Modified Advanced Encryption Standard algorithm for fast transmitted data protection

Huda H Ali ¹,², Prof. Assist. Dr. Shaimaa H Shaker³
¹ Al- imam Al-Kadhum College (IKC).
² Iraqi Commission for Computer & Informatics-Information, Institute for Postgraduate Studies
³ University of Technology.
Corresponding author’s e-mail address: huda.hamdan33@gmail.com

Abstract
With the exponential growth of digital data exchange over the computer network in recent times, protection of information content is becoming a major concern. There are many security risks, which can easily compromise the data transmitted over the network. Cryptography plays an important role in ensuring the security of digital data transmission over these unsafe networks, so in order to ensure secure and fast data transmitted over the network, an enhanced modification for Advanced Encryption Standard (AES) algorithm is proposed and implemented using additional key generated using linear feedback shift register (LFSR), which provide an efficient technique to pseudo random number generation, also rounds number are decreased. The proposed method give promised result comparing with original AES algorithm result for different data type text, image, and video.

Keyword AES Algorithm, Add around Key, Key, Modification, LFSR, random number

1. Introduction

Network technologies and digital devices are designed to make delivery of digital content fast and simple. Digital data transmission over public networks such as the internet is not secure, however. Methods for protecting digital data, especially sensitive data, are therefore extremely important. There are several ways to protect the data. The skill and science of message keeping is termed cryptography [1]. Encryption is a commonly used technique for maintaining image protection. Image and image encryption technologies include video devices, internet networking, medical imaging and military networking [2]. An application for the Federal Information Processing Standard (FIPS) has begun by the National Institute of Standards and Technology (NIST). This norm should be highly reliable, quick and flexible. This standard will replace that for Data Encryption. The latest standard is called Advanced Encryption Standard (AES) because of the improvement in the Data Encryption standard. Rijndael algorithm selected by NIST, which can be used in Advanced Encryption Standard (AES) [3]. (AES) is a symmetric key algorithm that offers higher security with faster encryption speed and throughput, but the performance is
being improved by modifications, researchers are also attempting to modify this algorithm in order to increase its stability, encryption-decryption time, and to increase the throughput as needed. Any of the modifications are addressed to boost AES [4]. Shtewi et al., presented an Advanced Encryption Standard (MAES) modification definition to reflect a high level of protection and better encryption of the file. The adjustment is performed by changing the phase Shift Row [5]. Abdulazeez & Tahir suggested two architectures: one for 128-bit AES Encryption and the other for 128-bit AES Decryption. Both architectures are built on an iterative framework and modifications such as merging transformation, Look Up tables for decryption, key generation and optimization of each clock cycle to integrate as many operations as possible to increase the output and hardware resources reducing [6]. Zahraa K. Taha, introduced a modification method for AES algorithm where the encryption method consists of the combination of different classical techniques such as techniques for substitution, rearrangement, and encoding transformation. The changes include introducing an arithmetic operation, and using two keys for data protection, the suggestion method for encrypting text (AES-2Keys) makes it more efficient to send text, because it is fast in both software and hardware [1]. Heidilyn et al., proposed Modified AES algorithm that addresses image encryption requirements. In replacement of Mix Columns, the modified algorithm used bit permutation to reduce the algorithm's computational necessity in encrypting images. Study results show that the modified algorithm showed faster time for the encryption and decryption in images [7]. Noor Kareem Jumaa, introduce A random number generator based on Linear Feedback Shift Register (LFSR) had solved the problem of hidden key exchange with the communicated parities. The encryption / decryption with random key generator is based on the Advance Encryption Standard (AES) [2]. While Shabbir Hassan and M. U. Bokhari, show that several cryptographic algorithms based on various technologies have been proposed to protect data from unauthorized users and to achieve a desired level of protection. When designing these cryptographic algorithms, the Linear Feedback Shift Register (LFSR) will play a significant role. Cryptographic algorithms based on LFSR are often lightweight in nature and better suited to resource constraint [8].

2. Methodology

Modify AES algorithm is used to have secure, fast data transmission with distributed system; data may be text file, images, or videos. In the next sections original algorithm details is shown, and then explain the modification steps, which are implemented to this algorithm.

2.1 Original AES algorithm

The AES algorithm is a symmetric cipher block encryption algorithm developed by Joan Daemen and Vincent Rijmen. It is implemented in applications requiring fast processing such as image-video encryption, cellular processing phones and smart cards [3]. The AES algorithm operates on a block size of a 4 set of bytes (128 bits) called a state. The state is subjected to a cycle of encryption or decryption consisting of four
procedures iterated over a certain number of rounds, depending on the key duration of the AES algorithm to turn the intelligible data into unintelligible details [9]. For the case of 128-bit keys, the algorithm uses 10 rounds of repeats, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys, depending on the key size. The key length is the number of bits, which a cryptographic algorithm uses in a key. It determines the security upper bound given by the algorithm [10].

Table.1 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       |

Table .1 contains parameters including round number, key size and block size along with the key length of the AES algorithm. The 128-bit keys have 10 iterations rounds with a key size of four words (equivalent to 16 bytes) and a block size of four. The 192-bit key has 12 iteration cycles, a key size of 6 words (equivalent to 24 bytes) and a block size of 4. The 256-bit buttons [11].

Figure (1) demonstrates the basic algorithm for Advanced Encryption and decryption procedures. In addition to an initial round key, the encryption protocol is performed in 4 steps: Sub Byte, Shift Row, Mix column, and Add Round Key transformations on the state block sequence. The repetition of round function 10, 12 or 14 rounds depends on the length of the key. The stage of the mix column is not stated at the last turn. The decryption method takes place in the same four steps as those used in the encryption process [12].
A simple overview of the four steps involved in the AES Algorithm process will be as follows:

**A. Add Round Key**

The transformation Add Round Key uses one of the sub-keys to execute a state operation. The operation is a simple XOR between each of the state bytes and each of the sub key bytes [9], as shown in figure 2.

![Add Round Key Diagram](image)

**B. byte substitution**

The Sub Byte method is a non-linear byte substitution, using a replacement table (S-box), ordered on the basis of multiplication. Figure 2 indicates a transformation stage for the Sub Byte[10], as shown in figure 3.

![Sub Byte Diagram](image)
C. Shift Rows

Shift Row is a mechanism involving a circular shift with dissimilar byte numbers (offsets) of the state rows. The offset is equal to the index of the row: the first row remains unchanged, the second row moves one byte to the left, the third row moves two bytes to the left and the fourth row moves three bytes to the left. Figure 3 demonstrates the transformation stage at Shift Rows[10], as shown in figure 4.

D. Mix Columns

After the Shift Rows step produces a new state column by combining the four bytes of each column, the Mix Column transformation effectively combines each state column with a fixed square matrix performing multiplication.

Bits in the state column and coefficient matrix are constructed as two bits, 8-bit words (or polynomials), in which bytes are multiplied by GF (28) with a fixed polynomial C(x) given by Equation 1[6]

\[ C(x) = 3x^3 + x^2 + x + 2 \] ......(1)

Figure 5 displays the stages of the Mix-column operation.
Then, the round key is applied to the Mix column tests. The final round consists of transformations to Sub Bytes, Shift Row, and Add Round Key. Same phase categorizations refer to the decryption process, similar to what is used in the encryption framework. The steps are 1. Inv-Sub Bytes 2. Inv-Shift rows 3. Inv-Mix-Column 4. Add round Key

**E. key expansion**

Routine is used to generate a key schedule. In Key Expansion, the AES algorithm uses the master key K as a 32-byte (256-bit) key for protecting the AES algorithm and creating a key schedule using a key expansion routine. The key expansion produces 11 sub-key arrays of 16 8-bit-length words denoted by \( w_i \): the initial key is the first sub-key. The sub-key is the same size as the state and is created for each round of encryption. Using input from a substitution table, the nonlinear and invertible S-Box is used to perform a one-by-one substitution of a Byte value [11].

**2.2 Proposed modification**

In this work the proposed modification of AES algorithm worked to generate another key and decrease number of round to get more fast and secure encryption algorithm, random key is generated using (Linear Feed Back Shift Register LFSR).
2.2.1 Random number generation

The terms "random numbers" are "pseudo random numbers;" because there were no genuinely random series but pseudo random series Numbers. Pseudo Random Numbers Generators (PRNG) are created by multiple internal equations with values. The kind of equations seem to be such that the values appear to be random, and probably even pass several statistical randomness tests. Result analysis Linear Feedback Shift Register (LFSR) is a PRNG. In the various applications such as communication channel, bank protection, etc. random numbers are very useful for producing data encryption keys.so LFSR is used as generators of pseudo-random numbers, pseudo-noise sequences, fast digital counters, and whitening sequences[14][8].

In this work, LFSR is used to generate random 256 keys, which used as second key added randomly to the Original text and original algorithm key (key 1).

2.2.2 Modified AES Algorithm:

the modification of algorithm correlated with additional key generation and add around key step, original step of algorithm is similar ,but the modification is take place as illustrated in the next section ;where:

1- Generate additional key (key2).
   a. Using seed
   b. Using 8-bit LFSR, Matrix of 256 key is generated depending on seed in step.
   c. At each round, generate random number using LFSR, which used for indicating key from key matrix (Key 2).

2- At add round key step, key1, key2 and original text are processed by XOR operation as shown in figure.8

3- Decrease Number of round to halve of original one.

The steps shown in figure 7.

Figure 7. Modification steps
2.2.3 8-Bit LFSR Its Design[7]

8-bit LFSR with maximum length feedback polynomial $X^8 + X^6 + X^5 + X^4 + 1$, that produces $2^8 - 1 = 255$ random outputs. Figure 9 displays circuit of 8-bit LFSR with maximum length feedback polynomial.

![8-bit LFSR circuit][7]

3. Results analysis and discussion

The modified algorithm is implemented to encrypted text, image video data files; the same file is encrypted using the original AES algorithm, the result is compared, comparison results is described on table 2.

Table 2. Result of encryption, decryption execution time

|           | Text file of size 12356 byte | Image of size 80714 byte | Video of size 9087087 byte |
|-----------|-----------------------------|--------------------------|------------------------------|
| Original AES |                              |                          |                              |
| Encryption time | 22 ms                      | 38 ms                    | 15302 ms                     |
| Decryption time | 74 ms                      | 121 ms                   | 48329 ms                     |
| Modified AES |                              |                          |                              |
| Encryption time | 19 ms                      | 26 ms                    | 8447 ms                      |
| Decryption time | 37 ms                      | 64 ms                    | 2261 ms                      |

Table 2. Show that the time needed for encryption and decryption is less in case of using the modified algorithm for text, image and video files. Files size also affected on execution time, note that time execution for video file is relatively longer than the time needed for image or text. At the same, time its clear the difference between the time of modified algorithm and
the original one. Although, the speed of encryption and decryption is very important in transmission, but still the other security criteria for the algorithm must be taken in account, to check and improve that, histogram analysis is done for image with three state (original image, encrypted image by original AES, encrypted image by modified AES). Figure 10. Described this analysis results. Histogram analysis determine randomness of pixels in image, success encryption algorithm histogram for encrypted image must be:- Dissimilar with the original image, Uniform in all pixels value intensity.

From figure 10, it is clear that the encrypted image histogram is different from the histogram and its uniform in all pixel intensity. This prove the great randomness, which appeared in, encrypted image pixels. This means that, this technique ensure strong resist against statistical attacks. National Institute of Standards and Technology (NIST) statistical evolution is done with the results of encrypted files, the test included:

Frequency test, test for frequency within a block, rank, Fourier transformation test, overlapping and non-overlapping matching test, universal test, serial test, cumulative sum, approximate entropy test and other. Figure 11 show the result of test for an image encrypted using modified algorithm, result of test is good where the algorithm pass more of important test standard.
4. Conclusion

Using of LFSR to generate addition key randomly, adding this key in each round at add around key step, make the algorithm more secure, decreasing number of round make the algorithm more fast than the original algorithm, this make the modified algorithm more appropriate to use for protection the data in distributed systems, that need to fast and secure technique to ensure reliability of the system. Security evaluation is improved; the result was very good compared with original algorithm results, this is proved by histogram analysis and NIST statistical test.

5. References

[1] Zahraa K. Taha 2016 Text Encryption using Modified AES-2 Keys, International Journal of Computer Applications (0975 – 8887), Volume 149 – No.4.
[2] Noor Kareem Jumaa 2018 Digital Image Encryption using AES and Random Number Generator, Iraqi Journal of Electrical and Electronic Engineering Volume 14, No. 1 Available at:https://www.researchgate.net/publication/325646196
[3] Kundankumar Rameshwar Saraf, Prof. Kushal Namdeo Mandge, Prof. Pratik Dilip Shah, Prof. Komal Shivaji Mule, Prof. Manishkumar Horilal Patel 2016 Secured Transmission of a Real Time Image and Text using Advanced Encryption Standard for Military Purpose, International Journal of Emerging Trends & Technology in Computer Science (IETTCS), Volume 5, Issue 4, July - August. Web Site: www.ijetcts.org Email: editor@ijetcts.org
[4] Mustafa Emad Hameed, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap 2017 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, Vol. 10 No. 1, p.193-145. 
[5] Shruti Hathwalia, Meenakshi Yadav 2014, Design and Analysis of a 32 Bit Linear Feedback Shift Register Using VHD, Journal of Engineering Research and Applications, Vol. 4, Issue 6 (Version 6), pp.99-102, June. Available at http://www.ijera.com/papers/Volume6/IJERA-Vol4-Issue6-Paper99102.pdf

[6] Abdulazeez, A. M., Tahir, A 2013 Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA, International Journal of Scientific & Engineering Research, 4(9), 1988-1993, ISSN 2229-5518. Available at https://www.ijser.org/paper/Design-and-Implementation-of-Advanced-Encryption-Standard-Security-Algorithm-using-FPGA.html

[7] Heidilyn V. Gamido, Ariel M. Sison, Ruji P. Medina 2018, Implementation of Modified AES as Image Encryption Scheme, Indonesian Journal of Electrical Engineering and Informatics (IJEII) Vol. 6, No. 3, September, pp. 301-308.

[8] Shabbir Hassan, M. U. Bokhari 2019 Design of Pseudo Random Number Generator using Linear Feedback Shift Register, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December.

[9] Shtewi, A.A., Hasan, B. E. M., Hegazy, A. El F. A 2010. An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. International Journal of Computer Science and Network Security (IJCNS), VOL.10 No.2. Available at: https://www.researchgate.net/publication/235692782_An_Efficient_Modified_Advanced_Encryption_Standard_MAES_Adapted_for_Image_Cryptosystems

[10] Ahmad Abdulqadir Alrababah, Muasaad Alrasheedi 2017, Digital Image Encryption Implementations Based On Aes Algorithm, Vawkum Transactions On Computer Sciences, Volume 13, Number 1, May-June.

[11] Kirti Prakash Choudhury, Sangeeta Kakoty 2017, Comparative Analysis of Different Modified Advanced Encryption Standard Algorithms over Conventional Advanced Encryption Standard Algorithm, International Journal of Current Research and Review, Vol 9 • Issue 22 •, DOI: 10.7324/IJCRR.2017.9227

[12] Purushottam Y. Chawke, R.V.Kshirsagar 2014 Design Of 8 And16 Bit LFSR With Maximum Length Feedback Polynomial Using Verilog Hdl, Proceedings Of 13th Irf International Conference, Available at: http://www.digitalxplore.org/up_proc/pdf/91-1406198475105-107.pdf

[13] William Stallings 2011, Cryptography and Network Security Principles and Practices, Prentice Hall, fifth edition.

[14] Application Note 4400 2010, Pseudo Random Number Generation Using Linear Feedback Shift Registers, Maxim Integrated Products, Inc. https://www.maximintegrated.com/en.html