A Review Paper on Audio Encryption

Ms. Vishakha B. Pawar[1], Prof. Pritish A. Tijare[2], Prof. Swapnil N. Sawalkar[3]
M.E.(Pursuing)[1],Associate Professors[2],Assistant Professor[3]
Department of Computer Science and Engineering[1, 3]Department of Information Technology[2]
Sipna College of Engineering and Technology,Amravati,Maharashtra,India[1, 2, 3]
vishakhapawarpaper2014@gmail.com[1] , pritishtijare@rediffmail.com[2],swapnil.sawalkar@gmail.com[3]

Abstract- The growth rate of the web exceeds day by day. With the quick growth of web, there's have to be compelled to defend the sensitive knowledge from unauthorized access. Cryptography plays a serious role within the field of network security. There are unit several encryption techniques on the market presently to secure the information. During this review paper we'll have an outline of encoding techniques. This paper chiefly focuses on encryption techniques for audio knowledge. This presents a study and comparison of basic encoding standards and a literature survey encryption technique that are used for encoding on audio data.

Index Terms- OFDM; encryption; orthogonal matrix; key.

1. INTRODUCTION

Cryptography can be outlined as the art or science of sterilizing information or modifying it to a chaotic state, so that the important information is tough to extract throughout transfer over any unsecured channel. Over the decades from Caesar cipher to RC4, an amount of diverse encryption methods have been purposed and implemented. Latest advancements in technology and new ideas like quantum cryptography have superimposed an entire new dimension to information security. The strength of this cryptographic technique comes from the very fact that nobody will scan (or steal) the data without sterilizing its content. This alteration alerts the communicators concerning the chance of a hacker and so promising an extremely secure information transfer. 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 information. Throughout the course of your time, numerous cryptography algorithms are developed to realize the final aim of safe atmosphere for information transmission. Though, the primary objective managing the planning of associate cryptography rule should be security against all attainable unauthorized attacks. However, for all sensible applications, performance and therefore the price of implementation are necessary issues. The simplest cryptographic rule is that the one that strikes a decent balance between security and performance. 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. However, most of the proposed techniques encrypt only text data, a very few technique are proposed for image, audio and video data. 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 protected and faster audio encryption technique. 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. U.S., Defense Department, began the work on audio encryption in late 1940’s. At the outset, the research was used in World War II for secured communication. For providing the security so that enemies could not understand the conversation among military people, the idea first was introduced by simply adding some noise to a voice signal. The main conception was, a noise signal is value-added by taking part in a recorded noise in synch with the voice signal and at the receiving point, the noise signal was deducted out in order to induce original voice signal. However, there was a requirement of same noise signal at both the ends, so the noise signal were created in pairs, one for sender and one for receiver . Therefore, the concept was terribly sturdy as by using only two copies of the signal, it absolutely was terribly troublesome to decrypt the encoded signal [1]. U.S. defense department had given this project to Bell laboratories, to implement this concept. The enforced system is called Sigsaly [2]. So the Sigsaly was the primary enforced plan of most secure voice encryption system. Selective encryption is a modern approach to scale back the process necessities for huge volumes of transmission data in distribution networks with diverse client device capabilities. OFDM was first projected by Chang [3]. Orthogonal frequency division multiplexing (OFDM) is a widely used modulation and multiplexing technology, that has become the premise of many telecommunications standards as well as wireless local area networks (LANs), digital terrestrial television (DTT) and digital radio broadcasting in much of the world. The OFDM concept relies on spreading the information to be transmitted over an oversized variety of carriers, each being modulated at an occasional rate. The carriers are made orthogonal to each other by appropriately choosing the frequency spacing between them [4]. The benefits of OFDM include: It can attain high data rate with excessive bandwidth efficiency and flexible underlying modulations. The secrecy of messages has become progressively more vital in the past decade. The majority standards have incorporated security algorithms to make sure that knowledge has been firmly transmitted over the channel. To make sure the secrecy of messages is not disclosed to unwanted parties, various encryptions mechanisms are usually applied to the messages before they are transmitted. Selective encryption is usually referred to as the partial encryption. Mainly, selective encryption can be utilized not only to realize a similar perceptual result of full encryption (that means of complete content protection) but also to preserve the original quality with restricted and controlled disturbance. In our technique, we encrypt the audio.

2. LITERATURE SURVEY

There are innumerable coding algorithms (encryption standards) within the field of cryptography. These are symmetric and asymmetric encryption algorithm. Some basic symmetric encryption algorithms are studied and elaborated below:-

DES-The DES (Data coding Standard) was produced by IBM in 1975.It was the primary coding commonplace and remained a worldwide commonplace for a protracted time and was replaced by the new Advanced coding commonplace (AES) [5].It provides a basis for comparison for brand new algorithms .DES could be a block cipher primarily based symmetric rule, same keys are used for each coding and secret writing. It makes use of 56 bits key. DES encrypts the knowledge in 64 bits data blocks. Triple DES (TDES) could be a block cipher fashioned from the DES cipher by exploitation it three times. DES isn't robust enough. Several attacks recorded against it.

Triple DES-It 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 alternative attacks, TDES was created as a same algorithmic rule with long key size. In 3DES, DES is performed thrice to extend security. It's conjointly a block cypher technology having key size of 168 bits and block size of 64 bits. DES is performed thrice, therefore it is slower algorithmic rule [5].Triple DES has low performance in terms of power consumption and outturn compared with DES. It continually needs longer than DES as a result of DES is continual thrice.

Blowfish- It is Block cipher primarily based secret writing algorithmic rule provided by Bruce Schneider in 1993. It has variable length key starting from 32 bits to 448 bits and block size of 64 bits [5].The algorithmic rule operates with two half's: a key growth half and an information secret writing part. The role of key growth half is to converts a key of at the most 448 bits into many sub key arrays to tailing 4168 bytes. All operations are EX-ORs and additions on 32-bit words. Blowfish is successor to Twofish [6]. It suffers from week key issues. So some attacks are probable against it.

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 relies on the utilization 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 transmitted on the Internet on the Cypherpunks anonymous remailer's list. The RC4 algorithm is remarkably simply and quite easy to explain. RC4 is appropriate 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. RC2 has disadvantage over further algorithms in terms of time consumption. RC2 is susceptible 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 [8]. RC6 uses a block size of 128 bits and having key sizes of 128, 192 and 256 bits. It is analogous to RC5 in structure. It is symmetric cipher algorithm.RC6 is susceptible to brute force attacks.

AES-It is most broadly adopted encryption standard. AES was originally referred to as rijndael. This commonplace 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 [9]. Number of rounds in the encryption or decryption processes depends on the key size. Overall operation is therefore the same as the Data Encryption Standard (DES). The algorithm was created by Carlisle Adams and Stafford Tavares. .It needs terribly low RAM space and is incredibly very fast. It can be used for encryption of Text, Audio, and Image data. AES provides tremendous Data Security.

Comparison table-

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

Sheetal Sharma, Lucknesh Kumar in [10] has projected associate degree coding algorithmic program for audio file victimization RSA algorithmic program. RSA is asymmetric coding technique. In this paper a frequency domain of the wave audio signal is taken for the coding and encoding. An audio signal may be separated into totally different frequency bins with concern to phase and magnitude values by applying DFT on the audio signal. RSA technique is employed for the coding and secret writing on the lower frequency bands as a result of all the frequency regions don't participate equally within the communication. Once applying the coding on totally different frequency bands, it's determined that, the coding on the lower band is simpler than the upper one. The technique is applied on section values. Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey in [11] has compared totally different coding techniques on MP3 compression. These techniques square measure applied on audio knowledge, for confidently conveying audio knowledge over the network. Total Data Encryption Standard (DES), total Advanced coding normal (AES) and selective AES coding techniques square measure applied on the measure audio knowledge. A comparison between these coding techniques is mentioned by hard the time consumption furthermore as SNR values. Experimental results demonstrate that the time consumption for selective AES coding on MP3 compression is a smaller amount than total AES and DES coding techniques on MP3 compression. So, the selective coding technique is best than total DES and AES coding techniques because it takes less time with degradation of signal that's unsounded to the unauthorized users. That the selective AES coding technique is best than the opposite 2 coding techniques. Bismita Gadanayak, Chittaranjan Pradhan in [12] have projected a brand new coding technique that provides smart security to the MP3 audio knowledge. This coding technique for the audio is applied at the time of compression. Advanced coding normal (AES) coding is applied. On the measure audio knowledge that is performed before the Huffman‟s entropy writing the coding technique is applied to the total audio knowledge, thus it's terribly troublesome for the unauthorized user to access the audio knowledge. The AES coding technique enhances the science security of the MP3 audio content. Zhaopin Su, Guofu Zhang and Jianguo JianG in [13] have surveyed Chaos-Based transmission coding techniques. One in every of the techniques is coding considering regions-of-interest. This approach is projected by Tzouveli. During this approach somebody's video object coding system supported logistical map is projected. In HVOE, face regions square measure 1st expeditiously detected, and after body regions square measure extracted victimization geometric data of the situation of face regions. Then, the pixels of extracted human video objects square measure encrypted supported logistical map. It will resist brute-force attack, different-key attack and differential attack, and it's economical in process resources and time period. But, these chaos-based transmission coding ways aren't nonetheless mature and additional efforts square measure required for its additional development toward sensible applications with high security, low process complexness, invariance of compression quantitative relation, format compliance, real-time, multiple levels of security, and powerful transmission error tolerance. Chaos-based transmission coding techniques may be used because the foundation of future analysis. Hong gang Wang, archangel Hempel, Dongming Peng Hamid Sharif associate degreed Hsiao-Hwa subgenus Chen in [14] has projected an index-based selective audio coding theme for WMSNs so as to make sure security, audio quality and energy potency. The theme protects knowledge transmissions by incorporating each resource allocation and selective coding based on modified discrete cosine transform (MDCT). During this theme, the audio knowledge importance is leveraged victimization the MDCT audio index, and wireless audio knowledge transmission take with energy economical selective coding. The projected approach offers a big gain in terms of energy potency, coding performance and audio transmission quality. R.Gnanajeyaraman K.Prasadh, Dr.Ramar have projected a unique higher dimensional chaotic system for audio coding in [15].In this system variables square measure treated as coding keys so as to realize secure transmission of audio signals. Since the sensitive to the initial condition of a system and to the variation of a parameter, and chaotic flight is thus unpredictable. This provides abundant higher security. The upper dimensional of the algorithmic program is employed to reinforce the key house and security of the algorithmic program. The protection analysis is completed. The experiments show that the algorithmic program has the characteristic of sensitive to initial condition, high key space; digital audio signal distribution uniformity and also the algorithmic program will not break in chosen/known-plaintext attacks.

3. CONCLUSION

In this paper, we have discussed various encryption algorithms for 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. In future also one can use the existing algorithms and develop more secure and faster encryption techniques.

Acknowledgments

It is a matter of great pleasure by getting the opportunity of highlighting fraction knowledge, I acquired during my technical education through this paper. I wish to acknowledge my guide Prof. P. A. Tijare and co-guide Prof. S. N. Sawalkar, with heartfelt gratitude for the valuable guidance I received from them through formal information, discussion & timely inspiration. I would like to thank my parents, friends and all of them who helped me directly or indirectly in my endeavor.

REFERENCES

[1] In May 2009 “Audio encryption using higher dimensional chaotic map” R Gnanajeyaraman, K.Prasadh 2, Dr.Ramar3, Research scholar, Vinayaka Missions University, Salem, Tamilnadu, India.

[2] History of Secure Voice Coding: Insights Drawn from the Career of One of the Earliest practitioners of the Art of Speech Coding, JOSEPH P.CAMPBELL, JR., and RICHARD A. DEAN.

[3] R.W Chang. Synthesis of band-limited orthogonal signals for multichannel data transmission. In Bell System Technical Journal, (45):1775{1796, 1966.

[4] Theory of Frequency Division Multiplexing: http://zone.ni.com/devzone/cda/ph/p/id/269.

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

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

[10] 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.

[11] 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.

[12] Bismita Gadanayak, Chittaranjan Pradhan “Encryption on MP3 Compression”MES Journal of Technology and Management.

[13] 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.

[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.