Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

Image Encryption Technique by Using Hybrid Pseudo Random Number Generator: A Review

Jaiganesh M
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: jaiganesh@jainuniversity.ac.in

Abstract

This paper introduces a genetic operations-based encryption scheme and a new hybrid pseudo-random number generator (HPRNG). Based on the linear feedback shift register (LFSR), chaotic asymmetric tent chart, and chaotic logistic map, the new HPRNG is built. To encrypt the picture blocks, the scheme uses XOR and genetic operations (mutation, and multipoint crossover). With the assistance of a pseudorandom bit sequence generated by the HPRNG, the first block of the plain image is encrypted. The subsequent blocks are based on the previous block of the cypher and the operator of XOR. To encrypt colour images and text as well, the scheme can be expanded. The created cypher images have very little correlation with their corresponding plain images and have high entropy values, making redundancies in the image pixel values unpredictable and difficult to detect. Compared to some existing schemes, more about the scheme was found and that the proposed scheme was comparatively safe and successful.

Keywords: *Correlation, Encryption, Image, Multimedia, Pseudo Random, Hybrid, Number generator.*

I. INTRODUCTION

The protection of knowledge has become part and parcel of today's world. Photos are the internet's most popular type of multimedia. During the transmission of information over the network, security has become one of the most important issues [1]. The primary objective of cryptography is to turn the data to be held secret by encryption into unrecognizable material such that only authorized persons can be able to recover the initial. Without decryption, the cypher image obtained after encryption has little relevance to the original image. Images have many unique properties that differentiate them from texts. These characteristics, such as high

content, redundancy and high correlation between the adjacent pixels, make the process of encryption worthy of concern. An effective algorithm for image encryption can produce a random cypher image at a good speed [2].

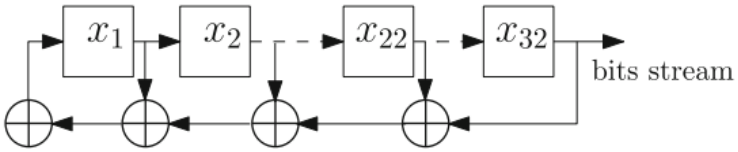

Figure 1: Illustrates the 32-bit LFSR

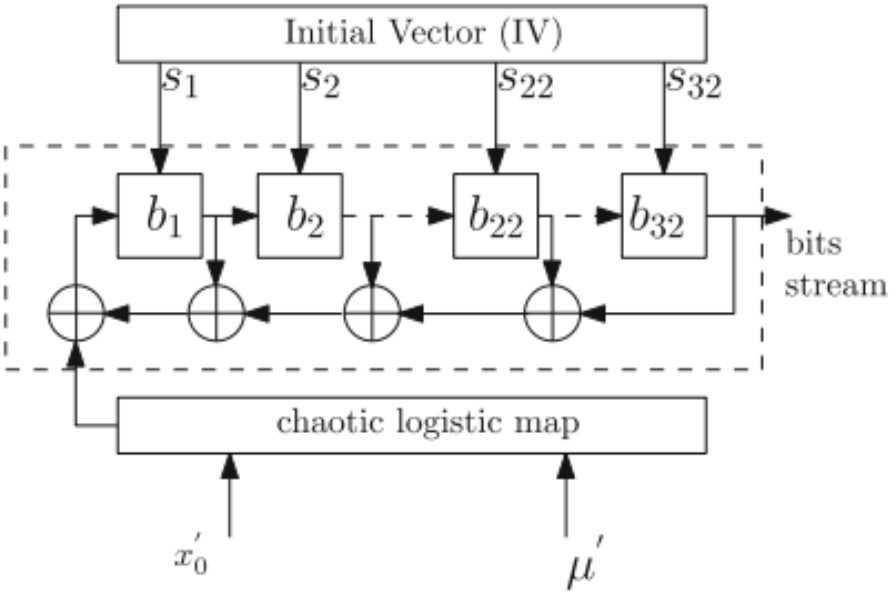

Figure 2: Illustrates the outline of the proposed method

Figure 3: Illustrates the real and encrypted images [3]

Figure 1: Illustrates the 32-bit LFSR. Figure 2: Illustrates the outline of the proposed method. Figure 3: Illustrates the real and encrypted images.

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

$$MAE = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}|p(i,j) - E(i,j)|$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$cov\ (x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\ (y_i - E(y))$$

$$r_{xy} = \frac{cov\ (x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)} \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K} (y_i - E(y))^2$$

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [5].

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K} (x_i - E(x))^2$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K} (y_i - E(y))^2$$

II. LITERATURE REVIEW

A novel chaotic image encryption technique based on several discrete dynamical maps was investigated by Khan et al. Dissemination of information over an insecure medium of communication is one of the most important aspects of the technologically advanced period. Electronic information travels in the form of binary bits. The protection of such digital content is one of the most important problems in today's world. In this article, we have used

several messy iterative maps to propose a novel image encryption technique. Confusion and diffusion have been applied to the proposed encryption in the system given, which is one of the most fundamental aspects of the encryption technique. Our predicted approach has been tested and compared with current findings against different performance analysis. The built scheme is capable of providing an excellent privacy to digital images.

III. DISCUSSION AND CONCLUSION

The suggested XOR operation and genetic operations (mutation and crossover) encryption algorithm are used. Pseudorandom bit sequences of length 256 are created for one time by the proposed process, which significantly reduces the computational overhead. The broad key space makes eavesdropper's encryption more secure and difficult to compromise the confidentiality of the encrypted data. Cipher image histograms are flat and consistent and have about the same frequency for each degree of intensity. The association in the cypher images between adjacent pixels turns out to be insignificant and nearly equal to zero. Another benefit of the approach proposed is that it can also be extended to text data, despite the fact that the analysis is only carried out on images. In this step, the previously encrypted block produces a random sequence for the current block. So, without the knowledge of the previous image block, one cannot decrypt the current cypher block. Several interesting features are provided in the proposed algorithm, such as a higher degree of protection, broad key use, and uniform distribution of pixel values.

IV. REFERENCES

[1] [1] E. N. Kumar and E. S. Kumar, “A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach,” 2013.
[2] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. 2016.
[3] N. Ameena Marshnil and M. C. Binish, “Image encryption based on diffusion process and multiple chaotic maps,” 2014, doi: 10.1109/EPSCICON.2014.6887501.
[4] M. Khan and T. Shah, “A Literature Review on Image Encryption Techniques,” Autoimmunity Highlights. 2014, doi: 10.1007/s13319-014-0029-0.
[5] Y. P. Zhang, Z. J. Zhai, W. Liu, X. Nie, S. P. Cao, and W. Di Dai, “Digital image encryption algorithm based on chaos and improved DES,” 2009, doi: 10.1109/ICSMC.2009.5346839.