IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 18, Issue 4 Ser. IV (Jul. – Aug. 2022), PP 24-29
www.iosrjournals.org

Image Encryption System Using Gauss Map and LFSR

Srushti Gandhi[1],Dhruvi Patel[2], Ravi Gor[3]
[1]*Research Scholar, Department of Mathematics, Gujarat University,Ahmadabad, Gujarat, India*
[2]*P.G. Student, Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University,Ahmadabad, Gujarat, India*
[3]*Department of Mathematics, Gujarat University,Ahmadabad, Gujarat, India*

Abstract: *In today's world, with the introduction of 5G (5th Generation) allied technologies, information transmission has increased rapidly. The use of the image in daily life has increased as information technology is developing. Therefore, the demand for a system of security in sending images through the internet is necessary. There are many types of securities, but encryption is one of the best techniques.It makes an image readable only to the authorized access. Data security is done either by cryptographic technique or chaotic technique. This paper presents image encryption and decryption using a chaotic Gauss map and Linear Feedback Shift Register (LFSR).Gauss map uses more controlled parameters as compared to another chaotic map, which increases the data security. Also, the Gauss map takes lesser time for encryption and decryption.*
Keywords: *Gauss map, Linear Feedback Shift Register (LFSR), Image Encryption-Decryption.*

Date of Submission: 15-08-2022 Date of Acceptance: 31-08-2022

I. INTRODUCTION

In today's world of technology, security is of prime importance. With the increase in cyber-crime, providing only network security is not sufficient. Security provided to images like the blueprint of company, secret images for the army or company's interest, using different techniques arebeneficial.

There are many techniques to secure images including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography, etc. In this paper, a procedure of encryption and decryption is presented.

Image data have distinct characteristics from text data. The image usually has bigger data size and a prominent level of redundancy as compared to text. In this present era of technology and digitization, for security purposes, image encryption is one of the ways to secure our data from hacking. Also, there are many algorithms to encrypt images efficiently using different techniques.

Images are characterized as (i) raster images and (ii) vector images [4]

Raster images are defined as bitmap images, which are made up of bits and pixels. Each bit can be pictured as a dot which is defined by the number of pixels per unit of measurement that determines the resolution of the image It is expressed as ppi (pixel per inch) or dpi (dots per inch).

Vector images are mathematical arrangements of points, where each point is connected by mathematical formulations. Most of the images are connected by straight lines.

The digital image is a collection of digital images called elements represented by the 2D matrix. Every color image consists of three planes: RGB (i.e., Red, Green, and Blue). During encryption, the image splits into small pixels. Encryption takes place by scrambling or arranging the pixel and then each bit of image XOR with the key which is generated by using a Gauss map and Linear Feedback Shift Register (LFSR) [4].

II. LITERATURE REVIEW

Rohith et.al. [3](2014) proposed a technique for image encryption and decryption using key sequence generated by the sequence of logistic map and sequence of states of LFSR. Their algorithm wasextremely sensitive to the initial value of "X_0" and the initial state of LFSR. Two 8-bit grayscale images were chosen for performance analysis of the algorithm. The results show that original and encrypted image were highly uncorrelated and perceptually different. The histogram plotted by the encrypted image was uniformly compared to encrypt using only a logistic map. It was also demonstrated that using the wrong key to decrypt an image result in a completely different image. Both the suggested and logistic map methods computed correlation, entropy, and mean square error between the original and encrypted image. It was discovered that encryption performs cryptographically better than encryption using a logistic map approach and offers the image with higher security.

Bangar et.al. [1] (2016) projected a technique for data and image encryption using the AES 256-bit algorithm for cryptography, image steganography, and image security. In the communication system, the image

which is sent was broken down into parts and encrypted individually and sent over the network. It became difficult for the hacker to get access to all the parts. Thus, the hacker cannot access the encrypted image. As a result, they raised the security of an image for transmission over a network unto$n$ times.They were increased by$2n$ times instead of one in a single information transmission. Higher the number of split blocks indicates more secure information.

Sahay et.al. [4](2017) demonstrated a procedure for color image encryption using Gauss iterated map. They show that the Gauss iterated map provides better security as compared to the logistic map. Also, they proved that for encryption and decryption, time taken by the Gauss map was less than the time taken by the logistic map. So, they concluded that Gauss iterated map performed better than the logistic map. Also, they mentioned that in future, this encryption technique can be extended to higher dimensions and can be applied in the field of watermarking.

Rahmawati et.al. [2] (2019) projected research on image compression and encryption put in on the structure. The compression conducted using DCT resulted in an excellent compression ratio that was 4 to 5 times smaller than the original size. While the chaos-based encryption, Gaussian map was carried out that resulted in cipher image. This result withstood the histogram analysis attack since it resulted in cipher image in which the histogram had a completely different pattern with the original image histogram.

III. TERMINOLOGY

ChaoticMap [3]

"Chaos" means "a state of disorder" which is studies on the behavior of dynamical systems. This is extremely sensitive to initial conditions. The butterfly effect is a popular term for a response. Small variations in initial conditions, such as those caused by rounding errors in numerical computation, result in sequences that are highly uncorrelated. This happens even though these systems are deterministic, indicating that their powerful proof is totally determined by their original conditions, with no random factors involved. To put it differently, these systems are unpredictable due to their deterministic nature. This behavior is known as deterministic chaos, or simply chaos.

It exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Chaotic maps often occur in the study of dynamical systems.

It is useful to ensure security. It has the properties like deterministic, easy to generate and difficult to estimate. Gauss map is a type of chaotic map which also generates a pseudo-random number which is used in this paper.

GaussMap[4]

Gauss map is also called a Gaussian map or Mouse map. It is a nonlinear iterated map of the realsintothereal interval as given Gaussian function:

$$X_{n+1} = e^{-\alpha X_n^2} + \beta$$

where α and β is the input parameter that will significantly affect the Gaussian map results.
This map uses more controlled parameters as compared to another chaotic map, which enhances the data security. Also, it takes lesser time for encryption and decryption.

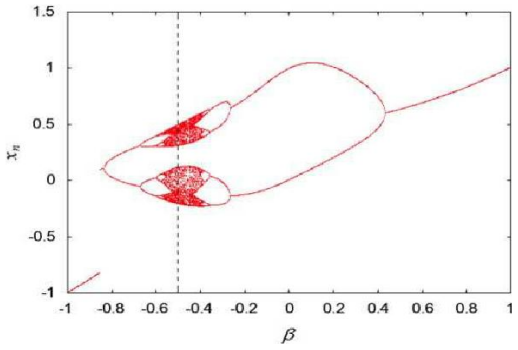

Figure 1: Gauss Map

This map shows the best result when the value of ∝ has some positive value that lie between $+1$ to $+6$ and valueβ lies between -1 to $+1$. The bell-shaped Gaussian function map is like the logistic map. Fig. 1 shows the Gaussian map with $\alpha = 4.9$ and $\beta = -1$ to $+1$ which resembles a mouse, which is why it is also called a

mouse map. There is a different map with a different value which shows that a slightchange in thesetwo parameters makes a momentous change in the solution of the system.
Choosing ,α,β,X_0a chaotic sequence $\{X_i\}$using the gauss map is generated with X_0 as the initial value. The chaotic sequence$\{X_i\}$is transformed into an integer in the range of 0 to 255 by multiplying the sequence elements X_i with 255.Round of the $X_i$value to the nearest decimal value. The generated sequence is intern converted into a sequence of 8-bit binary and which is used in the generation of key sequences. This sequence is referredas$\{K_1\}$.

$$K_1 = \text{Round}\,(X_i * 255)$$

Linear Feedback Shift Register (LFSR) [3]

LFSR method, for image encryption, produces random numbers used to the reorder position of the image pixels. The initial value will generate random numbers to reorder the position of each pixel in the row of the image in the first encryption process and each pixel in the column in the resulting image of the first encryption process.

An m-stage linear feedback shift register (LFSR) is characterized by feedback polynomial of degree-m over GF (2), if the feedback polynomial is primitive the sequence of states generated is periodic and is of period $(2^m - 1)$.Here, $m = 8$.There are 255 possible initial states. Each initial state generates a periodical sequence of states of periodic the sequence of states of the period$2^8 - 1 = 255$. The sequence generated with different initial states are shifted versions of each other.

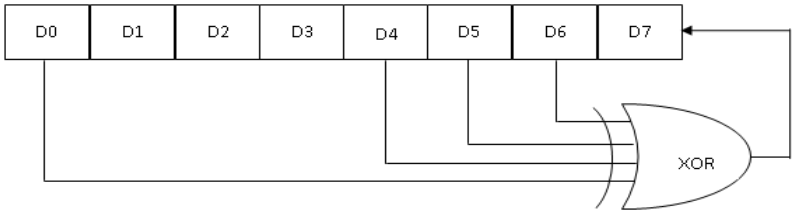

Figure 2: Linear Feedback Shift Register

In the purpose scheme sequences of 8 bit are used for generating key sequences. This sequence is denoted as$\{K_2\}$.

IV. PROPOSED WORK

Encryption Algorithm

Step 1: Choose the RGB image of size $M \times N$ pixels converted array of pixel $P = \{P_1, P_2, \ldots, P_n\}$, where i 1,2,3 ... . n and

$$n = M \times N.$$

Step 2: Bit by bit XOR operation is employed between generated sequences $\{K_1\}$ which are generated by Gaussmap and$\{K_2\}$
which isgenerated by LFSR using by $\{K_1\}$ to obtain final key sequence $\{K_i\}$.

$$K_i = K_1 \oplus K_2$$

Step 3: The RGB image pixels P_i are XORed with key sequence $\{K_i\}$ to obtain encrypted pixel $\{C_i\}$.

$$C_i = P_i \oplus K_i$$

Step 4: Repeat step 3 to encrypt all image pixels. Transform all encrypted digits $C'_i = \{C'_1, C'_2, \ldots, C'_n\}$ into anarray of size
$M \times N$ toobtain the encrypted image.

Decryption Algorithm

Step 1: Encrypted RGB image of size $M \times N$ pixels is transformed into array of pixel $C'_i = \{C'_1, C'_2, \ldots, C'_n\}$,where i =
1,2,3 ... . n and$n = M \times N$.

Step 2: The key sequence $\{K_i\}$ is obtained by $\{K_1\}$ and $\{K_2\}$ as defined in (3) is used to decrypt the image. Theobtained block of
decrypted 8-bit $\{D'_i\}$is converted into decimal digits and called as $\{D'_i\}$.

$$D'_i = C'_i \oplus K_i$$

Step 3: Array of decrypted pixels $D_i = \{D_1, D_2, \ldots, D_n\}$ of size $M \times N$ to obtain the decrypted image.

V. EXAMPLE

For the experimental results analysis, an image ('LENNA 64x64 image.png') is chosen of size 64 x 64 as shown in below Fig. Then generate a random number sequence using gauss map equation by taking$\alpha = 5.67, \beta = -0.567, X_0 = 0.231$.

Figure 3: Original Image

Encryption Process:

Step 1: An 8-bit RGB image of size M × N pixels:

```
(([[[230  132  107]      [204  101  105]
Array  [226  129  110] ... ... [178   86  107]
       [224  132  111]      [106   27   59]]
                  ... ....
        [[111   69   81]      [168  93  114]
        [220  166  179] ... ... [141  69   93]
        [210  144  146]      [106  37   65]]])
```

dtype = uint8

Step 2: For $\{K_1\}$ key which is generated by gauss map and multiply by 255 then choose a high value for $\{K_1\}$ key:

0.17192646431597913 gauss array: 43.84124840057468

0.27869383606564035 gauss array: 71.06692819673829

0.0767850758960249 gauss array: 19.58019435348635

... ...

0.14291168097724416 gauss array: 36.44247864919726

0.32365097206476523 gauss array: 82.53099787651513

−0.014848175557950705 gauss array: − 3.78628476727743

0.43175072563408234 gauss array: 110.09643503669099

The high value is 110. It converts in binary 01101110 which is $\{K_1\}$ key.

For $\{K_2\}$ key using LFSR, m = 8 chosen with polynomial $x^8 + x^6 + x^5 + x^4 + 1$.there are 255 possible initial states. Each initial state generates periodic sequence. States of 8-bit are used generate key sequence is called $\{K_2\}$ key which is 11011101.

$$K_i = K_1 \oplus K_2$$
$$K_i = 01101110 \oplus 11011101$$
$$K_i = 10110011$$

Step 3: Check for P_1 pixel which is 230 converts in binary 011100101 XOR with K_i (=10110011) it gives01010101 which is value ofC_1 .

$$C_1 = P_1 \oplus K_i$$
$$C_1 = 11100110 \oplus 10110011$$
$$C_1 = 01010101$$

Step 4: Repeat the step 3 to encrypt all image pixels. Transform all encrypted digits $C'_i = \{C'_1, C'_2, \ldots, C'_n\}$ into anarray of size
$M \times N$to obtain the encrypted image.

Figure 4: Encrypted Image

Decryption Process
Step 1: Encrypted RGB image of size $M \times N$ pixels is transformed into array of pixel $C'_i = \{C'_1, C'_2, \ldots, C'_n\}$.
Step 2: For decrypted image, C'_1 (=01010101) XORed with K_i $(= 10110011)$ it gives 11100110 which is value
ofD$_1$.

$$D_1 = C_1 \oplus K_i$$
$$D_1 = 01010101 \oplus 10110011$$
$$D_1 = 11100110$$

Convert D_1 in decimal which is the P_1 value.
Step 3: Array of decrypted pixels $D_i = \{D_1, D_2, \ldots, D_n\}$ of size $M \times N$ to obtain the decrypted image.

Figure 5: Decrypted Image

VI. RESULT AND ANALYSIS

For the analysis purpose, the parameter NPCR (number of pixels change rate) is used. NPCR focus on the percentage of different pixels between the original and encrypted image. Higher value of NPCR is appreciated for an efficient encryption procedure, which is our goal. The calculations of NPCR parameter are shown below:[5]

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100 \; D(I,J) = \begin{cases} 0, & I_o(i,j) = I_{ENC}(i,j) \\ 1, & \text{Otherwise} \end{cases}$$

By using the python tool, it gives the 100% difference between the original images. By comparing original and encrypted images, the encrypted image is 99.95% different compared to the original image. The white dot indicates the similar pixel value of original image and encrypted image.

Figure 6: Comparison between Original Image and Encrypted Image

Hence, Gauss map consumes less time to give result with high security. The Encryption took 3.9475000001232274e-05 sec and the decryption took 36.044229017999996 sec.

Comparison [5]

On comparing RSA algorithm with LFSR applied on digital image and Gauss chaotic map with LFSR applied on RGB image:

Type of image	RGB image	Digital image
Image form	Input image: .png Output image: .png	Input image: .jpeg Output image: .png
Generation of key	Chaotic Gauss map+ LFSR	RSA Algorithm+LFSR
Comparison between original & encrypted image	99.95%	99.88%
NPCR	100%	100%
Time taken for encryption	3.9475000001232274e-05 sec	0.019 sec
Time taken for decryption	36.044229017999996 sec	4.109375 sec
Strength	Gauss map produces a disordered key LFSR produces random and secure key	RSA algorithm produces a strong public key LFSR produces random and secure key
Limitation	Randomness of the key depends on the value of α and β	Strength of algorithm depends on the selection of the prime numbers

The above table shows that RSA algorithm with LFSR works better than the Gauss map with LFSR digital image.RSA+LFSR algorithm takes less time for encryption and decryption as compared to Gauss map+ LFSR.

VII. CONCLUSION

The key utilized for image encryption and decryption in this paper was produced using a Gauss map and Linear Feedback Shift Register (LFSR). The suggested approach is extremely sensitive toX_0's beginning value and the LFSR's initial state. A gauss map generates the first key, and LFSR uses the first key to generate the second key. Then both keys are XORed together to produce a strong key, which is the final key. As a result, the hacker will have a tough time guessing that key. As a result, if the wrong key is used (a slight difference in the beginning value of $'X_0'$ in the Key sequence), the image will be radically different.

The results show original and encrypted image is highly uncorrelated and perceptually different. Gauss map uses more controlled parameters as compared to another chaotic, which enhances the data security. Thus, the presented algorithm is efficient and secure. The result has been calculated using PYTHON.

REFERENCES

[1]. Bangar, S. S. (2016). Security of Image Processing Over a Network.
[2]. Rahmawati, W. M., & Liantoni, F. (2019). Image Compression and Encryption Using DCT and Gaussian map. InIOP Conference Series: Materials Science and Engineering (Vol. 462, No. 1, p. 012035). IOP publishing.
[3]. Rohith, S., Bhat, K. H., & Sharma, A. N. (2014, October). Image encryption and decryption using chaotic key sequence generated by a sequence of logistic map and sequence of states of Linear Feedback Shift Register. In 2014 international conference on advances in electronics computers and communications (pp. 1-6). IEEE.
[4]. Sahay, A., & Pradhan, C. (2017, April). Gauss iterated map based RGB image encryption approach. In the 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 0015-0018). IEEE.
[5]. Srushti, G., and Gor, R. (2022). Digital Image Encryption using RSA and LFSR. International Journal of Engineering Science Technologies, 6(4), 1-16. doi: 10.29121/IJOEST.v6.i4.2022.351
[6]. Thakkar A. and Gor R. (2022), "Cryptographic method to enhance the Data Security using RSA algorithm and Kamal Transform", IOSR Journal of Computer Engineering (IOSR-JCE), 24(3), 2022, pp. 01-07
[7]. Yau, H. T., Pu, Y. C., & Li, S. C. (2012). Application of a chaotic synchronization system to secure communication. Information technology and control, 41(3), 274-282.