JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Chaos Based 2 Dimensional Logistic Map for Image Security

Latha H R [1], Dr.A.Rama Prasath [2]

[1] Assistant Professor,Dept. of Computer Applications,Jindal College for Women, Bangalore, Karnataka,India.Research Scholar, Hindustan Institute of Technology and Science, Chennai. India

[2]Assistant Professor (Selection Grade), Department of Computer Applications, Hindustan Institute of Technology and Science, Chennai, India.

Email ID:[1] hrlatha01@gmail.com

Received: 01 May 2020 Revised: 23 June 2020 Accepted: 04 July 2020

ABSTRACT: Protection of digital data is the utmost requirement of the day. Everything in the world is being upgraded to electronic communication and this requires protection against data fraud. Data is nowadays not only text but also image, audio video individually and sometimes together as multimedia files. Encryption algorithms protect data against attacks and hackers. This paper proposes a new chaos based Optimization algorithm for enhanced image security, analyses several recent developments in encryption and decryption algorithms and summarizes different approaches, their benefits and limitations.

KEYWORDS: Logistic Map, Chaotic Map, Encryption, Decryption, Image Security

I. INTRODUCTION

Digital Image Processing is the most important and prominent domain of the word today. Web database is amalgamating itself with user data in the form of text and image. Secured storage and transmission of images over network is demanding improvisation of security techniques and development of new algorithms. Secured data transmission is the goal of cryptography. Cryptography provides privacy of information under hostile conditions. Many techniques have been adopted by the science of cryptography to overcome attacks. This paper describes one of the most important and efficient implementation of cryptography. Chaos theory has contributed much towards strengthening of cryptography algorithms. Chaotic cryptography is the consideration in this paper.

II. CHAOS THEORY

Chaos creates ambiguity in the image. It is capable of creating an unordered and messy structure. Chaos theory plays a very important role in representing and creating secret theories. Chaos theory is an offspring of non linear dynamics. Chaotic Synchronization principles were discovered b Pecora & Caroll[1]. They generate complex signals which have its application in security domain. Chaos looks random but it is derived from a deterministic process.

The clue that emphasizes chaos in different domains is its sensitivity to initial conditions. This sensitivity is the seed of further applications and adoptions. Chaos has potential application in digital communication.

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Figure1:Reversible chaos

The Two Dimensional Logistic Map

The two-dimensional logistic map is used for its complicated behaviors. It generates more random like and complex chaotic structures.

Mathematical Definition: A trajectory of the two Dimensional logistic map can be represented using equation 1, where r is the system parameter and (x_i,y_i) is the position at i^{th} iteration. By knowing (x_0, y_0, r, i) i^{th} point on the trajectory can be determined.

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y) \end{cases} \quad (1)$$

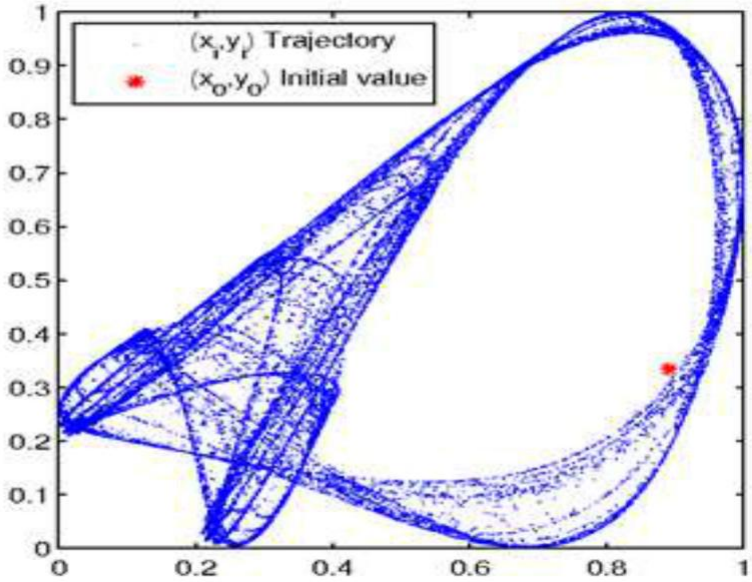

Figure: A trajectory of the two-dimensional logistic map

Chaotic Behaviour: According to the values determined for the parameter r, the logistic map evolves in different dynamics. The following equation represents chaotic behavior mathematically.

$$\begin{cases} x_i = L_x^{2D}(x_0, y_0, r, i) \\ y_i = L_y^{2D}(x_0, y_0, r, i) \end{cases} \quad (2)$$

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

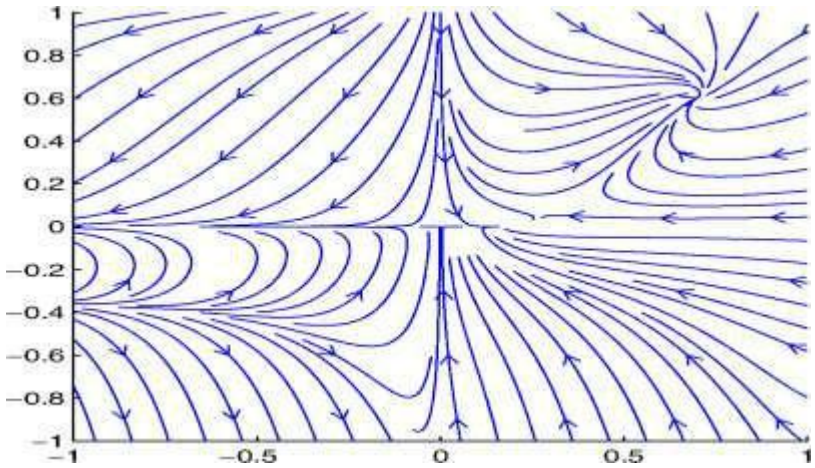

Figure: A phase portrait of the two dimensional logistic map

Based on the values selected for system parameter r and initial values (x_0, y_0) at i^{th} iteration, the behavior of the logistic map is predicted. The behavior of the map at different values of r is tabulated below.

Table1: Behavior of system at different values of the variable r

S.No.	R (system parameter)	Behaviors of the map
1.	$R \in (-1,1)$	➢ Encompasses 1 attractive node and 2 saddle points. ➢ Makes X and Y axes to become unstable in the system
2.	$R \in (1.11,1.19)$	➢ In between the "invariant close curve", there exist alterations with "oscillations, frequency locking, cyclic chaotic behaviors, contact bifurcations with basin boundaries, and single chaotic attractor".
2.	$R = 1$	➢ The NeimarkHopf bifurcation is undergone by the attractive focus of the system
3.	$R \in (1,1.11)$	➢ The "attractive focus" of the system becomes repellent and tends to cause "oscillations" in the system
5.	$R > 1.19$	➢ Unbalanced system

III. CHAOTIC CRYPTOGRAPHY: LOGISTIC MAP TO IMAGE ENCRYPTION

Chaos theory is very useful and effective for cryptography. Chaotic dynamics in cryptography mainly has two perspectives. First one uses pseudo random sequence generators to be part of key streams to mask plain images. Second one uses plain image as the initial state and proceeds by manipulating the pixels ordering. Deterministic and discrete chaotic behavior is imbibed in image security. Chaos applied on image data is reversible which is the most prominent and desirable property in image security. Ergodicity, sensitivity on initial conditions, mixing properties and system parameters are the key features which have contributed to chaotic cryptography.

Two dimensional nature of image data demands the usage of effective chaos generating technique to be adopted for creating secure images. This requirement is fulfilled by adopting two dimensional logistic map. 2D logistic map produce chaotic behaviors with basins and attractors. The random number patterns generated from logistic map are more complex.

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Some desirable properties of chaotic systems that make it suitable for image encryption can be listed as deterministic, unpredictable & non linear and random.

Deterministic: Chaotic systems are deterministic in nature. They can be represented using perfect mathematical equations with determined and iterating values for acertain variables. 2D logistic map generators make Chaos deterministic.

Unpredictable & Non-Linear: Chaos generated by 2D logistic map are unpredictable and non linear . They are highly sensitive to initial parameters. A minute change in the initial values produces enormous difference in the result.

Random: The patterns generated by the logistic sequence generator are unpredictable and are always out of order. They seem to be very confusing. Still the randomness in the sequence has deterministic variables embedded in them.

IV. OBJECTIVE

The objective of the proposed work is to enhance image security by adopting two dimensional chaotic mapping for image encryption process. The security is verified by different benchmarks like histogram analysis, key sensitivity analysis, entropy test and correlation co-efficient analysis.

Image encryption is the process of converting image to unreadable and unrecognizable format by the application of encryption algorithms which includes several intermediate processes like permutation, confusion, diffusion and transposition. All these actions are executed keeping in mind that these processes should be reversible. At the decryption end, these processes have to be capable of recreating the original image data.

Table1: Parameters of Chaotic systems and Cryptographic algorithms

Chaotic systems	**Cryptographic algorithms**
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	Rounds
Parameters	Key
Sensitivity to initial / control conditions parameters	Diffusion with a small change in the Plain Text / Key
Mixing	Diffusion
Ergodicity	Confusion
Deterministic dynamics	Deterministic pseudo-randomness
Structure complexity	Algorithm Complexity
Analytic methods	Algebraic methods

V. METHODOLOGY

Encryption Process:

Encryption is defined as the process of converting the input plain image data into unreadable format. It basically considers two major operations, namely, Confusion and Diffusion. To strengthen these properties encryption uses permutation, diffusion and transposition operations. Encryption process applies encryption algorithm to the plain image along with the key and produces unreadable cipher image as output. This process is represented in equation1.

C =Encryption Aalgorithm(P,K)…….(1)

Where C is the cipher image, E is the encryption algorithm, K is the key and P is the plain image.

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Decryption Process: The cipher image produced at the encryption end is totally unreadable. At the decryption end the unreadable image is converted into readable form. Decryption performs all activities of encryption process in the reverse order and generates plain image.

P = Decryption Algorithm(C,K)…….(2)

Where P is the plain image ,C is the cipher image, D is the Decryption algorithm, K is the key

Proposed Algorithm:

The proposed algorithm follows the below mentioned steps. The effectiveness of the algorithm depends on step3 which chooses initial parameters for the encryption process.

Flowchart

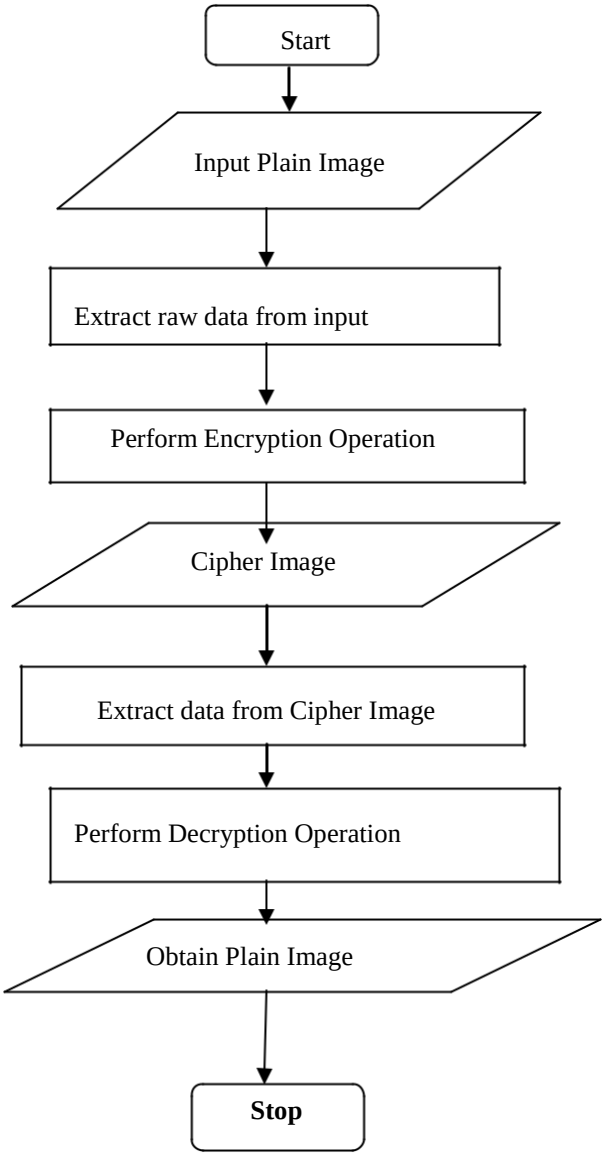

Figure: Flowchart to depict encryption and decryption process

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Algorithm: Encryption

Step 1: Extract the image to be encrypted which is plain image

Step 2: Extract raw data from the plain image

Step 3: Apply optimization algorithm to choose the initial parameters and the key

Step 4: Perform Encryption operation by considering the initial values chosen in step 3.

Step 5: Cipher Image is generated from Encryption phase.

Algorithm: Decryption

Step 1: Extract the image to be decrypted which is cipher image

Step 2: Extract raw data from the cipher image

Step 3: Apply decryption algorithm using the key

Step 4: Perform decryption operation

Step 5: Plain Image is generated from decryption phase

Analysis:

The encryption and decryption process is verified by benchmarks marked by experts for checking the quality of the entire process. Benchmarks identified for verificatin are key sensitivity analysis, histogram analysis, adjacent auto pixel correlation test, information entropy test and UACI & NPCR test.

VI. BENCHMARKS FOR OPTIMIZATION TEST

A. Key Sensitivity Analysis

The efficiency of an image encryption algorithm will be calculated depending on different cipher images it produces for the chosen key values. Any Encryption algorithm should be sensible to the key value chosen as the parameter for the encryption algorithm. It should result in different cipher images for a minute change in the key parameter.

B. Histogram Analysis

Quality of the cipher image is analyzed by the histogram generated by the cipher image. A good cipher image generates random like image which generates uniformly distributed histogram. Thereby making the cipher image far different from the input plain image.

C. Adjacent Pixel Auto-Correlation Test

Cipher image should possess low correlation among adjacent pixels. Pixel information redundancy is the general format of the plain image. The cipher image generated from the good image encryption algorithm should exhibit low correlation among its pixels.

D. Information Entropy Test

Randomness of an image is deduced by Information Entropy test. The scores of means and variances indicate the randomness in the cipher image. The output of the encryption algorithm generates diverse values for information entropy measurement.

E.UACI & NPCR Tests

The encryption algorithm should produce the cipher image with high resistance to differential attacks. Unified average changed intensity (UACI) and The number of changing pixel rate (NPCR) values judge how resistant the cipher image for differential attacks.

VII. CONCLUSION

The current research work proposes an optimized two dimensional chaotic mapping for encrypting the image data. Image Security is analyzed using the benchmarks of the optimization algorithms. The proposed optimization algorithm improves information entropy by using the new key generation strategy of the proposed algorithm.

VIII. REFERENCES

[1] L. M. Pecora and T. L. Carroll, “Synchronization in Chaotic Systems”, Physical Review Letters, vol. 64, no.8, pp. 821– 824, 1990.

[2] Cha-Cha Yu, Nan-Run Zhou, Li-Hua Gong, Zhe Nie,"Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system",Optics and Lasers in Engineering, vol.124, January 2020

[3] Xingyuan Wang, Hongyu Zhao, Le Feng, Xiaolin Ye, Hao Zhang,"High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices",Optics and Lasers in Engineering, col.122,pp225-238,November 2019

[4] Wang Xingyuan, Zhang Junjian, Cao Guanghui,"An image encryption algorithm based on ZigZag transform and LL compound chaotic system",Optics & Laser Technology,vol.119,November 2019

[5] C. Zhu and K. Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps," in IEEE Access, vol. 6, pp. 18759-18770, 2018.

[6] X. Zhang and X. Wang, "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem," in IEEE Access, vol. 6, pp. 70025-70034, 2018.

[7] M. Guan, X. Yang and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," in IET Image Processing, vol. 13, no. 9, pp. 1535-1539, 18 7 2019.

[8] G. R. W. Thoms, R. Muresan and A. Al-Dweik, "Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems," in IEEE Access, vol. 7, pp. 158697-158709, 2019.

[9] Hossein Nematzadeh, Rasul Enayatifar, Homayun Motameni, Frederico Gadelha Guimarães, Vitor Nazário Coelho,"Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices",Optics and Lasers in Engineering, Vol.110,pp.24-32,November 2018

[10] Qiaoyun Xu, Kehui Sun, Congxu Zhu. "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map", Physica Scripta, 2020Publication

[11] Ji Xu, Peng Li, Feifei Yang, Huizhen Yan. "High Intensity Image Encryption Scheme Based on Quantum Logistic Chaotic Map and Complex Hyperchaotic System", IEEE Access, 2019

[12] Seyyed Mohammad Reza Farschi, H. Farschi. "A novel chaotic approach for information hiding in image", Nonlinear Dynamics, 2012

[13] Chunyuan Liu, Qun Ding. "A Modified Algorithm for the Logistic Sequence Based on PCA", IEEE Access, 2020

[14] Mangore Anirudh K, M Roberts Masillamani, “Big data encryption in healthcare monitoring system”, Journal of Advanced Research in Dynamical and Control Systems, IISN:1943-023X Issue:13 Special Issue, Pg No: 2200-2209.