Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Various Encryption Techniques for Audio Data

Manpreet Kaur (12012134)
M-Tech CSE Research Scholar
Shri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Ms. Sukhpreet Kaur
Assistant Professor
Shri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, 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. In this review paper we will have an overview of encryption techniques. This paper mainly focuses on encryption techniques for audio data. This presents a study and comparison of basic symmetric encryption standards and a literature survey encryption technique that have been used for encryption on audio data. Finally this suggests a more secure algorithm for audio encryption.

Keywords: DES, 3DES, AES, RC2, RC4, RC6

I. 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 [1].

I (a). 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 [11].

II. 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 [1].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[1].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 [2].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 [7].

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. [1] [2].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. [3] 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 Cypherpunks anonymous remailer's list [13].The RC4 algorithm is remarkably simply and quite easy to explain [1].RC4 is suitable for text data [7].

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 [7].

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 [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. [4] .It can be used for encryption of Text, Audio, and Image dta.AES provides excellent Data Security [1] [2].

II (a). 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

III. RELATED WORK

Sheetal Sharma, Lucknesh Kumar in [11] has proposed an encryption algorithm for audio file using RSA algorithm.RSA is asymmetric encryption technique. In this paper a frequency domain of the wave audio signal is taken for the encryption and decryption. An audio signal can be separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. RSA technique is used for the encryption and decryption on the lower frequency bands because all the frequency regions do not participate equally in the communication. After applying the encryption on different frequency bands, it is observed that, the encryption on the lower frequency band is more effective than the higher one. The technique is applied on phase values.

Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey in [12] has compared different encryption techniques on MP3 compression. These techniques are applied on audio data, for securely transmitting audio data over the network. Total Data Encryption Standard (DES), total Advanced Encryption Standard (AES) and selective AES encryption techniques are applied on the quantized audio data. A comparison between these encryption techniques is discussed by calculating the time consumption as well as SNR values. Experimental results demonstrate that the time consumption for selective AES encryption on MP3 compression is less than total AES and DES encryption techniques on MP3 compression. So, the selective encryption technique is better than total DES and AES encryption techniques as it takes less time with degradation of signal that is inaudible to the unauthorized users. That the selective AES encryption technique is better than the other two encryption techniques.

Bismita Gadanayak, Chittaranjan Pradhan in [13] have proposed a new encryption technique, which provides good security to the MP3 audio data.This encryption technique for the audio is applied at the time of compression. Advanced Encryption Standard (AES) encryption is applied

On the quantized audio data which is performed before the Huffman's entropy coding the encryption technique is applied to the whole audio data, so it is very difficult for the unauthorized user to access the audio data. The AES encryption technique enhances the cryptographic security of the MP3 audio content.

Zhaopin Su, Guofu Zhang and Jianguo JianG in [10] have surveyed Chaos-Based multimedia encryption techniques. One of the techniques is Encryption considering regions-of-interest. This approach is proposed by Tzouveli et al. In this approach a human video object encryption system (henceforth called HVOE) based on logistic map is proposed. In HVOE, face regions are first efficiently detected, and afterwards body regions are extracted using geometric information of the location of face regions. Then, the pixels of extracted human video objects are encrypted based on logistic map. It can resist brute-force attack, different-key attack and differential attack, and it is efficient in computational resources and running time. But, these chaos-based multimedia encryption methods are not yet mature and more efforts are needed for its further development toward practical applications with high security, low computational complexity, invariance of compression ratio, format compliance, real-time, multiple levels of security, and strong transmission error tolerance. Chaos-based multimedia encryption techniques can be used as the foundation of future research.

Hong gang Wang, Michael Hempel, Dongming Peng Hamid Sharif and Hsiao-Hwa Chen in [14] has proposed an index-based selective audio encryption scheme for WMSNs in order to ensure security, audio quality and energy efficiency. The scheme protects data transmissions by incorporating both resource allocation and selective encryption based on modified discrete cosine transform (MDCT). In this scheme, the audio data importance is leveraged using the MDCT audio index, and wireless audio data transmission proceeds with energy efficient selective encryption. The proposed approach offers a significant gain in terms of energy efficiency, encryption performance and audio transmission quality.

R.Gnanajeyaraman K.Prasadh, Dr.Ramar have proposed a novel higher dimensional chaotic system for audio encryption in [15].In this system variables are treated as encryption keys in order to achieve secure transmission of audio signals. Since the highly sensitive to the initial condition of a system and to the variation of a parameter, and chaotic trajectory is so unpredictable. This gives much higher security. The higher dimensional of the algorithm is used to enhance the key space and security of the algorithm. The security analysis is done. The experiments show that the algorithm has the characteristic of sensitive to initial condition, high key space; digital audio signal distribution uniformity and the algorithm will not break in chosen/known-plaintext attacks.

IV. CONCLUSION

In this paper, 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. More secure and faster encryption techniques will always work.

REFERENCES

[1]. Gunjan Gupta''Review on Encryption Ciphers of Cryptography in Network Security" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue7.Julyl2012

[2]. Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad"Superior Security Data Encryption Algorithm (NTRU)"International Journal of Engineering Sciences, Vol.6, July 2012

[3]. 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

[4]. G Ramesh, Dr R Umarani"A New Symmetrical Encryption Algorithm with High Security and Data Rate For WLAN andwidth Line"International Journal of Information Technology, Vol.2, Isssue4, April2012

[5]. Milind Mathur, Ayush Kesarwani "Comparison between DES, 3DES, RC2, RC6, BLOWFISH AND AES"Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[6]. Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale"SMS Encryption Using AES Algorithm on Android "International Journal of Advanced Computer Applications, Vol.50, No.19.July2012

[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]. Agus Dwi Suarjaya"A New Algorithm for Data Compression Optimisation"International Journal of Advanced Computer Science and Applications, Vol.3, No.8.2012

[9]. Hyubgun Lee, Kyounghwa Lee, Yongtae Shin"AES Implementation and Performance Evaluation on 8-bit Microcontrollers" International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009

[10]. Zhaopin Su, Guofu Zhang and Jianguo Jiang "Multimedia Security: A Survey of Chaos-Based Encryption Technology "School of Computer and Information, Hefei University of Technology China, No.5.2012

[11]. 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

[12]. Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey"Comparative Study of Different Encryption Techniques on MP3 Compression "International Journal off Computer Applications (0975 – 8887) Volume 26– No.3, July 2011

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

[14]. Hong gang Wang, Michael Hempel, Dongming Peng Hamid Sharif and Hsiao-Hwa Chen"Index-Based Selective Audio Encryption for Wireless Multimedia Sensor Networks" IEEE TRANSACTIONS ON MULTIMEDIA, VOL.12, NO. 3, APRIL 2010

[15]. R.Gnanajeyaraman K.Prasadh, Dr.Ramar "Audio encryption using higher dimensional Chaotic map "International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

