Comparative Study of Different Encryption Techniques on MP3 Compression

Bismita Gadanayak
School of Computer Engineering
KIIT University
Bhubaneswar, India

Chittaranjan Pradhan
School of Computer Engineering
KIIT University
Bhubaneswar, India

Utpal Chandra Dey
School of Computer Application
KIIT University
Bhubaneswar, India

ABSTRACT

This paper presents different encryption techniques, which are applied on the Moving Picture Expert Group Layer III (MP3) compression, for securely transmitting audio data over the network. Here, 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 on MP3 compression are discussed by calculating the time consumption as well as SNR values. Experimental results demonstrate that the selective AES encryption technique is better than the other two encryption techniques.

Keywords

MP3; DES; AES; SNR; MDCT; Selective Encryption.

1. INTRODUCTION

Multimedia data like audio takes a huge amount of storage space and are extremely inefficient for transmission due to its high bitrate. To overcome these drawbacks, digital audio compression is used; which reduces the size of the audio data and reduces both transmission and storage cost with same signal quality [1]. Multimedia security is required in many audio applications, such as satellite broadcasting, for military communication, audio media delivery and communication via ISDN. In encryption technique, the original data known as plaintext change into ciphertext, that cannot be understood by an unauthorized users. Audio encryption plays an important role in duplication and redistribution during transmission. Digital audio encryption on MP3 compression gives protection on the audio data and limits the access to the unauthorized users.

Many encryption techniques on the MP3 compression have been proposed. The secured online music protection for MP3 audio data is discussed in [2]. When encryption technique is applied on a large amount of audio data, it takes more time [3]. So, selective encryption technique is applied to reduce the time consumption [4]. Here, the comparison between total DES encryption, total AES encryption and selective AES encryption are analyzed and discussed.

2. MP3 COMPRESSION

MP3 Compression preserved the quality of audio with 10:1 to 12:1 compression ratio. The MP3 uses switch-hybrid filterbank as a new feature than MPEG layer I and layer II. Filterbank with MDCT transform is called as switch-hybrid filterbank [5].The input signal is divided into 32 subbands which improved the efficiency of compression by reducing the redundancy. Then, each subband filtered output is passed through 18-point MDCT transform. So, the numbers of frequency components are 576 [6]. Simultaneously, the same signal passed through 1024-point FFT and then applies the psychoacoustic model. The psychoacoustic model is used for discarding the unwanted signals using the masking threshold. Then, the MDCT coefficients are quantized non-uniformly [7]. Each quantized MDCT coefficients are encoded by Huffman's entropy coding in which data is not lost. Finally, the encoded data are formatted using bit stream formatting as shown in Figure 1. Figure 2 shows the sam4 audio file after MP3 compression.

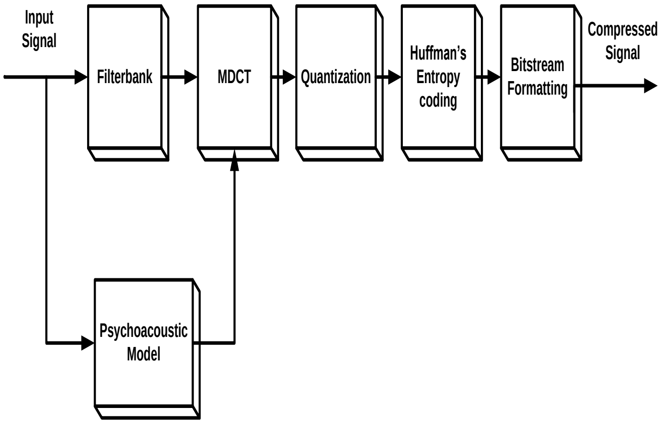

Fig 1: MP3 Compression

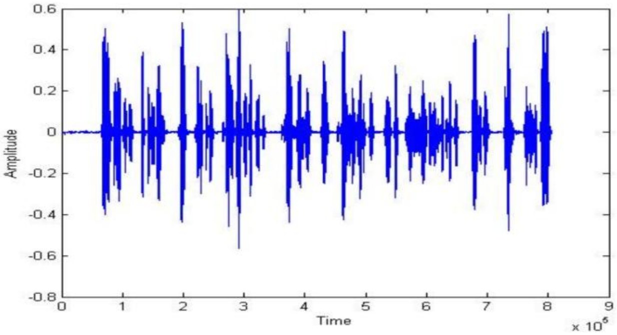

Fig 2: sam4 audio file after MP3 compression

3. TOTAL AUDIO ENCRYPTION BY USING DES

In order to provide secured audio distribution over network, a secured audio compression is required. Applying encryption on the audio data gives protection from the unauthorized users.

Here, the DES encryption is applied on the whole audio data. DES stands for Data Encryption Standard, which is a symmetric block cipher encryption. It uses 64 bits of plain text, 56 bits of key and 16 rounds for encryption [8]. Each round consists of substitution and permutation with using a unique key known as round key. The MP3 frame contains four granules and each granule contains 576 MDCT coefficients. Then, these MDCT coefficients are quantized non-uniformly. DES encryption is applied on these quantized MDCT coefficients which is shown in Figure 3.

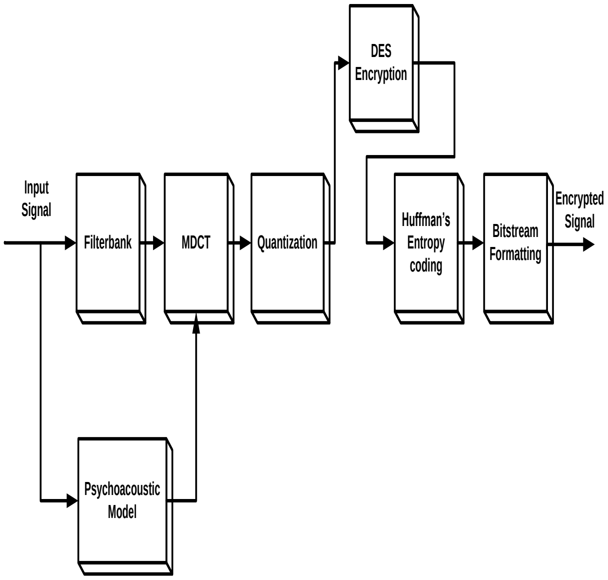

Fig 3: Total Encryption on MP3 Compression by using DES

Then, these data are compressed by using Huffman's entropy coding and are formatted using bit stream formatting. Finally, we get the encrypted signals. Figure 4 shows the sam4 audio signal after applying the DES encryption on the MP3 compression.

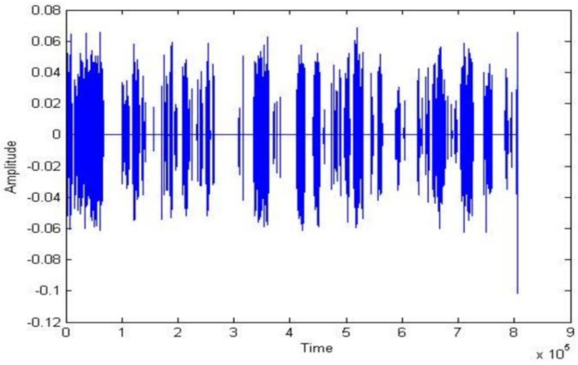

Fig 4:sam4 audio file after total DES encryption

4. TOTAL AUDIO ENCRYPTION BY USING AES

DES encryption technique takes more time and it is vulnerable to the brute-force attack. The attacker takes 2^{56} checks to break the key. The AES encryption technique gives better security than DES [9]. It uses 128 bits of key, which is resistance against the Brute-Force attack [10]. The attacker has to check 2^{128} time to break the key. So, the AES encryption algorithm is applied on the 576 quantized MDCT coefficients as shown in Figure 5. Then, the audio data are encoded using lossless Huffman's entropy coding and at last the encoded audio data are formatted using bit stream formatting to get the encrypted audio signal [11]. Figure 6 shows the sam4 audio file after applying the AES encryption on the quantized MDCT coefficients.

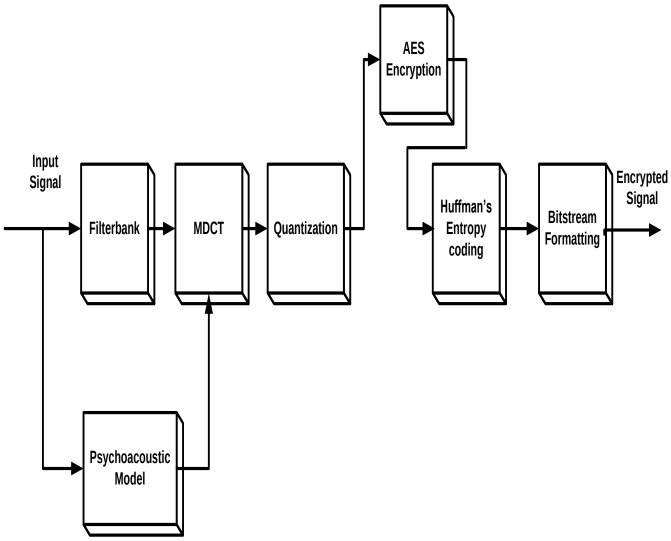

Fig 5: Total Encryption on MP3 Compression by using AES

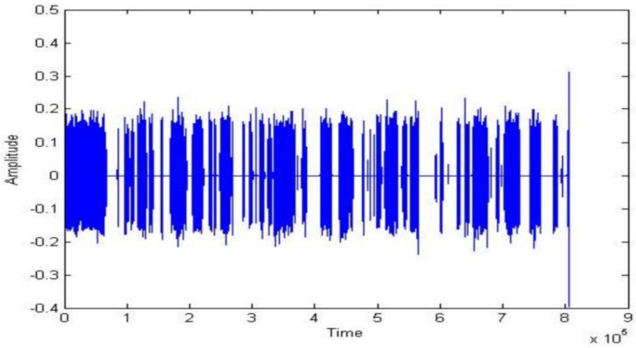

Fig 6: sam4 audio file after total AES encryption

5. SELECTIVE ENCRYPTION BY USING AES

When encryption is applied on the whole audio data, more amount of time is required for encrypting such a large amount of audio data. So, the selective encryption is applied on the audio data to reduce the time consumption with slight degradation of signal quality. After the quantization process, the even numbers of positions of quantized data are encrypted and odd positions data are not encrypted. The AES encryption algorithm is applied on the selected quantized value for encryption [12]. Then, the selected encrypted data are placed in their original positions. These encrypted quantized data are coded by Huffman's entropy coding and finally get the encrypted output. Figure 7 shows the selective encryption by using AES and Figure 8 shows the sam4 audio file after selective encryption.

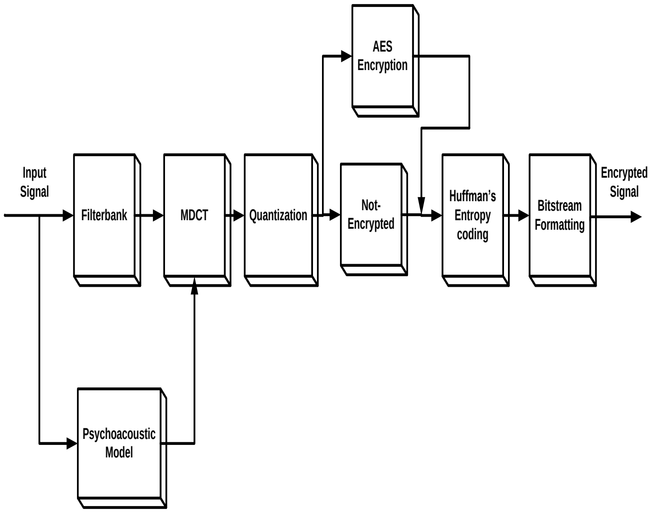

Fig 7: Selective encryption by using AES

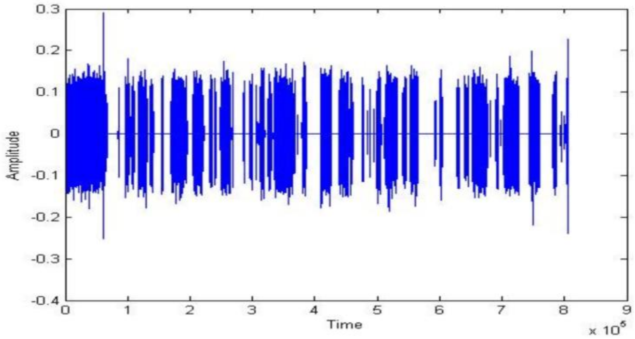

Fig 8: sam4 audio file after selective AES encryption

6. EXPERIMENTAL COMPARIAION

In this part, by taking a audio file, we have applied total DES encryption, total AES encryption and partial AES encryption on the quantized audio data. Figure 9(a) shows the c5 audio file without encryption. After applying total DES encryption on the audio file is shown in Figure 9(b). Figure 9(c) shows the waveform after applying total AES encryption and Figure 9(d) shows the waveform after selective AES encryption.

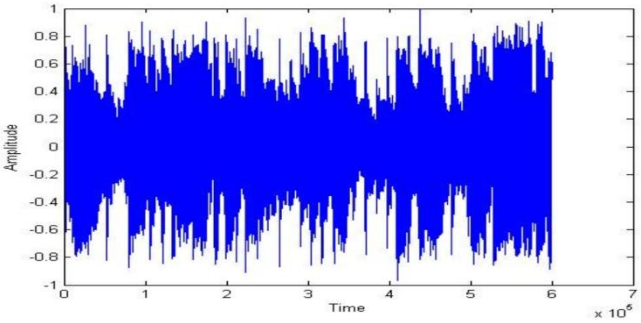

Fig 9 (a): c5 audio file without encryption

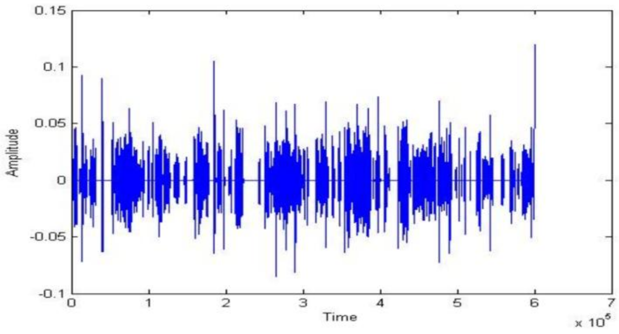

Fig 9(b): c5 audio file after DES encryption

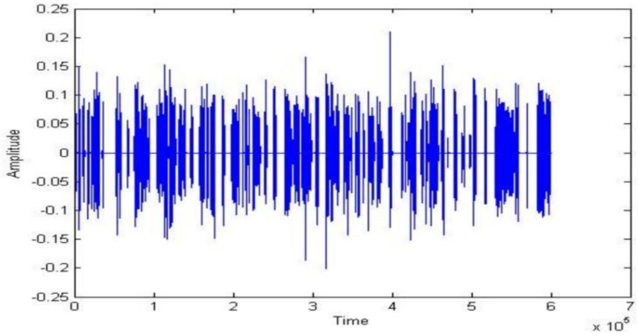

Fig 9(c): c5 audio file after AES encryption

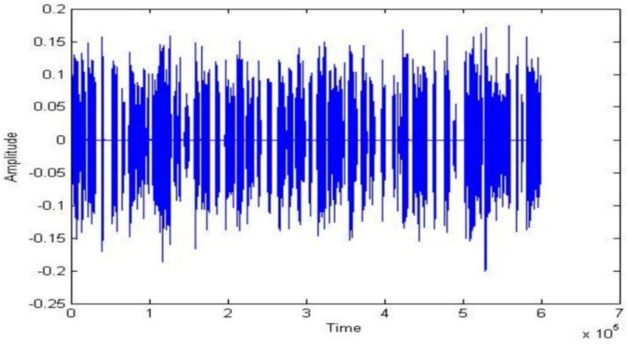

Fig 9(d): c5 audio file after selective AES encryption

We have calculated the time consumption for total DES encryption, total AES encryption and selective AES encryption on different audio files like sam4, c5, hindi5 and rock2 are shown in Figure 10. From the experimental results, we have found that, DES encryption consumes more time than AES encryption technique after applying on the quantized audio data. But, when we are applying the partial AES encryption, the time consumption is least.

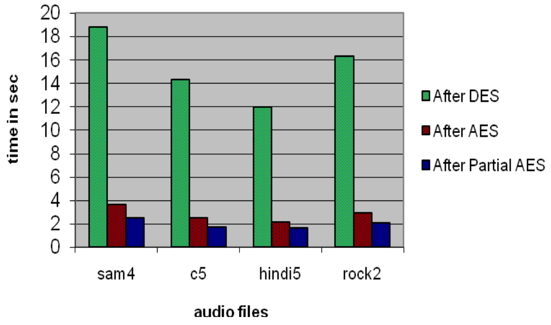

Fig 10: Time Consumption for Encryption

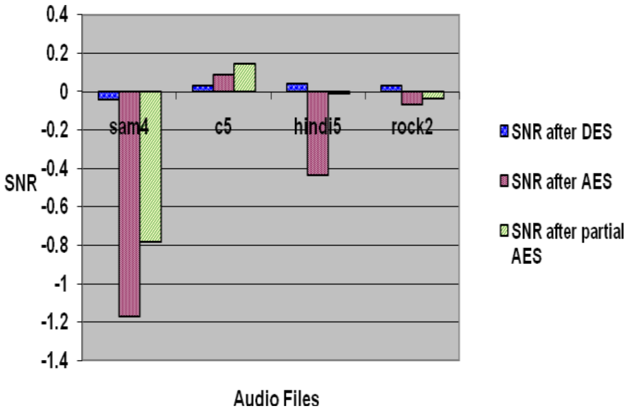

Fig 11: SNR Values after Encryption

Figure 11 shows the SNR values after applying total DES encryption, total AES encryption and selective AES encryption on the different audio files. From this experimental result, we have shown that the SNR value decreases when AES encryption is applied on the MP3 compression than DES encryption. But, when selective AES encryption technique is applied on the audio files, the SNR value increases than total AES; but less than total DES.

So, we have concluded that the selective AES encryption is better than other two encryption techniques. Because, the time consumption is less as compare to other encryption techniques. The SNR value increases but not so high that is audible.

7. CONCLUSION

Encryption techniques are often used to protect the multimedia content from the unauthorized users. In this paper, different encryption techniques are applied on the quantized MDCT coefficients at the time of MP3 compression. Here, the time consumption and SNR values after these encryption techniques are calculated. Experimentally, we conclude 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.

8. REFERENCES

[1] Ranjan Parekh's, Principles of multimedia. The McGraw-Hill, first ed., 2006.

[2] Ding, 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.

[3] Pichit Tananchai and Thumrongrat Amornraksa, "Selective encryption for compressed audio," IEEE, 2009.

[4] 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.

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

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

[7] Davis Yen Pan, "Digital Audio Compression," Digital Technical Journal, vol. 5, no. 3, 1993.

[8] "Data Encryption standard," Federal Information Processing Standards Publication, oct 1999.

[9] "Advance Encryption standard," Federal Information Processing Standards Publication , pp. 92–96, nov 2001

[10] Behrouz A. Forouzan, Cryptography and Network Security. The McGraw-Hill, fourth ed., 2004.

[11] Bismita Gadanayak, Chittaranjan Pradhan, "Encryption on MP3 Compression", MES Journal of Technology and Management, Vol. 2, Issue. 1, p.p. 86-89, 2011.

[12] Bismita Gadanayak, Chittaranjan Pradhan and Neha Baranwal, "Secured Partial MP3 Encryption Technique", International Journal of Computer Science and Information Technologies, Vol. 2 (4), 2011, p.p. 1584-1587.