# Efficient Design of Image Cipher Technique Using Reversible Logic

**B. Sarala.[1], Dr.G.A.Sathish kumar[2]**
Department of Electronics and Communication Engineering,
Sri Venkateswara College of Engineering, Sriperumbudur Tk. - 602 117, Kancheepuram District,
Tamil Nadu, India.

**Article History**: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

**Abstract**

The reversible cryptographic logic is a prominent field in the applications of optical estimating, discrete time signal process, nanotechnologies, bio-information and low-power and low weight applications. For the above applications,Security is the very vital factor to focus on.Power and area parameters are also viewed for cryptographic protocols.Moreover,the intruders or hackers may eavesdrop or modify the data which is transmitted through the channel.To prevent this situation,Reversible logic cryptography is established in this research with optimum quantum cost,area and power. With the help of RLC,the key generated by Linear feedback shift register is utilized for encipher and decipher methods in symmetric manner. The performances are estimated for conventional and proposed method. About 7% of performance is improved in reversible logic cryptographic design related to the traditional design such as AES and Chaotic map technique.

**Keywords:** Quantum cost, Field-programmable gate array, Reversible logic cryptography,LFSR,Power

## 1. Introduction

In recent days, reversible technique has brought out as a prominent technique due to low power demand. Losing information causes loss of energy. Information is vanished when an input cannot be taken back from its output.Reversible logic gates are employed to avert low power problems.Reversible system is a model where the operation to some range is time-reversible. The salient types of reversibility are logical type and physical type reversibility. Reversible cryptographic logic design performs direct mapping of input with output.As a result, there is no reduction of energy and data. In the reversible cryptographic logic, the main important factor for optimization is number of gates used in reversible logic[4]. In this paper,design of reversible logic circuit based cryptography is efficiently attained with reference to garbage output,quantum cost and delay time.

Encipher process is mainly used to protect the data from intruders and maintains confidentiality of data[1].Reversible logic is used to maintain confidentiality along with low power dissipation.[2-3] Reversible circuit is employed to recover the information without loss and with less power consumption [4]. Loss of information can be accomplished by recovering input data from output[5]. In the reversible logic,the preservation of data is more compared to Conventional binary logic. [6–8]. In the earlier system, the cryptographic circuit is designed with Chaotic random cipher[9], AES cryptography [10], etc. but, these conventional technique provides less security and more power dissipation.

A random genearated key is introduced in modern cryptography which is used for more confidentiality and better avalanche effect,but there is more delay dueo to more iterations [11]. In order the improve the above limitations present in conventional methods,reversible logic based encipher and decipher methods and LFSR key generator are proposed in this paper.For making security and confidentiality,symmetric random key is made by Linear feedback type shift register(LFSR) in One-pad manner.

This research work is composed as follows, Section-2 describes different types of reversible logic gates which decrease power consumption. In section-3,the detailed explanation of RLC architecture of encipher process is described, Section 4 and 5 explain experimental result and conclusion.

## 2. Different types of reversible gates

Quantum cost is the important metric for measuring and analyzing reversible gates.For each reversible gate,block diagram and its quantum cost are discussed in this section.

### A. Feynman Gate

It has two primary input nets A and B and outputs P and Q. The quantum cost is 1.The block diagram is displayed in Fig. 1

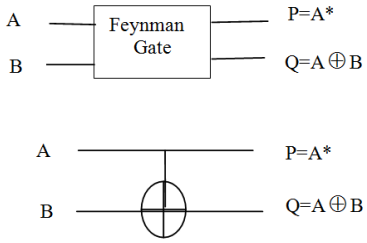


**Fig. 1. Feynman Gate**

**B. Toffoli Gate**

It has three input ports and three output ports. The quantum cost is 5.The block diagram is shown in fig.2

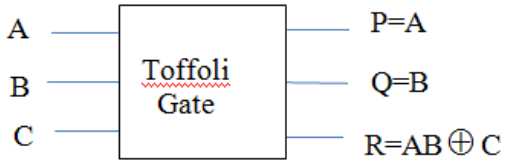


**Fig 2:Toffoli Gate**

**C. Fredkin Gate**

This gate has three input ports and three output ports. The quantum cost of Fredkin gate is 5. Block diagram is given in fig.3

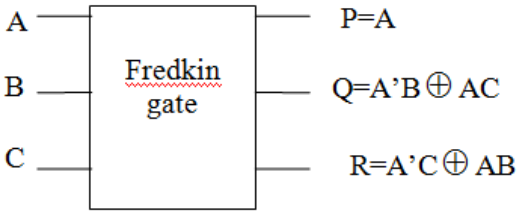


**Fig 3:Fredkin Gate**

**D. Modified Fredkin Gate**

This gate has three input ports and three output ports. The quantum cost of Modified Fredkin gate is 5. Block diagram is given in fig.4

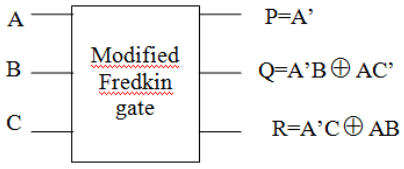


**Fig 4:Modified Fredkin Gate**

**E. SCL gate**

It has 4 input and four outputs. Output overflow is detected by SCL gate.Its quantum cost is 7.Its diagram is displayed in fig 5.

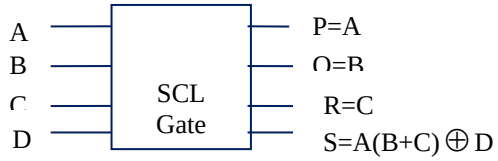

**Fig. 5:SCL gate**

F. **DFG gate**

This gate has three input ports and three output ports. The quantum cost of Modified Fredkin gate is 2. Block diagram is given in fig.6

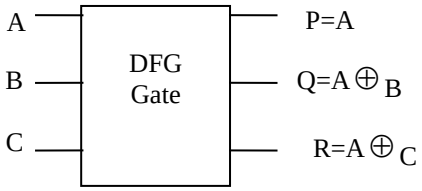


**Fig 6:DFG Gate**

**3. Architecture of Reversible logic Encryption and Decryption**

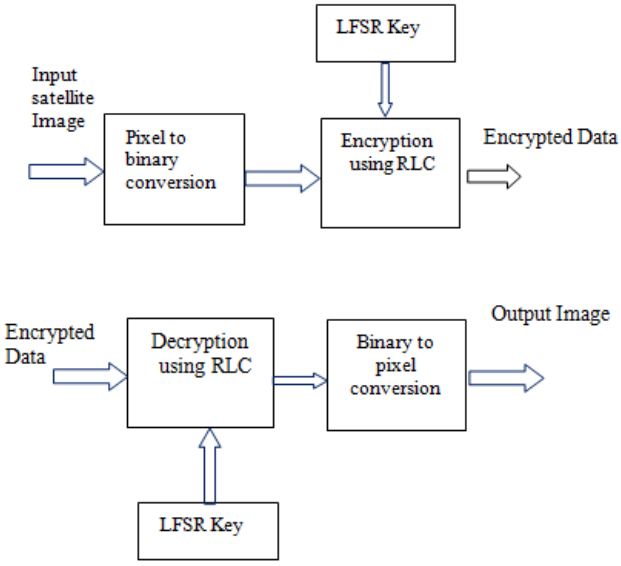


***Fig 7. Symmetric Encipher and Decipher process***

To overcome Lack of systematic key generation, unstructured FPGA design cryptography, RLC design with LFSR based key is realized in this paper. This design aids to accomplish the cryptographic process.

**3.1 RLC procedure**

Fig. 7 shows the block diagram of the entire symmetric cryptographic overall process. The operating concept of the proposed architecture is depicted below steps:

Step 1:In the transmitter section,The satellite image is converted into binary data using MATLAB.

Step 2:This binary input data is fed to the RLC based encryption block using symmetric LFSR key in VERILOG language.

Step 3:In the receiver section,the encrypted data is decrypted by using RLC based decryption block using LFSR based key in VERILOG .

Step 4:The decrypted binary data is converted into satellite image using MATLAB.

Consider the 8-bit input data x=10110110 for one pixel of image.RLC encryption produces the unique encrypted data y=00111000 and output is calculated as “10110110” using reversible manner.So,Each input creates unique ouput.

\

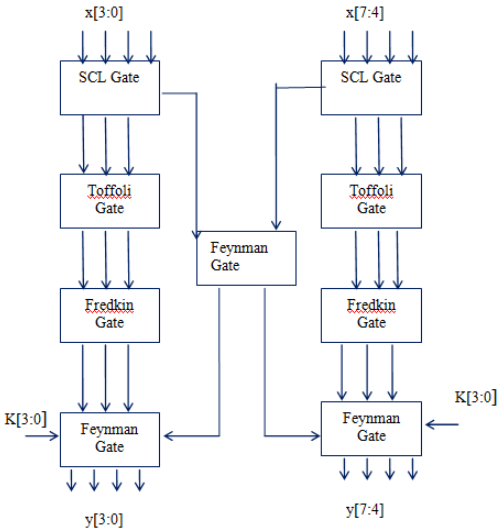


**Fig.8:Encryption process**

### 3.2 Encryption process

The encryption process is displyed in Fig. 8.

Step 1:Each pixel contains 8-bit binary value such as x[7:0].The eight bit binary data is decomposed into x[3:0] and x[7:4].

Step 2: x[3:0] is given to one SCL gate and x[7:4] is given to another SCL gate.

Step 3:From each SCL gate three outputs are given to Toffoli gate and one output alone is given 2-input Feynman gate.

Step 4: Toffoli gate outputs are given to Fredkin gate and Feynman gate using LFSR key k[3:0] and output of 2-input Feynman gate

Step 5:The outputs y[3:0] and y[7:4] are concatenated and 8 bit output x[7:0] is generated.

### 3.3 Decryption process

The decryption process is displayed in Fig.9. Here, encrypted binary value y[7:0] is fed as the input of the decryption process.

Step 1:The eight bit encrypted binary data is decomposed into y[3:0] and y[7:4].

Step 2: y[3:0] is given to one Feynman gate and y[7:4] is given to Feynman SCL gate.

Step 3:From each Feynman gate three outputs are given to Fredkin gate and one output alone is given 2-input Feynman gate.

Step 4: Fredkin gate outputs are given to Toffoli gate and SCL gate with the help of LFSR key k[3:0] and output of 2-input Feynman gate.

Step 5:The outputs x[3:0] and x[7:4] are concatenated and 8 bit output x[7:0] is generated which produces decrypted output.

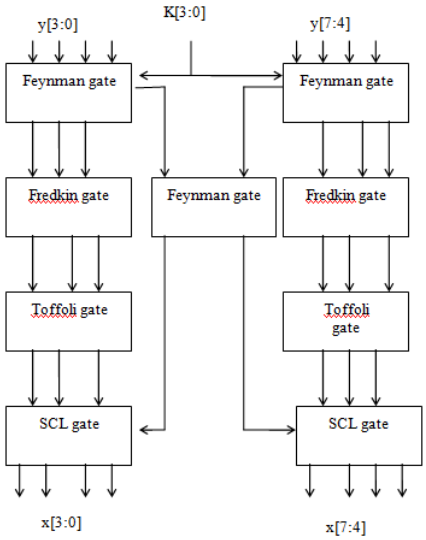


**Fig.9 :Decryption process**

### 3.4 Linear feedback shift register

LFSR is the random key stream generator, which is convenient to high-speed specifications.

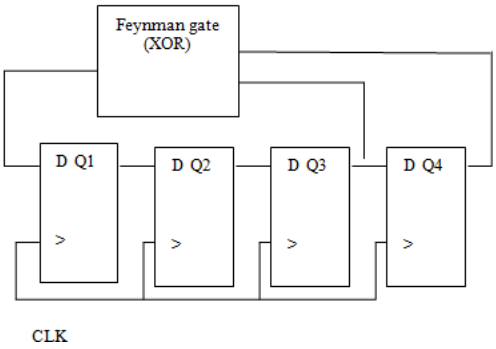


**Fig. 10:LFSR using D-Flipflop**

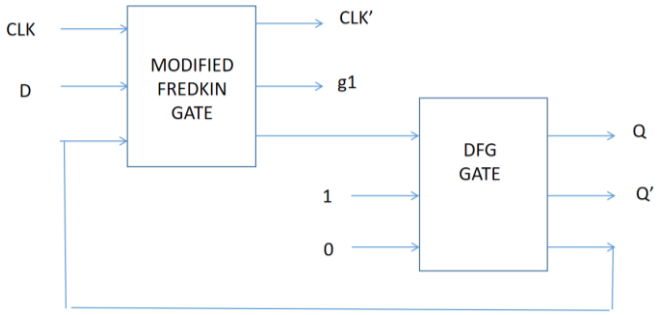


**Fig 11.D-Flipflop using Reversible gates**

The key size is the predominant factor in power and area-constrained Cryptosystem.A linear-feedback shift register (LFSR) in fig.10 and fig.11 is a shift type of register where linear operation of previous state bits contribute the current bit.EXOR or EX-NOR operation is utilized for linear operation. Here, input bit is created by EX-OR operation of output of third Flipflop and output of D-flipflop.EX-OR gate is designed with combination of Feynman gate .Truth table of LFSR is displayed in Table.1.To control this large key size problem, the random binary number is produced as a key with the help of LFSR design.

TABLE 1: TRUTH TABLE OF LFSR

| Clk | $Q_1$ | $Q_2$ | $Q_3$ | $Q_4$ | XOR-output |
|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | (0) |
| 1 | 0 | 1 | 1 | 1 | (0) |
| 2 | 0 | 0 | 1 | 1 | (0) |
| 3 | 0 | 0 | 0 | 1 | (1) |
| 4 | 1 | 0 | 0 | 0 | (0) |
| 5 | 0 | 1 | 0 | 0 | (0) |
| 6 | 0 | 0 | 1 | 0 | (1) |
| 7 | 1 | 0 | 0 | 1 | (1) |
| 8 | 1 | 1 | 0 | 0 | (0) |
| 9 | 0 | 1 | 1 | 0 | (1) |
| 10 | 1 | 0 | 1 | 1 | (0) |
| 11 | 0 | 1 | 0 | 1 | (1) |
| 12 | 1 | 0 | 1 | 0 | (1) |
| 13 | 1 | 1 | 0 | 1 | (1) |
| 14 | 1 | 1 | 1 | 1 | (0) |

## 4 Simulation results of encryption and decryption using Reversible logic

Simulation is a platform to display the characteristics of digital architectures. Simulation can be accomplished by altering levels of abstractions as gate level, register-transistor level (RTL) or behavioral level.

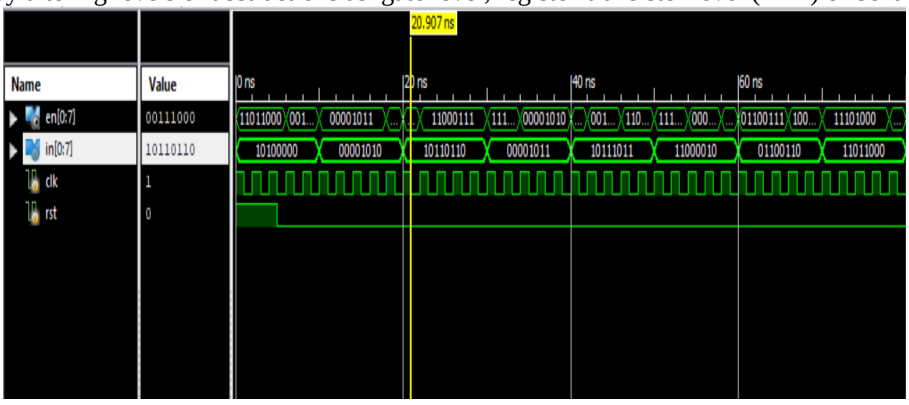


**Fig.12 :Timing diagram of Encrypted Output**

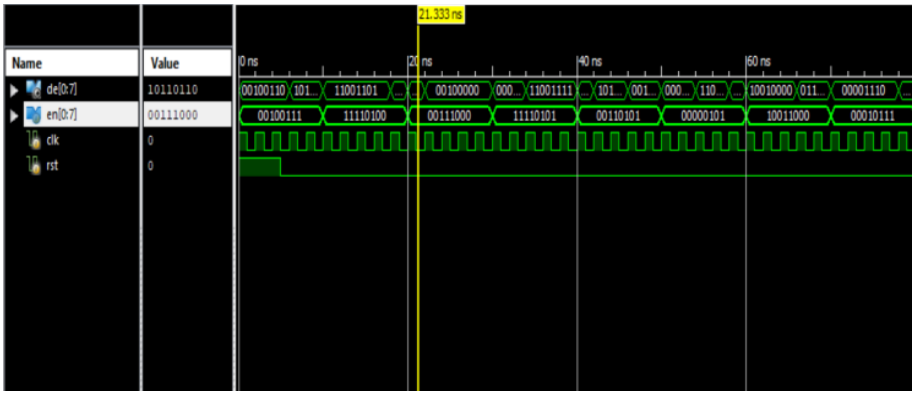


**Fig.13: Timing diagram of Decrypted output**

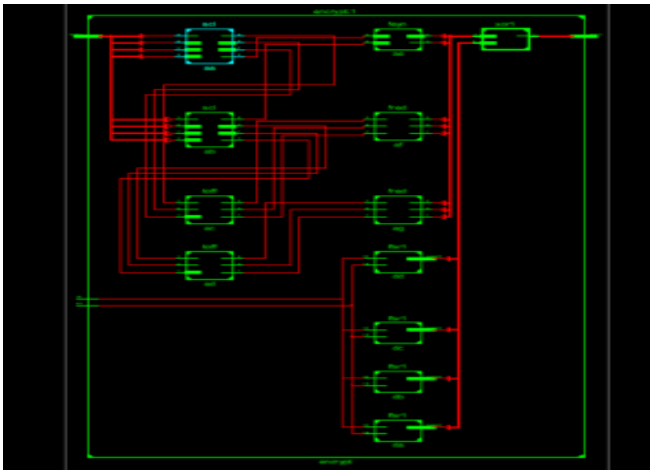

*Fig. 14: RTL Schematic for Encryption process.*

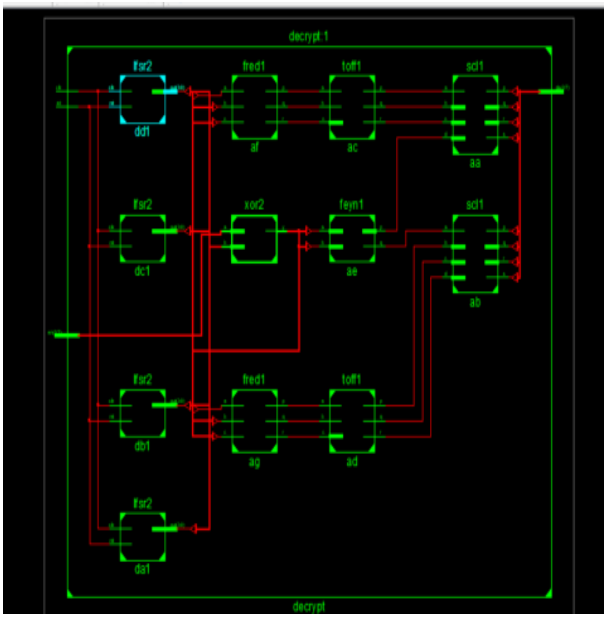


**Fig 15. RTL Schematic for Decryption process**

The cryptography issues secret and confidential information storage and transmission with less integrity with the aid of LFSR. Here the satellite image is read using MATLAB and each pixel is converted into 8 bit binary data.Serially ,each block of 8 bit binary data corresponds to each pixel is encrypted by 4 bit LFSR key.Each block can be decomposed into two sections and processed with LFSR key.LFSR concept gives more confidentiality and randomness during encipher and decipher process.Similarly,the same key known only for sender and receiver will be utilized for decryption also. Verilog in Xilinx software is used to perform encrypting data in sender side and decrypting the data in receiver side.

MATLAB is used to perform Pixel to binary conversion and Vice versa in the source and Destination.The reversible gates used in this cryptographic technique mainly contributes high security,quantum cost and less power consumption.

**Fig 16:Input Image**

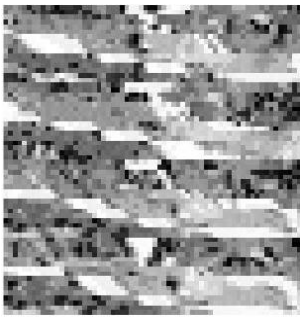

**Fig 17:Encrypted Image**

**Fig 18:Decrypted Image**

8 bit binary equivalent of each pixel is taken from MATLAB.Serially,each pixel data is fed to Xilinx-ISE software as an input message.Encryption and decryption process are performed with 4-bit symmetric key generated by LFSR.Verilog-HDL in Xilinx-ISE is utilized to simulate and synthesize encryption and decryption architecture.Finally, Decrypted data from Verilog is fed to MATLAB and converted back to decrypted satellite image.In MATLAB,Histograms of encrypted and decrypted image are quantitatively analyzed and compared and shown in fig.Using Xilinx-ISE,FPGA and performances are measured in terms of Area,Power and Delay for proposed method and correlated with existing methods such as AES and Chaos based design.RTL schematics for encryption process and decryption process shown in fig indicates there is good working condition in the proposed architecture. Timing diagrams and RTL schematics of Encryption Decryption process are shown in Fig.12-15.Original encrypted and decrypted satellite images using MATLAB are shown in fig.16-18.Quantitatively Histogram of encipher and Decipher process displayed in fig19-20 is used to explain change in pixel values in encryption and decryption process. Table 2 and 3 show the comparison of Reversible logic with AES and Chaotic type cryptography in respect of Delay ,power and Area and Quantum cost analysis of Encryption and Decryption.

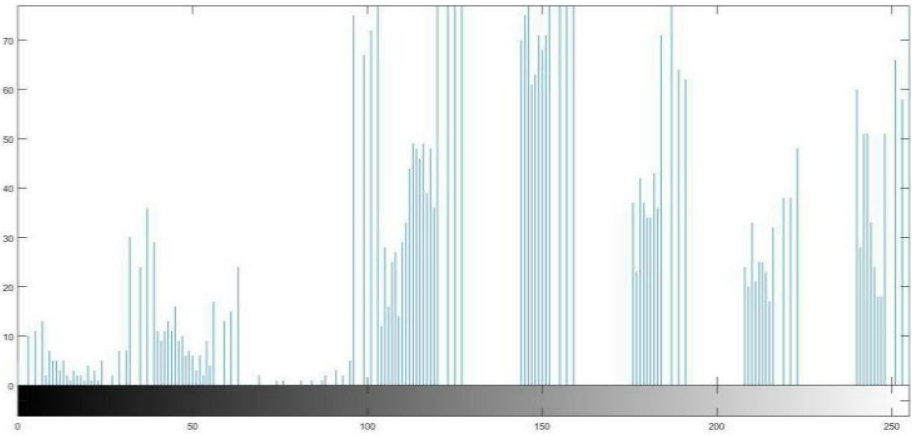


**Fig.16 :Histogram of Encrypted Image-No.of Gray levels Vs No of Pixels**

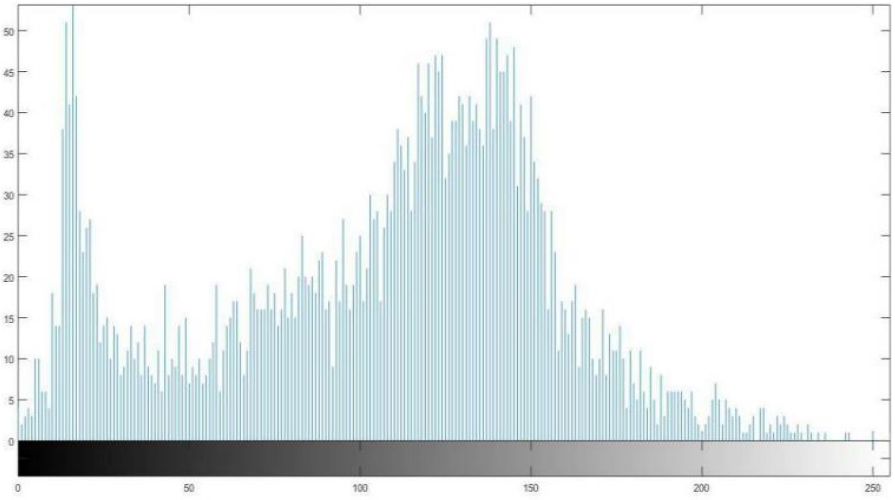

**Fig.17 :Histogram of Decrypted Image-No.of Gray levels Vs No of Pixels**

TABLE 2

COMPARISON OF AREA,POWER AND DELAY FOR VARIOUS METHODS

| **Method** | **Area ($\mu m^2$)** | **Power (mW)** | **Delay (ps)** |
|---|---|---|---|
| AES[10] | $5.21*10^9$ | 1.413 | 134.5 |
| Chaotic random method[9] | $6.547*10^6$ | 0.00154 | 198.5 |
| Proposed RLC method | $4.794*10^6$ | 0.00138 | 98.9 |

TABLE 3

ANALYSIS OF ENCRYPTION AND DECRYPTION

| **Design** | **Encryption** | **Decryption** |
|---|---|---|
| Total No of Gates | 13 | 13 |
| Quantum cost | 79 | 79 |
| Delay | 167 ns | 167 ns |

## 5. CONCLUSION

Reversible logic cryptography design of image encryption has been designed ans synthesized in Xilinx-ISE 9.1i software.High efficient reversible gates have been utilized to build the encipher process with reduced delay time, area and more quantum cost.Preprocessing and Postprocessing of images have been performed during encipher and decipher process in MATLAB. Even, the output images and histograms have been demonstrated and verified. In future, diverse type of RLC for encryption process in sender side and decryption in the receiver side will be depicted to refine the performance.

## References


1. Aditya Rawat, Ipshita Gupta, Yash Goel, Nishith Sinha, Permutation based im- age encryption algorithm using a block cipher approach, in: Advances in Com- puting, Communications and Informatics (ICACCI), 2015 International Conference on, IEEE, 2015, pp. 1877–1882.
2. Cheng, Chua Shin, Ashutosh Kumar Singh, Lenin Gopal, Efficient three variables reversible logic synthesis using mixed-polarity Toffoli gate, Procedia Comput. Sci. 70 (2015) 362–368.
3. Amrtha Anand K, Dheena Kurien.(2016) Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography. Current Trends in Information Technology. 2016; 6(2): 27-33
4. Bikromadittya Mondal, Palash Das, Pradyut Sarkar, Susanta Chakraborty,(2014) A comprehensive fault diagnosis technique for reversible logic circuits, Computers and Electrical Engineering 40 (7) 2259–2272.
5. Trailokya Nath Sasamal, Ashutosh Kumar Singh, Anand Mohan, Reversible logic circuit synthesis and optimization using adaptive genetic algorithm, Procedia Computer Scencei 70 (2015) 407–413.

6. P.Mercy Nesa Rani, Abhoy Kole, Kamalika Datta, Alok Chakrabarty, Realization of ternary reversible circuits using improved gate library, Procedia Comput. Sci. 93 (2016) 153–160.
7. Shijun Xiang, Xinrong Luo, Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group, IEEE Trans. Circuits Syst. Video Technol. 28 (11) (2018) 3099–3110.
8. Rigui Zhou, Yang Shi, Jian Cao, Transistor realization of reversible series gates and reversible array multiplier, Microelectronics Journal. 42 (2) (2011) 305–315.
9. I˙smail Koyuncu, Ahmet Turan Özcerit, The design and realization of a new highspeed FPGA-based chaotic true random number generator, Comput. Electr. Eng. 58 (2017) 203–214.
10. H. Zodpe, A. Sapkal, An efficient AES implementation using FPGA with enhanced security features, Journal of King Saud University (2018) .
11. Gajendra Singh Prof., Preeti Shukla, Design and development of new symmet- ric cryptography protocol to improve text security, International J. Adv. Res. Comput. Sci. Softw. Eng. 4 (11) (2014) November ISSN: 2277128X.