LOW AREA FPGA IMPLEMENTATION OF DROM-CSLA-QTL ARCHITECTURE FOR CRYPTOGRAPHIC APPLICATIONS

Shailaja A[1] and Dr Krishnamurthy G N[2]

[1]Research Scholar, V T U RRC, Belagavi, Karnataka, India
[2]Principal, B N M Institute of Technology, Bangalore, Karnataka, India

ABSTRACT

Nowadays, several techniques are implemented for the cryptosystems to provide security in communication systems. The major issues detected in conventional methods are the weakness against different attack, unacceptable data expansion, and slow performance speed. In this paper, a method Dual-port Read Only Memory-Carry Select Adder-Quantitative Trait Loci (DROM-CSLA-QTL) is introduced, which utilizes lower area than the existing method. The proposed system is implemented using DROM-CSLA, which occupies less area. The DROM-CLSA-QTL algorithm is implemented using tools such as MATLAB and Model Sim. Further for FPGA implementation, Virtex 4, Virtex 5 and Virtex 6 devices are used to determine the number of Lookup Tables (LUTs), slices, flip-flops, area and frequency. Mean, Variance and Covariance are evaluated in the MATLAB.

KEYWORDS

Cryptosystem, Dual-Port read-only memory, Carry select adder, Quantitative trait loci, and MATLAB.

1. INTRODUCTION

The encryption process employs a finite set of instruction which converts the real message into Ciphertext. Real message may consist of videos, images, voice, and text etc. which are encrypted by employing previously identified algorithms [1]. Information security becomes very essential for under resource-constrained environment. Light-weight Block Ciphers (LBCs) is an advanced methodology to deliver an adequate power consuming solution. Piccolo, Light Encryption Device (LED), PRESENT and LB are the various type of LBCs used in cryptography. These LBCs are implemented by using less than 3000 physical gate count [2]. The Light-weight cryptography is classified into two types such as LBC and light-weight asymmetric [3]. Light-weight cryptography is one of the developing domains which support the cipher design that results in low area requirement. The significant parameter in the Light-weight cipher design is the number of gates. Furthermore, the light-weight cipher is used in the resource-constrained applications where power, memory size, low area are the main requirements [4], [5].The effective communication channel is required to carry the digital data through the transmission channel. In the meantime, the security of the digital data becomes very important in data communication systems. The information or data to be transmitted can be protected by performing encryption using standards such as RSA or AES. Nowadays, highly secured encryption standards are used to encrypt the data for secure transmission so that, the information cannot be read or modified by others [6].

The light-weight cryptography domains revolve around light-weight cipher designs which are used for low-power and resource-constrained devices such as Wireless Sensor Node (WSN) and Radio frequency identification devices (RFID Tags) [7]. The methods used for encrypting images

DOI: 10.5121/ijnsa.2018.10303

are different from those used for encrypting text because of some inherent features of the image like large data size and high correlation among the pixels which are commonly difficult to handle by conventional methods [8]. An encryption algorithm for transmitting secret data by using encoding over a communication channel is transmitted in the application layer [9]. A modern block cipher is implemented based on Tweakable Enciphering Scheme (TES). The main disadvantage of TES construction is it involves only the encryption function of fundamental block ciphers [10]. To solve this problem, the DROM-CSLA-QTL method is introduced in this paper to reduce computation complexity and hardware usage. DROM is used to read the data from permutation. In add constants, CSLA is used to perform addition operation between one constant and D flip-flop output. In FPGA implementation, Virtex 4, Virtex 5 and Virtex 6 devices are used to determine the number of LUTs, slice, flip-flop, power, delay, and frequency. From the encrypted image, mean, variance, covariance, histogram and correlation coefficient is analyzed for the proposed method. Finally, the improved FPGA performances of DROM-CSLA-QTL method are compared with existing method.

The work is outlined as follows. Section 2 deals with previous related work. Section 3 includes DROM-CLSA-QTL architectural design and methodology. Experimental setup and performance analysis results are shown in Section 4 and Section 5 gives the conclusion of the work.

2. RELATED WORK

Klinc *et al.* [11] proposed an investigation over compression of information encrypted with block cipher chaining like Advanced Encryption Standard (AES), which shows that such information was possibly encrypted without the use of the secret key. A block cipher can operate in different chain modes. The message blocks cannot be re-encrypted after the modification of this technique.

Zha *et al.* [12] proposed the three-dimensional block cipher as a 3D version of AES that employs 3D state and even round functions. The work employed a known-key attack model implemented by Knudsen and Rijmen and developed distinguisher at the fifteenth rounds of 3-D. The distinguisher was created by employing rebound methods. The drawback of this method was that it considered limited rounds.

Z. H. A. O Guosheng and W. A. N. G. Jian [13] illustrated the safety of ciphertext. The implementation was based on confusion substitution of the Substitution box(S-box), hence changing the internal structure of the information blocks by 4-steps of matrix transformation. In this paper, the dynamic key was generated by utilizing Level Feedback Shifter Register (LFSR) which enhanced the stochastic characters of the secret key in each round cycle. In this paper, the security execution was evaluated by the simulation test. But LFSR is mostly used for the linear function of single-bit XOR operation.

Sanandaji *et al.* [14] proposed the utilization of a block cipher output as a confidential phase pulse compression. A key-based technique was implemented in this paper that was used for Electronic Warfare (EW) application. The main advantage of this method is an effective protection against some electronic attacks.

Aysu *et al.* [15] developed SIMON, which proved to be a low-cost substitute to AES on reconfigurable platforms. The Feistel structure network, the construction of the round function and the key generation of SIMON, enables bit-serial hardware architectures, which reduces the system cost. This method employs 128-bit input text and the 128-bit key to generate 128-bit ciphertext in 68-rounds.

All these related works contain several problems like more area, power, and high critical path utilization. Hardware and FPGA utilization is also more. The DROM-CSLA-QTL method overcomes these problems and improves the FPGA implementation results like LUTs, slices, and flip-flops.

3. DROM-CSLA-QTL METHODOLOGY

An existing Feistel Type Structure (FTS) [16] can change the half of the block data (message) in an iterative round. But DROM-CSLA-QTL architecture overcomes this limitation and changes all block messages. Hence, DROM-CSLA-QTL architecture has the speed of diffusion, Substitution permutation Network (SPN) structure, which increases the security of Ultra-light weight block ciphers (ULBC) in FTS. The DROM-CSLA-QTL design employs less area in the applications which require low power utilization constraints

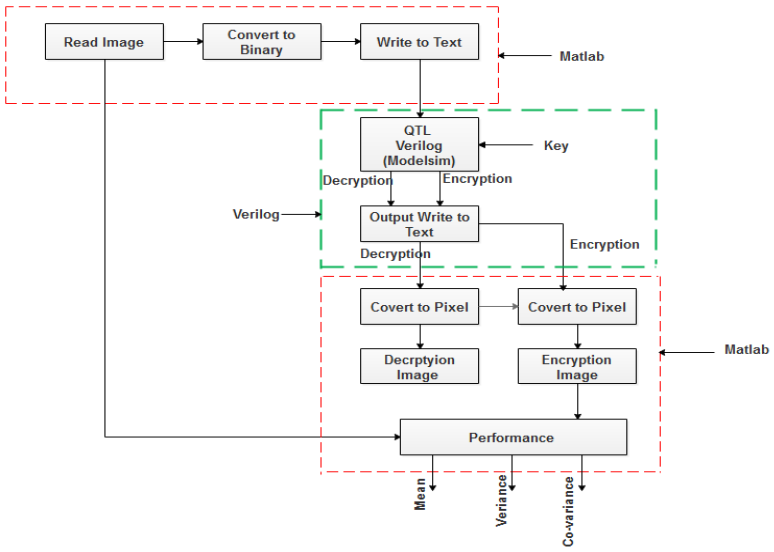

Figure.1 Block diagram of the DROM-CSLA-QTL Methodology.

DROM-CSLA-QTL is a modern variant of generalized Feistel Structure Network (FSN) algorithm which supports 64-bits block with 64-bits keys. The fig.1 shows the block diagram of the DROM-CSLA-QTL methodology. The working principle of the DROM-CSLA-QTL method is described below:

- The input image is read from MATLAB which is converted into binary values.
- The binary values are converted to text format in MATLAB.
- The DROM-CSLA-QTL requires a key for the encryption process. So, the key value is stored in Verilog.
- The text format output of MATLAB is input to Verilog (Modelsim).
- Encryption and decryption both processes are done in the Verilog (Modelsim).
- The Verilog output is in text format for both the encryption and decryption process.
- The encrypted and decrypted text values are converted into pixels, and these pixel values are converted into the image using MATLAB.
- The decrypted image is similar to the input image.

- In the final stage, the performances such as mean, variance, covariance and correlation coefficient, and histogram are taken from the encrypted and input image.

3.1. THE DROM-CSLA-QTL 64-BIT DATA PATH

A block diagram of the DROM-CSLA-QTL-64 bit data path is shown in the fig.2. Every round of architecture includes key addition, Add Constant, Round Constants, DROM, CSLA, permutation layer (P), right data addition and Round Transposing (RT). In this paper, the architecture basically needs eight 16-bits or 128 bits wide registers, each bit composed of D flip-flops and requires ten 2-to-1 MUX. The 64-bits plaintext is separated into four 16-bits inputs and then 4-plaintext inputs are stored in the four 16-bits large register. The 64- bits key is separated into four 16 bits inputs in the same way. The 4- key inputs are stored in the four 16 bits registers. The RCA is implemented as bit-wired XOR operations. The two key additions and the two right data additions are implemented as bit-wired XORs.

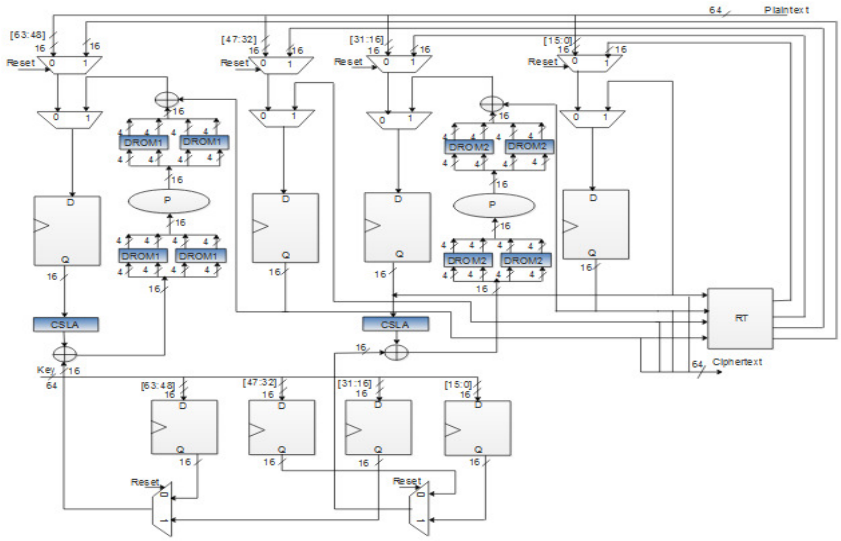

Figure.2 Block diagram of the DROM-CSLA-QTL data path.

3.1.1. DROM-CSLA-QTL STRUCTURE

The DROM-CSLA-QTL structure employs a Differential Characteristic Probability (DCP) and the best linear characteristic approximation, where the cipher schemes used for DCP and the linear analysis are secured in the cryptography systems. Thus, the DROM-CSLA-QTL structure design optimizes the security of ULBC in the FTSs. In this work, the DROM-CSLA-QTL structure design is different from a block cipher, which occupies less area in hardware design and simple cipher structure. The removal of the key schedule minimizes the area and energy requirements. The use of common Feistel- structure without key schedule makes the algorithm secured against related-key attacks and makes DROM-CLSA-QTL significant among existing cipher algorithms. Moreover, use of FTS in proposed system employs the same algorithm for Encryption and Decryption processes in the resource-constrained applications, which improves the low-area requirement.

3.1.2. FEISTEL FUNCTION

The Fiestel function employs a permutation (P) layer between two 4x4 DROM box layers. The Feistel function has the characteristic of lightweight and high security. The round constant does not require more memory resource to save the data. 16-bit round subkeys and inputs of 16 bits carry out the XOR operation. This structure does not require more cost for the hardware resource. Therefore, this Feistel function structure is suitable for ULBCs.

3.1.3. P-LAYER AND ROUND TRANSPOSE (RT)

This section improves the efficiency of the proposed algorithm and decreases of the hardware implementation cost. Two effective designs are applied for the linear layers such as P-layer and Round Transpose (RT). The P-layer has 16- bit permutations which can be easily implemented in the hardware. Moreover, it develops the security against cryptanalysis. The RT employs 16 bits words moving between the rounds instead of the cyclic shift of the bits in the standard generalized Feistel networks. Hence, the structure of RT is efficient, which can be used in software (S/W) and H/W constrained environments.

3.1.4. DROM DESIGN

In this work, DROM is used instead of S-box. The Left side of architecture contains two 2x2 DROM and right side contains two 2x2 DROM. The P -layer is bit wired and RT is 16-bits wiring. The control signals are handled by control logic module. The proposed algorithm (DROM-CLSA-QTL) encrypts a 64-bits plaintext with 64-bits key, using 16-clock cycles. Add constant process uses CSLA. The CSLA has reduced area requirement, cost and increases the system speed when implemented in the hardware and software.

3.1.5. CSLA DESIGN

In add constant, a new area efficient CSLA adder is used instead of the normal adder, which is presented in Fig.3. This adder achieves fast arithmetic operation in various data processing techniques. The main aim of using this adder is to minimize the area required, power dissipation, and delay. The CSLA is used in many computational implementations to cut the carry propagation delay. The basic idea is to use BEC (binary to excess-1 converter) instead of RCA (Ripple Carry Adder) with C_{in}=1. By using fewer numbers of logic gates, BEC logic is derived instead of using n-bit FA (Full adder).

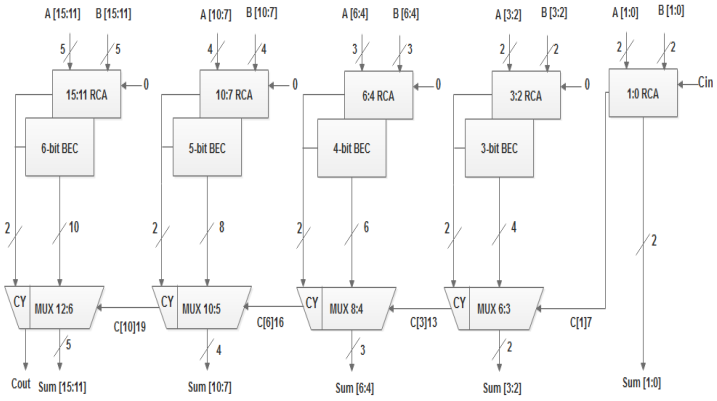

Figure.3 Block diagram of low-area CSLA.

The advantage of the BEC logic is that it uses lesser number of logic gates than the n-bit full adder structure. The group2 has one 2-b RCA which has 1 FA and 1 HA for C_{in}=0. Instead of 2-b RCA, 3-b BEC is used which adds one to the output from 2-b RCA. The input arrival time is lesser than the multiplexer selection input arrival time. Based on the selection line input C_{in}, this adder gives either BEC output or multiplexer output. The multiplexer delay and mux selection arrival time are derived from the different kind of groups. In FPGA implementation, the number of LUTs, slice, and flip-flop will be decreased in DROM-CSLA-QTL for different Virtex devices such as Virtex 4, Virtex 5 and Virtex 6.

4. RESULTS AND DISCUSSIONS

In the proposed algorithm, both encryption and decryption are performed in Modelsim by using the Verilog code. In Modelsim, the text format of input image is encrypted and decrypted using same key. The Verilog output is in text format for both the encryption and decryption process. FPGA performance was analysed for different devices of Virtex- 4, Virtex-5 and Virtex-6 by using Xilinx 14.4 ISE tool. The RTL schematic was taken from synplify pro tool.

Figure.4 Input image

```
01111001
01111001
01111000
01111001
01111101
01111111
01111100
10000100
10000111
10001111
10001100
10000111
```

Figure.5 Input binary image

The fig. 4 shows the input image (lena.jpg). The input image is converted into binary values using MATLAB. The output produced by MATLAB is in text format. Fig.5 shows binary values of the

input image. The text format output is input to Verilog. The Verilog outputs are in text formats for both encryption and decryption.

```
11101001
11010111
01001100
00011100
11100010
11010100
11001011
11111101
10111110
10001100
10111011
01011010
```

Figure.6 Encrypted binary value

```
01111001
01111001
01111000
01111001
01111101
01111111
01111100
10000100
10000111
10001111
10001100
10000111
```

Figure.7 Decrypted binary value

Figure 6 and 7 shows the binary values of encryption and decryption for the input image (lena.jpg). The text values are converted into pixel format, and pixels are then converted back into an image in MATLAB. Figure 8 shows the encrypted image of input image which reveals the effectiveness of hiding the information contained in it.

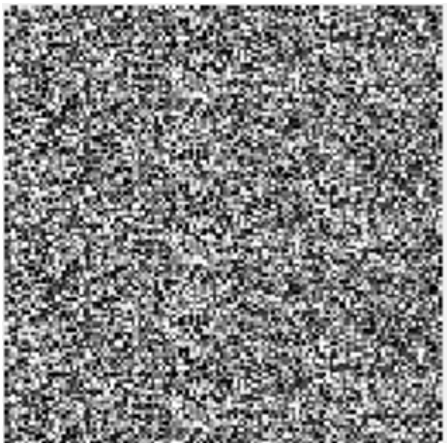

Figure.8 Encrypted image

Figure.9 Decrypted image

Fig. 9 shows the decrypted image of the input image. The decrypted image is similar to the input image showing the effectiveness of the proposed algorithm. The mean, variance, covariance and correlation coefficient performances are computed from the encrypted and input image.

4.1. FPGA Synthesis

The FPGA synthesis is implemented in Xilinx tool for different devices such as Virtex-4, Virtex-5, and Virtex-6. From this tool, the performances such as LUT, flip-flop, Slices, and Frequency are calculated.

4.1.1. LUT

A LUT stands for Lookup Table**.** It is basically a table that determines what will be the output for any given input(s). In the context of combinational logic, it is the truth table. This truth table effectively defines the behavior of combinational logic.

4.1.2. Flip-flop

Generally, the flip-flop is a memory element which stores data on the application of clock pulse with an FPGA circuit. On each clock edge, a flip-flop latches 1 or 0 (TRUE or FALSE) value on its input and holds that value constant until the next clock edge.

4.1.3. Slices

Logic resources are resources on the FPGA that perform logic functions. Logic resources are grouped in slices to create configurable logic blocks. A slice contains a set of LUTs, flip-flops, and multiplexers. A LUT is a collection of logic gates hard-wired on the FPGA.

4.1.4. Frequency

Frequency is defined as the number of occurrences of an event over a unit period of time or in a given sample.

Table.1. Comparison of various performance parameters on different Xilinx FPGA devices for Existing QTL and DROM-CSLA-QTL method.

Target FPGA	Circuit	LUT	Flip-flop	Slice	Frequency (MHz)
Virtex4 xc4vfx12	Existing QTL	599/10944	80/10944	367/5472	253.95
	DROM-CSLA-QTL	607/10944	80/10944	361/5472	307.43
Virtex5 xc5vlx20T	Existing QTL	254/12480	80/12480	101/3120	285.32
	DROM-CSLA-QTL	233/12480	133/12480	104/3120	467.68
Virtex6 xc6vcx75t	Existing QTL	47/46560	78/93120	34/11640	228.78
	DROM-CSLA-QTL	55/46560	71/93120	31/11640	248.17

Table.1 shows the Implementation of different Xilinx FPGA devices for existing and DROM-CSLA-QTL methods, used for analyzing the performance parameters such as LUTs, the number of flip-flops, slices, and operating frequency for different FPGA devices such as Virtex 4, Virtex 5 and Virtex 6. From this table, it is clear that the LUT, flip-flop, slices are reduced and operating frequency is increased in DROM-CSLA-QTL method than the existing method. Due to the reduction of these parameters, the area has been minimized in DROM-CSLA-QTL architecture. These FPGA results are taken from Xilinx software.

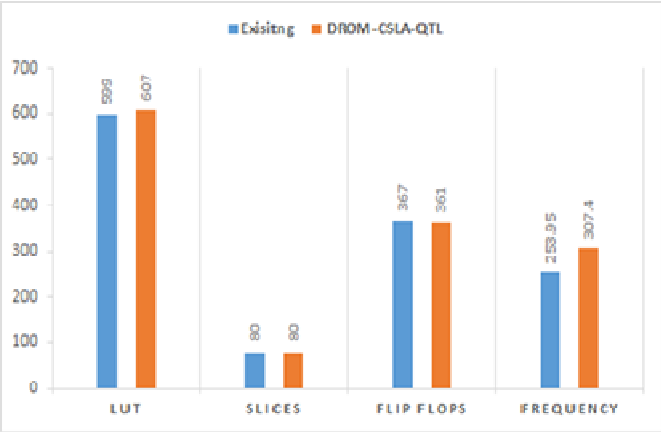

Figure.10. Comparison of the FPGA performance onVirtex-4 for Existing and DROM- CSLA-method.

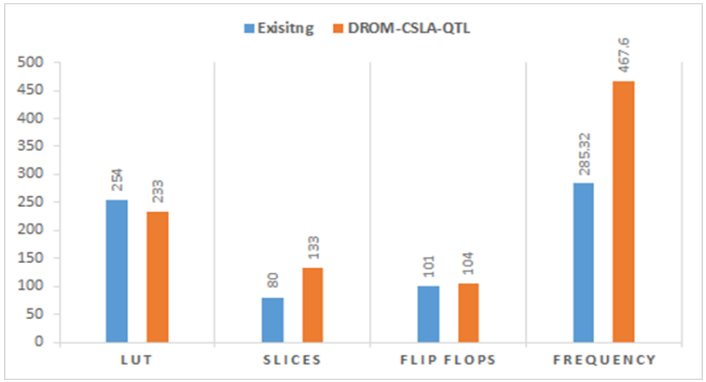

Figure.11. Comparison of the FPGA performance on Virtex-5 for Existing and DROM- CSLA-QTL method.

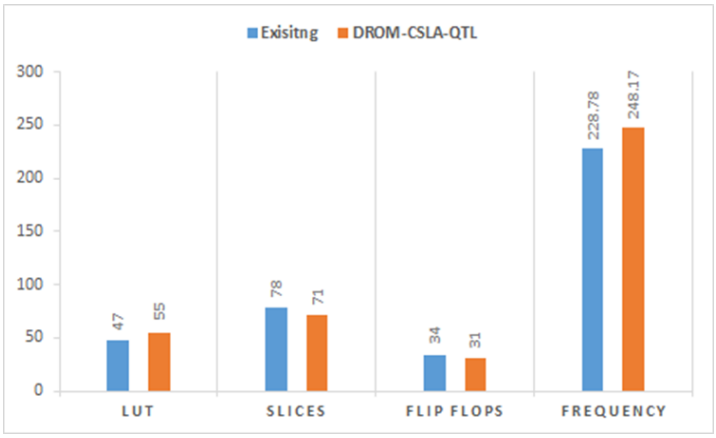

Figure.12. Comparison of the FPGA performance on Virtex-6 for Existing and DROM- CSLA-QTL method.

The performance of LUT, flip-flop, slices, and frequency for the Existing and DROM-CSLA-QTL method is shown in fig.10, fig.11, and fig.12. From the graphs, it is clear that the performances have improved in DROM- CSLA-QTL method than conventional methods. In the fig. 10, 11, and 12, the blue color denotes existing method and orange color denotes the DROM-CSLA-QTL method. The DROM-CSLA-QTL design timing diagram was verified in ModelSim by using Verilog code. Figure 13, shows the timing diagram for DROM-CSLA-QTL. The timing for encryption and decryption are indicated using yellow color in the timing diagram.

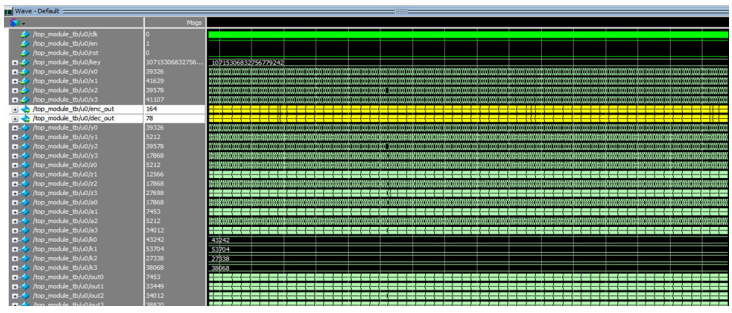

Figure.13 Timing diagram for DROM-CSLA-QTL

4.2 MATLAB PERFORMANCE

The mean, variance, and covariance performances are calculated from the encrypted image.

4.2.1. MEAN

The mean is the average of given number, which is called an arithmetic mean. To compute the mean, add all numbers in a group, and divide the sum by the total count of numbers. The mean value is computed using equation (1):

$$Mean(\mu) = \frac{1}{N}\sum_{n=0}^{N}\frac{1}{}\mu(n) \quad (1)$$

4.2.2. VARIANCE

Variance is a measurement of the distance between the numbers in a data group from the mean. The variance is computed by taking the difference between each number in the data group, and squaring the differences and dividing the total number of squares by the number of values in the group. The variance is calculated by using equation (2):

$$\sigma^2 = Var(X) = \sum_{n=0}^{N-1}(X - \mu^2) \quad (2)$$

4.2.3. COVARIANCE

Covariance is a measure of how two variables are related. A positive covariance means the variables are positively related, while a negative covariance means the variables are reciprocally related. Equation (3) is used for computing the covariance of sample data.

$$Cov(X,Y) = \frac{\sum E(X-\mu)E(Y-V)}{n-1} \quad (3)$$

Table.2. Mean, variance, co-variance performance of the DROM-CSLA-QTL method.

Source	Mean	Variance	Co-variance
Encrypted image	128.0326	5.5745e+05	56.0538

The Table 2 tabulates the mean, variance and covariance performances for encrypted image.

4.2.4. HISTOGRAM ANALYSIS

Histogram of an image usually changes even if there is a slight change in the image. The change in histogram depends on the changes in the images. In the proposed system, histograms of input image, encrypted image and decrypted images are taken.

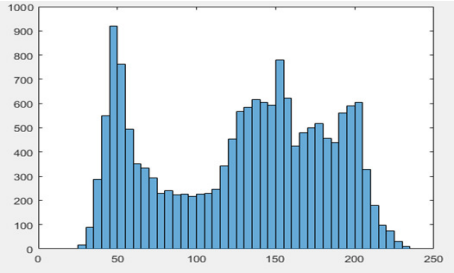

Figure.14. Histogram for Input image.

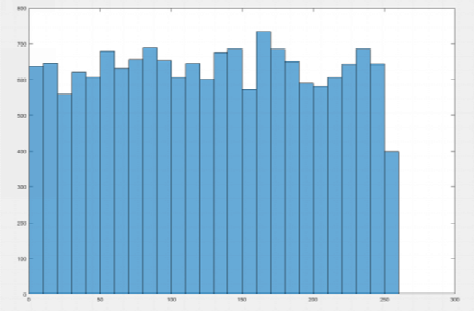

Figure.15 Histogram of Encrypted image

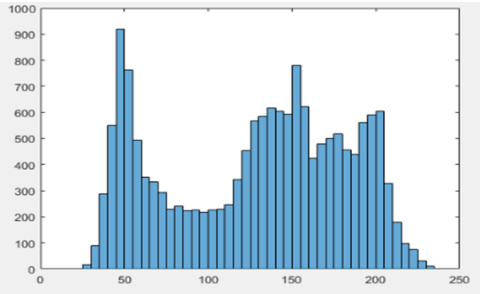

Figure.16 Histogram of decrypted image

Figure 14, 15 and 16 shows histograms of the input image, encrypted image and decrypted image respectively. The histogram of the input image and decrypted image are similar. The histogram of encrypted image is fairly uniform and different from the histogram of the input image which indicates that the proposed algorithm is efficient. From figure 16, it is clear that the decrypted image is not affected by the noise.

5. CONCLUSIONS

The DROM-CSLA-QTL architecture was implemented in Xilinx software by using Verilog code. The proposed method achieves low area and hardware (H/W) cost compared to the existing methods. In this work, the cryptographic system was implemented by using CSLA, which occupies less area. FPGA performance has reduced number of LUT, slices and flips flop and increased the frequency. The DROM-CSLA-QTL method improved the system performance compared to conventional methods.

REFERENCES

[1] Lang Li, Botao Liu, Hui Wang,"QTL: A new ultra-lightweight block cipher", (2016) Elsevier, journal homepage: www.elsevier.com,Microprocessors and Microsystems pp. 45–55.

[2] Zhang, Fan, Size Guo, Xinjie Zhao, Tao Wang, Jian Yang, Francois- Xavier Standaert and Dawu Gu (2016). "A Framework for the Analysis and Evaluation of Algebraic Fault Attacks on Lightweight Block Ciphers." IEEE Transactions on Information Forensics and Security 11, vol no. 5 : pp 1039-1054.

[3] Rohmad, Mohd Saufy, Azilah Saparon, Harith Amaran, Nazmin Arif, and Habibah Hashim. (2017) "Lightweight block ciphers on VHDL." In Computer Applications & Industrial Electronics (ISCAIE), IEEE Symposium, pp. 87-90.

[4] Bansod, Gaurav, Abhijit Patil, Swapnil Sutar, and N. Pisharoty. (2016) "An ultra-lightweight encryption design for security in pervasive computing in Big Data Security on Cloud (Big Data - Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 79-84.

[5] Zhang, Wentao, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. (2015) "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms." Science China Information Sciences 58, Volume no. 12: pp1-15.

[6] Mataram, Zaeniah-AMIKOM, and Bambang Eka Purnama-STMIK Nusa Mandir, 1.1(2015). "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm." Publikasi International conference .

[7] Patil, Jagdish, Gaurav Bansod, and Kumar Shashi Kant. "LiCi: A new ultra-lightweight block cipher."(2017) In Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference , pp. 40-45. IEEE, 2017.

[8] Amin, Mohamed, Osama S. Faragallah, and Ahmed A. Abd El-Latif. 15.11 (2010) "A chaotic block cipher algorithm for image cryptosystems." Communications in Nonlinear Science and Numerical Simulation: 3484-3497.

[9] Khiabani, Yahya S., Shuangqing Wei, Jian Yuan, and Jian Wang. (2012) "Enhancement of secrecy of block ciphered systems by deliberate noise." IEEE Transactions on Information Forensics and Security,Issue 7, Vol no. 5,pp 1604-1613.

[10] Sarkar, Palash. (2011) "Tweakable enciphering schemes using only the encryption function of a block cipher." Information Processing Letters 111, Vol no. 19: pp945-955.

[11] Klinc, Demijan, Carmit Hazay, Ashish Jagmohan, Hugo Krawczyk, and Tal Rabin. (2012) "On compression of data encrypted with block ciphers." IEEE transactions on information theory 58, Vol no. 11:pp 6989-7001.

[12] Zha, Daren, Shuang Wu, and Qiongxiao Wang(2015). "Improved known-key distinguisher on round-reduced 3D block cipher." Chinese Journal of Electronics 24.1 (2015): pp 199-204.

[13] Guosheng, Z. H. A. O., and W. A. N. G. Jian.(2016) "Security analysis and enhanced design of a dynamic block cipher." China Communications ,Issue13, Vol no. 1 (2016):pp 150-160.

[14] Sanandaji, Nader, and Mohammad Soleimani(2015). "Pulse compression security enhancement as an electronic protection technique by exploiting a block cipher output as phase-code." IET Radar, Sonar & Navigation 9.4 (2015): pp 384-391.

[15] Aysu, Aydin, Ege Gulcan, and Patrick Schaumont.(2014) "SIMON says: Break area records of block ciphers on FPGAs." IEEE Embedded Systems Letters 6.2 (2014): pp 37-40.

[16] Zhang, Lei, and Wenling Wu. "Improved Differential and Linear Active S-Boxes Search Techniques for Feistel Type Ciphers." Chinese Journal of Electronics 24.2 (2015): pp 343-348.