ijar
ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/1448
DOI URL: http://dx.doi.org/10.21474/IJAR01/1448

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN 2320-5470
Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

RESEARCH ARTICLE

EMBEDDED SYSTEM BASED ENCRYPTION AND DATA ACQUISITION ON FPGA FOR DEFENSE APPLICATION.

Monica Kamtamkar and Mrs. Prof. K S Bapat.
VLSI AND EMBEDDED SYSTEMS-E&TC, Department, MITCOE Savitribai Phule Pune University, Kothrud Pune (MH) India.

Manuscript Info

Manuscript History

Received: 12 June 2016
Final Accepted: 16 July 2016
Published: August 2016

Key words:-
Acquisition, Encryption, Decryption, FPGA.

Abstract

Recent developments in defense technology have changed the warfare scenario. The systems are more intelligent, robust and ruggedized. Defense technology demands high accuracy, precision and consistency. A major and important requirement in the field of defense technology is the security and confidentiality of data and information. The most adopted technique for securing the data or information is encryption of the data. The encrypted information can be later decrypted for safe application. In this paper the author has developed a secure data acquisition and Encryption system based on FPGA for defense application. The system consists of two stages, first is the data acquisition stage where the data will be acquired from real world and will be converted in digital form. In the second stage the acquired data will be encrypted and stored in FPGA memory. Later this encrypted data is decrypted to retrieve the original data. The input data chosen for this system is analog signals, as the concept behind this study is mainly for acquiring data from sensors which can be part of any missile or rocket. The data can be pressure, acceleration, temperature etc. which can be recorded from sensors mounted on intelligent systems.

Introduction:-

Embedded systems are being used in most of the defense application areas which includes missiles, rockets and ammunitions. The main concern of defense technology is the confidentiality of data such that enemy should not hack or utilize the confidential information. One way of securing the data is by use of encryption technique. Encryption technique has been used from decades and still is in practice. The encryption techniques have matured with the developing technology. Encryption technique has been used on speech, images and data which can be text or numerical data. In this paper the author has designed an embedded system based encryption and data acquisition system on FPGA. The concept is evolved keeping in mind the application covering defense area. In section 2 related works is presented, in section 3 proposed work is briefed, in section 4 the principle of working is explained and in section 5 of this paper the results and analysis is discussed. The results demonstrating the system functionality is shown in this section.

Corresponding Author: - Monica Kamtamkar.
Address: - VLSI AND EMBEDDED SYSTEMS-E&TC, Department, MITCOE Savitribai Phule Pune University, Kothrud, Pune (MH), India.

Related work:-

In [3] the author has designed FPGA based data acquisition system design for missile Telemetry and Telecontrol. In this paper the author reported and designed a three-rank sequence collected method. The designed method has been implemented on FPGA and gives high performance along with reduction of hardware complexity. Also, the system designed used VHDL implementation for coding further enhancing the system functionality as suggested by author.

In [1] the author proposed a system design for acquisition of data using Fast Fourier transform on FPGA. This method supported acquisition of huge amount of data by compression technique and enhanced the accuracy of acquisition system.

In [2] and [10] the author designed FPGA based multi channel data acquisition system based on. The acquisition systems designed were used for acquiring multiple data through channels and reduced the crosstalk and also integrated filter for reduction of the noise, thereby increasing the system performance. The additional factors of speed enhancement of the system, reduction in power consumption and decreased complexity were also achieved.

In [11] system design for data acquisition is carried out by using communication protocols such as RS232 and SPI. The author was able to achieve accuracy up to 86% by using FPGA platform along with usage of onboard ADC, decreasing the use of resource utilization for design implementation.

In [12] hardware description language (VHDL) is used for implementation of the design of acquisition system for measuring the environmental parameters such as pressure, temperature and level.

In [6] author implemented cryptographic Blowfish algorithm consisting of Encryption scheme and Decryption using VHDL language. The study carried out by author suggest that blowfish algorithm could be implemented for high speed application and provides high privacy of data

In [7] blowfish algorithm providing more throughput and reduced battery usage for text based input data cryptography has been implemented

In [5] FPGA based implementation of blowfish algorithm is proposed by author. The author concluded that the algorithm is highly reliable, provides high privacy of data acquired and is simple to implement on hardware platform.

In [4] Blowfish algorithm implementation on FPGA is studied along with author parameters such as security, resource utilization and avalanche effect. The author concluded that blowfish is efficient than other algorithm compared in the paper

In [8] blowfish algorithm effects due to changing input data is studied. The results provided consider various input signals such as voice, text and data and image. The key size variation has no effect on encryption and decryption time but changing the file size has effect on speed of performance.

In [9] and [16] comparative analysis of various cryptographic algorithms is studied. These paper analyse that blowfish algorithm is more secure and enhance privacy of acquired data as considered to other symmetric algorithms.

In [14], [15] and [13] implementation of AES and RAE algorithm on FPGA is designed. The AES algorithm implementation suggested reduction in power utilization, and dual key AES increased security of input as compared to AES In [15] the author has implemented AES algorithm using dual key. Also the resource utilization is reduced in dual key AES. In [13] REA symmetric algorithm is implemented. This suggest if resource utilization is not important than security can be increased by some factor in REA algorithm.

Proposed work:-

In this paper an embedded system design for encryption and decryption of information using FPGA, along with acquisition of data is implemented. For designing the proposed embedded system, FPGA is used which is more efficient than other controllers as the storage and reliability of the acquired data has been the main parameter considered for defense application. VHDL language is being used for the coding of cryptographic algorithm, which consists of encryption and decryption algorithms. The symmetric cryptographic algorithm namely, Blowfish algorithm is used for the implementation of security aspect of the overall embedded system design. This algorithm is preferred as the information to be acquired and secured is analog in nature and this cryptographic algorithm have not proven cryptanalyst until now, which ensures its excellent ability to secure data and information. The performance of Blowfish algorithm is also more efficient as compared to AES and DES Algorithm for text data encryption. In proposed work cryptographic algorithm “Blowfish algorithm” for analog information encryption and decryption is been used and as this algorithm is being implemented on FPGA the throughput and performance is analytically much more efficient than using other symmetric cryptographic algorithm considering the security aspect.

Principle of operation:-

The functional flow of Encryption and Data Acquisition using FPGA is described in fig1.

The designed embedded system for encryption and data acquisition consist of a FPGA SPARTAN 6 Series evaluation board and an ADC board.

- The signal is captured through a sensor for instance in case 1 experimental signal from signal generator is generated with different frequency and voltages is taken as signal source and in case 2 an acceleration sensor is used as signal source.
- The signal is then passed to an analog to digital convertor where the signal is converted and further passed to SPARTAN 6 evaluation board. The FPGA is programmed with the encryption and decryption algorithm and the data acquisition part.
- The signal received from the ADC output is first encrypted and when the encryption is completed it is displayed on PC using Docklight software. The same encrypted data is stored paralleled in the EEPROM memory.
- This first part of data acquisition and encryption is completed, after some delay decryption algorithm stored in FPGA is executed on the encrypted data stored on EEPROM.
- The decrypted data is again displayed on PC using Docklight software. The decrypted data is passed to digital to analog convertor where the signal is reconstructed again and it is displayed on oscilloscope. Thus the decryption and data retrieval part is completed.

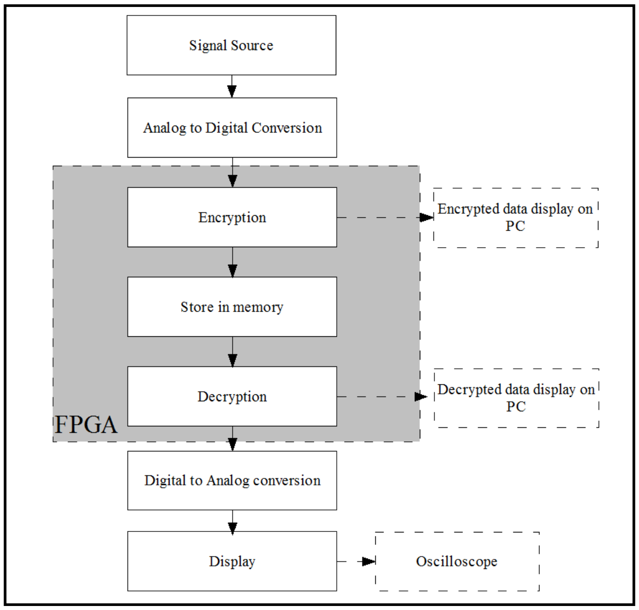
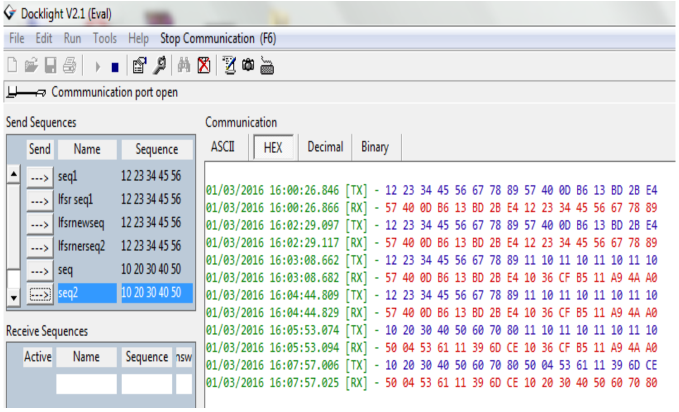

Signal Source
Analog to Digital Conversion
Encryption
Encrypted data display on PC
Store in memory
Decryption
Decrypted data display on PC
FPGA
Digital to Analog conversion
Display
Oscilloscope

Fig 1:- Functional Flow of Proposed Encryption and Data Acquisition Scheme.

Test setup and test Results:-

The embedded system is tested individually for the cryptographic algorithm part to ensure privacy, safety and security of acquired information, using Docklight software. The setup for this cryptographic algorithm testing consists of SPARTAN 6 FPGA board integrated with VHDL coded Blowfish algorithm along with PC interface for displaying the results. The tested results is displayed below in fig. 2



Send	Name	Sequence
--->	seq1	12 23 34 45 56
--->	lfsr seq1	12 23 34 45 56
--->	lfsrnewseq	12 23 34 45 56
--->	lfsrnerseq2	12 23 34 45 56
--->	seq	10 20 30 40 50
--->	seq2	10 20 30 40 50

```
01/03/2016 16:00:26.846 [TX] - 12 23 34 45 56 67 78 89 57 40 0D B6 13 BD 2B E4
01/03/2016 16:00:26.866 [RX] - 57 40 0D B6 13 BD 2B E4 12 23 34 45 56 67 78 89
01/03/2016 16:02:29.097 [TX] - 12 23 34 45 56 67 78 89 57 40 0D B6 13 BD 2B E4
01/03/2016 16:02:29.117 [RX] - 57 40 0D B6 13 BD 2B E4 12 23 34 45 56 67 78 89
01/03/2016 16:03:08.662 [TX] - 12 23 34 45 56 67 78 89 11 10 11 10 11 10 11 10
01/03/2016 16:03:08.682 [RX] - 57 40 0D B6 13 BD 2B E4 10 36 CF B5 11 A9 4A A0
01/03/2016 16:04:44.809 [TX] - 12 23 34 45 56 67 78 89 11 10 11 10 11 10 11 10
01/03/2016 16:04:44.829 [RX] - 57 40 0D B6 13 BD 2B E4 10 36 CF B5 11 A9 4A A0
01/03/2016 16:05:53.074 [TX] - 10 20 30 40 50 60 70 80 11 10 11 10 11 10 11 10
01/03/2016 16:05:53.094 [RX] - 50 04 53 61 11 39 6D CE 10 36 CF B5 11 A9 4A A0
01/03/2016 16:07:57.006 [TX] - 10 20 30 40 50 60 70 80 50 04 53 61 11 39 6D CE
01/03/2016 16:07:57.025 [RX] - 50 04 53 61 11 39 6D CE 10 20 30 40 50 60 70 80
```

Fig. 2:-Test results of hardware testing of Blowfish algorithm on FPGA.

The cryptographic Blowfish algorithm of encryption and decryption is further tested on hardware i.e. encryption and decryption of information is done by passing test data inputs in hexadecimal form from PC through serial communication port. The table I show the test sequences of hardware testing of information input, encrypted information and decrypted information.

Table I: - Test Sequences of Input information, Encrypted Information And Decrypted Information.

Test sequence	Encrypted sequence	Decrypted sequence
22 66 33 77 11 55 44 88	AB C1 26 13 55 10 D5 13	22 66 33 77 11 55 44 88
56 67 78 89 12 23 34 45	13 BD 28 E4 57 40 0D B6	56 67 78 89 12 23 34 45
40 10 50 80 70 20 30 60	61 50 11 CE 6D 04 53 39	10 20 30 40 50 60 70 80
34 5E 76 60 05 00 D2 FB	02 07 03 39 01 05 04 08	34 5E 76 60 05 00 D2 FB
0439 B2AC 01B0 01AB	0102 0BF9 039F 0506	0439 B2AC 01B0 01AB
02E0 48A7 AD73 985B	4768 9851 1276 4930	02E0 48A7 AD73 985B

The test setup for embedded system for encryption and data acquisition using SPARTAN 6 FPGA is shown in Fig.3.

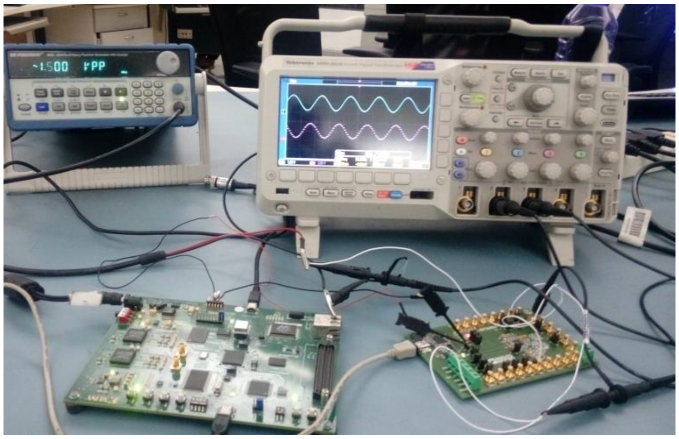


Fig.3:- Test setup for embedded system for encryption and data acquisition using SPARTAN 6 FPGA.

For testing the proposed system SPARTAN 6 FPGA board along with ADC and DAC is used. The input from signal generator with voltage and frequency levels which can be increased and decreased based on test cases are used. Then this acquired information signal is passed to SPARTAN6 through an ADC. The SPARTAN6 platform is used for storing encryption algorithm in program memory, where an encryption command is run on data/ information and the information is encrypted and stored. Here the data encryption and acquisition part is achieved. For verifying and retrieving the original information signal a decryption code stored in SPARTAN 6 program memory is run on the acquired encrypted data and stored previously. After decryption is over the data is passed to DAC where the output waveform is displayed and can be stored.

The designed system is tested using analog input from signal generator and accelerometer sensor. The results shown in Figures below verify the functionality of designed system

Case1: Analog input to the embedded system for encryption and data acquisition is given through signal generator

The Fig 4, Fig 5 and Fig 6 shows the test signals of input analog data and the output of the designed embedded system for encryption and data acquisition.

Case2: analog input to the embedded system for encryption and data acquisition is given through accelerometer sensor

The Fig 7 shows the input and output test analog signal generated by the designed embedded system for encryption and data acquisition. The input for Fig 7 is accelerometer and the generated output is measured and displayed in real time ensuring the efficiency of the designed system.

The Fig 8 shows the encrypted data of input test signal from Fig 4.

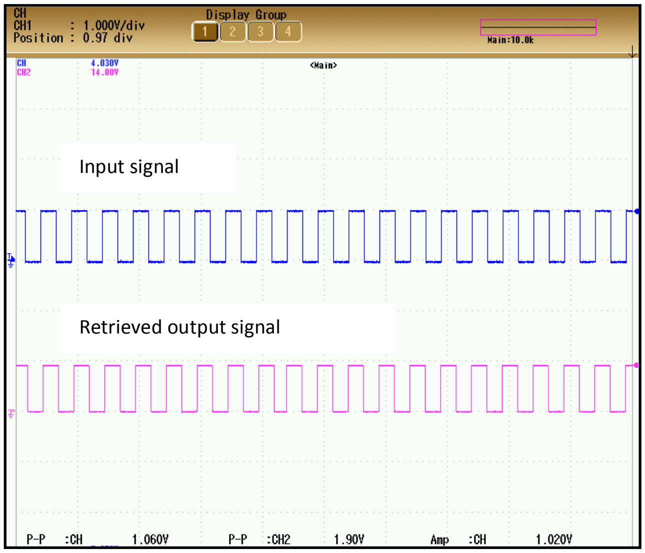


Fig 4:- Comparison of output and input signals of embedded system for encryption and data acquisition.

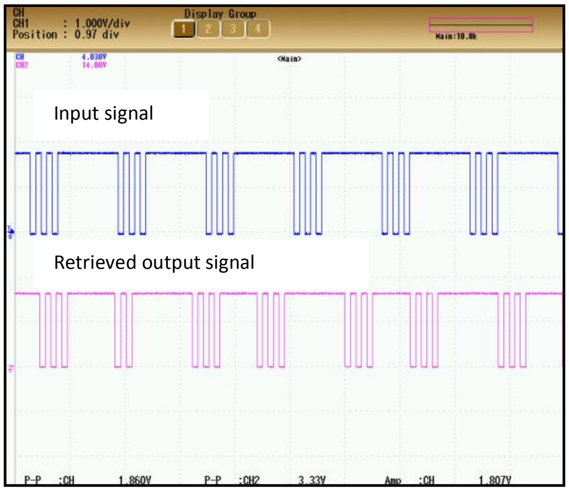


Fig 5:- Comparison of output and input signals of embedded system for encryption and data acquisition.

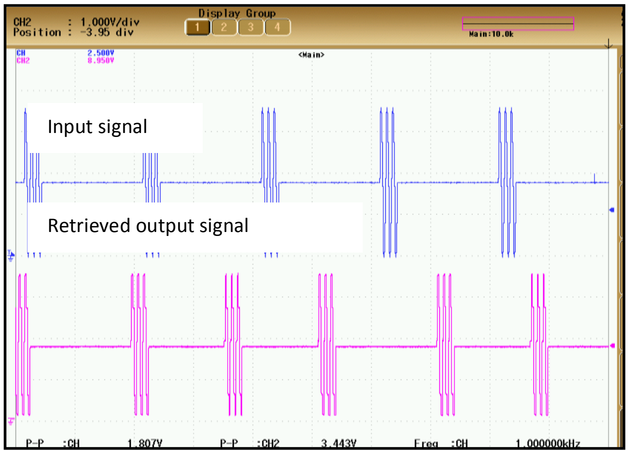


Fig 6:- Comparison of output and input signals of embedded system for encryption and data acquisition

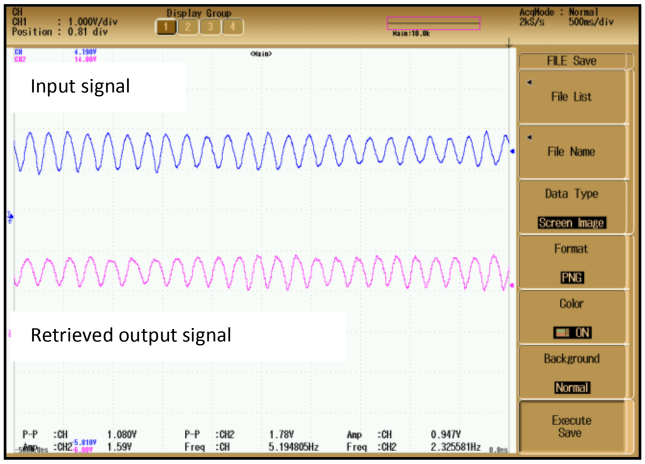


Fig 7:- Comparison of output and input signals of embedded system for encryption and data acquisition

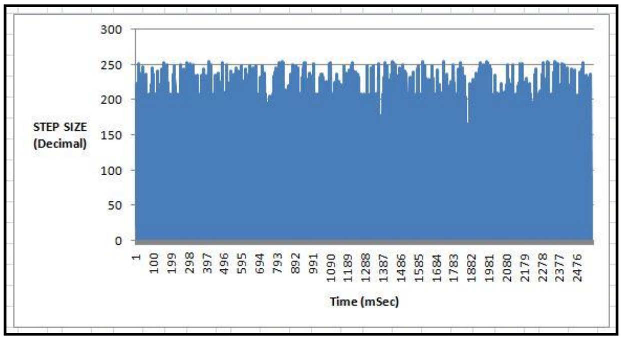


Fig 8:- Encrypted analog data for Fig 4

Conclusions:-

The embedded system designed for encryption and data acquisition system is tested both on software and hardware. Software testing is achieved through Docklight software. Hardware testing is realized through evaluation kits and signal generator along with sensors. Both the software and hardware performances are compared and the data acquisition and its encryption and decryption are achieved for defense application.

References:-

1. Santosh Gujare, Gaurav Jagtap, Damayanti Gharpure, S. Ananthakrishnan, "*FPGA based data acquisition and analysis system,"* Physics and Technology of sensors (ISPTS), IEEE 2012.
2. Su Shujing, Wang Zenggang, *"The design of multi channel data acquisition system based on FPGA,"* IEEE 2011.
3. Jiyang Dai, Guohui Wu, Qian Shuai, Jian Shi, "*Data Acquisition System Design for Missile Telemetry and Telecontrol Based on FPGA*," IEEE 2009.
4. Kurniawan Nur Prasetyo, Yudha Purwanto and Denny Darlis, S.Si. , "*An implementation of data encryption for internet of things using Blowfish algorithm on FPGA*," 2nd International Conference on Information and Communication Technology (ICoICT) 2014.
5. Ankita Deshpande and P.S.Choudhary, **"***FPGA Implementation of Blowfish Cryptographic Algorithm***,"** International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 4, April 2014.
6. L. Kranthi Kiran, J. E. N. Abhilash, P. Suresh Kumar,"*FPGA Implementation of Blowfish Cryptosystem Using VHDL***,"** International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January 2013.
7. Minta Thomas and Panchami V, *"An Encryption Protocol for End-to-end Secure Transmission of SMS,"* International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE 2015
8. Allam Mousa, "*Data Encryption Performance Based on Blowfish*,"47th International Symposium ELMAR-2005.08-1 0 June 2005.
9. Priyanka Raval and Jeegar Trivedi, "*Comparative Analysis of Eight Different Cryptographic Algorithms with Fourteen Factors*," International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 9, September 2014.
10. Liu Jun, Miao Changyun, BaiHua and Yang Yanli, "*Design of the Multi-channel Ultrasonic Signal Acquisition and Denoising Based on FPGA*," Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015.
11. Swamy TN and Rashmi KM, "*Data Acquisition system based on FPGA*," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 2, March -April 2013, pp.1504-1509.
12. H.S.Murali and M.Meenakshi, "*Design and Development of FPGA Based Data Acquisition System for Process Automation*," Communications in Control Science and Engineering (CCSE) Volume 1 Issue 1, January 2013.
13. Mohammad Iftekhar Husain, Kerry Courtright, Ramalingam Sridhar, "*Lightweight Reconfigurable Encryption Archtitecture For Moving Target Defense,*" Military Communication Conference IEEE 2013.
14. J.Balamurugan and Dr.E.Logashanmugam, "*High Speed Low Cost Implementation of Advanced Encryption Standard on FPGA*," 2nd International Conference on Current Trends in Engineering and Technology, ICCTET 2014.
15. Abhriam L S, Sriroop B K, Gowrav L, Punith kumar H L, Manjunath C Lakkannavar, "*FPGA Implementation Of Dual Key Based AES Encryption With Key Based S-Box Generation,*" IEEE 2015.
16. G. Muthukumar and Dr. E. George Dharma Prakash Raj "*A Comparative Analysis on Symmetric Key Encryption Algorithms,*" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.