American Journal of Computer Science and Technology
2022; 5(2): 41-48
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220502.13
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Enhanced Security of Advanced Encryption Standard (ES-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 Security of Advanced Encryption Standard (ES-AES) Algorithm. *American Journal of Computer Science and Technology*. Vol. 5, No. 2, 2022, pp. 41-48. doi: 10.11648/j.ajcst.20220502.13

Received: February 9, 2022; **Accepted**: March 16, 2022; **Published**: May 10, 2022

Abstract: Encryption is a method of coding information or any other form of confidential, private and sensitive information or data to prevent from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Now a day, 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 (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. On the other side, Shift Rows stage contribute to less security level of AES because it uses easy operation that is linear in nature. To overcome these challenges, in the designed symmetrical cryptography algorithm shift row stage of AES is replaced by symmetrical transposition technique to advance security. The simulation result of our Symmetrical Transposition technique has shown better security achievement, with greater than 50% avalanche effect, which means the proposed algorithm makes better confusion and diffusion. Hence, our proposed Enhanced Security of Advanced Encryption Standard (ES-AES) algorithm has better security when compared to original Advance Encryption Standard (AES) algorithm.

Keywords: AES, Avalanche Effect, Cryptography, Security, Modified AES, Security, Symmetrical Transposition, Confusion and Diffusion

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 [19]. Among such methods the dominant technique is used today is cryptography. Cryptography is the process of changing plain text in to encrypted text and encrypted text back to plain text. Cryptography in most literature is classified into symmetric and asymmetric cryptography. 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 [4, 5]. It is a replacement of DES. For data security, AES is the most used encryption algorithms from symmetric cipher. Every rounds within the secret writing method contains four operations [1, 3]. Sub Byte, Shift Rows, Mix Column and Add Round Key. 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 [1, 20-22].

Every round has four operations and 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. The state array 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. In AES, among the four stages that are used for encryption and decryption Shift Rows stage contribute to less security level of AES because it uses easy operation that is linear in nature [1, 22]. Thus, the study focuses on proposing a secured technique by modifying shift rows steps

of AES. For information or data security, AES is the most used encryption algorithms from symmetric cipher. In AES each rounds in the encryption process contains four operations as follows: Sub Byte, Shift Rows, Mix Column and Add Round Key [2, 6].

To overcome these challenges, symmetric key encryption algorism with less power consumption and better security level is necessary. Hence, this research work attempted to answer the following research questions:

1) How can we improve the security problem of Shift rows stage in AES algorithm?
2) How can we enhance data security of AES keeping the encryption efficiency level of AES not affected?

This study was Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm by using optimal technique. Specially, to design data encryption algorithm which enhances data encryption security of AES algorithm and evaluate our proposed technique against data encryption security of AES algorithm. This study enhances data encryption security of AES algorithm by replacing the low security level of AES by our proposed technique. It also provides new directions for the researchers in the future. The rest part of this paper is organized as follows: Section II, related works for cryptographic algorithms were presented. Then, the proposed technique symmetrical transposition for replacement of the shift rows is introduced in Section III. Section IV discusses implementation and performance analysis of the proposed techniques. Finally, conclusion and future work is discussed in.

2. Related Works

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 algorithmic that is used to code messages or information [7].

To collect information on AES algorithm, we tried to refer a number of journal and conference articles. But, in this thesis, 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), security (avalanche result, result of diffusion and confusion) of AES, and randomness of the output or mathematical soundness of the AES algorithm and throughput.

According to Rahman, A. et al. [2], it is 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 because the execution delay of mix column stage results is 60% of the whole computational time of AES rather than s-box stage of AES [1]. Therefore, this is not convenient with restricted resource and low power-driven devices.

Amina M. et al. [10] 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 like the follows figure.

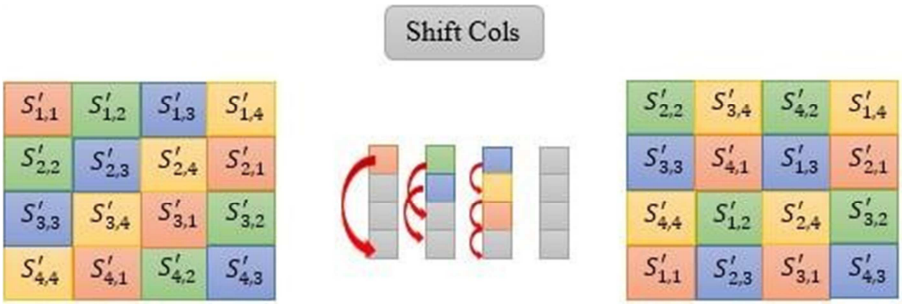

Figure 1. *The Transformation Shift-Cols after the whole processing Sub Byte and Shift Rows of AES.*

The proposed scheme achieves high speed encryption and decryption process specifically for media like image also for plaintext transfer by eliminate the complex process of the mix column. On the other hand, the security level of the algorithm will decrease significantly because the proposed stage-3 use shift column and 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, taking into consideration the powerful computational process for the attackers.

M. Vaidehi et al [11] 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) [11].

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 of mathematical structure of mix column stage operations [11].

Rizky Riyaldhia, et al, [12] 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 reduces 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. [13] 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 consume 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 algorithms such as DES (FIPS197, 2001), therefore this will not be good solution for high security requirements [13].

Shasi B. Rana Puneet Kumar [14] 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 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.

3. The Proposed Methods

In this section we have proposed one algorithm: Enhanced Security Advanced Encryption Standard (ES-AES, to improve the original AES algorithm. the algorithm is discussed in the following sections as follows:

Figure 2 shows the overall design of AES, MAES and ES-AES algorithm. The figure shows the stage difference between MAES algorithm and AES is in 3rd stage while the difference between ES-AES is on 2nd stage.

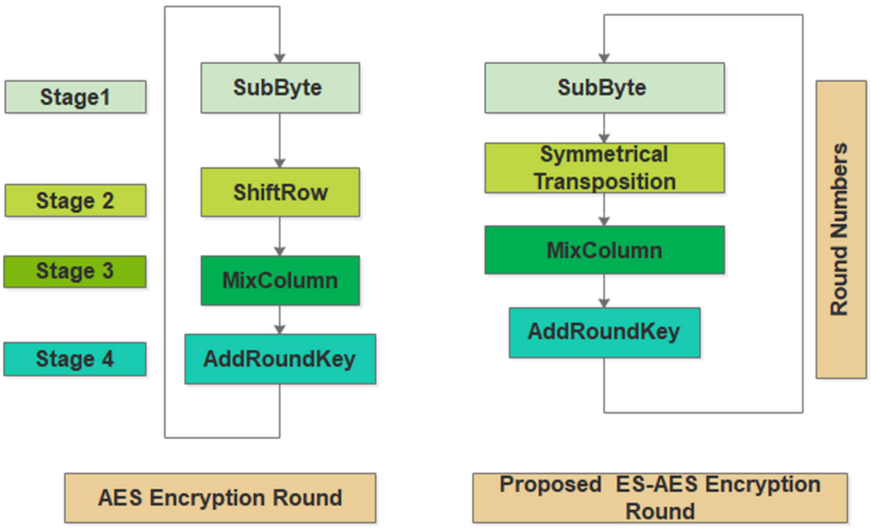

Figure 2. *The AES and ES-AES algorithm design.*

3.1. Enhanced Security Advanced Encryption Standard (ES-AES) Algorithm

To improve security of AES algorithm among its 4 stages, shift rows stage is substituted by our new stage called symmetrical transposition. This block brings a 4×4 matrix of bytes. This block comes into the state array. The state array is changed at every stage of AES. Similarly, the 128bit key is represented also as a matrix of 4×4 bytes. Key expansion

schedule generates a total of 10 rounds this 4×4-byte matrix (in one round we have 4 words or 16 bytes), with pre-round we have a total of forty-four words.

AES supports 3 key length alternatives: 128, 192, or 256 bits and a block length of 128 bits. But, in our proposed algorithm we choose to implement using 128-bits key length. The ES-AES algorithm's encryption and decryption process design with 128 bit are shown in Figure 3 and Figure 4, respectively.

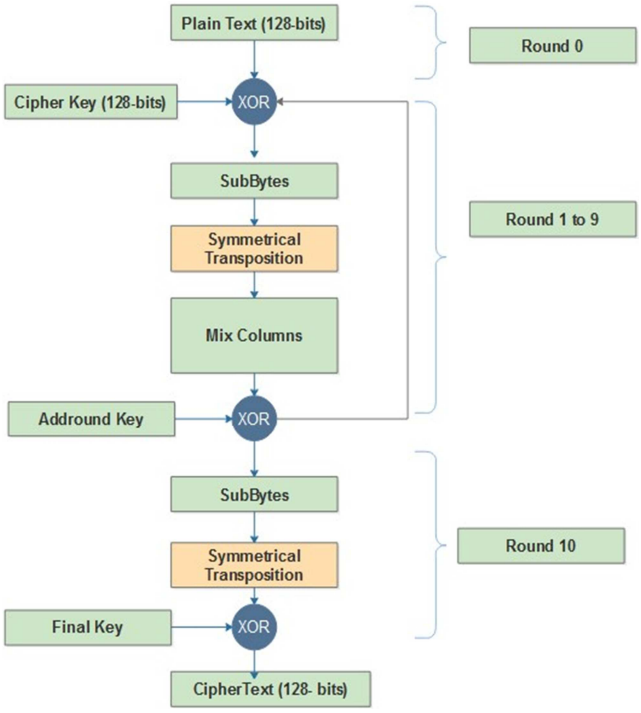

Figure 3. *ES-AES algorithm encryption process with 128 bit.*

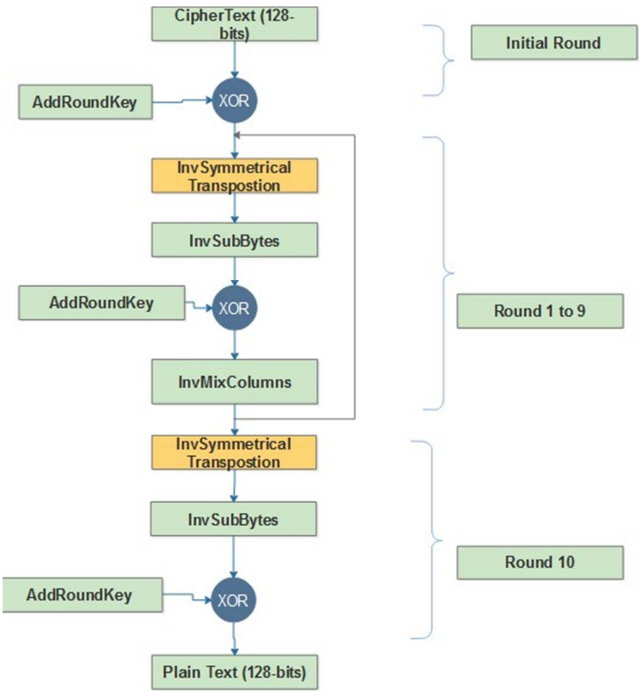

Figure 4. *ES-AES algorithm decryption process with 128 bit.*

3.2. Mathematical Model of Symmetrical Transposition Stage

Symmetrical Transposition Stage which is 2nd stage in the algorithm is substituted in the place of Shift Rows in AES enhances data encryption security of AES algorithm.

3.3. Symmetrical Transposition Rule

1) Interchanging the position of non-main diagonal elements that are symmetrical with respect to the main diagonal elements.
2) Interchanging the position of the main diagonal elements that are symmetrical with respect to the non-main diagonal elements.

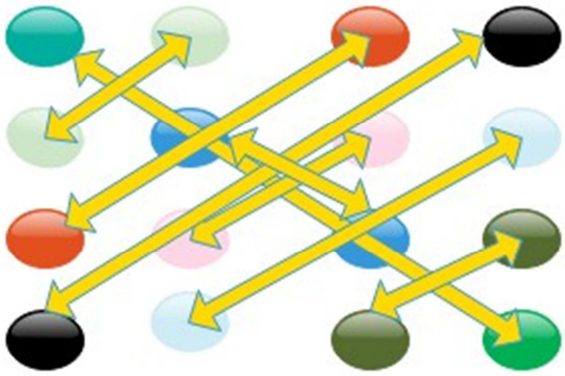

Figure 5. *Symmetrical Transposition Rule.*

3.4. The Internal Structure of Symmetrical Transposition

It showed significant confusion and diffusion in the output compared to the existing shift rows stage of the AES algorithm as shown in Figure 6.

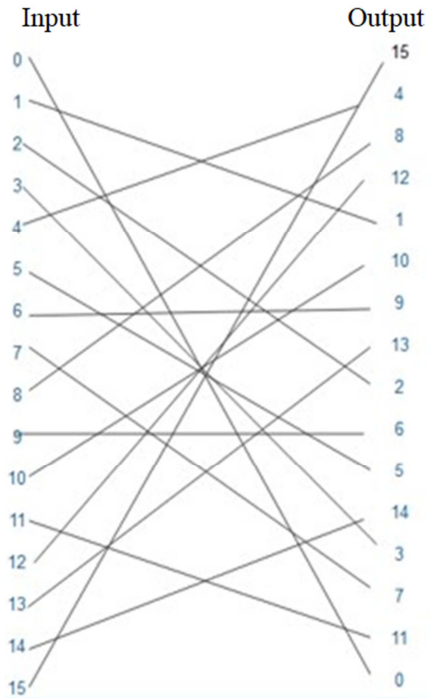

Figure 6. *The Internal Structure of Symmetrical Transposition.*

3.5. Algorithm of Symmetrical Transposition Stage

An algorithm could be a procedure or formula for solving a problem, supported by conducting a sequence of specific actions. A computer program is often viewed as associate degree elaborate algorithmic rule. In mathematics and computer science, associate degree algorithmic rule sometimes suggests that a little procedure that solves a continual downside. Therefore, the proposed algorithm procedure for our symmetrical transposition stage is shown in Algorithm 3.1.

Algorithm 3.1: Symmetrical Transposition Stage Algorithm

First, Accept 4×4 hex value array of matrix;

Next, Swap the position of non-main diagonal elements that are symmetrical with respect to the main diagonal; Then, reversing elements of major diagonal (a_{11} with a_{44} and a_{22} with a_{33}); Finally, display 4×4 hex value array of matrix.

4. Result and Discussion

Our proposed algorithm ES-AES is implemented and compared with original AES algorithms based on the following evaluation metrics: security (avalanche effect, soundness of mathematics, effect of confusion and diffusion and hamming distance) 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 algorithms using NetBeans IDE 8.0.1 software. Input to the algorithm is a block of 128-bit plaintext (data) and a 128-bit key.

4.1. Security Analysis Enhanced Security Advanced Encryption Standard (ES-AES) Algorithm

The security analysis was based on the following evaluation metrics: used are soundness of math, randomness of output, Avalanche effect, effect of diffusion.

To balance the tradeoff between efficiency and security we were working on shift row stage of AES replacing by symmetrical transposition technique. Firs we would like to compared the existing and proposed techniques as follows:

4.2. Comparison of the Existing Shift Rows and Proposed Symmetrical Transposition Based on Randomness of the Output

Example, let the message be considering this values is after Sub Bytes:

41	45	49	4D
42	46	4A	4E
43	47	4B	4F
44	48	4C	50

The same **Input** for existing **ShftRows** and proposed **Symmeteical Transpostion**

41	45	49	4D
46	4A	4E	42
4B	4F	43	47
50	44	48	4C

The **output** of existing **ShftRows**

50	42	43	44
45	4B	47	48
49	4A	46	4C
4D	4E	4F	41

The **output** of proposed **Symmeteical Transpostion**

Figure 7. *Shows identical input of shift rows and symmetrical transposition, however distinction output.*

Shift Row is a circular method that started from second row to fourth row on state key array. Table 1 Shows Degree of Input and Shift Row Output Confusion.

Table 1. *Degree of Input and Shift Row Output Confusion.*

Input	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**4A**	**4B**	**4C**	**4D**	**4E**	**4F**	**50**
Output	41	46	4B	50	45	4A	4F	44	49	4E	4B	48	4D	42	47	4C

Table 1 shows the input value 41 move to output value 41, then input value 42 move to output value 41 and so on. The output of the shift rows shows 75% randomness, which makes less confusion to compare the proposed symmetrical transposition.

Table 2. *Degree of Input and Symmetrical Transposition Output Confusion.*

Index	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**4A**	**4B**	**4C**	**4D**	**4E**	**4F**	**50**
Value	50	45	49	4D	42	4B	4A	4E	43	47	46	4F	44	48	4C	41

Table 2 shows the input value 41 move to output value 50, then input value 42 move to index value 45 and so on.

The output of the proposed symmetrical transposition shows 100% randomness, which makes better confusion. That the proposed methodology shows better randomness of in the output. Is shows better security is achieved [1].

4.3. Avalanche Effect

Avalanche effect, in cryptography, a property referred to as diffusion reflects cryptographically strength of associate degree algorithm. If there is small modification in associate degree input (plaintext or in secret key), the output changes significantly. This is also called avalanche effect. We have measured Avalanche effect using hamming distance. Hamming distance in information theory is measure of dissimilarity. We find hamming distance as sum of bit-by-bit xor (exclusive or) considering ASCII value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche result is desired. Avalanche result reflects

performance of cryptographically algorithm [1, 8, 9].

The avalanche effect formula shows as the follows equation:

$$\text{Avalanche effect\%} = \frac{Number\ of\ flipped\ bits\ in\ cipher\ text}{Number\ of\ total\ bits\ in\ cipher\ text} * 100$$

Where: Number of flipped bits in cipher text is Number of Changed bit in Cipher text.

Number of total bits in cipher text is total Number of block size of the algorithm in the cipher text.

Table 3. *Comparison of avalanche effect of ES-AES and AES algorithms for the same data size (128-bit).*

Index	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50
Value	50	45	49	4D	42	4B	4A	4E	43	47	46	4F	44	48	4C	41

Example: Key: 0123456789012345 for both ES-AES and AES.

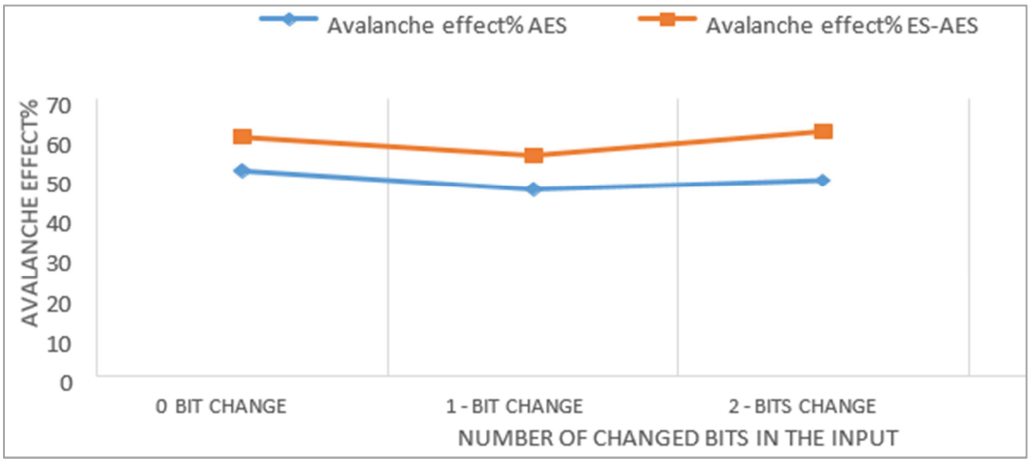

Figure 8. *Comparison of avalanche effect of proposed ES-AES and AES algorithms for the same data size.*

Avalanche effect result is extremely necessary characteristic for coding algorithm. This property seen one bit in plaintext then observance the change within the outcome of a minimum of 1/2 the bits within the cipher text [1]. Hence in the above graph showed ES-AES achieved better avalanche effect compared to AES.

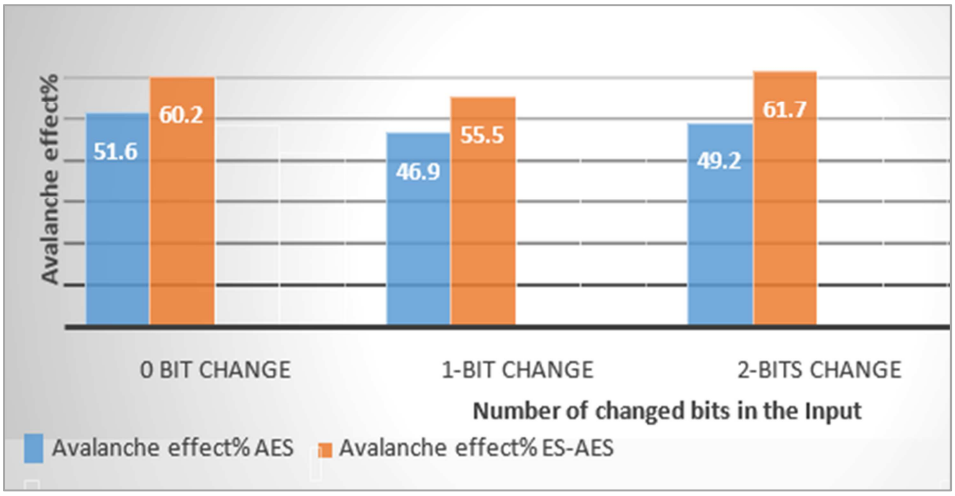

Figure 9. *Comparison of avalanche effect of ES-AES and AES algorithms for the same data size.*

4.4. Analysis of the Existing and Proposed Algorithm Effects on the Diffusion Property

In this section we evaluate of diffusion property of the proposed methods (symmetrical transposition) compared with diffusion of the shift rows of AES. Diffusion property calculated by using Hamming Distance (HD), wherever the HD could be a range of various symbols between 2 strings of equal length [15-18]. In the run time of two previous methods for testing the change in the cipher value and measured hamming distance between input and output for each round. We suggested the message "ABCDEFGHIJKLMNOP" as input for all methods that consist of 16 char which represent a one block and notice the changing. The following Table 4 showed a change in the cipher value and hamming distance for each round in the

shift rows. Table 5 showed a change in the cipher value and hamming distance for each round in the proposed method (symmetrical transposition).

Example 1: Key: 0123456789012345
Plain Text: ABCDEFGHIJKLMNOP

Table 4. *The Cipher Value and Hamming Distance for the Change Shift Rows Operation.*

No, Rounds	The Change Shift Rows Operation.	Hamming Distance
	Cipher text (Hex)	(bits)
1	A3 92 21 F3 8F 10 B6 38 21 F3 21 F3 4D 38 21 BC	69
2	CA 58 F1 EF2C 69 42 21 82 D2 F0 E0 4D E2 B0 09	66
3	39 8B 93 A7 E0 14 D7 FD C3 34 E4 49 E9 22 62CA	60
4	A0 42 FC CD CE F0 32 78 9E 6E D8 8A 10 8C 22BB	65
5	89 B5 10 83 74 E1 86 89 15 C4 D9 26 04 FE AC 94	57
6	43 71 C2 80 5E AC 57 84 6D 33 B1 81 F5 61 B4 F4	59
7	61 36 92 0F4A E2 DA 08 F0 32 66 A0 F7 A8 33 42	60
8	9B 1A CD B6 06 27 F4 F8 82 F8 A3 7916 0D 38 BB	66
9	4A8A D9 2E C7A2 DC 03 90 62 B2 EA 60 CFA4 FA	62
10	B6 F5 CA B0 38 E2 FD 06 C8 67 87 B7 29 6E 80 E8	63

Example 2: Key: 0123456789012345
Plain Text: ABCDEFGHIJKLMNOP.

Table 5. *The Cipher Value and Hamming Distance for the Change Symmetrical Transposition Operation.*

No, Rounds	The Change Symmetrical Transposition	Hamming Distance
	Cipher text (Hex)	(bits)
1	A3 38 21 38 92 8F F3 21 21 10 21 BC F3 B6 F3 4D	71
2	A7 16 66 83 B4 FF 78 AA 05 65 12 F4 B6 15 E2 64	73
3	2F AB 6A 3E 6D CE 2B 95 1E F0 A9 8B E4 27 53 A2	68
4	9A 5C 63 CD 77 C7 D3 E1 9E E9 7D 27 EA C1 DC 4E	66
5	91 39 8F FA FF 4D E8 3A 80 91 D4 BB D3 CE 20 E6	77
6	60 A5 90 39 06 5E B3 70 AE 40 0E D01E CA AF 05	60
7	58 EE 7D 4A 2C 3B EF BD 1A 21 1E 3C 96 23 5A AC	70
8	EA 53 2C 42 63 02 AB 25 2B CB CD B3 6E 9E AF 1D	59
9	BA 42 E9 8C4F BF C0 55 36 D0 B1 34 B7 3F B0 0E	74
10	51 BC 5C 03 EE 56 0C D8 1A 93 5C 79 8F 3A 58 74	65

From the results explained in Table 4 and Table 5, we notice the hamming distance values in Table 5 range from 59 bits to 74 bits, however the hamming distance values in Table 4 are ranged from 57 bits to 71 bits. When shift rows operation changes the position by exchange with sub operation, it caused less diffusion property. Therefore, the sequence of operations the proposed symmetrical transposition shows better diffusion.

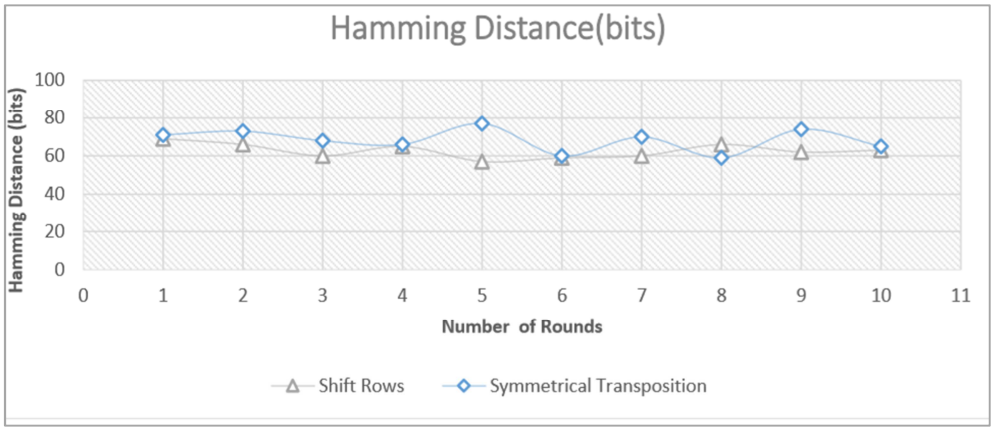

Figure 10. *Analysis of the existing shift rows and proposed symmetrical transposition Algorithm Effects on the Diffusion Property. As we have seen the above line graph, when hamming distance value is increased, the diffusion of bits in cipher text is increased and this makes our algorithm a more secure encryption algorithm.*

5. Conclusions

To enhance the security AES, we have designed ES-AES algorithm. ES-AES algorithm substitutes 2nd stage (shift rows) of AES with symmetrical transposition. The symmetrical transposition showed better security measured in metrics: hamming distance, avalanche effect, diffusion and

randomness of the output compared to the existing shift rows of AES algorithm. For example, it showed that the avalanche effect of our proposed algorithm is greater than 50% when compared to 49.2% avalanche effect of AES.

The outcome of the throughput also increased by 114.3% of Symmetrical transposition. because of symmetrical transposition when compared to AES algorithm. From this we can conclude that the proposed algorithm showed better security 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] 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 (IJCER) ISSN, (25 – 26).

[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] Awad, A. I. (2018, may 16). Introduction to information security foundations and applications. Research Gate, Retrieved from https://www.researchgate.net/publication/325170901.

[4] Alexandra Durcikova Murray E. Jennex. (2017). Introduction to Confidentiality, Integrity, and Availability of Knowledge and Data Minitrack. Hawaii: University of Oklahoma San Diego State University Retrieved from URI: http://hdl.handle.net/10125/41680

[5] Altatar, M. A. (2017, dece). Modified Advanced Encryption Standard Algorithm for Reliable Real-Time Communications.

[6] Amit Verma, Simarpreet Kaur, Bharti Chhabra M. Tech. (2016, Oct). Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish Research Scholar, International Research Journal of Engineering and Technology (IRJET).

[7] Sonia Rani Harpreet Kaur. (2017). Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal.

[8] Mutabaruka, E. (2016). Enhancing Data Security by Using Hybrid Encryption Technique (Advanced Encryption Standard and Rivest Shamir Adleman). Elsever.

[9] Avinash Kak. (2018, February 2). The Advanced Encryption Standard February. Springer.

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

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

[12] 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

[13] 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 Preventio.

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

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

[16] Junjie Yan and Feng. 2016). An Improved AES Key Expansion Algorithm, International Conference on Electrical, Mechanical and Industrial Engineering. ICEMIE.

[17] Pendli, V. Pathuri, M. Yandrathi, S. and Razaque, A. (2016) Improvising performance of Advanced Encryption Standard algorithm. Second International Conf. on Mobile and Secure Services (MobiSecServ). Gainesville, Florida, United States of America.

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

[19] 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.

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

[21] Weiman, D. (2012). Retrieved from http://creativecommons.org/licenses/by-sa/3.0/ASCII Conversion Chart.doc.

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