International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-12, December 2015

A Survey on Data Acquisition and Cryptographic Algorithms based on FPGA

Monica Kamtamkar, Mrs. Prof. K S Bapat

Abstract— **Data acquisition is an important parameter for various electronic systems. Technology is advancing towards new techniques which can provide more accurate data acquisition system designs with less complexity. The precise and accurate acquisition of data will provide accurate result. A method to acquire data with minimum loss of information is a priority for electronic designers. As for current scenario not only precise acquisition of information but its confidentiality is of importance. The security of information is also a major aspect of designers. Various fields like military, defense and industrial companies maintains security of information as there priority. Cryptography has been a field of interest from decades for designers. It has led to exploration of various methods in which data can be made secure from hackers and unauthorised users. A literature survey on data acquisition system with security of information as its main parameter is presented in this paper. To achieve more accurate results of data acquisition with less complexity of system design FPGA platform is considered. So an analysis on data acquisition scheme based on FPGA and encryption algorithm is carried out in this paper.**

Keywords-**Data Acquisition, cryptography, FPGA, Security**

I. INTRODUCTION

Data acquisition involves sensing, gathering, sampling and storage of data. In data acquisition the analog signals from surroundings are sampled and converted to digital signals which can be stored and again retrieved and converted back to analog signals for further analysis. The main parameter of data acquisition system is to sample the signal which after reconstruction will represent the original signal accurately. The resolution of the signal is also another parameter to be considered. Platforms like controllers and digital signal processors have been in use for data acquisition system design. As new technologies emerges in market various platform which are user friendly and more reliability is being developed. FPGA is a platform which provides accuracy with ease of design, high speed and field programmability features. These features help in designing data acquisition systems which are efficient than tradition data acquisition system design. FPGA provides high data storage capability compared to microcontrollers. Recent trends have shown FPGA use has increased because of these features in electronics system designs.

Information acquired by data acquisition system can be made secure by use of cryptography. Security of information has been a major concern of various applications. Security of information has been of interest for designers and can be traced way back to decades when technology was not matured enough. Ancient people used simple substitution, permutation and combination of data for making the data secure. As decades passed more efficient and secure algorithms were designed and used for making data secure. Cryptography provides security of information by using various encryption and decryption algorithms. Cryptography is a method in which we can make the data secure by encrypting it and again retrieve the data back by decrypting it. Cryptography is a process consisting of three main parameters. Plaintext - the data to be encrypted. Cipher text -the encoded information by using key. The third parameter is the key. This is the unique pattern which is used for encrypting the plaintext to convert it to cipher text. Encryption and decryption algorithms provide various ways to secure the data. These algorithms can be broadly classified as symmetric key cryptography and asymmetric key cryptography algorithms. Security of data can vary depending on the cryptographic algorithm used. Symmetric key cryptography uses same key for encryption and decryption of data. Asymmetric key cryptography uses two key, private and public key for encryption and decryption. Symmetric key cryptography is comparatively efficient than asymmetric key cryptography. Also it is less complex. Algorithms like AES, DES, RC2 and BLOWFISH are symmetric key cryptography algorithms. The BLOWFISH algorithm uses block cipher. This algorithm provides better performance compared to AES and DES algorithm on FPGA. And up till now there has been no major attacks reported like side channel attack, which affect the system performance vitally.

II. LITERATURE REVIEW

In [1] data acquisition is performed using FPGA and the communication is done using TCP server. Most acquisition system relay on computer for storing and querying data. The system presented in the paper provides function similar to the computer based acquisition system but has a degree of integrity and superior range.

In [2] PC based data acquisition for underwater sensor array is proposed. Multiple analog input channels are a major concern in underwater sensor array. Intel processor based 96 channel data acquisition scheme using PC is studied. As many channels are used the concerned problem of multi analog channel has been minimized. The system consist both of hardware and software components.

In [3] data acquisition system for nuclear imaging is implemented based on FPGA. This paper shows that implementation of DAC using FPGA which can provide a low cost alternative for nuclear imaging. The complexity of system is also reduced. The post processing is carried out on PC which is connected through RS232. Spartan3E kit was used.

In [4] data acquisition for telemetry is proposed. Hardware description language is used for coding. Three rank sequence methods are proposed which reduces the complexity of the system. The circuit's reliability was increased remarkably because of use of FPGA and the proposed three rank sequences. For developing telemetry for missile the main factors were low power consumption and small bulk. These factors were satisfied by the author proposed method.

In [5] data acquisition system design is proposed. The acquisition system is designed using the inbuilt ADC on the SPARTAN kit. External ADC is not used. Even by using onboard ADC the resource used on FPGA was reduced and noise of the system was minimized.

In [6] pipelined AES algorithm is implemented on FPGA. Virtex5 kit is used for analysis. The dual port BRAM, DSP blocks on Virtex5 is used. The use of BRAM and DSP blocks ensures minimization of usage of registers and lookup tables. Thus a new way of performing encryption and decryption using these blocks and increasing the performance is the main idea of the author.

In [7] Fast Fourier Transform is used. The use of FFT has made the acquisition process more accurate. The signal is divided into frequency slots and the processing of signal is done in frequency domain. The complexity of system reduces by using FFT. FPGA family used is SPARTAN.

In [8] multi channel data acquisition is considered. The author concluded that by using multi channel the complexity can be reduced and speed of system can be increased. A parallel approach is suggested by author and analog signals up to 32 channels can be acquired and processed 32 channel analog signal data is acquired.

In [9] the parameters considered are minimization of noise and accurate data acquisition. This system consumes less power. As the speed of system is also important for measuring the performance of a system the data collection and data detection time is analysed for various environmental conditions.

In [10] various cryptographic algorithms are analysed. These algorithms are highly efficient in securing the data in communication medium. The asymmetric key cryptographic algorithms provide non-repudiation. Symmetric key cryptographic algorithms are simple to implement and are used in many application.

In [11] analytical analysis of symmetric key cryptographic algorithms is presented. Symmetric algorithm likes AES, DES, BLOWFISH and various newly proposed algorithms are also studied. This shows that considering parameters like authenticity, integrity and security symmetric key algorithms are efficient in software. AES is efficient in software and hardware. AES is widely used in many applications.

In [12] FPGA based lightweight cryptographic function are implemented using various methodologies. The analysis show that full hardware acceleration gives reasonable performance compared to other methodology. The other methodology considered for comparison were software based design methodology and software/hardware co-design.

I. COMPARISON OF DATA ACQUISITION SYSTEMS

Nomenclature	**Software**	**Feature**	**Application**	**Results**
PC based data acquisition	MATLAB	FFT used for Beam forming	Under water sensor array	Saves money , time
FPGA based signal processing	MATLAB, VHDL	FFT and domain analysis	Medical imaging	Processing time reduced
Data acquisition and analysis system on FPGA	VHDL, MATLAB	FFT for compression of output data	Low frequency radio observations	Accuracy
Data acquisition for Gamma ray detection on FPGA	MATLAB	Pulse height estimation method , digitization of anode signals	Nuclear imaging	Low cost compared to traditional method ,reduced complexity
DAS design on FPGA	VHDL	3 Rank sequence	Telemetry and Telecontrol system	H/W Bulk reduces
Multichannel data acquisition on FPGA	VHDL	Parallel data acquisition	Defense	Speed of acquisition increased
Multi channel with noise reduction	VHDL	Average filter	Wireless communication	Speed increased and Denoising

In [13] VHDL is use for coding Blowfish algorithm. The encryption and decryption scheme of blowfish algorithm is implemented on hardware. As FPGA is used the system becomes more hardware specific. The FPGA implementation of blowfish algorithm is preferred for high speed application.

In [14] encryption algorithm analysed is blowfish algorithm. The author compared AES and Blowfish algorithm for implementing text data encryption. Blowfish algorithm was more efficient. This algorithm can be used for SMS and text encryption and provides security. As for SMS the power consumption is an important factor implementation of Blowfish algorithm on FPGA platform with less battery usage was main factor considered.

In [15] AES algorithm is implemented on FPGA. The paper showed that the performance was increased and power consumed per block was decreased by implementing algorithm on FPGA platform.

In [16] implementation of AES algorithm using dual key is analysed. In this method dynamic allocation of resources is used instead of static lookup table. This led to decrease in the attacks like cryptanalysis. Author proposed less complex algorithm which reduced the computational overhead in system design.

II. COMPARISON OF ENCRYPTION ALGORITHMS [18]

PARAMETERS	DES	AES	RSA	BLOWFISH
DEVELOPMENT	In early 1970 by IBM and Published in 1977.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
KEY LENGT	64 (56 usable)	128,192, 256	Key length depends on	Variable key length

H (Bits)			no. of bits in the module	i.e. 32 – 448
ROUNDS	16	10,12,14	1	16
BLOCK SIZE (Bits)	64	18	Variable block size	64
ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Key recovery attack, Side channel attack	Brute force attack, timing attack	No attack is found to be successful against blowfish.
LEVEL OF SECURITY	Adequate security	Excellent security	Good level of security	Highly secure
ENCRYPTION SPEED	Very slow	Faster	Average	Very fast

In [17] REA is considered. This algorithm has the property of re-configurability. This helps to improve the security of algorithm as the user can configure the algorithm by varying number of rounds and key used in algorithm. So the attack on this algorithm decreases. This algorithm is not resistant to timing attacks.

In [18] study on comparison of various encryption algorithms is shown. Table II shows the parameters of various encryptions algorithm of this paper. This gives the basic parameters used in encryption algorithms.

In [19] performance evaluation of various parameters for DES and Blowfish algorithm is studied. The parameters like encryption security, encryption speed and power consumption were analysed. The power consumption of both algorithms is almost same. The time required for encryption in DES is more comparatively.

In [20] DES algorithm is studied which shows that it is resistant to many DPA attacks practically. The goal was to study the real time DPA attack effect on DES algorithm. The DPA attack on FPGA is difficult because of the decoupling capacitor. The FPGA board has to be broken down physically before applying DPA. The decoupling capacitors are a countermeasure which helps to improve the security of DES algorithm.

III. Conclusions and Future Work

Data acquisition based on FPGA and various Cryptographic algorithms implemented on FPGA platform is presented in this paper. In Table I some parameters of Data acquisition are summarized. This gives a better understanding of data acquisition system design based on the feature and application of the system which the user wants to design. FPGA based implementation of Cryptographic algorithms for encryption and decryption is analyzed and its comparison with some features is shown in Table II.

From this analysis it is found that

1. Data acquisition system design using FPGA platform provides high performance and complexity of design is less as compared to tradition data acquisition system design which uses PC.
2. FPGA based data acquisition system consumes less power and the accuracy provided by these systems is high.
3. Cryptographic algorithms on FPGA increases the speed of encryption compared to implementation of algorithm on software platform.
4. The security of data is better by implementing cryptographic algorithm on FPGA.

The future scope can be a data acquisition system design which can provide security also, for applications which required confidentiality can be implemented. The accuracy can be increased to a high level by using FFT and parallel data acquisition approach. The main parameter for maintaining confidentially of application is the security of data. This can be provided by integrating the implementation of cryptographic algorithm on FPGA. So a FPGA based data acquisition system design which is robust to attacks from unauthorized user can be implemented. This will results in reduced cost and complexity of design as FPGA is more cost effective and user friendly. The analysis shows that algorithm like AES and BLOWFISH can be used for such applications.

REFERENCES

[1] A. Mazare, L. Ionescu, G. Serban, I. Lita, "*FPGA-based system for data acquisition and remote communication*" 20th International Symposium for Design and Technology in Electronic Packaging (SIITME) IEEE 2014.

[2] Umar Hamid, Rahim Ali Qamar, Mohsin Shahzad, "*PC Based Data Acquisition and Signal Processing for Underwater Sensor Arrays*" IEEE 2013.

[3] Fisikopoulos Eleftherios, Georgiou Mariaz et. al., "*A Spartan3e based low-cost system for gamma-ray detection in small SPECT or PET systems*"IEEE 2010.

[4] Jiyang Dai, Guohui Wu, Qian Shuai, Jian Shi, "*Data Acquisition System Design for Missile Telemetry and Telecontrol Based on FPGA*," IEEE 2009.

[5] 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.

[6] J. Senthil Kumar, C.Mahalakshmi, "*Implementation of Pipelined Hardware Architecture for AES Algorithm using FPGA*" International Conference on Communication and Network Technologies (ICCNT) IEEE 2014.

[7] Santosh Gujare, Gaurav Jagtap, Damayanti Gharpure, S. Ananthakrishnan, "*FPGA based data acquisition and analysis system,"* Physics and Technology of sensors (ISPTS), IEEE 2012.

[8] Su Shujing, Wang Zenggang, *"The design of multi channel data acquisition system based on FPGA,"* IEEE 2011.

[9] 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.

[10] Sourabh Chandra, Smita Paira, et.al. "*A comparative survey of symmetric and asymmetric key cryptography*" International Conference on Electronics, Communication and Computational Engineering (ICECCE) IEEE 2014.

[11] Bidisha Mandal, Sourabh Chandra, Sk Safikul Alam, Subhendu Sekhar Patra,"*A Comparative and Analytical Study on Symmetric Key Cryptography*" International Conference on Electronics, Communication and Computational Engineering (ICECCE) IEEE 2014

[12] Imene Mhaohbi ,Nejla Rejeb, Slim Ben Othman, Nabil Litayem, Slim Ben Saoud "*Design Methodologies Impact on the Embedded System Performances: Case of Cryptographic Algorithm*" IEEE 2014.

[13] 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.

[14] 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

[15] 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.

[16] 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.

[17] Mohammad Iftekhar Husain, Kerry Courtright, Ramalingam Sridhar, "*Lightweight Reconfigurable Encryption Archtitecture For Moving Target Defense*," Military Communication Conference IEEE 2013.

[18] Rajdeep Bhanot and Rahul Hans "*A Review and Comparative Analysis of Various Encryption Algorithms*" International Journal of Security and Its Applications Vol. 9, No. 4 (2015), SERSC 2015.

[19] Tingyuan Nie, Chuanwang Song, Xulong Zhi, **"***Performance Evaluation of DES and Blowfish Algorithms*" Biomedical Engineering and Computer Science (ICBECS), International Conference, IEEE 2010.

[20] Song Sun, Zijun Yan, Joseph Zambreno, "Experiments in Attacking FPGA-Based Embedded Systems using Differential Power Analysis" IEEE 2008.

Monica Kamtamkar received B.E degree in the field of Electronics and Telecommunication engineering in the year 2014 from PVG's COET, Pune. She is currently pursuing post graduation in VLSI & EMBEDDED SYSTEMS (E&Tc) from MITCOE, PUNE

Kalpana S. Bapat received M.Tech degree from COEP, Pune. She has 20 Years of experience in teaching field in college like Father Agnel Bandra, MIT Pune and Vivekananda Chembur. Her areas of expertise are Data Structures, Computer Network and Coding theory. She has 6 publications in National journals in the area of Image processing, Sensor Network and speech signal processing.