AES Algorithm on FPGA based Image Encryption and Decryption

Sneha Ghoradkar[1], Aparna Shinde[2]

[1]M.E. VLSI & ES, E&TC Department, D.Y.Patil college of Engineering, Akurdi, Pune–411044

[2]Assistant Professor, E&TC Department D.Y.Patil college of Engineering, Akurdi, Pune-411044

Abstract: ***Due to the increasing use of images in various applications, it is essential to protect the confidential image data from unauthorized access. In today's world most of the communication is done using electronic media. Security of data is widely used to ensure security in communication, data storage and transmission.Advanced Encryption Standard (AES) which is accepted as a symmetric cryptography standard for transferring block of data securely. The available AES algorithm is used for text and it is also suitable for image encryption and decryption to protect the confidential image data from an unauthorized access.This project proposes 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. This paper presents 128 bits of AES image encryption and decryption using Xilinx Platform Studio (XPS)-10.1.***

Keywords: Cryptography,AES algorithm, Image Encryption, Decryption.

1. Introduction

Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. It helps us to store sensitive information or transmit it across insecurenetworks so that unauthorized persons cannot read it. The exchange of digital data in cryptography results in different algorithm that can be classified into two cryptographic mechanisms: symmetric key in which same key is used for encryptionand decryption and in asymmetric key different keys are used for encryption and decryption. Symmetric key algorithms are much faster and easier to implement and generally requires less processing power when compared with asymmetric key algorithms.

For a long time, the Data Encryption Standard (DES) was considered as a standard for the symmetric key encryption. DES has a key length of 56 bits [2]. However, this key length iscurrently considered small and can easily be broken. The National Institute of Standards and Technology (NIST) declared Rijndael algorithm [1] as the Advanced Encryption Standard (AES) in October 2000. The Advanced Encryption Standard specifies a Federal Information Processing Standard (FIPS) that has approved cryptographic algorithm which is used to protect sensitive information. The AES algorithm is a symmetric key algorithm that encrypts and decrypts information. Encryption processconverts an original information (plain image) into encrypted image (cipher image). Decryption process is to convert the cipher image information back to plain image so that it can be readily understood.

AES algorithm is not only for the text data, it can applied for the images, usually image processing deals with images, which is composed of many image points, namely pixels, spatial co-ordinates that indicate the position of the points in the image and intensity values. The applications of the image processing have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc.

FPGA is an intermediate solution between general purpose processor(GPPs) and application specific integrated circuit(ASICs). It has advantages over both GPPs and ASICs. It provides faster solution then GPPs. Also, it has wider applicability then ASICs sincs its configuring software make use of broad range of functionality supported by reconfigurable device.

2. Proposed Work

AES Algorithm

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes data blocks of 128 bits using three different cipher key lengths 128,192 or 256 bits. Based on the key length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed implementation supports the AES-128 Encryption. The 128-data bits and 256-bit cipher key are formulated into a 4 x 4 state matrix and key matrix respectively. At the start of the algorithm, the state matrix is initialized with the original plain image while the key matrix is initialized with the input master key.

Figure 1.showsthe AES encryption. Procedure that consists of 14 rounds. Through each round, the two matrices are processed differently in an independent manner and their outputs are combined at the end of each round in the AddRoundKey phase.The algorithm begins with an Addround key stage followed by 13th rounds of four stages and a 14th round of three stages which applies for both encryption and decryption algorithm.

These rounds are governed by the following four stages:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The 14th round Mix columns stage is not included. The first 13 rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

Again the 14th round Inverse Mix columns stage is not included. The Overall flow of the encryption and decryption algorithm of the AES algorithm is show in Figure 1.

AES Encryption:

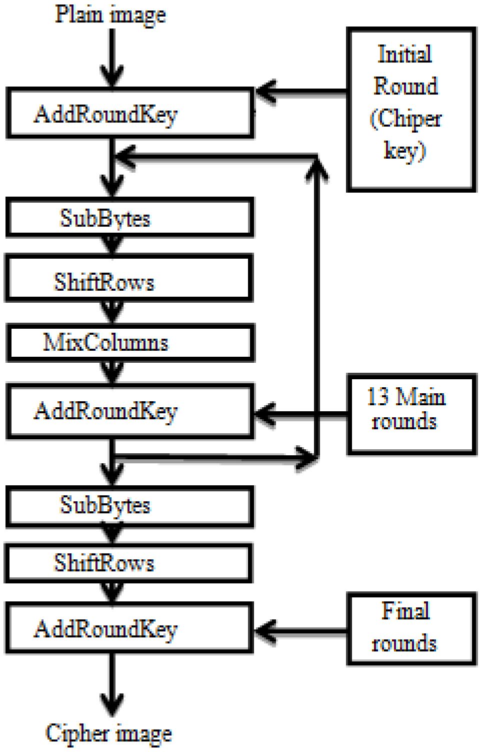


Figure 1: AES Image Encryption

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.

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.

AES Decryption:

AddRound Key:

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.

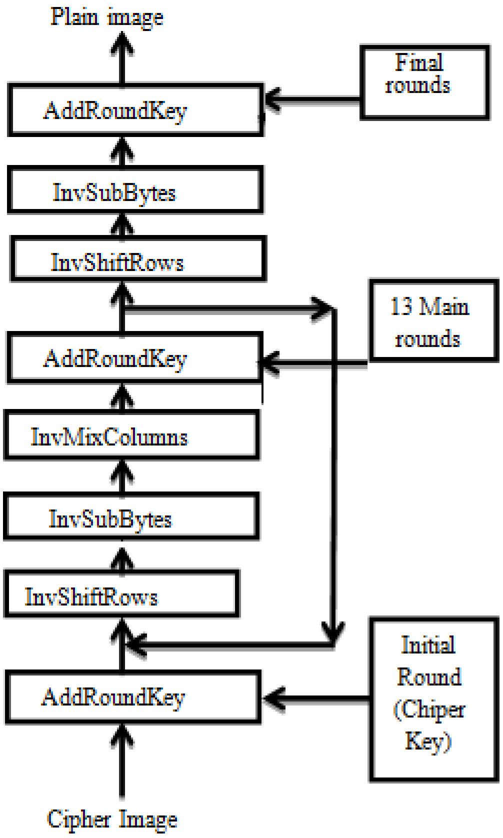


Figure 4: AES Image Decryption

InverseSubstituteByte

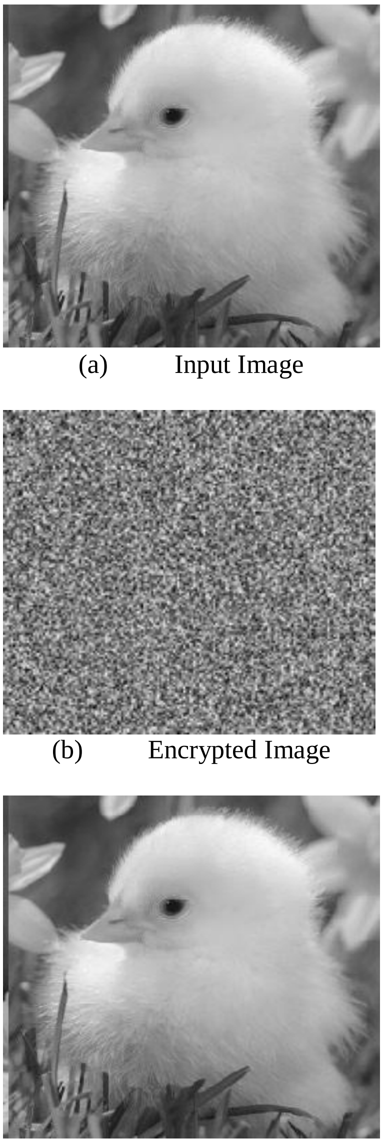
The InvSubBytes transformation is done using a once-precalculated substitution table called InvS-box. That InvS-box table contains 256 numbers (from 0 to 255) and their corresponding values.

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**.**

3. Results

A colour image is converted to grey using matlab and generates the header file in matlab. Figure 5(a) shows the converted grey image. Header file is then read in XPS using system c and after implementing on SPARTAN 3 EDK board we get the results as shown in figure 5.



(a) Input Image

(b) Encrypted Image

(c) Decrypted Image

Figure 5: (a) Input Image (b) Encrypted Image (c) Decrypted Image

4. Conclusion

AES algorithm on FPGA based image encryption and decryption has been proposed in this paper to protect the confidential image data from an unauthorized access. This AES algorithm can process with the data block of 128 bit and cipher key length of 256 bit. Same key is used to encrypt and decrypt the data. The use 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. Xilinx platform studio (XPS)10.1 with impulse c is used for synthesis of AES algorithm.

References

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

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

[3] 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.

[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] 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.

[7] 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.

[8] 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.