ISSN No: - 2456 – 2165

Image Security Using Linear Feedback Shift Register

Krishnapriya P V
MTech CSE,Department of CSE
Sree Narayana Gurukulam College of Engineering ,
Kadayirippu, kerala,India
E-mail: krishnapulickal93@gmail.com

Smitha Suresh
Assoc. Professor,CSE Dept.
SNGCE,Kadayirippu,Kerala
smithadeepak2006.sngce@gmail.com

***Abstract*- Encrypting data is a way to protect the data or to prevent the unauthorized access of data by others and these data can be text, image audio, video or anything. In order to protect data from unauthorized access a new concept is introduced and this is based on linear feedback shift register method. In this method two step encryption is provided to give more security to the data. The encrypted image can be decoded in the decryption stage. In the encryption stage the LFSR will generate random numbers to reorder positions of each pixels in the row of the image . After row encryption, column need to be encrypted by again generating random numbers using LFSR to reorder each pixels in the column of the image . Then we use XOR operation to shuffle all pixels to get the final encrypted image. To decrypt the image , reverse operation of encryption is performed . First step in the decryption process is XOR execution and then decrypt the column encrypted image and finally decrypting row encrypted image to reconstruct the original image.**

***Keywords*—*Linear Feedback shift Register, Encryption, Decryption, XOR, Random generator*.**

I. INTRODUCTION

Today, the demand of internet has made the transmission of digital media much easier and faster. Open nature of the internet, risks of illegitimate accessing and unauthorized tempering and access with transmitted data is increased day by day. Protection of secret information from unauthorized users in a public network has become an important issue in the internet world. As the cyber crimes are increased day by day, network security alone is not sufficient for securing data. Security is measured as a critical factor which is to be taken care of while transferring confidential data on the Internet. Since text, images, audio, video are the part of digital data that are transferred over open public network so there is need to protect this digital data. From the last few decades, various methods have been developed and implemented to impose security in various types of applications in the network.

Encryption is a way to ensure security to the image or data. Encryption process allows the data or information access to the authorized parties only [9]. Encryption can be achieved with some encryption algorithms.

Here we are introducing a new method for encryption using a Linear Feedback Shift Register[4], for encrypting the data before it is transferred to the communication channel.

II. LITERATURE SURVEY

Many researchers are introduced various techniques for encryption. These encryption methods have many applications in the real world applications such as the medical imaging , military communication, internet communication and so on.

Sivakumar *et al* [2] proposed a novel approach for image encryption using scan based pixels position permutation and random key stream. Namitha Tiwari [6] proposes a method which uses using two levels of encryption for encrypting an image. Two different techniques are used for this proposed encryption scheme. Mazumdar *et al* [7] proposes an efficient and secure method to modify the plain text into an encoded cipher text. This can provide about 80-85% data security as decoding of data involves inverting the feedback function produced by linear feedback shift register or generating the binary sequence which will help in retrieving the data after some recombination operation. Another method for image encryption is proposed by Huang *et al*.[3], proposes a chaotic system which is adopted as the fundamental base and combined with row, column shuffling, and gray-level encryption.

III. PROPOSED SYSTEM

The proposed system has got many advantages such as it reduces the risk involved in the implementation of other encryption algorithms. It also provides more security than other methods as it generates the random numbers using the random number generator[5]. Random generators use XOR operation to produce a random or periodic sequences. Previous sequence is given as the input bit to the linear function.

a) Methodology

Here we are considering the image encryption. This new method of image encryption is based on a linear feedback shift register(LFSR). In order to encrypt the given plain image we need to make use of the linear feedback shift register , which generates the random numbers used in the encryption process. Since we use the random number generator , the attacker cannot

ISSN No: - 2456 – 2165

guess the next number in the sequence, even if he/she have some idea about some numbers in the generated sequence.

This method proposes a new technique to encrypt the color image using LFSR to generate random numbers used in the reorder position of the image pixels. The method is divided in to two stages , namely, encryption and decryption. In the encryption stage uses two phases of encryption. First phase involved in the encryption stage is the row level encryption and the second phase is the column level encryption. Finally we need to apply the XOR operation to complete the encryption stage . since we use the XOR operation we need to convert the image into a binary format before encryption. So that we can perform a smooth encryption process. To decode or decrypt the image we need to do the reverse operation of encryption

b) Encryption

Encryption is the process of encoding the data to protect it from unauthorized access. The information can be text, image, audio, video, graphics or anything . The main and only concern is to provide security to these information before it is transferred into a communication channel. To provide more security to the data we use two level of encryption.[1] That is row wise encryption and the column wise encryption. Before encrypting the color image we need to convert this original color image into a binary image format which needs to be encrypted using the explained method

The first phase of the encryption stage , is to load the color image which needs to be encrypted . Then we need to generate the random numbers used for reordering the row wise pixel values of the intended image. This random numbers can be generated with the help of linear feedback shift registers. The seed value which is set to the LFSR can be used as the key value for the encryption process. This same key is used at the decryption stage but the random generated matrix will be different. After shuffling the row wise pixel values with the random numbers , we can obtain a row level encrypted image. That is almost 50 percent of the pixel values of the original image got changed or encrypted. This can be verified by calculating the NPCR value of the encrypted and the plain image.

The second phase of encryption is the column level encryption. We need to do the same steps as done in the row level encryption, instead of row the process needs to be applied in column wise. For column encryption again we need to generate a sequence of random numbers and these random numbers needs to be converted into a matrix . This process is done to rearrange or swap the pixel values of the image with the random matrix. The column wise encryption is done on the row encrypted image. After the pixel reordering we can obtain a column encrypted image. To complete the encryption step , finally we apply the XOR operation to the encrypted image which results in a complete encrypted image. The detailed representation of the encryption process is shown in Fig.1 [1].

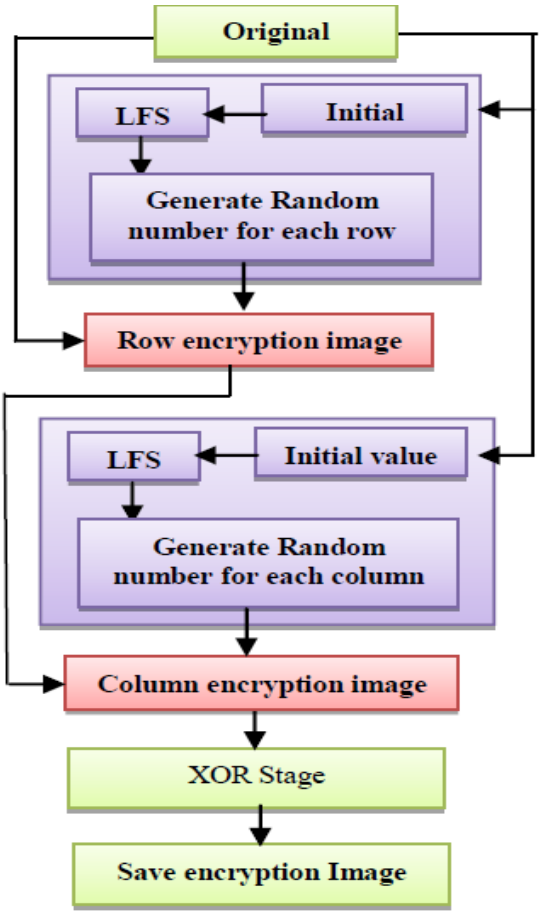

Fig .1 Different stages in Encryption

c) Decryption

Decryption is the process of decoding the encoded for encrypted image to obtain the original input image which will in the form of human readable or can be understood by machines. Decoding process is normally done at the receiver end to make the data readable to the intended receiver. Using the corresponding decryption algorithm and decoding key we can decrypt the cipher text back to the original format. The decryption process is not a complex process, if we have the key for decoding it is very easy to decrypt the information. Here we need to perform two level of decryption because at the encryption stage we perform a two level encryption. So in order to achieve the original data it requires two times decryption.

In the decryption stage , the reverse operation of the encryption process is performed. In the encryption stage we follow the processes in an order of row encryption, followed by column encryption and finally performed an XOR operation. So in order to decrypt these operations needs to be reversed. First we need to perform the XOR operation followed by column decryption and finally row decryption.

Therefore the first stage in the decryption process of the image is to perform the XOR operation, in which the column and the row pixel values of the image get XOR ed. The outputted image after the XOR operation is subjected to column decryption. In the

ISSN No: - 2456 – 2165

column decryption step , it is necessary to generate the random numbers for each column using the linear feedback shift register. In the column decryption, we use the key seed value used in the column encryption stage of the image. By combining the seed value and the randomly generated matrix we can decode each column of the encrypted image.

After this process, half of the decryption is completed. To obtain the remaining half we need to perform the row wise decoding , which will achieve the complete decrypted image.

To decrypt each row of the encrypted image , process performed to obtain the column decrypted image needs to be repeated with the row order. Again this process needs to call the linear feedback function to generate a sequence of random numbers which is converted to a matrix. With the random matrix and the key , we will be able to generate the row decrypted image. After performing the row level decryption , there obtained the original input image. The detailed representation of the decryption stage is shown in Fig.2.[1]

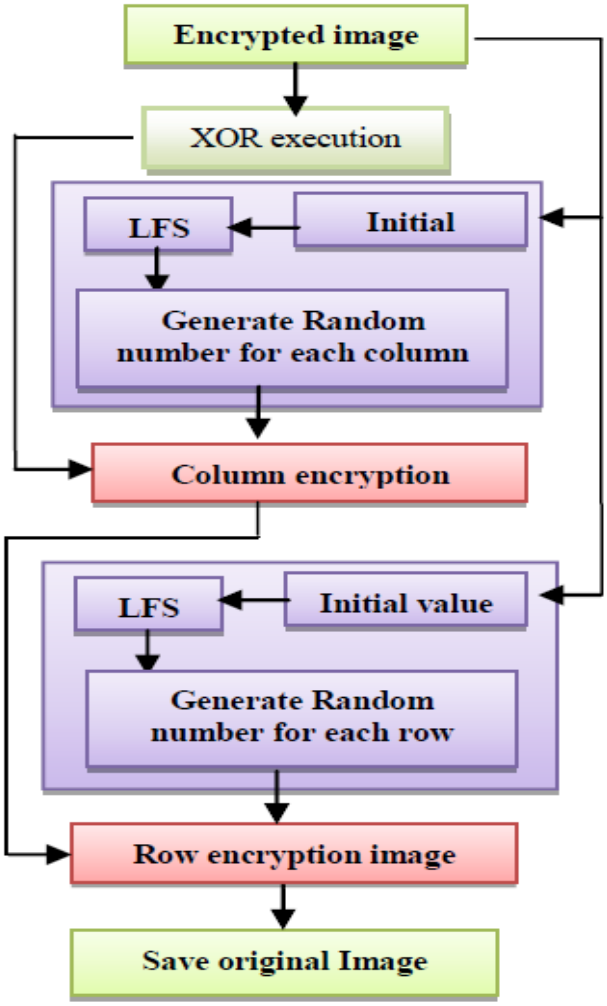

Fig.2 Decryption Stages

IV. RESULT AND ANALYSIS

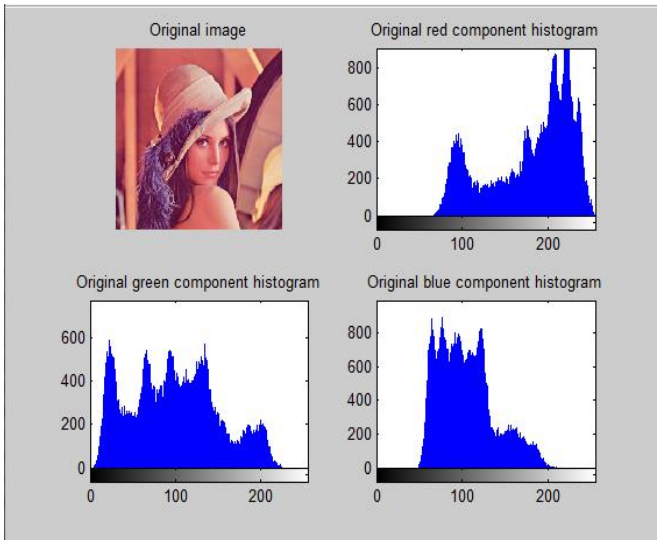

Fig .3 Original image and its Histogram

This method is successfully implemented on the standard test image ‘lena’ and ‘flower. Encryption and decryption are applied on these standard test images. The following figures shows the different stages of encryption and decryption of these images. Figure 3 shows the original image and its histogram to the RGB components of the image pixel . Before encrypting the image , the original image is transformed to a binary format which is shown in figure 4 . Figure 5 shows the different phases of the encryption performed on the input image shown in fig 4, namely ,the row encryption, column encryption and XOR operation.

Fig 4 Input image

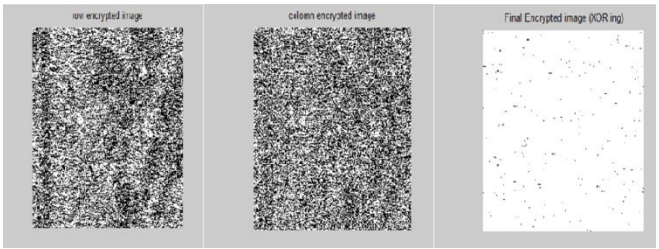

Fig. 5 Encrypted Image

ISSN No: - 2456 – 2165

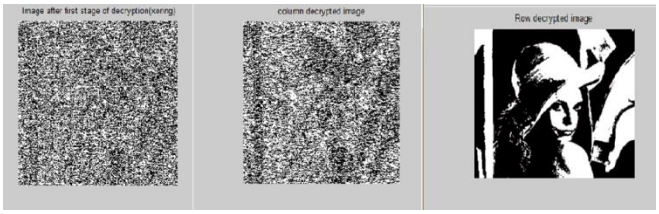

Fig. 6 Decrypted Image

Fig 6 shows the different levels of decryption in the encrypted image. First step shows the image after XOR ing then it is followed by the column and row wise decryption.

The Number of Pixel Change Rate(NPCR) is also calculated for this method. For the above test image the NPCR is calculated using the formula [8] which is given as follows:

$$\text{NPCR}=\sum i,j \frac{Z(i,j)}{H\times W} \times 100\%$$

Where 'H' is the height of the image and 'W' is the width of the image. The pixel positions (i,j) and X1(i,j) and X2 (i,j) , an array Z(i,j) is defined as : if X1(i,j)= X2 (i,j) then Z(i,j)=0, otherwise Z(i,j)=1. Based on this the NPCR value is calculated.

The NPCR value is obtained by comparing the encrypted image and the original image pixel values. By using the image encryption based on the linear feedback shift register method , NPCR value obtained is 99.5832. , which is an acceptable result using this method.

V. CONCLUSION

We use cryptography methods to provide an improved security to the data. This linear feedback shift register method provides a good level of security to the image. Since the security level is high, no one able to access the image data in the communication channel. The image or information obtained after encryption using this LFSR method is completely different from the original image. This can clearly understood by looking the NPCR value. By using this method the NPCR value obtained is 99.582 percent, which is an acceptable value and this shows that the high level of encryption that is the encrypted image is completely different from the original image in the range of around 100 percent.

REFERENCES

[1]. Salah T. Allawi, Dr.Jamila H.Al-A'meri ,"Image encryption based on linear feedback shift register method", 2016 Al-sadeq International conference on Multidisciplinary in IT and Communication scienece and applications, May 2016

[2]. T. Sivakumar and R. Venkatesan " Image EncryptionBased on Pixel Shuffling and Random Key Stream " , International Journal of Computer and Information Technology , volume 3- issue 06, November 2014.

[3]. C.K. Huang, C.W. Liao, S.L. Hsu, and Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", Telecommunication Systems, Vol. 52, pp563– 571, 2013.

[4]. Bhaskar Mondal, Nishith Sinha and Tarni Mandal," A Secure Image Encryption Algorithm Using LFSR and RC4 Key Stream Generator", Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Smart Innovation, Systems and Technologies 43, October 2016.

[5]. Vishal Kapur Surya Teja Paladi Navya Dubbakula , "Two Level Image Encryption using Pseudo Random Number Generators", International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 12, April 2015

[6] Arihant Kr. Banthia Namita Tiwari , " Image Encryption using Pseudo Random Number Generators ", International Journal of Computer Applications (0975 – 8887) Volume 67– No.20, April 2013

[7]. Subhra Mazumdar , Tannishtha Som , "Data Encryption with Linear Feedback Shift Register", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 .

[8]. Yue Wu, Joseph P. Noonan, and Sos Agaian, "NPCR and UACI randomness tests for image encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications, pp.31-38, 2011.

[9].https://www.tutorialspoint.com/cryptography/modern_cryptography.htm