International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

Design And Implementation of AES Algorithm with Biometric Key Schedule to Improve Security

Rachana Veerabommala
VLSI Design IGDTUW
Delhi, India

Ms. Greeshma Arya
Asst. Professor, ECE IGDTUW
Delhi, India

***Abstract*— Hardware Security plays a vital role in most of the applications such as net banking, e-commerce, etc. Cryptography is linked with the process of converting ordinary plain text into indistinct text and vice versa. Symmetric key algorithms i.e., Advanced Encryption Standard (AES), and Data Encryption Standard employs the same key for encryption and decryption. The proposed Bio-Metric 256-bit AES algorithm is highly utilized in terms of Key management for enhance the security. The enhancement has been done by selecting the various pixels from an image. This in turn results in a power reduction by a FPGA implementation. The entire process of the proposed implementation was done by using Virtex-7 FPGA. We used Xilinx software with the help of Verilog HDL .The expected output was collected and the simulation waveforms are verified.**

Keywords—Advanced encryption ,Data encryption, FPGA, Verilog HDL, Bio metric image.

I.INTRODUCTION

In these modern-days, block ciphers plays a major role in encryption technologies. Here ,the role of substitution-boxes is used to transform the normal text data to generate cipher-text data randomly with some appropriate disorder to confuse the attackers. We all know that the robustness and security of block ciphers will depends upon cryptographic strength of basic s-boxes .Because, these s-boxes are the most capable components which taken the responsible to fetch the randomness and to make the system complex to improve the security system that can confuse the attackers. Many concepts have been explored to build the strong s-boxes. In this paper, we have given a detailed knowledge of key generation with high security. This modular approach consists of three tasks i.e., modular inverses, new transformation and permutation. In this new approach ,we fixed the drawbacks in the existing system, such as non linearity and uniformity to demonstrate cryptographic potentiality. To this, an image encryption process is also implemented in the S-box to perform the shuffling of pixels, replace with strong statistical and differential encryption performance.

In today's technological life the data and information communication is considering as treasure to the individual or organization. If the privacy of the information is not secured, then the information will use for mischievous purposes. In present era, the innovations in technology is increasing the size of data transmission through the internet. So, the private information have to be secure from the invaders These methods will be more helpful to protect our data.

The cryptographic algorithms are one of the best method for protection of the data because it obtained from mathematical methods and set of calculations to convert messages to make hard to decode the original code. These methods helps to key generation and to secure the confidential data. Stream ciphers alters the data in a bit wise manner, the block ciphers converts the data into blocks which compress the large number of bits or bytes at the same time. These days ,block ciphers are considering as most effective tool for protection of data. protection. Advanced encryption, Data Encryption are the examples of block ciphers. The implementation of block ciphers are simple than stream ciphers. The SP network-based block ciphers are a type of block cipher that is commonly used. Thus, when utilizing block ciphers, the sender and receiver of the data encrypt and decrypt the data using the same key.

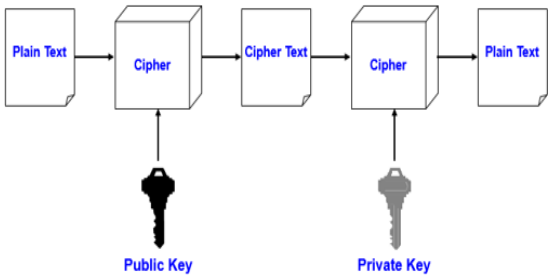


Fig. 1. Block diagram of an AES algorithm

A static s-box is used in each round of block cipher. It allows data analyses attack and eventually captures the sub keys using inverse sub byte. In this paper, we proposed a simple design and implement with low cost to existing AES to Dynamic s-box.. To make S-box as dynamic ,the current AES S-Box and new produced S-Boxes are employed to implement dynamic S-box.

The remaining part of this project work is mentioned as follows: The existing system are discussed and how to implement the key previously in section II.. In Section-III emphasizes the proposed implementation of key generation using bio-metrics. The section IV includes the suggested method synthesis results as well as other existing AES approaches and comparison between them. The suggested method is also included in the updated Modified key generation to complete AES metrics and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

to validate the findings using post-synthesis simulated result. Additionally, the suggested design Synthesized on Various FPGA boards for various performance analyses. Section V&VI explains about the advantages and applications. Section VII brings the paper to a Conclusion

II. EXISTING METHOD

So many technologies was implemented earlier to improve security , such as multi level AES transformation units are used for maximizing the confusion metrics during encryption process and the Combinational circuit is used for S-box implementation which will increase security. S-box is modified as one way mapping function. In this, the S box values are directly accessed from memory which leads more power consumption and path delay overhead and by using Cryptosystem-Key management is a major issues which will be the major cause in hacking. Although they created the key by adding 128 bits to 128 bits to make it as 256 bits which gives the high security ,the key leakage may happen sometimes at the time of decryption at receiver end. .By using this method the complexity is high and efficiency is also less. To overcome these drawbacks we implemented the proposed system.

III. PROPOSED METHOD

The prime objective of this proposed method is to increase the efficiency and to reduce the complexity. We demonstrate how a key size used and number of rounds will increase the computation complexity. To maximize the security and increase the resistance level cipher key length is need to increase. And to narrow down the design complexity without compromising the security different transformations can be used. In this paper 256 key size is used for AES and also incorporate different combination of transformations for each round for low complexity with improved randomness over cipher text conversion method. To overcome the key management problem associated to AES core digital biometric based fully automated key generation scheme is introduced. This auto key generation follows hierarchical steps which includes different level of confusion metrics for AES.

In a single image, there will be a greater number of Pixels available. So, Possibility to find out the pixels what we are using as key is highly complex one. Even though if someone find out the pixels count as well as pixel's location, they need to know the arrangement of pixels. The KEY origination is kept as a secret. So to hack the data is very tough.

A. Key generation by using the Biometric image

In this method first we have to convert the biometric image to digital image. i.e., made up of pixels. We can generate the key by using the following algorithm i. Selecting the location of the pixel. ii. By using random generator we have to concatenate the number and iii. We have to integrate the value. So, it randomly generates one key. By using the key we can encrypt the data. No one knows how the key was generated and they cannot know the arrangement of pixels. For decryption ,the encrypted data will transform back by giving cipher text with the help of the key we can get the plain text. It will use the same cryptographic keys at both sender end and receiver end.By using this method there is no need to remember and store the key to encrypt the data. This method gives more security than the existing system. Randomly we can change the key according to our wish. So that, there is no possibility to hack the data ,this method gives more accuracy and less complexity.

B. Cipher text

Cipher text is nothing but the information has to be hidden by giving some additional data to the original which cannot be read by human. The data is decrypted by using the key. There are two ways to implement the cipher text i.e, Stream Ciphers and Block ciphers. In stream ciphers the text is encrypted by using bit by bit or byte by byte. By using the block ciphers it encrypts by using blocks. Each block is operated independently. In cryptography the cipher text plays an important role to protect our data from the invaders.

Fig 3a. Biometric image

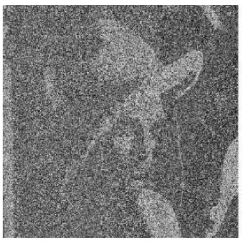


Fig 3b. Encrypted image

C .Random generator

The random generator will generates the random number with the help of AES algorithm .This AES algorithm deals with four operations .i.e., Sub Bytes, Add Round Key , Mix column, Shift Rows..256-bit AES encryption block is implemented in 14 rounds. For each round it will do the four operations .Round 0 consists of only Add round Key operation. Round 14 consists of Sub Bytes, Shift Rows and Add Round Key operations, which need 3 clock cycles. Rounds 1 to 13 consists of all the four operations. We do a distinct operation in each clock cycle. Hence once the hardware has been implemented for all four operations we can use the same hardware for all the 14 rounds. None of the four operations shares the same clock cycle. The sequence of round operation with specific sequence of 4 operations to complete the AES encryption. The AES method is a serial process. i.e., the first round output is connected to the second round and it will be the input for it. Hence, we can use the same hardware for each round. The data structure of 128-bit matrix. Each column consists of 4 elements of 8 bits each, so in total we have 32 bits per word.

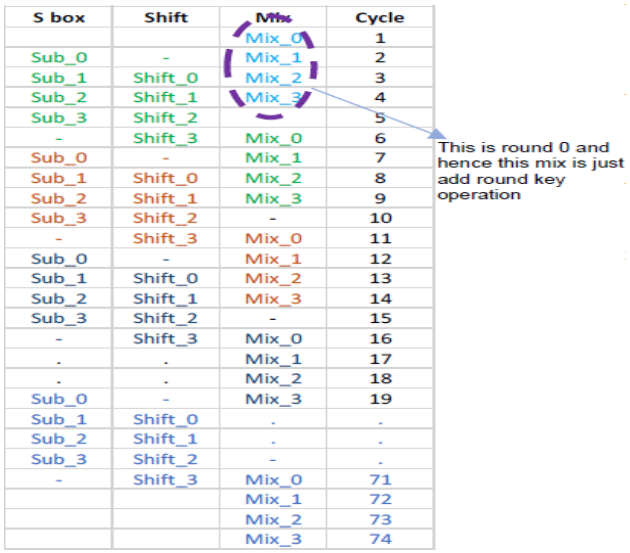
Round 0	01 cycle
Round 1 to 13	52 cycles
Round 14	03 cycles
Total	**56 cycles**

Fig.4 Cycles required in Each Round

We are using 14 rounds for both encryption and decryption. The cipher text after encryption will be transmitted across the channel. At the receiver end ,we will use the same key which used before in the encryption. Data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

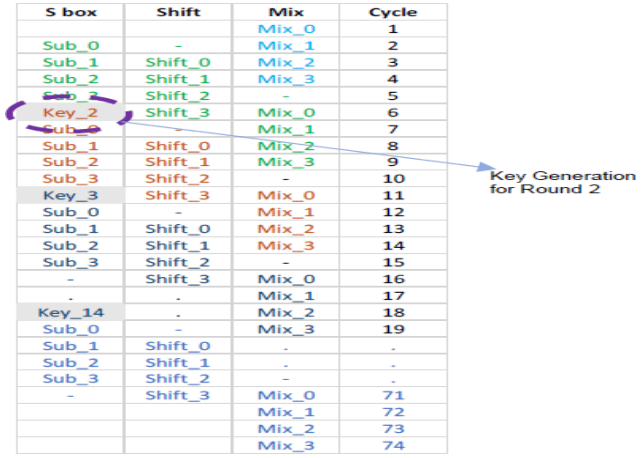
include message to be encrypted, cipher text and the decrypted message.



S box	Shift	Mix	Cycle
		Mix_0	1
Sub_0	-	Mix_1	2
Sub_1	Shift_0	Mix_2	3
Sub_2	Shift_1	Mix_3	4
Sub_3	Shift_2	-	5
-	Shift_3	Mix_0	6
Sub_0	-	Mix_1	7
Sub_1	Shift_0	Mix_2	8
Sub_2	Shift_1	Mix_3	9
Sub_3	Shift_2	-	10
-	Shift_3	Mix_0	11
Sub_0	-	Mix_1	12
Sub_1	Shift_0	Mix_2	13
Sub_2	Shift_1	Mix_3	14
Sub_3	Shift_2	-	15
-	Shift_3	Mix_0	16
.	.	Mix_1	17
.	.	Mix_2	18
Sub_0	-	Mix_3	19
Sub_1	Shift_0	.	.
Sub_2	Shift_1	.	.
Sub_3	Shift_2	-	.
-	Shift_3	Mix_0	71
		Mix_1	72
		Mix_2	73
		Mix_3	74

This is round 0 and hence this mix is just add round key operation

Fig 5.Operation of Mix block



S box	Shift	Mix	Cycle
		Mix_0	1
Sub_0	-	Mix_1	2
Sub_1	Shift_0	Mix_2	3
Sub_2	Shift_1	Mix_3	4
Sub_3	Shift_2	-	5
Key_2	Shift_3	Mix_0	6
Sub_0	-	Mix_1	7
Sub_1	Shift_0	Mix_2	8
Sub_2	Shift_1	Mix_3	9
Sub_3	Shift_2	-	10
Key_3	Shift_3	Mix_0	11
Sub_0	-	Mix_1	12
Sub_1	Shift_0	Mix_2	13
Sub_2	Shift_1	Mix_3	14
Sub_3	Shift_2	-	15
-	Shift_3	Mix_0	16
.	.	Mix_1	17
Key_14	.	Mix_2	18
Sub_0	-	Mix_3	19
Sub_1	Shift_0	.	.
Sub_2	Shift_1	.	.
Sub_3	Shift_2	-	.
-	Shift_3	Mix_0	71
		Mix_1	72
		Mix_2	73
		Mix_3	74

Key Generation for Round 2

Fig 6. Generation of key by using random generator

By using this random generator some values will produce randomly that will concatenate to the pixel location and then it will forms the key. The whole process is done in the process of pipelined structured method. It will gives more accuracy to generate the key.

D. PIPELINED STRUCTURED METHOD

In this project we used pipelining method .Pipelining is nothing but processing the data as input in continuous method without waiting for the current process to complete. In many processors pipelining concept was used in many ways. Here we are using registers to store the current output . So, instead of immediately transmitting each round's output to the next round, we now utilise a register that acts as a internal register.. Since the current rounds' value is stored in the register the next input to the current round can be given as the current output is obtained.

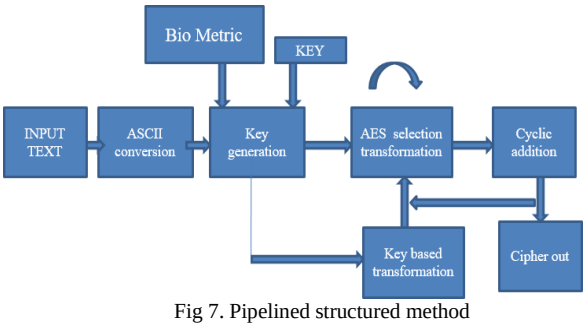


Fig 7. Pipelined structured method

The following diagram explains that the biometric image converts to the hexadecimal values that will take as the input and it will transforms to the ASCII conversion ,by using ASCII conversion the key will become more secure. In the next step the cipher text will be added by using AES algorithm method which gives the high security to the key and then the key will generates. By the help of key we can encrypt our data in secure manner.

E. VERILOG HDL

Today Verilog is the best language in the digital systems. Because it simplifies the process and the language is also easily understandable .Most of the designers are choosing the Verilog HDL as it permits to designs in the top-down or bottom-up methods. With the help of this we can perform the large circuits as it gives the RTL schematic along with the technology schematic methods. So that we can easily understand our circuits how we are designing. It creates the levels of abstraction which will hide the details of implementation and the technology. So many languages were introduced before such as system Verilog and VHDL .But these languages are complex when compare to Verilog. That's why most of the designers will choose the Verilog language .The syntax of Verilog is also simple and it is similar to C language so that it will easily understandable. Verilog is case sensitive and all the keywords are in the lower case. It has a facility to mix up the level of abstractions freely. For using Verilog, Xilinx is the good software to design the large circuits easily .It supports to design and to evaluate with boards such as FPGA , Microprocessor etc., It is flexible to adapt the new technologies.

F. MATLAB

For converting the image to digital format ,MATLAB is the best tool .As the name indicates it is nothing but Matrix laboratory which deals with matrixes. As it is well integrated it is easily understandable and also easy to perform the tasks. Most of the designers will choose this MATLAB because it performs image to data conversion easily and also easily understandable. For digital image processing matlab is very helpful as it provides the signal processing in easy way and also to analyze the data. Another reason to choose matlab is it controls the devices as well as the systems and also it provides the workflow by giving commands. It will also used for wireless communications, which will helps to eliminate the designing problems. In this project we used MATLAB.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

IV. RESULTS AND DISCUSSION

The proposed AES algorithm and existing AES algorithm both are functionally verified by using Xilinx 14.7 version. The proposed design has better area when compared to existing design without degrading the other factors. In the proposed method while we are using dynamic key it will decrease the area, improve the performance of the architecture.

RTL Schematic:

The below fig 8. Depicts the RTL schematic of the proposed architecture that is synthesized in Xilinx ISE 14.7 version tool. It shows the internal components that exists in the structure.

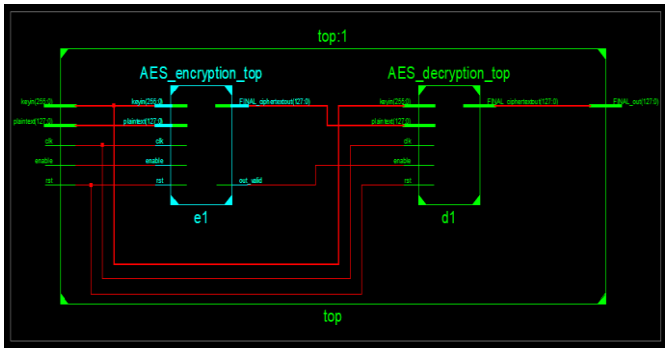


Fig 8.RTL Schematic diagram

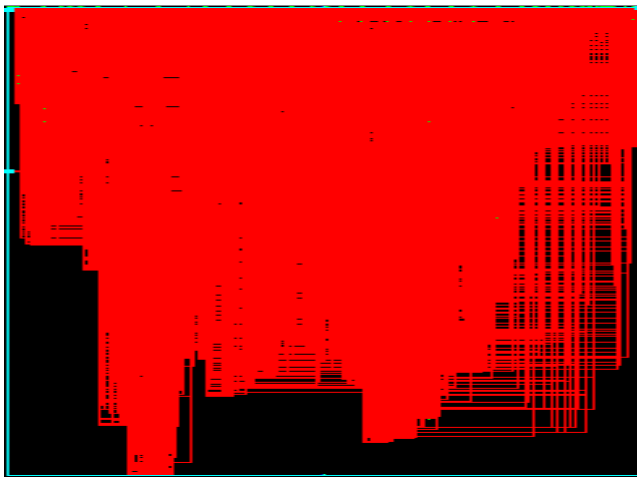


Fig 9. Technology Schematic diagram

Simulation Results: Output waveformsThe below figures are the simulation results of proposed structure which is implemented.

Fig.10.a. Input text in &out without ASCII

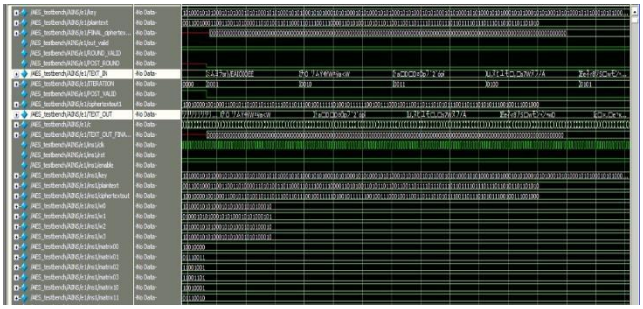


Fig 10 b. Input text in &out with ASCII

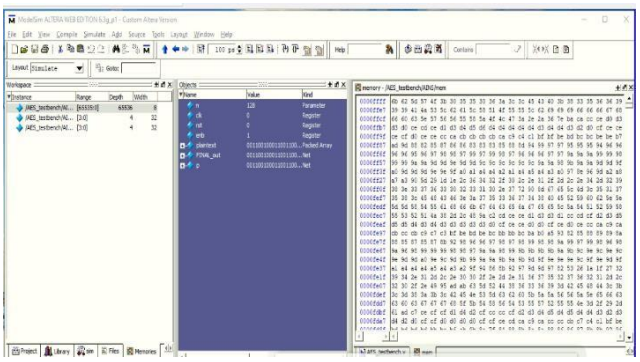


Fig 10c Combination of numbers by converting into pixels

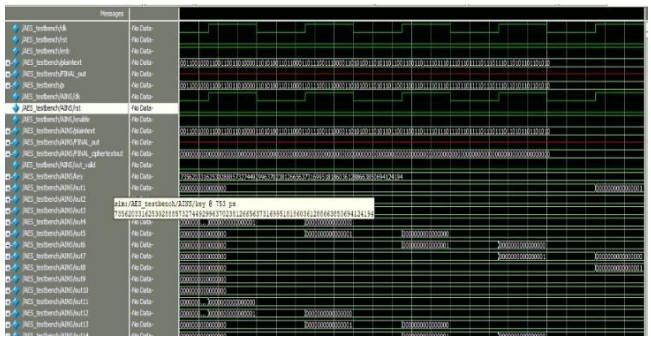


Fig 10 d .Generation of Key

In fig 10 a. the input text data is in the form of numerical values after adding the ASCII values to the input text we can get the different values with the help of the random generator i.e.,in Fig 10b.In Fig 10c,it is the hexadecimal values after we convert the biometric image to pixels .When we select one random number in pixels and it will concatenate with the ASCII value then it will generates the key which will be highly confidential ,the waveform in the Fig 10d. By using this key the data will encrypt as secure as possible.

Evaluation of Area, Delay report:

	Area	**Delay**
Existing	5706	33.346ns
Proposed	5279	13.377ns

Table1.Accuracy of existing & proposed methods.

The above Table 1 shows the comparison between existing and proposed structures of AES implementation

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

V. ADVANTAGES

a. The complexity of the system is low .
b. Outer level security is high.
c. Data rate in very high
d. It is able to process high level cipher in any real time data.
e. It has less area.

VI. APPLICATIONS

a. It can be used in Wireless Security
b. It can be used Processor security
c. It can be used for File encryption

VII. CONCLUSION

This paper presents a generalized design and a practical implementation of AES algorithm with key extracted from biometric. Instead of using static key, the proposed method had better performance in terms of security. The proposed AES and existing AES algorithm both are functionally verified by using Xilinx 14.7 version. The above results shows that the proposed design consists of less area and less delay when compare to the existing design. By using the proposed system the data will be more confidential.

VIII. REFERENCES

[1] Wei Wang ; Jie Chen ; Fei Xu ; “An implementation of AES algorithm Based on FPGA” 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery.
[2] N. S. Sai Srinivas ; Md. Akramuddin; “FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption” 2016 International Conference on Electrical, Electronics, and Optimization Techniques .
[3] S.P Guruprasad ; B.S Chandrasekar ; “An evaluation framework for security algorithms performance realization on FPGA” 2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC) .
[4] Vatchara Saicheur ; Krerk Piromsopa ; “An implementation of AES128 and AES-512 on Apple mobile processor” 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)
[5] M. Rajeswara Rao, Dr.R.K.Sharma, SVE Department, NIT Kurushetra “FPGA Implementation of combined S box and Inv S box of AES” 2017 4th International conference on signal processing and integrated networks (SPIN).
[6] C. Sivakumar ; A. Velmurugan ; “High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)” 2007 International Conference on Signal Processing, Communications and Networking.
[7] Shrivathsa Bhargav, larry Chen, abhinandan Majumdar, Shiva Ramudit “128 bit AES Decryption”, CSEE 4840 – Embedded system Design spring 2008, Columbia University.
[8] Yulin Zhang ; Xinggang Wang; “Pipelined implementation of AES encryption based on FPGA” 2010 IEEE International Conference on Information Theory and Information Security.
[9] Yuwen Zhu ; Hongqi Zhang ; Yibao Bao ; “Study of the AES Realization Method on the Reconfigurable Hardware” 2013 International Conference on Computer Sciences and Applications.
[10] Nalini C. Iyer ; Deepa ; P.V. Anandmohan ; D.V. Poornaiah “Mix/Inv Mix Column decomposition and resource sharing in AES” conference on information security.
[11] Xinmiao Zhang, Student Member, IEEE, and Keshab K. Parhi, Fellow, “High Speed VLSI architectures for the AES Algorithm”, IEEE. VOL.12. No.9. September 2004 .
[12] P. S. Abhijith ; Mallika Srivastava ; Aparna Mishra ; Manish Goswami ; B. R. Singh ; “High performance hardware implementation of AES using minimal resources” 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).
[13] Ashwini M. Deshpande ; Mangesh S. Deshpande ; Devendra N. Kayatanavar; “FPGA implementation of AES encryption and decryption” 2009 International Conference on Control, Automation, Communication and Energy Conservation.
[14] Tsung-Fu Lin ; Chih-Pin Su ; Chih-Tsun Huang ; Cheng- Wen Wu; “A high-throughput low-cost AES cipher chip” Proceedings. IEEE AsiaPacific Conference on ASIC.