Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 1932-1935

Research Article

Security Enhancement Of Information Using Multilayered Cryptographic Algorithm

Mrs.NathiyaDevi. K[1] , SaiMadhuri.N[2], Bhanuja.P[3] , Dhanusha.P[4]

[1]Assistant Professor, Department of ECE, R.M.D Engineerin College, TamilNadu,601206
[2]UG Students, Department of ECE, R.M.D Engineering College, TamilNadu,601206
[3]UG Students, Department of ECE, R.M.D Engineering College, TamilNadu,601206
[4]UG Students, Department of ECE, R.M.D Engineering College, TamilNadu,601206

Article History Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

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

Through centuries Cryptography has an interesting history which helps us to understand the encryption and decryption process in detail. Since ages of civilization keeping some facts hidden is always important. Individual Privacy is the most important thing which helps to reduce vulnerability. The cryptography has undergone many changes throughout history which follows the advances in technology. Cryptography methods began with a early man who carved unknown forms on wood or stone , then the intended user decrypt the unknown form to get original information. From this the cryptography has being evolved. Cryptography is a study of science that deals with secret writing. It is the art of providing data security by converting original text into an unreadable form and only the intended user can decipher to get the original data back. Hiding information from web is done through cryptography. Various transformation techniques are used for the conversion of original information into a cipher. Tampering of information that are stored within an office, organizations, Banks and other external bodies and establishments occurs when proper security techniques are not used. This leads to hand over sensitive data to the crackers which imposes the threats of jamming, DOS(Denial of service),impersonation of information, session hijacking, flooding, spoofing, sniffing, sleep deprivation, Byzantine attacking and many more. These many completely destroy an organization. Cryptography provides data integrity usually means avoiding unintended users to get the information. Cryptography provides integrity which strictly avoids undetected modification and repudiation. Hence Cryptographic algorithms need to be given primary importance. This helps to ensure that the intruders cannot access any data of an organization. There are two basic types of cryptography which are symmetric and asymmetric. In symmetric Cryptography, for both encryption and decryption a single key is used. In asymmetric cryptography, two keys namely public and private are used for encryption and decryption.

2. Existing method

Built-in Self-Test, or BIST, is the technique of designing additional hardware and software features into integrated circuits to allow them to perform self-testing, i.e., testing of their own operation using their own circuits, thereby reducing dependence on external automated test equipment (ATE).

Another one approach is Elgamal cryptography endto end security technique. It operates in two phases at first level, it works along with sub-server for providing authentication to access the real data server. In the second phase, Once user approaches to the real server he has to go through the public cryptography technique, where data is encrypted with Elgamal cryptography technique to provide end-to-end security

Disadvantages of Elgamal:

1.The potential disadvantage of the Elgamal system is that message expansion by a factor of two takes place during encryption(means the cipher text is twice as long as plain text)

2.It needs for randomness, and its slower speed(especially for signing).

Disadvantages of implementing BIST:

1.Reduced access times

2.Additional silicon area and fab processing requirements for the BIST circuits

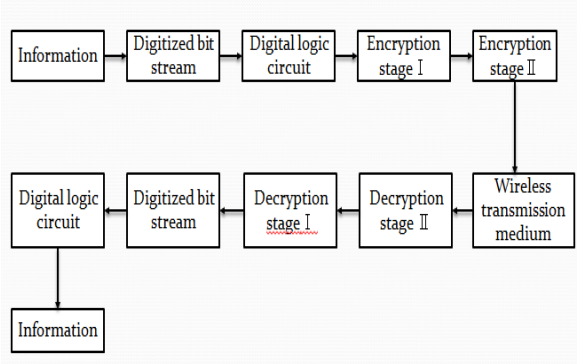
3. Proposed design

In Built-in-self test (BIST) cryptography, LFSR is used for error correction code and in field of communication for generating pseudo-noise sequences. Hence one of the low power architecture is proposed in this paper. In the proposed multilayered LFSR cryptography technique, multi-layers can be used to achieve higher security.

In the proposed work we increased the number of steps in both the encryption and the decryption process to attain the high security level of data. 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.

4. Block diagram



5. Methodology

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. 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 Matlab software.

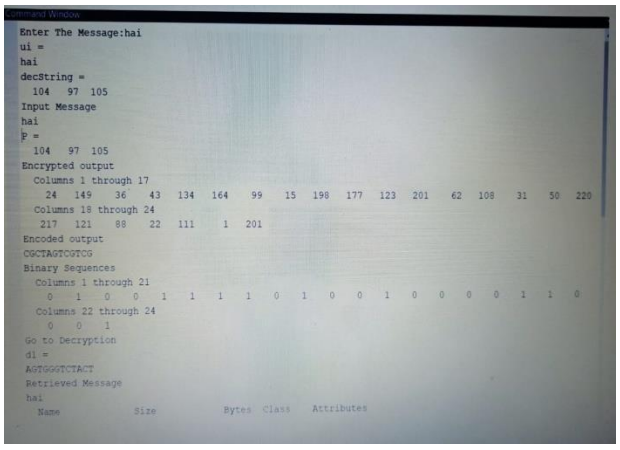


Figure:a Text encryption and decryption

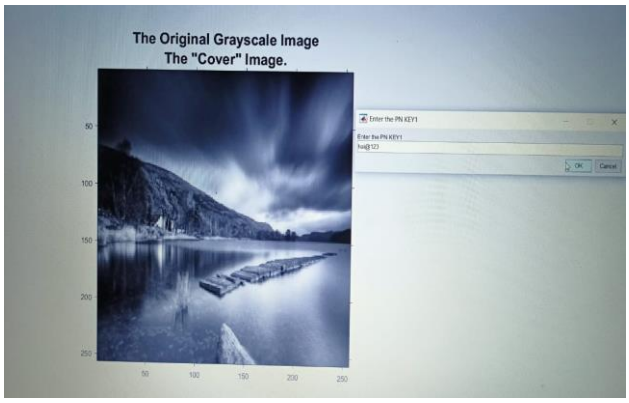


Figure:b Initial input image

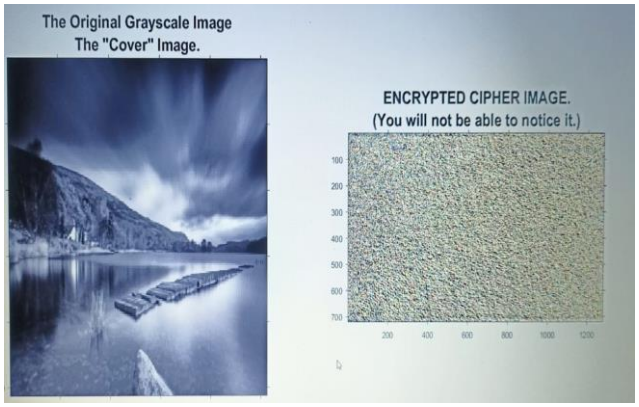


Figure: c Encrypted image

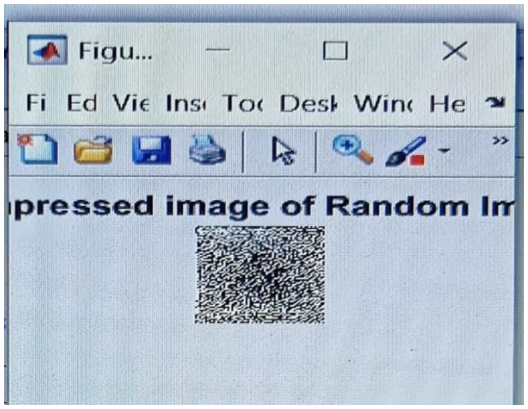
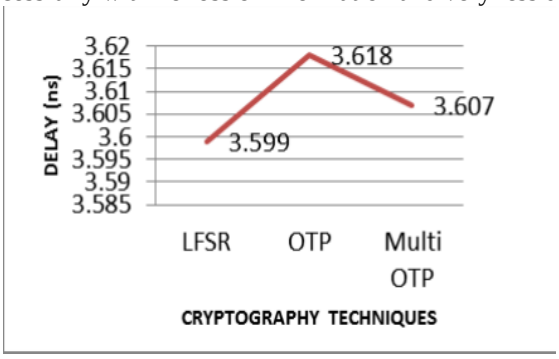


Figure: c Compressed image

Figure: d original image after decryption

6. Result & discussion

The encryption and decryption process using multi-layered LFSR cryptographic technique was done successfully with no loss of information and very less delay compared to existing method.



7. Conclusion

The multiple layers of cryptography are completed with the help of the LFSR cryptographic technique. Multilayered cryptography is used in both encryption and decryption process. security of the data has been enhanced by the LFSR cryptography. Processing of an image using multilayered cryptography was implemented successfully using matlab

References

1. Ramesh Yegiredddi, R kiran Kumar"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.
2. 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.
3. .Sourabh Chandra,SK Safikul Alarm, "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
4. 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
5. Alessandro Cilardo "Exploring the Potential of Threshold Logic for Cryptography-Related Operations" In IEEE Transactions On Computers, Vol. 60, No. 4, (April 2011).
6. 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, Part2 , May- June, 2015, ISSN 2091-2730.
7. 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).
8. 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.