A VLSI Hardware Architecture Implementation of Security System Using Encryption Algorithm

Ms.Ashwini Y. Mate, Prof.Brig.R.M. Khaire

Abstract— The paper proposed implementation of a hardware tectonics for video security system. The real time video camera will modulate the digital media system on chip with FPGA. The video processing and security function will be performed independently with FPGA having a novel security module. The real time video signal data is encrypted by associated AES Modulo algorithm rule and projected. Security module will code the weak video knowledge with a minimum operating frequency up to 50MHz. The paper objects that the encryption methodology enlists a high video streaming security system by using less hardware components. We have selected Sparten3EDK for implementation of AES algorithm through a softcore processor. Research proposes AES encryption and decryption algorithm with respect to key length of 256 bit. The Paper also gives comparative analysis between AES encryption for key length of 256 and 512 with respect to time.

Index Terms— AES, Decryption, EDK, Encryption, FPGA, JTAG.

1 INTRODUCTION

With rapid development in technicalities, more and more multimedia information are now been created and transmitted in various field that may contain some sensitive data that can only be accessed by specific user. Therefore security of such sensitive data and its transition has become an important issue. As the technology and popularity of wireless system such as CDMA, WLAN portable internet there has been considerable improvement in the area of multimedia streaming over a wireless network. Video communication is becoming increasingly important of wireless infrastructure. Thus encryption of useful video data for secure video communication becomes important. Therefore, it is important to build an embedded system with skilled design for hardware encryption module to achieve video encryption. M. Abomhara et al.[1] propose different encryption techniques using different algorithm.

Numerous papers have introduced encryption method for compressed visual signal data processing [2]-[6]. In order to emaciate computational loading of encrypted video, compressed video data should be considered. Using video compressed technique is limited in most of the application area such as image processing in medical field since it causes loss of partial information. The compression technique may not be used in most of the application as video property may not be admissible in transmission due to loss of information. The security of sensitive data is one of the most important needs for data communication. Symmetric key cryptography uses AES algorithm as one of the efficient method for encryption of both software and hardware implementation [7].

- ***Ms.Ashwini Mate,*** *M.Tech Electronics, Bharati Vidyapeeth College of Engineering, Pune, India, 7756050112 (e-mail: ashu78910mate@gmail.com).*
- ***Prof. R. M. Khaire****, Head of department in Electronics and Telecommunication Engineering, Bharati Vidyapeeth college of Engineering, Pune, India, (e-mail: rmkhaire@gmail.com).*

Recovery of original data from encrypted file is defined by decryption. FPGA is considered as one of the major platform for high speed embedded application performance and it also provides logic for reconfiguration with an improved clock frequency and design capabilities. FPGA provide performance gain in much application areas especially for processing of video signal. A Xilinx tool offers an efficient and effortless for transition between PC based model in Simulink and actual time FPGA based hardware architecture. Also implementation of a complete video system on FPGA fabric is done by Xilinx Embedded Development Kit(EDK) tool using hardware and software codesign method.

The paper proposes hardware architecture implementation of video security system using AES encryption algorithm. The main contribution of the paper can be divided into following parts:

i) At first we perform multiple process tasks on real time video using MATLAB for creating header file
ii) Next we establish communication link between real time video system and FPGA system running encryption and decryption of video through JTAG communication port

Thus a novel real time video security module using FPGA with low cost is proposed that applies efficient implementation of AES algorithm presented by *Vikas Kumar et al* [8].

The paper can be consolidated as follows. Section 2 gives implementation flow for proposed method. Section 3 describes an efficient design methodology for preprocessing of real time video signal for video to frame conversion. Section 4 put explains the AES encryption and decryption method, also gives diagrammatical view for video streaming security system. The AES cipher functions and key expansion module is also covered in this section. The implemented results and analysis is covered in section 5. The conclusion and remark are presented

in section 6.

2 IMPLEMENTATION FLOW

Symmetric encryption technique is used in order to encrypt the pixel value. Implementation can be classified into two parts 1) Preprocessing of video signal 2) Hardware deployment

Preprocessing of video signal

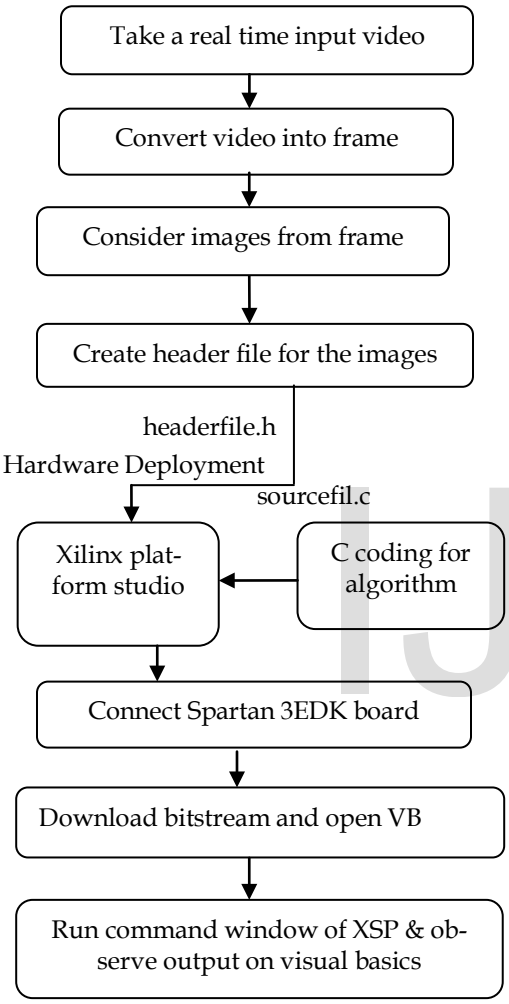

Figure 1: Implementation flow for Encryption and Decryption

3 PROCESSING OF REAL TIME VIDEO SIGNAL FOR VIDEO TO FRAME CONVERSION

The extraction of important data from video is done in order to process the data efficiently and reduce the transfer stress of the network. Segmentation is one the most important method for reduction of data carried by video signal. This section involves method for preprocessing of real time video which includes detection of frames from input video file.

The video to frame detection can be done by using much software available in market. However this paper propose use of MATLAB software to get optimized graphical output for user interaction also plotting the data easily and changing size, scale colors by using graphical interactive tools. Input video file can be taken in any format such as .avi, .flv, .3gp, .3g2 etc. The input video file is then extracted to frames using MATLAB commands for video to frame conversion [9]. Frame extraction plays a vital role in much application area such as CC camera, segmentation, Shot detection, Content based video retrieval etc. The study of characteristics of frames and analysis of properties of video by video to frame conversion is proposed by *Punith Kumar M B et al* [10].

In real time system data is commonly extracted in frame based formats. Acquisition of hardware data often operates by collecting a large number of signals sampled at high rate. The extracted frames are saved as images in project wizard. Header file is created for each frame.

4 DIGITAL VIDEO ENCRYPTION SCHEME

Figure 2 shows block for encryption and decryption of video signal.

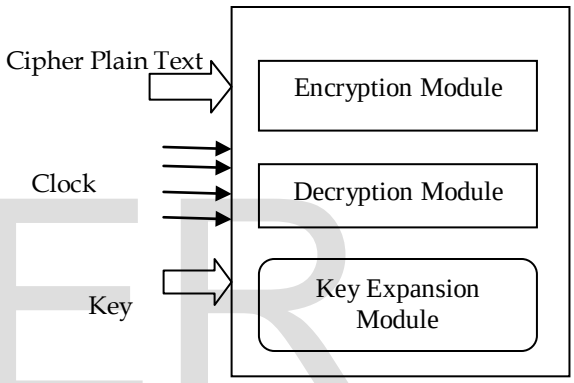

Figure 2. Encryption and decryption Module

4.1 AES Encryption Method

The AES is a block cipher depends on symmetric key algorithm for encryption and decryption [11]. Key length of 128bit, 192bit, 256bit is defined. The proposed method uses implementation of a stipulated size of 256bit. Fig.3 shows block of the propose AES encryption and decryption method for video running security system. The module consists of 64 bit architecture that process 4 byte data at one clock cycle. The AES algorithm composes of three main parts: cipher, key expansion module and inverse cipher. The number AES parameter depends on length of key. For key size of 128 bit the number of round is 10 whereas it is 12 and 14 for 192 and 256bit respectively [12].

The encryption algorithm start with add round key phase and is followed by 13 rounds of four phase which 14 round of three phases which can be given as:

1. Sub Bytes
2. Shift Row
3. Mix Columns
4. Add Round Key

The paper gives method that consists of generation of round key and storing it in block RAM. The generation of

round key utilizes same subbyte transformation which is used in encryption class.

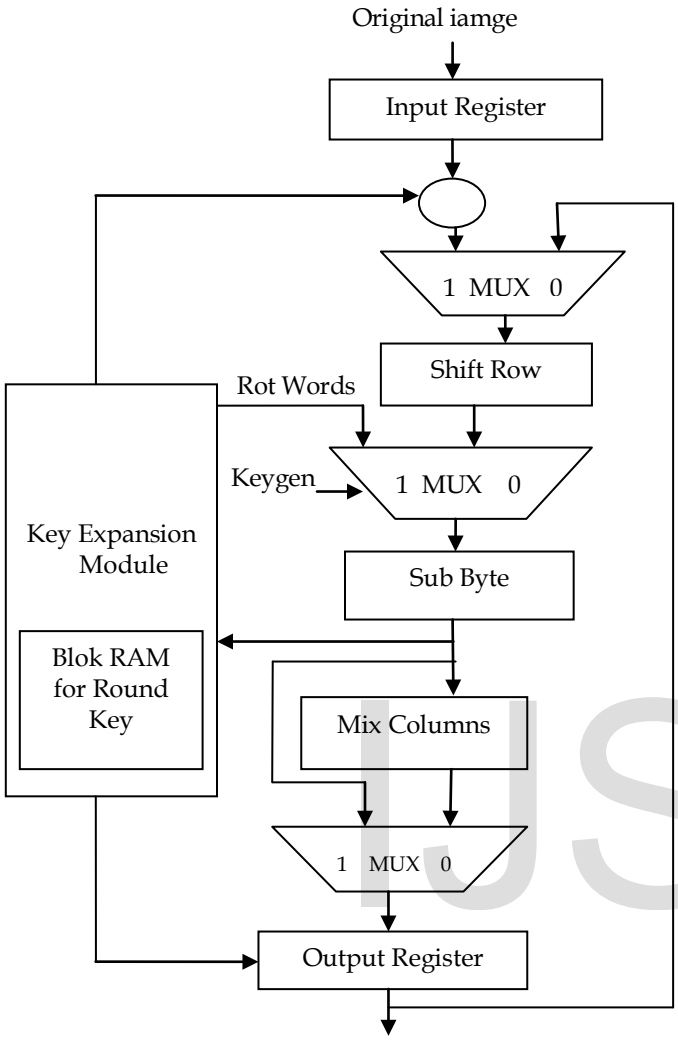

Figure 3. AES Encryption Method

4.2 Key Expansion Module

Key expansion must be done prior to encryption or decryption. This expanded key is used in add round key operation. Initially add round key operation function is called at every time and each of 32 byte of state is XORed versus each of portion of 32 bytes expanded key for current round. The expanded key must be strong enough in order to provide key material for every time execution of next adds round key function. The add round key function gets called at each stage. The length of the expanded key becomes 32 x (Number of rounds + 1) due to execution of add round key function at the beginning of algorithm.

A key expansion module performs execution of four continual functions. These are:

1. ROT Words
2. SUB Words
3. RCON
4. EK
5. K

A trek of above stapes is defined as round [13]. The degree of round of the cipher expansion module depends on length of key.

4.3 AES Decryption Method

Decryption of encrypted image start with AddRound-Key, plus InvShifrRow, InvSubBytes, InvMixColumns operation. The function AddRoundKey do not require inverse operation since it only XOR the state with SubByte. After decryption gets completed original image is recovered.

5 IMPLEMENTED RESULTS AND ANALYSIS

The image of evaluation board i.e. FPGA board and assembly board consisting real time video captured from computer embedded in VLSI fabric for video security system is shown in figure 4. The assembly board composes of 32 bit MicroBlaze soft processor with a RISC-based architecture. The encrypted and decrypted image using AES key length of 256 can be depicted in figure 5.

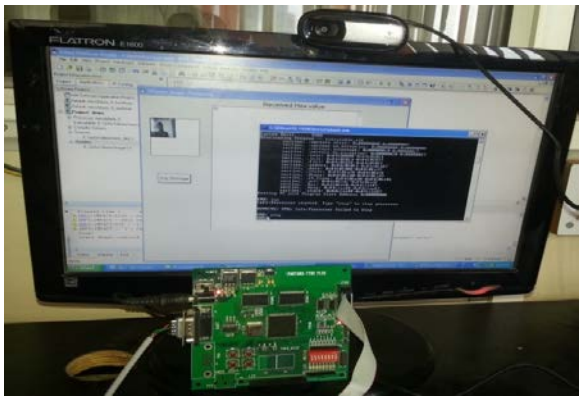

Figure 4(a) Evaluation Board

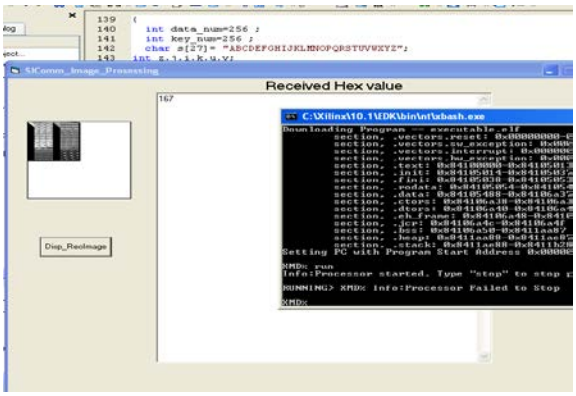

Figure 4 (b) Assembly Board

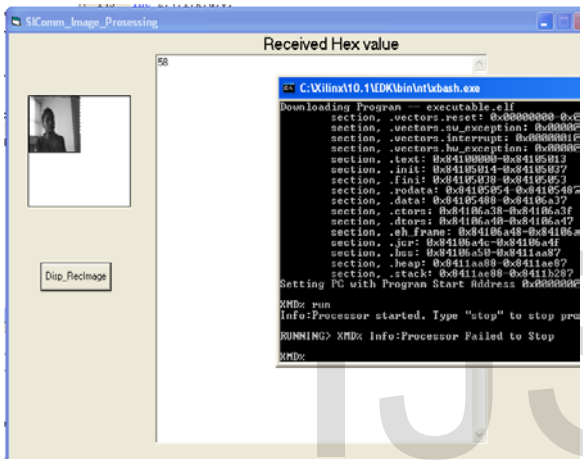

Figure 5 (a) Encrypted Image

Figure 5 (b) Decrypted Image

Implementation for both 256bit and 512 bit key length were carried out. Analytical results can be summarized in following table:

	128/256 bit algorithm	512 bit algorithm
AVI file 219Kbyte	4910	5389
JPG file 25Kbyte	318	566
PNG file 59Kbyte	945	3126

Table 1.Analysis of 256bit and 512bit algorithm with respect to time

The results show that the AES encryption for key length of 256bit takes half of time as compare to that of 512bit and the difference in time increases as data gets bigger. Though encryption with 512bit key length provides high level of security each round requires large memory space than 256 bit encryption. The objective device for performing real time video security module is FPGA board which is Spartan 3 starter kit board [14].

6 CONCLUSIONS

The paper presents a novel security scheme for video encryption using AES algorithm. The presented module used FPGA device with low cost to perform encryption for video running security system. The proposed video running security module process real time video data with least hardware components of FPGA fabric. In order to reduce hardware resources we propose qualified method that includes encryption of raw real time video data using 64 bit AES architecture. By converting RGB frames to grayscale images computational speed is improved as information needs to be provided for each pixel. Therefore the presented hardware architecture for video streaming security scheme is admissible for evolving user product for video surveillance.

ACKNOWLEDGEMENT

Most of the data in this paper is based on literature review of my M.Tech project.This research was supported by my project guide Prof.Brig. R.M. Khaire. I would like to show my gratitude to Prof.Brig. R.M. Khaire for his valuable support

and guidance.

REFERENCES

[1] M. Abomhara, Omar Zakaria, Othman O. Khalifa ,"An Overview of Video Encryption Techniques", *International Journal of Computer Theory and Engineering*, Vol. 2, No. 1 February, 2010

[2] Shiguo Lian, Jinsheng Sun, Guangjie Liu, and Zhiquan Wang, "Efficient video encryption scheme based on advanced video coding," *Multimedia Tools and Application.*, vol. 38, pp. 75-89, May 2008

[3] Shu-bo Liu, Zheng-quan Xu, Wei Li, Jin Liu, and Zhi-yong Yuan, "A novel format-compliant video encryption scheme for H.264/AVC stream based on residual block scrambling," *International Conference on Intelligent Computing*, vol. 5226, pp. 1087–1094, 2008.

[4] Rajdeep Bhanot1 and Rahul Hans , "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications, vol. 9,pp.289 – 306.

[5] Yuanzhi Zou, Tiejun Huang, Wen Gao, and Longshe Huo, "H.264 video encryption scheme adaptive to DRM," *IEEE Trans. Consumer Electron.*, vol. 52, no. 4, pp. 1289-1297, November 2006.

[6] David G. Messerschmitt "Some Encryption Algorithm", Suplymentry section for understanding network application: A first course Morgan Koufmann,1999.

[7] Sonia Kotel, Medien Zeghid, Adel Baganne, Taoufik Saidani, Yousef Ibrahim Daradkeh, Tourki Rached "FPGA-Based Real-Time Implementation of AES Algorithm for Video Encryption", Recent Advances In Telecommunications, Informatics And Educational Technologies

[8] Ritu Pahal and Vikas kumar, "Efficient Implementation of AES", IJARSE, Vol. No.3, Issue No.3, March 2014

[9] Dr. Brian Vick, "MATLAB Commands and Functions", Virginia Tech [online]. Available:http://www.hkn.umn.edu/resources/files/matlab/MatlabCommands.pdf

[10] Punith Kumar M B and Dr. P.S. Puttaswamy " Video to frame conversion of the TV news Video by Using MATLAB" , *IJARSE,* Vol. No.3, Issue No.3, March 2014

[11] Encryption Standard (AES), FIPS PUB-197, 26 November 2001.

[12] Minal Moharir and Dr A V Suresh "A Novel Approach Using Advance Encryption Standard to Implement Hard Disk Security", *IJNSA,* Vol4, No.1, January 2012

[13] Adam Berent, "Advanced Encryption Standard by Example" ABI software development [online]. Available: http://www.adamberent.com/documents/AESbyExample.pdf

[14] *Spartan-3 FPGA starter kit board user guide,* Xilinx, June 20, 2008.