Selective Encryption of MP3 Compression

Bismita Gadanayak
School of Computer Engineering
KIIT University
Bhubaneswar-751024, India

Chittaranjan Pradhan
School of Computer Engineering
KIIT University
Bhubaneswar-751024, India

ABSTRACT
This paper presents selective encryption technique for the audio which is applied at the time of compression. Here, Advanced Encryption Standard (AES) encryption is applied on the quantized audio data which is performed before the Huffman's entropy coding. 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. The selective technique will save the computational time with the provision of providing security on the audio data.

Keywords-*AES; MP3; FFT; MDCT; Selective Encryption.*

1. INTRODUCTION
The rapid development of the internet and the digital 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. So, in order to provide secure on-line music distribution, a secure audio compression format is required. Encryption on audio compression creates a protection shell around audio data; so that only the authorized user can access the audio data.

Multimedia data are encrypted basically in two ways. First one is to encrypt the content before the quantization and coding; and other is to encryption after the compression [1]. In this paper, we try to give the security to the MP3 audio data. Here, we proposed the encryption technique at the time of compression to provide security to the online music transmission and distribution. We apply the selective AES encryption algorithm; a block cipher encryption technique.

2. MP3 COMPRESSION TECHNIQUE
MPEG Layer III audio coder is the most complex compared to the other two layers, but it gives the best performance of the phase-1 coder. It introduced many new features, in particular a switched hybrid filter bank. The higher frequency resolution is achieved by subdividing each of 32 sub bands with an 18-point modified discrete cosine transform (MDCT). The maximum number of frequency component is 32×18=576, each representing a bandwidth of only 24000/576=41.67 Hz. The 18-point block transform applied because it provides better frequency resolution as in [2]. Each granule in MP3 contains 576 MDCT coefficients. The MDCT output samples are non-uniformly quantized. According to the MP3 definition, one MP3 audio frame contains four granules and each granule contains 576 of MDCT coefficients. The quantized values of these coefficients are further divided into three regions; such as big value, counter one region and zero regions. Then, these coefficients are subsequently compressed by four Huffman's tables [3]. One special feature of layer III is the bit reservoir, which leads to further saving in bit rate. In the first stage, the samples audio signals are divided into frames [4]. Then the signals are passed through the filter bank to time to frequency domain change of signal. The FFT is applied on the sampled data and passed through the psychoacoustic model which discarded the inaudible audio signal using the masking phenomenon. This model computes SNRs and takes the short term audio block to be coded. This model is only applied on the encoder side, so the decoder side is made very simple. The MDCT filter is applied to filter these data for quantization and coding as in figure1. Then the output data are passing through the entropy coding known as the Huffman coding. The final stage is the formatting the bit stream.

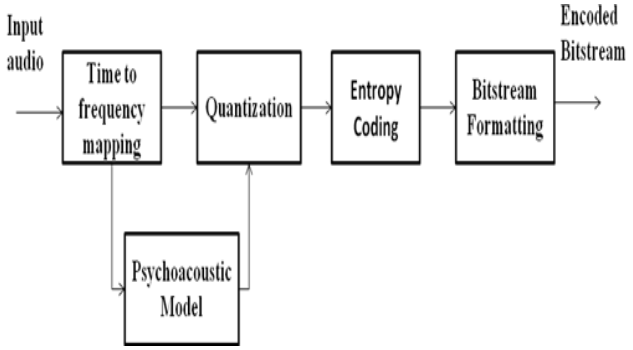

Figure 1 MP3 Compression.

Figure 2 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.

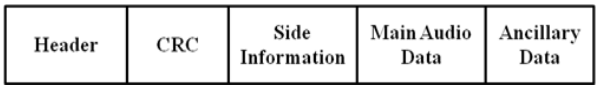

Figure 2 MP3 frame format

3. RELATED WORK

For securing the MP3 audio data, several security features are applied. Thorwith et al [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 MP3 standard. 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 bit stream 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.

4. 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

5. ENCRYPTION BY AES ALGORITHM

Here, we proposed an encryption technique which is applied at the time of compression. 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 real-time data transmission application. In MP3 (MPEG Layer III) compression method, the switch hybrid filter bank is used. The audio data are first divided into 32 sub-band signals. Then to achieve higher frequency resolution 18 point MDCT block transform with 50% overlap. So the maximum number of frequency components is 32×18=576 for one granule of audio data. Then these MDCT co-efficient are quantized non-uniformly. According to the MP3 concept, each MP3 frame contains four granules and each granule contains 576 MDCT coefficients. Then the quantized value of these coefficients is divided into three regions and sequence compressed with Huffman's coding. Then the audio data are sent to the bit stream formatting and get the compressed MP3 audio data. In the proposed technique, we apply the AES encryption algorithm on these 576 quantized audio data as shown in figure 3 and place them in the same position. Then, the encrypted data compressed using the lossless entropy coding, known as Huffman's coding. At the last stage, the bit stream is formatted and gives the encrypted MP3 audio files.

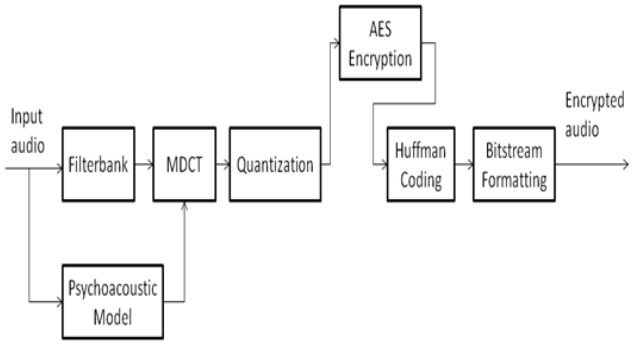

Figure 3 AES encryption on MP3.

For providing more security to MP3 data transfer, we have applied the AES encryption algorithm to the whole quantized audio data. Using this AES encryption, the whole audio data are encrypted. It gives better secure MP3 audio data for online music distribution.

6. SELECTIVE ENCRYPTION BY USING AES ALGORITHM

In this paper, the selective encryption technique is applied at the time of MP3 compression. By applying the full encryption to the whole audio data takes a huge amount of time and slows down the system [10]. This proposed selective encryption technique reduces the time consumption for encryption on MP3 audio data.

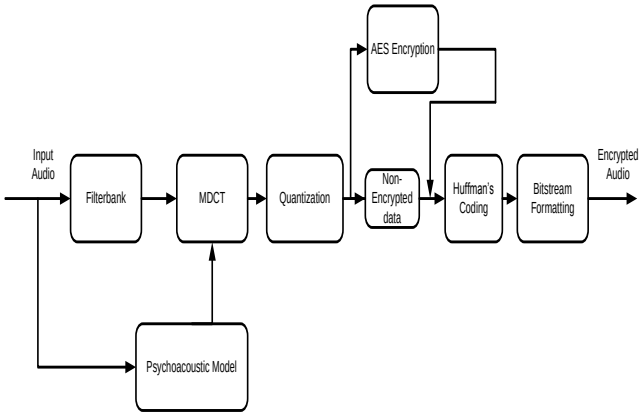

Fig. 4 Partial AES encryption Technique on MP3 Compression

In our proposed technique, we have applied the partial encryption method on the quantized audio data. We have selected the even numbered of positions from these quantized MDCT coefficients for encryption and the odd numbered positions quantized values are not encrypted. Then, we have applied the AES encryption technique on the selected parts of the quantized audio data as shown in Fig 4. After applying the encryption on the selected part, we place these encrypted quantized values on their respective original positions. The quantized MDCT coefficients are compressed by Huffman's entropy coding. The last stage is the bit stream formatting, in which all the audio data are encoded and formatted and finally we have get the encrypted MP3 audio data.

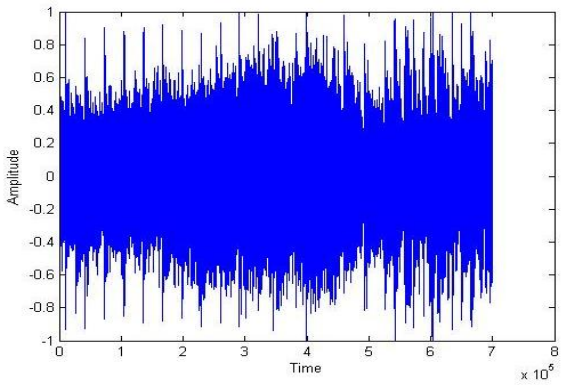

Fig. 5(a) rock1 audio file without encryption

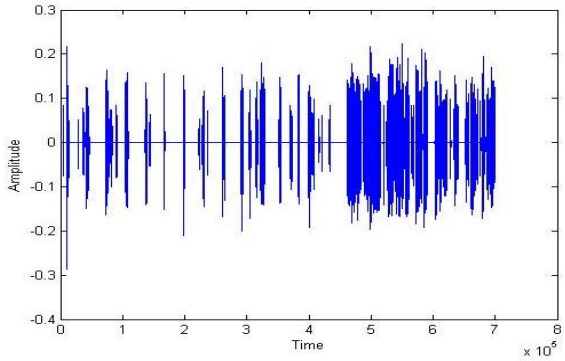

Fig. 5(b) rock1 audio file after AES full encryption

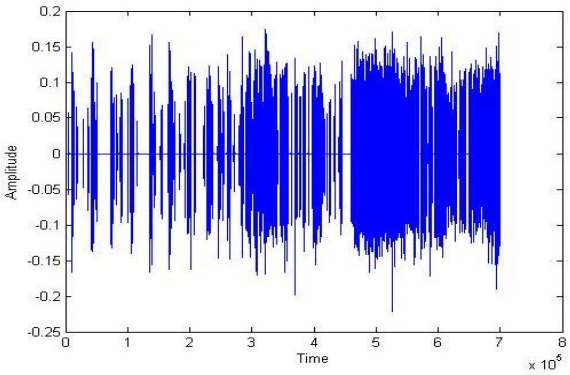

Fig. 5(c) rock1 audio file after partial AES encryption

We have taken rock1 wav file and applied the encryption on the quantized values. The Fig 5 (a) shows the waveform of rock1 audio file without encryption. Fig 5(b) shows the waveform of rock1 audio file after AES full encryption and Fig 5 (c) shows the waveform of rock1 audio file after partial AES encryption.

7. CONCLUSION

Encryption technique is often used to protect the multimedia content from the unauthorized user. In this paper, we have described about selective encryption technique at the time of MP3 compression. We have taken the selected quantized values and applied the AES encryption technique. Using this technique, the computational time for the encryption process decreases as compare to the encrypting the full audio data. This process is fast and provides more security for music e-commerce applications.

8. REFERENCES

[1] Wei-Gang Fu, Wei-Qi Yan, Mohan S. Kanakanhalli, "Progressive Scrambling for MP3 Audio", National University of Singapore, 2005.

[2] Peter Noll, "MPEG Digital Audio Coding",IEEE Signal Processing Magazine,1997.

[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] Joebert S. Jacaba, "Audio Compression Using Modified Discrete Cosine Transform: The MP3 Coding Standard",October 2001.

[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] Gang, 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] Bismita Gadanayak, Chittaranjan Pradhan, "Encryption on MP3 Compression", MES Journal of Technology and Management, Vol. 2, Issue. 1, p.p. 86-89