International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-6, Issue No.-6, November, 2018

A Systematic Image Encryption Technique using chaotic key sequence generated by Logistic Map and Random shuffling using stream cipher algorithm

Salil Bharany 1st
MTech Student, Department of Computer Engineering and Technology, GNDU
Amritsar, India
E-mail: salil.bharany@gmail.com

Prabhpreet Kaur 2nd
Assistant Professor, Department of Computer Engineering and Technology, GNDU
Amritsar, India
E-mail: prabhpreet.cst@gndu.ac.in

Abstract: Immense research has been going on with cryptography as the base. It's not about anything new it's just an intelligent communication without others getting to know about it. Encryption is more popular then Steganography and watermarking as it doesn't give a single data and differs from the initial image as its has redundancy and bulk of data capabilities as well support all types of digital files. other image encryption techniques likes AES,DES,RSA etc exhibit very weak security and weak anti-attack ability.. As an exchange of data through the internet, we have proposed a new method for encrypting and decrypting an image by based on chaotic logistic map sequence and random shuffling done by stream cipher algorithm .By using logistic map sequence a random sequence is generated as an array of dimensions of different numbers .Then the RC4 algorithm used for any random shuffling (dependent on the content of an array created by CLM) of the array created by the RC4 first algorithm. Then in the second RC4 algorithm in this cycle, the value of each color is been changed (by using the Array Result of the First RC4 algorithm) Pixel while all the pixels of the image has been changed so the encrypted image is more secure. And when we do that, we create an encrypted picture that is completely different and does not show any information regarding the plain image, suggesting that it is really a significant encryption that cannot easily be decrypted using brute-force or other types of attacks.

Keywords: Affine Transform, chaos based system, Cipher, Confusion and Diffusion, Image encryption, image cryptography, rivest cipher 4, XOR

I. INTRODUCTION

Encryption is being used by ancient Greeks and Romans to send secret messages with are being encrypted by a password Or secret key, although they focused on text only in the beginning, but then they try to implement these encoding and decoding techniques on the other types of multimedia like images, videos, etc. For now, we will focus on images as another example of multimedia protection, on the first years of work they used the same methods that have been used in the text (RSA, AES... etc.). However, those encryption schemes seem to be inappropriate for images because of some image features, such as high capacity, superfluous, and high-pixel correlations. In addition, these code schemes require additional operations on compressing an image data, so this requires a long calculation period and a high computing power In real time transmission significant latency is shown due to a low rate of encryption and decryption. In recent years, cryptographic projects have proposed new and effective ways to develop image encryption security. These schemes have a simple structure that implements changes by permutation and the diffusion stages. However, most algorithms face problems such as lack of stability and security [1]. In 1989[2] Chaos-based cryptographic graphical system is been introduced as an effective encryption. Chaos-based is used to hide digital information during transmission. It has many other features besides other algorithms, such as sensitive dependence on initial conditions, not period, exclusion, non-convergence and control parameters. The dimensional chaos system provides simplicity and high security and lot of studies are carried out which suggest to accept and approved it. One of the advantages of using chaotic system is its sensitivity means while having a change of bit will produce totally different cipher and leads to produce confusion and diffusion .In this article, we provide a digital encoding scheme based on RC4 stream cipher. RC4 is a simple algorithm, although there are some weaknesses as shown in fig [3] and [6], but will be integrated with the chaotic system to make it virtually impossible to break. We use the key generator used by [4] to divert the key to the initial value, then we use this initial value on the Logical Map Chaotic (CLM) function to generate the random number order. Which was then added to 256 Standard byte streams and modulo 256 when encryption was created (or by adding 256 to the encoded byte stream cipher, taken out of the pseudo-random number and removing module 256 when processing the decryption process). Image Encryption using Affine Transform and XOR by Amitava Nag: In this proposed algorithm there is 2-step encryption and decryption process in which affine transformation and then XOR operation is performed. The value of pixel of image is being redistributed to other location using a transformation with 8-bit keys. Block of 2*2 which we get by dividing the image into blocks (2*2) and then encoded with the XOR operation via four 8-bit key [10]. The total key size used in the algorithm is 64 bits. In this we can consider the result after transition and the relationship between pixels value is highly reduce-able.

Image Encryption and Decryption Using Blowfish Algorithm in Matlab[11]: Encrypting and Decrypting Images Using a

secret-key Block called 64 Bit Blowfish are considered to enhance security and increase productivity. This
the algorithm is used as a significant 448-bit key size. It uses the Feistel network in which a simple function is repeatedly used 16 times to enhance security. The algorithm is safe and highly secure against unauthorized attacks. The proposed algorithm was designed and implemented using MATLAB. So, if the number of iterations increases the algorithm becomes stronger. Since Blowfish has been known to be less and don't have any valid issues, it can be considered a perfect standard encryption algorithm.

A Keyless approach to Lossless Image Encryption [12]: This method uses a "no key" method optimized for image encryption without lossless of the RGB image by the other three methods to encrypt images: encrypted keys, split images, and multiple shares. This method increases security and increases storage capacity with SST technology. In this, the security is enhanced as to increase in dividing a bit more pixels over the image. The quality of decrypted is maintained using the keyless approach as it leads to maintain the originality of image.

Image Encryption using CAT Mapping and Chaos Approach: An Approach which uses CAT Mapping for achieving image discretization. This method uses regular changes to achieve image encryption. Different image sizes can use different encryption cycles for encryption. This encryption method has the ability to effectively encode by placing the best parameters to achieve the best encryption of the image. Sensitivity analysis has shown that this approach has the ability to scrambling pixel coding, image manipulation, and change. For encrypted security, this method is highly variable to the text which may attribute to handle the plaintext attack under different situations [13].

A robust image encryption algorithm resistant to attacks and chaotic logistic map: by using DNA (Deoxyribonucleic acid) operations and chaotic maps and encryption method is constructed [14]. The first step to DNA encodes and a mask is generated by using one-dimensional chaotic map, afterward, a mask is being added with the DNA encoding using DNA addition with the help of matrix permutation using 2d chaotic map the mean result is DNA complemented and then converting DNA to encrypted images.this technique is totally invertible and has the power to resist text and statistical attacks.

II. REALTED WORK

Many attempts have been made in the past to encrypt digital images. In [21] [22], they use two CLM functions, in which the first CLM is used to generate 24 pieces of real numbers which is then converted into integer form. Furthermore, 24 pieces of an integer are used to generate initial value and for the second CLM, which is used to perform image encryption process. Different approaches tend to do in [23], where they use a combination of CLM function and the genetic algorithm to encrypt the digital color image. CLM is used to generate 4 pieces of chaotic sequences which is then converted into 4 pieces of keystream. The generated key streams are then used to control the process of crossover and mutation. The use of CLM function is also used by [24], the combination of cipher block chaining (CBC) method and the CLM function is used to encrypt the image. The main idea is doing encryption on 4-bit of the most significant bit (MSB) at each pixel and then operate them in CBC mode.

The rest of the paper is organized as follows: on section II, we will explain our proposed algorithm with some examples to see how it works, after that we will make some tests to prove that this proposed algorithm has robust security this will be in section III, then the last section will be the conclusion section.

III. PROPOSED IMAGE ENCRYPTION SCHEME

In this, encryption and encryption of image are done by using chaotic key sequence generated by logistic map and random shuffling done by RC4.Chaotic maps are very nonlinear dynamic system which is very complicated and used in encryption because they are very much sensitive to the initial condition and capable of generating good pseudorandom sequences. Chaotic systems have certain properties such the sensitive dependence on initial condition and system parameters: non periodicity and topological transitivity .there are lots of chaotic based encryption schemes have been proposed and use a different type of chaotic maps. RC4 is stream cipher which provides byte-oriented operation and flexible key size. Basically, this algorithm is based on random permutation. It has been discovered that the algorithm has an overwhelming period of probably >10100 and the output byte requires 8 to 16 machine operation which makes hard to crack A key having the variable length of 1 to 256 bytes can be used for initializing a 256-byte state vector S ,having elements S[0],S[1]….S[255]. Output produced from S is a byte by selecting one of the 255 entities in a systematic way when each K value is generated; the entries in S are permutated once again.

First Stage: CLM In the first step, we take a key "owner key" which is 16 characters long, then it is converted to it hexadecimal equivalent and them it reaches to CLM block.
The goal of image encryption is being achieved by employing the chaotic logistic map.

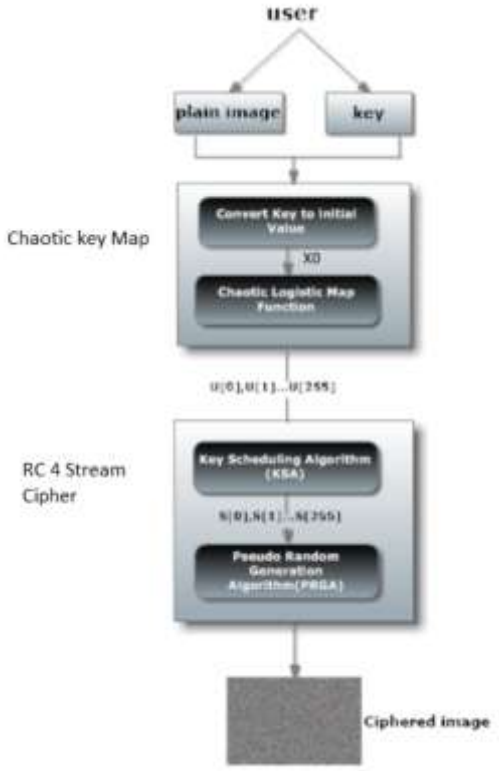


Fig 1 Proposed Image Encryption

$$X_{n+1} = \lambda . X_n (1 - X_n) \quad (1)$$

In this we take (i.e. $\lambda = 4$) as it is the system constant of which leads to highly chaotic case .With the help of logistic map we calculate the initial condition X0 with the following equation

$$X_0 = (X_{01} + X_{02}) \bmod 1 \quad (2)$$

To find (X_{01} and X_{02}) we need to split the external key into two groups G0 and G1. By using these two groups, the real numbers X_{01} and X_{02} can be calculated using equations (3) and (4)

$$X_{01} = (k_0 * 2^0 + \ldots + k_{15} * 2^{15}) / 2^{15} \quad (3)$$

$$X_{02} = (k_{16} * 2^0 + \ldots + k_1 * 2^{15}) / 2^{15} \quad (4)$$

By CLM equation is used by the initial value to generate an array of pseudo random numbers. Generally, the chaotic process uses initial value X_0 to get X_1, then X_1 value will be used to get X_2, and so on.

After obtaining each X_n value, we multiply it by image width and divide the result by image height. Then the result would be converted into integer, which is done by taking eight[1] points starting after decimal point of the real numbers. For example, if we take value of X_n after multiplication and division is *0.987654321* the result after conversion is *987654321*.

Algorithm 1: Initial Permutation
INPUT: Array S of integers in ascending order, Array U produced by CLM **OUTPUT:** Permuted array S

```
1. j ← 0;
2. For i ← 0 to 255
3.    j ← (j + S[i] + U[j]) mod 256;
4.    SWAP(S[i], S[j]);
5. End for
```

Algorithm 2: Pseudo-Random Generation Algorithm (PRGA)
INPUT: Permuted Array S
OUTPUT: Integer value between 0 and 255

```
1. i ← 0; j ← 0;
2. While ()
3.    i ← (i + 1) mod 256;
4.    j ← (j + S[i]) mod 256;
5.    SWAP (S[i], S[j]);
6.    t ← S[(S[i] + S[j]) mod 256];
7. return (t);
```

Stage Two: RC4 stream cipher

1) As a first step in RC4 algorithm, an array called "*S*" is created. Where the content of it are set equal to the values from 0 through 255 in ascending order; such as, S[0]=0, S[1]=1, …, S[255]=255.

2) In further step, initial permutation of array *S is produced* array *U*. For each *S[index]*, swap *S[index]* with another byte in *S* according to the content of *U[index]*, and other parameters (for better clarification, see algorithm 1). This will cause the content of *S* still contains all the numbers from zero through 255.

3) By using PRGA , Streams generation is done, and then swapping *S[index]* with another byte of *S* is do

Algorithm 3: Image Encryption
INPUT: Image, key
OUTPUT: Encrypted image

```
1.  For i ← 0 to Image Width -1
2.      for j ← 0 to Image Height -1
3.          Get pixel
4.          t ← PRGA
5.          R ← (pixel. RED + t) mod 256
6.          t ← PRGA
7.          G ← (pixel. GREEN + t) mod 256
8.          t ← PRGA
9.          B ← (pixel. BLUE + t) mod 256
10.         Set pixel ← (R, G, B)
11.     end
12. End
```

During the decryption process (Algorithm 4) adding of 256 to each byte of RGB is done then after this deducted from the output generated by the step three (PRGA) and then the result would be modulated by 256, this is also repeated to the other channels and to the rest of the image pixels values.

Algorithm 4: Image Decryption
INPUT: Ciphered image, key
OUTPUT: Plain image

1. **For i ← 0 to Image Width -1**
2. **for j ← 0 to Image Height -1**
3. Get pixel
4. t ← PRGA
5. R ← (pixel. RED + 256 - t) mod 256
6. t ← PRGA
7. G ← (pixel. GREEN + 256 - t) mod 256
8. t ← PRGA
9. B ← (pixel. BLUE + 256 - t) mod 256
10. Set pixel ← (R, G, B)
11. **end**
12. **End**

S	S'
0	154
1	67
2	232
3	229
4	92
5	11
6	141
7	176
8	174
9	207
10	6
11	19
12	177
13	34
14	79

(Algorithm 3) In this for every RGB channel the output of the last step to one of the channel value and afterward the modulo 256 is taken .This process is execute again and again for other channels and pixels..

While the decryption (algorithm 4) process is done by adding 256 to each byte of the RGB and subtracts it from the outcome of 3rd step and after it that would be modulated by 256 ,This process is execute again and again for other channels and pixels

IV. EXPERIMENTAL RESULTS

In this area, results of the new proposed encryption algorithm are here. Our encryption system works on both color and grey images with different sizes and image formats, however, the speed might vary with image size. By applying the algorithms above, we get the results in Table 1 and Figure. 2, which shows the keystream generated by chaotic logistic map, and some values of the initial condition.

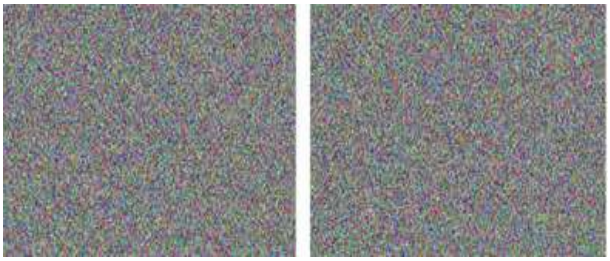
X	U
0.2061767578125	20617676
0.654671609401703	65467161
0.904306772980348	90430677
0.346144133288869	34614413
0.905313489114266	90531349
0.342883902168078	34288390
0.90125812720828	90125813
0.355967661397216	35596766
0.917018741746452	91701874
0.304381476128822	30438148
0.846933572473846	84693357
0.518548385162139	51854839
0.998623829631508	99862383
0.00549710609443652	549711
0.0218675516760921	2186755

Initial value generated X by use of the secret key and logistic map ,U is an array which is being produced from the initial value .S is initial array generated by KSA and S' is permutation produced by KSA .

V. SECURITY ANALYSIS

A encryption system should be secure and robust enough to handle all kinds of attacks In this section, to evaluate the efficiency of the new proposed algorithm different parameter are checked were to prove its robustness.

A. Key sensitivity analysis effective encryption algorithm should be sensitive with respect to key that means if an alteration of single bit is done in the key it will definitely create a different encrypted image [5] ,[7] . lets take a key "shdfhdhefoeuabhd" and the decrypted the cipher-image using another key which is different from first one with a single bit "shdfkdhefoeuabhd" . the result will be totally different from the original image .from the result shown it is clear that the decryption done with a key which is single bit different is producing different result and leads to high key sensitively.



A) *B)*

(c)

A. Key space analysis

In this encryption depends entirely on the secret keys means how much secure is key to be cracked and more large space for key leads to the more secure key. Large key space for key makes the brute force attack hardly possible .From the keyspace we are able to get a different pattern of keys . in our proposed image cipher there are 2128 different combinations hence not possible to have any kind of brute force attack.

B. Histogram analysis

An image-histogram is basically the representation of pixels at each color intensity level which is being distributed by graphing the pixels of an image. In order to have an idealistic ciphered image in histogram's sight of view, the histogram of the image must have the parallel distribution of pixels with the color intensity value. By analyzing histogram for the images in Figure. 4a, and Figure. 4b, We have seen in the histogram of each RGB channel is uniform and significantly different from the other histograms of the original image, and so it does not give any hint to employ

(a) Original image

(b) Encrypted Image

Figure 3. Key sensitivity analysis (a) ciphered image using specific key, (b) deciphered image using different key and (c) deciphered image using the correct key

whatever attack on the proposed image encryption procedure.

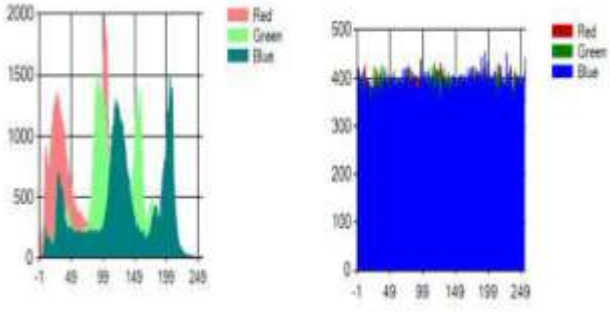


Figure 4. Histogram analysis (a) plain image, (b) ciphered image, (c), and (d) arehistograms of plane and ciphered image, respectively

VI. CONCLUSION

In this paper, we proposed a new encryption method based is one of the best chaotic logistic maps and RC4 fusion algorithm method .we just tried a better algorithm in respect to its security, robustness, and efficiency. it is basically developed to send an image on the internet without having any worry of information leak and also one of the important features that are key sensitivity and having on a chance of any brute force attack on it.

REFERENCES

[1] S. Ahadpour, Y. Sadra, Z. ArastehFard, "A Novel Chaotic Encryption Scheme based on Pseudorandom Bit Padding", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 1, No 2, January 2012.

[2] Y. Hashemi, "Design A new Image Encryption using Fuzzy Integral Permutation with Coupled Chaotic Maps", International Journal of Research in Computer Science, Vol. 3 Issue 1, 2013.

[3] http://imchris.org/crypto/html/ch07.html

[4] N.K. Pareek, Vinod Patidar, K.K. Sud, "Image Encryption using Chaotic Logistic Map" in *Image and Vision Computing*, Volume 24, pp. 926–934, 2006.

[5] Y. Wu, J. P. Noonan, S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.

[6] M. A. Orumiehchiha, J. Pieprzyk, E. Shakour, R. Steinfeld, "Cryptanalysis of RC4 (n, m) Stream Cipher", SIN '13 Proceedings of the 6th International Conference on Security of Information and Networks, pp. 165-172, 2013.

[7] K. Sakthidasan, B. V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology (IJIET), Vol. 1, No. 2, June 2011.

[8] N. K. Telem, C. Segning, G. Kenne, H. B. Fotsin, "A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network", Hindawi Publishing Corporation, December, 2014.
[9] Rasul Enayatifar et al(2011)" Image Security via Genetic Algorithm", International Conference on Computer and Software Modeling IPCSIT vol.14
[10] Amitava Nag et al (2011)"Image Encryption Using Affine Transform and XOR Operation", InternationalConference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)
[11] Pia Singh et al (July-2013) "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7.
[12] P. S. Ghode, (May 2014) "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE.), vol. 4, Issue. 5, pp. 1459- 1467.
[13] W. Zhu, (2014) "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8.
[14] A. Jain et al (February 2015) "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimedia Tools and Applications, An International Journal, Springer Science + Business Media Ne Yourk, pp. 1-18.
[15] D. P. Tian et al (2013) "A Review on Image Feature Extraction and Representation", Techniques International Journal of Multimedia and Ubiquitous Engineering, vol. 8, no. 4, pp. 385-396.
[16] Sonal Paliwal et al,(June 2016)"A survey on various Text Detection and Extraction technique from videos and images". IJCSEITR
[17] Bhomika Pandey et al, "A Comprehensive study on text and image stenography", IJETTCS, February 2016.
[18] Navneet kr. Kashyap et al, (may 2016)"Analysis of pattern identification using graph database for fraud detection",, OJCST.
[19] Poonam Singh et al (Sep 2015)" Performance analysis of image and video coding by Wavelet Transform Using Region of interest", IJERMT.
[20] Dixcha Gusain et al, (January 2016) " Comparative analysis of filters for extraction from noisy images", IJESRT.
[21] Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin," A Survey on Principal Aspects of Secure Image Transmission",World Academy of Science, Engineering and Technology 66 ,2012, pp 247 – 254.
[22] Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, A New Chaos-Based Image-Encryption and Compression Algorithm", Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012, Article ID 179693
[23] K.Sakthidasan Sankaran and B.V.Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of information and Education Technology, Vol. 1, No. 2, June 2011.
[24] Hazem Mohammad Al-Najjar, Asem Mohammad AL-Najjar," Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table".
[25] K. Kushwah, S. Shibu, "New mage Encryption Technique Based on Combination of Block Displacement and Block Cipher Technique," International Journal of Computer Science and Information technologies vol 4,no 1,pp61-65,2013
[26] P.Junwale, R.M Annapurna and G.Sobha "A Review on image encryption technique based on hyper image encryption algorithm ,IJARCSCE ,vol 3 no 11,pt 614-618

AUTHOR'S BIOGRAPHIES

Salil Bharany 1st , Mtech Student, Department of Computer Engineering and Technology ,GNDU , Amritsar, India salil.bharany@gmail.com

Prabhpreet Kaur 2nd Assistant Professor , M.Tech, Pursuing Ph.D ,Department of Computer Engineering and Technology ,GNDU ,Amritsar, India , prabhpreet.cst@gndu.ac.in

.