An Improved AES Cryptosystem Based Genetic Method on S-Box, With, 256 Key Sizes and 14-Rounds

Ashutosh Pandey[1], Umesh kumar Lilhore[2]

[1]*M.Tech Scholar, Dept. of CSE, NIIST Bhopal, India*
[2]*NIIST Bhopal, A.P Dept. of CSE, NIIST Bhopal, India*

Abstract— *Cryptography methods are widely use in digital communication for secure data transaction. Cryptography methods have two categories symmetric and asymmetric. Both types of encrypting have their own importance and limitations. In Symmetric key based encryption same key is use for encryption and decryption process. One of the most popular and widely used symmetric encryption methods is (AES) Advance encryption standard, which attracts researchers to develop more efficient AES cryptosystem. In this research work we are presenting an improved AES encryption method "IAES". Proposed IAES method uses a modified S-Box by employing Genetic algorithm (GA) with key size of 256 bit. In proposed method IAES, GA will be used in the S-box to perform various pipelined operations such as substitution, shifting of rows, mixing of column and to perform Add Round Key in the AES rounds. In this work proposed IAES and existing AES method both are implemented over MATLAB simulator and various comparison parameters such as encryption time, speed and decryption time and speed are calculated. The high level of system integration along with high speed and high throughput makes the proposed IAES based cryptosystem a perfect choice for a spread of application.*

Keywords— Cryptography, Symmetric, AES, S-box, S-box, Genetic Algorithm.

I. INTRODUCTION

In today's scenario people shares data and information to each other by using of network due to this more amount of information are so much private but some are less private due to this the attacker or the hackers are taking advantage and they are attempting to steal the information to overcome various used since 2001 since it provides high level of security and can be implementation easily [1,6]. With the introduction and revolution in communications, one more change that affected security is the introduction of distributed systems which requires carrying of data between terminal user and a set of computers.

Secret Key
Key Distribution
Secret Key
Secured Communication
Data in
Encrypt
Decrypt
Data out

Figure 1.1: Cryptography

Network security measures are needed to protect data during their transmission. The mechanisms used to meet the requirements like authentication and confidentiality are observed to be quite complex. Cryptography is the science of information and communication security. Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users [5].

II. AES ENCRYPTION

The Advanced Encryption Standard, in the following referenced as AES, is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power.

The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits. While AES supports only block sizes of 128 bits and key sizes of 128, 192 and 256 bits, the original Rijndael supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits.

2.1 AES APPLICATION-AES have following applications [22].

- **A)** Design of hardware and software-In various designing of H/w and S/w AES used.
- **B)** Design of processor-Various processor are based on AES method
- **C)** In basic encryption and decryption process-Various data security use AES encryption.
- **D)** Application archive and compression tools Like Rar and WinZip
- **E)** File encryption and disk or partition Encryption
- **F)** Security for communications in LAN IEEE 802.11i-2004, or 802.11i wireless networks
- **G)** Provides confidentiality and authentication For IPSec protocol
- **H)** SPN substitution -permutation networks uses the stages and rounds in AES.

III. GENETIC ALGORITHM-

A genetic algorithm is a randomized search that has proven to be reliable and powerful optimization technique which follows the principle of natural selection. It can be applied to both texts and images. Genetic algorithm is secure, since it does not utilize the natural numbers directly. The results obtained for generating keys using genetic algorithm should be good in terms of coefficient of autocorrelation [2].

The basic genetic algorithm operators are discussed as follows-

- **Selection-** It is the process of choosing the chromosomes from the initial population generated by function based on fitness value.
- **Crossover-** This operator combines the chromosome of one generation with another to reproduce a new set of values. Single point crossover, two point crossover and uniform crossover are the three types of crossover operators in GA.
- **Mutation-** This provides a genetic diversity of a chromosome in one generation. The chromosomes are flipped and a new chromosome is generated for a new generation.

IV. PROBLEM STATEMENT-

Cryptography methods are widely use in digital communication for secure data transaction. Cryptography methods have two categories symmetric and asymmetric. Both types of encrypting have their own importance and limitations. In Symmetric key based encryption same key is use for encryption and decryption process. One of the most popular and widely used symmetric encryption methods is (AES) Advance encryption standard, which attracts researchers to develop more efficient AES cryptosystem. In this research work we are presenting an improved AES encryption method “IAES”.

The key challenges in AES algorithm are-

1. High encryption time- Existing AES have high encryption time.

2. High the decryption time- Existing AES have high decryption time.

3. Slow Encryption Speed- Existing AES have low encryption speed.

4. Slow Decryption Speed- Existing AES have low decryption time.

5. Avalanche Effect- Existing AES have poor avalanche effect.

V. PROPOSED IAES METHOD-

Proposed IAES method uses a modified S-Box and P- Box by employing Genetic algorithm (GA) with key size of 256 bit. In this proposed method IAES, GA will be used in the S-box to perform various operations such as substitution, shifting of rows, mixing of column and to perform Add Round Key in the AES rounds.

An enhanced AES implemented using evolutionary approach is expected to improve the performance of the AES which are mentioned above.AES is a symmetrical block cipher which uses Substitution box (S-box) and Permutation box (S-box) for the process of encryption and decryption. Substitution box (S-box) is a keystone of AES symmetric cryptosystem.

5.1 WORKING OF PROPOSED IAES (ENCRYPTION)- Following steps are used in IAES-

Step 1-(divide plain text message in to equal size blocks) plaintext A in to A1 To An

Step 2-A (the 128-bit data path) consisting of 16 bytes A0, A1… A15 is arranged in a four-by-four byte matrix.

Step 3 The key bytes are arranged into a matrix with four rows and four (256-bit key).

Apply GA_Key();

Step 3.1 Key Generation Using GA-The process of generating the key from the Genetic Population has the following steps

3.1.1 In the first step a binary population is generated. Each cell is generated using the pseudo random number generator of the programming language. The number generated is one if the PRNG generates a number greater than 50 else it is 0. Each chromosome contains 25 such cells and the number of chromosomes in the experiment was taken as 1000.

3.1.2 Now for each chromosome we repeat the following process-

a) Divide the chromosome into 5 groups. Calculate the number of ones in each group. If the number of one's is greater than 2 then the new array will have 1 as its cell otherwise 0.

b) The above step converts the population of chromosomes having 25 cells as one having 5 cells.

c) Now we have a 5X 1000 array with us. The array is then read vertically 25 cells at the time.The first column followed by the second and so on.

d) The above step gives us an array of 25 X 200 which serves as the population now. This is followed by crossover and mutation operators being applied to the sample.

e) Now each cell is multiplied by $2^{(12-i)}$ where 'I' is the cell number. This generates a sample of 200 numbers.

f) Each number is then converted into an integer. The process is repeated 5 times.

g) The coefficient of auto correlation is then calculated. If the result is favorable then the population is accepted else the whole process is repeated.

Step 4-Use of Modify Byte Substitution layer S-box-

The first layer in each round is the Byte Substitution layer. The Byte Substitution layer can be viewed as a row of 16 parallel S-Boxes, each with 8 input and output bits.

In the layer, each state byte Ai is replaced, i.e., substituted, by another byte Bi: S(Ai) = Bi

4.1-The first step of S-BOX generation is finding the multiplicative inverse this requires using the irreducible polynomial p(x) defined by-

P(x) = x pow 8 + x pow 4 + x pow 3 + x +1, And inverse of a polynomial a(x) is calculated by A(x) pow -1=b(x) mod p(x)

4.2- Affine Transform- Affine transformation of a single column.

4.3-Diffusion Layer-The Diffusion layer consists of two sub layers, the Shift Rows transformation and the Mix Column transformation.

4.4-Shift Rows Sub layer- The Shift Rows transformation cyclically shifts the second row of the state matrix by three bytes to the right, the third row by two bytes to the rig and the fourth row by one byte to the right.

Step 5-MixColumn Sublayer-This step is a linear transformation which mixes each column of the state matrix. S represents the one complete column of the matrix B.

Step 6-Key Addition Layer-

The two inputs to the Key Addition layer are the current 16-byte state matrix and a subkey which also consists of 16 bytes (128 bits). The two inputs are combined through a bitwise XOR operation.

Step 7- Key Expansion-The Improve AES algorithm takes the Cipher Key, K, and performs a Key Expansion routine to generate a key schedule.

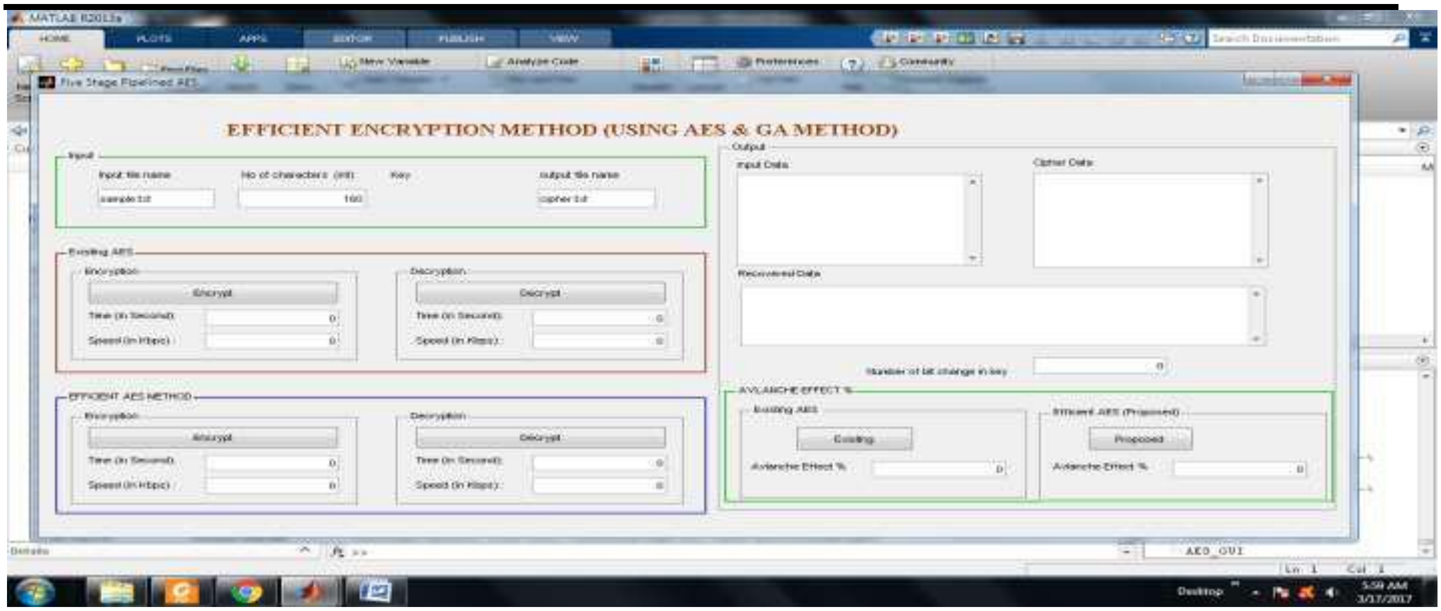
7.1 The Key Expansion generates a total of Nb (Nr + 1) words: the algorithm requires an initial set of Nb words, and each of the Nr rounds requires Nb words of key data.

The resulting key schedule consists of a linear array of 4-byte words, denoted [wi] with i in the range 0 £ i < Nb(Nr + 1)

Step 8- Decryption process – Reverse of encryption process.

VI. EXPERIMENTAL SETUP & RESULT ANALYSIS

In this research proposed and existing methods are implemented over MATLAB simulator fig 6.1. Following results are calculated-



EFFICIENT ENCRYPTION METHOD (USING AES & GA METHOD)

Input

Input file name: sample.txt

No of characters (int): 100

Key:

output file name: cipher.txt

Existing AES

Encryption — Time (in Second): 0 — Speed (in Kbpc): 0

Decryption — Time (in Second): 0 — Speed (in Kbps): 0

EFFICIENT AES METHOD

Encryption — Time (in Second): 0 — Speed (in Kbpc): 0

Decryption — Time (in Second): 0 — Speed (in Kbps): 0

Output

Input Data

Cipher Data

Recovered Data

Number of bit change in key: 0

AVLANCHE EFFECT %

Existing AES — Avlanche Effect %: 0

Efficient AES (Proposed) — Avlanche Effect %: 0

Fig.6: Simulation Screen

6.1 **Encryption time for AES Vs Proposed IAES-**Time that is require to convert a plain text to cipher text.

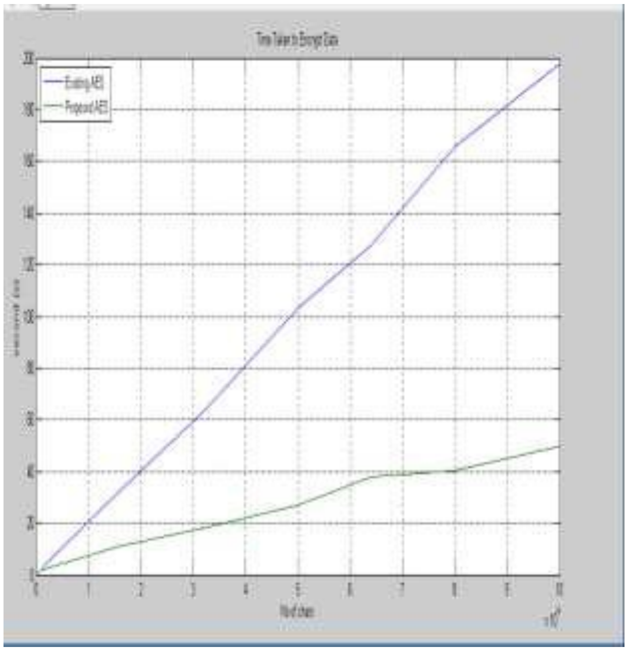


Fig.6.1: Encryption time for AES Vs Proposed IAES

6.2 Decryption time for AES Vs Proposed IAES - Time that is requiring converting a cipher text to plain text.

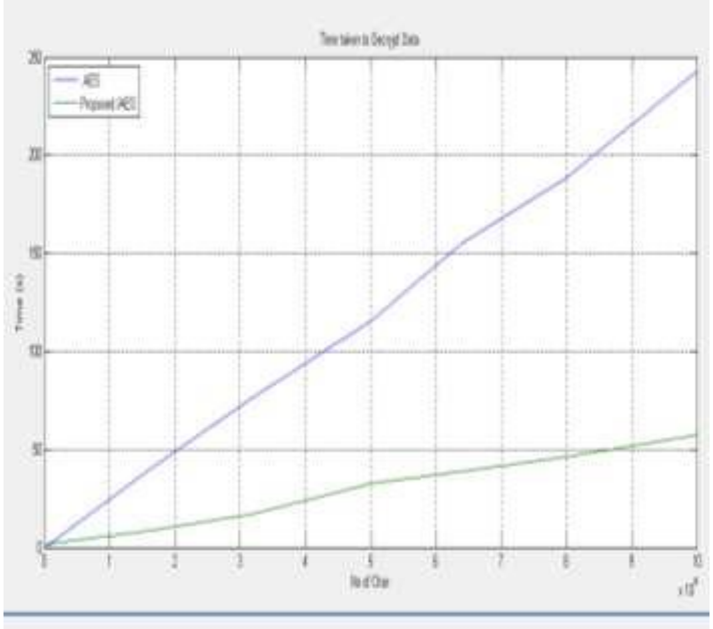


Fig.6.2: Decryption time for AES Vs Proposed IAES

6.3 Encryption speed AES Vs Proposed IAES- Processor speed/Time that is requires converting a plain text to cipher text.

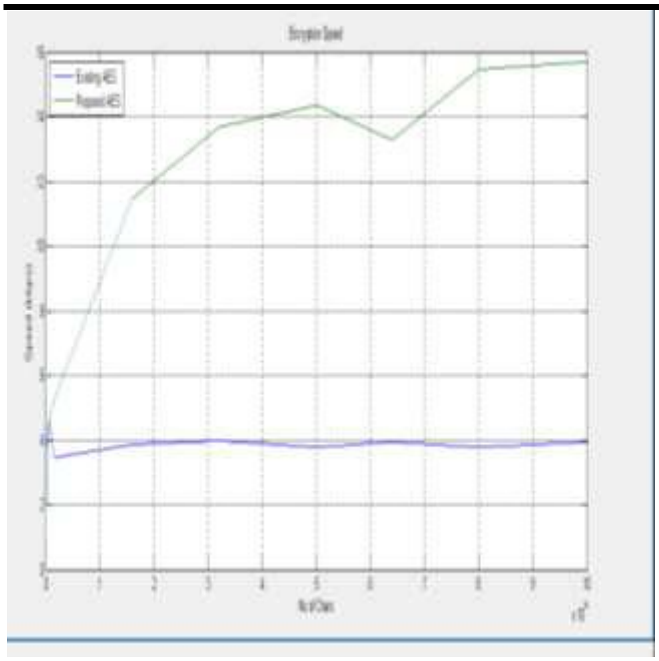


Fig.6.3: Encryption speed for AES Vs Proposed IAES

6.4 Avalanche Effect %- When changing some bit in plaintext and then watching the avalanche change in the outcome of the bits in the cipher text

Table.6.4: Avalanche Effect %

	Avalanche Effect %	
No of bit change	Existing AES	Proposed IAES
1	78	81
2	72	79
4	68	77

6.5 OVERALL COMPARISON RESULT-

An overall comparative analysis for the existing and proposed technique is presented in this section in terms of different relevant parameters-

Table.6.5: Overall comparisons of Existing and Proposed Technique

Sr. No	***Simulation Parameter***	***Existing AES 256***	***Proposed IAES 256***	***Well Performance***
1	*Encryption Time*	*High*	*Low*	*Proposed Technique*
2	*Encryption Speed*	*Low*	*High*	*Proposed Technique*
3	*Decryption Time*	*High*	*Low*	*Proposed Technique*
4	*Decryption Speed*	*Low*	*High*	*Proposed Technique*
5	*Avalanche Effect*	*Medium*	*High*	*Proposed Technique*

VII. CONCLUSIONS & FUTURE WORKS-

The AES encryption is widely used and most popular encryption standard. This is also used in various applications such as processors, hard disk portioning and secure data transmission. In this work an efficient AES encryption method (IAES) is described. Proposed IAES method uses a modified S-Box by employing Genetic algorithm (GA) with key size of 256 bit. In this proposed method IAES, GA is used in the S-box to perform various operations such as substitution, shifting of rows, mixing of column and to perform Add Round Key in the AES rounds. Results comparisons between AES and proposed IAES clearly show that, due to some effective design considerations the proposed IAES, performance is outstanding over existing AES.

In future we will apply this mechanism in real time implementation instead of just a simulation. IAES method can be implements with more multi stage processors to achieved high throughput.

REFERENCES

[1] Nishtha Mathura, Rajesh Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection", 7th International Conference on Communication, Computing and Virtualization, Science Direct, 2016, PP 1036 -1043

[2] K.kalaiselv, and Anand kumar," Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box", CNN Conference IEEE 978-1-5090-1936-6/16 2016, PP 216-222

[3] S.Rehman, S.Q. Hussain, W.Gul and Israr," Characterization of Advanced Encryption Standard (AES) Algorithm for Textual and Image data ", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016, Page No. 18346-18349

[4] D.Lohit Kumar, Dr. A.R.Reddy, Dr.S.A.K.Jilani "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)

[5] Amish Kumar, Namita Tiwari, "AES Security Enhancement by Using Double S-Box", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 ,3980-3984, ISSN-0975-9646, 2012.

[6] Kunal Lala, Ajay Kumar, Amit Kumar, "Enhanced Throughput AES Encryption" International Journal

of Electronics and Computer Science Engineering 2132, ISSN- 2277-2012.

[7] Abhilasha CP, Nataraj KR Engel, A. Uhl, A survey on JPEG 2000 encryption. Multimedia Systems, 2009.15(4): p. 243-270.

[8] Umalaxmi Sawant1, Prof. Kishor Wane 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

[9] Ankit K.Dandekar, Sagar Pradhan, Sagar Ghormade "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

[10] Pankaj Kamboj, and W Wan, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC,"in IEEE International Conference on Audio Language and Image Processing (ICALIP2010), pp. 396-400, Nov. 2010

[11] S.Suguna, Dr.V.Dhanakoti,R. Manjupriya and V kumar, "Efficient Implementation of AES ," in International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 3, Issue 7, July 2013,pp.290-295.

[12] D Jayasinghe, J Fernando, R Herath and R Ragel, "Remote Cache Timing Attack on Advanced Encryption Standard and Countermeasure," in IEEE International Conference on Information and Automation for Sustainability (ICIAFs),pp. 177-182,Dec. 2010.

[13] R Pahal and V kumar, "Efficient Implementation of AES ," in International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 3, Issue 7, July 2013,pp.290-295.

[14] C JunLi, Q Dinghu, Y Haifeng, Z Hao and M Nie,"Email encryption system based on hybrid AES and ECC," in IET International Communication Conference on Wireless Mobile and Computing (CCWMC2011), pp. 347 - 350, Nov. 2011

[15] V Patil, Prof.Dr.Uttam.L.Bombale ,P Dixit, "Implementation of AES algorithm on ARM processor for wireless network, " in International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, August 2013,pp.3204-3209.

[16] H. Tange and B. Andersen, "Attacks and Countermeasures on AES and ECC," in IEEE International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 1-5, Jun. 2013.