IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 7.047 ⁜ Vol. 10, Issue 2, February 2022

DOI: 10.17148/IJIREEICE.2022.10231

FPGA-based implementations– A Review

Jalaja GS[1], Mr. Praveen M [2], Dr. M Z Kurian[3]

[1]PG- Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka

[2]Assistant Professor, Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka

[3]Head of Department, Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka

Abstract: In recent days everywhere big data play a very important role. Development of big data is increasing day by day. With the development Security of data is also very important. the most important feature of big data is the length of the data is very large it affect the security of the data. Nowadays many algorithms are developed in order to increase the speed and reduce the delay of data transmission. AES (Advance encryption standard) play a major role in encryption. It encrypt the data quickly and also increases the speed and reduces the delay while transferring data. This paper carried out the literature survey of FPGA based implementations. This paper discusses about the implementation of FPGA in different applications. The papers which implement FPGA in their applications have been reviewed in terms of area utilization, power consumption and energy efficiency. This review will be helpful for those who are starting newly in FPGA to know about the area of its application. It also helps to know about the hardware on which these implementations have been tested.

Keywords: FPGA; Advance encryption standard; Big data;

1. INTRODUCTION

As the data length increases chances of leakage of data also getting increases. It affects the security of data while storing, processing and transferring of data. The solution of this problem is we need to increase the speed and reduce the delay of the data transmission. In early days (data encryption standard) DES is used worldwide. DES encryption is slow, and it increases the delay. AES is invented as the solution for DES. In AES there are many implementation are present like hardware implementation, software implementation. Hardware implementation is more safe then software implementation because unauthorized access cannot change them. There are many operation are conducted during data encryption like swapping, mapping, compression, shifting. FPGAs have their importance in embedded systems design from very old days. FPGAs are used in pre-silicon validation of chips while manufacturing and for prototyping the Application Specific Integrated Circuits. FPGAs can be reprogrammed several times before the design is final and bug-free which reduces the cost of manufacturing final design significantly. FPGA implementations can be done for a simple address circuit to complex neural networks. FPGAs access the machine's cache along with RAM memory and are very much faster than the CPUs Swapping operation leads to save the area. AES can be implemented on different processor in order to achieve maximum throughput and reduces the latency. mainly there are three major steps are performed that is key generation, encryption, decryption. In this paper AES is implemented on FPGA. AES increases the speed by utilizing lesser resources available on FPGA (Field programmable gate array). The data is encrypted and send to the machine and the data is decrypted in that machine.

2. LITERATURE SURVEY

Literature survey has been carried out in this section this section signify the importance of data encryption.

[1] This paper discusses the FPGA implementation of the famous Advanced Encryption Standard (AES) algorithm in cryptographic applications. In this paper AES encryption has been done utilizing the minimum hardware and area. Area reduction is achieved by combining the AES encryption algorithm with the improved S-box technique. Minimization of hardware is achieved by replacing the conventional multiplier with Vedic multiplier in the step of mix column transformation in AES encryption. Vedic multiplier has gained popularity in recent days because of low area, low power consumption and reduced complexity. This modified AES encryption algorithm using S-box structure has been implemented and tested on Virtex-4 XC4VLX200. Reduction in area, lesser hardware and increase in speed were observed on FPGA.

DOI: 10.17148/IJIREEICE.2022.10231

[2] With the advancements in Machine Learning, Convolutional Neural Network based techniques have been used in remote object detection and sensing. Implementation of these techniques in aerospace systems is still challenging because of the cost of its implementation. Hence to test, this paper describes the method of implementing in hardware for object detecting in remote sensing. For hardware implementation, the CNN based model will be optimized and then mapped onto the FPGA efficiently. To reduce latency in calculations and for complete memory bandwidth utilization, new access scheme and data storage has also been proposed. This optimized YOLO CNN has been deployed on Xilinx ZYNQ xc7z035 FPGA for design evaluation. Results suggest that this method has improved energy efficiency and can be deployed on embedded devices efficiently.

[3] Data security has become the major issue with the increase in availability of large amount of data. This paper proposes encryption of sound using chaotic systems based on the fractional order. With the use of fractional calculus in this chaotic system, it makes it difficult to hack and increases the control on the system. In the recent years, digital implementation of these fractional-order chaotic systems has been increased. Introduction of chaotic systems increased the efficiency of the cryptographic algorithms. Chaotic systems have been introduced in image and speech encryption. Implementation of fractional-order chaotic systems in sound encryption on FPGA was done and observed the usage of low power and area and increased efficiency because of the parallel execution.

[4] This paper discusses about the implementation of cryptographic algorithms for telecom applications. With the discovery of internet, there is huge development in the telecom sector from to 2G to 5G as it offers the faster downloading speed and connected devices for various IoT applications. Because of this interconnections, personal data threats have also been increased. This paper addresses such threats by implementing AES algorithm encryption to the electronic data on FPGAs. This paper proposes a method of high level synthesis to be used with AES encryption which results in high throughput. The design was deployed and verified on the Xilinx Virtex 6 and Kintex 7FPGAs and signification results were observed.

[5] Securing medical reports in normal life and mainly crime scene investigation has become a challenging task these days. Hence this paper proposes a method of image encryption using modified AES algorithm and chaos -based pseudo random number generator. This paper proposes the use of PRNG based on complex set in 2D logistic map and use of Henon's system during generation of key. In modified AES, operation of sub bytes is performed using S-boxes with increased complexity. Important step is performing only four rounds of encryption to reduce the execution time. The proposed method was deployed on Altera Cyclone III board with SD card for image storage and with VGA interface for image display. Results showed that complexity time was reduced by 97% with reduced power consumption and increased throughput.

[6] Internet of Things has become popular n recent years because of increase in connectivity and availability of internet to everyone. But it must fulfill the security standards of IoT. This paper uses frequency hopping for generating Pseudo Random Number pattern and it switches between the 5 cryptographic algorithms, OCB,ASCON, COLM, AEGIS and Deoxys. To switch between the 5 different ciphers in FPGA, Dynamic Partial reconfiguration has been used and provides with 58% reduction in area and 80% less in power consumption. The design was deployed and tested on Xilinx Vivado 2015.2.

[7] With the advancement in wireless technologies like Bluetooth, ZigBee, LoRa and with increasing importance in IoT, wireless networks have become popular these days. Security of the data that is exchanged between these nodes is a challenging task. This paper discusses about design and deploying a data exchange system on FPGA along with built in customized co-processors in which data will be exchanged between the wireless sensor nodes in a secured and faster way. Also key exchange protocol will be implemented based on Diffie Hellman protocol. The integrated co-processors are AES(Advanced Encryption System) for symmetric cryptography, Elliptic curve(ECC) for asymmetric and SHA-Secure hash algorithm for random key generation and authentication. The system was deployed on Artix-7 XC7A35T FPGA , equipped with 2.4 GHz nRF24L01 transceiver module.

[8] Steganography secures secret information by hiding sensitive information in images. The secret message will be hidden inside in an invisible way and thus making the steganography popular. This paper proposes a method of security using two levels of encryption. First the data will be encrypted by CBS - Character Bit Shuffler, an encryption method developed in Java. Next using LSB technique, data will be hidden inside the image. LSB technique changes only last bits of image. Proposed method shows reduction in area by 80%.

[9] This paper discusses implementation of invisible watermarking system using ALTERA Cyclone IV-E 'EP4CE115F29C7' FPGA board.For water mark encryption, algorithms were applied on color images using Discrete

DOI: 10.17148/IJIREEICE.2022.10231

Wavelet Transform. By comparing image encryption using C-Eclipse, security of the proposed model was increased. Experimental setup included VGA monitor for displaying images during the experiment. After implementation, robustness of the system, performance, area consumption and resources were measured.

[10] Lightweight cryptography is the recent development in the field of cryptography which is usually meant for deploying in the devices which are resource constrained. These algorithms assure moderate security because of the constrained resources. This paper proposes two architectures, one is suitable for low area implementation and other suitable for low power implementation. Suitable architecture will be chosen depending on the trade-offs between latency and performance. The designed systems were evaluated on Virtex4, Viretx 6 and Spartan 3.

CONCLUSION

The proposed project reduces the latency of data encryption while providing data encryption throughput much better to previous studies. The increase in encryption speed brings about the improvement of big data security. If this problem can be solved reasonably, the development of big data can be smoother.

REFERENCES

1. C. Arul Murugan, P. Karthigaikumar& Sridevi Sathya Priya (2020) FPGA implementation of hardware architecture with AES encryptor using sub-pipelined S-box techniques for compact applications, Automatika, 61:4, 682-693, DOI: 10.1080/00051144.2020.1816388
2. Zhang, N.; Wei, X.; Chen, H.; Liu, W. FPGA Implementation for CNN-Based Optical Remote Sensing Object Detection. Electronics **2021**, 10, 282. https://doi.org/10.3390/electronics10030282
3. Jamal, Ahmed & El-Kader, Ayman & Hassan, Bahy&Rihan, Nader &Tolba, Mohamed & Said, Lobna& Radwan, Ahmed & Abu-Elyazeed, M.F.. (2019). FPGA implementation of sound encryption system based on fractional-order chaotic systems. Microelectronics Journal. 90. 10.1016/j.mejo.2019.05.005.
4. Sikka, Prateek &Asati, Abhijit. (2020). Speed optimal FPGA implementation of the encryption algorithms for telecom applications. Microprocessors and Microsystems. 79. 103324. 10.1016/j.micpro.2020.103324.
5. Amal Hafsa, Mohamed Gafsi, Jihene Malek, Mohsen Machhout, "FPGA Implementation of Improved Security Approach for Medical Image Encryption and Decryption", ScientificProgramming, vol. 2021, ArticleID 6610655, 20 pages, 2021. https://doi.org/10.1155/2021/6610655.
6. Shady Soliman, Mohammed A. Jaela, Abdelrhman M. Abotaleb, Youssef Hassan, Mohamed A. Abdelghany, Amr T. Abdel-Hamid, Khaled N. Salama, Hassan Mostafa,FPGAimplementation of dynamically reconfigurable IoT security module using algorithm hopping,Integration,Volume 68,2019,Pages 108-121,ISSN 0167-9260,https://doi.org/10.1016/j.vlsi.2019.06.004.
7. Abdelmoughni Toubal, BillelBengherbia, Mohamed OuldZmirli, AbderrezakGuessoum,FPGA implementation of a wireless sensor node with built-in security coprocessors for secured key exchange and data transfer,Measurement,Volume 153,2020,107429,ISSN 0263-2241,https://doi.org/10.1016/j.measurement.2019.107429.
8. Alwatyan, Abdullah & Mater, Wesam& Almutairi, Omar & Almutairi, Mohammed & Al-Noori, Aisha & Abed, Sa'Ed. (2017). Security approach for LSB steganography based FPGA implementation. 1-5. 10.1109/ICMSAO.2017.7934929.
9. R. Kaibou and M. S. Azzaz, "FPGA Implementation of Mixed Robust Chaos-based Digital Color Image Watermarking," 2021 International Conference on Networking and Advanced Systems (ICNAS), 2021, pp. 1-5, doi: 10.1109/ICNAS53565.2021.9628906.
10. Ayesha, Nigar& Acharya, Bibhudendra. (2020). FPGA Implementation of PICO Cipher. 10.1007/978-981-15-5546-6_43.
11. M. A. Alomari and K. Samsudin, ‘‘A framework for GPU-accelerated AES-XTS encryption in mobile devices,’’ in Proc. IEEE Region Conf. (TENCON), Nov. 2011, pp. 144–148.
12. J. Ben-Othman and B. Yahya, ‘‘Energy efficient and QoS based routing protocol for wireless sensor networks,’’ J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 849–857, Aug. 2010.
13. C.-H. Liu, J.-S. Ji, and Z.-L. Liu, ‘‘Implementation of DES encryption arithmetic based on FPGA,’’ AASRI Procedia, vol. 5, pp. 209–213, Jan. 2013.
14. J. Kang, D. Nyang, and K. Lee, ‘‘Two-factor face authentication using matrix permutation transformation and a user password,’’ Inf. Sci., vol. 269, pp. 1–20, Jun. 2014.
15. S. Bajaj and R. Sion, ‘‘TrustedDB: A trusted hardware-based database with privacy and data confidentiality,’’ IEEE Trans. Knowl. Data Eng., vol. 26, no. 3, pp. 752–765, Mar. 2014.