Secure the Secret Data's by Double Encryption using Image Processing and VLSI Technology

R.Vinoth, M.Balaji, S.Shobana, D.Vinoth, R.Nivethitha

***Abstract*— Transmission of confidential data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity and non reproduction of exchanged information. This project combines the steganography and cryptography to protect the information. Least significant method is used to hide the information. The symmetric key algorithm of AES used to encrypt the image. The encrypted image has been implemented in FPGA.**

***Index Terms*— AES algorithm, FPGA,LSB**

I. INTRODUCTION

This project has a combination of steganography and cryptography. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". A cryptographic algorithm has three classifications: symmetric, asymmetric and cryptographic hash function. Data encryption standard (DES) is a widely-used method of data encryption. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.

A*dvanced encryption* **s***tandard (AES)* is a symmetric 128-bit block data encryption technique. The terms AES and Rijndael are used interchangeably; there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

II. PROPOSED METHOD

In the proposed method the combination of Image Steganography and cryptography has been achieved by using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES is used to encrypt and decrypt the stego image. To protect the confidential information from the unauthorized users the encrypted stego image has been implemented in FPGA.In this work a prototype has developed for providing security to confidential information's. The following figure shows the operation of proposed method:

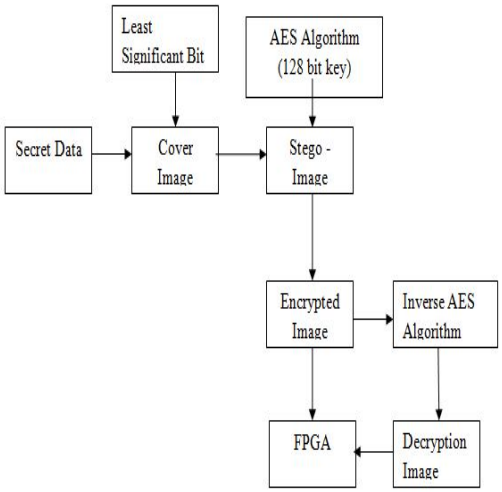

Figure:1 Block diagram of proposed method

A. AES Algorithm for Images

The AES algorithm is a symmetric key block cipher with a block length of 128 bits and a support for key lengths of 128,192 and 256 bits.AES algorithms is a symmetric key algorithm which means the same key is used for both encryption and decryption. Cipher text produced by the AES algorithm is same size as the plain text

Algorithm	Number of rounds(Nr)
AES-128	10
AES-192	12
AES-256	14

Table:1 AES keys and number of rounds

Manuscript received Nov 29, 2014

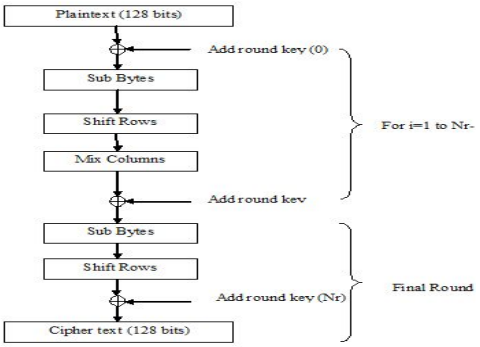

Figure: 2 AES algorithm encryption part

AES algorithm has following four transformations

- Add round key transformation
- Byte stub transformation
- Shift row transformation
- Mix column transformation

AES operates on 4x4 matrix of bytes termed as the State. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into final output cipher text. Each round consists of several processing steps including the one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plain text using the same encryption key. The figure 3.1 shows the operation of AES algorithm using 128-bit key

a. Addroundkey Transformation

The 128 bits of State array are bitwise XORed with the 128 bits of the round key (4 words of the expanded key).The operation is viewed as a column wise operation between the 4 bytes of the State array column and one word of the round key shown in figure

S(0,0)	S(0,1)	S(0,2)	S(0,3)
S(1,0)	S(1,1)	S(1,2)	S(1,3)
S(2,0)	S(2,1)	S(2,2)	S(2,3)
S(3,0)	S(3,1)	S(3,2)	S(3,3)

⊕

K0	K4	K8	K12
K1	K5	K9	K13
K2	K 6	K10	K14
K3	K7	K11	K15

3

Figure: 3 XOR operations between State and key word

b. Byte sub Transformation

It is a nonlinear byte substitution using a substitution table (s-box), which is constructed by multiplicative inverse and affine transformation. Byte Substitution controls each byte of state individually, with the input byte used to index a row and column in the lookup table to receive the substituted value. Figure 4 shows the operation of byte sub transformation

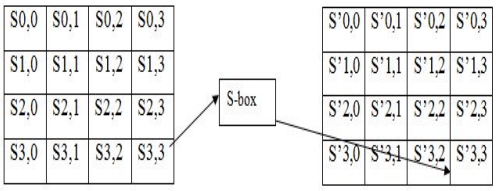

Figure:4 Sub-byte Operation

c. Key Expansion

The AES key expansion algorithm takes as input a 4-word (16-byte) key and gives a linear array of words, providing a 4-word round key for the initial Add round key stage and each of the 10 rounds of the cipher. It involves copying the key first in to the group of 4 words, and then constructing subsequent groups of 4 based on the values of the previous 4th words. The first word in each group of 4 gets "special treatment" with rotate + S-box + XOR constant on the previous word before XOR'ing the one from 4 back.

d. Shift rows Transformation

The first row of State array is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2- byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed. The operation of shift row is shown in figure 5;

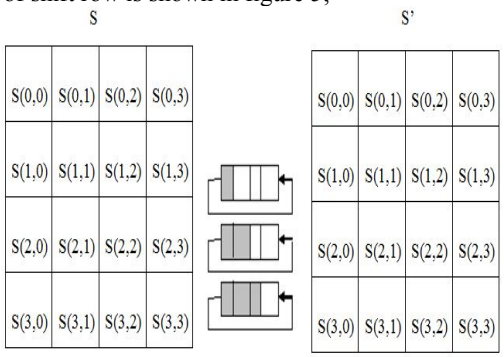

Figure: 5 Shift row operations

e. Mix columns Transformations

It operates on every column independently. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The substitution makes use of arithmetic over GF (28). It is designed as a matrix multiplication where each byte is treated as a polynomial in GF (28). The inverse used for decryption involves a different set of constants. This gives good mixing of the bytes within each column. Combined with the "shift rows" step provides good avalanche, that reflect within a few rounds, all output bits depend on all input bits. Figure 3.5 shows the operation mix column transformation

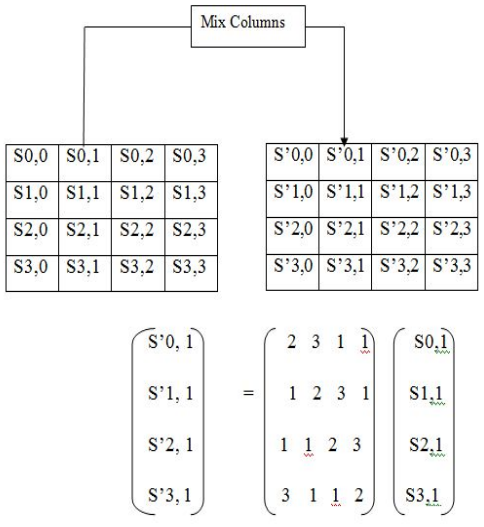

Figure: 6 Mix columns Operation

III. RESULT

For using 128 bit in AES algorithm has 10 rounds. Each round using the four transformations and the final round does not use the mix column operation. The following figure shows the final output of the encrypted image.

Input keys:

00000000000000010000001000000011000001000000010100000011100001000000010010000101000001011000001100001110100001111000001111

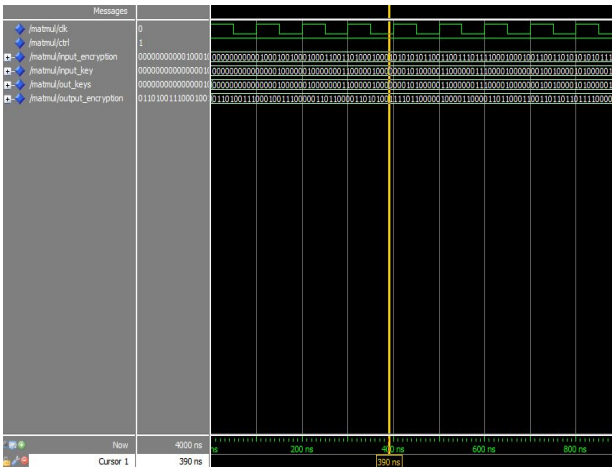

Figure: 7 Output of encrypted image

CONCLUSION

In this project, we proposed the combination of image steganography and cryptography has been achieved using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES is used to encrypt the stego image. Here the double encryption is used to encrypt the confidential information. The encrypted image has been implemented in FPGA.This method provides the most security for confidential information.

REFERENCES

[1.] Anil Kishor Saxena and Manoj Kumar Hemrajani (2013), 'Secured Steganography Approach Using AES', International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol.3, pp.185-192.

[2.] Abdullah Sharaf Alghamdi and Hanif Ullah(2010),'A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm' International Journal of Computer and Network Security,vol. 2, pp 78-84

[3.] Allin Christe.S, Vignesh.M and Kandaswamy.A (2011), 'An Efficient FPGA Implementation of MRI Image Filtering and Tumor Characterization Using Xilinx System Generator', International Journal of VLSI design & Communication Systems, vol 2, pp 95-109.

[4.] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda(2010), 'Image Encryption Using Advanced Hill Cipher Algorithm', ACEEE International Journal on Signal and Image Processing, Vol 1 ,pp 37-41

[5.] Cai-hong Liua, Jin-shui Jia and Zi-long Liua (2013), ' Implementation of DES Encryption Arithmetic based on FPGA', AASRI Conference on Parallel and Distributed Computing Systems pp 209-213

[6.] Hiral Rathod, Mahindra Singh Sisodia, Sanjay Kumar Sharma' Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)',International Journal of Computer Technology and Electronics Engineering (IJCTEE),vol 1,pp 7-13.

[7.] Jinu Elizabeth John and Ajay Daniel Peter (2013), 'FPGA based Secure Biomedical Image Transmission', International Journal of Computer Applications, vol 69, pp 39-43

[8.] Jagadeesha.D.H1, Mrs.Manjula.Y2, Dr.M.Z.Kurian3(2013), 'FPGA Implementation of X-Box Mapping For An Image Steganography Technique', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol 2,pp 2548-2554.

[9.] Khalil Challita and Hikmat Farhat (2011), 'Combining Steganography and Cryptography: New Directions', International Journal on New Computer Architectures and Their Applications (IJNCAA), pp-199-208.

[10.] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai (2012), 'A Secure Image Encryption Algorithm Based on Rubik's Cube Principle', Journal of Electrical and Computer Engineering, pp 1-13

[11.] Lakshmi.B, Kirubakaran.E and Prabakar.T.N (2010), 'Design and Implementation of FPGA based Dual Key Encryption', International Journal of Computer Applications, vol 3, pp21-27.

[12.] Mohamed M.A, Abou-Elsoud and Kamal El-din W.M (2012), ' Hardware Implementation of Multimedia Encryption Techniques Using FPGA',IJCSI International Journal of Computer Science Issues, Vol. 9,pp 290-300

[13.] Mohammad Ali Bani Younes and Aman Jantan (2008), 'Image Encryption Using Block-Based Transformation Algorithm', IAENG International Journal of Computer Science.

[14.] Neha. P. Raut1 , Prof.A.V.Gokhale2(2013), 'FPGA Implementation for Image Processing Algorithms Using Xilinx System Generator',IOSR Journal of VLSI and Signal Processing, vol 2,pp 26-3

[15.] Nithin, Anupkumar M Bongale, Hegde G.P (2013), 'Image Encryption based on FEAL algorithm', International Journal of Advances in Computer Science and Technology, vol 3, pp 14-20.

R.Vinoth was born in Tamilnadu, India in 1985. He received his Bachelors Degree, B.E- ECE from Mohamed Sathak Engg College, Keelakarai, Ramanathapuram, India, under the Anna University, Chennai, in the year 2007 and Masters Degree, M.E- VLSI Design from Muthayammal Engg College, Rasipuram, India under the Anna University of Technology, Coimbatore, in the year 2009 and Master of Business Administration, MBA-Human Resources Management from Periyar University, Salem in the year 2012. Currently he is pursuing Doctor of Philosophy, (Ph.D) in the area of VLSI Image Processing Under the Anna University, Chennai. His Area of Interest includes Image Processing, Signal Processing, VLSI design, etc. He is having more than 5 years of teaching experience in the Anna University Affiliated Engg Colleges. He published more than 10 research papers in International Journals and presented more than 10 papers in International and National Conferences. He is a Life Member of ISTE.

M.Balaji was born in Tamilnadu, India in 1988. He received his Bachelors Degree, B.E- ECE from M.P.Nachimuthu M.Jaganathan Engineering College, Erode India, under the Anna University, Chennai, in the year 2010 and Masters Degree, M.E- Embedded Systems from Sathyabama University, Chennai, in the year 2013. His Area of Interest includes Microprocessor, Image Processing, etc. He published more than 5 research papers in International Journals and presented more than 5 papers in International and National Conferences. He is a Life Member of ISTE.