ISSN:0975-9646
Bismita Gadanayak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1584-1587

Secured Partial MP3 Encryption Technique

Bismita Gadanayak[1], Chittaranjan Pradhan[2], Neha Baranwal[3]

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

***Abstract*— The encryption algorithms are applied for giving security to the audio data. Many encryption algorithms have been proposed to meet the security requirements of the different applications. But, lack of application friendliness limits those algorithms from practical implementation. Encryption technique can be applied on the Moving Picture Expert Group Layer III (MP3) audio data before the MP3 compression, at the time of the MP3 compression and after the compression. Here, we have applied the Advanced Encryption Standard (AES) encryption algorithm at the time of MP3 compression on the selected quantized audio data. The partial encryption technique applied on the audio data is to reduce the time consumption of encryption. This improved the cryptographic security of the algorithm will be well suited for real-time data transmission application.**

***Keywords*— MP3, MDCT, AES, Partial Encryption, Security.**

I. INTRODUCTION

Due to the rapid development of the modern computer, networking and information technology; the security of the multimedia data like audio are becoming more important. People are creating and sharing the multimedia data due to its flexibility and easy to use software and decreasing price of the digital data. The use of the electronics recording and the storage device has increases the use of the multimedia data. The reproduction of the multimedia data in digital form increases without any loss of quality. For giving security to the audio data, which are provided by some mathematical operations; can be achieved by changing the audio data into cipher data for protecting from the unauthorized users. This type of operation is known as encryption on the multimedia data. For secure audio distribution over the network, a secure audio compression format is required. The encryption on the compressed audio data provides high security on the audio data. When encryption process is applied on a huge amount of audio data, it takes more time and slows down the entire system. The selective encryption technique is applied to reduce the processing time of the encryption on multimedia data. In this technique some part audio data are encrypted and others are not encrypted.

Several security features are used to apply on the audio data has been proposed. Thorwirth and Horvatic in [1] encrypted the audio data using selective frequency data for secure online music delivery. Here, the unauthorized users are only hear the lower quality audio. The portions of the audio representing the high quality are still presented within the stream are permanently locked. And those portions can only be accessed by using the secrete key to the authorized listener. Gang et al [2] proposed different level of protection on online audio distribution. Their technique provides different protection level according to different sensitivity requirements. The first level is slight protection, in which the encrypted bitstream provides a satisfactory music quality for a casual listener, but not good enough for the Hi-Fi reproduction. The second level is moderate protection, where the encrypted data is meaningful and the main music content are kept, but with the degradation. For recover the quality of audio, the customer could pay and obtained the decryption key. The third level is the maximum protection, where the audio data is completely destroyed thus sending the MP3 bitstream is meaningless. This approach takes a huge amount of time for encryption and it is not practical feasible.

Chih-Hsu Yen et al [3] proposed the partial or adaptive encryption on MP3 audio data. In this approach, the selected audio data are enciphered by three techniques. These are encrypting the sign bit of frequency magnitude, Huffman's codes and side information. The result are analysed by Masking to Noise Ratio. Selective encryption on the compressed audio is proposed by Pichit Tananchai and Thumrongrat Amornraksa [4]. In this approach, four parameters are extracted from the side information for selective encryption. These are main_data_begin, scfsi, part2_3_length and table_select. Perceptual based approach for MP3 encryption is proposed by Torrubia and Mora [5]. In this approach, the Huffman's code bits were changed in such a way that the decoder could construct the corresponding 576 frequency lines. The Huffman's codes are replaced by another codeword of same size and then encrypted by XOR with the pseudo random bit-stream. For security reason, this technique is not suitable for real time application because the encryption technique is vulnerable against the Brute Force Attack. The partial encryption on the formatted multimedia data is proposed by Hong Heathern Yu [6]. In this approach, the stream formatted media data is partitioning into two parts, the cloak data and non-cloak data. Then the clock data are encrypted by some cryptographic algorithms and other data are not encrypted.

In this paper, a selective encryption method is proposed at the time of MP3 compression to protect the MP3 compressed audio data. Here, some parts of the MP3 data are extracted and AES encryption technique is applied on the selected part. In the next section, we have discussed about the MP3 compression technique. In section III, we have discussed about the proposed technique. In section IV, the experimental results are shown and discussed of the proposed technique. Finally, the last section gives conclusion of the work.

II. MP3 COMPRESSION

MP3 stands for MPEG-1 Layer III, which introduced new features as compare to other layers. This MP3 compression consists of subband filtering, MDCT transform, psycho-acoustic analysis, quantization and Huffman's entropy coding. It uses switched hybrid filterbank as a new feature as compare to the other layers, which is the combination of the filterbank with MDCT transform. The subband filterbank is used, which divides the signal into 32 subbands for time to frequency mapping. For achieving finer frequency resolution, each subband filter output is followed by 18 point MDCT block transform is used [7]. For saving the bitrate a buffer

technique is used, known as bit reservoir. Only the layer III provides the variable bitrate coding. The MP3 compression technique consists of different stages. First, the audio signal pass through the filterbank for time to frequency mapping which divides the signal into subbands and pass through the MDCT transforms. The second stage, 1024 point FFT is apply and then sent to the psychoacoustic model. The psychoacoustics model is used for discarding the in-audible audio data by using the masking and threshold value. The SMR values are calculated for each group of band in this model. This model is only used in the encoder, so the decoder is less complex than encoder. Then, the MDCT transform is applying on the output of the first and second stage audio data as shown in Fig 1. Each MP3 frame contains four granules and each granule contains 576 MDCT coefficients.

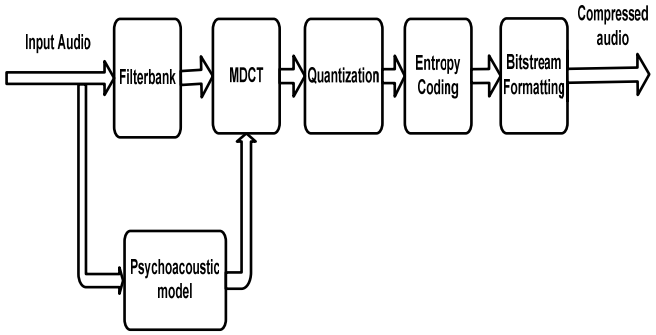

Fig. 1 MP3 Compression Process

Then, these MDCT coefficients are non-linearly quantized. The quantized MDCT coefficients are divided into three regions: big value region, counter one region and zero region. Each region is then compressed using the lossless entropy coding known as Huffman's entropy coding [8]. At last, the audio data is formatted using the bitstream formatting. The bit reservoir manages that the decoder buffer neither underflows nor overflows when the bitstream send to the decoder.

III. PROPOSED WORK

In this paper, the partial 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 partial encryption technique reduces the time consumption for encryption on MP3 audio data.

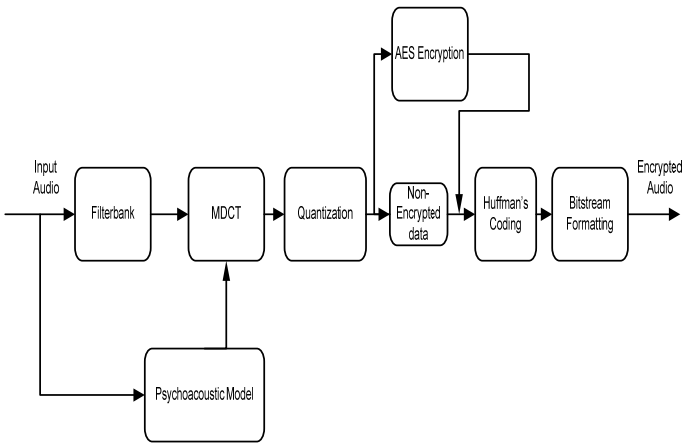

Fig. 2 Partial AES encryption Technique on MP3 Compression

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 2. 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 bitstream formatting, in which all the audio data are encoded and formatted and finally we have get the encrypted MP3 audio data.

For partial encryption, we have applied the AES encryption algorithm which is a symmetric key block cipher encryption technique [9]. The length of the block that used in this encryption technique is 128, 192 and 256 bits. The number of rounds used in AES encryption is 10, 12 and 14. The 128 bit of key size gives more security than other block cipher encryption algorithms.

IV. EXPERIMENTAL RESULT

In this section, we have performed the experimental results to evaluate the effectiveness and flexibility of our proposed work. In the proposed technique, we have used the 128 bits of key size for AES encryption on the quantized audio data. We compare the proposed, partial encryption technique with the full encryption technique. In full encryption, the AES encryption is applied on the whole quantized audio data.

For the analysis, we have taken different wav files and shown the waveforms before applying the AES encryption, after applying full AES encryption and the proposed partial AES encryption as shown in Fig 3 and Fig 4.

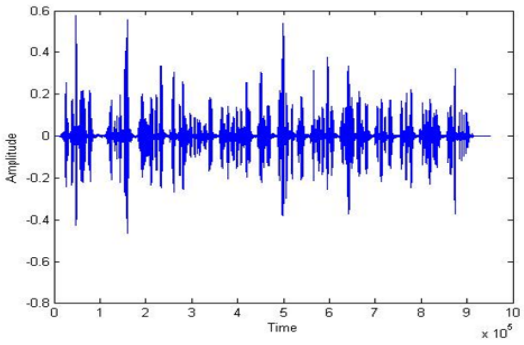

Fig. 3(a) sam1 audio file without encryption

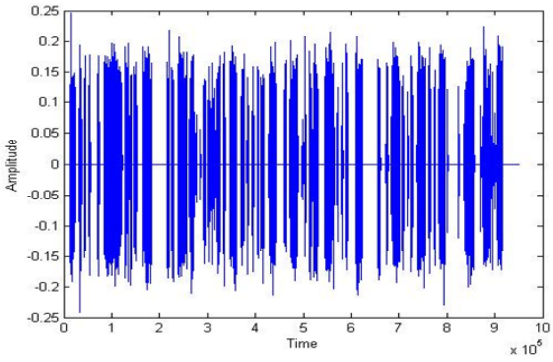

Fig. 3(b) sam1 audio file after AES full encryption

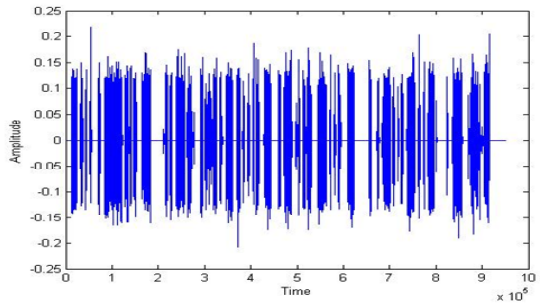

Fig. 3(c) sam1 audio file after partial AES encryption

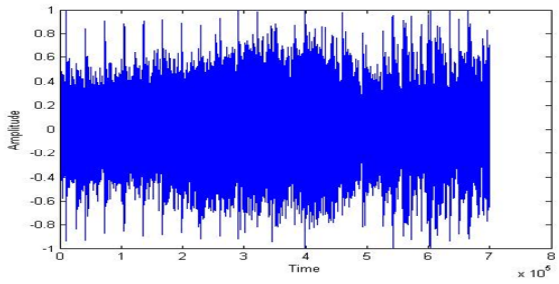

Fig. 4(a) rock1 audio file without encryption

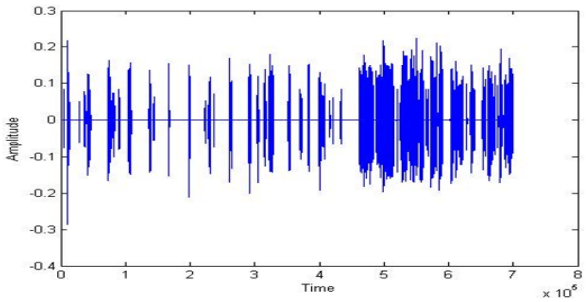

Fig. 4(b) rock1 audio file after AES full encryption

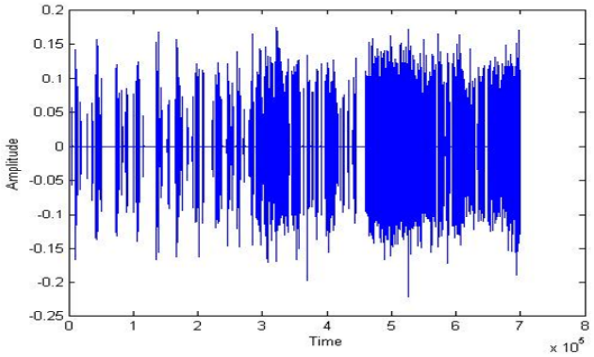

Fig. 4(c) rock1 audio file after partial AES encryption

We have taken sam1 and rock1 wav files and applied the encryption on the quantized values. The Fig 3 and 4 show the waveforms of the audio files sam1 and rock1 without encryption, after AES full encryption and after partial AES encryption. Fig 3(a) shows the waveform of sam1 audio file without encryption. Fig 3(b) shows the waveform of sam1 audio file after AES full encryption and Fig 3 (c) shows the waveform of sam1 audio file after partial AES encryption. Similarly, Fig 4 (a) shows the waveform of rock1 audio file without encryption. Fig 4(b) shows the waveform of rock1 audio file after AES full encryption and Fig 4 (c) shows the waveform of rock1 audio file after partial AES encryption.

TABLE I

TIME REQUIRED FOR PARTIAL AES ENCRYPTION

Audio	Size/ Length	MP3 Com-pression	Full Encryption	Partial Encryption
Sam1	1.81 Mb/ 21 sec	1.36 sec	4.3 sec	2.98 sec
Ins2	2.28 Mb/ 27 sec	1.65 sec	5.03 sec	3.40 sec
Rock1	124 Kb/ 15 sec	1.15 sec	3.19 sec	2.27 sec

In TABLE I, we have calculated the time required without AES encryption, after AES full encryption and after partial AES encryption applied on the MP3 compression. Each audio file has been encrypted with full AES encryption and partial AES encryption.

We have computed the computational time required for full encryption and selective encryption. From this experimental result it shows that the computational time decreases as compared to the full encryption. The proposed partial encryption technique is faster and can be applied on real time audio transmission.

TABLE II

SNR VALUES COMPARISON

Audio	Size/ Length	MP3 Compression	Full Encryption	Partial Encryption
Sam1	1.81 Mb/ 21 sec	22.700db	-1.5465db	-1.0291db
Ins2	2.28 Mb/ 27 sec	17.2984db	0.04363db	0.08343db
Rock1	124 Kb/ 15 sec	13.521db	0.08962db	0.17243db

The TABLE II shows the SNR values of different audio signals. The SNR values of partial AES encryption is more than that of full AES encryption. That means, the SNR value of partial AES encryption is higher, but not so high that is audible.

The security is very high when we are applying the AES encryption technique. The attacker takes very big calculation to break the key to decrypt the audio data.

V. CONCLUSIONS

In this paper, we have described about partial 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.

REFERENCES

[1] 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.

[2] 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] 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] Pichit Tananchai and Thumrongrat Amornraksa, “Selective encryption for compressed audio,” IEEE, 2009.
[5] 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.
[6] Hong Heather Yu, “Partial Encryption of stream-formatted media”, United State Patent, Jan, 2007.
[7] Peter Noll, “MPEG Digital Audio Coding”, IEEE Signal Processing Magazine, 1997.
[8] Joebert S. Jacaba, “Audio Compression Using Modified Discrete Cosine Transform: The MP3 Coding Standard”,October 2001.
[9] Federal Information Processing Standard Publication, “Advanced Encryption Standard”, November 26, 2001.
[10] Bismita Gadanayak, Chittaranjan Pradhan, “Encryption on MP3 Compression”, MES Journal of Technology and Management, Vol. 2, Issue. 1, p.p. 86-89.