IMPROVING THE SAFETY OF DATA WITH A MULTILAYERED ENCRYPTION AND DECRYPTION ALGORITHM

D.SAMPATH, ASSOCIATE PROFESSOR, HOD OF ECE, TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY KARIMNAGAR

Abstract: In order to address the issue of data hacking, this research proposes a multilayer linear feedback shift register (LFSR) secure mechanism for improving data security. The One Time Pad (OTP) algorithm, which is created in multilayer and specifies the signal transmission in the medium, is used to establish the safety of data. The seed values needed to describe OTP performance are obtained from the Pseudorandom Noise (PN) sequence produced by the basic polynomial. For an example of the security of digital data, the single-layered LFSR cryptography is examined using a cascaded LFSR security approach. In both the encryption and decryption processes, LFSR cascaded cryptography implements the circuits for generating authentication credentials for different bit handling levels in information transfer systems. The study of cascaded multilayer cryptography for enhanced security of data reveals which is performs efficiently for creating contemporary network-based services using operation frequency, power consumption, latency and memory utilization. It utilized Xilinx 14.5 and Verilog VHDL to implement this approach.

Key words: primitive polynomial, PN sequence, single-cascaded cryptography, LFSR, OTP algorithm and seed values.

INTRODUCTION

Hacking is emerged as a serious risk to data communication as it can result in information loss during transmission, which compromises security. During the data processing procedure, the user and confidentiality are impacted by this data attack. When processing data, a variety of strategies are used to ensure data security. The approach most frequently employed to solve this issue is cryptography. Applying an encryption key which is created by the sender to encrypt data is known as cryptography [3, 4]. To read the data, the recipient needs to use the key to decrypt it. Both the sender and the recipient can utilize a key. Employing the same key for both encryption and decryption is known as symmetric cryptography. The private key, which is used for both encryption and decryption, should be kept secret for both the sender and the recipient [7]. Numerous algorithms, including the AES algorithm [12], DES algorithm [14], Triple DES algorithm [8], Blowfish algorithm [6, 15] and others, are included in this symmetric cryptography. Block sizes for the AES method will be 128 bits and the longest key, 256 bits, will be used. The smallest key for the DES algorithm is 56 bits in length, while the block size is 64 bits. The triple DES algorithm uses a shorter key than the AES method, with a block size of 64 bits and a key length of 112 or 168 bits. Asymmetric cryptography [10,16] is a type of cryptography where the encryption and decryption processes employ distinct keys. The private key is used to decode data, whereas the public key is used to encrypt it. The RSA, HASH and digital signature algorithms are examples of asymmetric cryptography.

The Linear Feedback Shift Register (LFSR) mechanism emerged as part of the contemporary cryptography technique [2]. Both the encryption and decryption processes make use of this linear feedback shift register. A feedback shift register and the combinational logic will produce pseudo noise sequences, which will be the key utilized for encryption and decryption [5]. The output of the final flip flop in the shift register produces the pseudo noise sequence [1]. To create the one-time pad (OTP) and offer a safe cryptosystem, a variety of cipher types are available [10]. Because of its straightforward design, LFSR is employed to generate the pseudo-random number generator which is utilized in stream ciphers, particularly in military cryptography. The LFSR system is linear.

The multilayer approach is offered to raise the degree of data protection. The practice of encrypting previously encrypted data one or more times using the same method or other algorithms is known as multilayer cryptography [3, 9, 11].

ISSN: 2278-4632
Vol-15, Issue-06, No.01, June: 2025

Cryptography in a single layer

The technique of encrypting and decrypting data to increase its level of security is known as cryptography. The ciphertext is created by transforming the plain text during the encryption process. Transforming the ciphertext into plain text completes the decryption process. Figure 1 explains the encryption and decryption procedures.

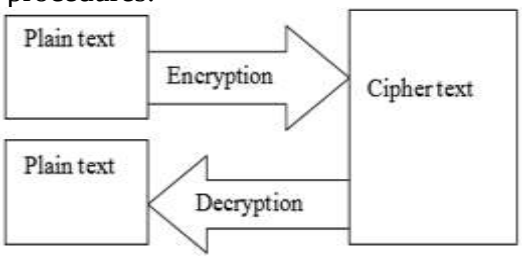

Figure 1: The fundamentals of cryptography

Numerous methods can be used to carry out this cryptography; the LFSR cryptographic approach is used below.

A. Contemporary LFSR Cryptography

Figure 2 depicts LFSR cryptography, in which the EXOR operation is the single method used for both encryption and decryption [4,5,13]. EXOR is performed between the ciphertext and the random key for the procedure for decryption and between the plain text and the random key for the procedure of encryption.

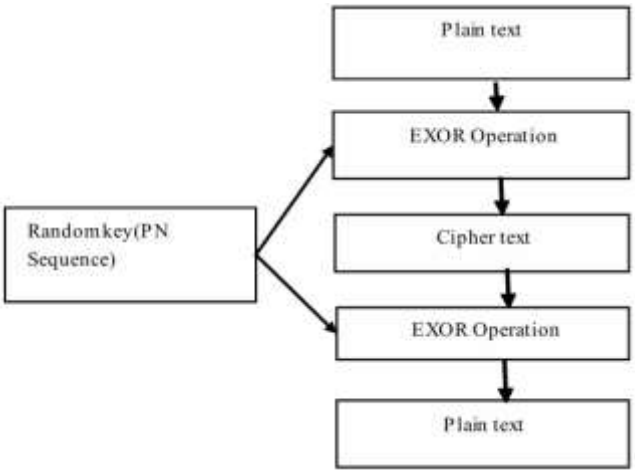

Figure 2: Practical cryptography for LFSR.

The following drawbacks apply to the pseudorandom number generator:

- The remaining bits in the key sequence can be easily created to hack the data when only a small portion of the plain text and its associated ciphertext are known.
- It results in a decrease in security.

PROPOSED LFSR CRYPTOGRAPHY

The LFSR technique uses an OTP encryption and decryption system. When LFSR OTP encryption, Figure 3(a) is presented.

ISSN: 2278-4632
Vol-15, Issue-06, No.01, June: 2025

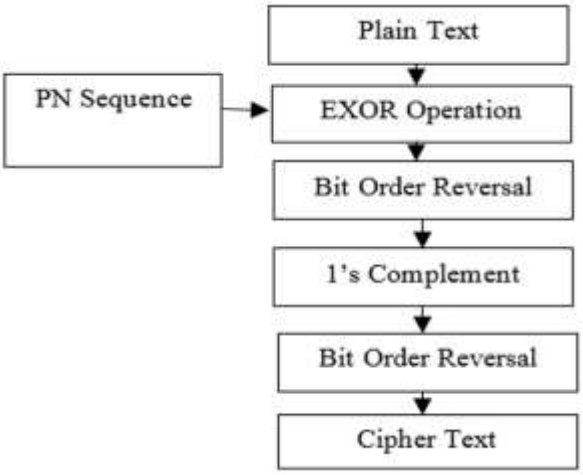

Figure 3(a): encryption using LFSR OTP

In order to ensure a high degree of data security, both the encryption and decryption processes now include more steps respectively. Here, the OTP algorithm is written so that, following the EXOR operation, a bit reversal procedure is included. The ciphertext is obtained by performing the bit reversal operation once again once the reversed sequence has been completed using a 1's complement operation. This enhances security over a single layer. For greater security, the LFSR cryptography approach mentioned above can use many layers.

Figure 3(b) depicts the decryption of the LFSR OTP. For the purpose of recovering the original data, the encryption procedure is carried out in reverse here. Next, the PN sequence is used to expose the sequence to the standard extraction procedure. Without understanding the OTP algorithm, it will be challenging to breach a network and access the data being sent.

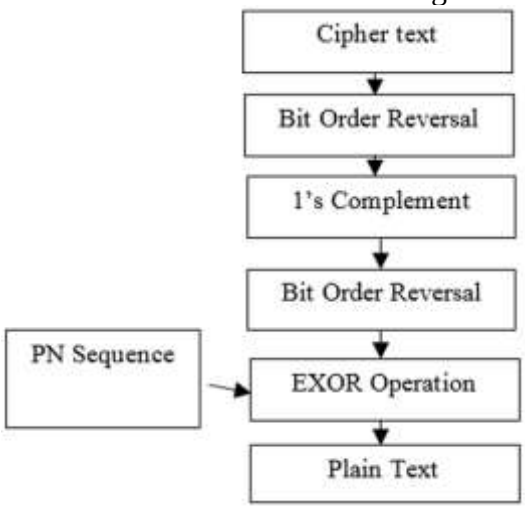

Figure 3(b): Decryption of LFSR OTP

A. Cascaded or Multilayer Cryptography

The technique of encrypting previously encrypted data twice or more, using either the same or other methods, is known as multilayer or cascaded encryption. Figure 4 provides an explanation of the block diagram for the proposed multilayer cryptography.

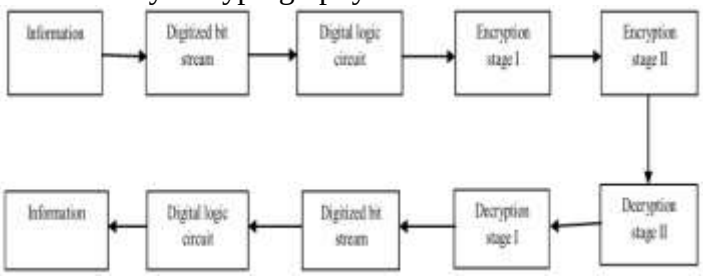

Figure 4: Block diagram

The input image in this block diagram is information. After that, the input image is transformed into the digital bitstream. For the encryption and decryption phases, this bitstream is used. The original input picture is then created from the resulting bitstream. Using the Matlab program, the picture is converted to bitstream and the bitstream is converted to an image. Matlab and the SIM model software are linked via Simulink.

B. Image to Bit Stream Conversion

The input image is transformed into a digital bitstream before to the cryptography procedure. The RGB input image is transformed into a grayscale image in order to convert it into the digital bitstream. Additionally, the matching matrix format is created simultaneously. In addition to converting a grayscale image to a black and white image, the matching matrix is created and shown. The encoding procedure is completed in order to get the digital bitstream. This digital bit stream, which is produced during picture processing, is crucial to the multilayer cryptography procedure. Figures 5(a) and 5(b) provide explanations of the multilayer LFSR OTP encryption and decryption algorithms, respectively.

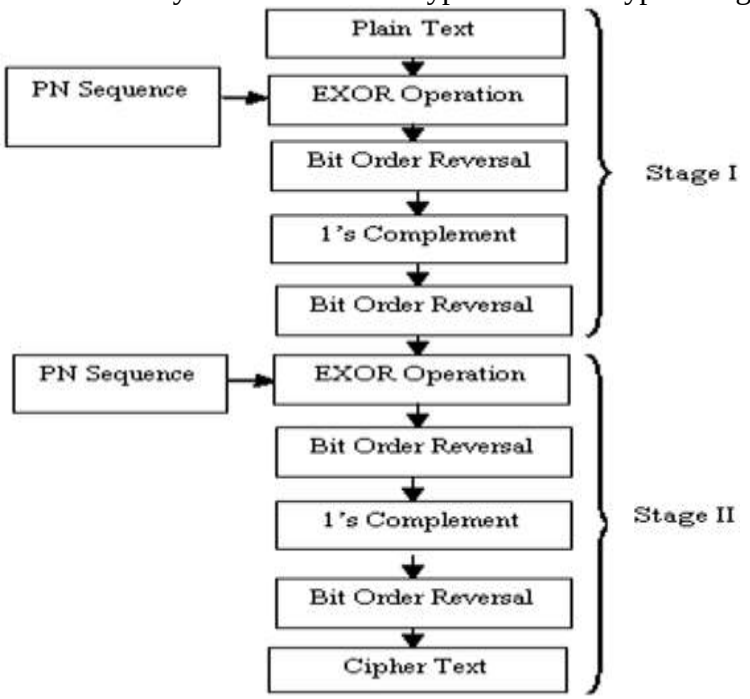

Figure 5(a): LFSR OTP encryption in two stages.

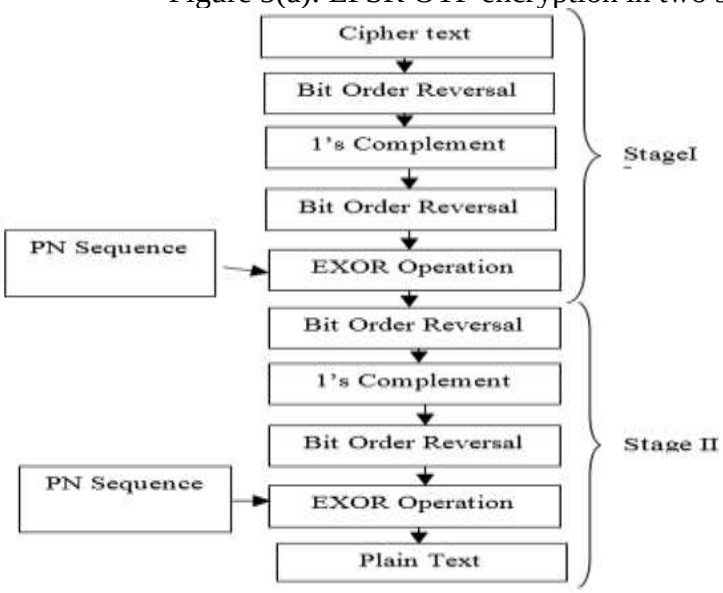

Figure 5(b): LFSR OTP decryption in two stages.

C. Algorithm for multilayer LFSR OTP encryption:

This multilayer LFSR OTP encryption ciphertext can be generated using the following mathematical formula:

$$\propto = N[\{(\mu \oplus \gamma) >>> n\} >>> n]^r \ldots . (1)$$

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

The OTP approach sequential steps are provided by the formula. In the first stage, the PN sequence produced by the LFSR operation must be EXORed with plain text. The circular shift register is used to reverse their bit order and take the resultant value. Then, employing the logic of 1's complement, the resultant result is reversed. Once more, the bit order is inverted for the outcome of the preceding step. The stage I encryption's ciphertext is the output value. The resultant ciphertext is the random key, which is the PN sequence EXORed with it. The circular shift register is fed the output from the previous stage in order to reverse its bit order. Calculate the output received by applying the inverter logic's 1's complement. The mathematical term which is displayed in formula (2) is used in this multilayer LFSR OTP decryption to extract the original plain text.

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

Where β = decrypted data,
α = encrypted data,
n = number of shifts,
N = number of layers,
μ = PN sequence,
>>> = circular right shift

According to formula (2), the following procedures can be used to get the original plain text. To change the bit order in the first stage, the circular shift register receives the ciphertext, which is just the value which became available via the multilayer LFSR OTP encryption process. The next step is to take the value which is acquired in the previous step and execute 1's complement. It reverses the bit order by taking the resulting value and feeding it into the circular shift register. After that, the final result is extracted and EXORed with the random key or PN sequence. The stage I decryption is the value which is produced. In order to flip the bit order, this value is extracted at the first step of decryption and supplied into the circular shift register. The value that was acquired in the previous phase is then subjected to 1's complement. The circular shift register is fed the output from the previous stage in order to reverse its bit order. The resulting value from the previous step and the PN sequence which is simply the random key produced by the LFSR are once more subjected to the EXOR operation. The resultant value for the stage II decryption is the original plain text. Following encryption, Matlab is used to import the resulting digital bitstream. Processing is done on the resulting digitized bitstream to obtain the matching binary image of the original image.

SIMULATION RESULTS

The image-based data must be processed in order to use encryption to secure the content. Here, the obtained image data is subjected to a multi-stage LFSR cryptography algorithm. The information obtained from the typical RGB input picture is referred to as the processing message, input information, or plain text. The Matlab comment is used to start the basic image analysis process and get the picture from the saved location. Below is a discussion of the outcomes of the corresponding simulation using the RGB input image for necessary analysis.

Figure 6(a) depicts the input RGB image, which is 128 x128 in size. Either a regular or watermarked image can be used as the input image. This input image is then transformed into a grayscale image with a resolution of 128 x128 pixels. The input for the multilayer LFSR algorithm must be binary-valued. The threshold value should thus translate the pixel intensity into binary

numbers. Any numbers which are over the cutoff are changed to 1, and any values that are below it are changed to 0. In figure 6(b), the binary image is shown. The length of the digitized bitstream can be increased to the value which results from multiplying 128 x 128 for an image size of 128 x 128. The picture must be compressed in order to lower complexity. Depending on our ease in simplifying, the compressed picture can be 8 x 8, 16 x 16, 4 x 4, or 2 x 2. Next, the reshape command is used to transform the matching matrix for the 2x2 binary picture into the digital bitstream. Figure 7 depicts the final result.

(a) (b)

Figure 6: (a) Input RGB image (b) Binary image

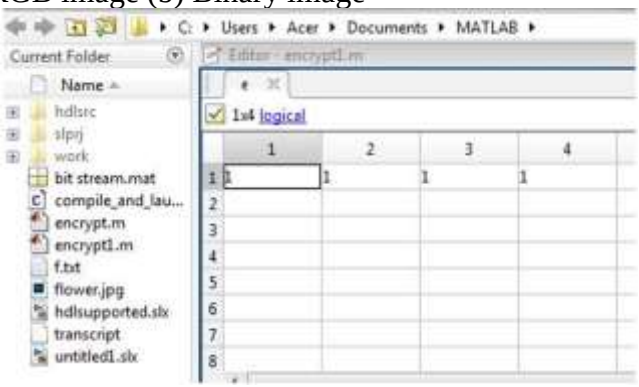

Figure 7: Bitstream of a 2x2 image

The LFSR coding is subsequently applied to the digital bit stream. The code for the 4-bit LFSR cryptography must be completed because it is the 4 bits. Figure 8 depicts the results of the simulation.

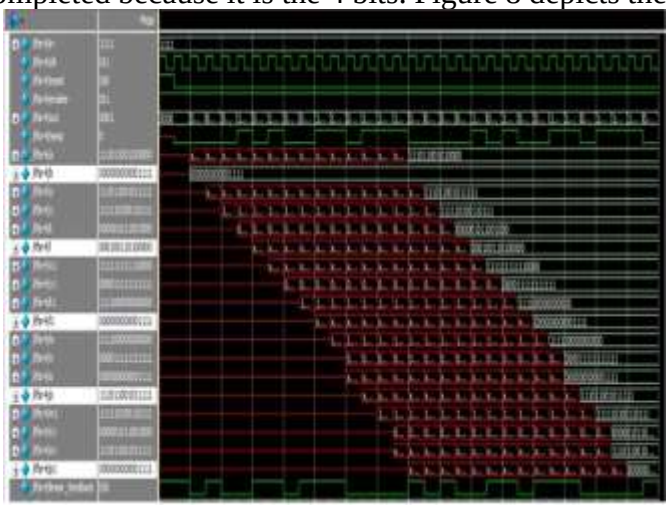

Figure 8. 4-bit simulation for LFSR

The multilayered cryptographic technology reduces the delay value while increasing power as compared to the single layer cryptographic technique which is already in use as it is being proposed. While the frequency remains identical, both the power and the memory are somewhat enhanced. Power must be sacrificed in order to improve security. Figures 9, 10, 11 and 12 compare memory, power, frequency and delay, respectively. In the future, power can be decreased by employing low power approaches.

ISSN: 2278-4632
Vol-15, Issue-06, No.01, June: 2025

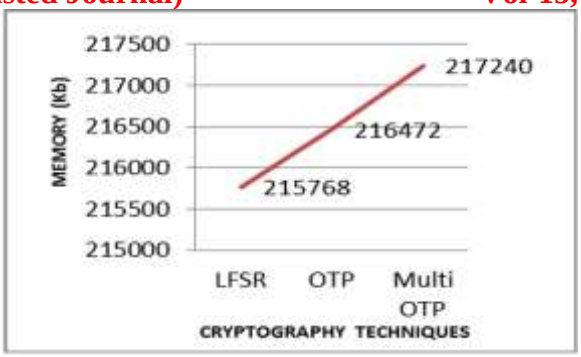

Figure 9: Memory Comparison

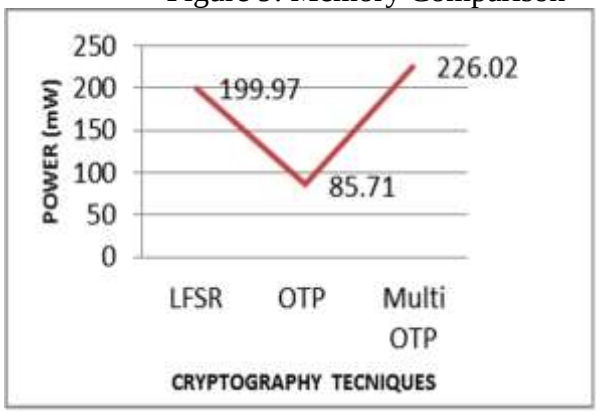

Figure 10. Power comparison

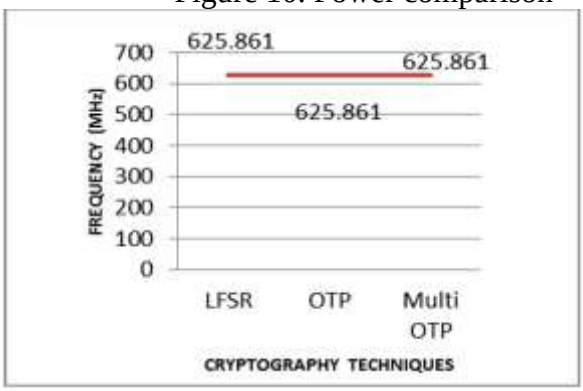

Figure 11: Frequency comparison

Figure 12: Delay Comparison

Software Tools

XILINX ISE:

The initial developer of the field programmable gate array (FPGA), the largest supplier of programmable common-sense devices worldwide, and the leading semiconductor company with a fabless manufacturing version is Xilinx, Inc. As intellectual property (IP) cores, Xilinx creates, develops and sells programmable logic products, including as integrated circuits (ICs), software design

tools and preset device functionalities, as well as design offers, customer education, area engineering, and technical support. Along with communications, commercial, customer, automotive and statistics processing, Xilinx provides both FPGAs and CPLDs, which are programmable common-sense devices, to manufacturers of electronic equipment in different markets.

The ALICE (A Huge Ion Collider test) at the CERN ecu laboratory on the French-Swiss border is even utilized Xilinx's FPGAs to track and decipher the motions of piles of subatomic debris. As the Vertex-II seasoned, Virtex-6, Virtex-five and Virtex-6 FPGA families include up to two integrated IBM PowerPC processors, they are primarily targeted for gadget-on-chip (SOC) designers. One of Xilinx's key digital design automations (EDA) product families is the ISE layout suite. Design access and synthesis support for Verilog or VHDL, place-and-route (PAR), finished verification and debugging with Chip Scope pro equipment and the introduction of bit documents which can be used to configure the chip are all elements of the ISE design suite. For Cool Runner XPLA3/-II and XC9600/XL/XV homes, XST-Xilinx Synthesis Era conducts device-specific synthesis and produces an NGC report that is prepared for the CPLD more fit.

LINX ISE 14.5i:

The most significant tool is Xilinx, which allows us to perform both simulation and synthesis.

Figure 13 Simulation Results for Multilayered Encryption

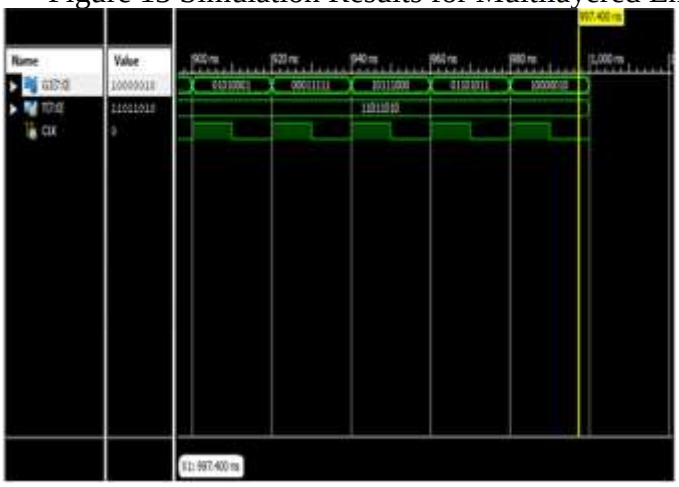

Figure 14 Simulation Results for Multilayered Decryption

CONCLUSION

The LFSR cryptographic technique is used to finish the first and second layers of cryptography. The LFSR cryptography's ciphertext is created. Here, the OTP algorithm handles both the encryption and the decryption. As a result, data security is improved and a summary of the different cryptographic approaches can be produced. Using the LFSR cryptographic technology, the study concentrated on designing efficient single-layered and multilayer encryption. By creating the authentication key, this LFSR cryptographic technology effectively implements several tiers of the bit handling process in the

data communication system. The Matlab program effectively incorporates the idea of image processing as well. The superiority of multilayered cryptography in raising the degree of data security during data transmission can be seen by a comparison with single-layer encryption.

FUTURE SCOPE:

For eight bits, it implemented multilayered LFSR cryptography in the proposed approach. In addition to being applicable to video formats, it can be expanded for more bits, such as 16, 32, ...

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, Xianwen Menga, "An efficient chaos pseudo-random number generator applied to video encryption" in ELSEIVER, OPTIK 127 (2016).
[5] Irith Pomeranz "Computing Seeds for LFSR-Based Test Generation from Non test 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] Noura Aleisa "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] Pushp Lata, 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] Shraddha Soni, 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] Yashwant kumar, Rajat joshi, 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.

