qrAs per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 03, pages 121-128.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue03.html
DOI: https://doi.org/10.46501/IJMTST1003019

Security Enhancement of Information using Multilayered Cryptographic Algorithm

Shaik Subhani, Balijepalli Vinay Kumar, Koppuravuri Venkata Sukumar, Anamalaboina Koteswara Rao, Anumolu Bhanu Pratap Reddy

Department of Electronics and Communication Engineering, Chalapathi Institute of Technology, Guntur, India.

To Cite this Article
Shaik Subhani, Balijepalli Vinay Kumar, Koppuravuri Venkata Sukumar, Anamalaboina Koteswara Rao, Anumolu Bhanu Pratap Reddy,Security Enhancement of Information using Multilayered Cryptographic Algorithm, International Journal for Modern Trends in Science and Technology, 2024, 10(03), pages. 121-128.https://doi.org/10.46501/IJMTST1003019

Article Info
Received: 30 January 2024; Accepted: 22 February 2024; Published: 01 March 2024.

ABSTRACT

The main aim of advanced Cryptographic techniques is to provide data security which helps to avoid data hacking and illegal access of data. Providing data confidentiality and strong peer to peer authentication using the multilayer linear feedback shift register (LFSR) cryptographic technique to reduce the cost of encryption as well as storage and computation. One Time Pad algorithm developed in multilayer which defines the signal transmission in the medium is used to provide information security. For various levels of bit handling in data communication systems authentication keys are implemented in LFSR cascaded cryptography in both encryption and decryption process. For improved data security cascaded LFSR cryptography is analyzed. While processing an image, two stages of encryption and decryption done using multilayered cryptography which enhances the data security

Keywords:: LFSR; OTP Algorithm; Single-cascaded Cryptography; PN Sequence; Seed Values; primitive polynomial.

1. INTRODUCTION

In the data communication process, hacking has become a great threat, which leads to the loss of information during the transmission causing insecurity. This data hacking affects the user and confidentiality during the data handling process. Data security is achieved using various techniques in the data handling process. The most familiar method used to overcome this problem is cryptography. Cryptography is the process of encrypting the data with the help of the key which is generated by the transmitter [3,4]. The receiver wants to decrypt the data with the key to read the data. Key may be common to both transmitter and receiver. Symmetric cryptography is the cryptographic technique that uses the same key for both encryption and decryption. Key used for both encryption and decryption is the private key which should be secret for both transmitter and the receiver [7]. This symmetric cryptography includes various algorithms such as AES algorithm [12], DES algorithm [14], Triple DES algorithm [8], Blowfish algorithm [6, 15], etc., For AES algorithm block size will be 128 bit and the key length will be 256 bit, which is the longest key. For DES algorithm, block size will be 64 bit and the key length will be 56 bit, which is the smallest key. In the triple DES algorithm, the block size will be 64 bit and the key length will be 112 bit or 168 bit, which is a shorter key compared to the AES algorithm. Asymmetric cryptography [10,16] is the cryptographic technique which uses the different key for encryption and decryption. Key used for encryption is the public key and the key used for the decryption is the private key. Asymmetric cryptography includes RSA algorithm, HASH algorithm, Digital signature algorithm, etc. The modern cryptographic technique includes the development of the Linear Feedback Shift Register (LFSR) system [2]. This Linear Feedback Shift Register is used for the encryption and the decryption process. Key used for encryption and decryption will be Pseudo noise sequences generated by a feedback shift register and the combinational logic [5]. The Pseudo noise sequence [1] is generated at the output of the last flip flop in the shift register. There are many types of ciphers are available to generate the one-time pad (OTP) to provide a secure cryptosystem [10]. LFSR is used for generating the pseudo-random number generator which is used in stream ciphers especially in military cryptography due to its simple construction. LFSR is a linear system. To enhance the data security level, the multilayer technique is presented. Multilayer cryptographic technique [3, 9, 11] is the process of encrypting the already encrypted information one or more by using the same algorithm or using different algorithms.

2. LITERATURE REVIEW

Exploring the Potential of Threshold Logic for Cryptography-Related Operations by Alessandro Cilardo - Motivated by the emerging interest in new VLSI processes and technologies, such as Resonant Tunneling Diodes (RTDs), Single-Electron Tunneling (SET), Quantum Cellular Automata (QCA), and Tunneling Phase Logic (TPL), this paper explores the application of the non-Boolean computational paradigms enabled by such new technologies. In particular, we consider Threshold Logic functions, directly implementable as primitive gates in the above-mentioned technologies, and study their application to the domain of cryptographic computing. From a theoretical perspective, we present a study on the computational power of linear threshold functions related to modular reduction and multiplication, the central operations in many cryptosystems such as RSA and Elliptic Curve Cryptography. We establish an optimal bound to the delay of a threshold logic circuit implementing Montgomery modular reduction and multiplication. In particular, we show that fixed-modulus Montgomery reduction can be implemented as a polynomial-size depth-2 threshold circuit, while Montgomery multiplication can be implemented as a depth-3 circuit. We also propose an architecture for Montgomery modular reduction and multiplication, which ensures feasible O(n ^{2}) area requirements, preserving the properties of constant latency and a low architectural critical path independent of the input size n. We compare this result with existing polynomial-size solutions based on the Boolean computational model, showing that the presented approach has intrinsically better architectural delay and latency, both O (1).

FPGA based N-bit LFSR to generate random sequence number by Babitha P. K, Thushara T, Dechakka M. P. - Random number generators are most prominently used in the area of communication to provide security for information systems through pseudo random sequences. It also applicable for key generation in cryptography applications and signature analyzer to generate test patterns for Built-In-Self Test. In conventional method, random numbers are generated by a reference value i.e., seed value, using a XOR gate. The new proposed methods present a linear feedback shift register (LFSR) which generates an arbitrary number based on XOR, XNOR gates with and without seed value using multiplexer. Multiplexer is appended to generate a random value at user defined state in runtime. Hardware complexity and power consumption is reduced by replacing the multiplexer with tristate buffers. Result analysis indicates that proposed LFSR with and without seed value gives a better performance, low power consumption and improves more randomness in runtime with Partial Reconfiguration (PR). Resource utilization for standard XOR based LFSR is compared with proposed LFSR using XOR and XNOR logic. Proposedmethod is designed in Verilog HDL, simulated with ISE Simulator, synthesized and implemented using Xilinx ISE, targeted for Spartan3E XC3S500E-FG320-4 andVirtex-5XUPV5LX-110T architecture.

A multilayered Secure for Transmission of Sensitive Information based on Steganalysis by Divya Jenifer D' Souza, Minu P Abraham-We propose a multilayered secure scheme to transfer sensitive text over an unreliable network. The secret text is first encrypted using the AES algorithm. The cipher text produced is hidden in an audio file. The audio file is in turn encrypted in parallel using the concept of Shamir's technique based on CRT to maximize resource utilization. These, audio shares are sent over different channels in the network for security. Experimental results show that, even if certain shares got lost over network, audio files could be recovered at the receiver with the remaining shares without sender needing to resend the file.

An efficient chaos pseudo-random number generator applied to video encryption by HuiXua, Xiaojun Tonga, XianwenMenga - Traditional cipher systems are not appropriate for video encryption due to the high computation overhead. Video encryption must take account of the trade-off of both data security and real-time performance. In this paper, an efficient chaos pseudo-random number generator is designed to generate key stream for encrypting video syntax elements of H.264/AVC. In view of the efficiency and security, the intra-prediction mode (IPM), signs of trailing ones (T1s), signs of non-zero (NZ) coefficients, signs of motion vector difference (MVD) are chosen for selective encryption. The proposed scheme provides sufficient protection for the video commercial value. Experimental results demonstrate that the course of encryption will not affect the coding efficiency of H.264/AVC by keeping exactly the same bitrate and negligible time overhead. Security analysis shows that the proposed scheme has the ability to resist malicious attacks.

Computing Seeds for LFSR-Based Test Generation fromNontest Cubes by IrithPomeranz-In test data compression methods that are based on the use of a linear-feedback shift register (LFSR), a seed that produces a test for a target fault is computed based on a test cube for the fault. With a given LFSR, a seed may not exist for a given test cube, even though a seed may exist for a different test cube that detects the same fault. This issue is addressed in this brief by computing seeds for LFSR-based test generation without using test cubes. Instead, the procedure described in this brief is based on the use of non-test cubes. A non-test cube for a fault must be avoided in any test or test cube for the fault in order to allow the fault to be detected. Therefore, non-test cubes do not limit the ability of the procedure to compute seeds with a given LFSR. Experimental results demonstrate the advantages that the use of non-test cubes provides, and the associated computational cost.

3.MULTILAYEREDCRYPTOGRAPHIC ALGORITHM

Proposed LFSR Cryptography

In this LFSR OTP encryption and decryption algorithm is used. LFSR OTP encryption is shown in Figure 1.

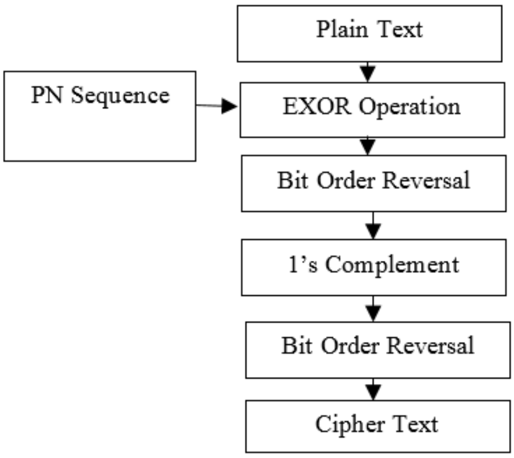


Figure 1: LFSR OTP encryption

The number of steps has been increased in both the encryption and the decryption process to attain the high security level of data. Here the OTP algorithm is presented in such a way that the process includes a Bit reversal process after the EXOR operation. The reversed sequence is performed with a 1's complement operation then once again the bit reversal operation is performed to get the Cipher text. This helps to improve security than a single layer. In the above proposed LFSR cryptography technique, multi-layers can be used to achieve higher security.

The LFSR OTP decryption is shown in Figure 2. Here the reverse process of the encryption process is performed to retrieve the original information. Then the sequence is made to experience the routine extraction process using the PN sequence. Without the knowledge of the OTP algorithm network hacking will be difficult on the information transmitted.

Multilayer or Cascaded Cryptography

Multilayer or cascaded cryptography is the process of encrypting an already encrypted data into two or more times either by using the same or different algorithms.

Block diagram for the proposed multilayer cryptography is explained in Figure 3

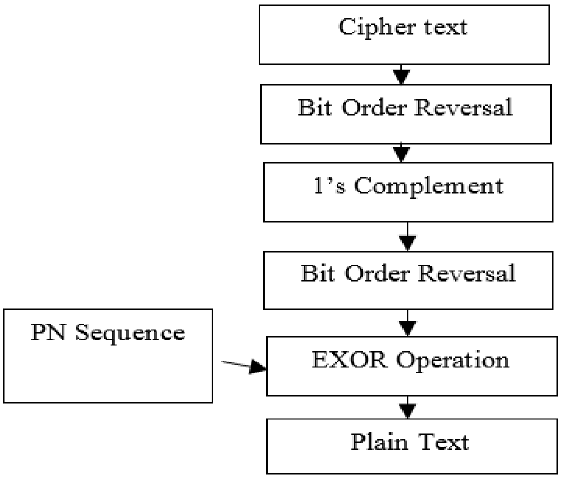


Figure 2: LFSR OTP decryption

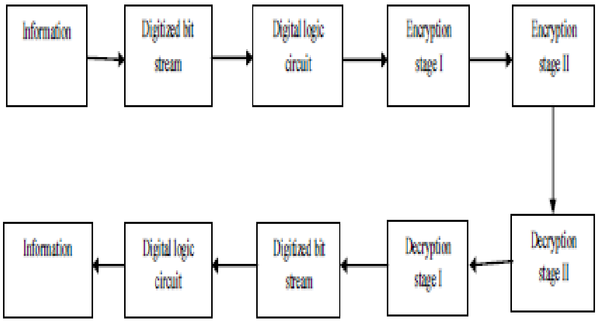


Figure 3: Block diagram of the cascaded crytography

In this block diagram, information is the input image. The input image is then converted into the digitized bit stream. This bit stream is taken for the encryption and decryption stages. The resultant bit stream is then converted into the original image which is the input. Conversion of the image into bit stream and bit stream into an image is done by using the MAT lab software. Simulink is used for linking the MAT lab and the model SIM software.

Conversion of Image into Bit Stream

Before doing the cryptography process, the input image is converted into the digitized bit stream. For converting the input image into the digitized bit stream the Input RGBimage is converted into the grayscale image. At the same time, the corresponding matrix format is also generated. A grayscale image is converted into a black and white image and the corresponding matrix is also generated and viewed. To attain the digitized bitstream, the encoding process is done. This digitized bit stream generated from image processing is very much important and used for the multilayer cryptography process. Multilayer LFSR OTP encryption and decryption algorithm is explained in the Figure 4 and Figure 5) respectively.

Multilayer LFSR OTP Encryption algorithm:

In this multilayer LFSR OTP encryption cipher text can be created by using the mathematical expression given as

$$\alpha = N\left[\{(\mu \oplus \gamma) >>> n\} >>> n\right]^{r} \quad ...(1)$$

Where, α = encrypted data,
N = number of layers,
>>> = circular right shift,
n = number of bits,
μ = PN sequence,
γ = input.

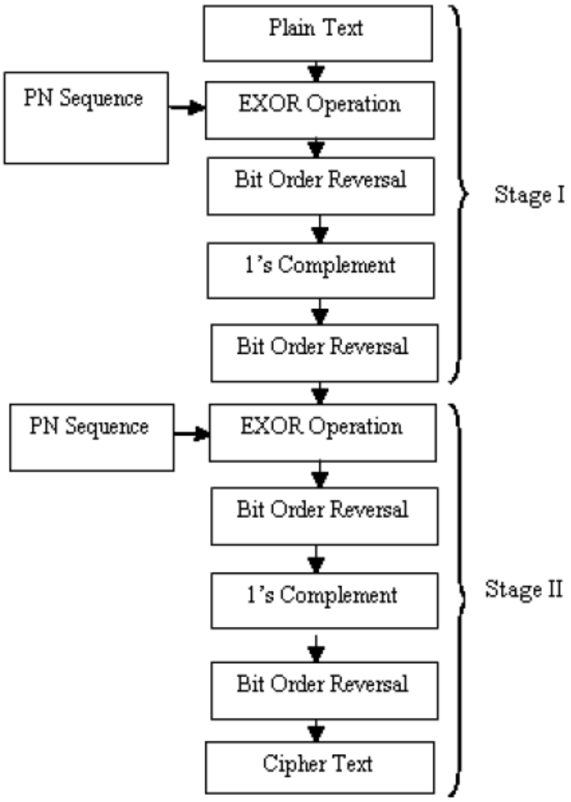


Figure 4: Two stages of LFSR OTP encryption

The equation provides the step-by-step process involved in the OTP algorithm. The first step, a plain text which is nothing but the PN sequence created in the LFSR operation is to be EXORed. The resultant value is taken and their bit order is reversed by using the circular shift register. Then, the obtained result is inverted by using the 1's complement logic. Again, the bit order is reversed for the result obtained in the previous step. The resultant value is the cipher text for the stage I encryption. The resultant cipher text is the EXOR ed with the PN sequence which is the random key.

The output obtained in the above step is taken and fed into the circular shift register to reverse their bit order. Perform 1's complement for the output obtained by using the inverter logic.

Multilayer LFSR OTP Decryption algorithm:

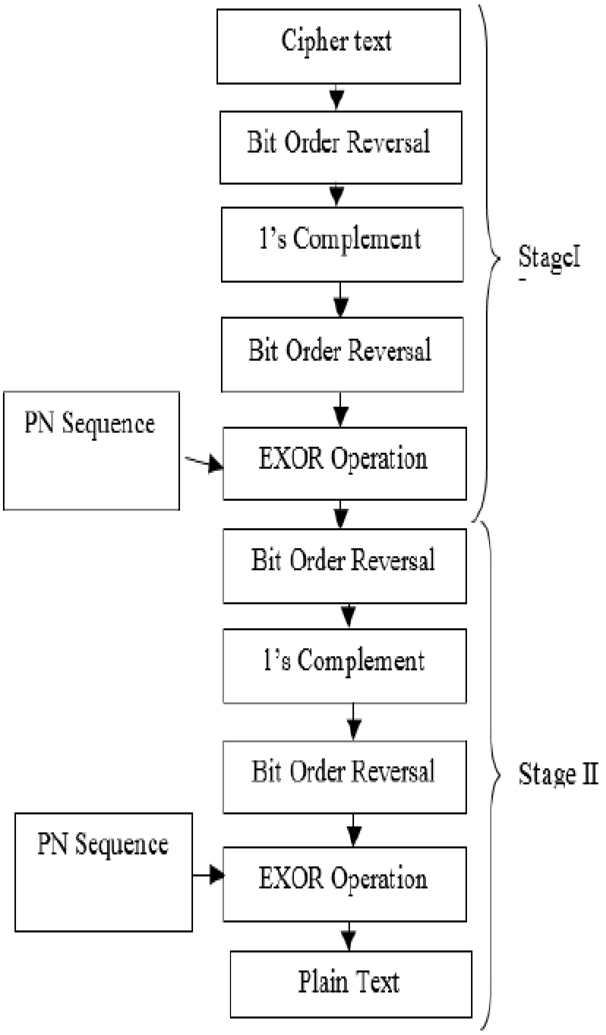


Figure 5: Two stages of LFSR OTP decryption

In this multilayer LFSR OTP decryption original plain text is retrieved by using the mathematical expression which is given in the equation (2).

$$\beta = N\left[\{(\alpha >>> n)^{r}\} \oplus \mu\right] \text{.......................}(2)$$

Where,

β = decrypted data,

α = encrypted data,

n = number of shifts,

N = number of layers,

μ = PN sequence,

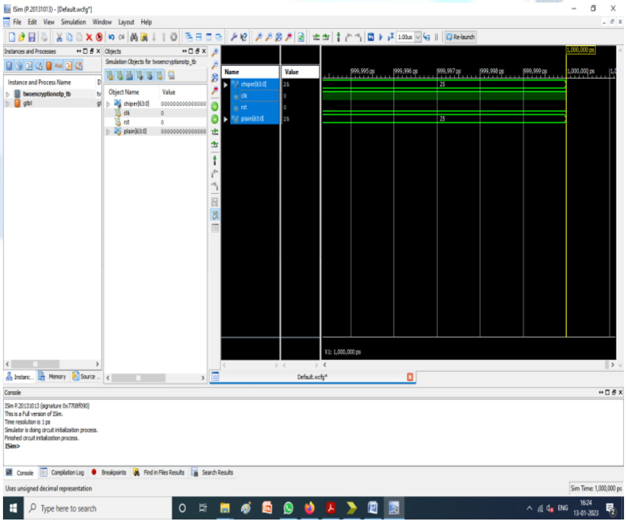
>>> = circular right shift

Equation (2) explains that the original plain text can be retrieved by using the following steps. In the first step, ciphertext which is nothing but the resultant value obtained in the multilayer LFSR OTP encryption algorithm is taken and fed into the circular shift register to reverse the bit order. The next step is to perform 1's complement for the resultant value obtained in the previous step. The resultant value is taken and fed into the circular shift register to reverse the bit order. Then, the final result is taken and EXORed with PN sequence which is nothing but the random key. The resultant value is the stage I decryption. This value in the decryption stage I is taken and fed into the circular shift register to reverse the bit order. Subsequently, this performs 1's complement for the resultant value obtained in the previous step. The output obtained in the above step is taken and fed into the circular shift register to reverse their bit order. Again the EXOR operation is performed between the resultant value obtained in the above step and the PN sequence which is nothing but the random key generated by the LFSR. The resultant value is the original plain text for the stage II decryption. After the cryptography process, the final digitized bitstream is taken into Matlab. To attain the original image corresponding binary image of the resultant digitized bitstream is processed.

.

4. RESULTS& DISCUSSION

Simulation results are integral to the success of VLSI design, helping designers ensure functionality, performance, power efficiency, reliability, and manufacturability of integrated circuits before they are physically fabricated.



Object Name	Value
chiper[63:0]	00000000000000
clk	0
rst	0
plain[63:0]	00000000000000

Name	Value
chiper[63:0]	25
clk	0
rst	0
plain[63:0]	25

```
ISim P.20131013 (signature 0x7708f090)
This is a Full version of ISim.
Time resolution is 1 ps
Simulator is doing circuit initialization process.
Finished circuit initialization process.
ISim>
```

Uses unsigned decimal representation

Figure 6: Simulation Result of the proposed system

Figure 6 shows the simulation result of two stage encryption otp. We give clk, rst and plain text input and we generate chipper text as output

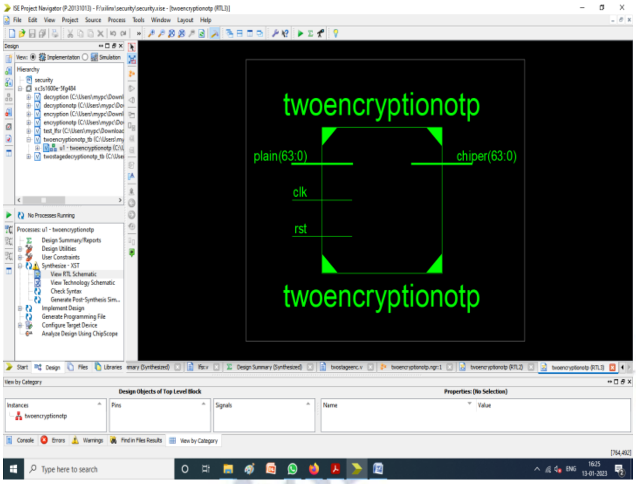


Figure 7: Block diagram of the proposed system

Figure 7 shows the Two-stage Encryption OTP block diagram consisting of clk, rst, plain text as input and chipper text as output

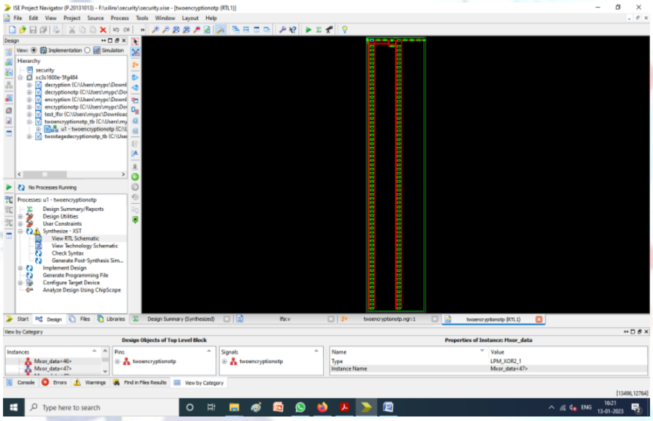
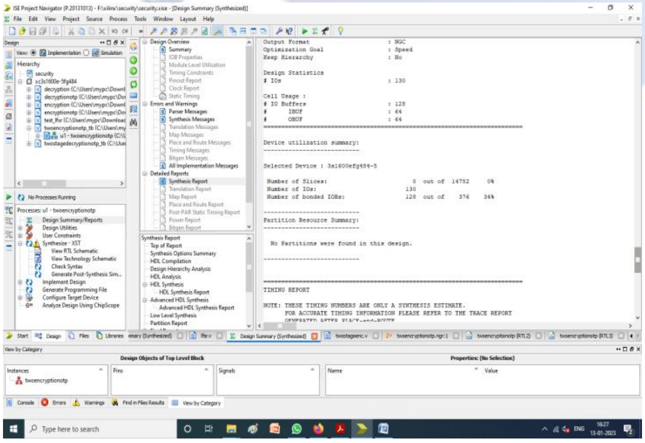


Figure 8: Block diagram of the proposed system

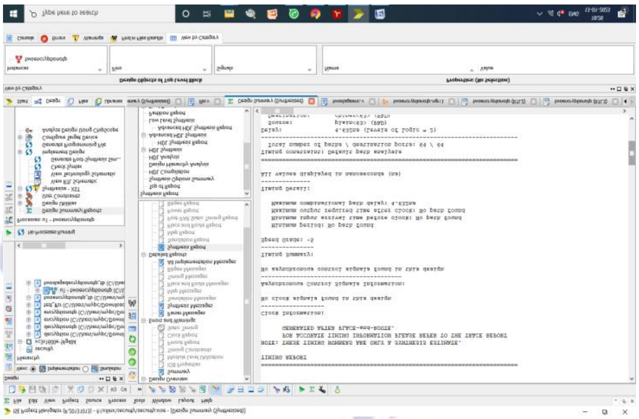
Figure 8 showsthe RTL schematic diagram of encryption which contains sub blocks as complement block, bit revisable block, LFSR and XOR logic block.



```
Output Format                      : NGC
Optimization Goal                  : Speed
Keep Hierarchy                     : No

Design Statistics
# IOs                              : 130

Cell Usage :
# IO Buffers                       : 128
#      IBUF                        : 64
#      OBUF                        : 64
=========================================================================

Device utilization summary:
---------------------------

Selected Device : 3s1600efg484-5

 Number of Slices:                       0  out of  14752     0%
 Number of IOs:                        130
 Number of bonded IOBs:                128  out of    376    34%

---------------------------
Partition Resource Summary:
---------------------------

  No Partitions were found in this design.

---------------------------


=========================================================================
TIMING REPORT

NOTE: THESE TIMING NUMBERS ARE ONLY A SYNTHESIS ESTIMATE.
      FOR ACCURATE TIMING INFORMATION PLEASE REFER TO THE TRACE REPORT
      GENERATED AFTER PLACE-and-ROUTE.
```

Figure 9: Device utilization of the proposed system

Figure 9 shows the area report of proposed system which contain the total number of LUT required for implementation



```
TIMING REPORT

NOTE: THESE TIMING NUMBERS ARE ONLY A SYNTHESIS ESTIMATE.
      FOR ACCURATE TIMING INFORMATION PLEASE REFER TO THE TRACE REPORT
      GENERATED AFTER PLACE-and-ROUTE.

Clock Information:
------------------
No clock signals found in this design

Asynchronous Control Signals Information:
----------------------------------------
No asynchronous control signals found in this design

Timing Summary:
---------------
Speed Grade: -5

   Minimum period: No path found
   Minimum input arrival time before clock: No path found
   Maximum output required time after clock: No path found
   Maximum combinational path delay: 4.632ns

Timing Details:
---------------
All values displayed in nanoseconds (ns)

=========================================================================
Timing constraint: Default path analysis
  Total number of paths / destination ports: 64 / 64
-------------------------------------------------------------------------
Delay:               4.632ns (Levels of Logic = 2)
  Source:            plain<63> (PAD)
  Destination:       chiper<63> (PAD)
```

Figure 10: Delay report of the proposed system

Figure 10 shows the delay report of circuit which show the overall delay of circuit.

4.CONCLUSIONS

The first layer and second layer of cryptography are completed with the help of the LFSR cryptographic technique. The cipher text for the LFSR cryptography is generated. Here both the encryption and the decryption process are done by the OTP algorithm. Due to this security of the data has been enhanced and the various cryptographic techniques have been summarized. The work focused on the design of effective single-layered cryptography as well as multilayer cryptography by using the LFSR cryptographic technique. Various levels of the bit handling process in the data communication system are implemented successfully through this LFSR cryptographic technique by generating the authentication key. The concept of image processing is also implemented successfully in the Matlab software. The multilayered cryptography is compared with the single-layer cryptography to prove that the multilayered cryptography is better enough to enhance the data security level during the data transmission.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Alessandro Cilardo "Exploring the Potential of Threshold Logic for Cryptography-Related Operations" In IEEE Transactions On Computers, Vol. 60, No. 4, (April 2011).

[2] Babitha P. K, Thushara T, Dechakka M. P. "FPGA based N-bit LFSR to generate random sequence number" in International Journal of

Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015, ISSN 2091-2730.

[3]Divya Jenifer D' Souza, Minu P Abraham "A multilayered Secure for Transmission of Sensitive Information based on Steganalysis" in ELSEIVER, Procedia computer science 78 (2016).

[4]HuiXua, Xiaojun Tonga, XianwenMenga, "An efficient chaos pseudo-random number generator applied to video encryption" in ELSEIVER, OPTIK 127 (2016).

[5]IrithPomeranz "Computing Seeds for LFSR-Based Test Generation FromNontest Cubes" in IEEE transactions on very large-scale integration (vlsi) systems, vol. 24, no. 6, june 2016.

[6]Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[7]Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014 ISSN 2278-6856.

[8]NouraAleisa "Comparison of the 3DES and AES Encryption Standards" in International Journal of Security and Its Applications Vol.9, No.7 (2015), ISSN: 1738-9976

[9]PushpLata, V. Anitha, "Multi-Layered Cryptographic Processor for Network Security" in International Journal of Scientific and Research Publications, Volume 2, Issue 10, October 2012 1 ISSN 2250-3153.

[10] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" in International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[11] Sahil Agarwal, Barkha Khattar , Dr. Inder Singh, "multi-layered security for private Communication (using steganography and cryptography)" in International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.4, Special Issue (01), March 2015 ISSN-2319-8354(E).

[12] ShraddhaSoni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012 ISSN:2277-3754.

[13] Sugitha,G A.Albert raj, A "CNLRA : Critical node and Link reconnect algorithm for wireless adhoc networks using graph theory" Asian Journal of Research in Social Science and Humanities Vol 6,no 8 , 2016,pp 1953-1963.

[14] Yashwantkumar, Rajatjoshi, Tameshwarmandavi, Simranbharti, Miss Roshni Rathour "Enhancing the Security of Data Using DES Algorithm along with Substitution Technique" in International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016.

[15] Maria Jessi, A,Albert Raj " A newfangled method to maintain Infrastructure and Mobility of Nodes by weigh based Clustering and Distributed Scheduling , International Journal of Printing & Packaging Allied Science,Vol 5, no 1 , 2017,pp 24-33 ISSN 2320-4287.

[16] Bommi,A,Albert Raj "A Low-Cost Image De-Noising Implementation Using Low Area CSLA for Impulse Noise Removal" Journal of Circuits, Systems, and Computers Vol 27 no 4 2018,pp 1850060-1-20.

[17] Ravikiran, D. N., & Dethe, C. G. (2018). Improvements in Routing Algorithms to Enhance Lifetime of Wireless Sensor Networks. International Journal of Computer Networks & Communications (IJCNC), 10(2), 23-32.

[18] Ravikiran, D. N., & Dethe, C. G. Fuzzy Rule Selection using LEACH Algorithm to Enhance Life Time in Wireless Sensor Networks. Advances in Wireless and Mobile Communications. ISSN, 0973-6972.

[19] Rajesh, G., Thommandru, R., & Subhani, S. M. DESIGN AND IMPLEMENTATION OF 16-BIT HIGH SPEED CARRY SELECT PARALLEL PREFIX ADDER.

[20] Polanki, K., Purimetla, N. R., Roja, D., Thommandru, R., & Javvadi, S. Predictions of Tesla Stock Price based on Machine Learning Model.

[21] Thommandru, R. A PROSPECTIVE FORECAST OF BRAIN STROKE USING MACHINE LEARNING TECHNIQUES.

[22] Rajesh, G., Raja, A., & Thommandru, R. OPTIMIZATION OF MINIATURIZED MICROSTRIP PATCH ANTENNAS WITH GA.

[23] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[24] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.

[25] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., & Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers. In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409). IEEE.

[26] Priya, S. S., Vellela, S. S., Reddy, V., Javvadi, S., Sk, K. B., & Roja, D. (2023, June). Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[27] Vellela, S. S., & Balamanigandan, R. An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Netw. Appl.(2023).

[28] Addepalli, T., Babu, K. J., Beno, A., Potti, B. M. K., Sundari, D. T., & Devana, V. K. R. (2022). Characteristic mode analysis of two port semi-circular arc-shaped multiple-input-multiple-output antenna with high isolation for 5G sub-6 GHz and wireless local area network applications. International Journal of Communication Systems, 35(14), e5257.

[29] Srija, V., & Krishna, P. B. M. (2015). Implementation of agricultural automation system using web & gsm technologies. International Journal of Research in Engineering and Technology, 04 (09), 385-389.

[30] Potti, D. B., MV, D. S., & Kodati, D. S. P. (2015). Hybrid genetic optimization to mitigate starvation in wireless mesh networks. Hybrid Genetic Optimization to Mitigate Starvation in Wireless Mesh Networks, Indian Journal of Science and Technology, 8(23).

[31] Potti, B., Subramanyam, M. V., & Prasad, K. S. (2013). A packet priority approach to mitigate starvation in wireless mesh network with multimedia traffic. International Journal of Computer Applications, 62(14).

[32] Potti, B., Subramanyam, M. V., & Satya Prasad, K. (2016). Adopting Multi-radio Channel Approach in TCP Congestion Control Mechanisms to Mitigate Starvation in Wireless Mesh Networks. In Information Science and Applications (ICISA) 2016 (pp. 85-95). Springer Singapore.

[33] S Phani Praveen, Sai Srinivas Vellela, Dr. R. Balamanigandan, "SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication", Journal of Next Generation Technology (ISSN: 2583-021X), 4(1), pp.25-36 . Jan 2024