journal of Computer Science and Security, Vol.1, Issue.1.

[14] Bismita Gadanayak , Chittaranjan Pradhan , "Encryption on MP3 Compression". MES Journal of Technology and Management.

[15] Sheetal Sharma, Himanshu Sharma and Lucknesh Kumar, " Power Spectrum Encryption and Decryption of an Audio File", International Journal of Research in Computer Science, Volume 1, August-2013.