IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

AN EFFICIENT VLSI DESIGN AND IMPLEMENTATION OF LFSR BASED HYBRID CRYPTOGRAPHY ALGORITHM

[1]G.RAVI KUMAR, [2]SANTHI PRIYA
[1]Assistant professor, Department of ECE, Anurag Engineering College, Anantha Giri, Telangana, India
[2]Assistant professor, Department of ECE, Vidya Jyoti Institute of Technology, Hyderabad, Telangana, India

ABSTRACT: Information is the key source to mankind and securing it is the biggest task. Unauthorized access of information deals with the security. Image security is emerging as a major problem with the exponential growth of data stored and transformed through the network around the world. Many cryptographic techniques are used for securing the data like images, audio and text files. These days, the security of information has become more vital in data transfer through networks and storages so everyone knows the importance of data encryption to maintain the confidentiality and privacy of information transmitted across different networks. Cryptography is linked with the process of converting ordinary plain text into indistinct text and vice versa. Symmetric key algorithms i.e., Advanced Encryption Standard (AES), employs the same key for encryption and decryption and is one of the most secured algorithms. Hence in this work, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm is presented. 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 is appropriate for encryption and decryption of online streaming data.

KEYWORDS: Data security, Image, Cryptography, Linear Feedback Shift Register.

I. INTRODUCTION

With the rapid development of information technology, people pay increasing attention to data security. Especially in some special application scenarios, a more open network environment is needed, and data scattered on the end nodes impose higher requirements on the traditional centralized data security sharing scheme [3].

The advance of sharing pictures among others is popular across the world nowadays, especially on the internet through social media such as Twitter, Facebook, WhatsApp, Viber, Telegram, etc. Therefore, the necessity of protecting pictures' privacy is required. Numerous breaches of data using the Internet have been the reason for deliberations on the Internet's security aspects that need consideration and resultant secure solutions. Data security has been an important focus of research. While data digitalization, increased efficiencies, and speeds have increased the vulnerabilities of data to cyber-attacks, data records appear to be a popular target for hackers [1].

All physical systems like environment monitoring, health care system, advanced metering in smart grids, etc, which are connected through Internet-of-Things (IoT) that generate a large amount of data that leads to the privacy and security issues. The transmitted data over the insecure network are protected by different cryptography algorithms. 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. Generally, cryptographic methods consist of fundamental components such as plain text, cipher text, key and cryptographic algorithm [6]. The cryptosystem is used widely with the rapid development of information technology. A

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

various encryption technique is used to make ensure of information security [4]. Cryptography develops a cryptosystem, which converts an original intelligible image, referred to as plain image, into apparently random cipher image and it also recovers the image back in its original form.

Recently, with the rapid development of network communication technology, the opportunities for global users to access the Internet have become more and more popular, and the dissemination of information and data has become more frequent. Multimedia and visual content already exist and are widely used in many domains, such as sharing military and medical personal information. Encryption methods are not only used in image multimedia, but also important for user security information (such as credit card numbers), cloud usage, etc. A good encryption scheme to protect information transmission security is of great significance. Therefore, encryption technology is receiving more and more attention.

Encryption and decryption technology plays an important role in protecting our property security, personal information, and so on. The implementation of encryption and decryption technology depends on algorithms and security mechanisms. Secure and efficient encryption and decryption algorithms and their correct application can effectively guarantee the security of the system [5].

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. Two methods of key generation exist: symmetric key generation and asymmetric key generation. The conventional cryptographic technique such as International Data Encryption Algorithm (IDEA), Rivest Cipher 6 (RC6), Triple Data Encryption Standard (TDES) and other block ciphers are well suited for encrypting textual data and less suited for digital image encryption as the digital images have inherent feature such as bulk data capacity, high correlation with neighboring pixel and high redundancy. Further the implementation of these conventional algorithms with commercial software tools or low computing devices are even more complicated. Mean while AES algorithm has the advantages of small memory, easy to implement, ability to resist a variety of cryptanalysis attacks, and high encryption efficiency [2].

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. Hence in this work, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm is presented. The remaining work is organized as follows: The section II describes the literature survey. The section III presents Hence in this work, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm. The section IV evaluates the result analysis of presented approach. Finally the conclusion is discussed in section V.

II. LITERATURE SURVEY

Z. Mishra, P.K. Nath and B. Acharya et. al., [7] describes High throughput unified architecture of LEA algorithm for image encryption. a high speed low area unified architecture for LEA algorithm for three different sizes of key. The pipelined implementation of the proposed design

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

improves operating frequency to a significant degree, with a little increase in the hardware costs. The design proposed in this paper notably supports three varying tile sizes, i.e. 256×256, 128×128, 64×64, of an input image. As resolution of an input image may not necessarily be an integer multiple of the size of tile, smaller tile sizes at the image boundary can also be handled by the same architecture. Proposed architecture shows 28%, 35% and 45% increment in the hardware resources with respect to available LEA architectures with single key. The incorporation of the unified key generation technique and pipeline implementation of the algorithm are the main reasons for the more hardware utilization.

P. Vinotha and Deepa Jose et. al., [8] describes VLSI Implementation of Image Encryption Using DNA Cryptography. Anew technique ofDNAcryptography provides high security based on DNA nucleotides bases A-Adenine, C-Cytosine, G-Guanine and T-Thymine. These alphabets can be easily assigned to binary values (A-00,C-01,G-10,T-11). In this model, Polymerase Chain Reaction encoding technique is used in which the image to be encoded is flanked between primer keys. The DNA codons are encoded by the base of four provides keys of 256 combinations for high security, and it reduces the size of cipher text. Primer keys are generated by pseudo random sequence generator. Deciphering the image is possible with encryption key and primer sequence key. The HDL synthesis report for hardware design is implemented for encryption using verilog code on a device Virtex VII.

Guangming Yanga, Jingying Mab and Zhenhua Tan et. al., [9] describes Design and Implementation of Image Encryption System Based on Random Grids and Mscan Patterns. A hybrid image encryption system is presented and designed by combining these two algorithms. This also considered the distortion, compressibility and encryption strength of the image. Using the defects of the MSCAN algorithm, a simulation attack was performed on the traditional Mscan (Modified Scan) encryption algorithm. Finally, statistical analysis and diffusivity tests are used to evaluate the design of the encryption system.

Balakrishnan Ramalingam, Amirtharajan Rengarajan, John Bosco Balaguru Rayappan et. al., [10] describes Hybrid Image Crypto System for Secure Image Communication- A VLSI Approach. This work presents permutation and diffusion based hybrid image crypto system in transform domain using combined chaotic maps and Haar Integer Wavelet Transform (HIWT). HIWT is used to transform the plain image and four sub-bands of the image coefficients are encrypted by combined chaotic maps. The combination of two one-dimensional chaotic maps results in better chaotic behaviour and generates unpredictable large random sequence that can be used for the encryption of the image. This design occupies only 4025 logical elements and takes 0.28 ms for encrypting an image of size 256×256. Robustness of the algorithm is estimated using quality metrics including statistical and differential attack analysis. This scheme is resistant to most of the known attacks and is more secure than other image encryption schemes.

III. EFFICIENT VLSI DESIGN AND IMPLEMENTATION

In this section, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm is presented. The Fig. 1 shows the block diagram of presented approach.

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

In a single image, there will be a greater number of Pixels available. So, Possibility to find out the pixels what we are using as key is highly complex one. Even though if someone find out the pixels count as well as pixel's location, they need to know the arrangement of pixels. The KEY origination is kept as a secret. So to hack the data is very tough. Initially, the input images are read using MATLAB and converted into a binary format.

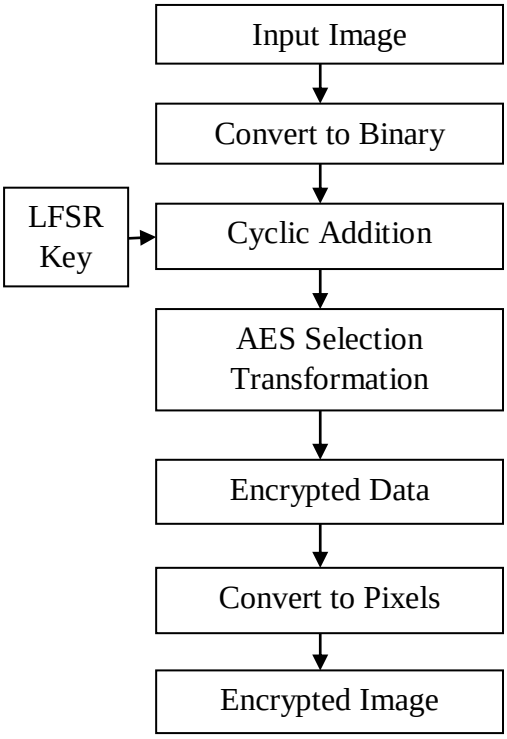


Fig. 1: Block Diagram of efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm

BW = im2bw (I, level) converts the gray-scale image I to binary image BW, by replacing all pixels in the input image with luminance greater than level with the value 1 (white) and replacing all other pixels with the value 0 (black). This range is relative to the signal levels possible for the image's class.

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. 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 AES algorithm produces transformation output, which is 8-bit cipher text. 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.

It employs polynomials to make the maximum possible LFSR length for each and every bit width. The generated key is applied to cyclic addition. The output of cyclic addition is applied to AES selection transformation. The AES algorithm deals with four operations .i.e., Sub Bytes, Add Round Key, Mix column, Shift Rows. 256-bit AES encryption block is implemented in 14 rounds. For each round it will do the four operations. Round 0 consists of only Add round Key operation. Round 14 consists of Sub Bytes, Shift Rows and Add Round Key operations, which need 3 clock cycles. Rounds 1 to 13 consists of all the four operations. In each clock cycle a distinct operation is performed. Hence once the hardware has been implemented for all four operations, same hardware is used for all the 14 rounds. None of the four operations shares the same clock cycle. The sequence of round operation with specific sequence of 4 operations are needed to complete the AES encryption. The AES method is a serial process. i.e., the first round output is connected to the second round and it will be the input for it. Hence, same hardware is used for each

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

round. The data structure of 128-bit matrix. Each column consists of 4 elements of 8 bits each, so in total we have 32 bits per word.

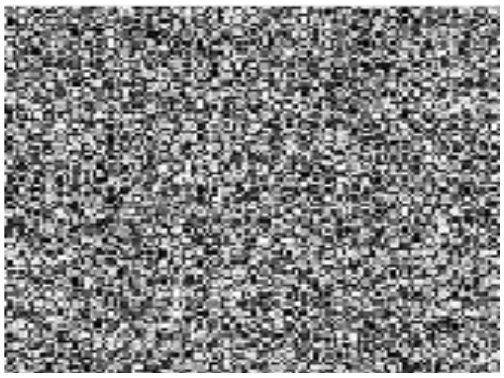
This AES algorithm provides secure message transmission with less integrity by using LFSR. The original image is divided into blocks and the blocks are processed one by one. Each block of image is encrypted using key generated by cyclic addition with LFSR. At the receiver end same key is used to decrypt the image. Hence, the LFSR concept provides more security and effectiveness in encryption and decryption process. By using the key one can encrypt the data. No one knows how the key is generated and they cannot know the arrangement of pixels. For decryption, the encrypted data will transform back by giving cipher text with the help of the key one can get the plain text. It will use the same cryptographic keys at both sender end and receiver end. The output of AES is converted to text format for both the encryption and decryption process. The encryption text values are converted back to the pixels, and the pixel values are converted into an image in the final step.

By using this method there is no need to remember and store the key to encrypt the data. This method gives more security than the existing system. Randomly one can change the key according to our wish. So that, there is no possibility to hack the data, this method gives more accuracy and less complexity.

IV. RESULT ANALYSIS

In this section, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm is implemented. The result analysis of presented approach is evaluated here. The Fig. 2 shows the input image (lena) and encrypted image.

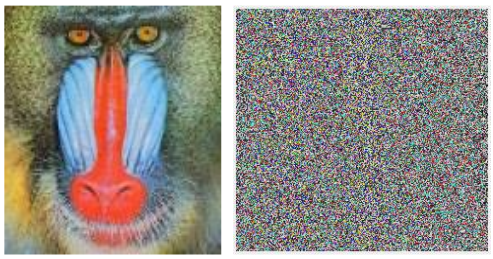
(a)



(b)

Fig. 2: (a) Input Image and (b) Encrypted Image

The Fig. 3 shows the baboon image and encrypted image.



(a) (b)

Fig. 3: (a) Input Image and (b) Encrypted Image

The histograms of plain and encrypted images are tested for evaluating the statistical Resemblances. The, uniformity of cipher images can be analyzed quantitatively by calculating the variances of histograms. The histogram variance can be calculated as

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

$$Var(H) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{(H_i - H_j)^2}{2} \quad (1)$$

where, H_i, H_j are the number of pixels at the gray scale levels i, j respectively. The variance value of the histograms are calculated for different secret keys on the plain image. Lower value of variance indicates the higher uniformity of the resultant cipher image. The Fig. 4 shows the histogram of input image.

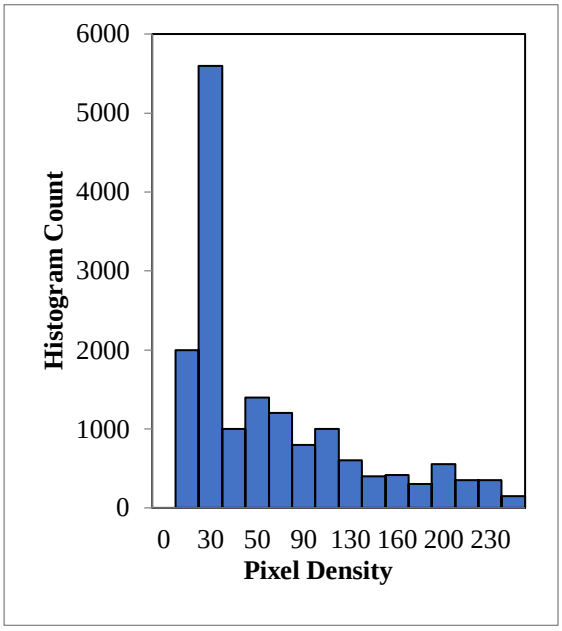


Fig. 4: Histogram of Input Image (baboon)

The Fig. 5 shows the histogram of encrypted image where x-axis represents the histogram count and y-axis represents pixel density.

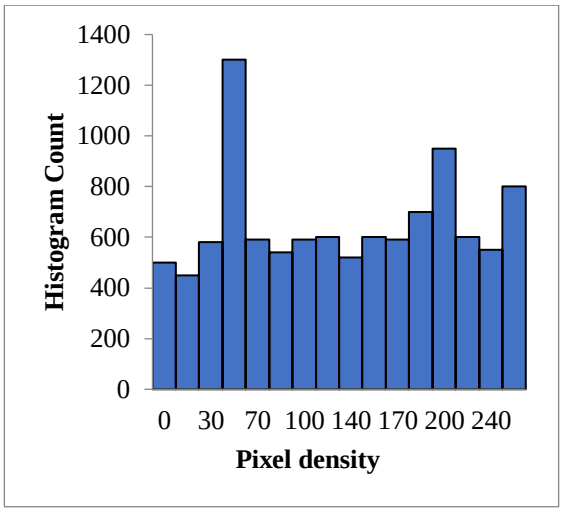


Fig. 4: Histogram of Encrypted Image (baboon)

The Fig. 5 shows the encryption time to encrypt the image where x-axis represents encryption algorithms and y-axis represents encryption time in terms of seconds.

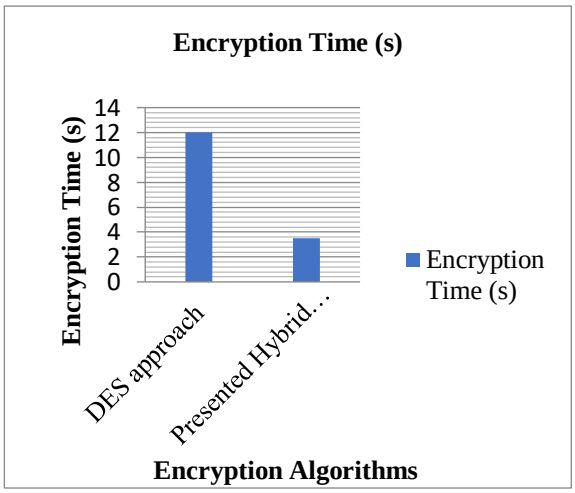


Fig. 6: Encryption Time Comparison

Compared to DES (Data Encryption standard algorithm, presented efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm has required less time for encryption. Hence, presented approach has shown efficient image encryption within less time. As a result this approach will have a great significance for secure image transmission.

V. CONCLUSION

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

The necessity to protect information and images is required more and more every day due to the increase of eavesdroppers in the network. Hence, n order to solve these issues, an efficient VLSI design and implementation of LFSR based hybrid cryptography algorithm is presented. First the input image is converted in to binary image. Advanced Encryption Standard (AES) is used in this approach, which is one of the most widely used algorithms for data encryption and decryption. Linear Feedback Shift Register (LFSR) s used the random numbers are generated for key generation. AES algorithm is the best way to protect information from eavesdroppers. AES algorithm provided secure message transmission with less integrity by using LFSR key. The original image is divided into blocks and the blocks are processed one by one. Each block of image is encrypted using key which is generated by cyclic addition with LFSR. The encrypted text values are converted back to the pixels, and the pixel values are converted to provide encrypted image. The histogram analysis is performed to evaluate the results. Compared to earlier algorithms, presented approach has required less time for encryption.

VI. REFERENCES

[1] Ala Saleh Alluhaidan, "Secure Medical Data Model Using Integrated Transformed Paillier and KLEIN Algorithm Encryption Technique with Elephant Herd Optimization for Healthcare Applications", Journal of Healthcare Engineering, Volume 2022, Article ID 3991295, 14 pages, doi:10.1155/2022/3991295

[2] Zhonghua Luo, Keyong Shen, Rongqun Hu, Yuhan Yang, and Rongchun Deng, "Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things", Computational Intelligence and Neuroscience, Volume 2022, Article ID 8424100, 11 pages, doi:10.1155/2022/8424100

[3] Lei Liu, Mingwei Cao, Yeguo Sun, "A fusion data security protection scheme for sensitive E-documents in the open network environment", PLOS ONE, doi:10.1371/journal.pone.0258464,December 15, 2021

[4] Mangal Deep Gupta, R.K. Chauhan, "Secure image encryption scheme using 4D-Hyperchaotic systems based reconfigurable pseudo-random number generator and S-Box", INTEGRATION, the VLSI journal 81 (2021) 137–159, doi: 10.1016/j.vlsi.2021.07.002

[5] Praveen Banasode, "Enhanced Computation Architecture For Big Data Analytics Using Encryption Algorithm", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 12 No. 5 Sep-Oct 2021, DOI: 10.21817/indjcse/2021/v12i5/211205010

[6] Jun-Dian Li and Chih-Peng Fan, "Design and VLSI Implementation of Low Latency IEEE 802.11i Cryptography Processing Unit", Journal of Advances in Computer Networks, Vol. 8, No. 1, June 2020, doi: 10.18178/jacn.2020.8.1.274

[7] Z. Mishra, P.K. Nath and B. Acharya, "High throughput unified architecture of LEA algorithm for image encryption", Microprocessors and Microsystems (2020), doi:10.1016/j.micpro.2020.103214

[8] P. Vinotha and Deepa Jose, "VLSI Implementation of Image Encryption Using DNA Cryptography", ICICV 2019, LNDECT 33, pp. 1–9, 2020, doi:10.1007/978-3-030-28364-3_17

[9] Guangming Yanga , Jingying Mab and Zhenhua Tan, "Design and Implementation of Image Encryption System Based on Random Grids and Mscan Patterns", IOP Conf. Series: Materials Science and Engineering 466 (2018) 012059 IOP Publishing doi:10.1088/1757-899X/466/1/012059

[10] Balakrishnan Ramalingam, Amirtharajan Rengarajan, John Bosco

Balaguru Rayappan, "Hybrid Image Crypto System for Secure Image Communication- A VLSI Approach", Microprocessors and Microsystems (2017), doi: 10.1016/j.micpro.2017.02.003