ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Rapid Encryption Method [REM] Derived from AES Algorithm for Grey Scale HD Image Encryption

Smita Bachal[1]
Computer Department, DCOER
Pune University
Pune – India

Prof. N.J. Kulkarni[1]
Computer Department, DCOER
Pune University
Pune – India

Abstract: ***Ciphering technique is very important operation to save the secrecy of digital images transmitted over public network spatially with rapidly growth in communication techniques. Encryption algorithm is best way used to handle the information security issue. Encryption algorithms change the information into an unreadable form. Advanced Encryption Standard (AES) is a renowned and well-built symmetric encryption algorithm. Original AES algorithm has some advantages in data ciphering area. However, AES suffer from some drawbacks such as high computations, sample in ciphered images, and hardware requirement. Furthermore, those problems are much more complicated when original AES algorithm will use for images ciphering especially for the HD images. Due to these reasons, some modifications are required to boost the performance of AES algorithm in terms of time ciphering and pattern appearance. First modification is reducing the number of rounds to one while the second modification is replacing the S-box with new S-box to decrease the hardware requirements. Applying modified AES in one of the ciphering mode solves the pattern appearance problems. The experimental results show that the proposed modifications make newer version of AES algorithm faster in the performance as well as fulfill the security requirements.***

Keywords: AES algorithm, AES version, pattern appearance, mode encryption, HD image.

I. INTRODUCTION

Rapid advancement in communication area such as satellite, mobile network, internet, earth communications, etc. make important to protect and preserve sensitive and critical public, private, and national infrastructures and their respected data against attacker and illegal copying and distribution [1].

To provide protection to the data transmission over insecure channels two kinds of cryptographic systems are used: Symmetric and Asymmetric cryptosystems. Symmetric cryptosystems uses same key for the sender and receiver; both to encryption and decryption purpose. Asymmetric cryptosystems uses different keys for encryption and decryption. Advanced Encryption Standard (AES) is a renowned and well-built symmetric encryption algorithm. AES encryption algorithm is an efficient system for both hardware and software implementation. As compare to software implementation, hardware implementation provides high level security and higher speed. Hardware implementation is useful in various applications such as wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication. The main objective of modification of AES is to achieve efficient hardware architecture design & implementation.

In image encryption does on image pixels by pixels locations (confusion) or pixels values (diffusion). One of the most popular public cryptography and widely used in large number of applications such as smart card, cell phone, automated teller machines, and www servers is the Advanced Encryption Standard (AES) [2]. The National Institute of Standard and Technology (NIST) accepted Advance Encryption Standard (AES) that produced by Rijndael in 2001. However, AES go

through from some drawbacks such as, large amount of encryption and decryption time, and patterns appearance in the ciphered image [3].

II. LITERATURE SURVEY

A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box [2]

In this paper, we present a novel Field Programmable Gate Array (FPGA) implementation of advanced encryption standard (AES-128) algorithm based on the design of high performance S-Box built using reduced residue of prime numbers.[1] The main motive is to present an efficient hardware usage of AES-128 using Very High Speed Integrated Circuit Hardware Description Language (VHDL).

The novel S-Box look up table (LUT) entries forms a set of reduced residue of prime number, which forms a mathematical field. The S-Box with reduced residue of prime number introduces more confusion to the entire procedure of AES algorithm and makes it more difficult and provides further resistance against attacks.

An FPGA is a digital integrated circuit that can be programmed after it is manufactured rather than being limited to a predetermined, stable hardware function. Latest FPGAs offer various math functions, embedded memories and storage elements, which makes the design of cryptography easier and provides reasonably cheap solution for designing and implementing various algorithms [5]. Implementation of security protocols on FPGA leads to the various benefits such as low cost, availability of sophisticated designing and debugging tools, in-circuit reprogramability facility and short amount of time to market which leads to the lower financial risk and provides much higher performance than software implementations. This novel FPGA implementation

Security of Image in Multimedia Applications [3]

It is necessary to protect the confidential image data from unauthorized access for multimedia applications. In this paper, independent efficient compression and encryption algorithm is suggested for multimedia applications. In order to overcome the amount of multimedia data over wireless channels, data compression techniques are widely used. Discrete cosine transform (DCT) is one of the most important compression technique. The Dynamic bit-width adaptation scheme in discrete cosine transform (DCT) is used as an efficient compression technique, where operand bit-widths are changed according to image quality and/or power consumption requirements and the new modified version of AES, a secure symmetric image encryption technique, has been proposed.

Original AES algorithm is not able to provide high level security and better image encryption. Therefore, this paper, suggest a Modified Advanced Encryption Standard (MAES) to achieve a high degree of security and better image encryption. The modification is done through adjusting the Shift Row Transformation. MAES gives enhanced encryption results in terms of security touching statistical attacks.

Improvement of an image encryption algorithm based on hyper-chaos [4]

This paper proposes enhancement in recently proposed image cryptosystem based on hyper-chaos. The updated version has been developed to resist against attacks made to break the original one and to faster in processing. The modification uses the two Boxes, namely P-Box and S-Box, which composed the original cryptosystem. As compared with standard encryption algorithm, AES and Triple-DES, the newer version of the cipher gives better performance.

- **Weaknesses of the original cryptosystem**
  - The keystream generation depends only on the secret keys; as a result, it is the same for every couple of plaintext/cipher text.

- The shuffling process can be separated from the confusion process, for this reason, special inputs (i.e. plain images) can be selected in a circumstance of plaintext attacks to break every key process.
- To shuffle the plain image, large amount of time is needed.

- **Proposed hyper-chaos based cryptosystem**

  This encryption algorithm must include two main steps as follows.

  1. **P-Box or permutation step:** In this step, the positions of the information unit are changed in the data sequence
  2. **S-Box or substitution step (or confusion-diffusion-step):** In this step, each piece of information is substituted by another symbol.

  The proposed cryptosystem will be designed in that way to fulfill security requirement. As a result, it is possible to improve the keystream using chosen ciphertext attacks (CCA) and chosen plaintext attacks (CPA).

Some modifications of a cryptanalized cryptosystem present some weakness in the generation of its keystream and also in the permutation process of algorithm. The modified cryptosystem emphasizes on designing the cryptosystem in a CBC mode to make the keystream changes when the plain image changes. Therefore, the two criteria are important to obtain good performance in cryptography, the confusion and the diffusion, are verified and compared with those of AES and Triple-DES where.

A low cost implementation of Advanced Encryption Standard algorithm using 8085A microprocessor [5]

The highly secured communication systems became an urgent need in recent years for both governments and peoples who need protection from signal interception. Advanced Encryption Standard (AES) is a renowned symmetric block encryption algorithm has several advantages such as reliable, flexible, and compatible with hardware implementation in data encryption. However, AES suffer from some drawbacks such as high computations, pattern appearance, more hardware requirements, and encryption time is long, especially with multimedia application. These problems are become more complicated when the AES algorithm is used for multimedia application. Therefore, modification of AES-128 algorithm takes place.

Modified AES algorithm reduces the computations and hardware requirements by enforcement Mixcolumn transformation in five rounds instead of nine rounds. Second modification is proposed that, make the use of new simple and same S-box for encryption and decryption process. An objective of this paper is to speedy, low cost implementation of Modified Advanced Encryption Standard (MAES) cryptographic algorithm using 8085A microprocessor.

An implementation of MAES algorithm focuses on simple item with low cost. 8085A microprocessor is very effective manner and reasonable speed processing tool used in this implementation. Figure-1 shows System block diagram used for implementation.

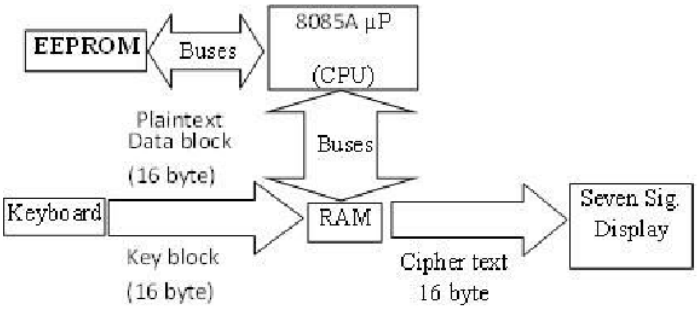

Figure-1: System Block Diagram [4]

The system consists of:

1. 8085A microprocessor: 8 bit processor from Intel family, Operating frequency is 5 MHz.
2. EEPROM: about 0.978 Kbyte used to saving the operating programs and S-Box and inverse S-Box.
3. RAM: about 0.76 Kbyte
4. Keyboard and 7-sigment display: to input the plaintext and key block from user and display the cipher text as outputs.
5. I/O ports.

III. WORKING METHODOLOGY

A. Advanced Encryption Standard [AES] Algorithm

The original AES algorithm is developed by Joan Daemen and Vincent Rijmen has been accepted by NIST as standard ciphering algorithm. AES algorithm have three versions based on the length of the key (AES-128, AES-192, and AES-256)bit and 128 bit block data which constructed in 4x4 matrix called state. AES algorithm carried out into four sequential operations; where these operations are made on a state with (10, 12, 14) rounds based on key length. AES algorithm uses four transformations as below:

- **SubByte transformation:** where nonlinearly substitute the state bytes independently using substitution table i.e. S-box.
- **Shift row transformation:** in this phase, apply on state rows where, 1^{st} row no shifted, 2^{nd} row shifted to right one time, 3^{rd} row shifted to right two times, and 4^{th} row shifted to right three times.
- **Mixcolumn transformation:** in which carries out on state column by column. Each byte is replaced by a value dependent on all 4 bytes in same column through multiplication state matrix in $GF(2^8)$.
- **Add Round Key transformation:** this phase is a simple bitwise XOR between 16 byte state matrix and a portion of the expanded key (16-byte key matrix).

B. Modified Advanced Encryption Standard [MAES] Algorithm

One main problem in original AES algorithm is patterns appearance in the ciphered image because of the presence a area with same color in original image. Modified AES algorithm proposed to overcome this problem. The modification is mainly concentrated on ShiftRow Transformations step in algorithm, if the value of 1'st element in state is even, the second and third rows are shifted right one and two times respectively, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows to take away the patterns appear.

C. Proposed Modifications

To enhance the performance of AES algorithm two modifications are introduced. Due to this modification, AES algorithm becomes more compatible with ciphering of images, especially for HD image encryption. Original AES algorithm requires large amount of time for encryption process. To reduce encryption time, first modification is decreasing the number of rounds to only one round instead of ten. As a result, encryption time is reduced approximately by 1/10. The second modification we suggested new and simple S-box to reduce the computation time. The suggested new S-box matrix has several advantages such as, simple, developed with very low calculations, same S-box used to encryption and decryption process instead of two S-box used in original AES algorithm where this lead to reduce the amount of Read-only memory used by 256 byte, therefore, reduces the hardware requirement.

IV. CONCLUSION

Standard AES algorithm is slower in performance especially for the HD image encryption because it is computationally expensive. Modifications on AES algorithm are proposed to overcome the above-mentioned drawbacks. These modifications involved AES algorithm with one round only and using newer version of S-box under CBC ciphering mode. Experimental results clearly show that new proposed modified AES algorithm makes it less computationally intensive and compatible with HD images while fulfills the security requirements.

References

1. Salim M. Wadi, Nasharuddin Zainal Rapid Encryption Method Based on AES Algorithm for Grey Scale. The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013).
2. Rais, M., H., Qasim., S., M. A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box.International Journal of Computer Science and Network Security, 2009, 9, 9, p. 5.
3. Telagarapu, P. , Biswal, B., Guntuku, V., S. Security of Image in Multimedia Applications.International Conference On Energy, Automation And Signal, IEEE, 2011, p.5.
4. Hermassi, H., Rhouma, R., Belghith, S. Improvement of an image encryption algorithm based on hyper-chaos. Telecommun Syst, Springer Science Business Media, 2011, p. 11.
5. Wadi, S., M., Zainal, N.A low cost implementation of Advanced Encryption Standard algorithm using 8085A microprocessor.3rd international technical conference (ITC2012),2012, pp. 157-163.
6. Jing, M., H., Chen, J., H., Chen, Z., H. Diversified Mixcolumn Transformation of AES. The 9th International Conference on Informationand Communications Security", IEEE, 2008, p. 3.
7. Hammad, I., M. Efficient Hardware Implementations for The Advanced Encryption Standard (AES) Algorithm. M.Sc. thesis, DalhousieUniversity Halifax, 2010, p. 174.
8. Huang, C., W. , Yen, C., L., Chiang, C., H., Chang, K., H., Chang, C., J. The Five Modes AES Applications in Sounds and Images.6th international conference on information assurance and security, IEEE, 2010, pp. 28-31.
9. Huang, C., W., Tu, Y., H., Yeh, H., C., Liu, S., H., Chang, C., J. Image Observation on the Modified ECB Operations in Advanced Encryption Standard.International Conference on Information Society (i-Society 2011), IEEE, 2011: p. 6.
10. Kamali, S., H., Shakerian, R., Hedayati, M., Rahmani, M. A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. International Conference on Electronics and Information Engineering, IEEE, 2010, 1, p. 5.
11. Borujeni, S., E., Eshghi, M. Chaotic image encryption system using phase magnitude transformation and pixel substitution, Telecommun Syst, Springer Science and Business Media, 2011, p.13.

