Design and Implementation of True Parallelism Quad-Engine Cybersecurity Architecture on FPGA

Nada Qaim Mohammed[1], Amiza Amir[2], Muataz Hammed Salih[3], Badlishah Ahmad[4]
Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), Ulu Pauh, Perlis, Malaysia[1, 2, 4]
IR4.0 and Intelligent Automation Group, Design and Engineering, Flex, Penang, Malaysia[3]

***Abstract*—Applications, such as Internet of Things, deal with huge amount of transmitted, processed and stored images that required a high computing capability. Therefore, there is a need a computing architecture that contribute in increasing the throughput by exploiting modern technologies in both spatial and temporal parallelisms. This paper conducts a parallel quad-engine cybersecurity architecture with new configuration to increase the throughput. using DE1-SoC and Neek FPGA boards and HDL. In this architecture, each engine operates with 600MHz maximum frequency. Each image is divided into four parts of equal size and each part processed by single engine concurrently to achieve spatial parallelism. Internally, engine is handling image's part in temporal parallelism and deep pipelining abstraction applied in every engine by dividing it to sub modules to execute different tasks concurrently. All data processed in engines is encrypted via AES algorithm that implemented as a significant part of engine architecture. The obtained results increased the throughput by four times, with 153,600Mbps, that make this computing architecture efficient and suitable for fast applications such as IoT and cybersecurity level of processing.**

Keywords*—Field programmable gate array (FPGA); spatial parallelism; cybersecurity; throughput component

I. Introduction

Data processing and transfer and store have grown dramatically in the last year because they are used in different applications via different communication networks. This growth requires an exploitation of modern technologies to enhance and increase this processing in a parallelism manner to achieve high throughput. Various algorithms and devices introduced by researchers to achieve this goal in both software and hardware implementations by exploit the available modern techniques and possibilities in temporal and spatial parallel processing [1]. Gaining high productivity requires devices that are reconfigurable, work in real-time, efficient, low power consumption, and the ability to perform parallel processing features. One of the candidates' approaches to spatial parallel processing is field- programmable gate arrays (FPGAs), whose features meet this. So, one can take advantages of FPGAs to implement a platform to achieve efficient parallelism for real time processing applications [2].

At the same time, much of the data, which are transferred through cyberspace, include confidential or personal information, so it has become a target for hackers and adversaries to access, change, or damage them. Therefore, it is necessary to use techniques that maintain the confidentiality and integrity of these data. One efficient way to achieve this is cryptography, in which various algorithms that vary in their security are proposed. An algorithm of cryptography, which has not yet been found a way to break it, is the AES algorithm [3]. However, the AES algorithm has high computational power to achieve its operations because of the large number of rounds that are used, and the need for more time to encrypt the data [4,5].

To obtain faster and more efficient computation power to encrypt massive data with high throughput, the AES algorithm must be implemented in a parallel manner. Therefore, the FPGA is a candidate approach to hardware implementation of the AES algorithm to ensure data protection, high-speed encryption rate, and high throughput.

This paper focuses on hardware architecture implementation on FPGA that based on true spatial and temporal parallelism using quad engines for cybersecurity. This architecture works through partition each image into four parts and distributes these parts to multiple engines that can process data in temporal and spatial parallelism the image parts concurrently.

The paper is organized to include a survey related work that has been conducted by some academic and researchers in Section II. Section III includes a detail description of the proposed architecture. Section IV contains the implementation results. It includes a new architecture to improve the performance in terms of the operating frequency and throughput of the AES algorithm. The results of the simulation and a comparison with previous studies are presented in Section V. Section VI presents the conclusions of the study.

II. Related Work

Different approaches have been proposed to enhance hardware implementation to obtain more image processing performance. The widespread deployment of field-programmable gate arrays (FPGAs) has enabled multi-processing in real-time processing applications, which has accelerated massive spatial parallel applications. Throughput increasing is one of the important criteria in measuring the efficiency of the used technique. To achieve this, there is a need to make use of spatial parallelism and duplicate processing units that execute simultaneously. This can done by divide the main task into several subtasks, each subtask is executed one processing elements [5]. Combining the FPGA features with spatial parallelism will help to decrease the complexity, cost, and power consumption and increase the throughput of the proposed systems. In [6], a design and

simulation was proposed to enhance the images using VHDL language using Xilinx Virtex- 2 Pro FPGA and MATLAB. In [7], the AES algorithm was implemented using Xilinx's Virtex-E and Virtex-II devices to achieve faster FPGA – based implementation. The obtained experimental results were throughput of 17.80 Gbps on a Virtex-II with a clock frequency of 139.1 MHz and 10750 slices were used.

The Altera FLEX FPGA family utility was used in [8] to execute different types of algorithms that deal with the image as a whole image instead of dealing with pixels values individually. For image encryption, Chang et al. al in 2009 implemented the AES algorithm on an FPGA using a Virtex22 device. The core of the AES was 32 bits, and it occupied 104 slices. The throughput of implementation was 794 Mbps and the efficiency was 7.93 Mb/slice [9]. In 2010, Kumar and Purohit implemented a 128-bit AES algorithm on an FPGA using a Xilinx Spartan 3 device to achieve high speed using low-cost devices [10].

In [11], Manoj and Manjula implemented an AES 128 bit using a Xilinx Spartan 6 device, 8-bit input (data pixels), and unrolled them to 128 bits. The throughput of encryption was 252.132 Mb/s, and the efficiency was 0.53 Mb/slice. In [12], Karimian, Rashidi, and Farmani implemented a 128-bit AES algorithm using an Altrea Stratix device, achieving a throughput of 617 MB/s and an efficiency of 0.76 Mb/slice. In [13], the throughput obtained from implemented a 128- bit AES using a Xilinx Spartan was 3.40 GB/s and efficiency of 5.43 Mb/slice. In [14], some algorithms for image enhancement were implemented using the Spartan3E FPGA kit to obtain high-performance digital signal processing applications. MATLAB, Xilinx ISE, Verilog HDL, and ModelSim were used for this implementation. In [15], Xilinx 14.2 software for2D and 3D image enhancement was used to design and develop algorithms to enhance the size of image pixels. In [16], the image enhancement and DE noising process was introduced using point processing methods by using a partial dynamic reconfiguration of the FPGA to decrease the requirement of resources and increase the performance. In [17], image enhancement approaches were introduced to enhance grayscale images by adopting a custom hardware processor on an FPGA. The implementation depended on the use of filters and the VERILOG hardware description language. The achieved image enhancement of these approaches used neighborhood processing operations in the spatial domain using parallel processing.

In [18], Rahimunnisa et al. the proposed structure is implemented in a Virtex-6 XC6VLX75T FPGA device, which gave a throughput of 37.1 Gb/s with a maximum frequency of 505.5 MHz in [19], Groth implemented AES encryption on a Xilinx Kintex27 FPGA for application data of the biometric image. The implementation throughput was 40 GB/s with an efficiency of 5.27 Mb/slice and a powerful performance of 286 GB/w. In [20], techniques to perform task-level out-of-order execution were proposed and implemented using the Xilinx Virtex-5 FPGA device to improve flexibility. The implementation results showed a better efficiency in terms of performance and resource usage. In [21], AES was implemented on FPGA; the obtained experimental results were a throughput of 113.5 GB/s on a Spartan-6 device. In [22], the focus was on exploring the features of FPGA parallelism to process image applications in spatial parallelism for real-time image processing. They used board DE2-115 as a vehicle project, while the VHDL hardware description language was used as the hardware design of the system. The operating frequency was 1GHz, and the system could be reconfigured to implement several algorithms using the same hardware. In [23]. In [24] architecture was conducted to optimize parallel processing and implement this architecture on FPGA. It improved the consumption of the power by 90% in compared with others. Its throughput was 1.34 GB/s at a 131.16 MHz operating frequency for processing images with a size of 512×512.

Presented two pipelined algorithms for effective processing time reduction using pipelined and parallel techniques to process the AES encryption algorithm using FPGA. Xilinx "Spartan-3A/3AN FPGA Starter Kit was used in the implementation of algorithms. The results showed that parallel implementation was good.

III. Proposed Hardware Parallelism Quad-Engine Architecture

The introduced architecture aims increasing the operating frequency and throughput, while decrease the power dissipation, area, and latency by exploiting a quad-engine with true parallelism. Each engine operates with 64 bits and a frequency of 600 MHz.

This section provides the structure of the proposed architecture and the mechanism for performing true parallelism quad-engine cybersecurity. The architecture in the spatial domain begins with the top-level design of the proposed architecture, as shown in Fig. 1.

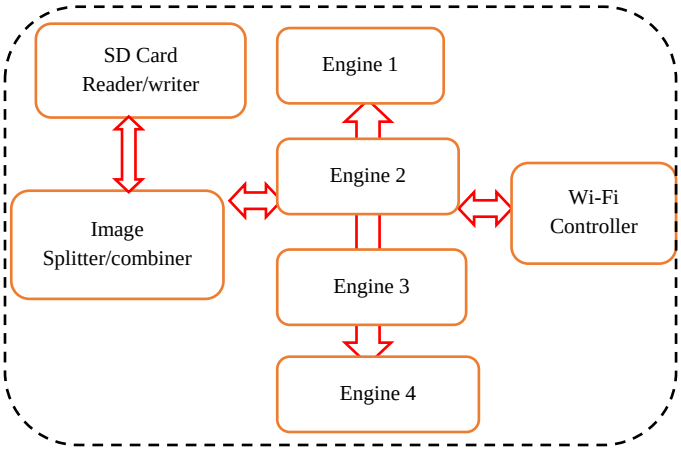

Fig. 1. System Top Level Design and Implementation True Parallelism Quad-Engine Cybersecurity Architecture.

A. Hardware Components

To implement the proposed approach, the following components are used:

- SD Card: used Micro SD card interface to read and store images.
- FPGA board: DE1-SoC board and NEEK board with the same TLD are used.

- Wi-Fi controller: Wi-Fi controller in DE1 as (Server) and Wi-Fi controller in NEEK board as (Client) to transfer the image between the two boards.

B. Software Component

The VHDL, synthesized by Altera Quartus II and simulated using Modelsim are used to implement the architecture.

C. The Proposed Algorithm

The design steps of the algorithm take traditional AES and apply it to an FPGA platform to exploit spatial and temporal parallelism to increase throughput of cybersecurity encryption/decryption processing.

Input: Images need encryption

Output: Encrypted message.

- Read four images each time and stores them on an SD card.
- Split each image spatially into equal four parts. Each part is represented by a matrix and takes a number of two digits, where the first digit is part number and the second digit is image number, (for image 1, the parts number are 11, 21, 31 and 41), Fig. 2.
- Make cycle shifting to the image parts. The shifting amount depends on the image number, as in Fig. 3.
- Sent each one of the four parts independently to one of the four-engine in the encryption/decryption unit, each engine will encrypt 1/4 image using AES 128-bit block.
- In each engine, a deep pipelining is used by divide it into sub modules to process different task.
- After encrypt the image parts, they are merged to create the encrypted image.

The cycle shifting of image parts is done as follow:

- Engine 1, will send the first part of all 4 images (11, 12, 13 and 14).
- Engine 2, will rotate (as a ring counter) forth index in this image 2 to become the first part (24, 21, 22 and 23), cycle shift by 1.
- Engine 3, will rotate again to start with the next index in image 3, cycle shift by 2.
- Engine 4, will rotate again to start with the next index in image 4, cycle shift by 3.

To decrypt the image, the encryption steps are executing in reverse order.

The architecture processes four parts at the same time, using spatial and temporal parallelism, where each engine processes one part from each image with 600MHz and 64 bits. The input images used in this approach can have different colors or grays of any size. The WIFI controller controls the transfer between the DE1-SoC board and NEEK board. It is necessary for the two boards to have the same TLD.

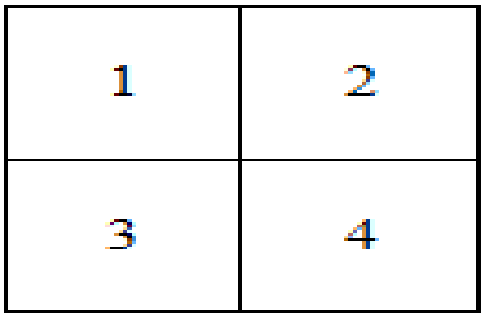

Fig. 2. Quad Sub Image.

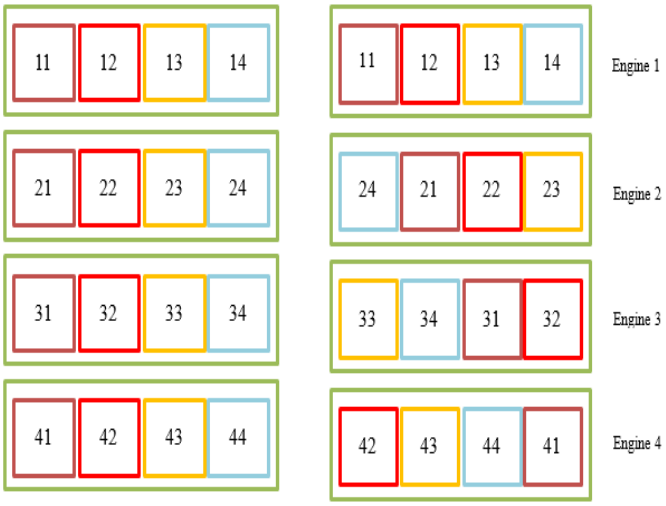

Fig. 3. Shifting Sub Image.

The throughput, number of bits processed per unit time, is measured using the following equations, specified in Mbps or Gbps.

$$\text{Throughput} = (F_{max} * 4 * \text{No.of bits processed}) \quad (1)$$

Where Fmax represent the maximum frequency and in the proposed design, taking 600 MHz for Fmax, No. of bits equals to 64 bit, whereas, the 4 represents the number of used engine.

IV. Implementation

The proposed architecture was used to implement the traditional AES algorithm as an application to encrypt four image at the same time.. To encrypt these images the DE1_Soc, Neek board FPGA device, and Wi-Fi (server and client) are connected together. The Altera Quartus Prime18.1 tool used for the synthesis. These images may have different types of colors or gray of any size.

First, the images were read, as shown in Fig. 4. After reading the image will be doing splitting process, each image was split into four sub-images. Fig. 5 illustrates the sequence of quad sub image 1, 2, 4, and 5.

Then perform the cycle shifting for parts of each image independently, Fig. 5.

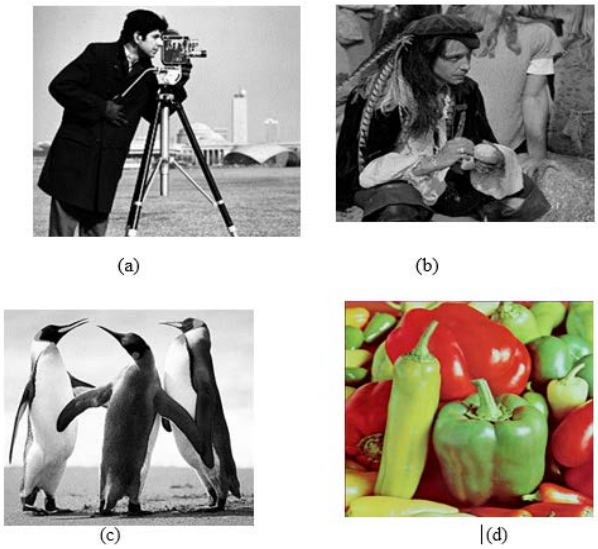

Fig. 4. Input Image.

Fig. 5. Step 1Split Image to Sub Images.

Now, each part is transferred to a separate engine for execution, which performed in a pipelining manner, temporal parallelism. The engine consists of the necessary operation of an encryption/decryption unit. Each engine operates at 600 MHz, and each sub-image part is encrypted by one engine. The four sub-image encryption was performed simultaneously, as shown in Fig. 6.

In Fig. 6 to 10 shows images of real-time execution on FPGA that are highlighted on the LCD touch screen of the NEEK board. VHDL is used to write the design code, in addition to use Altera Quartus II for synthesized. Fig. 6 shows the sub-images of the four image parts after the splitting process is performed.

Each part of the image is sent independently to one of engines, and then a new part of new image following it. Sub images are reordered and sent to make the system more secure.

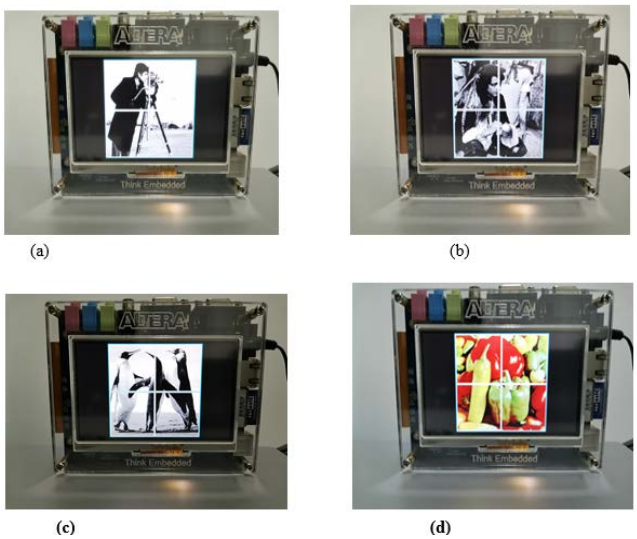

Fig. 6. Split each Image into 4 Sub-Images.

Fig. 7. Split Image Step to Sub Images.

Fig. 8. Real Live Implementation of First Splitting on NEEK Board.

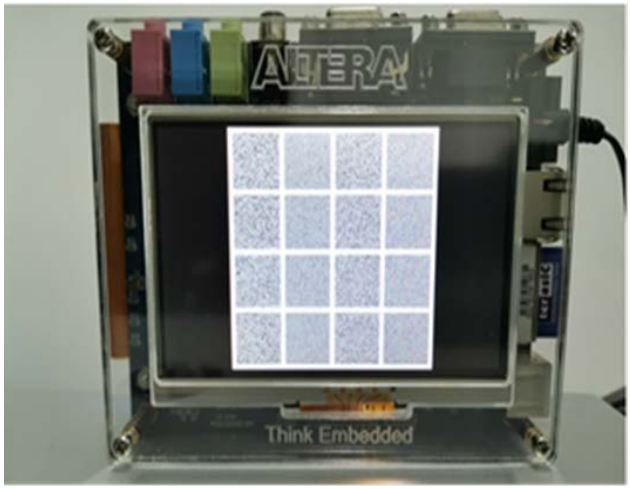

Fig. 9. Real Live Encryption of Images Splitting on NEEK Board.

Fig. 10. Real Live Implementation of Second Splitting on NEEK Board.

Table I includes the details Altera Quartus utilization and Table II includes performance comparisons with other works.

TABLE I. SUMMARY OF DEVICE UTILIZATION USING ALTERA QUARTUS

Resources	Available	Used	Utilization
Total Logic Element	25K logic elements (LEs)	19,351	77.4%
Dedicated Register	50	43	86%
Memory Bits	66 M9K	428,133	68%

TABLE II. PERFORMANCE COMPARISON

Reference	FPGA Device	Throughput
Our architecture	The DE1_Soc, Neek board	153,600Mbps
[7]	Virtex-II	17.8 Gbps
[9]	Virtex 22	794 Mbps
[11]	Xilinx Spartan 6	252.132 Mbps
[12]	Altera Statix	617 Mbps
[18]	Virtex 6	37.1 Gbps
[21]	Spartan 6	113 Gbps
[23]	Spartan 3A/3AN	1.34 Gbps

The obtained results showed the increasing in the throughput by four times, the throughput rate becomes 153,600Mbps that make this introduced architecture efficient and suitable for fast applications Area utilization was specified with respect to the number of slices used in Altera FPGAs. Additionally, four look-up tables (LUTs) and eight storage elements exist in each slice of the Altera FPGA.

V. CONCLUSION

This study demonstrates the architecture ability to perform the AES algorithm in spatial and temporal parallelisms. To implement this project, several Altera® Nios II Embedded Evaluation Kit and Cyclone III Edition features were harnessed, such as switch inputs and the LCD touch screen alongside the LEDs. Each of the four engines operates with maximum 600 MHz clock frequency, and the implementation results throughput rate is 153,600Mbps. These results make this introduced architecture efficient and suitable for fast image processing, such as using complex cyber security algorithms for secure information.

ACKNOWLEDGMENT

I would like to thank my supervisors Dr.Amiza Amir and Dr. Muataz Hameed, UniMAP staff, my family, and everyone who supported me to make this work.

REFERENCES

[1] A.A Purkayastha, S.A. Shiddhibhavi, and H.Tabkhi , “Taxonomy of Spatial parallelism on FPGAs for Massively Parallel Applications”,in proc 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, USA). pp. 55-60. . (2019).

[2] N. Q. Mohammed , M. H. Salih , R. Aliana , Q. M. Hussein and N. and Aldeen A. Khalid, “FPGA Implementation of Multiple Processing algorithms using spatial parallesim" , ARPN Journal of Engineering and Applied Sciences, VOL. 13, NO. 15, PP.4556-456,. 2016.

[3] N. Q. Mohammed, Q. M., Hussein, S. M. A,K, and Layth A.A, “Hybrid Aproach to Design Key Generator of Cryptosystem”, Journal of Computational and Theoretical Nanoscience, Volume 16, Number 3, pp. 971-977, 2019.

[4] M. E. Hameed, M. M. Ibrahim, and N. A. Manap, “Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security”, Journal of Telecommunication, Electronic and Computer Engineering, Vol. 10, No. 1, pp. 139 – 145, 2008.

[5] F. A. Habib and Q. M. Hussien, “Survey on Data Security Techniques in Internet of Things” , AL-Kunooze Scientific Journal, vol. 2, no. 2, pp: 27 – 37, 2021.

[6] L. Lan, “The AES Encryption and Decryption Realization Based on FPGA”, Seventh International Conference on Computational Intelligence and Security, Sanya, China, pp 603-607, 2011.

[7] K. Jarvinen, M. Tommiska, and J. Skytta, “A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor,” Proceedings of the 2003 ACM/SIGDA Eleventh International Symposium on Field Programmable Gate Arrays, Monterey, California, USA pp 207-215.

[8] O. F. Yousif, M. H Salih, L. A. Hassnawi, M. A. Albreem, M. Q Seddeq. and H. M Isam, "Design and implementation computing unit for laser jamming system using spatial parallelism on FPGA", In proc. IEEE International Conference on Signal and Image Processing Applications (ICSIPA), Kuala Lumpur, Malaysia, pp. 38-43, 2015.

[9] K.H. Chang, Y.C. Chen, C.C. Hsieh, C.W. Huang and C.J. Chang, “Embedded a low area 322bit AES for image encryption/decryption application” in Proc. IEEE International Symposium on Circuits and Systems, Seoul, pp. 1922–1925, 2009.

[10] Y. Kumar and P. Purohit, “Hardware Implementation of Advanced Encryption Standard” in Proc. International Conference on

Computational Intelligence and Communication Networks, Bhopal, pp.4402442, 2010.

[11] B. Manoj and N. Manjula, “Image Encryption and Decryption using AES. International,” Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 5, pp. 210822112, 2012.

[12] G.H Karimian., B. Rashidi. and A. Farmani, “A High Speed and Low Power Image Encryption with 1282Bit AES Algorithm,” International Journal of Computer & Electrical Engineering, vol. 4, no. 3, pp. 290-294, 2012.

[13] M. Gore. and V. Deotare, “FPGA Implementation of Area Optimized AES for Image Encryption/Decryption Process", international journal of next generation computer application (IJNGCA), vol. 1, no. 9, pp 23-26, 2013.

[14] P. vanaparthy,. G, K. Sree and C.D. Naidu. "FPGA implementation of image enhancement algorithms for biomedical image processing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 2, no. 11, pp. 5747-5753, 2013.

[15] P.S., R. India, A.Kumar and N.Singh, "FPGA Implementation of 2D and 3D Image Enhancement Chip in HDL Environment", International Journal of Computer Applications, vol. 62, no. 21, pp. (0975-8887), 2013.

[16] C. K. Sundaram, M. Elango and P. Marichamy, "Implementation of Image Processing Algorithm Using Partial Dynamic Reconfiguration in FPGA", International Journal of Innovative Research in Science, Engineering and Technology. Vol. 3, no. 3, pp. 1457-1462, 2014.

[17] K. B. Ravi Teja, A. S. Warrier, A. S. Belvadi, and D. R. Gawhane, "Design and Implementation of Neighborhood Processing Operations on FPGA using Verilog HDL", IOSR Journal of VLSI and Signal Processing (IOSR-JVSP). Vol. 4, no. 1, pp. 75-80, 2014.

[18] K. Rahimunnisa, P. Karthigaikumar, Soumiya Rasheed , J. Jayakumar and S. SureshKumar, "FPGA implementation of AES algorithm for high throughput using folded parallel architecture, security and communication network, vol. 7, pp. 2225-2236, 2014.

[19] T. H. Groth, "FPGA Optimization of Advanced Encryption Standard Algorithm for Biometric Images", M.S. thesis, Luleå University of Technology, Sweden, 2014.

[20] Chao Wang, Junneng Zhang, Xi Li, Member, Aili Wang, and Xuehai Zhou, "Hardware Implementation on FPGA for Task-Level Parallel Dataflow Execution Engine", IEEE transaction on parallel and distributed systems, vol. 27, no. 8, pp. 2303-2315, 2016.

[21] U. Farooq and M. F. Aslam, “Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA,” Journal of King Saud University-Computer and Information Sciences, vol. 29, no. 3, pp. 295–302, 2017.

[22] N.Q. Mohammed , M.H. Salih, R. Aliana, Q. M. Hussein and N. A. Khalid, "Design and implementation Image Processing functional units using spatial parallelism on FPGA", ARPN Journal of Engineering and Applied Sciences, vol. 13, no. 15, PP. 4514-452, 2018.

[23] A. Phadikar, H. Mandal and T. L. Chinu, "Parallel hardware implementation of data hiding scheme for quality access control of gray scale image based on FPGA", Multidimensional system and signal processing, volume 31, pp. 73-101, 2020.

[24] M.Nabil1 , A.A. M. Khalaf2 , S.M. Hassan Design and implementation of pipelined and parallel AES encryption systems using FPGA. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 20, No. 1, pp. 287-299. 2020.