American Journal of Engineering and Technology Management
2022; 7(3): 59-65
http://www.sciencepublishinggroup.com/j/ajetm
doi: 10.11648/j.ajetm.20220703.13
ISSN: 2575-1948 (Print); ISSN: 2575-1441 (Online)

Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm

Nahom Gebeyehu Zinabu[1], Samuel Asferaw[2]

[1]Department of Computer Science, Unity University, Addis Ababa, Ethiopia

[2]Department of Information Technology, College of Computing, Debre Berhan University, Debre Berhan, Ethiopia

Email address:
gebeyehunigusu@gmail.com (N. G. Zinabu), amannuel2007@gmail.com (N. G. Zinabu), samasferaw@gmail.com (S. Asferaw)

To cite this article:
Nahom Gebeyehu Zinabu, Samuel Asferaw. Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm. *American Journal of Engineering and Technology Management*. Vol. 7, No. 3, 2022, pp. 59-65. doi: 10.11648/j.ajetm.20220703.13

Received: May 4, 2022; **Accepted**: May 30, 2022; **Published**: July 12, 2022

Abstract: Encryption is a method of coding information or sensitive data or asset, to prevent unauthorized users from accessing it. Currently, it is essential to secure data that is at rest in our computer or is transmitted via web against attacks. Several of cryptographic techniques are being used to preserve security and could be classified as: symmetric and asymmetric. A symmetric algorithm named as Advance Encryption Standard (AES) is selected for enhancement due to its applicability and widely used algorithm. In AES, among the four stages that are used for encryption and decryption, Sub Bytes and Mix Column produce more delay. From the two, mix column accounts 60% of the whole delay. To overcome these challenges, in the designed symmetrical cryptography algorithm mix column stage is replaced by bitwise reverse transposition technique. This helps to improve the speed efficiency of the existing Advance Encryption Standard (AES) and Modified Advance Encryption Standard (MAES) algorithm. The simulation result of our Bitwise Reverse Transposition technique resulted in better encryption speed and decryption speed time when compared with original Advance Encryption Standard (AES) and Modified Advance Encryption Standard (MAES): 128.953% and 115.4% encryption and decryption speed performance. This is because of bitwise reverse transposition. Taking average of ten trials; 140.8% increased the throughput because of bitwise reverse transposition. Hence, our proposed Enhanced-Efficiency Advanced Encryption Standard (EE-AES) has better encryption and decryption speed performance and throughput when compared to original Advance Encryption Standard (AES) and Modified Advanced Encryption Standard (MAES).

Keywords: AES, Bitwise Reverse Transposition, Cryptography, Efficiency, Modified AES, Security

1. Introduction

Information security is process or method designed and implemented to secure electronic or other form of confidential personal and sensitive data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Among such methods the dominant technique used today is cryptography. Cryptography is the process of changing plain text into encrypted text and encrypted text back to plain text. Cryptography in most literature is classified into symmetric and asymmetric cryptography [11]. Advanced Encryption Standard (AES) is one of the most popular symmetric cryptography encryption with block cipher structure. It was introduced by Rijndael who is from US National Institutions of Standard and Technology Computation in 2001 [12]. It is a replacement of DES. For data security, AES is the most used encryption algorithm from symmetric cipher. Every round within the secret writing method, contains four operations: Sub Byte, Shift Rows, Mix Column and Add Round Key [10]. The algorithm is capable to use key lengths of 128, 192 and 256 bits and also the range of rounds 10, 12 and 14 severally [10]. Every round has four operations and is repetitious in nature. So, the output of 1st round is input to the second round and performs constant operations with another set of keys. This method continues until the last round reaches. In the last round, there is no mix-column operation [5]. The state array is obtained when the last round is cipher text for transmission. AES has four stages for encrypting and decrypting message. These are: Sub Bytes, Shift Rows, Mix Columns and Add Round Key. Among them, Sub bytes and Mix Columns produce more delay [10, 5]. The execution delay of Mix Columns accounts

for 60% of the total delay [5]. Due to this, AES algorithm is not adopted for IoT, wireless detector networks, low power devices like PDAs. Therefore, cost effective symmetrical data encryption algorism with less power consumption is critical for these environments [8]. Thus, the study focuses on proposing an efficient technique by modifying mix column stages of AES. To overcome these challenges, symmetric key encryption algorism with less power consumption and better security level is necessary especially for small battery capability. Hence, this paper work attempted to answer the following research questions:

1. How can we improve the execution delay of Mix Columns in AES which accounts for 60% of the total delay of AES algorithm's?
2. How can we enhance data encryption efficiency of AES keeping the security level of AES not affected?

2. General Objective

The general objective of this study was Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm by using optimal technique, while not minimizing the protection level of the algorithm.

2.1. Specific Objectives

The specific objectives of this study include:

1. To design data encryption algorithm which enhances data encryption speed of AES algorithm.
2. To evaluate our proposed techniques against data encryption efficiency of AES algorithm.

2.2. Significance of the Study

This study enhances data encryption efficiency of AES algorithm, which would be more important especially for battery scarce devices by replacing the more power consuming stage of mix column of AES by our proposed efficient technique. It also provides new directions for researchers in the future.

3. Organization of the Paper

The rest part of this paper is organized as follows: First literature review and related work for cryptographic algorithms were presented. Next, the proposed technique bitwise reverse transposition for replacement of the mix column is introduced. Then discusses implementation and performance analysis of the proposed technique is presented. Finally, conclusion and future work is discussed.

4. Literature Review

In this section we surveyed related literature and related work about information security, cryptography, symmetric cryptography and AES algorithm. These include concepts of security, cryptography, encryption and decryption of AES. In addition, we included further ideas about related work Modified Advanced Encryption Standard (MAES) which particularly focuses on enhancing data encryption security and efficiency of Advanced Encryption Standard algorithm.

Follow up work on Original Advanced Encryption Standard Algorithm (AES)

Many researchers had conducted a number of researches in the area of cryptography following the arrival of technology; because everything is completed over internet, which results in the upgrading of algorithms using encrypt information or data. Of the various encryption algorithmic, Advanced Encryption Standard (AES) is the most generic algorithm that is used to code messages or information. To collect information on AES algorithm, we tried to refer to a number of journal and conference articles. But, in this paper, we focused on the recent papers which were published between 2015 up to 2019. And from this literature review, we determined three parameters that are necessary within the AES algorithm: efficiency (Encryption time, decryption time) and throughput.

Rahman, A. et al. [2] presented under the title of "a modified version of AES for Resource Constraint Environments." A replacement Substitution Box is proposed which works over the Galois Field (2^4) by constructing a novel affine transformation equation. The result shows that it extends the battery lifetime of low power-driven devices by consuming less amount of energy. However, the speed of the algorithm will not increase significantly due to mix column stage. This is because the execution delay of mix column stage result is 60% of the whole computational time of AES rather than s-box stage of AES [8]. Therefore, this is not convenient with restricted resource and low power-driven devices.

Amina M. et al. [1] focus on the title of "Secure Encryption for Wireless Multimedia Sensors Network". The concept of the approach is predicated on the AES algorithm with shifts rather than the arithmetic operations named the Shift-AES. During this approach, the Mix-Columns method of the AES algorithm is replaced by another shift transformation of columns as follows:

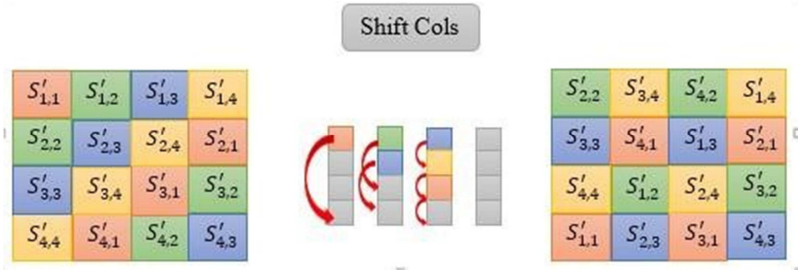

Figure 1. *The Transformation Shift-Cols after the whole processing Sub Byte and Shift Rows of AES.*

The proposed scheme achieves high speed encryption and decryption process specifically for media like image also for plaintext transfer by eliminating the complex process of the mix column. On the other hand, the security level of the algorithm will decrease significantly, because shift column uses similar operation like shift rows stage of AES. Here, the only difference is rows and columns. In AES Shift row stage, there is less security level stage due to its usage of simple operation and linear in nature. Therefore, this will not be good solution for high security requirements [3].

M. Vaidehi et al [4] Focus on "Enhanced Mix Column Design for AES Encryption." In this research work, Structure of Mix Column for AES Encryption has been realized to improve the hardware architecture of AES Encryption algorithm. Reducing the Common Sub-Expression Elimination (CSE) technique has been employed in this analysis work to reduce the hardware structure of mix column design. More technique of increased Inverse Mix Column is employed in decipherment side. The main goal of the analysis work is to cut back the hardware Slices, Lookup Tables (LUTs) and Power consumption of AES encryption architecture. Designed of proposed increased encryption has been designed with the assistance of Verilog Hardware Description Language (Verilog HDL) [4]. The proposed scheme improves the hardware architecture of AES encryption algorithm. It offers 10.93% reduction in Slices, 13.6% reduction in LUTs and 1.19% reduction in delay consumption than the existing Mix Column transformation architecture of AES Encryption. But it focuses on hardware architecture of AES Encryption algorithm rather than reducing execution time through mathematical structure of mix column operations [4].

Rizky Riyaldhia, et al, [8] Focus on "Improvement of advanced encryption standard algorithm with shift row and s-box modification mapping in mix column." The improvement has been made by reducing shift row circular process and S-Box modification for Mix Column transformation. The result showed that improvement on encryption process is 86.143% and decryption process is 13.085%. But, the techniques need to consume bigger memory to store two modified S-Box map and Array Shift Row map. And the approach is not considering security issue of AES.

Mahmoud A. eltatar, et al, [6] focus on "Modified Advanced Encryption Standard Algorithm for Reliable Real-Time Communications". The first goal of the MAES algorithm is to extend the speed of the coding and decoding algorithms. In the MAES design, the Mix Columns stage is replaced with xor operation between the input state and random vector called IV. The mix column stage is the most calculation demanding stage in the AES design and, therefore, it consumes most of the time needed for encryption and decryption. So the modification can increase the speed of the algorithm by replacing the mix column stage with xor operation. On the other hand, the security level of the algorithm will decrease significantly because of the using of the old and part of an in secure algorithm such as DES (FIPS197, 2001). therefore, this will not be good solution for high security requirements [4].

Shasi B. Rana Puneet Kumar (2015) [9] Introduced "parallel computation victimization multicore processors by parallelizing the execution of the algorithmic program in multiple cores/ Moderate Security/." This paper presents the protection and comparison for the data with the AES. Throughout this analysis, it increases the number of rounds (Nr) to sixteen for the coding and decoding method of AES algorithmic, which ends up in further security to the system. The generation of the key has been finished by the help of the Polybius square. Therefore, the protection of the system has been improved. However, with the increase in sort of rounds it is going to take loads of machine time.

Aparna V Sa, c et al [16] In this paper AES encryption and decryption is applied to provide secure communication channel for data transfer. A key length of 128 bit is used for the encryption of text and image inputted. With the help of MATLAB software the whole algorithm is being coded and simulation is shown in the result. The encrypted output (cipher) is in such a way that no unauthorized user can identify the message. The decrypted output is same as of the input and there is no indulgence of distortion. This shows that the AES algorithm is highly efficient as we are able to recover the original message as the output of decryption, without any leakage in data during the transfer. The algorithm has high practical implementation in military field, banking, intelligence and many more. But this paper focused on Implementation of AES Algorithm on Text and Image using MATLAB.

Mustafa Sabah et al [14, 15] In this paper, the major aim is to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were not guarantee that steganography can be used as an alternate to Cryptography as each aspect has its peculiarities. Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages, while Steganography refers to the ways of concealing a secret message into a cover message in a manner that its existence is completely hidden. Using only one of these techniques will render the system vulnerable to the third party. Therefore, the combination of Steganography and Cryptography give more security and robustness.

5. The Proposed Enhanced – Efficiency Advanced Encryption Standard Algorithm

In this section we have proposed Enhanced Efficiency Advanced Encryption Standard (EE-AES) to improve the original AES and MAES algorithms. The proposed algorithm is discussed in the following sections as follows: Figure 2 shows the overall design of AES, MAES and EE-AES algorithm. The figure shows the stage difference between MAES algorithm and AES is in 1st and 3rd stages while the difference between EE-AES is on 3rd stage.

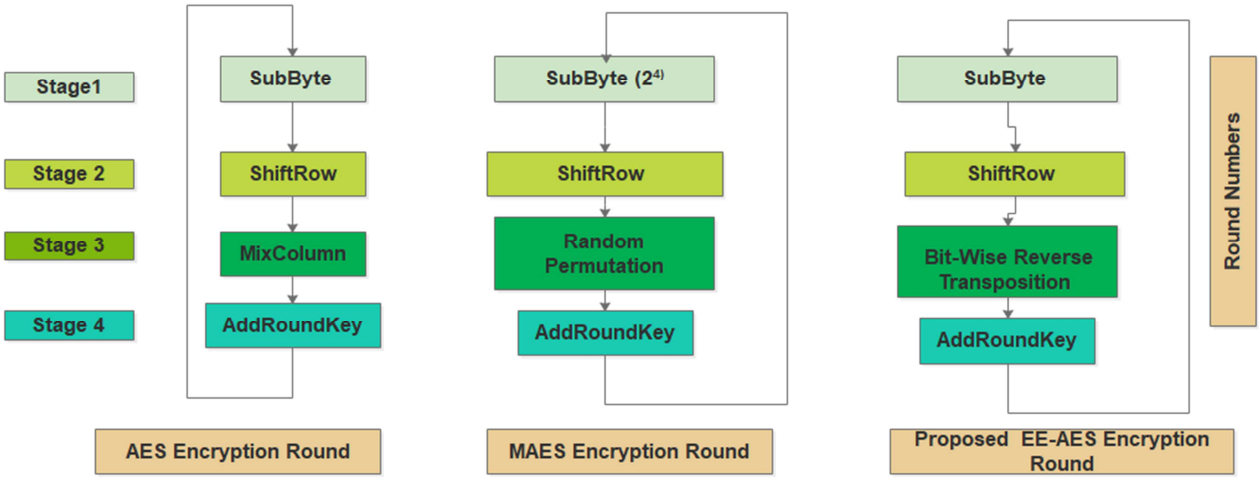

Figure 2. *AES and MAES algorithm compared with our proposed Stage (EE-AES algorithm design).*

5.1. Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm

The primary goal of the proposed EE-AES scheme is to enhances the computational time of the AES and modified AES algorithm. In the proposed EE-AES design, the mix column stage is replaced with a bitwise reverse transposition. This operation decreases the calculation demands of the original design mix column stage of AES with keeping the security level of AES algorithm. Therefore, to improve efficiency of AES algorithm among its 4 stages, mix columns stage is substituted by our new stage called bitwise reverse transposition technique. The proposed diagram of the EE-AES encryption and decryption process with 128-bit design are shown on Figure 4 and Figure 5, respectively.

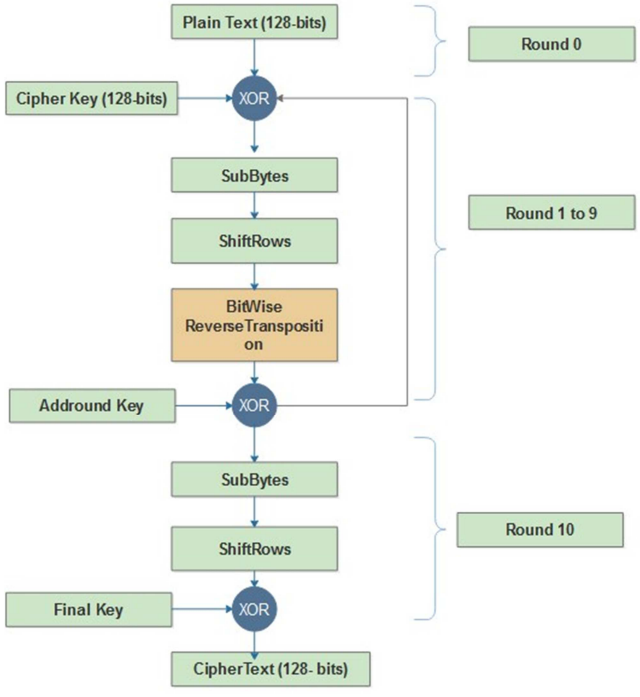

Figure 3. *EE-AES encryption process with 128 bit.*

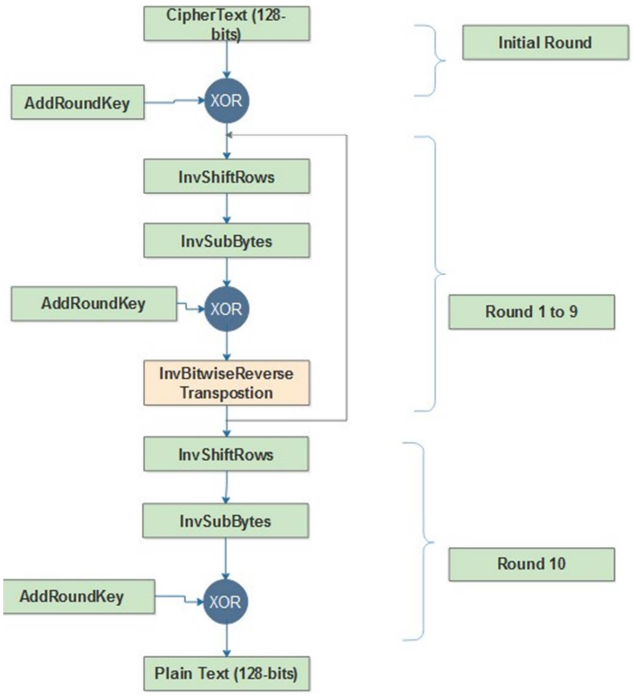

Figure 4. *EE-AES decryption structure of proposed Algorithm.*

5.2. Mathematical Model for Bitwise Reversed Transposition

In this section, we have proposed efficient data encryption technique that can be named as bitwise reversed transposition operation, which enhances data encryption speed of AES algorithm by using bitwise reverse transposition, which remove the complexity of addition and multiplication operations of the current mix column stage of AES. The proposed EE-AES algorithm's, bitwise reversed transposition operation, mathematical model or rules and algorithms of bitwise reverse transposition stage are discussed as follows:

Examples of bitwise reversed transposition string of an array input and output.

00	04	08	0C	00	20	10	C0
01	05	09	0D	80	A0	90	B0
02	06	0A	0E	40	60	50	70
03	07	0B	0F	C0	E0	D0	F0

We use hex (00-09 and 0A-0F) as a result of two hex digit maps to eight binary bits perfectly, rather than writing 00001010, we have to use 0A (10 decimal). We will tell Java to use hex (literals) by beginning with 0x as in 0x0A. As declared before, we must always output 80 (00000001 to 00001000) sifting eight bit.

6. Bit Wise Reverse Transposition Rule

1) Taking the 1st row elements of the input to the 1st column in the output, and then interchanging a_{21} with a_{31} and reverse bit wise in the output.
2) Taking the 2nd row elements of the input to the 3rd column in the output, and then interchanging a_{23} with a_{33} and reverse bit wise in the output.
3) Taking the 3rd row elements of the input to the 2nd column in the output, and then interchanging a_{22} and a_{32} and reverse bit wise in the output.
4) Taking the 4th row elements of the input to the 4th column in the output, and then interchanging a_{24} and a_{34} and reverse bit wise in the output.

This method is not similar to the original AES and MAES design method. It showed easy operation and better efficiency as compared to the existing mix column of AES and MAES method. In this method we take an array as follows:

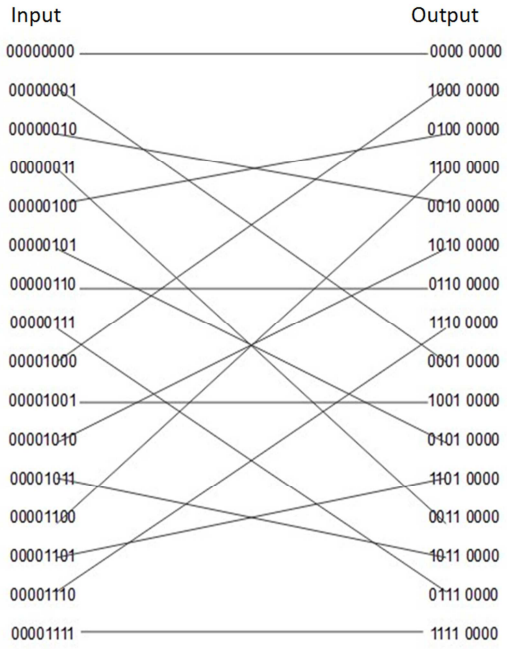

Figure 5. *The Internal structure of bitwise reverse transposition.*

The above diagram shows that almost all the input data are significantly producing confusion in the output.

Algorithm of Bitwise Reverse Transposition Stage

First Accept 4x4 hexa value String Array;
Then convert hexa value to binary;
Next apply reverse order bit wise in byte by byte;
Then convert binary to hexa value;
Finally, Display 4x4 hexa value String array;

or

```
Accept Input I
Get Length of I, L
Declare Input matrix IM
Declare BitRevorder of Input = BR
For (i = 0; I < L; i++)
        Im[i]=GetAscii(I[i]);
        Decimal = get Decimal (Im[i]);
        BR[i] = getBitReverse (decimal);

        Display: IM
                 : BRmatrix
```

7. Implementation and Performance Evaluation

Our proposed algorithm, EE-AES is implemented and compared with original AES algorithm based on the following evaluation metrics: efficiency (Encryption time, decryption time), and throughput. The implementation is conducted using Intel-R, Core-TM i5, CPU 2.7-GHz, 64-bit Processor with 4 GB of RAM. We have implemented these algorithm using NetBeans IDE 8.0.1 software. Input to the algorithm is a block of 128-bit plaintext (data) and a 128-bit key.

7.1. Performance Analyses: Enhanced Efficiency Advanced Encryption Standard (EE-AES) Algorithm

The analysis is based on metrics: Encryption Speed and Decryption Speed. Here the performance of our algorithms are compared with AES and MAES algorithms.

7.2. Encryption Speed

The Encryption time is one of the vital parameter when observing performance of any kind of cipher [13]. Comparison of *Encryption time taking average of 10 trials (*16 byte*)* for AES, MAES and EE-AES algorithms of *10 trials (*16 byte shows in Table 1. bellow. As it is possible to see from table ten trials were taken to test the encryption time of the proposed algorithm.

Table 1. *Encryption time taking average of 10 trials (16 byte).*

Algorithms	Encryption Time Efficiency comparison		
	Encryption Time (sec)	Encryption Time (ms)	%
AES	0.4749	474.9	100%
M-AES	0.3865	386.5	118.5%
EE-AES	0.3374	337.4	128.953%

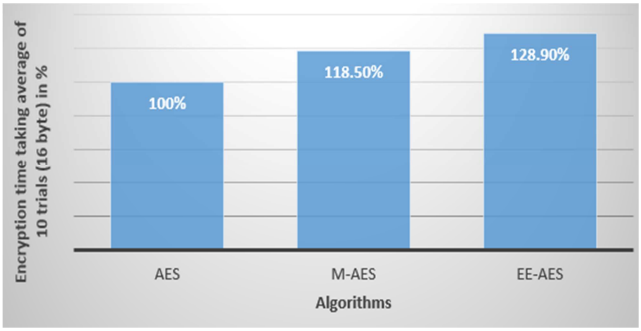

Figure 6. *Encryption time bar graph of taking average of 10 trials (16 byte).*

The above bar graph showed comparison of AES, M-AES and EE-AES algorithms, as we have seen the encryption time, the proposed method (EE-AES) were better performance when compare to the existing AES and MAES.

7.3. Decryption Speed

Decryption time is the time to recover plaintext from cipher text is named decipherment time. The decipherment time is desired to be less almost like encoding time to create system responsive and quick. Decipherment time affects performance of system [10, 7]. In our experiment, we've got measured decipherment time is milliseconds as follows:

Table 2. *Decryption time taking average of 10 trials (16 byte).*

Algorithms	Decryption Time Efficiency comparison		%
	Decryption Time (sec)	Decryption Time (ms)	
AES	27.579	27579.2	100%
EE-AES	4.264	4264.2	15.46

7.4. Throughput

The throughput is outlined as variety of bits which will be encoded and decoded throughout one unit of time. Thus, in variety of equation the throughput is outlined as: [3].

$$THR_{AES}=128/T_{ENC}$$

$$THR_{BWRT}=128/T_{ENC}$$

Where, THR_{AES} is representation of throughput for AES algorithm. THR_{PBWRT} is representation of throughput for proposed bitwise reverse transposition algorithm. T_{ENC} denotes the time taken to cypher the 128-bit block message.

Table 3. *Comparison of throughput at encryption side of AES, EE-AES based on ten trails experimental result.*

Evaluation matrix	AES	EE-AES
Throughput	269.5	379.4
%	100%	140.8%

8. Conclusions and Future Work

To enhance the encryption-decryption performance speed of AES, we have designed EE-AES algorithm. EE-AES algorithm substitutes 3rd stage (mix column) of AES with bitwise reverse transposition. The bitwise reverse transposition resulted in better encryption and decryption speed when compared to the existing mix columns stage of AES and the modified AES algorithm. The experimental result showed 128.953% encryption speed increase by bitwise reverse transposition stage when compared to AES and MAES algorithm.

The outcome of the throughput also increased by 140.8% of bitwise reverse transposition because of bitwise reverse transposition when compared to AES algorithm. From this, we can conclude that the proposed algorithm showed better encryption decryption speed and throughput performance than AES algorithm. As a future work, one can consider testing our algorithm with different bit size and comparing it with most state-of-the-art algorithms. Implementing the algorithm in real environment with different size of text, image and video.

References

[1] Amina Msolli Abdel hamid Helali Haythem Ameur Hassen Maaref. (2017). Secure Encryption for Wireless Multimedia Sensors Network. 18. Retrieved from www.ijacsa.thesai.org

[2] Arnab Rahman Chowdhury, Junayed Mahmud, Abu Raihan Mostofa Kamal, Md. Abdul Hamid, Member. (2018). MAES: Modified Advanced Encryption Standard for Resource Constraint Environments IEEE.

[3] Ayushi Arya et al. (2016). Effective AES Implémentation. International Journal of Electronics and Communication Engineering & Technology, (6-7).

[4] M. Vaidehi and B. Justus Rabi. (2015, December). Enhanced Mix Column Design for AES Encryption ISSN.

[5] Mary James, Deepa S Kumar P. G Scholar (2016, March 03). An Optimized Parallel Mix column and Sub bytes' design in Lightweight Advanced Encryption Standard. International Journal Computational Engineering Research (IJCER) ISSN, (25 – 26).

[6] Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, (2018, JUNE 22). A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention ISSN.

[7] Mustafa Emad Hameed (2018, October 20). Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security. Journal of Telecommunication, Electronic and Computer Engineering. Retrieved from https://www.researchgate.net/publication/323081584, Iraq

[8] Rizky Riyaldhia, et al, (2017., October 13-14). improvement of advanced encryption standard algorithm with shift row. Elsevier B. V. Retrieved from www.sciencedirect.com

[9] Shashi B. Rna, Puneet Kumar, (2015. November 24). Development of modified AES algorithm for data security. Elsevier.

[10] Stallings, W. (2014). Cryptography and Network Security - Principles and Practice. (6th Edn), Upper Saddle River, New Jersey.

[11] Avi Kak, AES: The Advanced Encryption Standard, Avinash Kak, Purdue University, January 31, 2019, page 20-11.

[12] Hasanen S. Abdulah, et al. (2018). Analysis of AES Algorithm Effects on the Diffusion Property. University of Al-Nahrain, Journal / Issue (29).

[13] Dr. N. Suba Rani, et al an Image Encryption & Decryption and Comparison with Text - AES Algorithm International Journal of Scientific & Technology Research Volume 8, Issue 07, July 2019.

[14] Avi Kak (kak@purdue.edu) The Advanced Encryption Standard Algorithm on "Computer and Network Security" May 7, 2020.

[15] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi. School of Co Combination of Steganography and Cryptography: A short Survey 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).

[16] Aparna V Sa, c et al Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Implementation of AES Algorithm on Text And Image using MATLAB Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8 India.