International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Optimized S-box and Mix-Columns for AES Architecture for live IP video Encryption and Decryption by Key Generation Through face Recognition

Jayanthi K Murthy, Sneha N S

Abstract - This paper proposes an AES based Encryption and Decryption of a live IP video used for security in surveillance systems. Here, the key is generated based on neural networks techniques for facial recognition. Principal component analysis and Eigen vector algorithms are used to extract biometric facial features which are used to train the neural network. At the receiver side, the original video plays only if the user is authenticated or else it plays an encrypted video. This work proposes an AES architecture based on optimizing timing in terms of adding inner and outer pipeline registers for each round and Key Expansions. Further by optimizing the Crypto Multiplication for Mix columns via LUT based approach aid in further optimization in terms of timing. LUT and Pipelined based implementation techniques are optimal for FPGA based implementations. ROM table and pipelining are the two techniques used to implement AES. Result indicates that with the combination of pipelined architecture and Distributed/Split LUT-Pipelined techniques, the encryption has higher throughput and speed.

Index Terms— AES, Look up table, LUT Pipeline architecture, principal component analysis.

I. INTRODUCTION

With the current day technological advancements in the field of communication, there is an ever increasing threat to data due to cryptographic attacks. Due totheadvancement in internet applications, a lot of critical data is shared by the user which needs to be protected from illegal use by the hackers. So the never changing attribute which is of utmost prominence is the protection of data. With the increasing inclination towards information security, there was even more predilection in regards to security algorithms which acts as a barricade between the hacker and the critical data. This resulted in plenty of security algorithms which evolved out of the cause each gaining its own appreciation at different fields of use. The US government has standardize a cryptographic algorithm which will be used universally by them called Advanced Encryption Standards (AES) [1]. The NIST has selected AES as the standard for giving security to the data.

Manuscript published on 30 August 2019.
***Correspondence Author(s)
Dr. Jayanthi K Murthy, Associate Professor in Department of Electronics and Communication, BMS College of Engineering, Bangalore, India
Sneha N S, Department of Electronics and Communication, BMS College of Engineering, Bengaluru, India.

Therefore, AES is used for giving the security and it can provide both software and hardware reconfigurability for many applications with good performance, flexibility, and efficiency[2].This paper proposes anew efficient method of AES implementation with improved speed and the key generation through facial recognition and neural networks. The main purpose of choosing facial recognition is to overcome the drawbacks of other securitymethodslike password and biometric techniques like iris, fingerprint. The passwords can be easily stolen, tampered and detected by existing software.Iris recognition too has a disadvantage as it could even detect artificial iris, fingerprint straps can identify a wrong face. Face recognition can be performed in two ways: Face identification and Face verification. Face identification refers one to many matches while Face verification refers one to one matching. The modules present in the recognition process are detection, alignment, feature extraction, and matching. The face has many biological biometrics that includes the distance between eyes, the height of the nose, shape of eyes, shape of the head and many more that identifies individuals uniquely[3]. The booming technology for object recognition and detection, action recognition and face recognition, is the neural networks techniques. Face recognition technology has varied applications in the fields of banking (password service), forensics, national security etc [4]. A neural network consists of many interconnected neurons. Each of the neurons in a network are assigned with weights and they can hold biological features of the face. So, by adding more biological features of the face to the neural network the accuracy can be increased. Each biological features in the face are eigenfaces. The eigenfaces are extracted by principal component analysis and these will be coded in neural network. By the combination of facial recognition and neural networks the AES accuracy can be enhanced [5].

II. ADVANCED ENCRYPTION STANDARD

AES algorithmic rule could be a radially symmetrical block cipher that may cipher (encipher)and decrypt (decipher) the information. Encryption converts knowledge to associate in nursing unintelligible kind referred to as cipher-text. The plaintext is obtained from the decryption of the ciphertext. The plaintext and cipher text output for the AES algorithms is each of 128 bits. The cipher key is chosen to be a sequence of 128, 192 or 256 bits (4, 6, 8 words). Cipher key size decides the number of encryption rounds.

In this work 128 bits of cipher key with 10 rounds has been chosen. AES algorithm involves four step, each step performs operations on 4x4 array matrix. Each byte is called a state and denoted as $S_{n,m}$, n and m are rows and columns respectively. Each state has in it the plain text initially. Substitutions and permutations are done on these states to produce the cipher. Once this is done the result is copied to ciphertext as output. This is described in the Fig1.

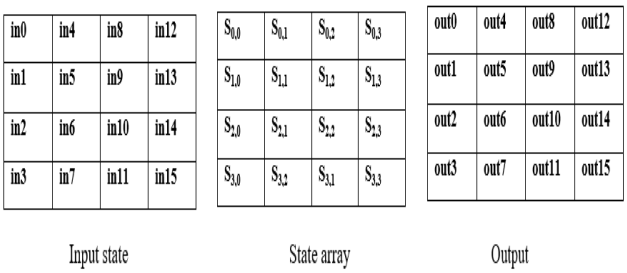

Fig 1. State Results

Initially the input matrix array is copied into the State as shown in equation 1

$$S[n,m] = in[n + 4m] \quad \text{for } 0 \le n < 4 \text{ and } 0 \le m < 4 \quad (1)$$

The output array State is derived from the top of the cipher as shown in equation 2

$$Out[n+4m] = S[n,m] \quad \text{for } 0 \le n < 4 \text{ and } 0 \le m < 4 \quad (2)$$

This algorithm constituted of ten rounds and each round has four transformations namely SubBytes, ShiftRows, MixColumns, and AddRoundKey. For each round 128-bit input and 128-bit key has to be given. This results in 128-bit ciphertext as output. At start of the encryption algorithm there is an Addround key stage after which is nine round of operations. Each round consists of above four transformation except the last round, the last round has no MixColumn transformation. Decryption is the reverse operation of encryption as shown in Fig 2. The S-box is a lookup table that consists of 16×16 matrix of byte values. Look-up table (S-box), given in equation (3).

The S-Box is predetermined for using it in the algorithm.

$$S_{n,m} = S[b_{n,m}] \quad (3)$$

A. *SubBytes*

The substitution operation done on each byte of the state is called SubBytes. S-box is an important part of SubByte transformation. In the process of mapping each element of a State with the substituted alternative taken from S-box a non-linearity is introduced for its next state. The SubBytes substitute each byte in state array with the element in S-Box as shown in equation (3).

B. *ShiftRows*

ShiftRows is a cyclic modification that is applied to each row of the state. ShiftRows transformation refers to cyclorotation of bytes in row-wise manner except the first row over state array. The n^{th} row will be shifted by (n-1) byte shift.

C. *MixColumns*

Mix column transformation is done by operating on column individually. Each column of the state matrix is multiplied with the standard GF (2^8) matrix using polynomial ($x^8+x^4+x^3+x+1$) which is equal to the XOR operation.

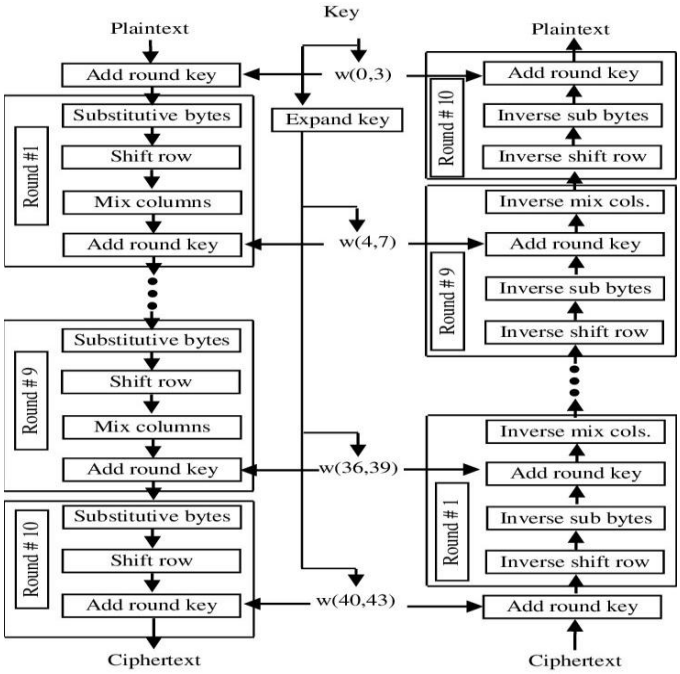

Fig 2. Steps involved in AES Encryption and Decryption

D. *AddRoundKey*

In this stage the 128 bits of the state are bitwise XOR - ed with 128 bits of the round key. The operation will be observed as a column wise process between the 4 bytes of a state column and one word of the round key. This change is simple which is not only efficient but will also affect every bit of state.

E. *Neural networks and facial recognition*

A neural network has layered structure and the structure of neurons in the brain can be given as its analogy, with layers of connected nodes. Neuron is a basic element of a neural network which contains a single bit of information. Neural network breakdowns the input into layers of many neurons and it learns from data sets and gets trained to identify patterns, data classification and predict future events. Its behavior depends upon the strength and weight of the neurons. The weights that are assigned to the neurons, are adjusted automatically by the algorithm in the trainings phase because of the specified learning.This is repeated until the desired task is predicted. Neural networks are ideal for face recognition. Facial recognition is a biometric technique used for identifying the user's face to unlock some functionality. When compared to the other biometric techniques, the facial recognition is non-contact in nature and requires less interaction with the user while capturingthe images.

Retrieval Number: J11060881019/19©BEIESP
DOI: 10.35940/ijitee.J1106.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

As a consequence, no user can successfully duplicate any other person. Facial recognition is mostly used for security purposes as it is a cheap technology with less processing involved, unlike in other biometric techniques.

III. LITERATURE SURVEY

Authors in the paper[5] have explained the AES implementation by the pipelined architecture for all 10 rounds of encryption and decryption, and at the end of each round, they placed 5 registers which result in the increase ofthe speed of operation and which will be operating at 254.453 MHz.Optimization techniques has been applied on each AES transformation. For efficient utilization of the resources available, they have used BRAM with multiplexing inverse method in order to implement the SubBytes. This includes dividing the 128- bit input into 4 words each consisting of 32- bits. They have implemented this by using mux, counters, dual port RAM, and TDM. The bit basher is a bit converter which can be able to convert 128 to 32 bits and vice versa by selecting the input wires. The bit basher is used to extract 8 bits from 32-bits. This 8 bit is given as input for shift rows. The 8-bit selection is done by simply selecting the wires using mux. The shifting and addition methods are used for implementing the MixColumn. In order to generate the round key, the bit basher is used to convert the 128-bits to 8 bits. The 4th column of the key matrix is used to generate the 1st column of the round key using SubBytes. Then the rotate and xor operations are performed on SubBytes and the1st column of the key respectively.Divya Mangala B. S and Prajwla N.B in paper [6] explained a methodology by using eigenfaces for facial recognition of humans. For the eigenfaces, they have calculated the Euclidean distance. The principal component analysis is used for facial recognition. They have detected facial expressions like sad, surprised, neutral, and angry. They have done this in 3 steps, the first stage is face recognition, where the RGB image is converted into a grayscale image and resized. Then using eigenvalue and eigenvector covariance matrix was formed and Euclidean distance calculated. The second stage is feature extraction in which they are some facial features by PCA which results in the reduction of the dimension of the image. At last they have done the classification of images. The authors in paper [7] implemented a face recognition on FPGA using neural networks. They used ORL dataset and proposed an architecture that is called Levenberg-Marquardt feed-forward training method on neural networks and implemented on VIRTEX-7 FPGA platform that gives enhanced recognition rate and high performance. Feature extraction is done by histogram algorithms and neural network is used for classification. Swinder Kaur, Prof. RenuVig in paper [8] has explained the implementation of AES on FPGA which works at a frequency of 119.954 MHz using VHDL. As FPGAs are reconfigurable they can give more flexibility, high speed and physical security for the cryptographic algorithms. The author concludes that by balancing the combinational path and the critical path leading to an increase in the speed of the design. They have done this by placing the pipelined register after each round AES transformation.

IV. IMPLEMENTATION DETAILS

The proposed architecture is based on optimizing timing in terms of adding inner and outer pipeline registers for each round and Key Expansions. Further by optimizing the Crypto Multiplication for Mix columns via LUT based approach aid in further optimization in terms of timing. Implementation techniques like LUT and Pipelined are optimal for FPGA based implementations. With the use of fully pipelined architecture and Distributed/Split LUT-Pipelined techniques, the throughput and speed of the encryption are increased tremendously. The optimization on S-box and MixColumns has been done which comprises of Pipelined and LUT based implementation of high-speed AES algorithm using Verilog HDL.

A. S-BOX Optimization using Distributed Logic

The SubBytes and the Addround key module in the AES system utilizes S-Box for its operations. Input to S-Box is 8 bits which act as address and output is the substituted value. The depth of S-Box is 256 bits and width is 8 bits, hence the access time for the 8 bits is large, this can be broken down into 2 bits or 4 bits addressing as shown in the below Fig 3. Also, pipeline registers can be placed at optimal locations which will increase its throughput.

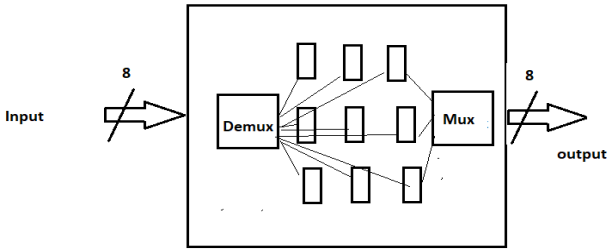

Fig 3. Optimized S-Box

B. MixColumns Module Optimization

The other important block of AES design is Mix Columns, whichisalso timing critical. It performs modulus multiplication as per crypto arithmetic, which has crypto multiplier and XOR blocks. Fig4 shows the optimized implementation of mod mul2 and mod3 engine which is used for optimization. This is further improved by optimizing the shifter module and inserting pipeline.

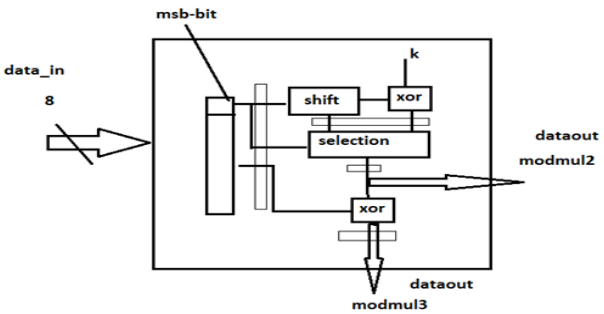

Fig 4. Optimized Mix Coulmns

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. SYNTHESIS RESULTS

The Artix7 Part No: xc7a100t-3csg324 FPGA family is used for implementation. The design has been implemented using Vivado 14.4 tool, Xilinx ISE is used for simulation and synthesis.It operates on 317.040MHz frequency. Architecture without pipelined and with pipelined techniques named as AES_Base and Optimized AES respectively are implemented.The frequency of operation results of AES_Base and optimized AES implementation is shown in table 1.

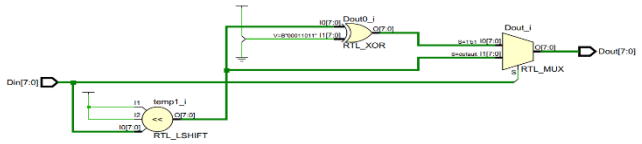

Fig5. Mix Column schematic

Fig 6. Top level encryption and decryption

Architecture type	AES_Base	Optimized AES
Maximum Frequency	44.680MHz	317.040MHz
Minimum period	22.381ns	3.154ns
Minimum input arrival time before clock	22.132ns	18.291ns
Maximum output required time after clock	0.640ns	0.640ns

Table 1. Frequency table

Above are the timing results for AES_Baseand Optimized AES. As can be seen, there is a 70% of improvement in the speed with our techniques. The advantaged of this architecture is it can work under high-speed design applications which require data to be encrypted.

A. Comparison with previous implementations

Device utilization summary (estimated value)			
Logic utilization	Used	available	utilization
Number of slice registers	384	126800	0%
Number of slice LUT's	9392	63400	14%
Number of fully used LUT-FF pairs	208	9568	2%
Number of bonded IOBs	385	210	183%
Number of BUFG/BUFGCTRL/BUFHCEs	1	128	0%

Fig 7. AES _Base architecture

Device utilization summary (estimated value)			
Logic utilization	Used	available	utilization
Number of slice registers	2816	126800	2%
Number of slice LUT's	10544	63400	16%
Number of fully used LUT-FF pairs	2598	10762	24%
Number of bonded IOBs	257	210	122%
Number of BUFG/BUFGCTRL/BUFHCEs	1	128	0%

Fig 8. Optimized AES architecture (optimized S-Box , Mux column & pipelining)

From the device utilization summary in Fig 7 and 8 we can say that our optimized implementation occupies 2816 slice registers out of 126800 (2%) which will be less than as reported in [5] [7] and our design is working at high frequency as compared to the previous implementations [5], [7]. This show that the architecture proposed will give better speed and will offer greater operating frequency when compared to high level language implementations.

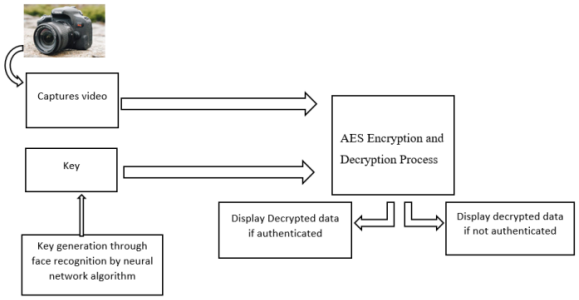

Fig 9. Implementation of AES by generating key through face recognition

VI. CONCLUSION

The entire AES architecture was pipelined at outer stages to get the optimized speed. Pipelining of registers breaks the timing critical path and hence aids in increased throughout. From the above observation, it can be concluded that the optimized architecture works well to increase the speed and throughput. Along with the HDL model for AES, An application using AES cryptography and key generation using facial recognition system was built to showcase its real-time application. Future work is to optimize the area.

REFERENCES

1. William Stallings, Cryptography and Network Security- Principles and Practice, third edition, Pearson Education.
2. Xinmiao Zhang, Keshab K. Parhi,"High-Speed VLSI Architectures for the AES Algorithm", IEEE transactions on very large scale integration (vlsi) systems, vol. 12, no. 9, september 2004.
3. R.Saranya1, S.Prabhu "Image Encryption using RSA Algorithm with Biometric Recognition", International Journal of Engineering and Computer Science ISSN: 2319-7242.
4. Vinita Bandiwad, Bhanu Tekwani, "Face Recognition and Detection using Neural Networks", International Conference on Trends in Electronics and Informatics ICEI 2017, 978-1-5090-4257-9/17©2017 IEEE.
5. S. M. Umar Talha, Mir Asif "Efficient Advance Encryption Standard (AES) Implementation on FPGA Using Xilinx System Generator", IEEE 2016 6th International Conference on Intelligent and Advanced Systems (ICIAS).
6. Divya Mangala, B.S and Prajwala N.B, "Facial Expression Recognition by Calculating Euclidian Distance for Eigen Faces using PCA", IEEE International Conference on Communication and Signal Processing, April 3-5, 2018, India.
7. M Tousif Ahmed, Sanjay Sinha, "Design and Development of Efficient Face Recognition Architecture using Neural Network on FPGA", Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018) IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN:978-1-5386-2842-3.

8. Swinder Kaur, Prof. RenuVig, "Efficient Implementation of AES Algorithm in FPGA Device", IEEE International Conference on Computational Intelligence and Multimedia Applications 2017.

AUTHORS PROFILE

Dr. Jayanthi K Murthy is presently serving as an Associate Professor in Department of Electronics and Communication, BMS College of Engineering, Bangalore, India with 24years of experience. She has authored more than 18 research papers in international conferences and repute journals.

Sneha N S is currently pursuing her final year M. Tech in Electronics from Dept. of Electronics and Communication, BMS College of Engineering, Bengaluru, India. She received her Bachelor of engineering in Electronics and Communication from Visweswaraya Technological University, Belgaum, India. Her current research interests include VLSI Design, Deep Learning and NanoTechnology.