Study of AES Techniques used for Image Hiding

Vijimol V K
Assistant Professor
Department of Electronics and Communication
Trinity College of Engineering
Naruvamoodu
Trivandrum, Kerala, India

Abstract:- **This paper will take an in-depth look at image cryptography technique, and brief history of Cryptographic and take one of this technique (AES) to implement encoding secret data in images JPG kind by using VHDL language. The paper will close by looking at how we can use image cryptography in open-systems environment such as the Internet, as well as some of the tools and resources available to help us accomplish this.**

I. INTRODUCTION

Computer has become an essential component presently. The importance of computer is to store data and send the data from one spot to other. The data that is collective must be transported in a weak manner. To avoid these situations data can be coded to some formats that is incomprehensible by an illegal person. Cryptography is one of the methods of information security which has become a very critical aspect of modern computing systems to secure the data transmission and storage.

The exchange ofdata in cryptography outcome in different algorithm that can be classified into two cryptographic mechanisms: symmetric key and asymmetric key Symmetric key algorithms are much more rapidly and easier to put into operation and generally requires less processing power. In October 2000 The National Institute of Standards and Technology (NIST) acknowledged Rijndael algorithm as the Advanced Encryption Standard and it is a symmetric key algorithm that encrypts and decrypts the data.

Encryption changes and converts an original message into encrypted message that is a cipher text alter the cipher text message back to plain text so that it can be easily understand.

AES algorithm can apply for the images. The image points that is pixelsand spatial co-ordinates that shows the position of the points in the image, values of intensity respectively. All the applications spread around in the areas of Defense, Forensic a, Robotics, smart systems, etc. The proposed work do the implementation the AES algorithm with image as input data and three different length keys which can be applied for both hardware and software implementation.

II. AES ALGORITHM

The AES algorithm otherwise known as Rijndael algorithm which is a symmetric block cipher that work on the data blocks of 128 bits with the cipher key of length 128, 192, or 256 bits. Each of the data block consists of a 8×8 array of bytes called the **state**, where the basic operations of the AES algorithm are performed. Following a primary round key addition, a round function consisting of four special transformations—SubBytes(), ShiftRows(), Mix Columns() and AddRoundKey() is applied to the State array.

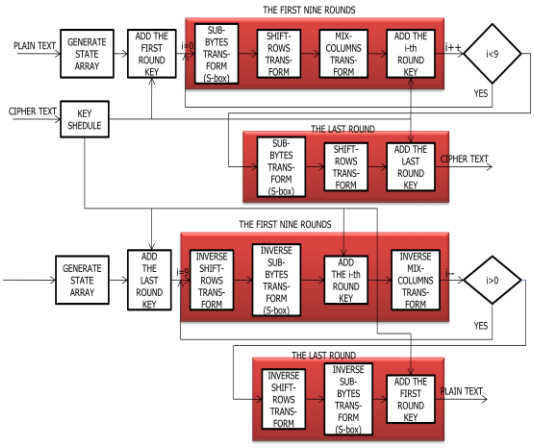


Figure 1. Block Representation of AES algorithm

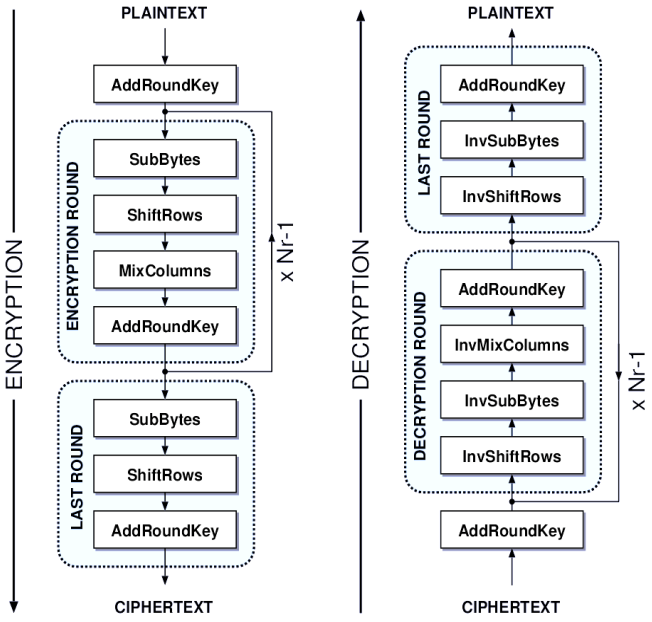


Figure 1.Encryption and Decryption Flow chart.

The round functional presses are performed iteratively for 10, 12, or 14 times, depending on the key length. In the last round, Mix- Columns () does not applied. The four transformations are described briefly as follows

1. SubBytes: a non-linear byte substitution that operates independently on each byte of the State using a substitution table (called the S-box).

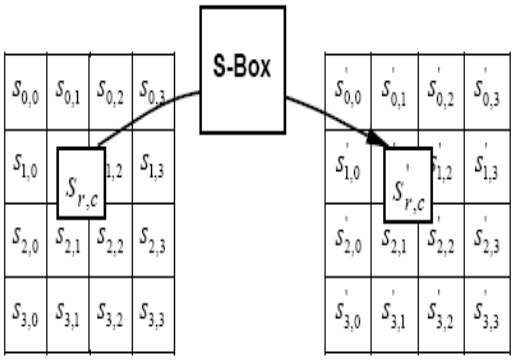


Figure 3.operation of Subbyte

2. ShiftRows: a circular shifting operation on the rows of the State with different numbers of bytes

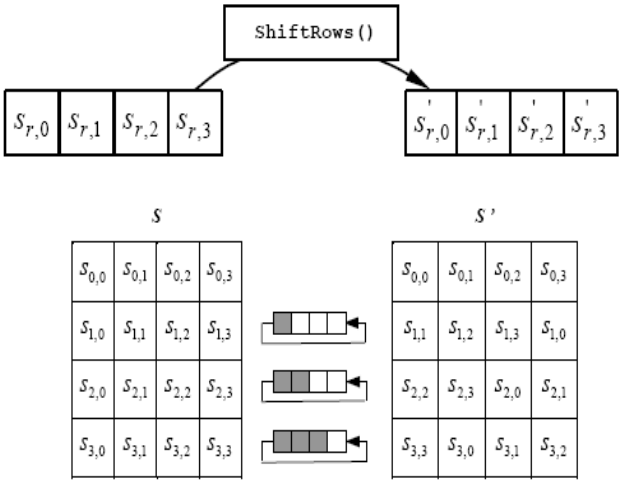


Figure 4. Operation of shift row

3. MixColumns: the operation that mixes the bytes in each column by the multiplication of the State with a fixed polynomial of modulo x4 + 1.

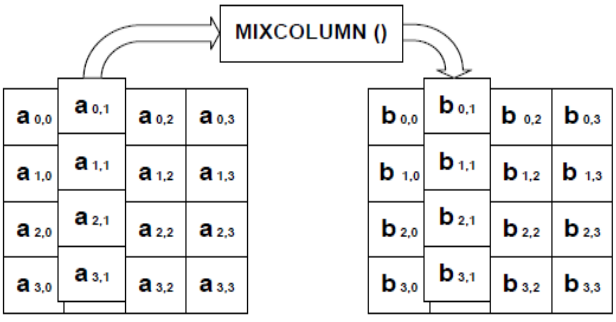


Figure 5 .operations of Mixcolumn

4. AddRoundKey: it is an XOR operation that adds a round key with the State in each iteration. Here the round keys are formed during the key expansion stage.

There are three steps, in the Key schedule round.

Rotate: takes a four-byte word and rotates one byte to the left.

Subytes: takes four-byte input word by replacing each byte in the input to another byte according to the S-Box.

Rcon: The first byte of a word is XORed with the round constant. Each value of the Rcon chart is a part of the AES finite field. Add round key is identical for the both encryption and decryption.

Alike decryption procedure rearranges the order so that the order of transformations in the decryption keep regular with that in the encryption. Also, sharing source will be enabled.. In the decryption, the modified round keys should be useful to the original generated roundkeys using InvMixColumn transformation. SubBytes and InvSubBytes transformations are combined using composite field arithmetic. ShiftRows and InvShiftRows are simple shifting transformation process. MixColumn and InvMixColumn transformations are optimized and merged.

In the decryption process the round key is first added to the state and then the result is possible with the InvMixColumn part. Then only the rest of the process can take part.

Block length = 128 bits, $0 \le n < 16$;
Key length = 128 bits, $0 \le n < 16$;
Key length = 192 bits, $0 \le n < 24$;
Key length = 256 bits, $0 \le n < 32$.

III. TAKING IMAGE AS AN INPUT DATA

Here our input or information is as the form of image. An image can be encrypted by combining MATLAB with the encoder. Every pixel in an image is represented by 8 bits,ie 1 byte. Using MATLAB convert the pixel values into bytes. Byte values are then used as input to the encoder. The encoder then converts this byte into corresponding encoded byte. The output from encoder is then converted into decimal values for pixels. Repeat this operation for each pixel.

IV. ENCRYPTION MODULE

This proposed system can designed as 8×8 matrix. that means at a time we can operate 32 bits. Here we integrated the blocks to reduce the memory taken. Thus we can increase the speed of processing.

To implement the AES algorithm using VHDL coding in the Xilinx 12.4, we continue with the encryption and decryption with key of any 128,192 and 256 bits. The encryption parameters are the input image, the key of three different lengths (128,192 and 256) and the output cipher

text. First, we have to map the 32 byte input image pixel values in the correct order to the 8*8 byte state, calculate the number of rounds based on the key Size and expand the key using our key schedule. At the first round, the input created from image and key is XORed and rest of the rounds has to apply all four operations: Sub bytes, Shift rows, Mix columns, Add round key. The last round Mix columns stage is not integrated and round key was generated during each iteration. Here simple XOR of each byte of the key with the particular byte of the state is done to get cipher text.

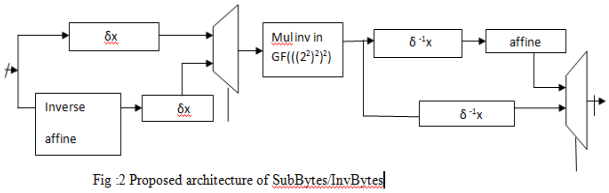


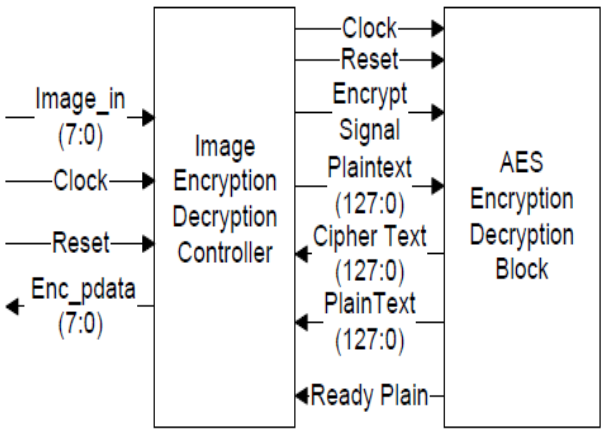
Fig :2 Proposed architecture of SubBytes/InvBytes

V.DECRYPTION MODULE

For AES decryption part, the same encryption process occurs in reverse manner. The decryption parameters are the input cipher text, the key and the output should be same as encryption input. In decryption the key schedule is same as the encryption part ; the process we are doing is the Inverse sub Bytes, shift Rows and mix Columns, but add Round Key remains the same.

VII. IMAGE ENCRYPTION AND DECRYPTION PARTS

To Encrypt, Decrypt the image pixel, 8 bits is the input and output with the 128 bit AES algorithm. We have to shift the 8 bit input to 128 bit register and feed it to the AES Encryption algorithm to get the Encrypted 128 bit data and from the 128bit register shift 8 bit data to Image per clock to get the encrypted image. To get back the original image feed the Encrypted image to the AES Decryption part.



VIII.CONCLUSION

In this paper, Image Encryption and Decryption using AES with three different key is designed and implemented to protect the confidential image data from an unauthorized access. A Successful implementation of AES algorithm is one of the best encryption and decryption standard available in market. It helps to explore the path to implement such an algorithm using VHDL code that is synthesized and simulated using the ISE 12.4 in Xilinx Family Spartan-6.If we can apply pipelining or sub pipelining methods to this proposal it will provide us a higher throughput.If we can optimize the architecture of on-the-fly key with three different keys and both encryption and decryption can handled, which can generate more than a 128-bit key in one cycle.

REFERENCES

[1] Eric Cole, Ronald D. Krutz, Consulting Editor (2003), Hiding in Plain Sight, Steganography and the Art of Covert Communication, Wiley Publishing, Inc.
[2] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.
[3] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.
[4] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.
[5] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) "Pattern Based 3D Image Steganography", 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.
[6] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) "Steganography Based On Random Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.
[7] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.
[8] B. Sharmila and R.Shanthakumari, (2012) "Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392.
[9] National Institute of Standards and Technology, "Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES)," Nov. 2001.
[10] William Stalling, Cryptography and Network Security: Principles and Practices, Principles and Practices, 4th ed. Prentice Hall, 2006.
[11] Charles H Roth, Jr. Digital Systems Design Using VHDL, Thomson, India Edition 2007.
[12] Atul Kahate, Cryptography and Network Security, Second Edition, Tata McGraw-Hill Edition 2008.
[13] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2,pp.226-232 February 2010.
[14] P.Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, pp166-172, 2011.
[15] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare "FPGA Implementation of AES Algorithm" IEEE, pp.401-405, 2011.
[16] Xinmiao Zhang, Keshab K. Parhi, Fellow, "High-Speed VLSI Architectures for the AES Algorithm" IEEE Transactions on vlsi systems, vol. 12, no. 9, pp.957-966, September 2004.