Sharda Y.Salunkhe, Prof. (Mr.) A.R.Nigavekar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1774-1777

MP3 Music File Protection Using Digital Rights Management and Symmetric Ciphering

Sharda Y.Salunkhe
Dept. of E & Tc. Engg.
K.I.T.College of Engg.Kolhapur,
India.

Prof. (Mr.) A.R.Nigavekar
Dept. of Electronics Engg.
K.I.T.College of Engg.Kolhapur,
India.

Abstract

This paper presents an encryption technique for the Digital Rights Managements which are applied to Mp3music file. Encryption algorithms are used to provide security to the multimedia data. Here, Advanced Encryption Standard (AES) encryption is applied on the audio data with the use of MATLAB tool. The specific work that was conducted in the protection of the MP3 music files and on the specific mechanisms of the DRM platform. Experimental results demonstrate that AES encryption technique provides high security against cryptographies attacks. Here, we have applied the AES encryption technique to different audio files and its utility in the real time systems.

Keywords: DRM, MP3 music file, AES algorithm, RSA algorithm

I. INTRODUCTION

The rapid development of the communication technology and the digital form of information caused a major change in the way the people communicate. People are using more multimedia data due to ease of use and decreasing price of the digital devices. In past decade, digital audio has been favored over analogue recordings because of its robustness against degradations that arise due to transmission. Due to the huge sizes of the digital audio signal, storage requirements increase rapidly thereby increasing the cost. Even if there is sufficient storage space, such files require a large data transfer rate that may be beyond the capabilities of both the processor and hard disk**.** Compression reduces the file sizes using Mathematical algorithms, after which it becomes much easier to manipulate these files. Due to the flexibility in distribution and lower cost of digital information arise copyright issue. Digital data can be duplicated and redistributed at practically no cost. Unauthorized music distribution through internet is a big problem for the music industry. Because of digitization of content enable editing, distributing, shearing, etc.illegaly. In such systems, there are various security issues, which must be considered such as eavesdropping, intrusion, forgery, piracy and privacy, etc.

Digital Rights Management-- a term commonly reduced to the acronym "DRM".

Digital Rights Management is a collective name for technologies or a range of techniques that prevent one from using a copyrighted digital work beyond the degree to which the copyright owner (or a publisher who may not actually hold a copyright) wishes to allow one to use it. It is actually a range of techniques that use information about rights and rightsholders to manage copyright material and the terms and conditions on which it is made available to users.

In terms that are more formal DRM has been described as 'a way of addressing the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over tangible and intangible assets, including management of rightsholders relationships Two possible interpretations of the term digital rights management are:

Management of digital rights: The responsibility of expressing and managing the rights to content in electronic or digital form, as a corollary to content in print.

Digital management of rights: The ability to physically manage intellectual property and proprietary rights in content by way of an electronic system or process associated with copyright management systems. Digital refers not to rights in information but to the medium in which the information is expressed. The rights one is managing are not digital. It is the content of the work that is in digital form. Digital Rights Management systems can be used to protect high-value digital assets and control their distribution and usage. A DRM system offers a persistent content protection against unauthorized access to the digital content, limiting access to only those with the proper authorization. It should be flexible to manage usage rights for different kinds of digital content (e.g. music files, video streams, digital books, images) across different platforms (e.g. PCs, laptops, PDAs1, mobile phones) and control access to content delivered on physical media or any other distribution method (e.g., CD-ROMs, DVDs, flash memory). In this paper, we try to give the security to the MP3 audio file. Here, we proposed the encryption technique to provide security to the music transmission and distribution. We apply AES encryption algorithm, a block cipher encryption technique. In section II, we describe about the MP3

frame format. In section III, the previous work on encryption techniques are discussed. In section IV, we describe about the AES encryption technique. In section V, the purposed techniques for encryption of mp3 audio data is described. In section VI, the experimental results of the proposed algorithm are described.
The final section gives the conclusion.

II. MP3 FRAME FORMAT

Figure 1 shows the structure of the mp3 frame format. The sampling frequency, bitrates and the modes are included in the header part of the mp3 frame. The CRC is used to detect the error in the header and the side information. The main audio data contains the actual compressed audio data. The last parameter, which contains the ancillary data, is ignored by the decoder.

Header	CRC	Side Information	Main Data	Ancillary Data

Figurer 1.mp3 frame format

An MP3 file structure is composed by MP3 frames which have a mandatory header with 4 bytes length (Figure 2) and a variable length payload with the audio samples. Each of the MP3 frame headers is composed by a set of different fields: Sync, ID, Layer, Protection bit, Bit-rate, Frequency, Padding bit, Private bit, Channel Mode, Mode Extension, Copyright, Original/Copy and Emphasis [2, 3].

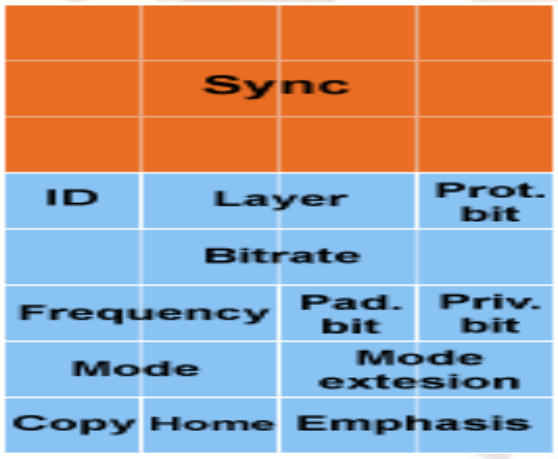

Figure 2.mp3 header

III. RELATED WORK

For securing the MP3 audio data, several security features are applied. Therewith all [5] presented a secure method for online music delivery. In their approach, encryption is applied on the basis of quality of audio layer. The audible frequency spectrum is encoded into MP3standard. Later, for the online music protection on mp3 was purposed by Gang et al [6].Their approach provide different level of protection on music distribution. The first level was “Slight protection”, where the encrypted bit stream provided good quality of music for the causal listener but not good enough for Hi-Fi reproduction. Level two was “moderate protection”, where the encrypted content is meaningful and the main music feature are kept, but with degradation. Level three was “maximum protection”, where the music content is completely destroyed thus renders the MP3 bitstream meaningless. This approach takes a long time for encryption and it’s not practical. The perceptual based approach for MP3 encryption was proposed by Torrubia and Mora [7]. In this approach the Huffman’s code bit were changed that the decoder could construct the corresponding 576 frequency
Lines. The Huffman’s codes are modified by another
Codeword of same size and then encrypted by XOR with the pseudo random bit-stream. But this approach is lack of security because the encryption technique is vulnerable against the Brute Force Attack. The partial or adaptive encryption approach on MP3 was purposed by Chih-Hsu Yen et al [3]. In this approach, three types of partial encryption techniques are applied on the MP3 audio data. These approaches are sign bit of frequency magnitude, Huffman codes and side information encryption. In sign bit encryption when the value of the sample is less than 0, the sign bit is set as 1, otherwise it set to 0.In this paper, and full encryption technique is applied on MP3 file
.

IV. AES (ADVANCED ENCRYPTION STANDARD)

The AES is a symmetric block cipher that process data block of 128 bits using cipher keys with length 128,192 and 256 bits as in [8]. The number of rounds is either 10 or 12 or 14. Each round contains four parts, which are add round key, substitution bytes, shift row and mixed column. This AES encryption method gives more security as compare to other block cipher encryption method. The 128 bit of key size used in AES is resistance against the cryptanalysis attack and the Brute force attack. From the comparisons from TABLE I for different encryption algorithms, the AES encryption algorithm is better in security aspects and for the memory requirement aspects as compare to the other encryption algorithms [9]. Due to the security reason, we have applied the AES encryption technique in this paper.

TABLE I COMPARATIVE RESULT

Encryption Technique	*Complexity*	*Memory Requirement*	*Key Type*	*Key Length*	*Security*
DES	Complex	N/A	Private key	56 bits, 48 bits sub key	Low
RSA	Simple	N/A	Public key	Variable	High
IDEA	Simple	N/A	Public key	128 bits	High
AES	Complex	Very low	Private key	128 bits, 192 bits, 256 bits	High

V. PROPOSED WORK

Here, we proposed an encryption technique which is applied on the MP3 file. We apply AES encryption algorithm which gives good protection to the audio data. This enhances the cryptographic security of the algorithm which will be well suited for online & offline data transmission application.fig shows proposed scheme. When client want to access any song or list of song then it sends the request of song to the server.

Sever send this song for encryption this module is nothing but AES encryption module. Encryption requires Ks (symmetric key) used for AES Encryption. This encryption gives cipher text. This can be sending through internet or any other sending media to the receiver. Encrypted song can be stored in secondary storage media. Encrypted song the goes for decryption but it requires Ks (symmetric key) this key is received from RSA algorithm. Here RSA algorithm plays important role for secure key transmission between client and server. User can access songs multiple times so it requires Ks to K_{sn} (nth key).RSA use two types of key public and private key for encryption and decryption (Ku-public key, kr-Private key)

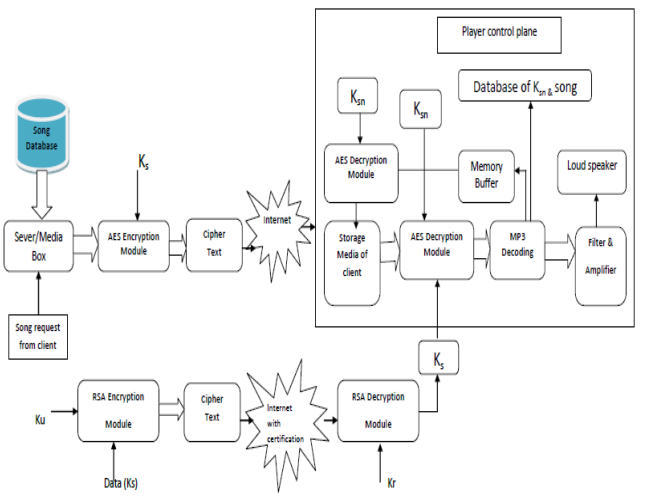

Figure 3. *Block Diagram*

V. EXPERIMENTAL RESULTS

In this section, we evaluate the experimental result of our proposed technique, where we have implemented the AES encryption algorithm on the MP3 file. Here, 128 bits of key is used which gives the protection Figure 4 shows the waveform of an audio file before encryption and after encryption in different combination of both signal like addition and subtraction).

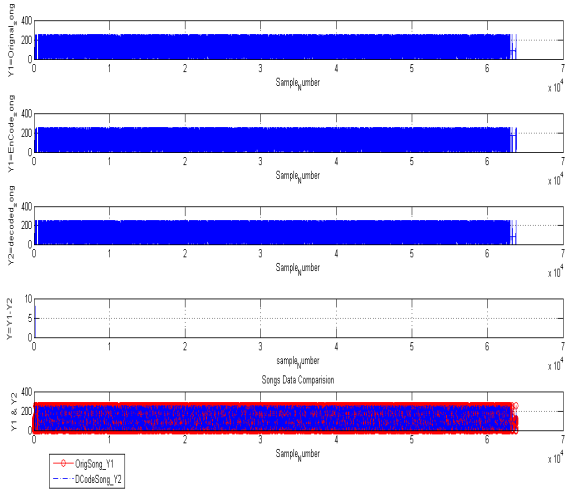

Fig.4 Resuls of 1)Original sinal2)Y1-Ecrypted signal
3)Y2-Decrypted signal4)Y1-Y25)Y1 &Y2

VI. CONCLUSION

Encryption technique is often used to protect the multimedia content from the unauthorized user. In this paper, we have proposed a new encryption technique, which provides good security to the MP3 audio data. Here, we apply the encryption technique to the whole audio data, so it is very difficult for the unauthorized user to access the audio data. Thus, the AES encryption technique enhances the cryptographic security of the MP3 audio content. In a model for increasing the security of audio data presented .the approach, which is based on concept from digital Rights management, add a measure of integrity protection but is primarily intended to aid in relay preventions.

REFERENCES

[1] MP3 licensing web-site, http://www.mp3licensing.com
[2] Technical information about the MP3 file format, http://www.mp3-tech.org/
[3] Chih-Hsu Yen, Hung-Yu Wei, and Bing-Fei Wu, "New Encryption Approaches to MP3 Compression", Department of Electrical and Controling Engineering, National Chiao Tung University, 2003.
[4] Digital Rights Management and consumers' use of music: An activity

theory perspective by Jenny Waycott, Margaret Jackson, Supriya Singh RMIT, Jenine Beekhuyzen, Griffith University

[5] Thorwirth, N.J., Horvatic, P., Weis, R., and Jian Z., 2000, "Security Method for MP3 Music Delivery", Proceedings of the 34th Asilomar Conference on Signals, Systems and Computers 2000, Vol. 2, Oct. 29 - Nov. 1, pp. 1831-1835..

[6] JGang, L., Akansu, A. N., Ramkumar, M., and Xuefei, X., 2001, "On-Line Music Protection and MP3 Compression", Proceedings of 2001 International Symposium on Intelligent Multimedia, Video and Speech Processing, May 2-4, pp. 13 – 16

[7] Torrubia, A. and Mora, F., 2002, "Perceptual Cryptography on MPEG 1 Layer III Bit-Streams", Proceedings of International Conference on Consumer Electronics (ICCE 2002), June 18-20, pp. 324 - 325.

[8] Federal Information Processing Standard Publication, "Advanced Encryption Standard", November 26, 2001

[9] Ming Yang, N Bourbakis and S.Li, "Data Image & Video Encryption", IEEE, 18th October, 2004

[10] C. N. Zhang. C. Yang and A. Kostiuk, "A Secure MP3 Codec Supporting Encryption and Watermarking", 13th International Conference on Parallel and Distributed Computing Systems, August 2000, Las Vegas, pp 640-645.