Review on Image Encryption and Decryption using AES Algorithm

Sneha Ghoradkar,
(M.E. VLSI & ES) Department of E&TC,D.Y. Patil College of Engg, Akurdi,Pune

Aparna Shinde
(Assistant Professor) Department of E&TC,D.Y. Patil College of Engg., Akurdi,Pune

ABSTRACT
An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm is proposed in this paper. Due to increasing use of image in various field, it is very important to protect the confidential image data from unauthorized access. The design uses the iterative approach with block size of 128 bit and key size of 256 bit. The numbers of round for key size of 256 bits is 14. As secret key increases the security as well as complexity of the cryptography algorithms.This paper presents a algorithm in which the image is an input to AES Encryption to get the encrypted image and the encrypted image is the input to AES Decryption to get the original image.

Keywords
AES algorithm, image encryption, image decryption

1. INTRODUCTION
The use of the internet and wireless communications has been rapidly growing andoccupying a wide area in everyday life. Millions of users generate and interchange large amount of electronic data on a daily basis in diverse domains. However, the issue of privacy and security is on the top of the crucial concerns which determine the diffusion of such applications into the daily life. Hence, cryptography turns to become the key for the reliability and effectiveness of the embedded

Technologies [1].Nowadays cryptography has a main role in Embedded systems designs. In many applications, the data requires a secured connection which is usually achieved by cryptography. Cryptography is divided in two types first is symmetric key cryptography (sender and receiver shares the same key) and the second one is asymmetric key cryptography (sender and receiver shares different key) [2].

Symmetric systems contains Data Encryption Standard (DES), 3DES, and AdvancedEncryption Standard (AES) use an identical key for the sender and receiver.

DES (Data Encryption Standard) was considered as the standard of symmetric keyencryption, which has a key length of 56 bit. This key length is considered as very small and can be easily broken. The National Institute of Standards and Technology(NIST), proposed Rijndael algorithm as the Advanced Encryption Standard(AES) in October 2000 providing strong security and high flexibility. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

2. PREVIOUS WORK
In paper [1] Mazen El Maraghy et. Used AES-128 bit algorithm for optimization of area and speed. They have used 128 data bits as well as 128 bit cipher key. The implemented hardware design is evaluated in real time. M.Sambasiva Reddy et. [2] used the same AES-128 bit algorithm for speed, power consumption and area. They have implemented the AES algorithm using EDK. Hoang Trang et.[3] This gives low complexity architecture and easily achieves low latency as well as high throughput. The design used an iterative looping approach with block and key size of 128 bit, lookup table implementation of S-box.Kamali S.H et. [4] used the modified advanced encryption algorithm to reflect a high level security and better image encryption.The modification is done by adjusting the ShiftRow Transformation.The author have compared the results of the previous AES algorithm and modified AES algorithm.

3. PROPOSED WORK
3.1 AES Algorithm
The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed system consists of block size of 128 bits and key size of 256 bits. The algorithm is applied for both image encryption and decryption. As the key size is of 256 bits it will take 14 rounds.

3.1.1 AES Image Encryption
Conversion of original image i.e plain image into encrypted image i.e cipher image is known as image encryption.

The round consists of the following stages for image encryption shown in fig 1.:

- SubstituteBytes
- ShiftRow
- MixColumns
- AddRoundKey

SubstituteBytes:
The SubBytes transformation includes non-linear byte substitution, operating on each of the state bytes independently. This is done by using a once-precalculated substitution table called S-box. S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values.

ShiftRow:

ShiftRows transformation includes, the rows of the state are cyclically left shifted. Row 0 remain unchange; row 1 does shift of one byte to the left; row 2 does shift of two bytes to the left and row 3 does shift of three bytes to the left.

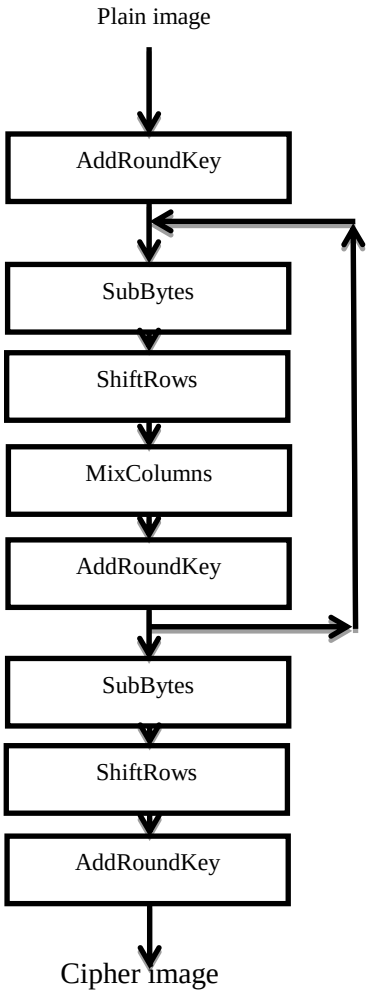

Figure 1: AES Image Encryption

MixColumns:
In MixColumns transformation, the columns of the state are considered as polynomials over GF (2^8) and multiplied by modulo $x^4 + 1$ with a fixed polynomial c(x), given by:

c(x)=$\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.

AddRoundKey:

In the AddRoundKey transformation, a Round Key is added to the State resulted from the operation of the MixColumns transformation by a simple bitwise XOR operation.

The RoundKey of each round is derived from the main key using the KeyExpansion algorithm. The encryption and decryption algorithm needs fourteen 256-bit RoundKey.

3.1.2 AES Image Decryption:

Reverse of encryption is called decryption. It means conversion of cipher image into plain image.
The round consists of the following stage for image decryption shown in fig 2.

- AddRoundKey
- InverseShiftRow
- InverseSubstituteByte
- InverseMixColumns

AddRoundKey:
AddRoundKey is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order.

InverseShiftRow:
InvShiftRows exactly functions the same as ShiftRows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.

Table 1: AES Parameters

Algorithm	Key length	Block size	Number of round
ASE-128	4	4	10
ASE-196	6	4	12
ASE-256	8	4	14

InverseSubstituteByte:
The InvSubBytes transformation is done using a once-precalculated substitution table called InvS-box. That InvS-box table contains 256 numbers (from 0 to 255) and their corresponding values.

InverseMixColumns:
In the InvMixColumns transformation, the polynomials of degree less than 4 over GF(28), which coefficients are the elements in the columns of the state, are multiplied modulo (x4 + 1) by a fixed polynomial d(x) = {0B}x3 + {0D}x2 + {09}x + {0E}, where {0B}, {0D}; {09}, {0E} denote hexadecimal values.

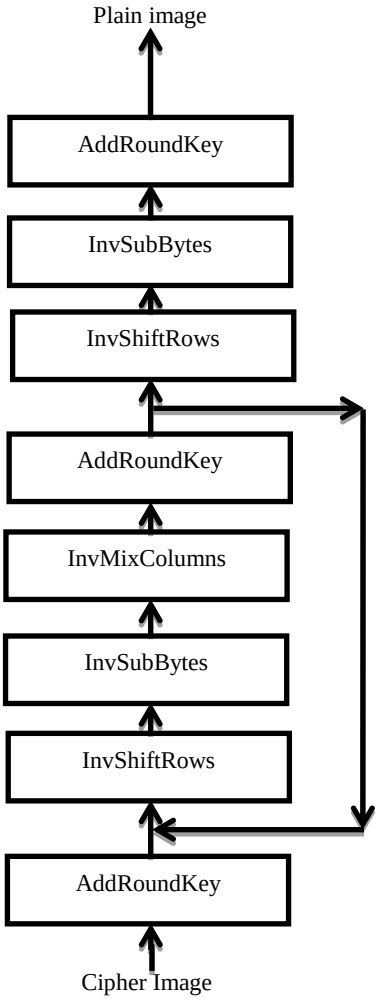

Figure 2 AES Image Decryption

4. CONCLUSION& FUTURE SCOPE

In this paper image encryption and decryption using Advanced Encryption Standard (AES) algorithm is proposed

for image encryption and decryption that can process with the data block of 128 bit and cipher key length of 256 bit. The usage of 256 bit cipher key to achieve the high security, because 256 bit cipher key is difficult to break. As a result of this secure transmission of image can be possible. Future scope is, it can be used in various applications like Military communication, Forensics, Intelligent systems etc.

5. REFERENCES

[1] El Maraghy M, Hesham S and Abd El Ghany M.A, "Real-time Efficient FPGA Implementation of AES Algorithm", IEEE International SOC Conference (SOCC), page 203-208, Sept 2013.

[2] M.Sambasiva Reddy and Mr.Y.Amar Babu, "Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, page 3341-3347, July 2013.

[3] Hoang Trang and Nguyen Van Loi, "An Efficient FPGA Implementation of The Advanced Encryption Standard algorithm", IEEE International Conference on Computing and Communication Technology, page 1-4, Ho Chi Minh city, 2012.

[4] Kamali S.H, Shakerian R, Hedayati M and Rahmani M, "A new modied version of Advanced Encryption Standard based algorithm for image encryption", (ICEIE) International Conference On Electronics and Information Engineering, volume 1, page 1250-1255, Aug 2010.

[5] Ahmad N, Hasan R and Jubadi W.M, "Design of AES S-box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), page 512-517, Oct 2010.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:3, page 726-731, 2007.

[7] FIPS 197, "Advanced Encryption Standard (AES)," November 26, 2001.

[8] National Institute of Standards and Technology (NIST), "Data Encryption Standard (DES)," National Technical InformationService VA 22161, 1999.