Received: January 30, 2019

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

VLSI Implementation of Hybrid Cryptography Algorithm Using LFSR Key

Shailaja Acholli[1]* **Krishnamurthy Gorappa Ningappa[2]**

[1]*Visvesvaraya Technological University, India*
[2]*Bhageerathi Bai Narayana Rao Maanay Institute of Technology, Bangalore, India*
* Corresponding author's Email: sb_shastri@rediffmail.com

Abstract: The security and confidentiality of the information has become a significant factor in the communication field. Several techniques for encryption and decryption are proposed to promote the security of the communication systems. Most powerful and significant part of the encryption is a key generation. Presently, hackers are able to break the key with help of the modern high computing machines. In this research, hybrid cryptographic algorithm - Extended Tiny Encryption Algorithm (XTEA) combined with International Data Encryption Algorithm (IDEA) was implemented for improving the security in real-time applications. A large key size ensures the randomness, but proportionally maximizes the network load with high complexity. To overcome this problem, the random numbers were generated using a Linear Feedback Shift Register (LFSR) scheme for key function. This algorithm was appropriate for encryption and decryption of online streaming data. The proposed method is named as International Data - Extended Tiny based Encryption Algorithm –LFSR (ID-XT-EA-LFSR) method. The ID-XT-EA-LFSR method improves the FPGA performances up to 50.43% compared to the QTL, DROM-CSLA-QTL and XTEA algorithms.

Keywords: Decryption, Encryption, Extended tiny encryption algorithm, Hybrid cryptography, International data encryption algorithm, Linear feedback shift register.

1. Introduction

Cryptography is the technique of hiding data so that only authorized receivers can view it. It is a powerful way of securing information in communication [1]. Generally, cryptographic methods consist of fundamental components such as plain text, cipher text, key and cryptographic algorithm [2]. Enhancing the privacy of the information against unauthorized access is the major objective of the cryptographic mechanism. The key steps that relay on this cryptographic mechanism are encryption and decryption [3]. The data encryption is the most traditional approach that secures highly confidential information by employing some conventional algorithm, which already exists or is pre-written. The key generation is one of the most important part of the encryption process [4]. Two methods of key generation exist: symmetric key generation and asymmetric key generation [5]. Data Encryption Standard (DES) is one of the well-known algorithms, which is most widely used in security of the network. Though, serious consideration arises for long-term security due to the relatively short key length [6].

Tweakable Enciphering Scheme (TES) approach uses a hash key that has a key length as long as the message length, which is the major drawback of the TES approach [7]. The Blowfish algorithm is accepted as one of the strong encryption algorithm. In the blowfish algorithm, avalanche effect is not enough for providing strong security [8] and it is affected by weak keys problem [9]. Researchers have developed several techniques for improving the performances of the cryptosystem methods, but yet there is a scope for developing the existing methods to further improve the security level [10]. In this research, two algorithms namely, XTEA and IDEA are combined to produce a hybrid algorithm which is used for encryption and decryption. The random numbers are generated using LFSR method for key purpose. The major objective of the proposed ID-XT-EA-LFSR algorithm is to provide high encryption

and decryption quality with minimum FPGA requirement and computational time. The performance of the ID-XT-EA-LFSR algorithm is evaluated in terms of LUT, Number of Flip Flops, Slice and frequency. The results are compared with the existing cryptographic algorithms such as QTL, DROM-CSLA-QTL and XTEA.

The research work is composed as follows; Section-2 presents survey of recent papers on encryption and decryption algorithms. Section-3, gives brief explanation of the ID-XT-EA-LFSR algorithm. In section-4, the comparative experimental results of the proposed algorithm with existing encryption and decryption algorithms are discussed. The research work's conclusion is made in the section-5.

2. Literature survey

Many researchers have suggested several algorithms on cryptosystems. A brief review of some important contributions of the existing algorithms are presented below.

M. Mozaffari-Kermani, K. Tian, R. Azarderakhsh, and S. Bayat-Sarmadi [11] proposed an error detection technique for a Light-weight block cipher (LBCs) implemented with XTEA. Three different types of error detection techniques were presented in this research such as XTEA, PRESENT and SIMON. The proposed fault diagnosis techniques provided high error coverage at the expense of acceptable overheads on the FPGA platforms, making the hardware architectures of the XTEA more reliable. The proposed schemes could be used to protect the extremely sensitive and resource-constrained applications but at the cost of more area.

S. M. Subramanian, K. Mozaffari, R. Azarderakhsh, and M. Nojoumian [12] proposed a two underlying block ciphers such as Light Encryption Device (LED), and HIGHT for the authenticated encryption process. The error detection technique used for a light weight block ciphers encryption system includes variants of re-computing with Signature Based Scheme (SBS) and encoded operands to detect both transient and permanent faults. This proposed method achieved high efficiency while maintaining high error coverage. But, the transient and permanent faults were not properly detected hence system security was affected.

D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin [13] proposed an investigation over compression of information encrypted with block cipher chaining like Advanced Encryption Standard (AES). This block ciphers operating in different chaining modes were considered and it was showed how compression range could be achieved without compromising security of the encryption technique. But, the message blocks cannot be re-encrypted after the modification in this technique.

D. Talukdar, and L. P. Saikia [14] proposed Rivest Shamir Adleman (RSA) algorithm, a common public key based technique for encryption and decryption. The strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and mitigate the overheads of the system. The key length was directly proportional to security and inversely proportional to performance. Hence, hacking time was reduced, which represent that time available for the hackers has been reduced. The RSA algorithm was very slow for the systems where large amount of data was to be encrypted.

A. M. Abdullah, and R. H. H. Aziz [15] proposed an efficient technique for cryptography based on static LUT and dynamic key. The symmetric encryption and decryption was used in this algorithm. The proposed technique was much secure and simple to implement. This application utilizes built in android intents and SMS manager to send and receive messages. The dynamic keys must be identical between the senders and receivers. When the cryptography keys between sender and receivers are not even, communication breaks down because receivers were no longer capable to decrypt messages from senders.

The existing QTL [16] minimize the cost of energy consumption in hardware implementation of the cipher while maintaining security. The Dual Port Read Only Memory-Carry Select Adder based QTL method is introduced to reduce computation complexity and hardware usage for image encryption and decryption process [17]. A light weight cryptographic with a chaotic map based key generation scheme is proposed for efficient security purpose [18]. Compared to these methods the proposed ID-XT-EA-LFSR algorithm provides better security performances.

To overcome these problems, this paper introduces ID-XT-EA-LFSR algorithm, implemented using Xilinx tool. The ID-XT-EA-LFSR algorithm improves the performance of the cryptosystem.

3. ID-XT-EA-LFSR cryptosystem

In this section, a combination of the Extended Tiny and International Data encryption algorithm with efficient LFSR is introduced for strong security applications. In past decades, the performance evaluation of block ciphers using resource

constrained microcontroller has received much attention by researchers. Among those, the XTEA and IDEA are the most efficient cryptography algorithms for real time cryptographic applications. The general description of the XTEA and IDEA algorithms are briefly described in the following sections.

3.1 Extended tiny encryption algorithm

The XTEA is the most efficient cryptography algorithm, it is mostly utilized in real time cryptography applications. The XTEA has very small code size, which uses the simple operations in terms of addition, shift functions and XOR. Hence, this algorithm provides minimum power and l The traditional XTEA algorithm consists of two stages. The top stage requires two n-bit as an inputs that are stored in two registers- $register$ 1 and $egister$ 2 . At initial step, values of register 2 are applied left and right shift operations, which are then XORed. This result (R) is added to value in register 2. On the other side, delta and key values are added and then XORed with R. This result is added to contents of register 1. All the steps of the top stage are repeated in the bottom stages. The output is the encrypted value. Decryption is performed in using the same XTEA algorithm.

3.2 International data encryption algorithm

The IDEA is one of significant cryptographic algorithms, which is suitable for hardware implementation. The IDEA consists of three operations such as modulo addition & multiplication and XOR. The modulo addition sums up two inputs of n- bit length and mods output by $2n$. The modulo multiplication multiplies two inputs of n- bit length and the mods the output by $2n + 1$. An input value of zero is consider as $2n$.
Hence, the input length of modulo multiplication is $n + 1$ when the input value is 0. The encryption and decryption process of IDEA comprises eight rounds with similar design and the final output transformation. But, these two cryptographic algorithms have large key generation function, so they are not suitable to some key attacks and hence increase system complexity. To solve this problem, the hybrid cryptographic algorithm was introduced; the brief explanation of the algorithm is as follows.

3.3 ID-XT-EA-LFSR algorithm

Fig.1 depicts the block diagram of ID-XT-EA-LFSR algorithm. The fundamental design of the proposed algorithm employs five various algebraic operations: addition shift function, bitwise exclusive OR, addition modulo and multiplication modulo. To enhance the performance of encryption and decryption process, the main focus is on key generation using random numbers. The working principle of the ID-XT-EA-LFSR is briefly explained in the following sections.

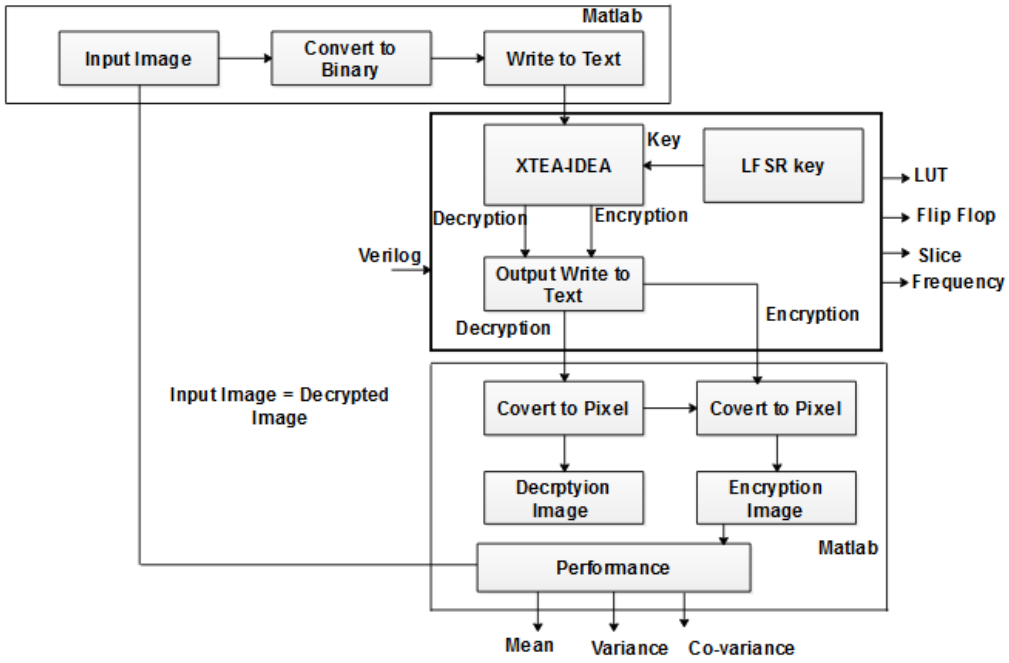


Figure.1 Block diagram of the ID-XT-EA-LFSR

The ID-XT-EA-LFSR algorithm consists of six steps. Initially, an input baboon image is read using MATLAB and converted into a binary format. In the second step, the binary value is converted to text format. This text format is input to Verilog. Both encryption and decryption process is performed in the Verilog. The algorithm requires a key for the encryption/decryption process. Hence, random numbers are generated using LFSR which is the key input to the Verilog in the fourth step. In the next step, the Verilog output is converted to text format for both the encryption and decryption process. The encryption and decryption text values are converted back to the pixels, and the pixel values are converted into an image in the final step. The decrypted image is similar to input image. Fig. 2 shows the architecture of the proposed hybrid cryptographic algorithm. In the proposed algorithm, features of IDEA and XTEA are combined to improve the performance of encryption and decryption process. The first half of the hybrid cryptosystem is designed using initial stage of the XTEA architecture and second half of the hybrid cryptosystem includes IDEA architecture based on modulo multiplication. The same algorithm is used for encryption and decryption. The text values of the test image are input to this cryptosystem which generates cipher text. The hybrid cryptosystem is one of the efficient algorithms to secure information as it provides improved security level performance compared to the existing cryptographic methods.

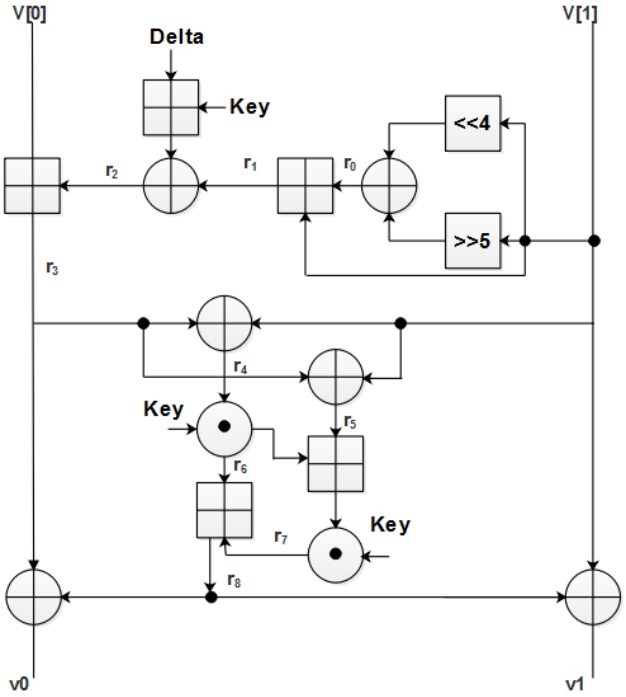


Figure.2 Architecture of the proposed algorithm

The proposed architecture is shown in Fig. 2. The data block of the 8-bits is divided into 2-cycles of 4-bit each, which are represented as $v[0]$ and $v[1]$. This network has cycles, which are represented as N. The permutation is the initial part and sub-key generation is the second part. The sum is the function, which is used to select sub key block based on the 0^{th} and 1^{st} bits. The XOR, addition, multiplication and shift operations are used for encryption and decryption process. Fig. 2 shows the flow of converting the plain text to the cipher text and vice versa. The bits of $v[1]$ are shifted left and right by 4 and 5 respectively. The outputs of shift operations are XORed with each other. The XORed value is added to $v[1]$. The result is r_1. The delta value of 8 is added with key. This result is XORed with r_1 to produce r_2. After this process, value in r_2 is added with $v[0]$ to produce r_3. The value of r_3 and initial value of $v[1]$ is XORed in second stage of the proposed cryptosystem architecture which gives r_5. The value in r_5 is XNORed with the key which generates r_6. The values r_5 and r_6 are added and the result is XNORed with key. This output is represented as r_7 which is then added with r_6 to produce the output r_8. This r_8 is XORed with r3 and $v[1]$ to produce two results V0 and V1 respectively. V0 and V1 are concatenated to produce the encrypted results. This encrypted value is given to the $v[0]$ and $v[1]$ to get the decrypted results.
The IDEA derives much of its security by interleaving operations from different sets: modular addition & multiplication, and XOR. It is reducing the circuit complexity and significantly improves the performance of the whole cryptography. In this research, the combination of the ID and XE encryption algorithm is much suitable for real time cryptography application due to its low computation complexity. Lightweight encryption with strong security is achieved using highly randomized LFSR based key generation. The Key Schedule process is described in the next section.

3.4 Key schedule

The LFSR generates random numbers which can be used as key in stream ciphers. It is well suited for ciphers with low and high speed requirements. Several techniques are implemented for key generation to improve the efficiency, security and performance of cryptographic algorithms, such as pairwise key distribution, matrix based key distribution, etc. The size of key is much significant in the energy constrained cryptosystems. A large key size ensures the randomness, but proportionally maximizes the network load with high complexity.

Table 1. Performance evaluation of the different Virtex devices for exiting and and ID-XT-EA-LFSR algorithm

Target FPGA Devices	Cryptography Algorithms	LUT	Flip Flop	Slice	Frequency (MHz)	Required time (sec)
Virtex6 xc6vcx75t	QTL [16]	47/46560	78/93120	34/11640	228.78	2.765
	DROM-CSLA-QTL [17]	55/46560	71/93120	31/11640	248.17	2.770
	XTEA [18]	388/46560	15/93120	103/11640	70.168	9.298
	ID-XT-EA-LFSR	37/46560	18/93120	16/11640	707.164	6.019
LP- Virtex6 xc6vlx75tl	QTL [16]	47/46560	78/46560	32/11640	188.04	3.428
	DROM-CSLA-QTL [17]	55/46560	55/46560	38/11640	204.165	3.434
	XTEA [18]	392/46560	15/93120	107/11640	73.99	9.836
	ID-XT-EA-LFSR	37/46560	18/93120	15/11640	738.007	7.155
Virtex 7 Xc7vx330t	QTL [16]	47/204000	55/408000	36/51000	271.894	2.352
	DROM-CSLA-QTL [17]	55/204000	55/408000	36/51000	293.608	2.357
	XTEA [18]	364/204000	15/408000	105/51000	81.746	0.915
	ID-XT-EA-LFSR	37/204000	18/408000	16/51000	823.588	2.145

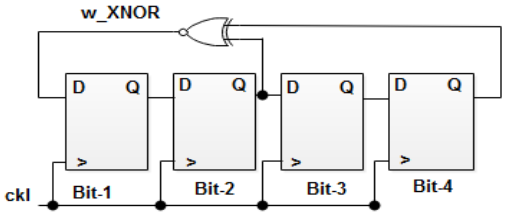


Figure.3 Block diagram of the linear feedback shift register

To overcome this problem, random numbers generated using LFSR are used as key in the proposed algorithm. The sub keys are generated from the original key in each round. Sub keys are applied to the 8-input blocks. The final step consists of an output transformer; it employs just four sub-keys. The ID-XT-EA-LFSR algorithm produces transformation output, which is 8-bit cipher text.

Block diagram of the LFSR is shown in the Fig. 3. The LFSR is implemented as a series of the flip flops inside of the FPGA platform. A number taps off of the shift register chain are utilized to either an XOR/XNOR gate. The output of this gate is employed as feedback to the beginning of the shift register chain, therefore the feedback in LFSR. When an LFSR is running, the pattern is generated by individual flip flop is pseudo random number. It's not completely random since form any state of LFSR pattern. The Verilog creates 4-bit LFSR key. It employs polynomials to make the maximum possible LFSR length for each and every bit width. The hybrid algorithm provides secure message transmission with less integrity by using LFSR. The original image is divided into blocks and the blocks are processed one by one in Verilog. Each block of image is encrypted using key generated by LFSR. At the receiver end same key is used to decrypt the image. Hence, the LFSR concept provides more security and effectiveness in encryption and decryption process.

4. Result and discussion

The ID-XT-EA-LFSR algorithm was implemented in the Xilinx tool by using Verilog code. Baboon image as input image has been considered here. Initially the image is converted into binary format in MATLAB, which is input to Verilog. The proposed ID-XT-EA-LFSR algorithm was implemented in FPGA platform. This platform is much suitable for VLSI implementations because of its flexibility, low power, and upward compatibility compared to the ASIC platform. Generally, the VLSI circuits for the bitwise algorithms require high performance and low latency under limited chip area and complexity. It is because the circuits commonly require to support high data rates of the communication networks. The FPGA performances for ID-XT-EA-LFSR algorithm are computed on Virtex6 xc6vcx75t, Low Power- Virtex-6 xc6vlx75tl, Virtex-7 Xc7vx330t, which are high configuration devices.

Performance evaluation of the different Virtex devices for existing and ID-XT-EA-LFSR algorithm is tabulated in Table 1. Results show that LP-Virtex-6 device has efficiently reduced the performance of the FPGA in terms of LUT, flip-flop and slice compared to Virtex-6 and Virtex-7. If the number of LUT, flip-flop and slices reduce then the area of ID-XT-EA-LFSR algorithm also reduces. The proposed ID-XT-EA-LFSR algorithm has improved the performance of FPGA on LP-Virtex-6 device by 21.27 % of LUT, 76.92% of flip-flop and 53.125% of slice compared to the QTL algorithm [16]. From the Table 1, it is clear that the number of LUT, flip-flop and slices are reduced and the operating frequency has increased compared to the existing algorithms such as QTL [16], DROM-CSLA-QTL [17], and XTEA [18]. The key management is an important task in a cryptosystem. The existing QTL [16] does

not consider the key scheduling scheme. A large key size ensures the randomness, but proportionally increases the load with complexity in QTL [16]. In DROM-CSLA-QTL [17], the hardware utilization is high compared to proposed ID-XT-EA-LFSR algorithm. But, it provides efficient security. The chaotic map based key is used for encryption and decryption process. It is not suitable for high data rate process [18]. So, in ID-XT-EA-LFSR algorithm, key generation portion of an algorithm must be designed carefully in order to ensure the security of the system. It consumes more computational levels for the strong key without any correlation with the next generated key value. Increase in the randomness of key is more important to ensure the strength of algorithm. The operating frequency of ID-XTEA-LSFR algorithm is 823.588 MHz for Virtex-7 device. If size of the key is increased, then the area complexity also increases exponentially. Here, the delay of encryption and decryption process is less since ID-XT-EA-LFSR algorithm has achieved high frequency. The time required for the ID-XT-EA-LFSR algorithm was analysed for three different types of the Virtex devices such as Virtex-6, low power Virtex-6 and Virtex-7. The cryptographic recovery time is less in Virtex-7 -1.94 seconds (on average) than other two devices. High configuration devices produce better performance than lower configuration devices.

Figs. 4, 5 and 6 show the comparative FPGA performance analysis for existing and ID-XT-EA-LFSR algorithms on three Virtex devices. The ID-XT-EA-LFSR is suitable for Virtex-6, LP-Virtex-6, and Virtex-7, which provides better performance compared to Virtex-4 and Virtex-5. Figs. 4, 5, and 6 clearly show that ID-XT-EA-LFSR has efficiently reduced the FPGA performance in terms of LUTs, flip flops and slices than QTL [16], DROM-CSLA-QTL [17], and XTEA [18]. Fig. 7 shows the output waveform of the ID-XT-EA-LFSR algorithm, taken from ModelSim. The light green line in Fig. 7 represents the LFSR key and the two yellow lines represent encryption and decryption output.

Figs. 8 (a), (b) and (c) represent the sample of proposed input, encryption and decryption image. The ID-XT-EA-LFSR algorithm is tested using the baboon image. Figs. 8 (a) and (b) show decrypted image is similar to the input image and the input image is not affected in the encryption process. The proposed ID-XT-EA-LFSR algorithm provides high encryption and decryption quality with minimum FPGA requirement and computational time.

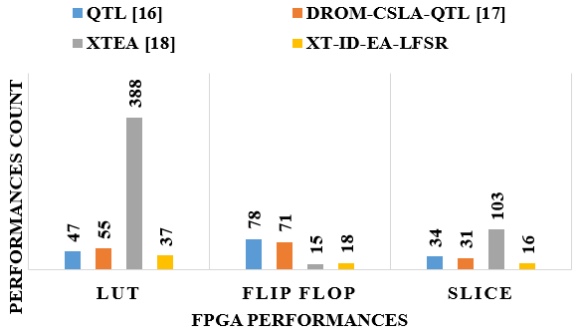


Figure.4 Comparative analysis of Virtex-6 FPGA performance for the existing and ID-XT-EA-LFSR algorithm

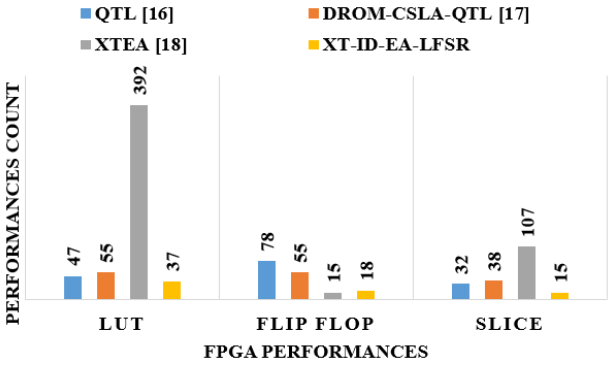


Figure.5 Comparative analysis of LP-Virtex-6 FPGA performance for the existing and ID-XT-EA-LFSR algorithm

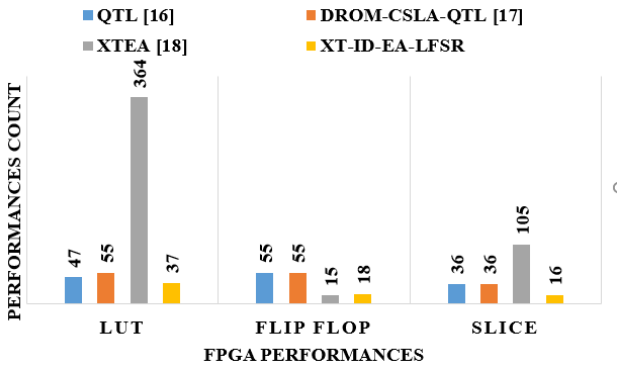


Figure.6 Comparative analysis of Virtex-7 FPGA performance for the existing and ID-XT-EA-LFSR algorithms

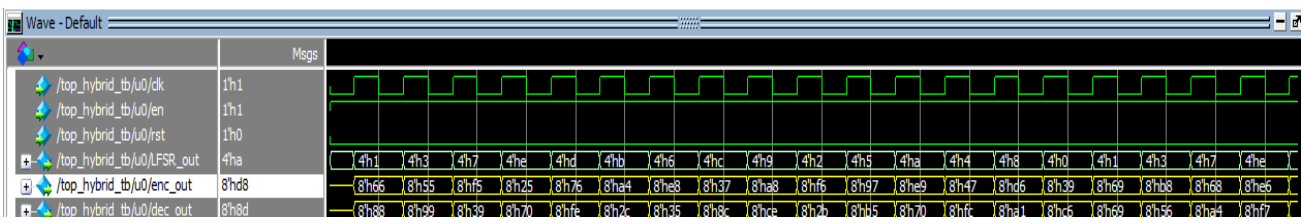
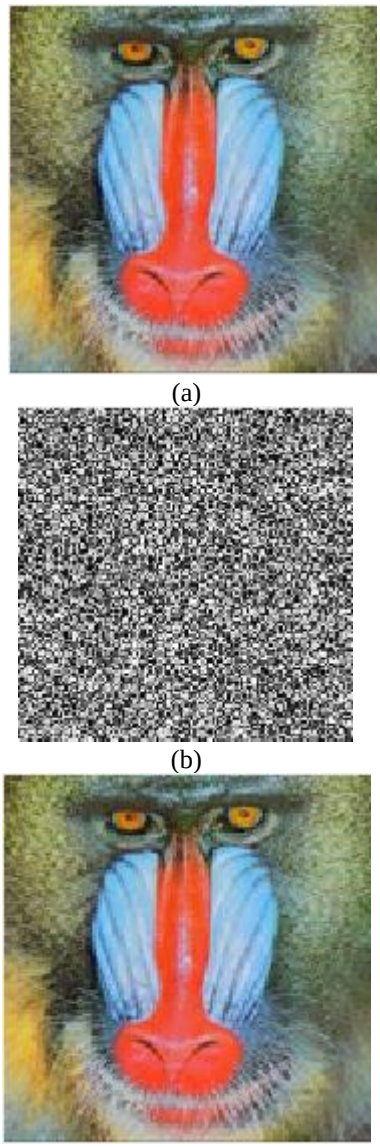


Figure.7 The output waveform of the ID-XT-EA-LFSR algorithm



(a) (b) (c)

Figure.8 Sample image: (a) input image, (b) encrypted image, and (c) decrypted image

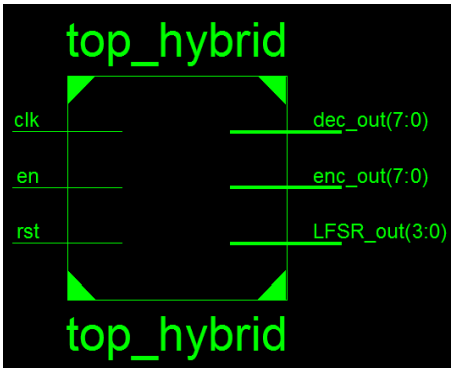


Figure.9 RTL view of the top module for a ID-XT-EA-LFSR algorithm

Fig. 9 depicts the RTL view of the top module for ID-XT-EA-LFSR algorithm taken from the Xilinx tool software by using Verilog. In this research, the ID-XT-EA-LFSR algorithm has separate code for each block such as encryption, decryption, and LFSR. In MATLAB, 128×128 size of the image is processed and the pixel is converted into binary. Each pixel size represents 8-bits and entire depth of the image is 16384 bits. Fig. 10 shows the internal block of the top module for the ID-XT-EA-LFSR algorithm. In the Fig. 10, all the internal blocks are connected by using red colour wire like the main module.

4.1 MATLAB performance

In the experimental simulation, ID-XT-EA-LFSR was implemented using MATLAB (Version 2018a) on Personal Computer (PC) with the 64-bit operating system. The mean, variance and co-variance are analysed for encrypted images, which show differences between input and encrypted image.

4.1.1. Mean

The mean is the average of the given FPGA performance. To compute the mean, add all FPGA performance in a group, and divide the sum by the total count of LUT, slice and flip flop. The mean value is computed using Eq. (1),

$$Mean(\mu) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

Here, μ is mean, n is number of terms and x_i is the value of each individual in the list of being averaged.

4.1.2. 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 groups by the number of values in the group. The variance is calculated by using Eq. (2),

$$\sigma^2 = \frac{\sum(X-\mu)^2}{N} \quad (2)$$

Here, σ^2 is variance, N is divided by the number of terms in distribution.

4.1.3. Covariance

Covariance computes how 2-variables are related. A positive covariance denotes as the variables are positively related, while a negative covariance denotes the variables are reciprocally related. Computing the covariance of sample data by using Eq. (3).

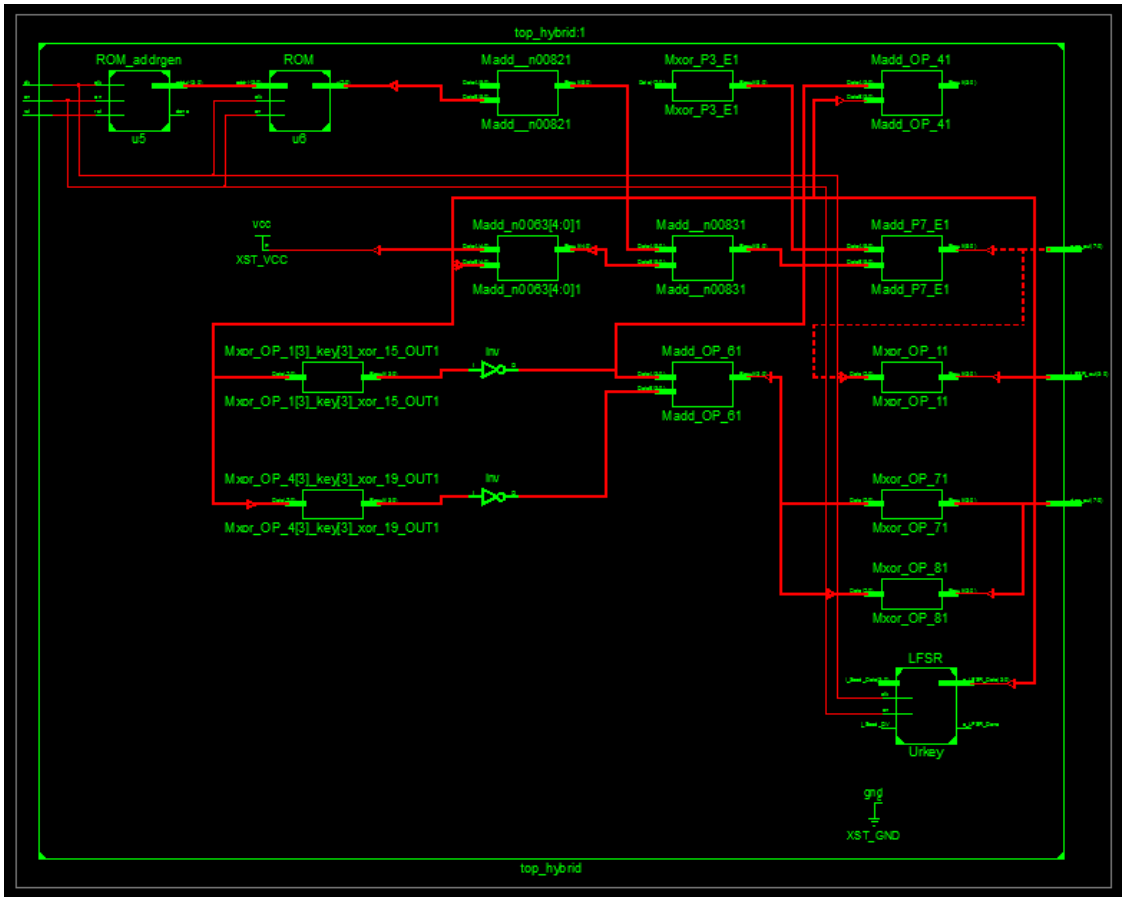


Figure.10 Internal block of the top module for the ID-XT-EA-LFSR algorithm

$$Cov(A,B) = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{n-1} \quad (3)$$

Here, X is independent variable, Y is dependent variable, n is number of data points in the samples, $\bar{X}$ is mean of the independent variable$X$, $\bar{Y}$ is mean of the independent variable Y.

Table 2 shows the MATLAB performance evaluation of encryption process for different images. The mean, variance and co-variance are computed for the encrypted image. In this research mean, variance and covariance are computed for three different kinds of images such as Lena, pepper and baboon image. Here, the mean value given the contribution of the individual pixel's intensity for the whole image. The variance also computed to detect how each and every pixel varies from the neighbouring pixels and it employed into various regions. The covariance is calculation of how much two random variables change together. Fig. 11 shows a histogram of the input baboon image. Histogram of the encrypted and decrypted image is presented in Figs. 12 and 13 respectively.

Table 2. MATLAB performance evaluation of encryption process for different images.

Image	Method	Mean	Variance	Co-variance
Lena	QTL [16]	139.6632	740320	436.337
	DROM-CSLA-QTL [17]	128.0326	557450	56.0538
	XTEA [18]	129.611	379850	77.87
	ID-XT-EA-LFSR	127.153	274550	47.779
pepper	QTL [16]	90.061	734980	1426
	DROM-CSLA-QTL [17]	90.061	734980	1426
	XTEA [18]	118.42	540160	294.83
	ID-XT-EA-LFSR	130.82	326270	65.32
Baboon	QTL [16]	132.4677	381380	132.26
	DROM-CSLA-QTL [17]	132.4677	381380	132.26
	XTEA [18]	127.870	234900	53.16
	ID-XT-EA-LFSR	127.7268	200260	45.6716

The decrypted image is similar to input image; which shows the effectiveness of proposed ID-XT-EA-LFSR algorithm. So, it clearly showed that encryption and decryption processes are not affected by any kind of noise. Hence, the information is safely transmitted to the receiver by using the ID-XT-EA-LFSR method. The ID-XT-EA-LFSR has improved the quality of the encryption process compared to the existing methods.

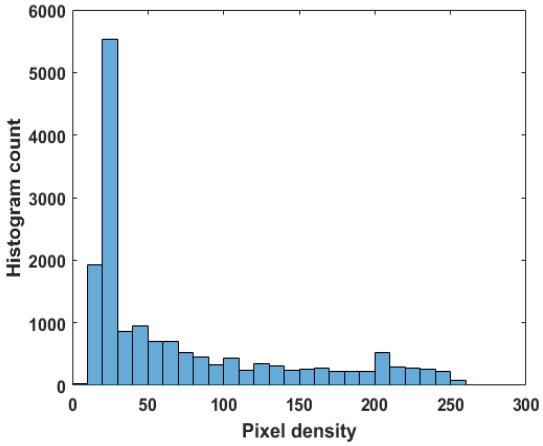


Figure.11 Histogram of the input image

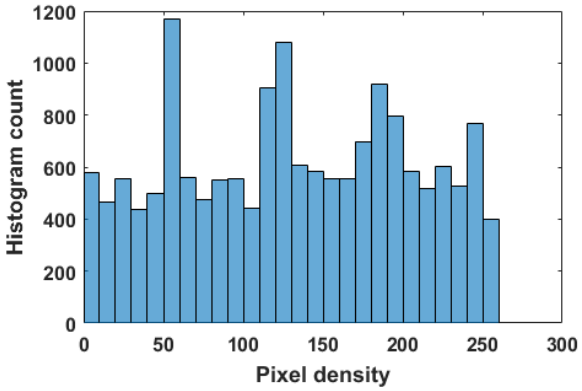


Figure.12 Histogram of encrypted image

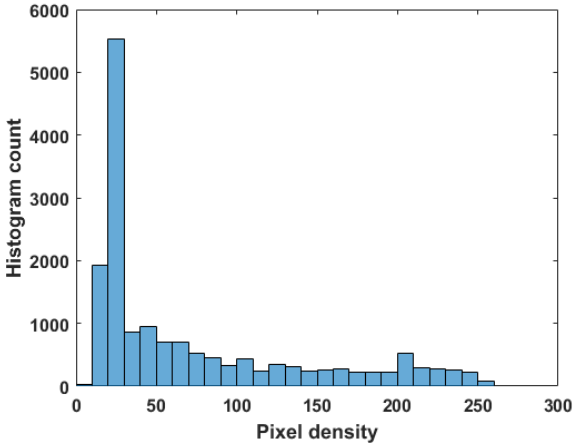


Figure.13 Histogram of decrypted image

5. Conclusion

Nowadays, the cryptography plays a significant role to convert digital data into the intelligible form. This paper presents a state of art investigation work in the area of popular information security approaches like cryptography. In this research, the image was converted into binary format by using MATLAB version 2018a. The binary value is given to Verilog as an input as it does not accept the image format. The ID-XT-EA-LFSR algorithm was implemented in the Xilinx tool by using Verilog code. The performance of the ID-XT-EA-LFSR algorithm was analysed in the FPGA platform over high configurable Virtex devices such as Virtex-6, LP-Virtex-6 and Virtex-7. The ID-XT-EA-LFSR has achieved strong security by employing highly randomized LFSR key generation. In LP-Virtex-6 performance, 21.27 % of the LUT, 76.92% of the flip-flop and 53.125% of the slice are obtained compared to the QTL algorithm. In future work, advanced encryption process with different technique for key generation can be used to improve the efficiency and performance.

References

[1] D. K. Sarmah and N. Bajpai, "Proposed System for data hiding using Cryptography and Steganography", *International Journal of Computer Applications*, Vol.8, No.1, pp. 7-10, 2010.

[2] A. Mehndiratta, "Data hiding system using cryptography & steganography: a comprehensive modern investigation", *International Research Journal of Engineering and Technology*, Vol.2, No.1, pp.397-403, 2015.

[3] P. Geetha, V. S. Jayanthi, and A. N. Jayanthi, "Optimal visual cryptographic scheme with multiple share creation for multimedia applications", *Computers & Security*, Vol.78, pp.301-320, 2018.

[4] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and Hybrid Encryption Techniques: A Survey", *Networking Communication and Data Knowledge Engineering*, pp.239-248, 2018.

[5] R. Tripathi, and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques", *International Journal of Advance Foundation and Research in Computer*, Vol.1, No.6, pp.68-76, 2014.

[6] W. Shan, X. Chen, B. Li, P. Cao, J. Li, G. Gao, and L. Shi, "Evaluation of Correlation Power Analysis Resistance and Its Application on Asymmetric Mask Protected Data Encryption

Standard Hardware", *IEEE Trans. Instrumentation and Measurement*, Vol.62, No.10, pp.2716-2724, 2013.
[7] P. Sarkar, "Tweakable enciphering schemes using only the encryption function of a block cipher", *Information Processing Letters*, Vol.111, No.19, pp.945-955, 2011.
[8] M. S. Mahindrakar, "Evaluation of blowfish algorithm based on avalanche effect", *International Journal of Innovations in Engineering and Technology*, Vol. 4, No.1, pp.99-103, 2014.
[9] A. Gupta, and N. K. Walia, Cryptography algorithms: A review", *International Journal of Engineering Development and Research*, Vol.2, No.2, 2014.
[10] S. V. Appaji and G. V. S. Acharyulu, "Recent Advancements on Symmetric Cryptography Techniques-A Comprehensive Case Study", *Global Journal of Computer Science and Technology*, Vol.14, No.2, 2014.
[11] M. Mozaffari-Kermani, K. Tian, R. Azarderakhsh, and S. Bayat-Sarmadi, "Fault-resilient lightweight cryptographic BCs for secure embedded systems", *IEEE Embedded Systems Letters*, Vol.6, No.4, pp.89-92, 2014.
[12] S. M. Subramanian, K. Mozaffari, R. Azarderakhsh, and M. Nojoumian, "Reliable hardware architectures for cryptographic block ciphers LED and HIGHT", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol.36, No.10, pp.1750-1758, 2017.
[13] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers", *IEEE Transactions on Information Theory*, Vol.58, No.11, pp. 6989-7001, 2012.
[14] D. Talukdar and L. P. Saikia, "Simulation and Analysis of Modified RSA Cryptographic Algorithm using Five Prime Numbers", *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol.5, No.6, pp.224-228, 2017.
[15] A. M. Abdullah and R. H. H. Aziz, "New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm", *Image*, Vol.143, No.4, 2016.
[16] B. Li, L. Liu, and H. Wang, "QTL: a new ultra-lightweight block cipher", *Microprocessors and Microsystems*, Vol.45, pp.45-55, 2016.
[17] A. Shailaja and G. N. Krishnamurthy, "Low area FPGA implementation of DROMCSLA-QTL architecture for cryptographic application", *International Journal of Network Security & Its Applications*, Vol.10, No.3, 2018.
[18] C. Baskar, C. Balasubramaniyan, and D. Manivannan, "Establishment of light weight cryptography for resource constraint environment using FPGA", *Procedia Computer Science*, Vol.78, pp.165-171, 2016.