Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 2, Issue 3, June 2018

A Highly Secure Algorithm to Encrypt a Data Using a Low Area AES Implementation

Shruthi H[1], Dr Bindu S[2]

1. Student, VLSI Design and Embedded Systems, M.Tech, BNMIT, Bengaluru.
2. Professor, Dept. Of ECE, BNMIT, Bengaluru.

Abstract: In modern world information security plays an important role in data transfer, sharing and data storage. It is important to secure the information so that nobody can hack the personal information. Medical images, surveillance images, personal photos, video recordings need to be well protected, transmission and storage of these images in cloud environment is very challenging. Media images and video recordings must be highly encrypted so that loss of information during encryption and decryption process is avoided. The different architectures for Mix Column approach and the one with low area will be implemented further in AES. Also, the conventional Visual Cryptography techniques consumes more channel bandwidth, since each pixel gets divided into two pixels with the same share. Thus, with an intention of higher security, AES will be merged with a novel visual cryptographic technique.

Keywords: secret sharing, Visual Cryptography, Unauthorized users.

I. INTRODUCTION

In encryption the information is referred to as plain text, and this plain text is encrypted using an encryption algorithm a cipher, generating a cipher text which can be read only if it is decrypted. There are different types of encryption algorithms, they are Advance Encryption Standard (AES), Data Encryption Standard(DES), Triple DES, etc., AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. 128 bit AES will be implemented as part of the project work. In this project the authentication to the text message such as user name and password are converted into predefined images with the pixel intensity of 4*4. Later the pixels are shared between the user name and password; one round of AES encryption is done. Operations such as Add Round Key, Substitution Bytes, Shift Rows and Mix columns are performed on the images. Later the images are split into shares using Visual Cryptography and transmit the images, the transmitted images are encrypted and very difficult to read the data by the unknown users. The data can be read only if it is decrypted. The different architectures for Mix Column approach and the one with low area AES will be implemented further. The conventional Visual Cryptography techniques consume more channel bandwidth, since each pixel gets divided into two pixels with the same share. As the text is converted into image the loss of information during transmission and storage is reduced and the information is more secured compared to other encryption methods.

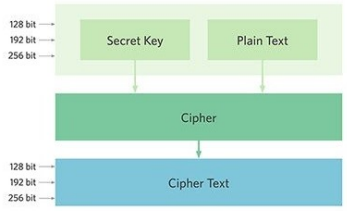

Fig 1. AES Design

The different architectures for Mix Column approach and the one with low area will be implemented further in AES. Also, the conventional Visual Cryptography techniques consumes more channel bandwidth, since each pixel gets divided into two pixels with the same share. Thus, with an intention of higher security, AES will be merged with a novel visual cryptographic technique.

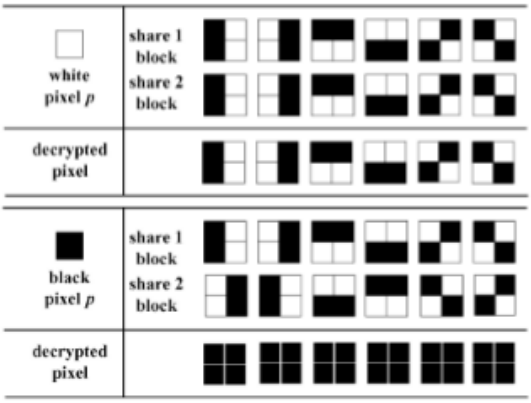

Fig 2. Visual Cryptography

Visual Cryptographic Scheme (VCS) is a technique of secret sharing of Binary image. In a k-out-of-n scheme of VCS, a secret binary image is cryptographically encoded into n shares of random binary patterns. The shares are Xeroxed onto transparencies respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any transparencies together. The secret cannot be decoded by any k−1 or fewer participants, even if infinite computational power is available to them. Naor and Shamir proposed a VCS which serves as a basic model for many applications. Apart from the information hiding, there are many applications of visual cryptography, they are visual authentication and identification, biometric privacy, watermarking , general access structures etc. Due

to advancements in the field of technology in the recent years, even AES hasn't escaped from the threat of hacking. Thus, a necessity to devise a more secure algorithm to encrypt the data arises. With an intention of further enhancing the security levels, a highly secure algorithm to encrypt data using a low area AES implementation and combined with visual cryptography approach on FPGA will be explored.

II. RELATED WORKS

Praveen kumar B and Sabitha S in their paper "User Authentication using Visual Cryptography" proposed a new protocol to authenticate user to the server. The concept of visual cryptographic scheme can be used to create user authentication despite of its limitations. Previously established communication channel is required, also this scheme can be used to create a secured channel for encryption. The computing power for the system is reduced compared to other existing systems.

Quist-Aphetsi Kester, Laurant Nana and Anca Christine Pascu explained that the encryption of the stored images in the cloud for the generation of shared secret key and used in the RGB pixel shuffling and displacement algorithm. There is no loss of image quality because there was no pixel expansion and the method was proposed in the paper "A Novel Cryptographic Encryption technique for Securing Digital Images in the cloud using AES and RGB Pixel Displacement". The total size of the image was not changed during encryption and decryption process.

M. Naor and A. Shamir proposed a simple version of secret sharing of collection of black and white pixels and they are separately handled. Each share is a collection of m black pixels and white subpixels in the paper "visual cryptography". The information can be decoded without any computations of cryptography and it is very simple to implement.

III. METHODOLOGY

The text entered and the password will be converted into images, one round of AES encryption is performed for the images. Operations such as Add Round Key, Substitution Bytes, Shift Rows and Mix columns are performed on the images. Later the images are split into shares using Visual Cryptography and transmit the images, the transmitted images are encrypted and very difficult to read the data by the unknown users. The data can be read only if it is decrypted.

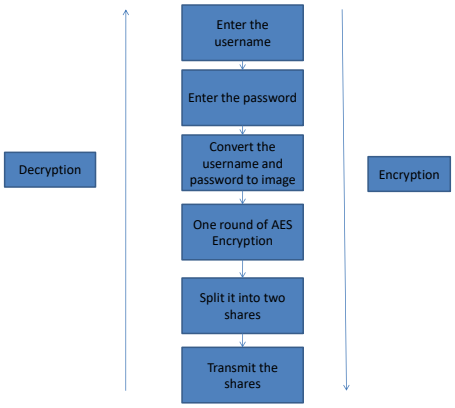

Fig 3. Process of Encryption or Decryption

A. Add Round Key

In Add Round Key operation, each sub key is combined with the state which is of the same size as the state. The sub key is bitwise EX-OR with the state.

B. Substitution Bytes

The 512-bits input plaintext is organized in array of 64- bytes and is substituted by values obtained from Substitution boxes. This is done to achieve more security according to diffusion-confusion Shannon's principles for cryptographic algorithms design. To overcome the overhead of the huge data size used (512- bits), the Substitution boxes are implemented as lookup tables, and accessed in parallel. After the original 512-bit data is substituted with values from the S-boxes, the rows of the resulting matrix are shifted in a process called Shift Row transformation.

The sbox is generated by using the multiplicative inverse of a given number in Rijndael's finite field. The matrix multiplication can be calculated by the following algorithm.

1. Let S be the 8 bit unsigned variable input number
2. Let the answer be 0
3. For 5 times
   - XOR answer with S
   - Rotate S by one bit to the left

After the matrix multiplication is done, XOR the value by the decimal number 99, it will generate the above Sbox in hexadecimal notation. Sbox is used in encryption algorithm.

C. Shift Rows

In this part the bytes in each row in the input data matrix will be rotated left. The number of left rotations is not the same in each row, and it can be determined by the row number. For example, row number zero is not shifted, the first row is shifted by one byte, and so on. Now, and after the rows of the input data are rotated left by different offsets, an operation must be applied to the columns of the data matrix.

$$A = \begin{bmatrix} a_{(0,0)} & a_{(0,1)} & a_{(0,2)} & a_{(0,3)} \\ a_{(1,0)} & a_{(1,1)} & a_{(1,2)} & a_{(1,3)} \\ a_{(2,0)} & a_{(2,1)} & a_{(2,2)} & a_{(2,3)} \\ a_{(3,0)} & a_{(3,1)} & a_{(3,2)} & a_{(3,3)} \end{bmatrix}$$

$$A' = \begin{bmatrix} a_{(0,0)} & a_{(0,1)} & a_{(0,2)} & a_{(0,3)} \\ a_{(1,1)} & a_{(1,2)} & a_{(1,3)} & a_{(1,0)} \\ a_{(2,2)} & a_{(2,3)} & a_{(2,0)} & a_{(2,1)} \\ a_{(3,3)} & a_{(3,0)} & a_{(3,1)} & a_{(3,2)} \end{bmatrix}$$

Fig 4. Shift Rows Technique

D. Mix Column approach

The Mix Column transformation multiplies the columns of the data matrix by a pre-defined matrix. The AES-512 and original AES process the data in bytes basis. Each byte is considered as polynomials over GF (2^8) with 8 terms. To explain how the Mix Column works, we

have to explain the concept of polynomials over GF(2 n) in general and for GF (2 8) as example when n=8. A binary extension field element Y (x) is a polynomial of degree less than n and greater than -1, (i.e. Y (x) 0), and has coefficients in GF(2). The polynomial basis is one representation for the elements of GF(2 n). The addition in GF(2 n) corresponds to a polynomial addition, which is done as a bitwise logic exclusive OR operation between the two bit vectors being added. An irreducible field polynomial p(x) of degree n is used to reduce intermediate results in GF(2 n). In other words, the polynomials are reduced mod p(x) through long division operation to keep their degree less than n. The Mix Column operation multiplies the columns in the data matrix with a fixed polynomial of a(x).

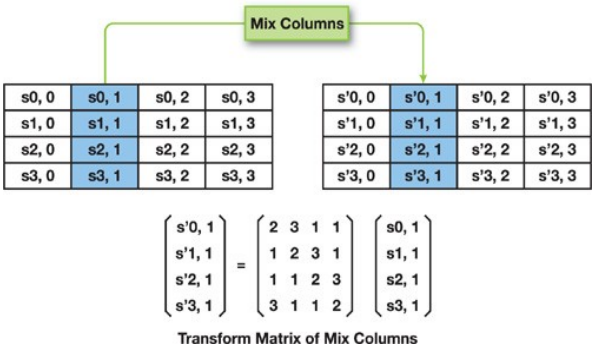

Fig 5. Mix Column Technique

IV. PROPOSED SYSTEM

In the proposed system, the mix column approach is done using logarithmic and antilogarithmic table . the logarithmic value of shift row output is ex-or with the corresponding key value, the ex-or value is viewed in the antilogarithmic table, if the value is more than decimal 255, the answer is subtracted by 255 and ex-or with decimal 1. The procedure is called as Finite Field or Galois Field.

A. Galois Field

Galois Field, named after Evariste Galois, also known as finite field, refers to a field in which there exists finitely many elements. Galois field is particularly useful in translating the computer data which are represented in binary forms. That is, computer data consist of the numbers which are the combinations of 0's and 1's, whereas the components of Galois field consists of two elements. Representing data in the form vector in a Galois Field allows the mathematical operations to acquire the data easily and effectively.

The elements in a Galoi's field is defined as,

$$\begin{aligned} gf(p^n) \;=\; & (0,1,2,\ldots,p-1)\cup \\ & (p,p+1,p+2,\ldots,p+p-1)\cup \\ & (p^2,p^2+1,p^2+2,\ldots,p^2+p-1)\cup\ldots\cup \\ & (p^{n-1},p^{n-1}+1,p^{n-1}+2,\ldots,p^{n-1}+p-1) \end{aligned}$$

V. CONCLUSION

The different architectures for Mix Column approach and the one with low area AES will be implemented further. The conventional Visual Cryptography techniques consume more channel bandwidth, since each pixel gets divided into two pixels with the same share. As the text is converted into image the loss of information during transmission and storage is reduced and the information is more secured compared to other encryption methods.

Table 1. Conventional Mix Column design summary

Logic utilization	Used	Available	Utilization	Delay
No. of slices	4441	960	462%	18.870ns
No. Of 4 input LUT's	8800	1920	458%	
No. Of bonded IOB's	256	108	237%	

Table 2. Proposed Mix Column design summary

Logic utilization	Used	Available	Utilization	Delay
No. of slices	134	960	13%	7.232ns
No. Of 4 input LUT's	**252**	**1920**	**13%**	
No. Of bonded IOB's	**256**	**108**	**237%**	

REFERENCES

[1] Praveen kumar B and Sabitha S, "User Authentication using Visual Cryptography", Nov 2015.

[2] Quist-Aphetsi Kester, Laurant Nana and Anca Christine Pascu, "A Novel Cryptographic Encryption technique for Securing Digital Images in the cloud using AES and RGB Pixel Displacement", 2013 European Modelling.

[3] M. Naor and A. Shamir, "Visual cryptography", in: Advances in Cryptology (Eurprocrypt94), Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 1-12

[4] Goel, Bhagat and Katankar, "Authentication Framework Using Visual Cryptography" in URET, Volume: 02 Issue: 11, Nov-2013, pp. 271-274

[5] Divya James, Mintu Philip, "A Novel Phishing framework based on Visual Cryptography" in International Journal of Distributed and Parallel Systems Vol.3, No.1, January 2012, pp. 207-218

[6] C. N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognit. Lett., vol. 25,2004, pp. 481-494

[7] Xiang Li, Jing Liu, Jun Han, and Qian Zhang, 2011. "The architecture design of micro-learning platform based on cloud computing". In proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11). ACM, New York, NY, USA, 80-83. DOI-10.1145/2071639.2071659

[8] Tuylset.al, "XOR-based Visual Cryptography Schemes, in Designs, Codes and Cryptography", 37, 2005, pp. 169-186

[9] Moni Naor and Benny Pinkas. "Visual authentication and identication". In Lecture Notes in Computer Science, Springer-Verlag, 1997, pp. 322-336

[10] Kunal Sain, Mardula Sharma, Suneeta Agarwal, ASPS: "An Authentication Scheme using Pre-formed Visual Cryptographic Shares", SIN 12, 2012, pp. 25 – 27

[11] Sabahi, F., "Cloud computing security threats and response", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, Vol., no., pp. 245,249, 27-29 May 2011 doi: 10.1109/ICCSN.2011.6014715

[12] Diego Perez-Botero, Jakub Szefer, and Ruby B. Lee. 2013. "Characterizing hypervisor vulnerabalities in cloud computing servers". In Proceedings of the 2013 International workshop on security in cloud computing (Cloud Computing' 13), ACM, New York, NY, USA, 3-10. DOI-10.1145/2484402.2484406.

