International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

AES 256 Key Secured FPGA Communication using Bluetooth & XBEE

S.M.Turkane†* and M.D.Rahane†

†Department of E & TC, Savitribai Phule Pune University, Pravara Rural Engineering College, Loni, India

Accepted 31 July 2015, Available online 11 Aug 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

Now a day's extended number of wireless communication users have increasing demand of security and protecting data transmitted by the user over unsecured network so that unauthorized persons cannot access it. the data share through wireless network so it must provide data with authentication. The security between the wireless devices is most important part in wireless communications. Bluetooth is small range and the low power consumption that connect through various devices. This project presents the development of secure wireless connection terminals on a field programmable gate array (FPGA). The wireless connection has been established using Bluetooth technology & XBee and the initialization of a secure algorithm for data exchange is implemented using the advanced encryption standards (AES).The proposed system has been validated and demonstrated using an image processing application which involves the encryption and decryption of acquired images from camera. The evaluation of different building block has been carried out in terms of speed, distance and time.

Keywords: *FPGA, AES, cryptography, VHDL, encryption/decryption implementation*

1. Introduction

This Paper presents the implement of secure wireless connections on a field programmable gate array (FPGA).The wireless connection completed using Bluetooth technology, XBee and the initialization of a secure algorithm for data exchange is implemented using the advanced encryption standards (AES 256).

Bluetooth connectivity offers short distance, point to multipoint data exchange. It operates over the unlicensed band with a carrier frequency of 2.4 GHz which is industrial, scientific and medical (ISM) band.

While XBee offers long distance, point to multipoint data exchange with low power consumption. The transmitter block obtain image From Camera. AES algorithm is then used to securely transmit the image using Bluetooth connectivity & XBee to the receiver block.

FPGA processes the received data and operates as the station of the transferred data. It is equipped with the Xilinx Spartan 3XC3S250E-4 PQ208 FPGA chip, and supported with different peripherals to suit a range of applications. Bluetooth connection has been established using the RN41 chipset with 89562 microcontrollers on both transmitting and receiving terminals. Another Wireless Connection has been established using XBee.

*Corresponding author: **S.M.Turkane; M.D.Rahane is M.Tech Scholar**

Capturing of image when intrusion is detected. Apply AES 256 key to captured image Store the image simultaneously in hardware and PC. Comparison of image data stored on hardware and PC. Receive Original loss-less image.

2. Literature works

R.Shorey and B.A. Miller (2000) : special interest group (SIG) introduced wireless communication technology Bluetooth in 1998. Bluetooth connectivity,data exchange with small distance. It operates over the unlicensed band, carrier frequency 2.4 GHz

Lanping Deng, K. Sobti, C. Chakrabarti(2008): Previous technology has been designed for portable devices where power consumption is an important issue to be addressed.

Hasan Taha, Abdul N. Sazish, Afandi Ahmad, Mhd Saeed Sharif, and Abbes Amira (2010): The previous system has been validated and demonstrated using an image processing application which involves the AES-128 encryption and decryption of acquired images from FPGA prototyping board's camera.

In this implementation we used AES-256 key Encryption & Decryption with wirless connectivity using Bluetooth & XBee. also received Lossless Image at the Second FPGA Board.

3. System Block Diagram

The Spartan XC3S250E-4PQ208 family of field Programmable Gate Array (FPGAs) is specifically

designed to meets needs of high volume, cost-sensitive consumer electronics applications. The FPGA Spartan XC3S250E-4PQ208 family builds on the success of the earlier FPGA family by significantly reducing the cost per logic cell, incrementing the amount of logic per I/O, New features improve system performance & reduce the cost of configuration. The Spartan-3E Family is a superior alternative to mask programmed ASICs.

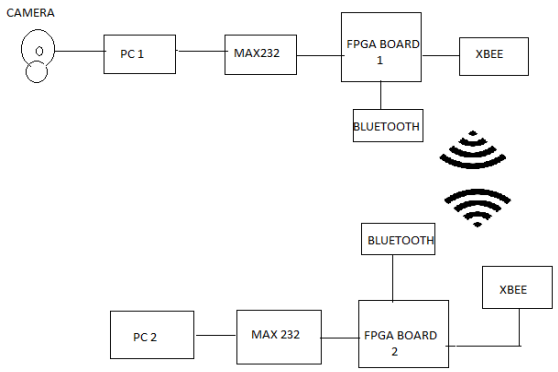


Fig.1 System Block Diagram

3.1 FPGA

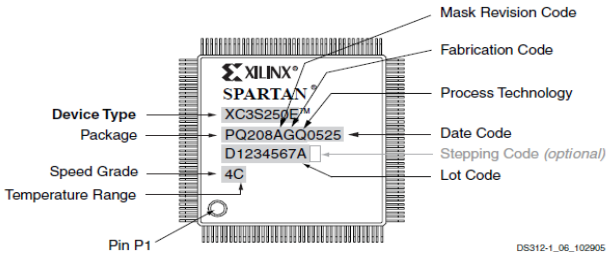


Fig.2 Spartan XC3S250E-4PQ208

1) Very low cost, high performance logic solution for high volume.
2) Multi voltage, up to 376 I/O pins.
3) 3.3V,2.5V,1.8V,1.5V&1.2V signaling
4) Enhanced double data rates support

3.2 Camera

Fig.3 Intex Night Vision Camera

1) Image Resolution :16.0 Mega pixels (4608x3456) interpolated
2) Image Control: Brightness, contrast, hue, saturation, gamma, White balance.
3) Image Flip: Horizontal, vertical
4) Focus Distance:4cm ~infinity
5) Image Format :RGB 24,I420
6) Power Consumption:160mW typical

3.3 RN41/RN41N Class 1 Bluetooth Module

The RN41 Bluetooth is a small, low power, class 1 Bluetooth radio that is ideal for communicating with other devices. The RN41 speed up to a 3-Mbps for distances 100 meters.

Fig.4 RN41 Bluetooth

3.4 XBee Module

Fig.5 XBee Module

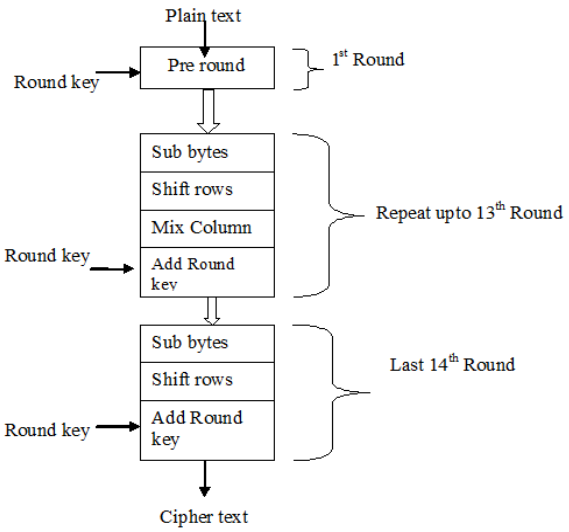
XBee module having 2.4GHz frequency. IEEE Standard 802.15.4,simple command set, this module communicate between microcontrollers, computer systems. Point to point and multi-point networks

1) 3.3V @ 50mA
2) 250kbps Max data rate
3) 1mW output (+0dBm)
4) 300ft (100m) range
5) FCC certification
6) 6 10-bit ADC input pins
7) 8 digital IO pins
8) Local or over-air configuration

4. Advanced Encryption Standard

In the Encryption process we have a plaintext of 128 bits and key of 256 bits size. The number of rounds in AES 256 is 14. The first round consists of all the five operation like Pre round operation, sub byte, shift rows, mix columns and Add round key operations. From 2nd round to 13th round have four operations sub byte, shift rows, mix columns and Add round key operations. And the last 14th round consists of three operations sub byte, shift rows and Add round key operations.

4.1 Flow chart AES Encryption



4.2 Flow chart AES Decryption

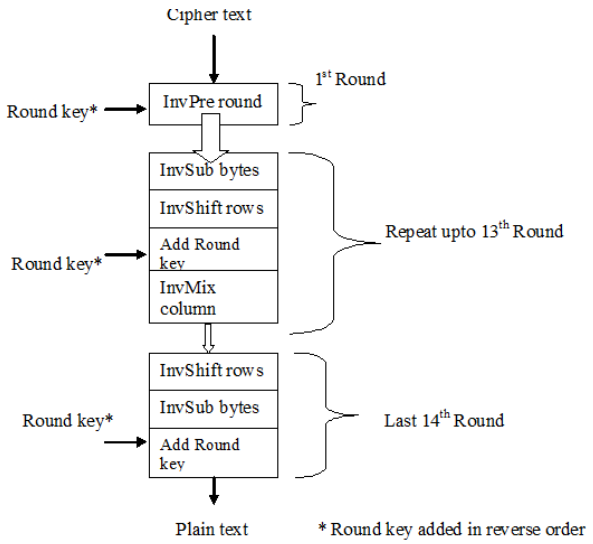


Table 1 Key-Block-Round Combinations

AES	Key Length(Nk words)	Block Size(Nb words)	Number of Rounds(Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

5. Software Design

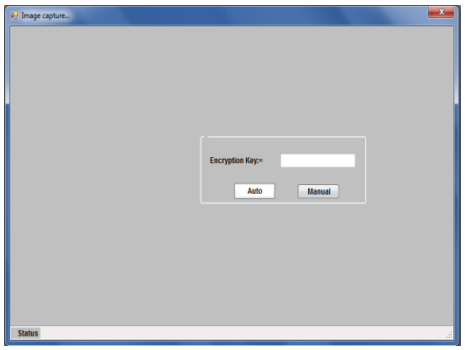
The software is the program which runs on the processor & does all the activities assigned to it. The software in embedded system also called as firmware. In this implementation languages used is VB.NET 2008. The hardware programming of the processors is done in Hyper terminal used for serial communication. The complete PCB is done in OrCAD software. The task assigned to software is: Camera interfacing with PC. Serial communication using Application Software between PC and FPGA.

6. Experimental work

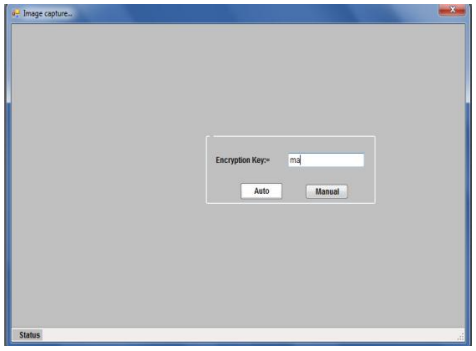
6.1 Transmission side Steps are

1) open web based camera

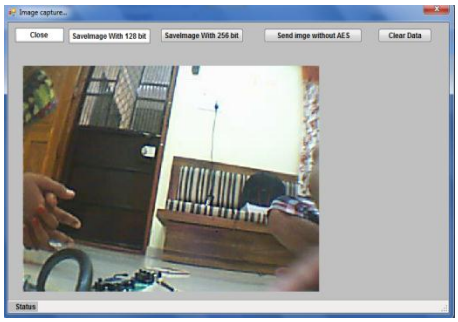
2) Encryption key window



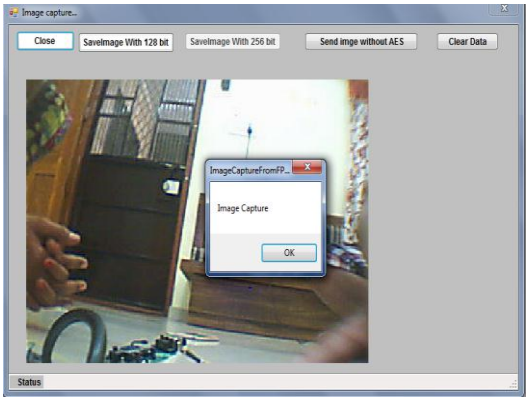
3) enter Encryption key



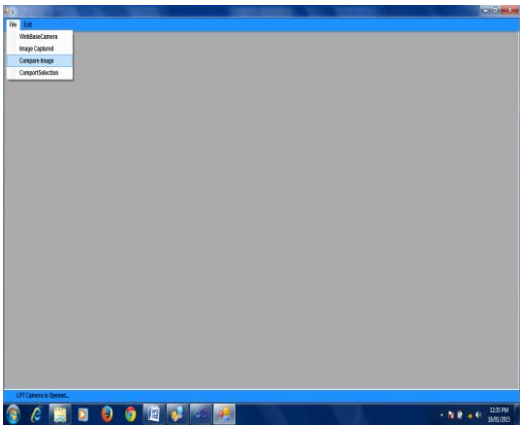
4) Save image



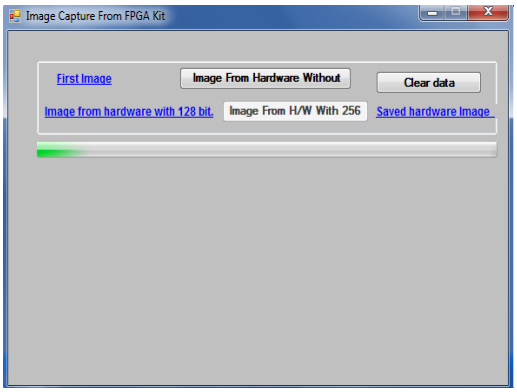
5) Step 5:Image capture



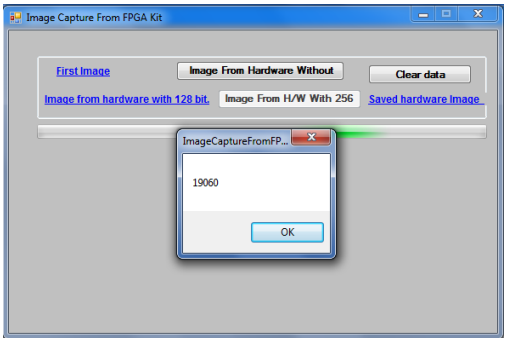
6) compare image



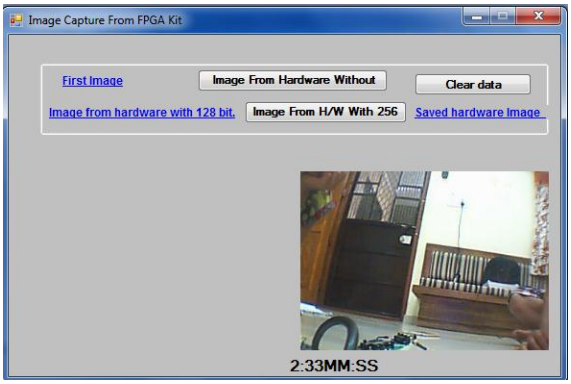
7) load image to FPGA board



8) image from hardware

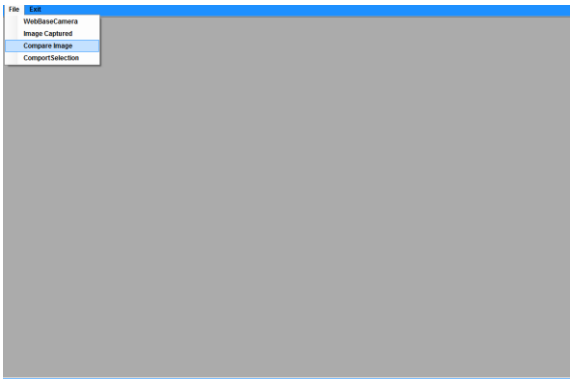


9) image load on fpga board

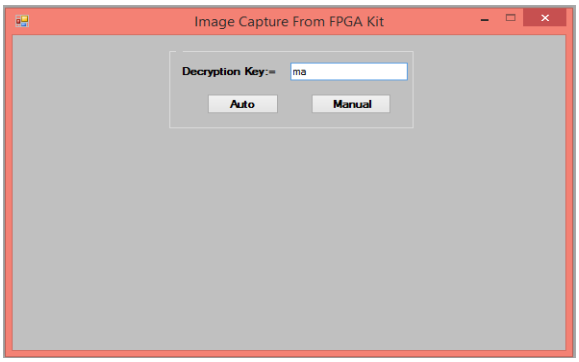


6.2 Receiver side Steps are

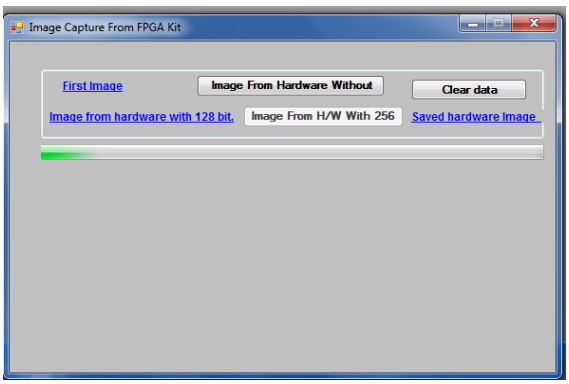
1) compare image



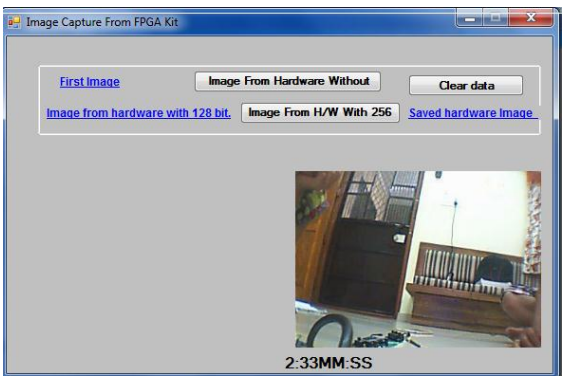
2) enter Decryption key



3) image from second FPGA board



4) Final image receive at second FPGA Board



In this way we obtain a Secure Loss-less Image at the second FPGA Board from First FPGA board with the help of Bluetooth & XBee Wireless terminals.

7. Advantages of the System

1) AES algorithm provided secure data transmission between the two terminals, which increases the security level of data transmission occur between two FPGA boards.
2) Lossless Image Transmission & Reception using AES also.
3) FPGA available today have different sizes at low price. So it is effective for cost saving.

8. Applications of the System

1) In Biomedical Field for Lossless Secure Image Transformation.
2) In internet banking security services.

Conclusion

Benefit of Work

It provides effective use of FPGA board for hardware implementation. It could also be used in educational establishments where the prototyping board does not need to be changed from workstation to workstation.

AES algorithm can resist any kinds of password attacks with a strong practicability in information security and reliability. The Advanced Encryption Standard algorithm provide security Through the use of cipher keys with lengths of 128, 192, and 256 bits.

An efficient implementation of AES 256 encryption for wireless communication system has been presented in this paper. The AES algorithm has been implemented to capture, store and transmit frames by the camera in real-time.

Device Utilization Summary

Table 2 Device Utilization

Logic Utilization	Used	Available	Utilization
Number of Slice F/F	171	4,896	3%
Number of 4 input LUTs	297	4,896	6%
Logic Distribution			
Number of occupied Slice	193	2,448	7%
Number of Slice containing only related logic	193	193	100%
Number of Slice containing unrelated logic	0	193	0%
Total Number of 4 input LUTs	314	4,896	6%
Number Used as logic	192		
Number used asroute-thru	17		
Number used for dual port RAMs	16		
Number used for 32x1 RAMs	52		
Number used as Shift Register	37		
Number of bonded IOBs			
Number of bonded	23	158	14%
IOB Flip Flop	17		
Number of RAMB16s	1	12	8%
Number of BUFGMUXs	2	24	8%
Number of DCMs	1	4	25%

Comparison Result

Table 3 comparison Bluetooth & XBee

Sr. no	Parameter	Image transfer	
	Wireless terminals	Bluetooth	XBee
1.	Time	Approx 2min	2-3 min
2.	No. of round AES	14	14
3.	Baud rate	9600	9600
4.	Max. distance	10m	50m
5.	Power Consumption	High	Low

Future scope of System

Future work, include

1) The system implemented has also been developed for edge detection.
2) The system implemented has also been demonstrated for biometric based security based on Rijndael algorithm. it is bit faster and highly efficient which is obtained by the optimized coding. High Security is provided as there is 256 bit processing. In order to crack the code it takes some billions of years.

References

R. Shorey and B.A. Miller,(2000) The Bluetooth technology: merits and limitations.In Personal Wireless Communications, IEEE International Conference , pp. 80–84,

Lanping Deng, K. Sobti, and C. Chakrabarti,(2008) Accurate models for estimating area and power of fpga implementations. In Acoustics,Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference , pp: 1417–1420

Hasan Taha, Abdul N. Sazish, Afandi Ahmad, Mhd Saeed Sharif, and Abbes Amira,(2010)Efficient FPGA Implementation of a Wireless Communication System

Using Bluetooth Connectivity 978-1-4244-5309-2/10 IEEE International Conference pp:1767-1770

L.Thulasimani,(2010),A Single Chip Design and Implementation of AES-128/192/256 Encryption Algorithms"- International Journal of Engineering Science and Technology, Vol. 2(5), ,pp. 1052-1059.

Anurag Gupta, Afandi Ahmadd, Mhd Saeed Sharif And Abbes Amira,(2011) "Rapid Prototyping Of AES Encryption for Wireless Communication System On FPGA". At IEEE 15th International Symposium on Consumer Electronics, 978-1-61284-843-3ISSN 0747-668X, IEEE 2011.

Ai-Wen Luo, Qing-Ming Yi, Min Shi,(2011)"Design and Implementation of Area-optimized AES Based on FPGA", 978-1-61284-109-0/11/2011 IEEE.

S. Kim and S. Lee. (2003)Design of Bluetooth baseband controller using FPGA. Journal of the Korean Physical Society, 42:pp.200–205

Pawel Chodowiec and Kris Gaj.(2003), Very compact FPGA implementation of the AES algorithm. Cryptographic Hardware and Embedded Systems-CHES 2003,pp. 2779:319–333

G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat. (2004), Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications. In Information Technology: Coding and Computing, 2004.Proceedings.ITCC2004. International Conference on, volume 2, pp. 583–587

Kimmo U. J¨arvinen, Matti T. Tommiska, and Jorma O. Skytt¨a. (2003)A fully pipelined memoryless 17.8 gbps AES-128 encryptor. In FPGA '03: Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays, pp. 207–215, New York, NY, USA