Encryption and Compression of Audio-Video Data Using Enhanced AES and J-Bit Algorithm

Manpreet Kaur Grewal[1] Ms. Sukhpreet Kaur[2]
[1]M.Tech Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Shri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Abstract— AES is considered a good encryption algorithm in terms of providing security to a network in passing information (data) in form of audio, string, and video and in any other form. However it yields a low throughput resulting in slowness and increasing energy dispensation of server or an application. The Enhanced AES algorithm is proposed in this paper which works by using sequence counters and provides improved throughput as compare to conventional AES algorithm. The J-Bit Encoding is being a compression algorithm in lossless category which doesn't decrease the quality but reduce the size of data to some extent. It has been observed that the proposed encryption algorithm integrated to J-Bit Encoding algorithm will provide the effective security measures as well as increased throughput as a parameter and less bandwidth usage as the actual size of data shall not be sent along the network.

Keywords: AES, J-Bit, MP3

I. INTRODUCTION

Cryptography can be defined as the art or science of changing or altering information to a chaotic state, so that no one can read the real information when it is transferred over the network or any unsecured channel. Due to the rapid growth of internet, there is need to protect the sensitive data and advancements in technology are of great need to keep data secure from malicious users. The main strength of the cryptographic techniques is that no one can read the information without altering its content which is not an easy task. During the course of time, many encryption algorithms have been proposed to achieve the goal of safe environment for data transfer. The main objective for designing an encryption algorithm must be security against all possible unauthorized attacks. However, for all practical applications, performance, processing time, power consumption and the cost of implementation are also important factors to be considered...The good security algorithm is the one that strikes balance between these factors [3][16].

A. Audio-Video Encryption

Encryption is very important when confidential data is transmitted over the network to keep the data secure. Encryption is a technique used to transmit secure information. During the course of time various encryption techniques have been implemented. But many techniques encrypt only text data, a very few technique are implemented for multimedia data such as video and audio data. The techniques proposed for text data can also be applied to multimedia data but have not attained reasonable results. Various encryption techniques are implemented for multimedia data. Many of them are not sufficient to meet real time requirements and some provide poor security measures. Encryption process for of audio and video data is complex than the methods used for text data. Multimedia encryption ensures secure data transmission. With the fast growth of communication technology, protection of multimedia from the hackers became an important aspect for the technologist. So there will always be a need of a more secure and faster audio encryption technique [11] [16]

II. RELATED WORK

M. Anand Kumar, Dr.S.Karthikeyan [3] in 2012 has proposed a method which evaluates the performance of two commonly known symmetric key algorithms. These algorithms are tested according to different performance metrics. The simulation results showed that the performance of Blowfish is better performance than AES in almost all the test cases. It is concluded that blowfish is good for text based encryption where as AES has better performance for image encryption. It is also identified that there is change in performance when there is a change in key size of AES algorithm.

Milind Mathur, Ayush Kesarwani [5] in 2013 has conducted a comparison for the performance -DES, 3DES, RC2, RC6, BLOWFISH AND AES algorithms. Results shows that here is no significant difference in the case of either in hexadecimal base encoding or in base 64 encoding, Blowfish has better performance than other common encryption algorithms used. In the case of changing packet size, RC2, RC6 and Blowfish has disadvantage over other algorithms. In the case of changing data type such as image instead of text.

Jawahar Thakur, Nagesh Kumar [6] in 2011 proposed a method for simulation based performance analysis of most common symmetric key cryptography algorithms: DES, AES, and Blowfish. This evaluated performance of algorithms under different settings. Results showed that Blowfish has a better performance than other common encryption algorithms used.AES showed poor performance results compared to other algorithms since it requires more processing power. Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks.

Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey [8] in 2011have proposed a method presenting different encryption techniques, which are applied on the Moving Picture Expert Group Layer III (MP3) compression, for securely transmitting audio data over the network. Experiments concludes that the time consumption for selective AES encryption on MP3 compression is less than total AES and DES encryption techniques on MP3 compression.

Agus Dwi Suarjaya [9] in 2012 have proposed and confirmed a data compression algorithm that can also be used to optimize other algorithm. This algorithm is called j-

bit encoding (JBE).The algorithm will manipulates each bit of data inside file to minimize the size without losing any data after decoding which is classified to lossless compression. The performance of this algorithm is measured by comparing combination of different data compression algorithms. An experiment was conducted by using 5 types of files with 50 different sizes for each type, 5 combination algorithms tested and compared. When inserted between move to front transform (MTF) and arithmetic coding (ARI), this algorithm gives better compression ratio.

Hyubgun Lee, Kyounghwa Lee, Yongtae Shin [10] in 2009 proposed the solution of reliable sensor network through measuring performance of AES encryption algorithm by plaintext size to analyze the communication efficiency and cost of operation per hop according to the network scale. They analyzed the performance of AES encryption algorithm on ATmega644p in 8-bit microcontroller. As a result, scale of the sensor network grows, the delay is doubled and energy consumption also increased accordingly.

R.Gnanajeyaraman K.Prasadh, Dr.Ramar [11] in 2009 has proposed a novel higher dimensional chaotic system for audio encryption in. Variables are treated as encryption keys in order to achieve secure transmission of audio signals. This gives much higher security. The higher dimensional of the algorithm is used to enhance the key space and security of the algorithm. The experiments show that the algorithm has the characteristic of sensitive to initial condition, high key space; digital audio signal distribution uniformity and the algorithm will not break in chosen/known-plaintext attack.

III. RESEARCH METHODOLOGY

Methodology of constructing the proposed system will consists of various modules. Each module uses different techniques and algorithms to perform its specific tasks. After a particular module completes its task, its output will become input for the next module. In the end the combined effort of each module will be displayed. The working modules of the proposed work are detailed below

A. Module 1-Symmetric Key Algorithm

The AES cryptographic algorithm falls under the symmetric encryption, i.e. the same key is used at both ends to encrypt and decrypt the data. However, AES actually depends on the sequence counter instead of the encryption key. The major benefit of using AES over other encryption algorithms is its power of customization. The user can manipulate the sequence counter according to his needs; whether he wants it to be simple and faster or hard to crack and secure.

Sequence Counter - Sequence counter is used to provide the dynamic behavior while converting the characters from one form to another. Sequence counters are the imposed temporary key to alter the characters and bits in the original data. The sequence is applied to the chosen number of data bits and the sequence number changes according to an algorithm, which needs not to be saved or transferred over the network.

The sequence counters in the proposed algorithm are used at following levels:

1) Block level

This is the uppermost level where blocks characters of a single block or line are transposed according to the sequence counter.

2) Character Level

Every character have an equivalent ASCII value, which can be merged with the sequence counter.

3) Binary Level

The binary level is lowermost level. The calculation done here is totally is in form of 0 and 1. Bit level calculation provide more security because its effect are visible to all the level above it include character level.

The encryption process for the proposed work is shown below.

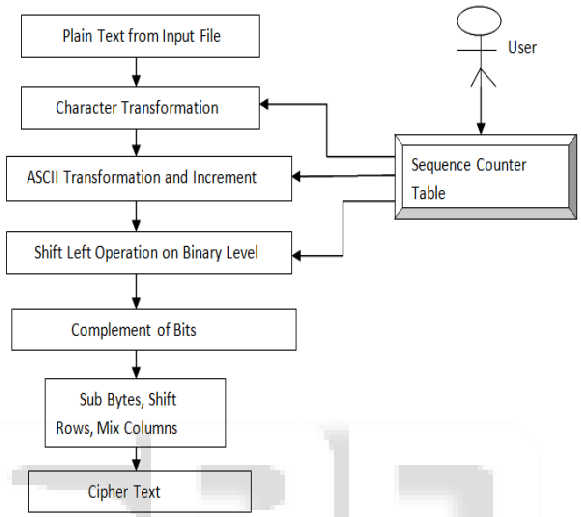

Fig. 1: Enhanced AES encryption process

The decryption process for the proposed work is shown below.

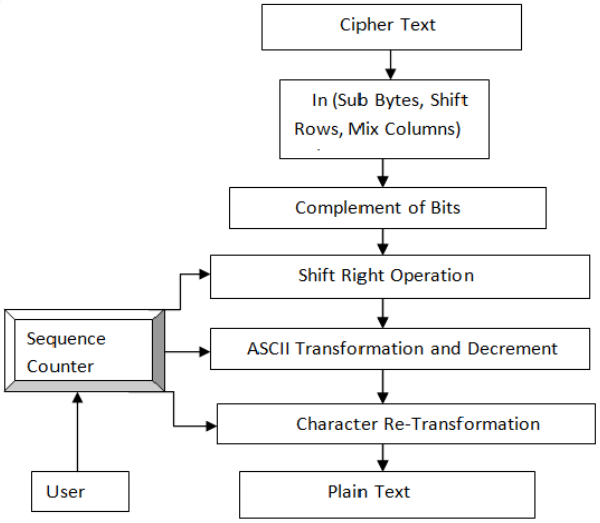

Fig. 2: Enhanced AES Decryption Process

The algorithm proposed in this paper works using Sequence Counters is based on the concept of user customization. The algorithm doesn't use the traditional approach of using an encryption key; but defines a series of sequence-counters for encoding. The cryptosystem gives extra power to the user i.e. to choose the sequence counters.

Thus it is up to the user to maintain a balance between speed and security provided by the algorithm. The user can increase or decrease security and speed depending

upon his/ her needs. The cryptographic algorithm is based partially on both stream and block encryption, hence the output of same input block over same input sequence-counter is dissimilar and provides enhanced security.

B. Module 2-J-bit encoding (JBE) Algorithm

J-bit encoding (JBE) works by manipulate bits of data to reduce the size and optimize input for other algorithm. The main idea of this algorithm is to split the input data into two data where the first data will contain original nonzero byte and the second data will contain bit value explaining position of nonzero and zero bytes. Both data then can be compress separately with other data compression algorithm to achieve maximum compression ratio.

Step-by-step of the compression process can be describe as below:

(1) Read input per byte, can be all types of file.
(2) Determine read byte as nonzero or zero byte.
(3) Write nonzero byte into data I and write bit '1' into temporary byte data, or only write bit '0' into temporary byte data for zero input byte.
(4) Repeat step 1-3 until temporary byte data filled with 8 bits of data.
(5) If temporary byte data filled with 8 bit then write the byte value of temporary byte data into data II.
(6) Clear temporary byte data.
(7) Repeat step 1-6 until end of file is reach.
(8) Write combined output data
    (1) Write original input length.
    (2) Write data I.
    (3) Write data II.

Step-by-step of the decompression process can be describe below:

(1) Read original input length.
(2) If was compressed separately, decompress data I and data II (optional).
(3) Read data II per bit.
(4) Determine whether read bit is '0' or '1'.
(5) Write to output, if read bit is '1' then read and write data I to output, if read bit is '0' then write zero byte to output.
(6) Repeat step 2-5 until original input length is reach [9]

IV. RESULTS

A. Analysis For Audio Data

1) Encryption Time for Audio Data

The table given below shows the encryption time consumed by AES and the enhanced AES when audio files of different size are encrypted.

Sr No.	Audio File (KB)	AES (ms)	Enhanced AES (ms)
1	8884	980	955
2	8800	960	940
3	8282	825	800
4	7844	785	765
5	6867	690	675
6	6488	685	650
7	4677	575	556
8	2826	385	360
9	387	90	70
10	33	10	5

Table 1: Encryption Time for Audio Data

2) Bar graph of encryption time

The graph below shows how much time the AES algorithm and the enhanced AES will take in encrypting the audio files of different size.

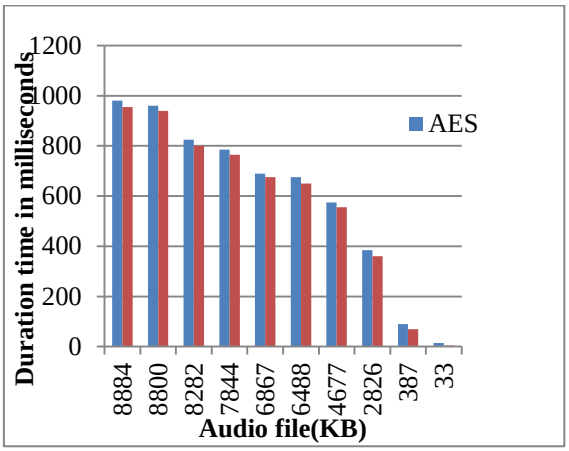

Fig. 3: Comparative status of encryption time amongAES and enhanced AES (audio)

3) Average encryption time for audio data

The table below shows the average encryption time for audio data.

Audio File (KB)	AES (ms)	Enhanced AES (ms)
8884	980	955
8800	960	940
8282	825	800
7844	785	765
6867	690	675
6488	685	650
4677	575	556
2826	385	360
387	90	70
33	10	5
Average time	5985	5776
Throughput	9.29	9.53

Table 2: Average Encryption Time For Audio Data

4) Bar graph of average encryption time

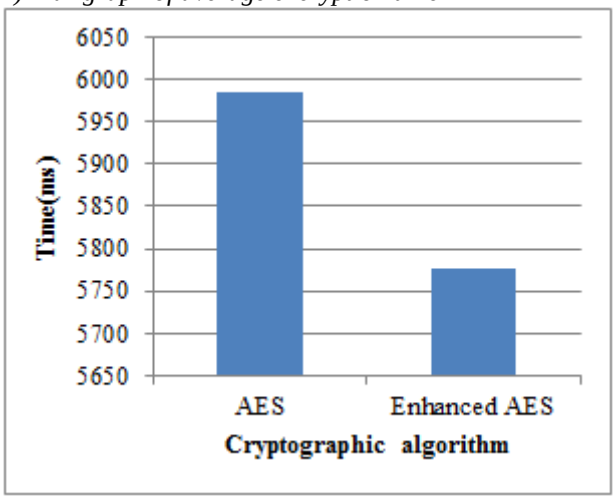

Fig. 4: Average encryption time for audio data

5) Decryption time for audio data

The table given below shows the decryption time consumed by AES and the enhanced AES when audio files of different size are decrypted.

Audio File (KB)	AES (ms)	Enhanced AES (ms)
8884	985	957
8800	967	944
8282	833	805
7844	790	769
6867	697	678
6488	690	655
4677	582	559
2826	390	365
387	100	77
33	15	9

Table 3: Decryption Time For Audio Data

6) Bar graph of decryption time

The graph below shows how much time the AES algorithm and the enhanced AES will take in decrypting the audio files of different size.

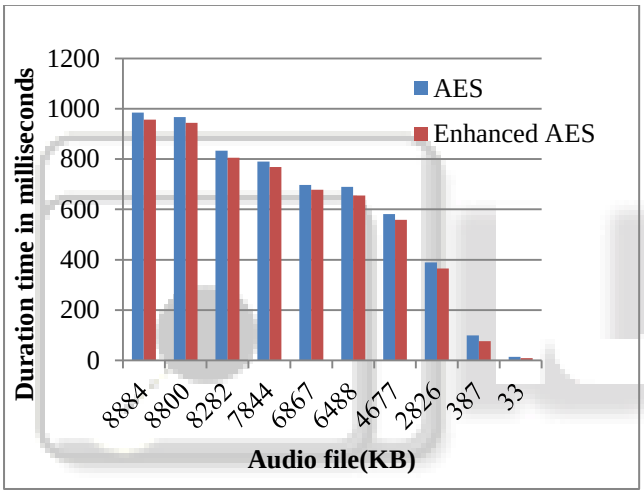

Fig. 5: Comparative status of decryption time among AES and enhanced AES (audio)

7) Average decryption time for audio data

The table below shows the average decryption time for audio data.

Audio File (KB)	AES (ms)	Enhanced AES (ms)
8884	985	957
8800	967	944
8282	833	805
7844	790	769
6867	697	678
6488	690	655
4677	582	559
2826	390	365
387	100	77
33	15	9
Average Time	6049	5818
Throughput	9.10	9.46

Table 4: Average Decryption Time For Audio Data

8) Bar graph of average decryption time

The plot given below shows the bar graph of average decryption time.

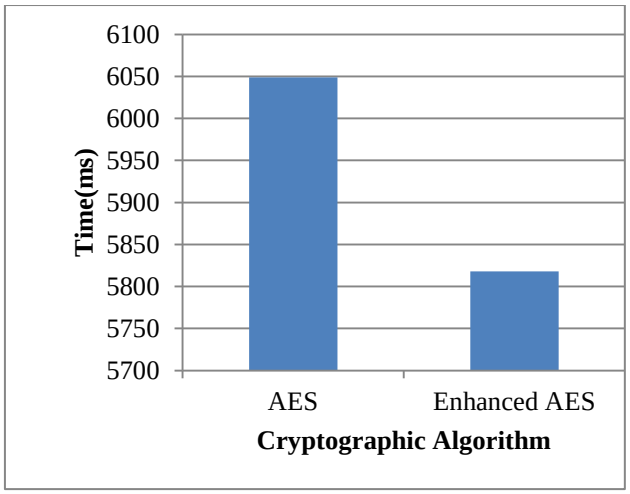

Fig. 6: Average decryption time for audio data

9) Throughput at encryption side (audio):

In the graph below, throughput for encryption side is drawn.

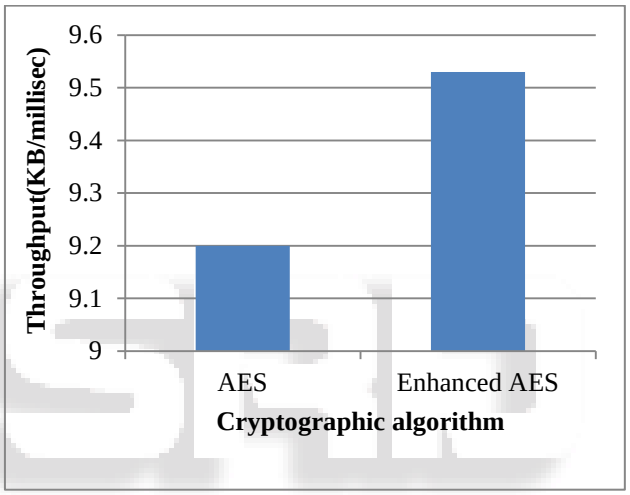

Fig. 7: Comparison of throughput at encryption side (audio)

From the above plot, it is observed that the throughput at encryption end of enhanced AES is more than that of AES algorithm.

10) Throughput at decryption side (audio)

In the graph below, throughput for encryption side is drawn.

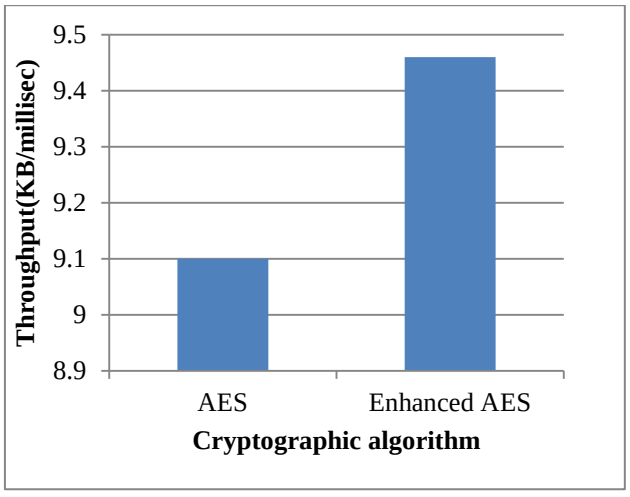

Fig. 8: Comparison of throughput at decryption side (audio)

From the above plot, it is observed that the throughput at decryption end of enhanced AES is more than AES algorithm.

B. Analysis For Video Data

Encryption Time for Video Data: The table given below shows the encryption time consumed by AES and the enhanced AES when video files of different size are encrypted.

Sr No.	Video Files (MB)	AES (ms)	Enhanced AES (ms)
1	1013.76	57828	56700
2	892	42594	41300
3	701	36688	35250
4	372	14703	12980
5	157	6031	5050
6	103	4094	3090
7	89.2	3484	2754
8	54.1	2187	2000
9	16.9	782	601
10	2.74	125	112

Table 5: Encryption Time For Video Data

2) Bar graph of encryption time

The graph below shows how much time the AES algorithm and the enhanced AES will take in encrypting the video files of different size.

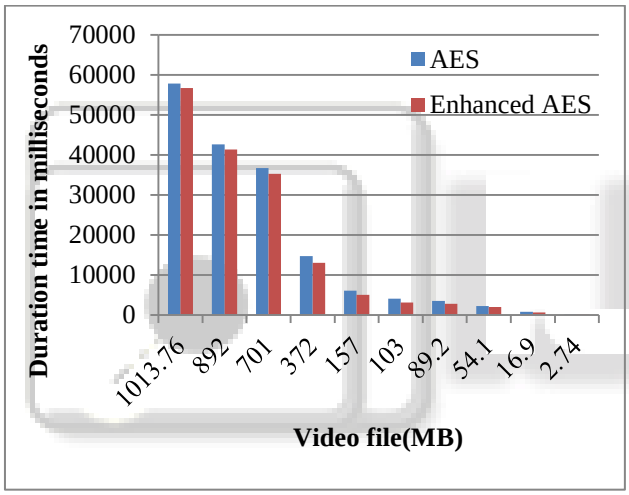

Fig. 9: Comparative status of encryption time among AES and enhanced AES (video)

3) Average encryption time for video data

Video Files (MB)	AES (ms)	Enhanced AES (ms)
1013.76	57828	56700
892	42594	41300
701	36688	35250
372	14703	12980
157	6031	5050
103	4094	3090
89.2	3484	2754
54.1	2187	2000
16.9	782	601
2.74	125	112
Average Time	168471	159837
Throughput(MB/ms)	20.06	21.79

Table 6: Average Encryption Time For Video Data

4) Bar graph of average encryption time

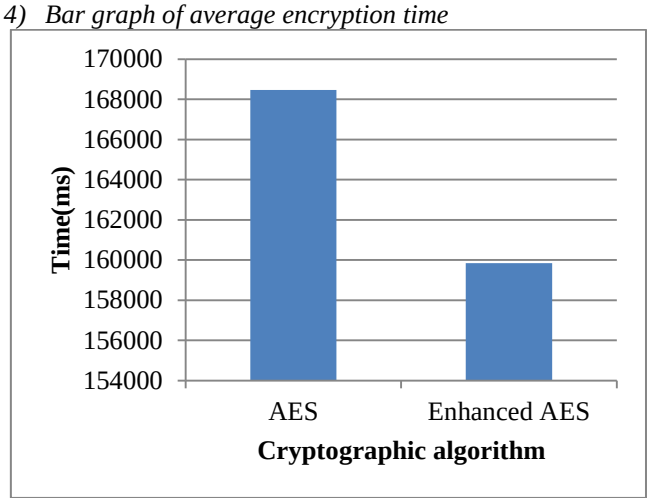

Fig. 10: Average encryption time for video data

5) Decryption time for video data:

The table given below shows the decryption time consumed by AES and the enhanced AES when video files of different size are encrypted.

Sr No.	Video Files (MB)	AES (ms)	Enhanced AES (ms)
1	1013.76	62140	61031
2	892	59859	57900
3	701	33984	32015
4	372	17172	16056
5	157	7297	7176
6	103	4859	4704
7	89.2	4156	4087
8	54.1	2532	2405
9	16.9	828	743
10	2.74	156	138

Table 7: Decryption Tine For Video Data

5) Bar graph of decryption time

The graph below shows how much time the AES algorithm and the enhanced AES will take in decrypting the video files of different size.

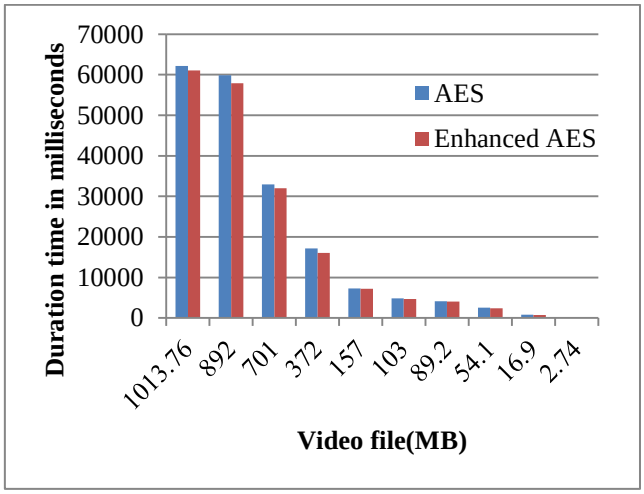

Fig.11: Comparative status of decryption time among AES and enhanced AES (video)

From the above plot, it is observed that the throughput at encryption end of enhanced AES is more than that of AES algorithm.

7) Average decryption time for video data

Video Files (MB)	AES (ms)	Enhanced AES (ms)
1013.76	62140	61031
892	59859	57900
701	33984	32015
372	17172	16056
157	7297	7176
103	4859	4704
89.2	4156	4087
54.1	2532	2405
16.9	828	743
2.74	156	138
Average Time	191983	186255
Throughput(MB/ms)	18.2	18.7

Table 7: Average Decryption Time For Video Data

8) Bar graph of average decryption time

The plot given below shows the bar graph of average decryption time.

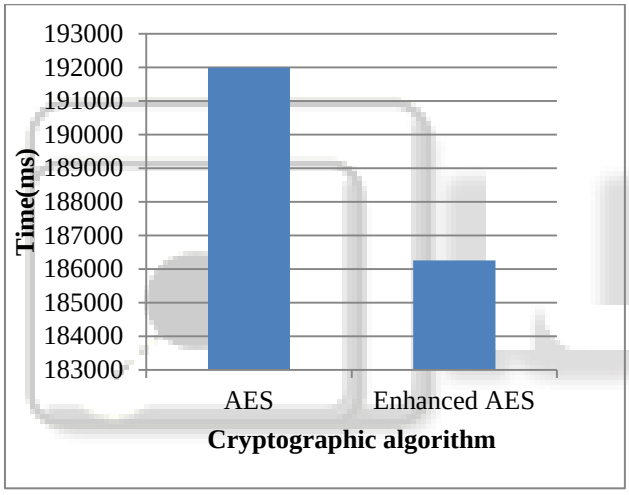

Fig. 12: Average decryption time for video data

9) *Throughput at decryption side (video)*

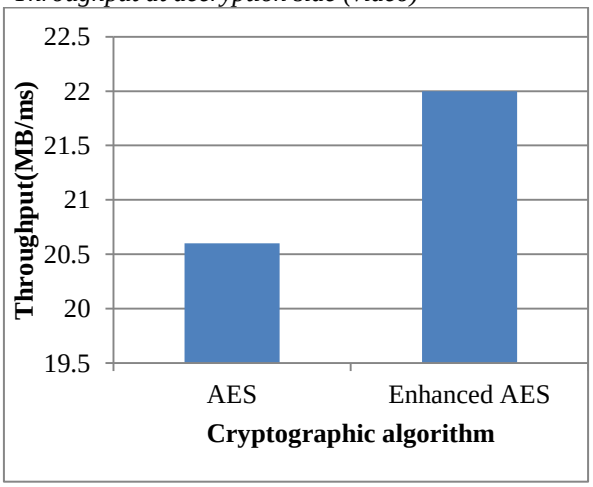

Fig. 13: Comparison of throughput at encryption side (video)

10) Throughput at decryption side (video)

In the graph below, throughput for decryption side is drawn.

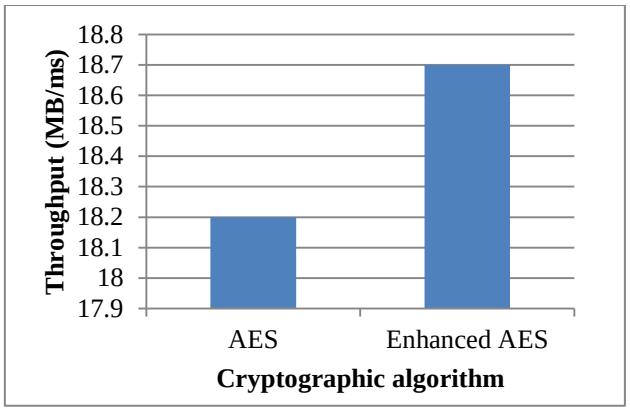

Fig. 14: Comparison of throughput at decryption side (video)

From the above plot, it is observed that the throughput at encryption end of enhanced AES is more than that of AES algorithm.

V. CONCLUSION

The main goal of this thesis is to improve the throughput and security of the AES algorithm with the design of the enhanced AES algorithm and to compress the encrypted data so as to transfer the data fast over the network. This paper presented an enhanced AES algorithm along with a lossless compression technique. Algorithm is implemented for audio and video data. The encrypted data is further compressed by J-Bit Encoding, a lossless compression algorithm. Results shows that the algorithm requires less encryption and decryption time to process audio and video files as compare to conventional AES.The algorithm gives improved throughput than conventional AES.

REFERENCES

[1] Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale, "SMS Encryption Using AES Algorithm on Android", International Journal of Advanced Computer Applications, Vol.50, No.19, July 2012.

[2] 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-April 2012.

[3] M. Anand Kumar, Dr.S.Karthikeyan, "Investing The Efficiency of Blowfish and Rajindael (AES) Algorithms", International Journal of Engineering Research and Applications, Vol.22, No.28, Feburary 2012.

[4] Ritu Pahal, Vikas Kumar, "Efficiencnt Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, No.7, July 2013.

[5] Milind Mathur, Ayush Kesarwani," Comparison between DES , 3DES , RC2 , RC6 , Blowfish and AES ",Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[6] Jawahar Thakur, Nagesh Kumar, "AES, DES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol.1, Issue 2, Dec 2011.

[7] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES And RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.
[8] Bismita Gadanayak, Chittaranjan Pradhan, Utpal Chandra Dey, "Comparative Study of Different Encryption Techniques on MP3 Compression", International Journal of Computer Applications (0975 – 8887) Vol.26, No.3, July 2011.
[9] Agus Dwi Suarjaya, "A New Algorithm for Data Compression Optimization", International Journal of Advanced Computer Science and Applications, Vol.3, No.8, 2012.
[10] Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, "AES Implementation and Performance Evaluation on 8-bit Microcontrollers", International Journal of Computer Science and Information Security, Vol. 6, No.1, 2009.
[11] 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
[12] Swati Paliwal, Ravindra Gupta, "A Review of Some Popular Encryption Techniques", International Journal of Advanced Computer Science and Applications, Vol.3, No.2, Feb 2013.
[13] S.Pavithra and Mrs. E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", Vol.3, No.8, Aug 2012.
[14] E. Thambiraja, 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,Issue7, July2012.
[15] Manpreet Kaur, Ms. Sukhpreet Kaur, " Survey of Various Encryption Techniques for Audio Data", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 5, May 2014.
[16] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, May 2010.

