IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, Mar 2019 E-ISSN: 2347-2693

A Modified Image Encryption Technique Using Two Dimensional Sine Logistic Map

Subodh Kumar[1], Rajendra Kumar[2*]

[1,2]Dept. of Computer Science, Jamia Millia Islamia University, Delhi- India

**Corresponding Author: subodhkumar588@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.11101115 | Available online at: www.ijcseonline.org

Accepted: 24/Mar/2019, Published: 31/Mar/2019

Abstract: A color image Chaotic systems are commonly used in cryptosystems because chaotic system is very sensitive to initial conditions and also have the property of unpredictability as well as ergodicity. We have modified the two dimensional logistic sine map. This modified two dimensional sine logistic map enhanced the unpredictability and ergodicity. It also enhances the range of chaotic map. With the help of this modified two dimensional sine logistic map image encryption is performed. In the proposed technique confusion and diffusion both operations are performed, further to enhance the security level random values are added to the original image. With the help of simulation results and analysis of security, it can be proved that modified two dimensional sine logistic map can encrypt several types of images. The proposed algorithm also has the ability to resist from different types of attack.

Keywords: Chaotic Logistic map, XOR operation, Modified Sine Logistic Map System

I. INTRODUCTION

Many applications used in every aspects of daily routine have attractive features and easily understandability [1]. Unauthorized users or attackers can easily gather significant data from image during transmission over internet. Therefore, numerous research groups are working in this domain because security of images is very important. Sensitivity and randomness fulfill the need for a better cryptographic system. Both randomness and sensitivity concern is better improved by the chaotic based encryption techniques. In recent chaotic theories, pseudo random numbers were generated using one dimensional chaotic map. It was not capable to counterattack. The iteration time was more. Several research groups have made the significant contribution in the recent years to tackle these issues. Researchers introduced the complex chen system, complex Lorentz system [2], chaotic Logistic map, diffusion, permutation, XOR, three dimensional cat map system [3], fusion of maps [4] and some ancient algorithm. Xu, Li and Hua developed a technique using a bit level chaotic map [5]. Atta Ullah et.al developed a technique using substitution boxes [6]. Different cryptographic models for picture encryption utilizing disorderly frameworks have been talked about in [7]. Guo et al. [8], He Y et al. [9], Kurths et al. [10] and Ravichandran et al. [11] as of late anticipated a few encryption plans utilized various encoding techniques using different DNA sequence activities. Numerous other presented different strategies for Fourier [12], discrete wavelet [13] and various other new transformations [14,15] for image encryption. Wang et al. [16] uses dna permutation based on the lorenz system for color image encryption. In this model disordered succession relies upon the information plain content picture and mystery encryption keys. The model can without much of a stretch break the bit planes of the plain picture by using the DNA stage and expansion or subtraction tasks. Zhang et al. discussed an image encryption scheme founded on the mlncml system using dna sequences [17]. Zhang, Wang [18] performed analysis and improvement using a bit-level permutation and developed a chaos-based symmetric image encryption scheme. Liang et al. proposed a chaos-based symmetric image encryption scheme which uses a bit-level permutation. Zhang, Wang. Worked on spatio temporal chaos in mixed linear nonlinear coupled logistic map lattice [20].

Zhang et al. [21], presented a picture encryption conspire utilizing spatio worldly disorder of blended straight nonlinear coupled guide cross section. The discussed model improves the affectability regarding the plain content by using using both DNA and one-time confusion encryption approach and makes the framework resistive against different attacks such as differential attacks, plain text and brute force attacks. Lian et al., for image encryption cryptanalyzed the model based on chosen and known plain text attacks [22,23]. Further, he found that Arnold's Cat map isn't appropriate in cryptography in the event that it is connected straightforwardly in picture encryption and give the spontaneous creation in picture encryption demonstrate utilizing bit-level change. In correlation with one dimensional turbulent frameworks, as of late the reasonableness of spatio fleeting turmoil in coupled guide grid (CML) in picture encryption models including different types of coupling has been examined in [24–25]. CML improves the dynamic properties of a Lorenz system successfully [26-27].

The rest of the paper is organized as: section 2 discussed the proposed encryption technique. In section 3 results are presented. Section 4 gives the conclusion.

II. THE PROPOSED ENCRYPTION TECHNIQUE

We proposed a two dimensional modified sine logistic map. It modifies the pixel based on sorting and mixing of different channels red, green and blue channels. Exclusive-or operation is performed using random number generated from complex Chen and complex Lorentz system.

2.1 Chaotic Logistic map

Chaotic logistic map is basically an equation of second degree. The behavior of chaotic logistic map is derived from the dynamic equations. This equation can be written mathematically as mentioned below:

$$y_{n+1} = ry_n(1 - y_n) \quad (1)$$

Here the range of is between 0 and 1. It basically shows relationship between existing populace to the maximum possible populace. On the other hand, value of r is chosen in the intermission [0,4].

2.2 Sine Logistic map

Mathematically two dimensional sine logistic map is defined as below.

$$x_{i+1} = \gamma(\sin(\pi y_i) + \delta)x_i(1 - x_i) \quad (2)$$

$$y_{i+1} = \gamma(\sin(\pi x_{i+1}) + \delta)y_i(1 - y_i) \quad (3)$$

Here the value of γ is within the range of [0, 1] and value of δ is fixed as 3. This two dimensional logistic map is formed using Sine and Logistic maps. Logistic equation is scaled by using and then output is given to the input of sine logistic map.

2.3 Modified Sine Logistic map

Mathematically two dimensional sine logistic map is defined as below.

$$x_{i+1} = \sin(\pi\, \gamma(y_i + \delta)x_i(1 - x_i)) \quad (4)$$

$$y_{i+1} = \sin(\pi\, \gamma(x_{i+1} + \delta)y_i(1 - y_i)) \quad (5)$$

Here the value of γ is within the range of [0, 1] and value of δ is Using sine and logistic maps. Logistic equation is scaled by using γ and then output is given to the input of sine logistic map. Modified two dimensional sine logistic map has more complicated output in comparison to the logistic map and sine map.

2.4 Trajectory

In case of dynamical systems, trajectory depicts the way of its yields. Fig. 1.1 shows the trajectories of two dimensional logistic map. Fig. 1.2 depicts the trajectories of two dimensional sine map. Fig. 1.3 depicts the trajectories of two dimensional modified sine map. In all trajectories the native values are set as (0.1, 0.2) and parameters are set in such a way that chaotic map could distribute in larger area. It can be seen from figures 1.1, 1.2, 1.3 modified sine map distributed in complete range. It also has larger area in comparison to other maps. so it can be concluded that two dimensional modified sine map shows better ergodicity and more arbitrary.

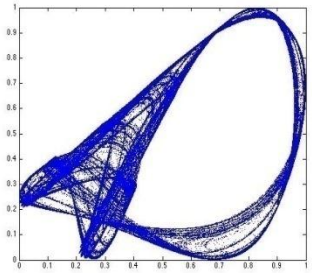

Fig.1.1 Logistic map with parameter *r* =1.19

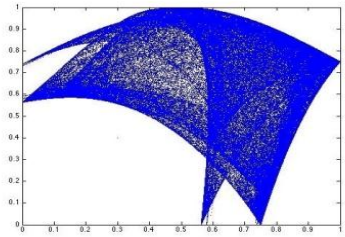

Fig. 1.2 Sine map parameters α = 1, β=3

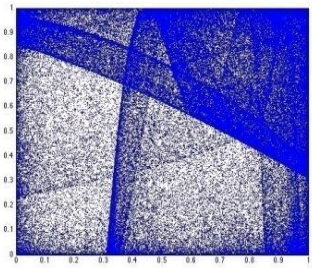

Fig. 1.3 Modified Sine map parameters γ =0.89, δ =3

2.5 Lyapunov exponent

Lyapunov exponent (LE) is used to measure the behavior of chaotic system. Lyapunov exponent (LE) define the degree of divergence in case of two nearby trajectories. When the value of Lyapunov exponent (LE) is positive then difference of the divergence of two trajectory increases in each iteration. so it can be concluded that scheme is chaotic if Lyapunov exponent (LE) is positive [28].

2.6 Kolmogorov entropy

This is basically an entropy which define the randomness of data. Its mathematical definition is given as

$$KE = \text{limit } \tau^{-1} \text{ limit } K_{m,\tau}(\varepsilon), \quad (6)$$

Where $\tau \to 0, \varepsilon \to 0, m \to \infty$, m is the embedding dimension,
$K_{m,\tau}(\varepsilon) = -p(i_1, i_2, \ldots, i_m) \log p(i_1, i_2, \ldots, i_m)$,
Where $K_{m,\tau}(\varepsilon)$ represents the joint probability of correctly predicting the trajectory partition [29].

2.7 Diffusion Process

In encryption technique diffusion method is introduced due to the following reason: firstly, it basically discretizes the chaotic map non-invertible. Second one, it spread the effect of every single bit of the original image over ciphered image [30]. So it can be concluded that diffusion process is essential for a secure encryption algorithm otherwise attacker can disrupt the cryptographic system simply by comparing the pairs of cipher text and plaintext to gather fruitful information. Hence xor with mod operation is introduced in this encryption technique [31-33].

2.8 Proposed Encryption Technique

The basic approach to encrypt the color image is to shuffle the pixel position and hide the pixel value using different techniques. In the proposed techniques we have used multiple approaches. The image of size 256x256 is used to define the encryption procedure. It is six steps process.

Step 1: First of all, a secret key of 232 bits is generated with the help of modified two dimensional sine logistic map.
Step 2: Modified two dimensional sine logistic with the help of secret key generate four chaotic matrices S1, S2, S3 and S4.
Step 3: Arbitrary values are added to the surroundings of original image.
Step 4: Diffusion operation is performed as it changes the pixels' values.
Step 5: Confusion operation is performed as it shuffles the pixels' positions.
Step 6: Step 4 and 5 i.e. diffusion and confusion are repeated four times.

III. RESULTS AND DISCUSSION

Our experiment has been conducted under MATLAB (R2013) in a computer with the Windows 7 Professional (32-bit) operating system. An encryption scheme is contemplate as good if the encryption scheme combats all types of identified attacks.

3.1 Secret key

To withstand from brute force attack, secret key should have in the proposed encryption algorithm, we have used 232-bit secret key that is enough to fulfill the criteria of key space. In spite of having larger key space, secret key must be very subtle in encryption and decryption process, image also be totally different from the original image.

As depicted in Fig. 1.5 below, when original image is encrypted with different keys i.e. K1, K2 and K3 respectively, then obtained encrypted or ciphered images are completely different. Thus it can be concluded that modified sine logistic map is highly perusal to transmute of its secret key. For both encryption and decryption processes, it shows the key sensitivity perusal. K1 is the original key, K2 and K3 are secret key with the difference of one bit, where-

K1=Q12W13E14R56T78Y80U8906IO780PA4321SD6545FGHJ678KLZXCVBNM80,
K2=Q12W13E14R56T78Y80U8906IO780PA4321SD6545FGHJ678KLZXCVBNM81,
K3=Q12W13E14R56T78Y80U8906IO780PA4321SD6545FGHJ678KLZXCVBNM82

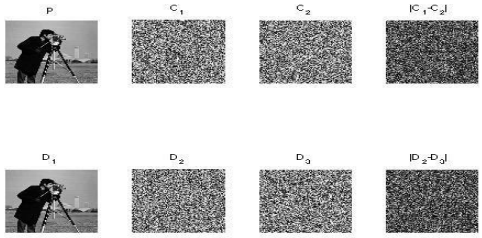

Fig.1.5: Image encrypted and decrypted with same key, with one-bit change key and difference of decrypted images with one-bit difference.

3.2 Analysis to withstand chosen - plaintext and chosen cipher text attacks

There are two different types of security attack models viz chosen plaintext and cipher text attack in cryptographic system. With the help of chosen plaintext attack to encrypt the image and attacker analyze the cipher image or on the other hand with the help of cipher text attack, attacker retrieves the original image. Finally, attacker can easily find a relation between cipher text and plaintext or even attacker can retrieve the secret key if it is not secure enough. In modified sine logistic map specific structure is defined to resist the chosen plaintext and cipher text attack.

3.3 Statistical analysis

Shannon introduced confusion and diffusion to annoy the powerful attacks. Hence statistical attacks can be resisted.

Histograms of encrypted images

Lena image of size 512*512 is selected with several 256 grey-scale images having dissimilar contents. After that their histograms are calculated. Figure 1.6 shows histogram of ciphered image and original image. It can be seen that histogram of cipher image is homogeneously disseminated that is contrary from the plain image or original image.

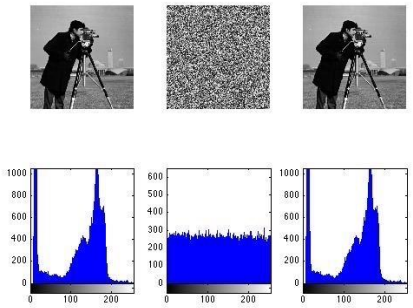

Figure 1.6: Histograms of the plain image and ciphered image

3.4 Analysis for common attacks

When any cryptography algorithm is developed, it is needed to examination its performance by exposing it to dissimilar kinds of attacks. The common attacks that the cipher image may confront are Gaussian, salt & pepper, Poisson and speckle. Gaussian attack is effectuated with zero mean and 0.001 variance. In all cases the image can be procure with decent SNR and SPCC values. The decrypted image before and after the attacks on ciphered image are depicted in Fig. 1.7.

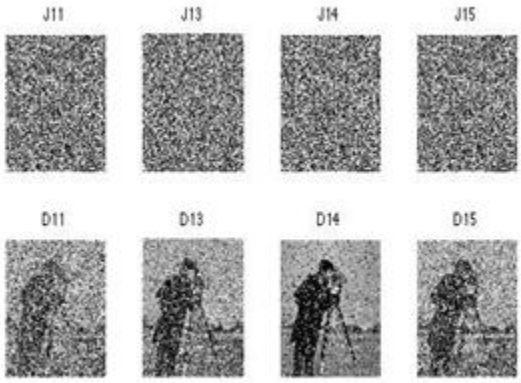

Fig.1.7:a) Gaussian b) Poisson c) Salt & pepper d) Speckle

3.5 Correlation analysis

This is defined as a catalog to quantify the image randomness. In case of plain images adjacent pixels are highly correlated in all courses i.e. horizontal, vertical and diagonal direction. But highly correlated adjacent pixels are more prone to attack. In Order to resist attacks, correlation of adjacent coefficient in horizontal, vertical and diagonal direction should be very less in ciphered image. We selected 1500 pairs of two adjacent pixels arbitrary in all direction.

Correlation coefficient for plain image is close to one on the other hand correlation coefficient for encrypted or ciphered is nearly to zero along all directions. It can be concluded that ciphered image has high randomness. It can be seen in the fig. 1.8 that the dotted points are positioned along the diagonal. It shows high correlation of adjacent pixels of plain image in the all courses but for the encrypted image dotted points are dispersed over the complete plane image. Further table 1 shows the correlation coefficient.

Table 1: Correlation coefficient for Original image and Ciphered image

Orientation	Original Image	Ciphered image
Horizontal	0.9577	0.0015
Vertical	0.9799	0.0015
Diagonal	0.9421	0.0027

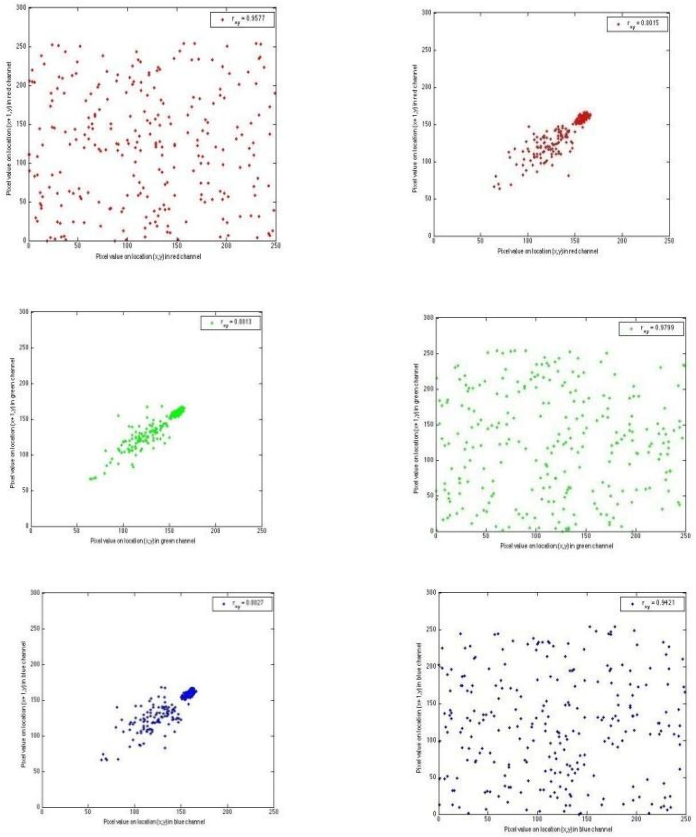

Fig. 1.8 Correlation of red, green and blue channel in original and in cipher image

IV. CONCLUSION

In the proposed work an innovative two dimensional modified sine logistic map has been developed. It is developed with the assist of logistic map and sine map. Then phase plane is comprehended from one dimension to two dimension. Trajectory, Lyapunov exponent and Kolmogorov entropy were evaluated to prove the ergodicity, extended chaotic range and unpredictability. Using two dimensional modified sine logistic map , an image encryption technique is developed. It basically has three main steps i.e. addition of pixels, diffusion and confusion. The addition of pixels to the original image results into different ciphered image. Four times diffusion and confusion is applied to support the diffusion and confusion. Security analysis and simulation results proved that modified sine logistic map can encrypt several types of images into higher security level.

REFERENCES

[1]. Zhou et.al, A novel image encryption algorithm based on chaos and Line map, Neurocomputing (2015)150-157.

[2]. Lu Xu, Zhi Li, Jian Li and Wei Hua, A novel bit level image encryption algorithm based on chaotic maps, optics and Lasers in Engineering (2016) 17-25.

[3]. Zhou et.al, Encryption method based on a new secret key algorithm for color images, International Journal of Electronics and communication (2016) 1-7.

[4]. Aditya and Deepak, Selection of Best Sorting Algorithm, International Journal of Intelligent Information Processing, 2(2) July-December 2008; pp. 363-368.

[5].https://www.cs.cmu.edu/~adamchik/15121/lectures/Sorting%20Algorithms/sorting.html.

[6]. Ullah, Atta, Sajjad Shaukat Jamal, and Tariq Shah. "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range." *Nonlinear Dynamics* 88.4 (2017): 2757-2769.

[7]. Özkaynak F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dynamics 2018;92(2):305–13.

[8]. Wei X, Guo L, Zhang Q, Zhang J, Lian S. A novel color image encryption al- gorithm based on {DNA} sequence operation and hyper-chaotic system. J Syst Software 2012;85(2):290–9.

[9]. Liu L, Zhang Q, Wei X. A rgb image encryption algorithm based on dna en- coding and chaos map. Comput Electr Eng 2012;38(5):1240–8.

[10]. Wu X, Wang K, Wang X, Kan H, Kurths J. Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing 2018;148:272–87.

[11]. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R. Chaos based crossover and mutation for securing dicom image. Comput Biol Med 2016;72:170–84.

[12]. Rao KD, Gangadhar C. Discrete wavelet transform and modified chaotic key- based algorithm for image encryption and its vlsi realization. IETE J Res 2012;58(2):114–20.

[13]. Mahesh M, Srinivasan D, Kankanala M, Amutha R. Image cryptography using discrete haar wavelet transform and arnold cat map. In: 2015 International Conference on Communications and Signal Processing (ICCSP); 2015. p. 1849– 55.

[14]. Saffari RM, Mirzakuchaki S. A novel image encryption algorithm based on dis- crete wavelet transform using two dimensional logistic map. In: 2016 24th Iranian Conference on Electrical Engineering (ICEE); 2016. p. 1785–90.

[15]. Kumar M, Kumar S, Das M, Budhiraja R, Singh S. Securing images with a diffusion mechanism based on fractional brownian motion. Journal of Information Security and Applications, 2018;40:134–44.

[16]. Wang X-Y, Li P, Zhang Y-Q, Liu L-Y, Zhang H, Wang X. A novel color image encryption scheme using dna permutation based on the lorenz system. Multimed Tools Appl 2018;77(5):6243–65.

[17]. Zhang Y-Q, Wang X-Y, Liu J, Chi Z-L. An image encryption scheme based on the mlncml system using dna sequences. Opt Lasers Eng 2016;82:95–103.

[18]. Zhang Y-Q, Wang X-Y. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 2014;77(3):687–98.

[19]. Liang Zhu Z, Zhang W, Wong K, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 2011;181(6):1171–86.

[20]. Zhang Y-Q, Wang X-Y. Spatio temporal chaos in mixed linear nonlinear coupled logistic map lattice. Physica A 2014;402:104–18.

[21]. Zhang Y-Q, Wang X-Y, Liu L-Y, He Y, Liu J. Spatio temporal chaos of fractional order logistic equation in nonlinear coupled lattices. Commun Nonlinear Sci Numer Simul 2017;52:52–61.

[22]. Zhang Y-Q, He Y, Wang X-Y. Spatiotemporal chaos in mixed linear nonlinear two-dimensional coupled logistic map lattice. Physica A 2018;4 90:14 8–60.

[23]. Xiang T, Wong K, Liao X. Selective image encryption using a spatiotemporal chaotic system. Chaos 2007;17(2):023115.

[24]. Li P, Li Z, Halang WA, Chen G. A stream cipher based on a spatiotempo- ral chaotic system. Chaos Solitons Fractals 2007;32(5):1867–76.

[25]. Wang S, Kuang J, Li J, Luo Y, Lu H, Hu G. Chaos-based secure communications in a large community. Phys Rev E 2002;66:065202.

[26]. Li H, Wang S, Li X, Tang G, Kuang J, Ye W, et al. A new spatio temporally chaotic cryptosystem and its security and performance analyses. Chaos 2004;14(3):617–29.

[27]. Lü L, Li Y, Sun A. Parameter identification and chaos synchronization for un- certain coupled map lattices. Nonlinear Dyn 2013;73(4):2111–17.

[28]. Leyuan Wang, Hongjun Song and Ping, A novel hybrid color image encryption algorithm using two complex chaotic systems optics and Lasers in Engineering (2016) 118-125.

[29]. X.Y. Wang and L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal process, (2012), 1101-1108.

[30]. Yu Changa, GuanrongChenb, Complex dynamics in Chen's system, Chaos, Solitons & Fractals Volume 27, Issue 1, January 2006, Pages 75–86.

[31]. Guanrong Chen, Yaobin Mao, Charles K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, chaos, Solutions and Fractals 21(2004) 749-761.

[32]. Mahmoud GM, Bountis T, Mahmoud.EE, Active control and global synchronization of the complex Chen and Lüsystems.Int. J Bifurcat Chaos2007; 17 (12):4295–308.

[33]. Xiao-Jun Tong, Design of an image encryption scheme based on a multiple chaotic map, Commun Nonlinear Sci Number Simulation 18 (2013) 17251733.

Author Profile

Rajendra Kumar is presently working as Assistant Professor in the Department of Computer Science, Faculty of Natural Sciences, Jamia Millia Islamia (Central University), New Delhi-110025, INDIA. He has an excellent academic background with a very sound academic and research experience.
He has published various research papers in the conferences of international/national repute. His research interest includes: cyber security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT, Software Security, Requirements Engineering, Security Policies and Standards, Software Engineering, Access control and Identity Management, Vulnerability Assessment etc.

Subodh Kumar is presently working as a Research scholar in the Department of Computer Science, Faculty of Natural Sciences, Jamia Millia Islamia (Central University), New Delhi-110025, INDIA.
He has a very good academic background. He is NET-JRF qualified. His research interest includes: Cyber Security, Cryptography, image encryption etc.

