A Review on Audio Cryptography

Mansi, Mrs Raman Chawla

***Abstract*— Today there is large demand of internet applications that requires data to be transmitted in a secure manner. Data transmission in public communication system is not safe and secure because of interception and improper manipulation by eavesdropper. In cryptography technique, 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. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something. This paper provides a review on audio cryptographic techniques.**

***Index Terms*— Audio Cryptography, Audio Steganography, Cryptography, Encryption etc.**

I. INTRODUCTION

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 [4]. 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.

The Internet and its most popular application, the World Wide Web, are completely public systems. Unless one takes precautions, any information sent over the Internet is potentially audible and visible to all. Sending an e-mail, for example, is like posting a letter without an envelope: anybody can intercept the message and read its contents as it is routed towards its recipient. Similarly, when your web browser logs into a web server, anyone can listen in to the information that is exchanged between your computer and the remote server or any other computer [3]

A. CRYPTOGRAPHY

Cryptography refers to the study of mathematical techniques and related aspects of Information security like data confidentiality, data Integrity, and of data authentication. Cryptography as the study of secret (crypto) writing (graphy) can be defined as the science of using mathematics to encrypt and decrypt data back. It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper known as Eve will not be able to listen in on their communication.

Mansi, M.Tech, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India

Mrs Raman Chawla, Associate Professor, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India

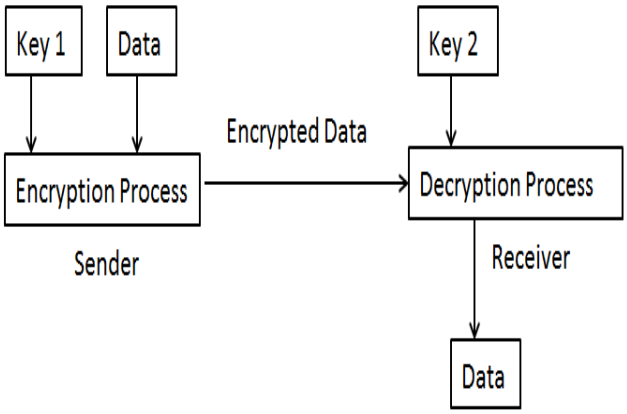

Fig 1.1 Basic cryptographic process [7]

With rapid advancement in technology, steganographic software is becoming effective in hiding information in image, video, audio or text files

.

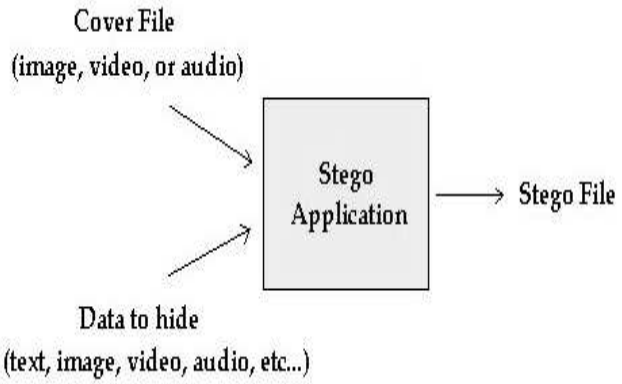

Figure 1.2. Steganography Application Scenario

B. AUDIO STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which means covered or secret and -
graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information [2]. A secret information is encoded in a manner such that the very existence of the information is concealed.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed [2].

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

C. 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. The detailed explanation of these two types is given in the following section [6].

Symmetric Encryption

The term ―Symmetric states that both encryption and decryption of the data are carried out with the same secret key. Hence, the key must be known to both sender and the receiver in order to perform any secure communication. The major advantage of using symmetric encryption is for its fastness. However, it is not possible for two people who never met to use such schemes directly. Block ciphers and stream ciphers which belongs to this category performs encryption faster.

Asymmetric Encryption

In terms of asymmetric encryption, the key used for encryption is different for it is used in decryption procedure. The encryption key is public as the decryption key remains private. Since there is no need of sender or receiver to agree on the sharing of secret key, these schemes are more functional than the symmetric techniques. More number of features are added to asymmetric schemes. However, asymmetric schemes have two major disadvantages; they are based on nontrivial mathematical computations, and much slower than the symmetric ones.

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 [5].

A. AUDIO 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) [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 [5].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[5].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 [5].

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 [5].

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 Cypher punks anonymous remailer‟s list [13].The RC4 algorithm is remarkably simply and quite easy to explain. RC4 is suitable for text data [5].

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[4].RC2 has disadvantage over other algorithms in terms of time consumption. RC2 is vulnerable to differential attacks [5].

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. 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 [5].

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 [5]. 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. The overall summery of all the methods is given below:

Factors	Block size	Cipher Type	Security
DES	64 Bits	Block Cipher	Inadequate
3DES	64 Bits	Block Cipher	Inadequate
RC2	64 Bits	Block Cipher	Vulnerable
RC4	Byte Oriented	Stream Cipher	Weak Security
RC6	128 Bits	Symmetric Algorithm	Vulnerable
Blowfish	64 Bits	Symmetric Block Cipher	Less Secure

III. COMPARISON TABLE

This table compares the above stated encryption standards based upon different factors [5]

Factors	*DES*	*3DES*	*Rc2*	*RC4*	*RC6*	*BLOWFISH*	
Key Size	56 Bits	168 Bits	8-128 Bits	40-128 Bits	128,192 or 256 Bits	32-448 Bits	128,192 or 256 Bits
Block size	64 Bits	64 Bits	64 Bits	Byte Oriented	128 Bits	64 Bits	128,192 or 256 Bits
Cipher Type	Block Cipher	Block Cipher	Block Cipher	Stream Cipher	Symmetric Algorithm	Symmetric Block Cipher	Symmetric Cipher Algorithm
Keys	Private Key	Private Key	Single Key	Single Key	Single Key	Private Key	Private Key
Attacks	Vulnerable to Differential and Linear Attacks	Vulnerable to Differential,Bruite Force Attacks	Vulnerable to Differential,Bruite Force Attacks	Vulnerable to Bruit Force Attacks	Vulnerable to Differential,Bruite Force Attacks	Vulnerable to Differential, Bruite Force Attacks	Strong Against Differential, Bruite,Linear Force Attacks
Security	Proven Inadequate	Inadequate	Vulnerable	Weak Security	Vulnerable	Less Secure	Considered Secure

IV. CONCLUSION & FUTURE SCOPE

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. In this paper basically we have provided a review of various audio steganographic & cryptographic methods.

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] Miss. Divya Sharma" Five Level Cryptography in Speech Processing using Multi Hash and Repositioning of Speech Elements" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 5, May 2012. Pp. 21-27.

[4] 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.

[5] Manpreet Kaur 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.

[6] 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.

[7] Ashima Wadhwa " A Survey on Audio Steganography Techniques for Digital Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014. Pp. 618-622.