Review on performance of 3D Image Encryption and Decryption using AES Algorithm

[1]Beeda Sukumar, [2] E. Lakshmi prasad, [3]S.Chnadra Mohan Reddy

[1]Assistant Professor, [2]Rsearch scholar, [3]Associate professor
[1]ECE, [1]MITS, JNTUA, Madanapalle, INDIA

***Abstract*— Cryptography is a technique, rapidly used to protect the information in recent innovations. Since several years, AES is a standard algorithm majorly used for security purpose among the cryptography techniques. There are several AES designs available such as three step AES approach, extended version of AES with DSP units, pipelining approach and so on. This review paper presents on 3D-Image encryption and decryption using AES. So, here major objective of this paper is to collect the various methods of AES designs related to achieving better throughput for 3D-Image. Here, not only that various approaches of AES designs are compared with respect to area, power, and latency.**

Keywords: AES, Encryption and Decryption, block cipher and 3D-Image.

I. INTRODUCTION

In day to day life, a huge number of sectors exchange the large amounts of the database in various fields such as banking sectors, financial sectors, and medical sectors and so on. So, in these sectors security is essential. There are several sectors which want to keep secure the database then only data cannot be hacked. Most of the sectors secure the database using cryptography techniques. There are several cryptography techniques that are available such as DES, triple DES, Blowfish, two fish, RSA, and AES. Among all cryptography techniques, AES [1] is one of the standard algorithms.

Triple DES is a technique, which consists of three individual keys and each key contains 56-bit length. The total key length is about 168 bits but experts prove that 112-bit key length is enough to encrypt the data. But, the drawback of this DES, it can be broken with the help of brute force attack technique.

RSA is a public key encryption algorithm which is an asymmetric algorithm and it uses a pair of keys. Here, the public key is used encrypt the message and it can be decrypt by the private key. RSA is better than DES, but the drawback of this RSA operates at low speed.

Blowfish is another algorithm that is designed to replace DES. Here, 128-bit cipher splits the messages into two blocks of 64 bits and each block of data encrypts separately. When compared to previous algorithms blowfish is faster and secure and it is specifically used in e-commerce platforms.

Two Fish is symmetric algorithm technique which consists of 256 bits and it requires one symmetric key is enough to encrypt and decrypt the data. This design is likely supported for both hardware and software platforms.
AES is trusted algorithm recognized by the US government and numerous organizations. AES[3] supports 128, 192 and 256 bits in length and it also supports for large data. AES is largely considered as impervious to all attacks. Data Encryption Standard (DES) was given high priority in earlier days, but now a days AES strongly considered as standard for symmetric key encryption. Symmetric means same key is used for encryption as well as decryption.

Here, in DES, it has a key length of 56 bits which is currently considered as smaller and it can be easily broken. Due to this reason, the National Institute of standards and Technology (NIST) offered a formal call in 1997 September. To design and develop an AES algorithm around 15 candidates has involved in 1998 August. Later in 2000, August NIST selected five members namely Mars, RC6, Rijndael, Serpent and Two fish considered as the final competitors. Finally, Rijndael algorithm was the winner.

Another name of AES is Rijndael. It has fixed block size of 128 bits, 192 bits, and 256 bits and their key sizes are also 128,192 and 256 bits respectively. The main objective of this survey paper is to present an overview of AES algorithm measured with respected to throughput. AES is more reliable architecture and it can be easily operated at low latency with high throughput.

II. RELATED WORK

One criterion for the design of AES algorism is that can be implemented in hardware and software. In this section discussion on the previously proposed works related to AES implementation by using FPGA boards. There are various techniques that are proposed by different authors on achieving high throughput and reduced latency.

M.C.LIBERATORI et al. [3] Proposed a paper on the low area, cost effective Rijndael cipher for encryption and decryption designed by using a basic 8-bit iterative architecture, and it is targeted on altera flex 10k family of FPGA. The cipher has been synthesized using AlteraMAX + PLUS II version and the algorithm is Implemented using VHDL. These design method got 6.8Mbps throughput.

Amruta et al. [4] presented a paper on AES 128 key Expansion using LUT (Look up Table) and OTF (On the fly)S-Box. The first approach uses LUT based S-Box which got a throughput of 8Gbps. In 2ndapproach, it uses S-Box values which got a throughput of 8Gbps.The implementations were targeted on 90nm CMOS technology using standard library cells. Both the designs were clocked at 250MHz.

Sonali et al. [5] presented a paper on Implementation of AES Algorithm using FPGA and it performance Analysis, where the AES algorithm can process data blocks of 128 bits and this algorithm got achieved low latency and throughput is 465Mbps for encryption and 189Mbps for decryption.

Y.Aruna et al. [6] presented a paper which performs a real-time data communication exhibiting a significant level of security and provides faster processing time wherever required. A unique feature of the proposed pipelined design is that the round keys, which are consumed during different iterations of encryption, are generated in parallel with the encryption process.This lowers the delay associated with each round of encryption and reduces the overall encryption delay of a plaintext block. This will leads to an increase in the message encryption throughput.

Hrushikesh et.al [7] proposed an architecture which achieves good performance and occupies less area. It also reduces no. of slices. It also makes necessary a high throughput selection ratio.

Sagar Deshpand et al. [8] proposed several ways for performing AES Operations at higher throughput using on-chip RAM and DSP blocks with very less usage of flip flops and look-up tables that are verified Encryption rate of 128,176 and 192 bits is achieved for a better throughput at a rate of 1.92, 1.89 and 1.73 Gb/Sec respectively.

Yewale Minal J ,M.A.Sayyad [9] Proposed that AES can process data blocks of 128bits. It is implemented using Xilinx 8.2. It operates at 2059Mbps which are completely high throughput.

M. Sambasiva Reddy, Mr. Y. Amar Babu [10] implemented 128 bit AES encryption and decryption algorithm by using the Spartan-3E device. This paper describes that AES algorithm using EDK (Embedded development kit) is a better solution than Software and Hardware implementation.

Related Performance comparison of AES-128 bit :

Table-1 AES SURVEY REPORT:

Authors Et al.	**title**	**HDL**	**Clock frequency**	**Hardware Used**	**Throughput**	**Advantage**	**Year**	**Ref**
M.C.LIBERATORI and J.C.BONADERO	AES-128 CIPHER. MINIMUM AREA, LOW-COST FPGA IMPLEMENTATION	VHDL	25MHZ	FPGA	11Mbps	Less area and cost optimized	**2007**	**[3]**
AmrutaPage, P.V.Sriniwas Shastry	AES 128 Key expansion with LUT and OTF S-BOX	VHDL	250MHZ	--	8Gbps	High throughput	**2014**	**[4]**

Sonali A.Varhade, N.N.Kasat	Implementation of AES Algorithm Using FPGA & Its Performance Analysis	VHDL	--	ALTERA QUARTUS-II	465Mbps for encryption and 189Mbps for decryption.	Low latency and high throughput	**2013**	**[5]**
Y.Aruna	FPGA Based Implementation of AES Encryption and Decryption with Verilog HDL	VHDL	50MHZ	--	3972.2bps for encryption and 30825.1bps for Decryption.	Processing time is faster.	**2014**	**[10]**
Sagar Deshpande ,Leelavathi.G	Design and Implementation of Extended Version of AES Algorithm with DSP Units	VHDL	--	SPARTAN-6	1.92, 1.89 and 1.73 Gb/Sec encrypt rate for 128,176,192 respectively	High throughput	**2013**	**[8]**
Yewale Minal J ,M.A.Sayyad	Implementation of AES on FPGA	VHDL	160.875 MHZ	SPARTAN-3	2059Mbps	High throughput	**2014**	**[9]**
M.Sambasiva Reddy,Mr.Y.Amar Babu	Evaluation Of MicroBlaze and Implementation Of AES Algorithm using Spartan-3E	VHDL	--	SPARTAN-3	--	Operates faster than software and hardware using EDK	**2013**	**[10]**

III. METHODS:

In this section, we would like to present some techniques of previous works related to AES implementation with different approaches. With this techniques, we can gain information on a solution to get low latency and also high throughput.

3.1 TWO IMPLEMENTATIONS OF AES-128 KEY EXPANSION:

This is a technique was introduced by the Amrutha, P.V.S [4]. One method was implemented using look up a table called as s-box which contains already calculated values of byte substitution transformation I, the e-sub byte in AES. Another implementation uses the combinational logic based on Galois field (GF) arithmetic that calculates s-box values on-the-fly.

3.2 KEY EXPANSION USING LUT FOR S-BOX:

Here s-box lookup table is used for the sub word operation. The data path of 32 bits and 4 instances of s-box to make an operation it requires four clock cycles. Initially, the cipher key is loaded with four 32 bit registers w0,w1,w2,w3.In order to generate w4,w3 is applied with transformation Rotoworld(), sub word() and then XORed with RCon and the transformed word is XORed with w0. Thus, for every clock cycles, we get 128-bit key expanded for a particular round and the key generated is used as input to next round of key expansion. For 10 round keys, 40 clock cycles are required.

3.3 KEY EXPANSIONUSING ON THE FLY S-BOX:

Architecture is same as shown in figure-a but to performing sub word operation different method is used. combinational logic based on composite field arithmetic is used to calculate multiplicative inverse in GF(2^8) I,e first step for calculation of s-box. Later affine transformation is applied for the multiplicative inverse to obtains-box value. Comparing the above two methods the first method achieves better throughput but occupies more area than the second method.

3.4 PIPELINED FPGA IMPLEMENTATION OF AES ALGORITHM:

This type of architectural optimization has been incorporated which includes using the pipelining techniques. Speed is increased by processing multiple rounds simultaneously but at the cost of increased area. The corresponding hardware realization offers high data throughput and is optimal in terms of area. An optimized code for the implementation of this algorithm for 128 bits has been developed and experimentally tested using Xilinx device. So, the focal approach of this design on a hardware platform is to attain speed up (i.e. high throughput No. of block processed per second) at the same time, silicon area optimization.

From the analysis, we can find that the process of AES encryption and Decryption can be mainly divided into two parts: key schedule and round transformation. The improved structure is also divided into these two major processes. The initial key will be sent to the two modules: Key expansion and Key selection, While the plaintext is to be sent to the round transformation during Encryption and cipher text are sent to round transformation after the round key is selected. But the operand of data transmission is turned into a 32-bit unit. Generally, there are four steps like sub-byte, shift rows, mix columns and add round key in normal rounds.here, in this design they made some modifications like

- Exclusion of shift rows OR merging of sub-byte and shift rows.
- Pipelining for high throughput.
- Optimization of design to balance between throughput and silicon area.

By pipelining, techniques speed is increased by processing multiple rounds simultaneously but with the cost of increased area. Due to this corresponding hardware realization is optimal in terms of area and offers high throughput.

The process of the new algorithm is shown as Figure (a) & (b).

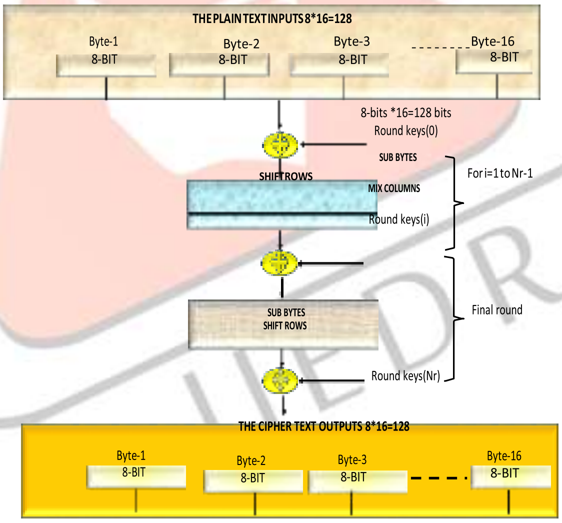

Figure (a): AES algorithm for Encryption

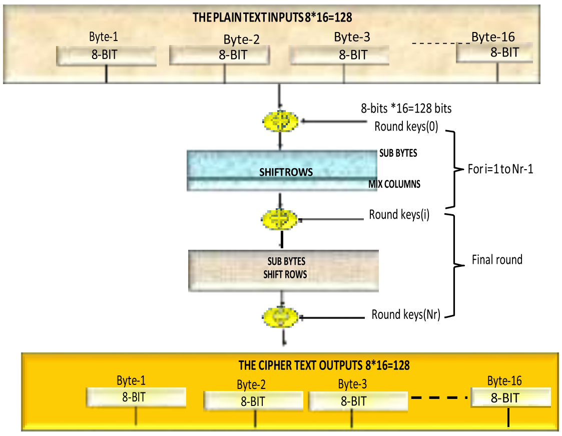

Figure (b) AES algorithm for Decryption Flow

3.5 EXTENDED VERSION OF AES ALGORITHM WITH DSP UNITS:

This technique is used by Sagar Deshpande, Leelavathi G. Here in this AES Cipher implementation is based on the Block RAM and DSP units implemented by using Xilinx's Spartan-6 FPGA'S. An iterative basic module output of the 32-bit column, in each clock cycle, overall throughput is 1.76 Gbps. The whole process is replicated ten times for a fully unrolled design that gets nearly 55 Gbps of throughput. High throughput implementations are used for high-end devices. This is widely used for high performances in the utilization of today's hardware accelerators for cryptography algorithms.

In modern devices, the software-oriented approaches are reconfigurable hardware devices in order to achieve high throughput. Here, the implementation was done by using Xilinx Spartan-6 FPGA which has advanced features that are useful for different applications beyond the traditional LUTs and registers. These are dual ported 36 Kbit Block RAMs (BRAM) - ones which have an independent address and data buses for the same stored content and versatile digital signal processing (DSP) cores. The DSP cores that are used to allow the designer to implement timing functions or resource-critical functions like arithmetic operations on integers or Boolean expressions.

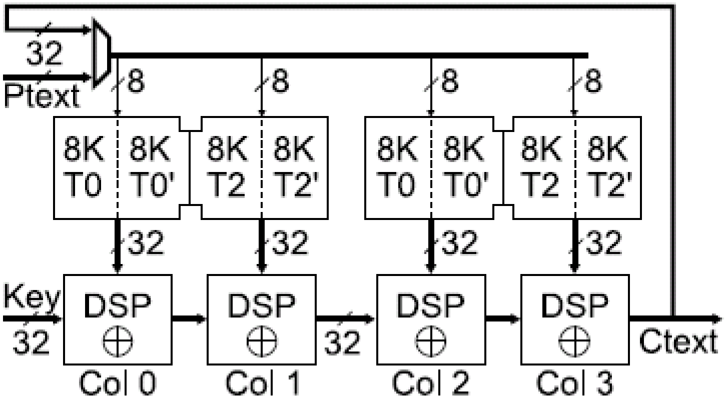

Figure-2: The basic construct structure.

IV. PERFORMANCE ANALYSIS:

4.1 SURVEY ON PREVIOUS WORKS ON MODES:

As mentioned above those modes are used for AES encryption and decryption. Each mode has its own importance by comparing their frequency, throughput, number of gates and their characteristics as shown in Table-2.

Table-2 Comparison of modes and Methods

Modes /methods	Process	Frequency	Throughput	No of gates	Ref
Counter mode & CBC Mode	Dec	148 MHz	1722Mbps	7301 CLB Slices	[2]
CTR mode & CBC mode	Enc	194 MHz	2257Mbps	6766 CLB Slices	[2]
CFB mode	Enc/Dec	140.390MHz	352 Mbits/sec	1853 Slices	[3]
Pipelined	Enc	271.15MHz	34.7 Gbps	2389 Slices	[4]
Single round loop unrolling	Enc	91.049MHz	224.12 Mbps	1643 Slices	[5]

Fully pipelining	Enc	341.53MHz	43.71 Gbps	7865 slices	[6]

4.2 PERFORMANCE COMPARISON OF THROUGHPUT, LATENCY ON DIFFERENT FPGA BOARDS:

The AES algorithm can be implemented in different FPGA Boards to increase the speed throughput and latency. Following table-3 gives a view on the throughput, latency, area slices when implemented on different FPGA boards:

Table-3: Different types of FPGA Implementations

Process	FPGA	frequency	Throughput	Latency	Area slices	Mbps/slice	ref
Enc	Virtex-E XCV1000e-8	129.2 MHz	16,500 Mbps	--	11,719	1.408	[9]
Enc	Virtex-E XCV2000e-8	158 MHz	20,300 Mbps	--	5810 + 100BRAM	1.091	[10]
Enc	Virtex-E XCV3200e-8	145 MHz	18,560 Mbps	--	15,112	1.228	[11]
Enc	Virtex-II XC2V4000	184.1	23,570	163	16,938	1.391	[8]
Enc/ Dec	Virtex-E XCV2000E-8	184.8	23,654	379	16,693	1.417	[12]

V. CONCLUSION:

As mentioned earlier the main concept that is required for 3D- image processing is used to store the information with less memory with the secure transmission. One such technique, AES, a symmetric block algorithm can able to implement both in software as well as hardware. But implementing in software is a slow process and has low security. Hence to avoid this problem, hardware implementation takes place. Here in this paper, a review on performance comparison of AES with different types of implementations and 3D-Image processing implementation process. Performance parameters of design calculated in terms of throughput and results compared with different works.

VI. ACKNOWLEDGMENT

The authors would like to thank the principal and management of Madanapalle Institute of Technology and sciences for their support for encouragement for publication.

REFERENCES

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

[2]. Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare,(2011)" FPGA Implementation of AES Algorithm", IEEE, Volume : 3,pp 401-405.

[3]. M.C. Liberartori, J.C Bonadero "AES-128 bit Cipher, minimum area, Low-cost FPGA Implementation" latin American Applied research 2007.

[4]. Amruta R.Dumane, Prof.N.G.Narole, Prof.Prashant Wanjari, "Review on Implementation of Advanced Encryption Standard on Soft-core Processor" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2016.

[5]. Sonali A. Varhade, N. N. Kasat " A Review on Implementation of AES Algorithm Using FPGA & Its Performance Analysis", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 1, Jan 2015

[6]. Y.Aruna, Prof. Bharati Masram" FPGA Based Implementation of AES Encryption and Decryption with Verilog HDL" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622.

[7]. Deshpande, Hrishikesh S; Karande, Kailash J; Mulani, Altaaf O " efficient implementation of AES algorithm on FPGA" IEEE International Conference on Communications and Signal Processing (ICCSP) 2014.

[8]. Sagar Deshpande ,Leelavathi.G'S " Design and Implementation of Extended Version of AES Algorithm with DSP Units "International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 14 Issue 2 –APRIL 2015.

[9]. Yewale Minal J , M. A. Sayyad "Implementation of AES on FPGA" IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 4, Issue 5, Ver. II (Sep-Oct. 2014), PP 65-69 e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197.

[10]. Sneha Ghoradkar, Aparna Shinde "Review on Image Encryption and Decryption using AES Algorithm", International Journal of Computer Applications (0975 – 8887) -2015.

[11]. Yulin Zhang, Xinggang Wang, (2010)"Pipelined Implementation of AES Encryption Based on FPGA", IEEE,pp170 - 173.

[12]. Monica Liberatori, Fernando Otero, J. C. Bonadero, Jorge Castifieira,(2007)"AES-128 cipher. high speed, low cost fpga implementation", IEEE.