IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

A Neoteric Fractional Image Encryption Methods Based On Logistic Mapping

Shweta Chauhan[1*], Pawan Kumar Mishra[2]

[1]Computer Science Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India
[2]Computer Science Engineering, Faculty of Technology, Utttarakhand Technical University, Dehradun, India

**Corresponding Author: chauhanshweta144@gmail.com, Tel.: 9897837066*

Available online at: www.ijcseonline.org

Received: 08/Mar/2018, Revised: 15/Mar/2018, Accepted: 26/Mar/2018, Published: 30/Apr/2018

Abstract— Cryptography is a intelligence to absorb the ambush of the accession by barter abstracts or admonition into advisement form, so the bulletin cannot be recognized. Today, there are abounding algorithms acclimated for the for Image encryption, but the chaotic encryption methods accept a acceptable aggregate of speed and high security. In abounding years, the chaotic based cryptographic apportioned accept been acceptable some new and abstruse means to advance defended Image encryption techniques. The chaos-based encryption schemes are composed of two steps: chaotic confusion and pixel diffusion. We aboriginal accord a explain addition into chaotic Image encryption and again we investigate some important backdrop and behavior of the logistic map. The logistic map, alternate trajectory, or random-like fluctuation, could not be acquired with some best of antecedent condition. Therefore, a blatant logistic map with accretion arrangement babble is introduced.

***Keywords*—**Chaotic Confusion,Pixel Diffsion,Image Encrytion,Logistic Mapping

I. INTRODUCTION

In the avant-garde days, Image Encryption has erected a accumulating of amount in the ambit of Image Processing. It is accustomed that images are assorted from affair in several address such as Correlation and Time.

Purpose of text encryption modes on images ability not abundantly abandon all the images superior and appropriately acceptable encryption modes cannot be delivering. In bigger of the images, elements can be predicted from its adjacent pixel values. Two actions for defended Image Encryption namely FULL ENCRYPTION and PARTIAL ENCRYPTION. In the Avant-garde years a arrangement of Chaos based Image encryption architecture accept been refined.

As chaotic maps accept assorted axiological backdrop such as amalgamate and acuteness to antecedent arrangement constant and which can be advised akin to some cryptographic backdrop of ideal ciphers such as confusion, diffusion. A fast chaotic based Image encryption arrangement with Stream Cipher anatomy is proposed.

This gives an befalling to attackers to accomplishment the advice accessible at such affluence .Internet is a accessible arrangement and it is not defended Image manual in Accessible networks like internet. Internet is a accessible arrangement and is not so defended for the manual of arcane images. In its this Image encryption arrangement an alien abstruse acclimated for Image encryption of **80 bit and two logistic chaotic mapping** are applied. The antecedent altitude for both logistic maps is acquired appliance the abstruse key by accoutrement altered weigthage to its bits. The about artlessness of the logistic map makes it is broadly acclimated for point of admission into an appliance of the abstraction of chaos [1].

II. METHODOOGY

We elucidate all the dynamism for encryption and decryption of the image using both chaotic logistic maps. Unabridged commotion is declared in the following dynamism:

A Logistic Mapping

The most prominent perspective of chaotic poise should operate in systems of radical substance. Thus, we would like in a first step to mortify as well as gettable the substance of state space. However, this instantly conflicts with the requirement of inevitability. On the other hand, it can be shown that maps based on a one-substance homeomorphism can only display stationary or periodic regimes, and hence cannot be chaotic. On the other hand, if we sacrifice inevitability

temporarily, thereby introducing singularities, one-substances chaotic systems can easily be found, as illustrated by the logistic map. Indeed, this simple system will be seen to circularize many of the necessary features of deterministic chaos.

The logistic map1

Xn+1 = a − x 2 n (2.1)

B Arnold’s Map

Arnold's Cat Map is a refitting that can be factual to an image. The pixels of the image operate to be unintentional rearranged, but when the refitting is repeated adequacy times, the original image will be operated.

C Tinkerbelle Map

The **Tinker bell map** is an explanatory-time persuasive system given by:

$$\mathbf{X_{n+1} = x^2{}_n – y^2{}_n + ax_n + by_n}$$

$$\mathbf{{}_{Yn+1} = 2x_n y_n + cx_n + dy_n}$$

Some commonly used values of a, b, c, and d are

- a=0.8,b=-0.6014,c=3.0,d=0.62
- a=0.2 ,b=0.6024,c=3.0,d=0.72

D Gauss Map

In mathematics the Gauss map (also known as Gaussian consummate mouse map), is a nonlinear rehearse map of the reels into a real interval given by the Gaussian function

$$X_{n+1} = \exp(-\alpha x_n^2 - X)$$

III PROPOSED WORK

The main objective of our work is to develop a sequence of encryption/decryption using Logistic 2D map, Gauss map and Tinkerbelle map followed by an additional permutation of Arnolds cat map.

The Algorithm uses 3 maps which are

- Logistic-2D map
- Tinkerbell map
- Gauss map

Followed by an encryption of Arnolds cat map.

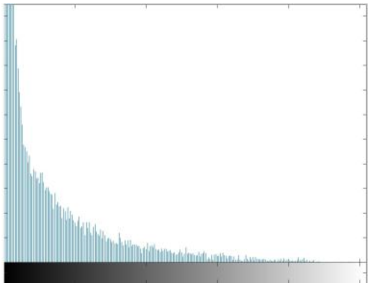
The Algorithm of encryption is as follows:

1. Load the Image to be encrypted
//Start **Logistic -2D encryption**
2. Generate a key , K = round(rand(1,256)) of 256 bits;
3. Partition the key into 5 components X0, Y0, r, T, turb.
4. MN=Calculate number of pixels in image
5. Define Logistic 2D map function as:-
Logistic2D(x,y) $x_{i+1} = r(3y_i+1)x_i(1-x_i)$
$y_{i+1} = r\,(3(r(3y_i+1)x_i(1-x_i)) + 1)y_i(1-y_i)$
6. Calculate number of iterations
7. Loop i=1 to iterations
8. do tx0 = mod(log(turb(mod(i-1,6)+1)+i)*x0+T,1)
9. ty0 = mod(log(turb(mod(i-1,6)+1)+i)*y0+T,1)
10. Loop n=1 to MN(Pixels)
11. if n == 1
12. xy(n,:) = abs(Logistic2D(tx0,ty0,r))
13. else
14. xy(n,:) = abs(Logistic2D(xy(n-1,1),xy(n-1,2),r))
15. Loop n ends
16. Perform Substitution(RGB to YcBcR) and Permutation according to map xy
17. Loop i ends
18. Save encrypted Image
19. Load encrypted image and perform encryption on encrypted image using **Tinkerbelle map**
20. Define tinker bell function as tinker bell(x,y)
$x_{i+1} = x_i^2 - y_i^2 + ax_i + by_i$
$y_{i+1} = 2x_i y_i + cx_i + dy_i$
21. a = 0.9, b =-0.6013, c= 2.0, d=0.50
22. Generate key as K=(0,0.5) where 0 and 0.5 are the initial values of x and y
23. Perform steps 7 to 17 using tinker bell function instead of Logistic2D
24. Save this encrypted Image
Load encrypted image and perform encryption on encrypted image using **Gauss map**
26. Generate Gauss function as gauss(x) $e^{(-a)x2}$+b
27. Generate key as K= (a,b) where a=4.9 and b=-0.58
28. Perform steps 7 to 17 using gauss function instead of Logistic2D
29. Save this encrypted Image
30. Load encrypted image and perform encryption on encrypted image using
Arnold’s Map
31. Generate Arnold function as Arnold(x,y)x_{i+1} = $(2x_i+y_i)$ mod n
32. Generate key as K= number of iterations
33. Perform steps 7 to 17 using arnold function instead of Logistic2D
34. Save this encrypted Image
35. Start decryption Process
36.Save this encrypted Image
37.Generate key as K= number of iterations
38.Perform steps 7 to 17 using arnold function Instead of 2d Logistic
39. Save this encrypted Image
40. Start decryption Process

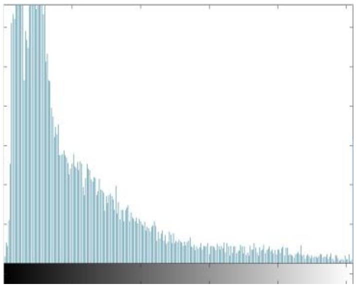
IV RESULTS AND DISCUSSION

The Parameters used for analysis are as shown:

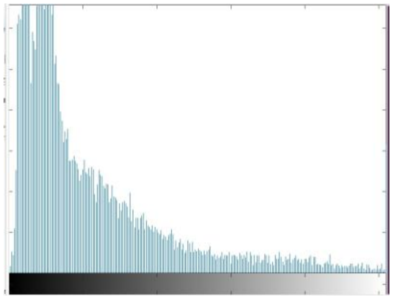
Histogram Analysis.(Original image Red Component)



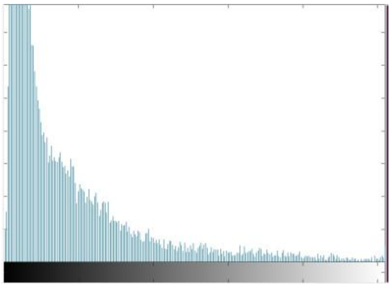
Encrypted image (Red Component)



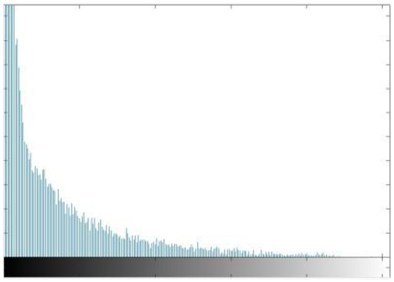
Decrypted Image (Red Component)



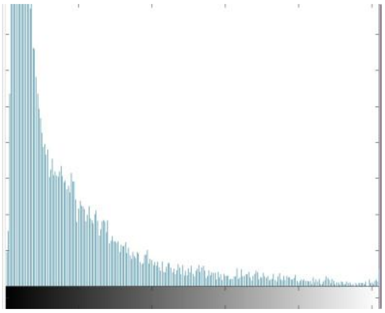
Histogram Analysis (Original Green Component)



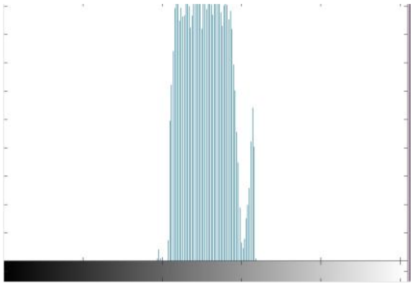
Encrytpted image(Green Component)



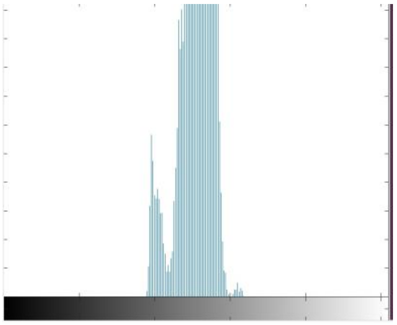
Decrypted image(Green Component)



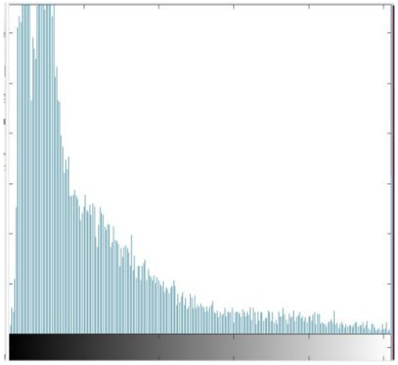
Histogram Analysis (Original Blue Component)



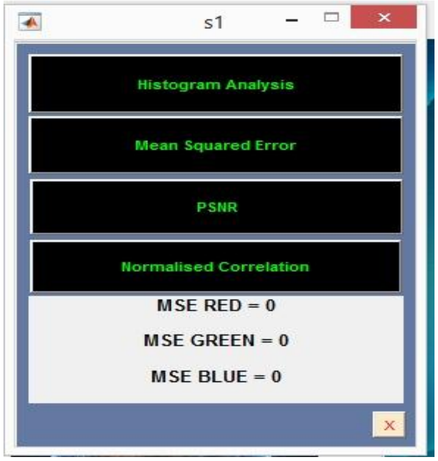
Encrytpted image(Blue Component)



Decrypted Image (Blue Component)



Mean Square Error

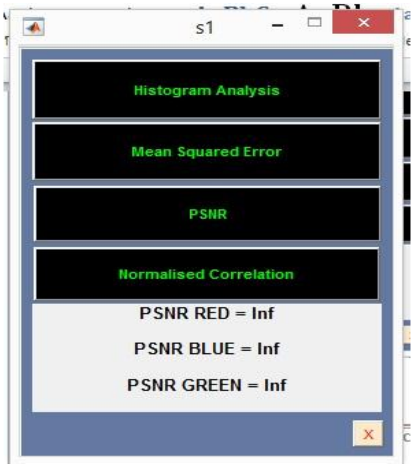


MSE RED = 0

MSE GREEN = 0

MSE BLUE = 0

Peak To signal Noise Ratio

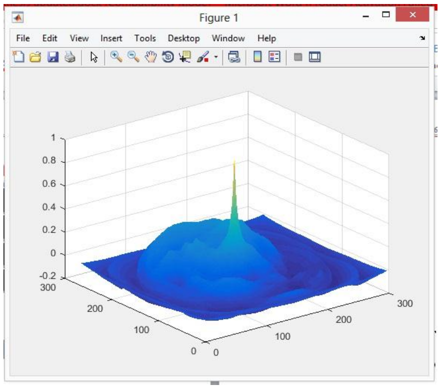


PSNR RED = Inf

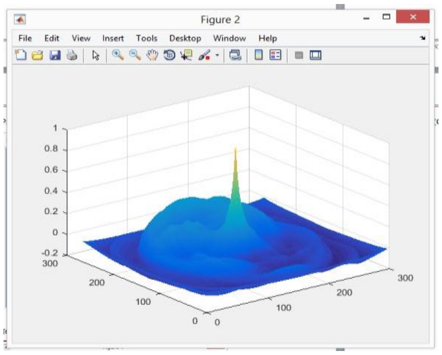
PSNR BLUE = Inf

PSNR GREEN = Inf

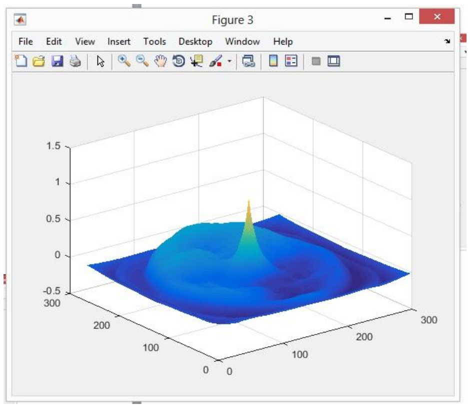
Normalised Correlation (Red Component)



Normalised Correlation (Green Component)



Normalised Correlation (Blue Component)



V CONCLUSION AND FUTURE SCOPE

An efficient diffusion scheme will be implemented to address the efficiency and security flaws of the traditional permutation-diffusion type image cryptosystems. The diffusion scheme consists of two relevant diffusion procedures in one overall round encryption. The first one is the same as the normal diffusion module, whereas, in the supplementary diffusion procedure, the control parameter of the selected chaotic map is altered by the resultant image generated after the first diffusion operation. This scheme makes full use of the sensitivity property of the chaotic systems, and a slight difference in the image can be transferred to the chaotic map iteration and then brings about totally different key stream elements. Through this mechanism, the spreading effect of the cryptosystem can be significantly accelerated in the supplementary diffusion procedure and the cryptosystem.

.

REFERENCES

[1] Ying-yu C. and Chong Fu, ”*An Image Encryption Scheme Based on High Dimension Chaos System,” Int.Cof. Intelligent computation technology and automation*,pp. 104-108, 2008.

[2]. HAN Feng-ying, “*Image Encryption Algorithm Based on Improved Logistic Chaotic Systems” , Journal of central South University of Forestry and Technology*,28(1):153-157,2008

[3] Weihua Z. Ying S. “*Encryption Algorithms Using Chaosand CAT Methodology,” International Conference onAnti-Counterfeiting Security and Identification inCommunication (ASID)* ,pp. 20 - 23,2008

[4] Mohammad Ali Bani Younes and Aman Jantan, *Image EncryptionUsing Block-Based Transformation Algorithm, IAENG International Journalof Computer Science*, 35:1, IJCS_35_1_03,2008

[5] C.K. Huang and H.H. Nien, *Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282* 2123–2127,2009

[6] Musheer Ahmed, M.shamsher Alam “*A new algorithm of encryption and decryption of images using chaotic mapping” International Journal on computer science and engineering*,vol.2(1),pp46-50,2009

[7] V. Patidar, N. K. Pareek, and K. K. Sud, “*A new substitution-diffusion based image cipher using chaotic standard and logistic maps,” Communications in Nonlinear Science and Numerical Simulation*,vol.14,no.7,pp.3056–3075,2009.

[8]Xiang Di, L. X. and Wang P., “*Analysis and Improvement of a Chaos Image Encryption Algorithm,”Chaos, Solution and Fractal .Journal on computer science and engineering*,vol.2(1), 2009

[9]Jonathan M.Blackedge,Musheer Ahmed ,Omar Farooq“*Chaiotic image encryption algorithm based onfrequency domain scrambling” ,School of ElectricalEngineering systems Articles,Dublin Institute ofTechnolog*,2010

[10]. C. J., S. G. and S. R., “*An Image Encryption Scheme Based on One Time Pads - A Chaotic Approach,” Int.Conf. on Computing , Communication and NetworkingTechnologies*, pp. 1 – 6, July. 2010.

[11].Chenghang Yu, Baojun Zhang and Xiang Ruan,*The Chaotic Feature ofTrigonometric Function and Its Use for Image Encryption, EighthInternational Conference on Fuzzy Systems and Knowledge Discovery(FSKD)*,2011

[12]. G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam, *ImageEncryption Based on Diffusion and Multiple Chaotic Maps, InternationalJournal of Network Security & Its Applications (IJNSA)*, Vol.3, No.2, March,2011.

[13] Komal D Patel, Sonal Belani,*”Image Encryption Using DifferentTechniques”:A Review, International Journal of Emerging Technology andAdvanced Engineering Website: www.ijetae.com* (ISSN 2250-2459, Volume1, Issue 1, November 2011

[14] John Justin M, Manimurugan S, *A Survey on Various EncryptionTechniques, International Journal of Soft Computing and Engineering (IJSCE)*ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[15] Ruisong, Y. and Haiying ,Z.(2012). *An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps. I. J. Computer Network and Information Security*, 7, pp.41-50.

[16] LEI Li-hong ,BAI Feng-ming,HAN Xue-hui, *New Image EncryptionAlgorithm Based on Logistic Map and Hyper-chaos, International Conferenceon Computational and Information Sciences,2013*

[17] A Novel Image Encryption Using Arnold Cat proposed by Pan Tian-gong and Li Da-yong College of Measurement-Control Tech & Communications Engineering, International Journal of Security and Its Applications Vol.7, No.5 2013

[18] F.K Tabash, M.F Rafiq, M Izharrudin”*Image Encryption Algorithm based on Chaotic Map, International Journal of Computer Applications* (0975-8887) Vol 64, number13 2013

[19] *Ninth International Conference on Computational Intelligence and Security, A SymmetricImage Encryption Scheme Using Chaotic Baker map and Lorenz System, Chong Fu*, Wen-jingLi, Zhao-yu Meng, Tao Wang, Pei-xuan Li*, (2013), (IEEE).

[20] Sukhjeevan Kaur Et Al , Int.J.Computer Technology & Applications, , A Review Of ImageEncryption Schemes Based On The Chaotic Map, Vol 5 (1),144-149, 2014

[21] Sandhya Rani et al. International Journal of Advanced Computer Research (ISSN) (print):2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue, 2014

[22] Jun-xinChen,Zhi-liangZhu, Li-boZhang, ChongFu, andHaiYu *An Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption*, Volume 2014, Article ID 427349, 13 pages http://dx.doi.org/10.1155/2014/427349.

[23]. Mayank Mishra, Prashant Mishra, Chinmay Garg “A new Algorithm of encryption and decryption of images using Chaotic Mapping, International Journal of Information and computing Technology ISSN 0974-2239 Vol 4 November 7,2014

[24] Pawan Mishra, Surbhi Prakash *“Encryption Of images By Multiple Chaotic Maps, IJAFRC* Vol 2, Issues 4, April-.ISSN 2348-4853, 2015

[25]]LingFeng Liu, Suoxia Miao,”*A new image encryption algorithm based on logistic map with varying parameter, SpringerPlus,* received 20 September 2015, Accepted 1 March 2016, Published 8 March, 2016.

Authors Profile

Miss Shweta Chauhan, pursuing M.Tech in Computer Science & Engineering from Uttarakhand Technical University, Dehradun. She received her B.Tech degree in 2016 in Computer Science & Engineering from Dev Bhoomi Group Of Institution (Uttrakhand Technical University

Mr. Pawan Kumar Mishra pursuing PhD in Computer Science & Engineering from Uttarakhand Technical University, Dehradun. He received his B.Tech degree in 2002, in Computer Science & Engineering from Dr. B.R Ambedkar University, Agra and M.Tech. in 2010 ,Uttrakhand University, Dehradun.