www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18346-18349

Characterization of Advanced Encryption Standard (AES) for Textual and Image data

S. Rehman [1*], S.Q. Hussain [1], W.Gul [2] and Israr [3]

[1] Department of Computer System Engineering,

University of Engineering and technology, Peshawar, Pakistan

[2] Department of Mechanical Engineering,

CECOS University of IT & Emerging Sciences,Peshawar,Pakistan

[3] Department of Electrical Engineering,

University of Engineering and technology, Peshawar, Pakistan

*Corresponding Author: sakhi.uet@gmail.com

Abstract— Safekeeping of multimedia data is an imperious concern for the reason that fast progression of digital data exchanges (DDE) over unsafe network. Multimedia data safety is accomplished by methods of cryptography, which is concerned with encryption of data. Standard symmetric encryption algorithms are responsible to enhance security for the multimedia data. The problem of computational head is always on the way. To overwhelmed that delinquent, we examine the Advanced Encryption Standard (AES) and amend it, to diminish the calculation of algorithm and for enlightening the encryption performance. In this paper, an improved AES algorithm has been investigated. As an alternative of using Mix column we practice with modified step, takes a stable modified step key Mk, and perform expansion routine by using Randal's key schedule to generate a modified step schedule. When the Mk length is 128 bit, then the Expansion generates a total 11 sub Mk arrays of 128 bits, and Xor with state array in every rounds except final round. Hypothetical analysis and experimental results provide evidence that this technique has the capability of high speed as well as fewer overheads on data. Modified-AES algorithm is a quick trivial encryption algorithm for security of multimedia data. All above advantages put together algorithm highly appropriate for the images and plain text transfer as well.

Keywords— Advanced Encryption standard (AES), cryptography, DES, Mk,encryption, multimedia data, symmetric key algorithms.

I. INTRODUCTION

It is a substantial facet to assist the secret multimedia information from unauthorized access. Multimedia incorporates a mix of content, representation and sound and so forth. This sort of interactive multimedia substance is secure by multimedia security approach. This can be accomplished by systems which are essentially in light of cryptography. These sort of systems encourage correspondence security and wellbeing, security and assurance [1].

Large size of images cases a number of challenges for encryption. Normally a typical textual content or visual image features a vast size. Applying standard encryption algorithm will create encryption challenging for any multimedia data, we require such algorithms that need considerably less calculation as a consequences of the substantial size of data [1, 2]. Symmetric key algorithms are less computationally more genuine than any Asymmetric key algorithms. Normally, symmetric key algorithms have a tendency to be thousands times sooner than the ones from asymmetric key algorithms [3]. For this reason the better desirable method to encrypt the multimedia information is definitely symmetric key encryption algorithms to encrypt with symmetric key. One of the methods commonly utilized for low level encryption, to secure any kind of multimedia content is to encrypt that data with Data Encryption Standard (DES). DES, the encryption algorithm is quite perplexed and it involves substantial computations. The DES implementation software package is simply not so fast to process the huge amounts of multimedia generated data [2].

Resulting from hardware implementation AES is incredibly quick symmetric key block algorithm. These kind of method is known as naive method. Applying the naive method on a huge amount of data will take large computation and create the encryption speed slower because of variety of limitations [1].

Specifically, we make it Secure making use symmetric key encryption method such as (AES, DES) by applying on multimedia info as sequence of binary. But regrettably when we apply these techniques on more composite multimedia (mostly images) or when the size of the text data is extremely large, it produces significant computational overhead. I.e. required lots of processing time [1, 2].

The research is referred with enhancing the exiting standards of cryptography Advanced encryption system for images & textual content data encryption and decryption. Additionally it is sloping towards exploiting the huge amount of data, in order to achieve desired speed. This specific edited AES is referred to as a new Modified AES algorithm. Often the modification is done by adding the recon table expanding to thirty six bytes

and operated having shift row values in each round, in order to enlarge often the encryption and decryption effectiveness. The actual modification indisputably increase the effectiveness of encryption and decryption makes the algorithm speedier when compared with exiting one.

This paper is arranged the following. Brief introduction to AES is comprehensive in section II. Proposed technique is clarified in section III. In section IV, experimental result and performance are talked about. The paper is come to the conclusion in section V.

II. ADVANCED ENCRYPTION STANDARD

Joan Daemenand Vicent Rijmen urbanized a block cipher known as Rijnael. In AES the actual span of each block as well as key can be autonomously described to be 128, 192 or even 256. The AES arrangement exploit data associated with 128 bits and exact same three size alternatives [4]. This 128 bit data may be broken into four operations blocks, which are represented as a square matrix of bytes. These operation blocks are usually put into a state array. The state array is organized as a 4X4 matrix [2, 4]. The data is conceded by N rounds N= 10, 12, 14 for encryption. These rounds are performed by the following transformation:

- Transformation of Sub Bytes: within this process 128-bit block is usually replaced with another 128-bit block, for substitution purpose use S-Box [4].
- Transformation of Shift Rows: In this process, we leave the first row of data, perform once left on the second row. Two time shift left on the third row and three time shift left on firth row. It is a simple permutation [4].
- Mix columns Transformation: Is a substitution, the bytes in the columns are linearly combined. The matrix multiplication is performed over the same GF (8) as used in the design of the S-Box.
- Add Round Key Transformation: When working state and scheduled key are XOR with each other, process is called Add Round Key [4, 5].

All four layers expressed above (Including scheduling key) have an analogous converse method [6]. Procedure of encryption, follows more than few ladders. An initial add round key is applied. After this a round function is applied to block. Each block consists of byte sub, shift row, mix columns and add round key transformation. These blocks are repeated N times, depending upon the key length applied [4]. Same sequence of transformation is applied on decryption stricture as which is applied in encryption structure. The transformation i.e. Inverse Sub bytes, Inverse Shift Rows, Inverse Mix Columns, and Add round Key permission the type of key schedules to be matched for encryption and decryption [2, 4]. Here it must be noted that the Mix Columns reverse operation requires matrix elements.

III. METHODOLOGY

Before To overcome the problem of high calculation and computational overhead, we examine the AES and modify it, to reduce the calculation of algorithm and for bettering the encryption performance. So we develop and implement a modified AES base algorithm for text data and images. The basic purpose to modify AES is to provide less computation and improve security for data. The modify algorithm conforms to provide best encryption and decryption speed.

In modified AES the block length and the key length are defined according to the following specification: Four key length alternatives 128, 192, 256, or 512 bits and block length of 128 bits. We presume a key length of 128 bits, which is mostly implemented.

In Modified AES encryption and decryption process differ to that of AES, in account of number of rounds and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mix column step and add Modified step. Mix Column gives better security but it takes large calculation that makes the encryption algorithm slow. The other three steps remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithm. This block is a 4x4 square matrix consisting of bytes. This block is copied into state array. The state array is modified at each stage of encryption of decryption. Similarly the 128-bit key is also depicted into a square matrix.

The 128-bit key is uttered into an array of key schedule words: each word is of four bytes. The total key schedule words for ten rounds are 44 words; each round key is similar to one state. The block diagram of the Modified AES Algorithm with 128 bits data is shown below.

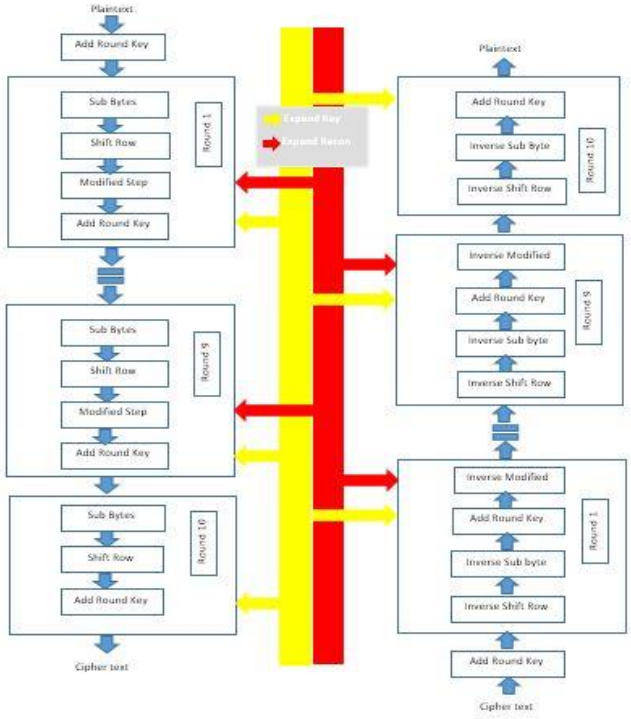


Fig.1 Modified Advanced Encryption System

A. Round of Modified AES Algorithm

Length of the input output block and the state is 128-bit for Advance Encryption System. This is symbolized by Nb = 4, which reflects the number of 32-bit words in the state. For the AES Algorithm 128, 192, 256, or 512 bits is the length of the Cipher key. The key length of the block is denoted by Nk and its value is 4, 6, 8, or 16. This value reflects the number of 32-bit words in the Cipher Key.

Table 1: Key Block Round Combination

Algorithm	Block Size (Nb words)	Key length (Nk words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14
AES-512	4	16	22

For the algorithm, throughout the execution of algorithm the numbers of rounds to be executed are dependent on the key size. Nr is used to represent the number of rounds. The combination of Key block Round that conform to this standard are shown in table 1 above.

Algorithm uses a round function for both its Cipher and Inverse Cipher. This function is composed of four different byte oriented transformation: byte substitution using a substitution table (S-box), shift rows using shift rows function, bit-wise adding a specified data to the state array, adding round key to the state. No of round keys generated by key expansion algorithm.

There are 10 rounds of AES-128 for full encryption or decryption. The four different stages that we for Modified AES Algorithm are:

- Substitution
- Shift Rows
- Modified Step
- Add round Key

Substitution Bytes, Shift Rows and Add Round Key remain unaffected as it in the AES. Here the important function is Modified step which is used instead of Mixcolumn.

These rounds are managed by the following the conversions shown in fig.1

Modified Step Key (Mk) expansion for AES-128 using Rajindael Key Scheduling

The expanded Mk can be seen as an array of 32-bit words (columns), numbered from 0 to 43. The first four columns are filed with the given Modified step key. Words in position that are multiple of 4 (M4, M8… M40) are calculated by:

Applying the bit shift and sub bytes transformation to the previous word Mi-1.

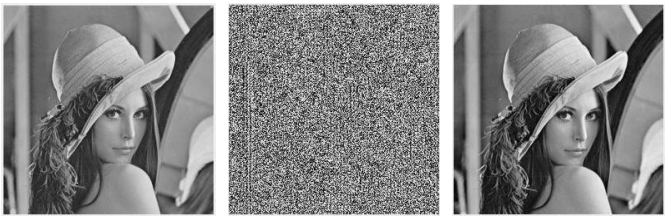
Adding (XOR) this result to the word 4 position earlier Mi-4, plus a round constant Rcon.

The remaining 32-bit word Mi, are calculated by adding (XOR) the previous word Mi-1, with the word 4 position earlier Mi-4.

The AES algorithm takes a fixed modified step key Mk, and perform expansion routine by using Rindael's key schedule to generate a modified step key schedule. When the Mk length is 128 bit, then the Expansion generates a total 11 sub Mk arrays of 128 bits, denoted Mi and the first Mk is the initial Key. We need previous sub keys, two tables, RCon and S Box to generate the Mk Key for Modified steps.

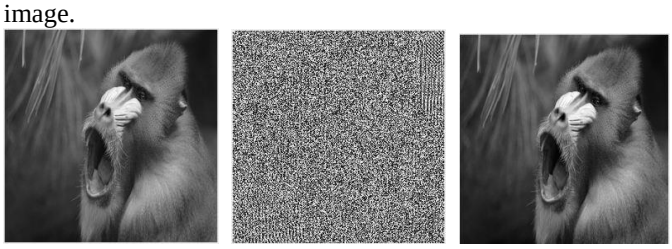
IV. EXPERIMENTAL RESULT AND PERFORMANCE

Results of some experimentations are given to evaluate its efficiency of algorithm to digital images. We use various images as the original images. The encrypted images are portrayed in fig.2a1-3b1. As shown, the particular encrypted images regions are totally invisible. The decrypted images are shown in fig.2a2-3b2. The visual assessment of figs.2-3 show the possibility of applying the proposed Modified AES successfully in both encryption and decryption. Also its tells its effectiveness inside hiding the information contained in these.



a) Original *a1) Encrypted* *a2) Decrypted*

Fig.2 Application of Modified AES to Lena Plain/Cipher image.



b) Original *b1) Encrypted* *b2) Decrypted*

Fig.3 Application of Modified AES to Baboon Plain/Cipher image.

Apart from security considerations, some other problems for image cryptosystem algorithm are also essential. This includes typically the running speed, particularly for real time internet multimedia application. Some experimental tests are given to show the efficiency of our scheme. A listed image of "Baboon" is used as a plain image and encryption of this image is show in fig 3. The personal computer used in all programs and test was Intel Core (TM) i3 CPU M370 @2.4GHz with 3.00GB of memory and 500GB hard disk capacity. Table.2 shows performance of AES and Modified AES encryption on 256, 512 and 1024 gray scale image of different sizes, kept at the same word size w=32 , number of round r=22 and secret key length b=16 and kept at CBC mode of operation.

Table.2 Performance of Modified AES and Original AES

Image size in pixels	Image size on disk	Encryption time in Seconds with AES	Encryption time in seconds with Modified AES
256x256	86KB	8.60	5.45
512x512	462KB	32.05	19.15
1024x1024	462KB	99.26	73.46

V. CONCLUSION

In this paper a modified version of AES is proposed. The modification is done by replacing the mix column step with modified step. The proposed algorithm does not require any additional operations rather than the original AES. We have shown that Modified AES gives better encryption and decryption results in term of Run time efficiency.

REFERENCES

1. Shtewi, A.M., *"An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems"*. IJCSNS International Journal of

Computer Science and Network Security, 2010. Vol.10 No.2(226-232).

2. Engel, D., T. Stutz, and A. Uhl, *A survey on JPEG2000 encryption.* Multimedia Systems, 2009. 15(4): p. 243-270.
3. Bin Muhaya, F., M. Usama, and M.K. Khan, *Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption*, in *Emerging Intelligent Computing Technology and Applications, Proceedings*, D.S. Huang, et al., Editors. 2009. p. 1014-1024.
4. Krishnamurthy G N, V.R., *"Making AES Stronger: AES with Key Dependent S-Box"*. IJCSNS International Journal of Computer Science and Network Security, Septamber 2008. VOL.8(NO.9): p. pp 388-398.
5. Phillips, P.J., et al., *The FERET Evaluation Methodology for Face-Recognition Algorithms.* IEEE Trans. Pattern Anal. Mach. Intell., 2000. 22(10): p. 1090-1104.
6. P.Noo-intara, S.C., and S.Choomchuay, *"Architectures for MixColumn Transform for the AES"*. Department of Electronics, Faculty of Engineering, and Research Center for Communications and Information Technology (ReCCIT) King Mongkut's Institute of Technology Ladkrabang (KMITL): Bangkok 10520, Thailand.