IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. V (Nov – Dec. 2014), PP 07-13
www.iosrjournals.org

High Performance Data Encryption based on Advanced Encryption Standard using FPGA

M. Amr Mokhtar
Assoc.Prof., Elect. Eng. Dept., Fac. of Eng., Alex. Univ., Alexandria, Egypt,

Abstract: *Many digital services, such as confidential video conferencing, medical, military imaging systems and the rapid progress of Internet, require reliable security and encryption in real time to store and transmit these digital images/videos.In this paper, a parallel implementation of the advanced encryption standard (AES) using pipelining technique is proposed. For more security, a pseudo random sequence generator (PRSG) is used in advance. The goal is to achieve a high-speed reliable security system for real time application. The parallel architecture is implemented on Field Programmable Gate Arrays (FPGA) family of Spartan_6 (XC6SLX16) using Very high speed Hardware Description Language (VHDL). An image encryption is taken as a case study. The system is capable to process image (256*256) in (0.00053) seconds; consequentially the real time requirement is achieved.*

Keywords: *Image encryption, FPGA, Pipeline design, AES.*

I. Introduction

Advanced growth in communication and computer techniques has led to an increased need to provide high security protection for files stored and transmitted information to manipulate them, hence the urgent need to find a science appeared for the provision of security to protect the information by changing the content of this data and convert it into a form, that is not understandable, using a secret key which transfers plain text to encrypted text that others cannot read it. In 1993, the US government was aware that the Data Encryption Standard (DES) algorithm were not operating with high performance as well as it was about to be broken due to the use of a small number of bits, 56-bits only for the size of the user key in the encryption. In October 2001, the National Institute of Standards and Technology (NIST) announced the Rijndael algorithm as the standard for advanced encryption (AES) [6], which has been used to protect sensitive information, and has replaced the DES algorithm**.** This type of encryption is asymmetric-key encryption where any encryption and decryption process is based on symmetric key. Since the adoption of the Advanced Encryption Standard (AES) algorithm by the National Institute of Standards and Technology, research rolled in the use of the algorithm to encrypt different types of data, due to its strong robustness against attacks, as well as its flexibility in dealing with different sizes of data. In 2009, Fatimah SA[1] processed encryption of both algorithms AES and RC4 and preceded the encryption process this ash of the elements of the image to reduce the correlation between adjacent elements of the process, using the principle of generating random sequence, followed by a single application of the algorithms mentioned for the final encrypted image. In 2010, [2] measured the efficiency of the performance of the three types of algorithms, AES, Serpent and Towfish. It is known that these species share the same length as the volume of data, as well as the key. In addition, research has been on the comparison of speed performance of these algorithms, results showing that AES algorithm is the most efficient. In 2012, [3] proposed an ideal technique for the implementation of the Mix Column on the FPGA to reduce the space needed for the implementation of architectural AES, and that relying on multiplication the number 2 in the encryption process, either in the decryption process based on the process of multiplication the 2 and 0.9**.** Architecture was designed to implement. (Xilinx Spartan3E (XC3S100E) using the program8.1 ISE**.** In 2012, [4] proposed three architectures for the implementation of the Mix Column algorithm of AES and was first a mathematical method, the second based on the use of tables, and the third was based on the binary system characteristics. It has been proven that third architectural was efficient in terms of reducing the space and increasing the speed compared to other algorithms. In 2013, [5] proposed a new architect for the s-box algorithm for the AES, where the architectural design was based on the logic gates AND, OR, NAT XOR, so as to reduce the space necessary as well as opportunities to improve the performance of the system by use of the pipeline technique, which consisted of four stages of the formation of the S-box space, and the architectural application designed to chip Xc4vf100 Xilinx Virtex IV(Xc4vf100) using the program7.1 ISE V. Depending on the properties of AES in terms of speed and reliability of the system, this architectural proposal for a hybrid system of the AES with stream cipher for encrypting information (image as a case study) in real time has been in search. Since then, t he AES algorithm is used widely in a variety of important applications such as secure communication systems, smart cards and in multimedia applications as image encryption, video, audio, etc...More services and applications emerge that need high security to meet the user requirements has begun in recent years such as

mobile phones and PDA requirements which provide extra functionality of the most important provision of the exchange of multimedia messages, that the spread of this kind of multimedia technology enhanced the importance of this type of information that require high safety to meet the user's privacy. These applications, in addition to their need for high safety, need to encrypt in real time. The speed factor will be the main focus of research in this paper. Part 2 presents brief profiles of cryptography. Part 3 introduces the principle of generating random sequence and stream encryption. Part 4 illustrates the concept of pipeline techniques while displays the proposed 5 architectural part, the remainder is a discussion of the results obtained in this research.

II. Cryptography Science

The science that deals with encryption for various types of data, by carrying out mathematical functions and constant set of steps to implement the encryption and decryption process, and consists of any type of encryption algorithms of the three main parts of an encryption and decryption key, as apart of the basic and important in each algorithm. The encryption process converts the original text to an encrypted text or cipher text, while the decryption process restores the cipher text to its original form. The encryption science is divided mainly into two basic types, symmetric encryption, which uses one key in the encryption and decryption process in agreement between the two parties(the sender and the recipient), this type of encryption can be performed by encrypting data either in the form of blocks of words; which in turn consist of a set of data sizes which vary according to the algorithm type, after completion of the current block moves to another block, and so on, it is also called Block Cipher, as in the AES, DES and 3 DES algorithms, as shown in Figure(1); or the second type shall encrypts data with less size, where the block size to one word and is called Stream Cipher. This type increases the speed compared to the previous type as in the case of RC4 algorithm. The second kind is the basic asymmetric encryption type which uses an encryption key different from the decryption key.

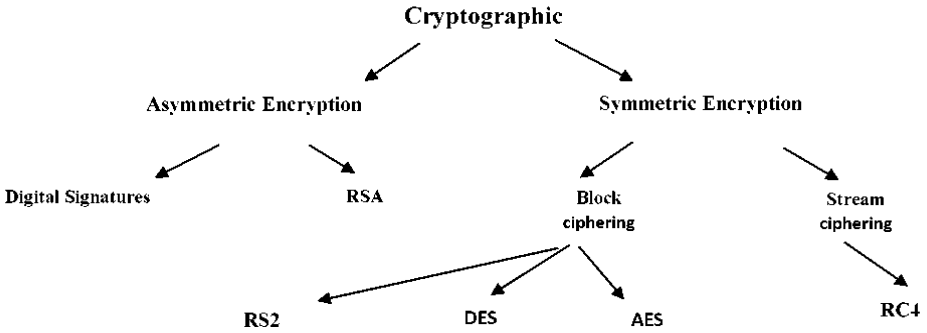


Figure 1. An overview of the encryption algorithms

a. AES algorithm (Rijndeal)

Advanced Encryption Standard algorithm has several rounds, and is divided depending on the encryption key size, with a note that the block size to be encrypted is constant for all types and equal to 128 bits. Each type specifies the number of round types.

The AES algorithm can be divided into three types:

1. AES_128 bit consists of 10 rounds.
2. AES_192 bit consists of 12 rounds.
3. AES_256 bit consists of 14 rounds.

Each round consists of four stages, except for the last round, which consists of three stages, this applies in encryption rounds, as well as in the decryption rounds. Figure 2 shows the structure of the AES algorithm with all its rounds and stages in the encryption and decryption.

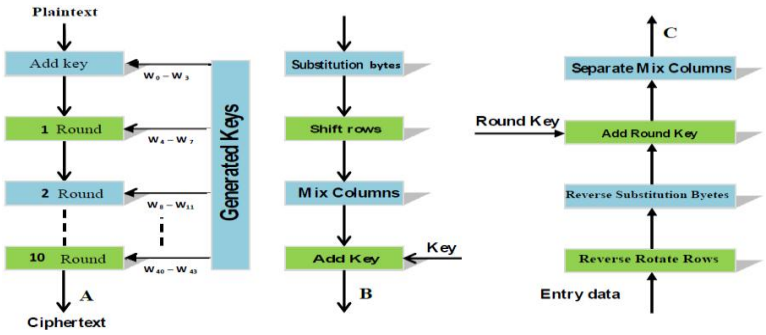


Figure 2. A. represents encryption rounds in AES algorithm,B.represents stages per one round in encryption process,C.represents stages per one round in decryption process.

b. The One Round Stages.

i. Substitution

At this stage, the input is replaced by a different output. This process is executed at the level of a single byte, where each byte of input is non linearly replaced, and this is done using a table called the S-Box, as shown in Figure 3, which different values in encryption case differ than in the case of decryption, this stage is performed to reduce the correlation between the input and output.

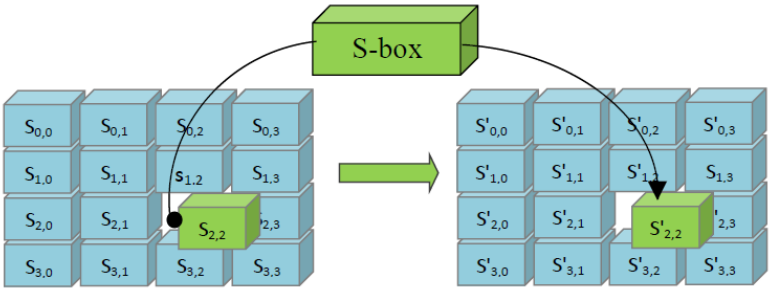


Figure 3. Sbstitution Process.

ii. Shift Rows

For the input s', which is in the form of a square matrix of4*4 (16 byte),the first row stays the same while the second row is shifted left by1 byte, while the third row is shifted by 2 byte, and so on ...as shown in Figure 4, in the encryption case. While in the decryption case, the mechanism remains the same but it only changes direction to become right shifted, and the aim of this stage is to change the byte value within each block (128 byte).

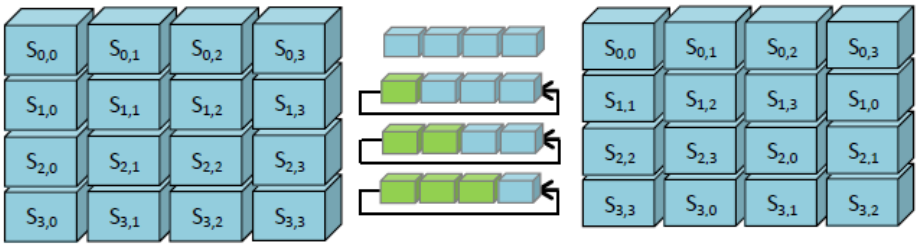


Figure 4. Rotate process

iii. Mix Columns

In this stage, matrix columns coming from the previous stage is being mixed with another constant matrix columns as shown in Figure 5, which is different in the encryption state than it is in the case of decryption.This process provides an increase in the changed block parameters in addition to hide the correlation between the original and the encrypted text. At this stage when finding a particular item value, it takes into account the values of adjacent items. By this stage, the encryption has arrived to the bit level.

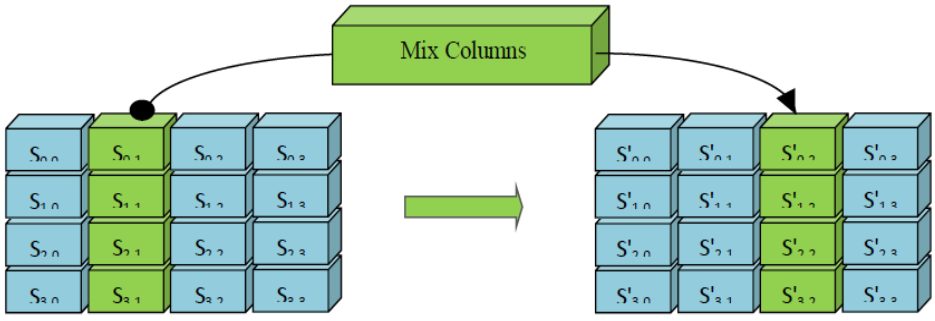


Figure 5. Mix Columns

iv. Add Round Key

This is the most important stage, because the encryption entire process depends on a secret encryption key, with a length of 16 byte, generated using the original key with each round. If the AES-type has10rounds, It will generate 10 keys. Each key consisting of (16 byte), is used for the XOR operation linking the next text from the previous phase with the generator key in conjunction with the current round, as shown in Figure 6. At the generation process of each key, same operations in the previous stages of shift row and substitution are

performed. It is worth mentioning that the key generated is used in the encryption process, as well as in decryption process since the classification of this type of encryption is symmetric.

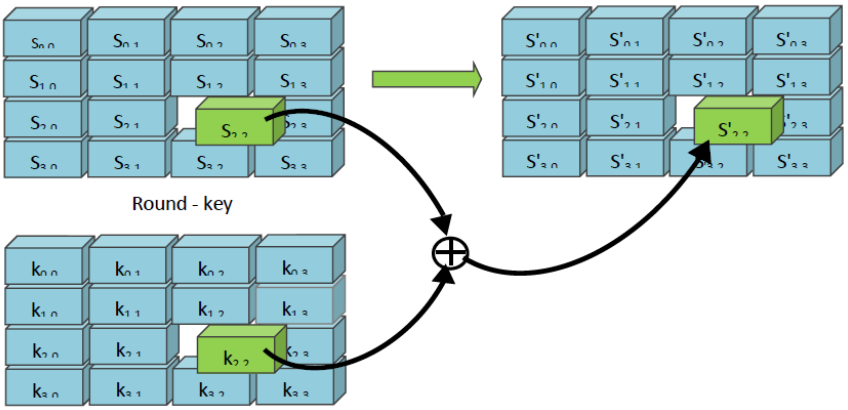


Figure 6. Add Round Key

All rounds contain the previous stages, except for the last round which misses the third stage, mixing stage of columns. The final round of the decryption process lacks mix columns separation stage.

III. The Principle Of Generating Random Sequence (PRSG) And Stream Cipher

This type of generation depends on the number of shift registers which share the clock pulse (Clk), as shown in Figure 7, and therefore, the number of sequences that can be generated by this generator depends on the number of these registers as described in equation (1). Concatenation these sequences is theoretically not randomly, but in some practical applications can be considered random because the number of sequences generated depends on the number of registers. If we have a 32 register, the number of sequences would be 4294967295, and this is a big number enough for most practical applications [7]. If n is the number of registers, then

$$Number\ of sequences = 2^n - 1 \quad (1)$$

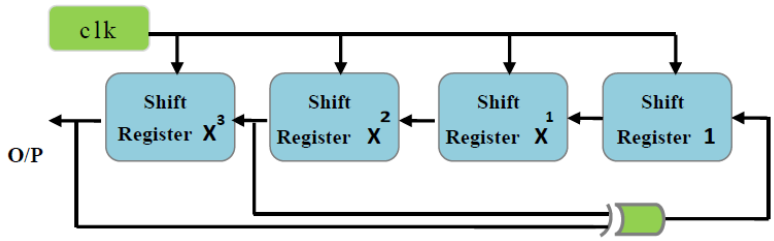


Figure 7. The mechanism of action of random sequence generator at n=4.

In this research, 8 registers has been used to commensurate with the byte size and thus the number of sequences is 255 sequence according to equation (1), when the number of registers is determined, the generator will be condemned by a fixed standard equation that differ depending on the number of registers. When taking the initial value of the generator, this equation will get according to a certain order the first sequence, which is considered the initial value to find the second sequence, and so on, until access to the last sequence. This type of generation is used as the entrance to the stream cipher, which is classified as asymmetric encryption, which uses a single key for encryption and decryption. This type of encryption is characterized by block length equal one word or one byte. The advantage of this type of encryption is high speed, in addition to its simplicity in handling, and easy to apply programmatically and financially [8].

IV. Pipeline Technology

This is a technique based on the existence of a series of consequence stages separated from each other by latches as shown in Figure 8, and is controlled by a common pulsed clock, each of these stages is represented by certain process according to design practice, and these stages are performed by combinational circuits, each latch that separates these stages store the result of the current task to allow preceded stage to perform sequence tasks**.**

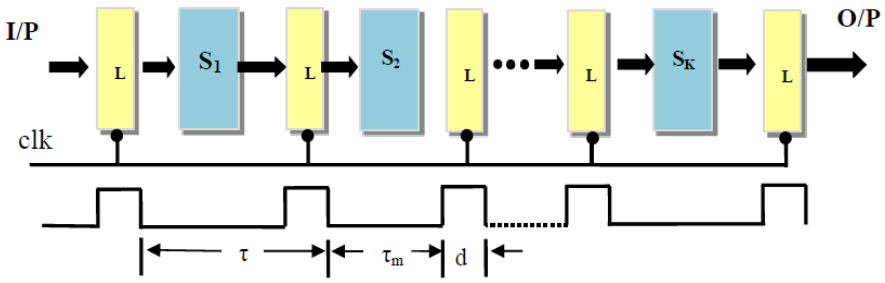


Figure 8. Pipeline stages technology

External entries are fed in the pipelinetechniqueduringstageS1, then pass through the entire process, till it reaches Sk. the preferred design of the entire technique leads to almost equal delay in all stages, these delays through which the number of pulses are being calculated that are necessary for the implementation of sequential tasks and speed calculation. This allows the possibility of structural time-sharing, so that the data in the first stage and the second operating at the same time without affecting each other, and this is what will be achieved in the practical part of the search when usinga multi-media data. Description language of hardware (VHDL) allows possibility of generating pipeline technique stages through the use of directive process and synchronized by (CLK) signal defined at the beginning of the program.

V. The Proposed Encryption Architecture

The proposed architectural is efficient to work in real-time, and as an example, image encryption application has been used. The image consists of a group of pixels, which in most cases are correlated, so the architecture proposed is to overcome this kind of problems using the principle of generating random sequence, the proposed architecture consists of two parts as shown in Figure 9, where the first part uses random generation principle, through an XOR operation between the value generated by the random generator with the value of each pixel of the image as shown in Figure9.

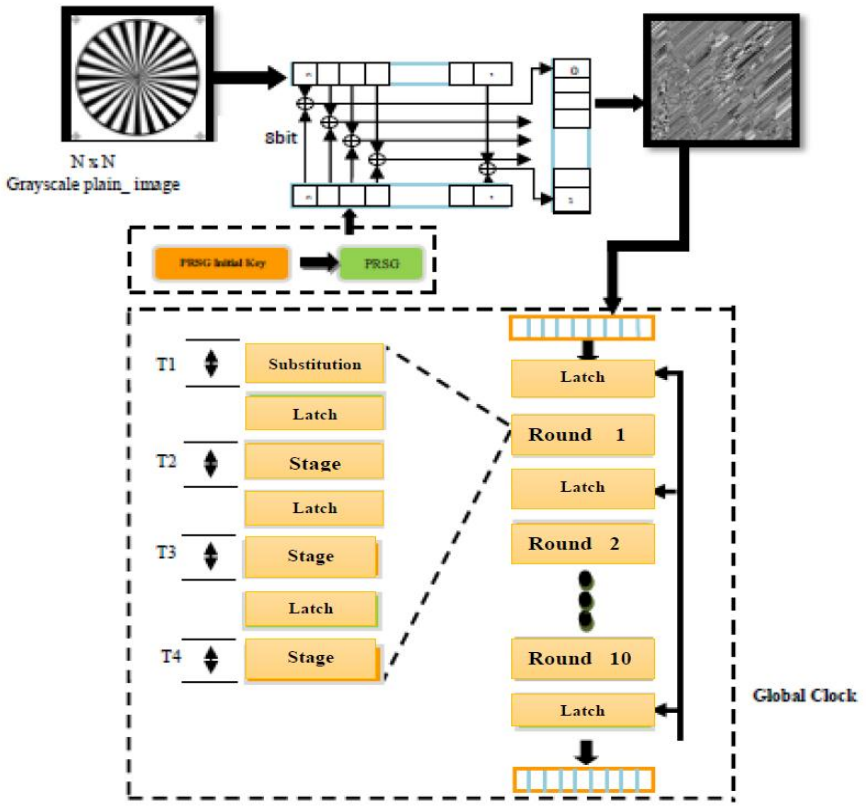


Figure 9. The proposed architectural mechanism work.

The second part takes the picture and divides it into a group of blocks, each block represents 16 bytes, enter each block alone in order to be processed during each round of the AES algorithm rounds according to standard processes that have been mentioned previously in section (1-a). The control on the data flow and to achieve synchronization (to prevent the interference between the blocks) during the transition process within the architectural cross generator, a global clock has been used. The choice of frequency of the clock is according to

equation (2). Any defect in the synchronization process, even for a bit, leads to the failure of the process completely, then the recover data process be impossible.

$$fg = \frac{1}{\tau} \quad (2)$$

$$\tau = max(\tau_i) + d \qquad 1 \le i \le k \quad (3)$$

τ : Clock pulse time of pipeline technology.
τ_i: Delay time of stage i.
d : Latch time delay.
k : Number of stages.

- ***Image storage process.***

Image storage for the purpose of processing in the available memory blocks in the chip FPGA, through the image data entry which is represented by pixels in allocated storage places, and then the reading process in accordance with pulses compatible with the processing time required for each block is being read. According to the proposed algorithm and the timeline in Figure 10, the time required to encrypt each image can be calculated according to equation (3). the necessary data can be observed in Figure 10.

*The time required to encrypt image= {[((N * M) / Ps) *B] + R} / F* (4)

M, N*:* Total number of pixels for each row or column in the image (256).
Ps*:* Number of bytes of the block within the AES algorithm (16).
B: Number of pulses between the encrypted blocks (19).
R: Number of pulses to complete one block encryption (221).
F: Frequency used (144.972 MHZ).

*The time required to encrypt image={[((256 *256) / 16) *19] +221} / 144.972 MHz*
=0.538 ms

- Note that the above time much less than the required time in the video processing (33 ms), so the proposed system can be applied to video images. In the same way the time required for the processing of a group of gray images that have different sizes and are used in the processing can be calculated, which real-time can be achieved and thus the comparison between different size images can be done, as shown in Table (1).

TABLE I. The time required for processing different sizes of images

Size	Time taken
32*32	9.9 µsec
32*64	18.3 µsec
256*256	0.538 msec
1920* 1080: High-definition television (HDTV)	16.986 msec

VI. The Simulation Results

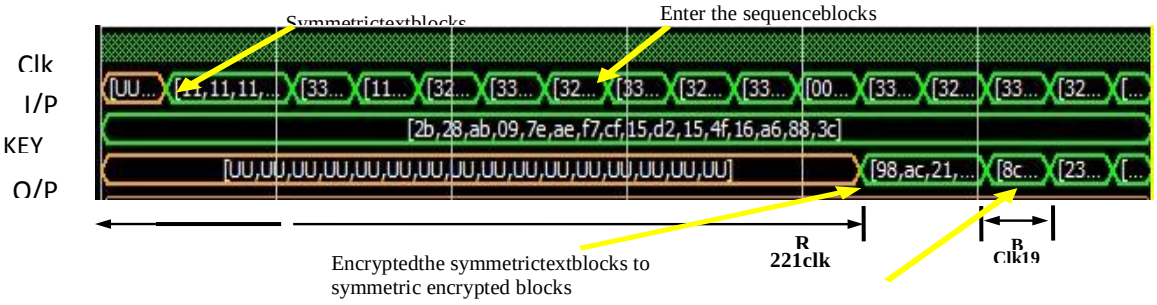


Figure 10. The simulation results of the architectural designer

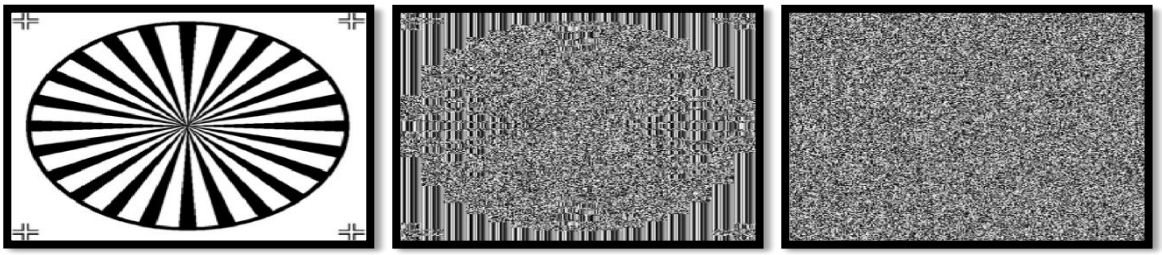
Implementation of the proposed architecture on-chip Spartan 6 (xc6slx16) by using ISE 14.2 program, is shown in Figure 10. Timeline (Timing diagram) describes the mechanism of action of the proposed encryption system in a pipeline method. After the full pipeline stages and flow the sequence tasks, in which it will start giving the encryption information after each pulse of global clock, i.e. after each pulse will have an encrypted block ready to send. Figure 10 shows the enter blocks to be encrypted by consequence form, and then exit by sequence form also. As well, as shown that blocks with symmetric values be encrypted to symmetric value encrypted blocks with the observation that all the blocks are encrypted and decrypted by the same key. The block entry process is every 19 Clk matched with the time delay stages and the output will be obtained also every 19 Clk.

The amount of material resources used for the construction of the proposed architecture when using Xilinx Spartan 6 (xc6slx16) can be observed in Table (2). The output frequency was F_{max} = 144.972MHz.

TABLE II. Shows the amount of resources used to build the architecture when using a chip Spartan 6 (xc6slx16)

Logic Utilization	Used	Available	Utilization
Number of Slice Registers	6996	18224	38%
Number of Slice LUTs	5732	9112	62%
Number of fully used LUT-FF pairs	3677	9051	40%

- Note from the table above, the possibility of the proposed architecture application on this chip as the space required was only 38% of the total volume available.
- Figure 11 shows the importance of the use of stream cipher stage before applying the image to the AES proposed system, where the connection of the encrypted image data when not using stream cipher, figure11-B, may then be separate and removed when it is used as a primary stage in image encryption operations, figure 11-



(A) (B) (C)

Figure 11. (A)-Represents the original image, (B)-Image encrypted by the AES algorithm, (C)-Image encrypted according to the proposed architecture.

VII. Connection Between Sender And Receiver

To make the connection process between the sender and the receiver, it requires two FPGA chips, one for encryption and another for decryption, the first part to send data that is already stored to the chip, which in turn encrypts data through real-time and therefore are sent encrypted data to the second chip, which are designed to perform decryption process in real time also for the recovery of the original data and then send them to a second part. This process is limited to the data flow in one direction and the first chip is designed to perform encryption only and the second for decryption. If required, data processing in two different directions at the same time, the design is based on each chip is able to make encryption and decryption in the same time. The secret key is being send by a separate channel.

VIII. Conclusions

This research concludes that the use of the pipeline technology on the AES algorithm led to the achievement of high-speed, with suitable applications as in real-time image encryption or video in multimedia applications. In addition, when using a stream cipher as a first stage to encrypt the pixel's value before introduction of the image to AES algorithm, this haslead to good results to improve encryption efficiency while preserving speed of the system.

References

[1] Fatimah, Sh., "On the security of Bitmap Images using Scrambling based Encryption Method", Journal of Engineering and Development, Vol. 13, No. 3, September (2009) ISSN 1813-7822.

[2] Hanna, R., "Efficiency of AES finalist candidate algorithms", Al-Nahrain University, 10th Scientific Conference 24-25 Oct.2009.

[3] H.K.Reshma R., Dr. N. Na., "Fault Detection Scheme for AES Using Optimization for Mix Column", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.

[4] Sliman, A. , A., Abderrahim Tragha , alah eddine Khamlich , "Design and Implementation A different Architectures of mixcolumn in FPGA", International Journal of VLSI design & Communication Systems (VLSICS), Vol.3, No.4, August 2012.

[5] Bahram, R., Bahman, R., "FPGA Based A New Low Power and Self-Timed AES 128-bit Encryption Algorithm for Encryption Audio Signal", I. J. Computer Network and Information Security, 2013, 2, 10-20.

[6] Bin Liu, Bevan M. Baas, "Parallel AES Encryption Engines for Many-Core Processor Arrays", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3, MARCH 2013.

[7] Peter, A., "Efficient Shift Registers, LFSR Counters, and Long Pseudo- Random Sequence Generators", XILINX.

[8] Michalis G., Paris K. et al, "Comparison of the Hardware Implementation of StreamCiphers", International Arab Journal of Information Technology, Vol. 2, No. 4, October 2005.