Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security

Mustafa Emad Hameed[1,2], Masrullizam Mat Ibrahim[1] , Nurulfajar Abd Manap[1]
[1]Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[2]Department of Computer Techniques Engineering, Bilad Al-rafidan University College, Diyala, Baqubah - Baghdad New Road-5, Baqubah, Iraq
mihhh221@gmail.com

***Abstract*—Multimedia data (text, audio, image, animation and video) have been widely used in the past few years for advanced digital content transmission. With the network technology focusing on Internet of Things (IoT) nowadays, the security of the multimedia content has raised researchers' concerns. The exchange of digital data over a network has exposed the multimedia data to various kinds of abuse such as Brute-Force attacks, unauthorized access, and network hacking. Therefore, the system must be safeguarded with an efficient media-aware security framework such as encryption methods that make use of standard symmetric encryption algorithms, which will be responsible for ensuring the security of the multimedia data. For the encryption of electronic data, one of the most prominent cryptographic algorithms is the Advanced Encryption Standard algorithm: A symmetric block cipher that was established by the U.S. National Institute of Standards and Technology (NIST). However, some of the challenges arising from the use of this algorithm are computational overhead, use of a fixed S-Box (which is a point of weakness) and pattern problems, which occur when handling more complex multimedia data such as text, image and video. Many researchers have carried out research aiming at improving the algorithm's performance. This paper summarizes the modifications and benchmarks the performance results of the modified AES algorithms proposed by researchers in the previous studies.**

***Index Terms*— AES; Differential Cryptanalysis; Level of Security; MAES; Time Execution.**

I. INTRODUCTION

Computer and internet technology have undergone rapid and constant evolution over the past few years. Multimedia data (text, images, audio, animation and videos) is now commonly used in many aspects of daily life, including politics, education and commerce. Thus, it is crucial to ensure that this data is secured against brute-force attacks and unauthorized access, particularly for sensitive and important multimedia data. Therefore, with the continuous increase in the use of digital data transmission, multimedia security has become one of the most important aspects of communications [1]. Through the use of various cryptography methods, the multimedia content can be secured prior to its storage or transfer across a network [2].

Cryptography is divided into two broad categories; symmetric key and asymmetric key cryptography. The first category, symmetric key cryptography (otherwise called secret-key cryptography) uses the same key at the source and destination. The second category, asymmetric key cryptography uses different keys (called the public key) at the source and destination [3]. There are two processes in cryptography: The first is the encryption process which entails converting the intelligible data into unintelligible data using a cryptography algorithm and encryption key. The second process is decryption, which involves converting the unintelligible data into intelligible data using the same algorithm and a decryption key. For example, data can be encrypted using a cryptographic algorithm in conjunction with a key management algorithm. It is transmitted in an encrypted state and afterwards decrypted by the intended receiver. However, it is difficult to decipher if a third party intercepted the data. The modern cryptosystem is not dependent on the secrecy of the algorithm but is contingent on the secrecy of the comparatively small fragment of information, referred to as the cryptography key. The fundamental purpose of cryptography is to ensure confidentiality, integrity and availability through the application of encryption methods.

This paper discusses the latest modifications of the Advanced Encryption Standard (AES) algorithm for encrypting multimedia data (such as text, image and video) as was done by researchers in previous studies and used to benchmark their performance results. This paper is organized as follows: a description of the AES algorithm is provided in Section II; a literature review is presented in Section III; the research conducted in this study, on the AES algorithm is discussed in Section IV; a discussion is presented in Section V, and the conclusion is presented in Section VI.

II. ADVANCED ENCRYPTION STANDARD ALGORITHM

The AES algorithm is a symmetric encryption block cipher algorithm established by Joan Daemen and Vincent Rijmen [4]. It is implemented in applications, which require fast processing such as image-video encryption, cellular phones and smart cards. The AES algorithm functions on a 4×4 array of bytes (128 bits) block size referred to as a state. The state is subjected to an encryption or decryption process comprised of four procedures iterated over a particular number of rounds, based on the key length of the AES algorithm, so as to transform the intelligible data into unintelligible data.

Depending on the key size, the algorithm uses 10 rounds of repetitions in the case of 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. The key length is the number of bits in a key used by a cryptographic algorithm. It defines the upper bound of security provided by the algorithm.

Table 1 is comprised of parameters, including the number of rounds, key size and block size along with the key length of the AES algorithm. The 128-bit keys have 10 rounds of iterations with a key size of 4 words (equivalent to 16 bytes) and a block size of 4. The 192-bit keys have 12 rounds of iterations, a key size of 6 words (equivalent to 24 bytes) and with a block size of 4. The 256-bit keys have 14 rounds of iterations, a key size 8 words (equivalent to 32 bytes) and a block size of 4.

Table1
AES Algorithm Parameters

AES Algorithm	**128 Bit**	**192 Bit**	**256 Bit**
Number of rounds	10	12	14
Key size	4	6	8
Block size	4	4	4

Figure 1 shows the encryption and decryption procedures of the Advanced Encryption Standard algorithm. The encryption procedure is applied in the course of four steps: SubByte, ShiftRow, Mixcolumn and AddRoundKey transformations on the state block array in addition to an initial round key. The round function repetition of 10, 12 or 14 rounds depends on the key length. The Mixcolumn step is not applied on the last round. The decryption procedure is carried out in the same four steps used in the encryption procedure.

A brief discussion of the four steps involved in the operation of the AES Algorithm is as follows:

A. Key Expansion

The AES algorithm takes the master key K as a 32-byte (256-bits) key that is used to protect the AES algorithm, and to generate a key schedule using a key expansion routine. The key expansion generates a total of 11 sub-key arrays of 16 words of 8 bits length denoted by *wi*: the first sub-key is the initial key. The sub-key is the same size as the state and is created for each encryption round. The S-Box, which is nonlinear and invertible, is used to perform a one-by-one substitution of a byte value using input from a substitution table.

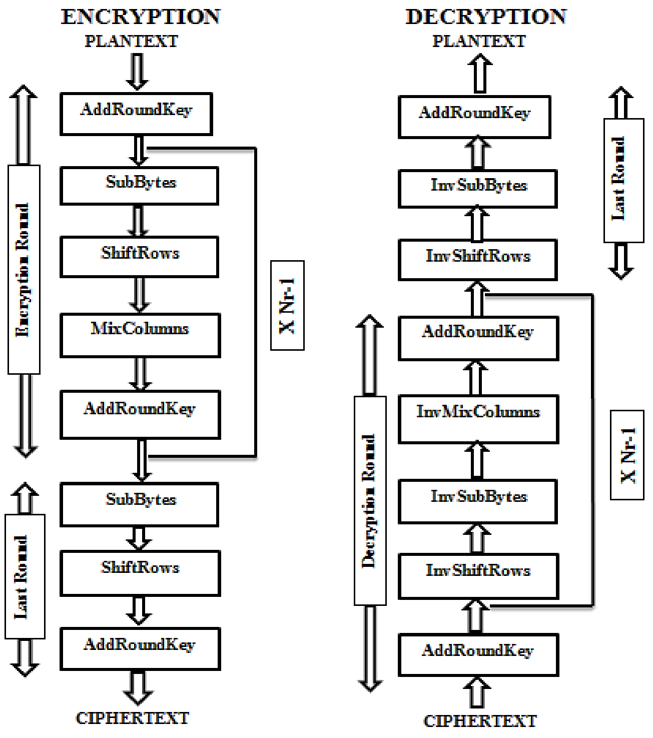


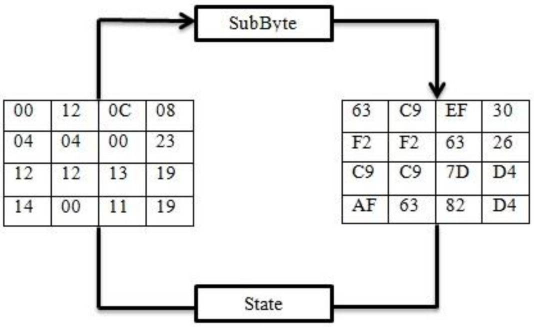
Figure 1. Block diagrams of AES algorithm

B. AddRoundKey

The AddRoundKey transformation uses one of the sub-keys to perform an operation in the state. The operation is a simple XOR between each byte of the state and each byte of the sub-key.

C. SubByte

The SubByte process is a non-linear byte substitution, using a substitution table (S-box), which is organized based on multiplication. Figure 2 shows the SubByte transformation step.



00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	19

63	C9	EF	30
F2	F2	63	26
C9	C9	7D	D4
AF	63	82	D4

Figure 2. Block diagrams for Substitution step

D. ShiftRows

ShiftRow is a process involving the circular shift of the rows of the state with dissimilar numbers of bytes (offsets). The offset is equal to the row index: the first row remains unchanged, the second row is shifted one byte to the left, the third row is shifted two bytes to the left, and the fourth row is shifted three bytes to the left. Figure 3 shows the ShiftRows transformation step.

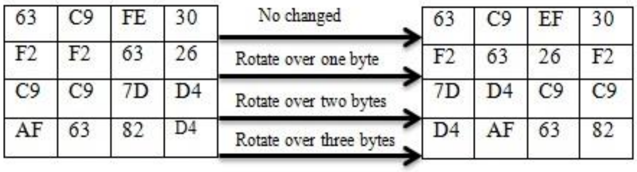


Figure3. Block diagrams for ShiftRows step

E. MixColumns

After the ShiftRows step creates a new column of the state by mixing the four bytes of each column, the MixColumn transformation essentially combines each state column by carrying out matrix multiplication with a fixed square matrix.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \qquad (1)$$

The bytes in the state column and coefficient matrix are construed as two bytes, 8-bit words (or polynomials), wherein the multiplication of bytes is done in GF(2^8) with a with a fixed polynomial *C(x)* given by Equation 2 [5].

$$C(x) = 3X^3 + X^2 + X + 2 \qquad (2)$$

Figure 4 shows the steps of the Mix-column transformation.

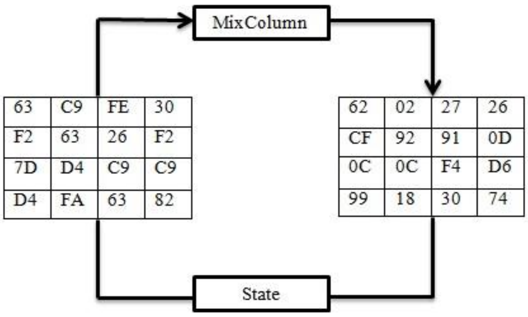


Figure 4. Block diagrams for MixColumn step

The round key is then added to the results of the Mix-column. The final round consists of SubBytes, ShiftRow and AddRoundKey transformations. Same categorizations of steps are applied to the decryption structure, similar to what is applied in the encryption structure. The steps are:

1. Inv-SubBytes
2. Inv-Shiftrows
3. Inv-Mix-Column
4. AddroundKey

A key expansion routine is used to generate a key schedule. The **Inv Mix-Column** reverse operation requires matrix elements similar to the Mix-Column step. If the two constant matrices are inverse of each other, it is easy to prove that the two transformations are inverse of each other.

III. Literature Review

In this study, we found and reviewed around 65 journal and conference articles on the improvement of the AES algorithm over the past years. In this paper, we focus on the papers published between the year 2011 and 2016. Drawn from this literature review, we were able to identify three parameters that are important in the AES algorithm: time execution, differential cryptanalysis and the level of security.

A summary of the cited publication and the proposed methods for improving AES algorithm for multimedia data such as text, image and video are presented in Table 2, 3 and 4 respectively. The 16 studies highlighted included the measures of the differential cryptanalysis, execution time and level of security boasted by the improved AES algorithm as well as the specification of the proposed techniques and data sizes. The differential cryptanalysis was measured on The Unified Average Changing Intensity (UACI) and Number of Pixel Change Rate (NPCR). The execution time depends on the time taken to carry out the encryption and decryption processes. The comparison of the results of the original AES algorithm against those of the modified AES algorithm is also included in the tables.

IV. Discussion

This paper provides a summary of the modification techniques and a benchmark of the resulting performances. The parameters that are involved in the algorithm performance are namely, the time execution, differential cryptanalysis and level of security. However, there is a substantial divergence in the size of the utilized data used in the proposed methods by researchers. Hence, this makes it difficult to compare the proposed works in terms of performance parameters due to these divergences.

A. Execution Time

Execution time is the time duration of the encryption and decryption processes, which serves as a parameter through which the speed of the AES algorithm can be determined. The performance of the encryption and decryption processes can be compared by taking note of the processing times of the original AES algorithm and comparing it with that of the improved algorithm.

Abdulgaber et al. [6] focused on the S-box and the MixColumn step using a different data size which had an execution time of approximately 68% of the original AES algorithm's execution time. Another new approach introduced in [7], interchanged the Mix-Columns transformation with new Henon Chaotic Map using a data size ranging from 3 to 53 frames. This approach boasted decreased execution time compared to the original AES algorithm.

Two other studies presented in [8] and [9] used the same technique of skipping the MixColumn transformation. The drawback is that the skip results in a much large calculation thereby making the encryption algorithm slower.

The study presented in [12] introduced a reduced execution time for the Mix-column transformation, created a new simple S-box, enhanced the key schedule operation and used a modern block schedule operation. The execution time of the modified AES was decreased by approximately 35% of the original AES.

Table 2
Summary of cited publication and proposal methods they are uses improvement AES for text.

Proposed Methods/ Level of Security/ Data Size	**Differential Cryptanalysis**		**Original AES Time Execution**		**Modified AES Time Execution**	
	NPCR (%)	**UACI (%)**	**Encryption**	**Decryption**	**Encryption**	**Decryption**
Introduced parallel computation using multicore processors by parallelizing the execution of the algorithm in multiple cores/ Moderate Security/ (500-4500) MB [19].	-	-	(153-1777) ms	-	(89-401) ms	-
Increased the number of rounds from 10 to 16 rounds for 128-bit key size/ High Security/ (15-412) KB [15].	-	-		-	(23-684) s	-
Used the permutation step and replacement with the Mix-column step/ Low Security/ 16-byte [9].	-	-	(1.925) s	-	(1.874)s	-
The new algorithm for a round key expansion/ High Security/ 16-byte [22].	-	-	-	-	(2.99) s	(5.99) s
Increased the complexity of the encryption process by the creation of a new S-Box / High Security [20].	-	-	-	-	2 (µs) 6 (µs)	3 (µs) 5 (µs)
Defined a new affine transform technique for S-Box operation/ Moderate Security/ (4-10) KB [17].	-	-	(3600-8800) µs	-	(3100-8300) µs	-
Interchanged the Mix-column transformation with the permutation/ Low Security/ (10-90) KB [8].	-	-	(01.96-36.00)s	-	(00.73-17.11)s	-
Used cipher encryption and decryption data with a block size of 512 bits and with a key size of 128 bits/ High Security/ (1-100) KB [16].	-	-	(0.046-4.12) ms	-	(0.031-3.93) ms	-

Table 3
Summary of cited publications and proposed methods used for improved implementation of AES encryption for Images

Proposed Methods/ Level of Security/ Data Size	**Differential Cryptanalysis**		**Original AES Time Execution**		**Modified AES Time Execution**	
	NPCR (%)	**UACI (%)**	**Encryption**	**Decryption**	**Encryption**	**Decryption**
The employment of some cyclic shifting on the S-Box based on the round keys. The replacement of the Mix-Column step with the chaotic system/ High Security/(192-768) KB, (2.2)MB [6].	(99.56-99.61)	(33.47-33.49)	(96.9-1546) s	(118.5-1899) s	(89-401) ms	(31.8-463.6) s
-Created a new simple S-Box and decreased the execution time of the MixColumn transformation. - Enhanced the key schedule operation. -Used modern block ciphers in AES/ High Security / (GS- RGB) Image [12].	-	-	(1.181.28) s (3.43-3.73) s	-	(704-709) s (2.03-2.03) s	-
-Modified ShiftRow transformation. -Modified MixColumn using the reverse of the state matrix before applying the MixColumn transformation. -The Rcon value is continuous but it's formed from an initial key itself. / Moderate Security/ (104-760) KB [10].	-	-	(6.65-19.07) s	-	(4.31-16.35) s	-
- Reduction the number of rounds to one instead of the original ten rounds. - New and simple S-Box -Used modern block ciphers in AES (ECB,CBC,CFB and OFB)/ High Security/ GS Image [13].	-	-	(137-138.4) s	(142.2-145.4) s	1185.8-1286.7) s	(1189.9-1292.4) s
-Enforcement of the Mixcolumn transformation in five rounds as a replacement for the nine rounds as in the original AES-128. - New simple S-box used for the encryption and decryption processes/ Moderate Security/ 16-byte [11].	-	-	-	-	8.56 (ms)	-
Interchanged the Mix-column transformation with the permutation/ Low Secure/ (40-110) KB [8].	-	-	(00.30-02.26)s	-	(00.14-01.22)s	-
Increased number of sequences initiated by an Initial Vector (IV) and an additional key to ensure that each block in the image file is changed. For each round inside a block, the original secret key must be inserted before encryption or decryption [21].			92.8 ms	312.8 ms	944.3 ms	2889.5 ms

Table 4
Summary of cited publication and proposed methods used for improved implementation of AES encryption for Videos

Proposed Methods/ Level of Security/ Data Size	Differential Cryptanalysis		Original AES Time Execution		Modified AES Time Execution	
	NPCR (%)	UACI (%)	Encryption	Decryption	Encryption	Decryption
-Interchanged the Mix-Columns transformation with new Henon Map Chaotic/ High Security / (3-53) frame [7].	(99.62- 99.66)	(33.40-33.52)	(389-492) ms	(1033-1331) ms	(231-287) ms	(305-387) ms
For encryption of MPEG videos, Modified AES applied an efficient and secure way by adjusting the ShiftRow transformation/ Moderate Security/ (1.1-4.4) MB [14].	-	-	(925-2576) ms	(2101-4903) ms	(917-2476) ms	(2011-4923) ms

Wadi et al. [13] proposed another technique by reducing the number of rounds to one instead of ten; the new S-Box and modern block cipher decreased the execution time by about 80% of the initial AES algorithm. By adjusting the ShiftRow transformation [14], this method has been able to decrease the processing time by around 30% of the AES algorithm before modification. Otherwise, research in [15] proposed the increase of the number of rounds from 10 to 16 for the 128-bit key size with the use of 15-412 KB of data. The results showed that the technique expended more execution time for all the file sizes in the encryption process.

In four of the studies presented in [10, 11, 16, 17], the details of the decryption execution time were not provided, but the encryption process time was measured showing a substantial divergence in the size of the data used in the proposed methods. The research in [19] introduced parallel computation using multicore processors for parallelizing the execution of the algorithm in multiple cores for the range of data sizes in 500 to 4500 MB. The value of execution time in parallel computation started with 38% for very small size files up to 45% for large files in comparison to sequential computation. Therefore, it can be seen that the performance of parallel computation is not fixed; it provides less efficiency for small size files and increases proportionately with the file size.

In the two studies [20] and [22], which used different methods to improve the AES algorithm, the effect of these methods on the algorithm cannot be compared because of the differences in the techniques used and the data size of the original AES algorithm. C.-W. Huang et al. [21] proposed the increased number of sequences initiated by an Initial Vector (IV) and an additional key to ensure that each block in the image file is changed. For each round inside a block, the original secret key must be inserted before encryption or decryption. Through the benchmark provided by researchers in some of the articles on the improvement of the AES algorithm [6] [12], it can be seen that the proposed techniques provide better results compared to other proposed techniques.

B. Differential Cryptanalysis

Differential Cryptanalysis is a general form of cryptanalysis which applies primarily to cryptographic hash functions, stream ciphers and block ciphers. In a sense, it is the study of how making a specific change in the plaintext input affects the resultant ciphertext output. The Unified Average Changing Intensity (UACI) and Number of Pixel Change Rate (NPCR) are the most commonly used measures to assess the accuracy and strength of the AES algorithm in resisting differential cryptanalysis before and after improvement for image and video applications [26]. The Unified Average Changing Intensity (UACI) measures the average intensity of differences between the encryption process and the decryption process. UACI is represented by Equation 3:

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}^{N,M} \frac{C1(i,j) - C2(i,j)}{255}\right] \times 100\% \qquad (3)$$

The UACI can be mathematically defined by Equation (3), where symbol M denotes the width of the pixel value compatible with the ciphertext, symbol N denotes the height of the pixels in the ciphertext and subscripts (i,j) denote the pixel value. The Number of Pixel Change Rate (NPCR) means the number of pixels that change in the encryption and decryption processes when only one pixel is changed in the original data. NPCR is given by Equation 4.

$$NPCR = \frac{\sum_{i,j}^{N,M} Diff(i,j)}{M \times N} \times 100\% \qquad (4)$$

The NPCR is mathematically defined by Equation (3), where M and N are the width and height of the pixels and frames respectively. C1(i,j) is the initial cipher and C2(i,j) is the initial cipher changed by some level of pixels and frames.

In the present study, only two works in [6] and [7] calculate NPCR, which is measured using a different technique to interchange the MixColumn state. This indicates that the proposed methods are highly delicate with regard to small changes in the plain image and video application. Therefore, these methods are powerfully accomplished by resisting the differential attack. Only two studies out of those reviewed are concerned with differential cryptanalysis by calculating UACI and NPCR. Other articles concentrate on the expanded level of security and speed of performance of the AES algorithm.

C. Level of Security

The level of security is an essential parameter for examining the proficiency of the AES algorithm. Most of the previous works done proposed approaches for improvement of the level of security of the AES algorithm. In the current study, there are significant variations in the level of security for the improved algorithms. The variation arises due to the different techniques proposed by researchers in these articles techniques as well as the step of the AES algorithm which has been modified. The highest levels of security are shown in the works done in [6, 7, 12, 13, 15, 16, 20, 22] which focused on the steps that affect the security level of the algorithm.

The researchers in [6] and [7] proposed a complex replacement system with a Mix-column step using a chaotic system that applies a Henon chaotic map. However, in the works [12] and [13], they used one of the modern block ciphers (ECB, CBC, CFB and OFB) to enhance the key schedule operation. Another work in [15] proposed an increase in the number of rounds from 10 to 16 for the 128-bit key size in order to make it difficult for the hacker to break the system. For this reason, research presented in [16] used a 512-bit block size with the 128-bit key size, which means that the block size of the initial block was four times larger.

A new approach in [20] and [22] applied the Field Programmable Gate Array (FPGA) for the purposes of enhancing the key expansion and increasing the complexity of the encryption and decryption processes. Otherwise, five of the studies [10, 11, 14, 17, 19] provided a moderate level of security because they focused on other routines in arriving at an improved AES algorithm. A low level of security was presented in two studies [8] and [9], whereby the MixColumn transformation was skipped and replaced with the permutation step, which does not provide improvements in security performance in the AES algorithm.

V. Conclusion

This paper reviews and discusses the latest improvements in the AES algorithm as introduced by researchers around the world between the year 2011 and 2016. The performance parameters discussed in this paper include the processing speed, level of security, and accuracy of the algorithm. Based on this review, there is still room for improvement on the AES algorithm. We found that the maximum data size that can be encrypted using AES cannot exceed 1 GB; therefore, researchers can look into the use of the AES algorithm for encryption big data. The accuracy of the AES algorithm depends on differential cryptanalysis and enhancement of the level of security in the face of future technology, especially the Internet of Things (IoT). Thus, it is valuable to venture into research that proposes a novel approach for improving the performance of the AES algorithm which exhibits high security against Brute-Force attacks, unauthorized access, and network hacking.

Acknowledgment

The authors would like to thank to the Ministry of Higher Education (MOHE) of Malaysia, Mybrain15 and Centre for Telecommunication Research and Innovation (CeTRI), Faculty of Electronic and Computer Engineering (FKEKK), Universiti Teknikal Malaysia Melaka (UTeM) for sponsoring this research study.

References

[1] P. Telagarapu, B. Biswal, and V. S. Guntuku, “Security of image in multimedia applications,” Proc. - 2011 Int. Conf. Energy, Autom. Signal, ICEAS - 2011, pp. 144–148, 2011.

[2] Y. C. Mei and S. Zarina Md Naziri, “The FPGA implementation of multiplicative inverse value of GF(28) generator using Extended Euclid Algorithm (EEA) method for Advanced Encryption Standard (AES) algorithm,” ICCAIE 2011 - 2011 IEEE Conf. Comput. Appl. Ind. Electron., no. Iccaie, pp. 12–15, 2011.

[3] M. S. Reddy and Y. A. Babu, “Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E,” vol. 2, no. 7, pp. 3341–3347, 2013.

[4] R. Concepts, “White Paper AES Encryption and Related Concepts,” pp. 0–4.

[5] S. C. Dhatrika, D. Puvvula, and S. V. Gopal, “A Novel Approach For AES Algorithm In Image Encryption,” vol. 8354, no. 4, pp. 85–92, 2015.

[6] A. Abdulgader, M. Ismail, N. Zainal, and T. Idbeaa, “Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption,” J. Theor. Appl. Inf. Technol., vol. 71, no. 1, pp. 1–12, 2015.

[7] S. Ali Abaas and A. Kareem Shibeeb, “A New Approach for Video Encryption Based on Modified AES Algorithm,” IOSR J. Comput. Eng., vol. 17, no. 3, pp. 2278–661, 2015.

[8] S. Hameed, F. Riaz, R. Moghal, G. Akhtar, A. Ahmed, and A. G. Dar, “Modified Advanced Encryption Standard For Text And Images,” vol. 1, no. 3, pp. 120–129, 2011.

[9] P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, “Modified Advanced Encryption Standard,” Int. J. Soft Comput. Eng., vol. 4, no. 1, pp. 21–23, 2014.

[10] Harleen Kaur, Reena Mehla "Image Encryption Using AES with Modified Transformation" International Journal of Science and Research (IJSR), Volume 3 Issue 7, July 2014,pp.360 – 363.

[11] S. M. Wadi and N. Zainal, "A low-cost implementation of modified advanced encryption standard algorithm using 8085A microprocessor," J. Eng. Sci. Technol., vol. 8, no. 4, pp. 406–415, 2013.

[12] S. M. Wadi and N. Zainal, “High Definition Image Encryption Algorithm Based on AES Modification,” Wirel. Pers. Commun., vol. 79, no. 2, pp. 811–829, 2014.

[13] S. M. Wadi and N. Zainal, “Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption,” Procedia Technol., vol. 11, no. Iceei, pp. 51–56, 2013.

[14] P. Deshmukh, V. Kolhe “Modified AES Based Algorithm for MPEG Video Encryption" International Conference on Information Communication and Embedded Systems (ICICES2014), IEEE.

[15] P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security,” Optik (Stuttg)., vol. 127, no. 4, pp. 2341–2345, 2016.

[16] A. M. Sagheer, S. S. Al-Rawi, and O. A. Dawood, “Proposing of developed advance encryption standard,” Proc. - 4th Int. Conf. Dev. eSystems Eng. DeSE 2011, pp. 197–202, 2011.

[17] O. B. Sahoo, D. K. Kole, and H. Rahaman, “An optimized S-Box for advanced encryption standard (AES) design,” Proc. - 2012 Int. Conf. Adv. Comput. Commun. ICACC 2012, pp. 154–157, 2012.

[18] Hasan M. Azzawi “Enhancing The Encryption Process Of Advanced Encryption Standard (AES) By Using Proposed Algorithm To Generate S-Box” Journal of Engineering and Development, Vol. 18, No.2, March 2014, ISSN 1813- 7822, pp. 89- 105.

[19] V.Pandli, m.Pathuri, S. Yandrathi and A. Razaque “Improvising performance of Advanced Encryption Standard Algorithm”. Mobile andSecure Services (MobiSecServ), Second International ConferenceIEEE, 24 March 2016.

[20] A. A. Abed and A. A. Jawad, “FPGA implementation of a modified advanced encryption standard algorithm,” 2013 Int. Conf. Electr. Commun. Comput. Power, Control Eng. ICECCPCE 2013, pp. 46–51, 2014.

[21] C.-W. Huang, Y.-H. Tu, H.-C. Yeh, S.-H. Liu, and C.-J. Chang, “Image observation on the modified ECB operations in Advanced Encryption Standard,” Inf. Soc. (i-Society), 2011 Int. Conf., pp. 264–269, 2011.

[22] D.Rahul Gandh, V.Kamalakannan, R.Balamurugan and R.Balamurugan "FPGA Implementation of Enhanced Key Expansion Algorithm for AdvancedEncryption Standard" International Conference on Contemporary Computing and Informatics (IC3I),2014, pages 409 – 413.

[23] L. Scripcariu and M. D. Frunză, “Modified Advanced Encryption Standard,” vol. 3, no. 23, pp. 23–26, 2012.

[24] C. Science, “Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent S-Box,” in IEEE, 2015, pp. 44–53.

[25] M. Cretu and C. G. Apostol, “A modified version of Rijndael algorithm implemented to analyze the cyphertexts correlation for switched S-Boxes,” 2012 9th Int. Conf. Commun. COMM 2012 -

Conf. Proc., no. 3, pp. 331–334, 2012.

[26] Y. Wu, S. Member, J. P. Noonan, and L. Member, "NPCR and UACI Randomness Tests for Image Encryption," Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun., pp. 31–38, 2011.