An Enhanced Image Cryptographic Method Based on AES Rijndael Algorithm

Sindhu G R[1] Anitha D B[2]
[1]P.G. Scholar [2] Associate Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]VVIET Mysuru, India

Abstract— Now a day's a lot of internet and wireless connections customers has led to an enhancing need for solutions of security measures and devices for protecting the consumer details approved on over the unsecured network so that unlawful people cannot access it. As we share the important details through wireless media it should provide details comfort, stability and entity confirmation. The symmetric block cipher works a big part in the bulk details protection. Advanced Encryption Standard (AES) as Rijndael algorithm provides data protection. AES has the key advantages of being used in both software and hardware. Hardware implementation of the AES has a lot of benefits such has prolonged throughput and better protection level. The design uses an iterative looping approach with block 128 bits and key size of 128 bits, 192 bits and 256 bits, the lookup table implementation of S-box so as to reach the purpose of improving the system computing speed the pipe-lining and parallel processing methods were used. Components Performance for 128 bit AES (Advanced Security Standard) protection and decryption has been made using VHDL. The recommended requirements for encryption and decryption aspect will functionally verified using modelsim, will be synthesized using Xilinx_ISE_13.2 software Spartan-3 FPGA platform and assess the design for the power, throughput & area.

Key words: AES, Rijndael, Block cipher, Encryption, Decryption, FPGA, VHDL

I. INTRODUCTION

In today's world most of the communication is done using digital media. Information security works a significant part in such communication. Improving need of data manages in computer Program and interaction technology capable of excellent huge of data and knowledge needs to be interchanged by public connection techniques. Each day a lot of customers generate and change considerable amounts of details in various areas, such as financial and legal information, medical opinions and bank services via internet. These and other types of applications have entitlement to a special treatment from the security viewpoint, not only in the transport of in the same way details but also in its storage space. In this sense, cryptography techniques are especially appropriate. This performance will be useful in wireless protection like military connections and mobile phone where there is a higher concentrate on the speed of connections. Cryptography is the technology of key specifications, enabling the comfort of connections through an insecure port. It protects against unlawful activities by preventing unauthorized difference in use. Generally, it uses a cryptographic system to change a plaintext into a cipher published written text, using most of the time a key. In this sense, cryptography techniques are especially appropriate. This implementation will be useful in wireless protection like military connections and mobile phone where there is a higher concentrate on the speed of communication. The Advanced Encryption Standard (AES) was launched by the National Institute of Standards and Technology (NIST) in 2001. AES is a symmetric block cipher that was created to return DES as the approved conventional for a huge number of applications. In evaluation to public-key ciphers such as RSA, the residing of AES and most symmetric ciphers is quite complex and cannot be described as easy as many other cryptographic techniques. AES has already acquired comprehensive use because of its protection, premier in both hardware and software. Many implementations are done in software but it seems to be too gradual for convenient applications such as routers and some wireless connection techniques. The several of AES elements performance architectures and optimizations have been appropriate different applications. The AES algorithm is a symmetric block cipher that can protect and decrypt information. AES is based on a design known as a substitution-permutation system, a combination of both alternative and permutation, and is fast in both software and hardware. In evaluation to its precursor DES, AEs does not use a feistel system network.

II. LITERATURE REVIEW

Wang Wei, Chen Jie, Xu Fei [1] presented the mathematic concept, security procedure and logic framework of AES criteria. So as to achieve the objective of helping the system handling rate, the pipelining and parallel handling methods were used. The simulation results show that the high-speed AES security criteria applied properly. Using the method of AES security the information could be successfully secured. AES is a repetitive team rule with the key. The security procedure contains a preliminary key-addition known as add round key, then a preliminary circular transformation for 1 r N −times, lastly a last circular modification again. All the circular alterations and preliminary key-addition make a state and a round key as the input, and each pattern provides out four different functions to the data circulation, sub-bytes, shift rows, It is not compatible to apply the AES criteria on hardware between the throughput and element source.

Jun, Ding Jun Li, Na Guo Yixiong [2], [3] presented the system is targeted at reduced elements structure. Compared with the direction, structure, it has less elements resources as well as cost-effective and this system has great protection and stability. This AES system can be widely used in international terminal accessories. An AES protection requirement contains a key development process and encryption process. The protection process contains an initial add a round key of the initial circular, and then works several models of round realignment, and the last circular also work round adjustment The overall structure of the designed reduced AES protection and decryption system in which the

upper half part is the protection system, the second part is the decryption system.

Hoang Trang, Nguyen Van Loi [4] presented FPGA-based execution of the Advanced Encryption Standard (AES) algorithm. The design uses a repetitive looping strategy with block and key size of 128 bits, lookup table execution of S-box. This gives low complexes structure and easily accomplishes low latency as well as high throughput. Simulator outcomes, efficiency answers are provided and in contrast to past revealed styles. The AES criteria runs using a 128-bit block of data and implemented Nr - 1 cycle times. A cycle is known as a circular and the number of versions of a cycle, Nr, can be 10, 12, or 14 based upon on the key time frame. The key duration is 128, 192 or 256 bits in duration respectively.

Kbanob, Thongkhome, Chalermwat Thanavijitpun [5] offered the efficiency result on the focused FPGA, the main recurring AES protection can offer the throughput and one stage sub pipelined AES can offer the throughput to increase the efficiency. AES main of practical, challenging generate can be designed in either main recurring AES or one stage sub-pipeline AES framework according to the details amount required. The same set of elements is reprocessed for all the ten editions. This framework is entirely based on the recurring strategy of design for protection techniques. The key growth avoid creates the key required for the corresponding edition on the fly. This design uses the parallelism in the AES requirements and increases the throughput of the design. It is an improvement of the main recurring framework with regards to rush. Recommended AES main framework can be selected upon amount or throughput need for supporting practical challenging generate details protection.

Pravin B. Ghewari, Jaymala K. Patil [7] Offered the cryptographic techniques can provide with the application or created with authentic elements. However Field Programmable Gate Arrays (FPGA) performance provides a quicker remedy and can easily be enhanced to add any technique changes. This contribution looks into the AES protection and decryption cryptosystem relevant to FPGA and Very High Speed Integrated circuit Hardware Description Language (VHDL). Improved and Synthesizable VHDL concept is created f2or the performance of both 128-bit information protection and decryption process.

Amaar, I. Ashour and M. Shiple [8] offered a light-weight performance of Advanced Encryption Standard (AES) using different devices of FPGA technological innovation. This implementation can be taken out through several trade-offs between position and amount. The main point of the recommended framework is to deal the position and amount. Register- Transfer-Level (RTL) is analyzed frequently to avoid recurring elements growth. suggested framework is implementing 128 bit data-path for both cipher key and plaintext. The developed framework delivers together main framework with one round and reducing technique to deal the position with amount.

III. AES RIJNDAEL ALGORITHM

AES comes in three designs, specifically AES - 128, AES - 192, and AES-256, with the variety in every part talking with the dimensions (in bits) of the key used. All the ways are done in 10, 12 or 14 circular depends on the dimensions of the block and the key length selected. AES are only allowed 128 bit details, duration that can be partitioned into four important functional blocks. These blocks form condition by operating on an array of bytes and consisting as a 4*4 structures or matrix. The criterion begins with an Add circular key level took after by nine units of four levels. 10th circular includes three levels, which are applicable for both encryption and decryption criteria.

The units for algorithm are applied by the four levels here.

- Substitute Bytes
- Shift Rows
- Mix Column
- Add Round Key

In the tenth (final) circular Mix line level is omitted. The preliminary nine units of the decryption criteria are applied by the associated with four stages.

- Inverse Substitute Bytes
- Inverse Shift Rows
- Add Round Key
- Inverse Mix Column

Again in the last (tenth) circular Inverse Mix columns level is excluded. The figure1 (a) and 1 (b) shows the overall circulation of the AES Rijndael algorithm.

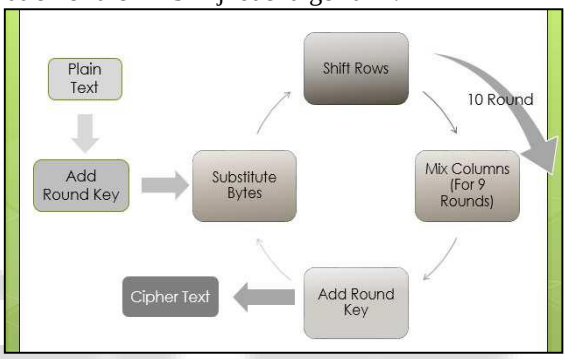

Fig. 1 (a): AES Encryption Process

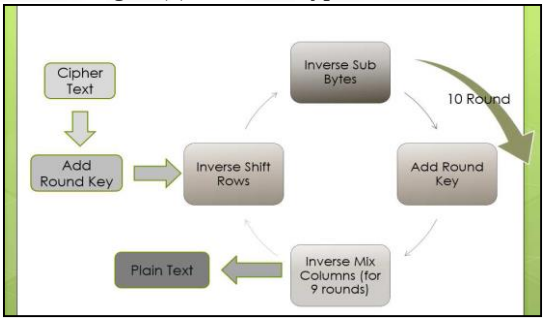

Fig. 1 (b): AES Decryption Process

IV. METHODOLOGY

The AES uses a 128-bit key and 128-bit data block. The 128-bit plaintext and the 128-bit initial key, as well as the 128-bit output of cipher text, are all divided into four 32-bit consecutive units respectively controlled by the clock. In order to accommodate the several rounds using a single key in both encryption and decryption, a key expansion algorithm is used. Throughout the steps of operation, the current value for the system is stored in a dual port RAM. . In order to keep the operation of the AES core simple, memory mapping is used. The system state is a 128-bit variable that starts with the contents of the plaintext, and ends with the contents of the cipher text. The 128-bit data input is viewed as a byte matrix with four rows and four columns. The major steps involved

in each round are the Byte Sub, Shift Row, Mix Columns, and Add Round Key these four transformations are described as follows:

A. *Byte Substation*

Each byte of the state is replaced with an 8-bit value from the S-box. The S-box contains a permutation of all possible 256 8-bit principles. It is a nonlinear function and the only non-linear modification in this process. The S-box is obtained by a multiplicative inverse over GF (2^8) and an affine convert. The sub bytes function is needed for both security and key development and its inverse is done for decryption. Its execution has a primary effect on the overall throughput. The figure2 illustrates the byte substitution transformation.

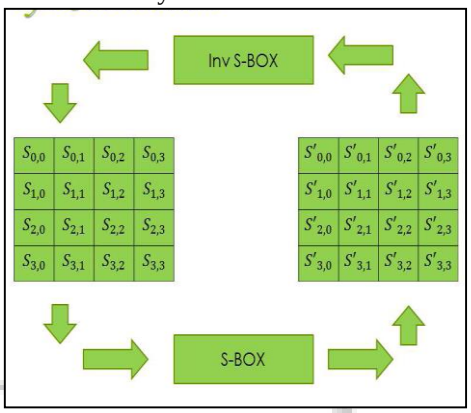

Fig. 2: Byte Substitution Transformation

B. *Shift Row*

Shift Rows are relatively simple. Cyclically shifts the rows of the state over different offsets. The state is the impressive cipher outcome that can seem as a rectangle-shaped number of bytes, having four rows. The figure3 illustrates the shift row transformation. In the immediate Shift Rows modification, the first type of state is still same, the second wide range, third wide range and 4th wide range respectively ring shift remaining 1byte, 2 bytes, and 3bytes.

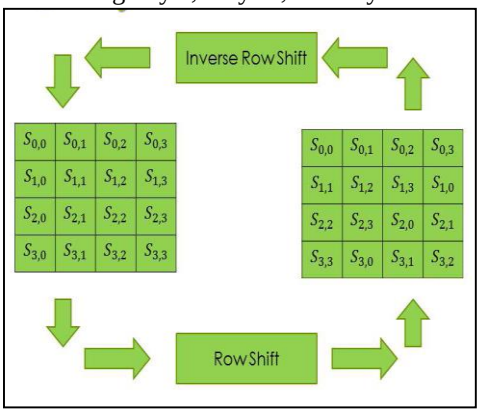

Fig. 3: Shift Rows Transformation

C. *Mix Column*

The mix Column function works on the condition column by column, dealing with each column as a four-term polynomial over GF (2^8) The Mix Column component doesn't function in the last circular of the criteria. The figure4 shows the mix column transformation.

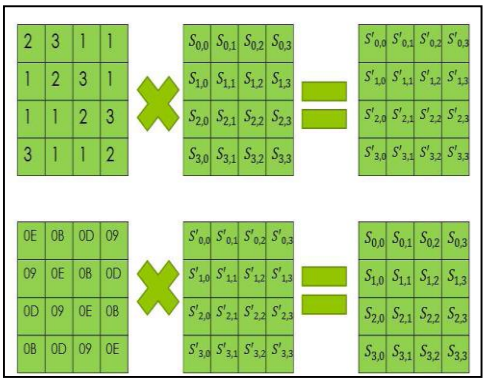

Fig. 4: Mix Column Transformation

D. *Add Round Key*

It performs bitwise X-OR operation. The modification in the cipher and inverse cipher in which a circular key is included in the condition using an XOR function. Round keys important factors are principles based on the cipher key using the Key development routine. The figure5 shows the add round key transformation.

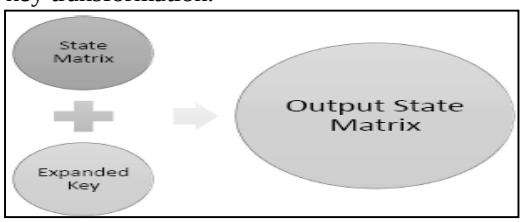

Fig. 5: Add round Key Transformation

E. *Key Expansion*

It is the schedule used to have a sequence of circular key factors of the cipher key. Key Expansion is carried out for the phrase, and with this two word handling features are presented which are termed replacement (Subword) and word spinning (RotWord). Subword needs a four-byte input term and is applicable an S-box for each of the four bytes to generate an outcome term. RotWord needs a four-byte word and works a cyclic permutation.

V. AES ALGORITHM IMPLEMENTED IN FPGA

AES cipher is operating on data frames having the length of 128bits with a symmetric key, which may have an overall length of 128, 196 or 256 items. Features are implemented on a matrix of dimension 4 x 4 bytes known as a state. The factors contains following activities. First, the details held in state array are involved mod 2 with the real key with the operate Add-Round Key. The next activities are rounds repeating Nr periods. Each round performs 4 following operations: alternative of bytes Sub-Bytes, sequence, shifting Shift-Rows, mixing of material Mix-Column, and Add-Round Key. The amount of rounds Nr depends on the key length; for the 128-bit key Nr = 10. The last stage performs 3 operations: Sub-Bytes, Shift-Rows and Add-Round Key. At each stage another key created as a development by the procedure Key Expansion is roofed. Figure6 illustrates the design flow of Rijndael algorithm. Whereas the decryption procedure is relatively performing the same process as what encryption is done except it is performing the inverse of the encryption which are Inverse Sub-bytes, Inverse Shift-row, Inverse mix-column and Inverse Add-Round key.

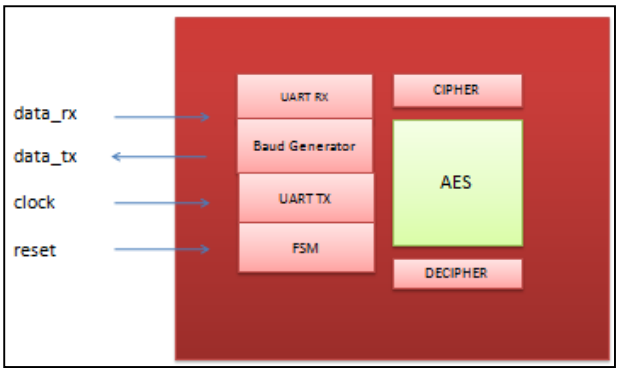

Fig. 6: Top Level RTL Design for AES

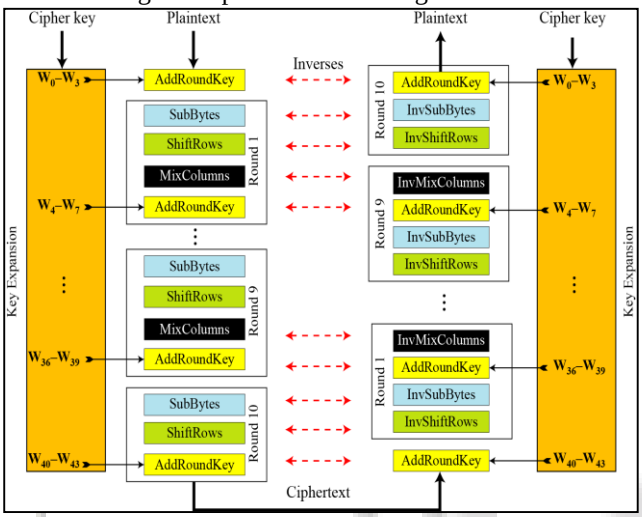

Fig. 7: Design Flow of Rijndael Algorithm

In proposed system AES structure is developed through VHDL terminology using Xilinx 13.2 for Spartan 3AXC3s500e FPGA. This structure requires 128 bits of information as input along with the 128 bits of keys along with three management indication clock, go_i, and totally reset indication each of individual bit. Figure7 illustrates the RTL style of the AES block.

Signal Name	Direction	Size	Functionality
Data	Input	128	Input information from the Host
Key	Input	128	Security signal
Clk	Input	1	System time indication input
Go_i	Input	1	Control signal
Reset	Input	1	Master totally reset signal
Cipher	Output	128	Encrypted output
Decipher	Output	128	Decrypted output

Table1: AES Core Signal Description

Inside of AES consists of Cipher unit and a Decipher unit. Cipher block is linked to decipher block. Cipher unit requires all the input offered to AES core and provides us a cipher written text of 128 bits as an outcome. Cipher unit manages the handling of decipher unit, it keeps decipher in wait around condition unless it is prepared with the cipher text. Decipher unit requires the cipher text as feedback (input) and offer us the decipher text which would be exactly just like input information.

VI. EXPERIMENTAL RESULTS

This design is accomplished via Verilog HDL hardware description language by Xilinx 13.2 software simulated with MATLAB, and finally implemented on FPGA in Spartan-3A family. Power is analyzed to Xilinx Power. This design has a high speed, high throughput and low power consumption. It is really suitable for highly secured image encryption and also the time of its converting is low.

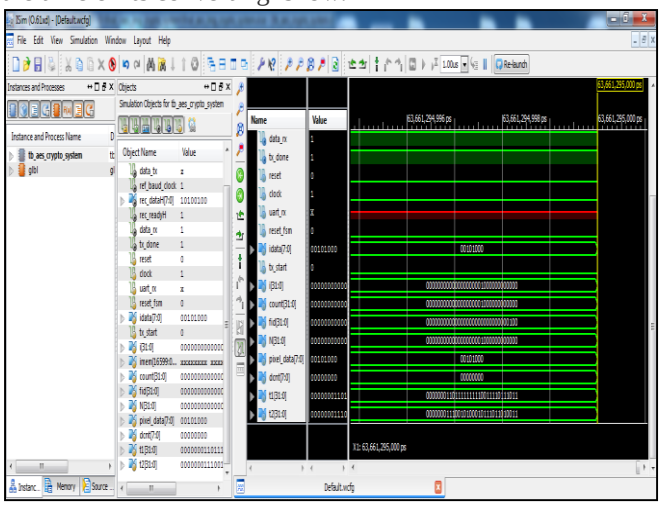

Fig. 7: Simulation waveform

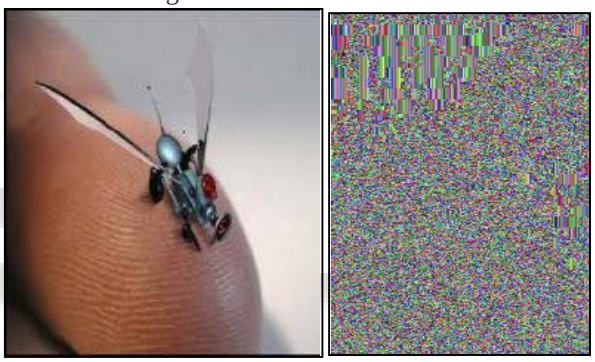

Fig. 8: Original Image and Encrypted Image

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	1579	5888	26%
Number of Slice Flip Flops	797	11776	6%
Number of 4 input LUTs	3002	11776	25%
Number of IOs	10		
Number of bonded IOBs	6	372	1%
Number of BRAMs	16	20	80%
Number of GCLKs	2	24	8%

Table. 2: Device Utilization Summary

Timing Summary	
Factors	Values
Speed Grade	-5
Minimum Period	2.384ns
Baud Rate	9600
Maximum Frequency	119.27MHz
Minimum input required time after clock	3.761ns
Maximum output required time after clock	6.767ns
Throughput	1526.6Mbps

Table. 2: Device Utilization Summary

Parameter	[11]	[2]	Proposed
FPGA Device Package	EP4CGX30 B	VIRTEX -2 PRO	Spartan XC3S700 A
Number of Slices	16663	808	1579
Maximum Clock Frequency(MHz)	1000	475	119.27
Power Dissipation(mw)	1200	301	460
Throughput(Mbps)	1280	617	1526.6

Table. 4: Comparison of proposed method with respect to slices, frequency, throughput etc.

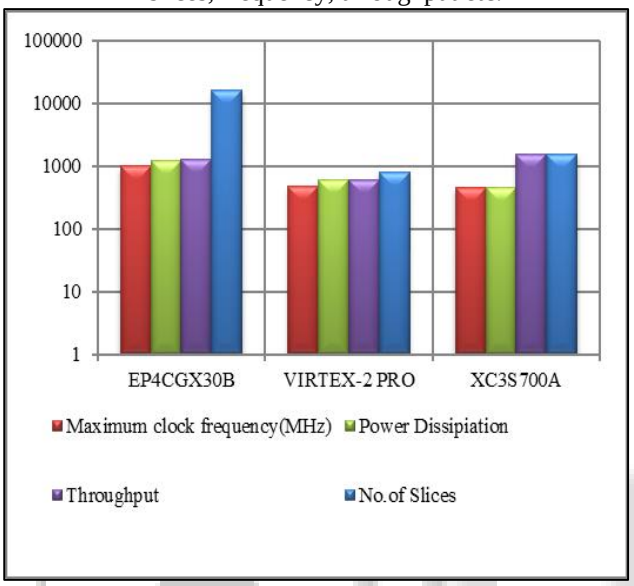

Fig. 9: Graphical Comparison of Proposed Method

VII. Conclusion & Future Scope

From this work we have determined that the idea of Pipelined AES structure can be essentially implemented. It has been noticed that the execution of AES encryption on the FPGA is effective and several information inputs. The cipher key can be modified with regard to the consumer specifications. The result reveals that the design with the pipelining technology and special information, transmitting method can improve the chip area successfully. Meanwhile, this design decreases energy intake at any level, for the ability intake is proportional to the chip area. Therefore the encryption system applied in this method can fulfill some real applications. As the S-box is implemented by look-up-table in this design, the chip area and power can still be enhanced. All the changes of criteria are simulated using a repetitive style strategy in order to reduce the component intake. So the future work should concentrate on the execution method of S-box. Arithmetic in Galois field can achieve the byte substitution of the AES criteria, which could be another idea of further research. While applying the AES algorithm, the crucial part was the area utilization. Which was done using the execution of features for different sub segments in the algorithm the work has approximately decreased around 10% usage of processor as in comparison to primary available segments. We have efficiently implemented AES encryption on FPGA. We have achieved the information encryption as per 100% precision as in comparison to data encryption component available online. The next step is to study the actions of the AES design with dimensions and to apply as an ASIC. There is a provision and adaptability to get rid of or add any other cryptographic standards.

References

[1] WANG Wei, CHEN Jie, XU Fei, "An Implementation of AES Algorithm Based on FPGA", Proc. 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 1615- 1617 2012.
[2] Yang Jun Ding Jun Li Na Guo Yixiong "FPGA-based design and implementation of Reduced AES algorithm," International Conference on Challenges in Environmental Science and Computer Engineering. 2010.
[3] Chih-Chung Lu，Shau-Yin Tseng. Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter [C]. Proceedings of the IEEE International Conference on Application-specific, Systems, Processors (ASAP'02), California, 2002.
[4] Hoang Trang, Nguyen Van Loi "An efficient FPGA implementation of the Advanced Encryption Standard algorithm" IEEE Symposium on Industrial Electronics& Applications (ISIEA), pp. 696-699 2012.
[5] Kbanob Thongkhome, Chalermwat Thanavijitpun,"A FPGA Design of AES Core Architecture for Portable Hard Disk" 20ll Eighth International Joint Conference Computer Science and Software Engineering (JCSSE).
[6] Saurabh Kumar, V.K. Sharma, K. K. Mahapatra, "Low Latency VLSI Architecture of S- box for AES Encryption", International Conference on Circuits and Computing Technologies, pp. 694-698 2013.
[7] PRAVIN B. GHEWARI1 MRS. JAYMALA K. PATIL1 AMIT B. CHOUGUL,"Efficient Hardware Design and implementation of AES Cryptosystem" Internationa Journal of Engineering Science and Technology Vol. 2 (3), 2010, 213-219.
[8] A. Amaar, I. Ashour and M. Shiple "Design and Implementation A Compact AES Architecture for FPGA Technology", World Academy of Science, Engineering and Technology 59 2011.
[9] Daemen J., and Rijmen V, "The Design of Rijndael AES- the Advanced Encryption Standard", Springer- Verlag, 2002.
[10] Y. Cheng, C. C. C. Hsieh, C. W. Huang, and C. J.Chang, and K. H. Chang, "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application,"Circuits and Systems, ISCAS 2009. IEEE International Symposium on, pp. 1922–1925, 2009.
[11] Vinay Firake, Dr. A. M. Patil, "Implementation of AES Algorithm", International Journal of Engineering Reasearch Vol.3, Issue.4, 2015.
[12] G.H. Karimian, B.Rashidi, and A. Farmani "A High Speed and Low Power Image Encryption with 128-Bit AES Algorithm", International Journal of Computer Engineering,Vol. 4, no.3, June 2012.

