Novel Method of Secure Communication using Logistic Map

Supriya Khaitan, Rashi Agarwal, Mandeep Kaur

Abstract*: Significant research efforts have been invested in recent years to export new concepts for secure cryptographic methods. Many mathematicians are attracted by Chaos functions as it has sensitive nature toward its initial conditions and their colossal suitability to problems in daily life. Inspired by new researches, a new chaotic cryptography algorithm is proposed in this paper. The key feature of this approach is that instantaneous key is generated at host independently that is used to determine the type of operations on each pixel. The information available in images is 24 bit RGB these value are modified mathematically using eight reversible operations. Also during encryption, the control parameter of the chaotic system is updated timely.

Index Terms: Chaotic Map, Encryption, Decryption, Security, Logistic Map.

I. INTRODUCTION

Chaos theory has been receiving enormous response in the last two decades by the scientific community. The logistic map is a dynamic population model that is non-linear in nature and was originally introduced by Pierre François Verhulst [5].

For distinct applications and the complexity of research done on various logistic mapp, anyone may refer to Ausloos [5], Bunde & Havlin [7], Crownover [8], Holmgren [10], Peitgen, Jurgens and Saupe [13] and [14].

The most promising application of chaotic maps in the area of cryptographic algorithms relies on the properties that chaotic are similar to noise and depends on initial parameters. Chaotic map fulfills the basic requirements of cryptography because of its sensitiveness towards the initial conditions. Therefore, the secret keys are usually the system parameters and initial conditions.

Many chaotic systems have been created so far. The highest acclaimed cryptosystems is formed on the ergodic property of chaotic maps. It has received lionized attentions in the past literature [1] - [4], [9], [11], [12], [22] and [23]. Pecora and Carroll showed application of chaos in masking the message for transmitting signals [12]. In 1998, Baptista proposed a new cryptosystem [6] that encrypts the message into different iterations for chaotic map to purview a domain on a phase space that harmonize to the text.

Wong examined Baptista's approach and found some limitations like the dissipation of the cipher-text is not homogeneous. A random number sequence is generated for every block of text. After examining the drawbacks, a solution was proposed by Wong that gave a much deflated distribution of cipher-text using the same logistic map [22]. After that, scientists proposed a time efficient chaotic-cryptographic algorithm that uses a dynamical look-up table that updated continuously depending on the plaintext instead of static one [23].

Rani and kumar gave a new kind of iteration called superior iteration in analyzing, generating and studying the behavior of fractals and chaotic maps [18] – [21]. In 2009, Rani and Agarwal have increased the stability of logistic map using superior iterations in the map [15] and also generate beautiful fractals [16]. Also, the above same authors have shown superior fractals are more stable under high strength of dynamic noises as compared to classic fractals [17]. Many have used [24][25] a bit scrambling algorithms with chaos concept to change position of pixels.

Seeing the applications of chaos and fractals, we proposed a new encryption method based on it. This method is based on multiple, dynamic and one time usable keys generated from logistic map without involving the exchange of key.

In Section 2, we describe the iteration technique that we use in our proposed model using example. In Section 3, we have given the analysis and applications of the proposed model followed by Section 4 that presents the conclusions related to security and utility of the chaotic model.

II. PROPOSED METHODOLOGY

A. Chaos Theory

Chaos is a non deterministic method based on non linear system. It focuses on behavior of dynamic systems; those are highly sensitive to initial condition.

Mathematically, the extensively simple looking one-dimensional logistic map is given by the equation

$$x_{n+1} = r * x_n (1 - x_n), \quad (1)$$

Where x_n is any value between 0 and 1 and it represents the population for a particular year n. Therefore, x_0 epitomize the initial population and r speaks to a positive joined rate for proliferation and starvation [5] and [8].

Revised Manuscript Received on July 5, 2019.

Supriya Khaitan, Research Scholar, CSE Department, SET Sharda University, Uttar Pradesh, India, Assistant professor ITS Engineering College, India,supriyakhaitan@gmail.com

Rashi Agarwal, Master of Computer Applications, Galgotia College of Engineering & Technology, Uttar Pradesh, India..

Mandeep Kaur, CSE Department, SET Sharda University, Uttar Pradesh, India.

The proposed image encryption process is using two one dimensional chaotic logistic maps based on equation (1). The value of r is 3.99, a highly chaotic case.

B. Key Generation

Following are steps for generation of encryption key:

- A ten character long key is used. The key is represented in 8 bit ASCII format.
- The key is divided into 8 bit blocks.
- Convert the first 3 block of key into binary. Divide the binary representation into two parts.
- Convert the both part to into a real number X_{01} & X_{02}.
- The formula to calculate the value of $X_0 = (X_{01} + X_{02}) \bmod 1$, where X_0 acts as initial-condition to generate First Logistic-map.
- For calculating Y_0 use the next three block of key and convert it into binary. Calculate $Y_0 = (Y_{01} + Y_{02}) \bmod 1$ where Y_0 acts as initial -condition for second logistic map

C. Encryption

- By iterating the First Logistic-map 24 real numbers are generated. These numbers are separated into 24 disjoint intervals
- Read the RGB values of the image.
- The operations on the RGB pixel values are decided by the iteration of second logistic map as described in Table I.

Table I: Operations performed on the group

	Initial Condition	Operation
a.	0.10-0.15,0.30-0.35,0.50-0.15	NOT operation
b.	0.16-0.18, 0.36-0.38, 0.56-0.58	XOR operation of Red(R) with K1, Green (G) with K2 and Blue (B) with K3
c.	0.19-0.22, 0.39-0.42, 0.59-0.62, 0.80-0.85	XOR operation of Red (R) with K7, Green (G) with K8 and Blue(B) with K9
d.	0.23-0.26, 0.43-0.46, 0.63-0.66	NOT (XOR operation of R with K1, G with K2 and B with K3)
e.	0.27-0.29, 0.47-0.49, 0.67-0.69	XOR operation of R with K4, G with K5 and B with K6
f.	0.70-0.0.75	NO Operation
g.	0.76-0.78, 0.86-0.88	NOT of R, NOT of G, NOT of B
h.	0.78-0.79, 0.88-0.9	XOR operation of R with K8, G with K9 and B with K10

Decryption is opposite process of Encryption.

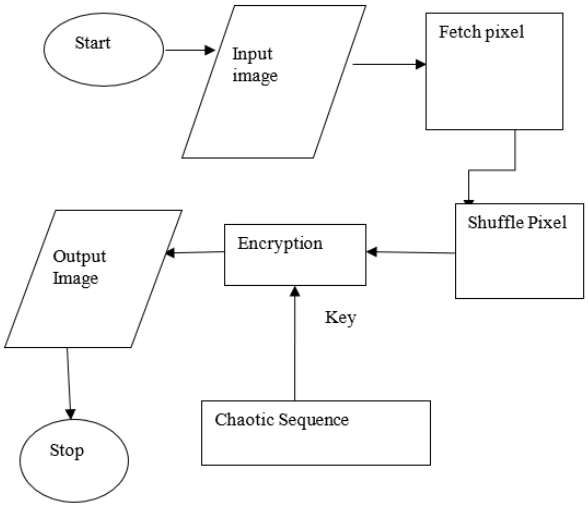


Figure 1: Encryption Process

III. ANALYSIS

A. Histogram analysis

A histogram is a graphical representation that demonstrates the visual effect of circulation of pixels by inspecting the distinct pixel at every gray-scale level.

The histograms of the image (Fig-a) i.e. test picture and (Fig-c) encrypted picture formed by the proposed scheme are shown in (Fig-b) and (Fig-d), correspondingly. It's vibrant from Fig. that the pixels in the encrypted picture are impeccably evenly distributed therefore is not being responsible for any statistical analysis.

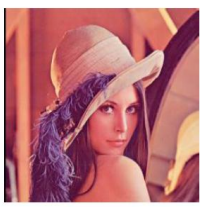


Figure (a) Plain Image

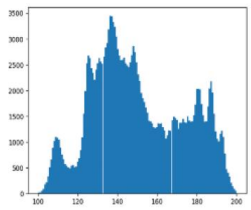


Figure (b) Histogram of Plain Image

Figure (c) Encrypted Image

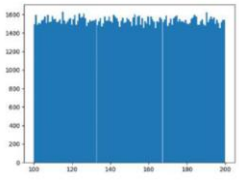


Figure (d) Histogram of Encrypted Image

Figure 2: Histogram analysis

B. Correlation Coefficient

Correlation coefficient is the degree of similarity between two variables. The purpose of this parameter is to calculate the quality of the cryptosystem. Correlation coefficient can be calculated by using the following formula:

$$corr(x,y) = n(\frac{\sum xy) - (\sum x)(\sum y}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \quad (2)$$

Where, x and y are the dim scale estimations of two neighbouring pixels in both the plain-image and cipher-image. N is absolute number of pixels chosen from image.

The visual analysis of the association of neighbouring pixels can be prepared by random selection of N where normally N is greater than 2000, pairs of adjacent pixels in all directions (horizontal, vertical diagonal) of image. One such horizontal representation of neighbouring pixels is shown in Fig. 2, by employing each value of x and y pair.

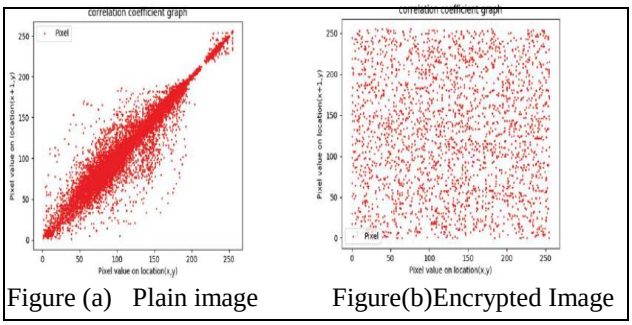


Figure (a) Plain image Figure(b)Encrypted Image

Figure 3: Correlation analysis between Horizontal Pixels

IV. Sensitivity Analysis

A. NPCR (Number of Pixel Change Rate):

NPCR is used to verify the effect of single pixel shift on full image. This will show the amount of advancement in the pixels of two images.

Let Io (I, j) and IENC (I, j) be the pixels estimations of unique and scrambled pictures, Io and IENC, at the i^{th} pixel in succession and j^{th} pixel in a segment, separately. NPCR can be calculated by using the following equation:

$$NPCR(Io, IENC) = \sum_{i,j} \frac{D(i,j)}{wh} \times 100\% \quad (3)$$

$$D(i,j) = \begin{cases} 1 & if\ Io(i,j) = IENC(i,j) \\ 0 & if\ Io(i,j) \neq IENC(i,j) \end{cases} \quad (4)$$

Where w is the width and h is the height of encrypted image.

It has been shown in Table II and Table III that using our encryption scheme NPCR value is above 99.60 % in all cases. This shows that our proposed methodology is highly sensitive to small changes.

B. Unified Average Changing Intensity (UACI):

A small change in plain picture must trigger a major shift in cipher picture.

UACI gives the standard force of contrast in pixels among the any two pictures. UACI can be calculated as follows:

$$UACI(I, IENC) = 1/wh(\sum_{i,j} |Io(i,j) - IENC(i,j)|/2^L - 1) \times 100\% \quad (5)$$

It has been shown in Table II & Table III that using our encryption scheme UACI value is above 49.4 in all cases. This shows that our encryption scheme is resistant to cryptanalytic attacks

Table II: 16 bit block cipher analysis with 10 rounds

Description	Size	Type	Correlation Coefficient	NPCR	UACI
House	256x256	Color	0.011599	99.61141	49.85657
Tree	256x256	Color	0.012494	99.60073	49.48425
Moon	256x256	Gray	0.010004	99.62107	49.89471
Clock	256x256	Gray	0.010916	99.59717	49.80164
Girl(Lena)	512x512	Color	0.005051	99.60848	49.76768
Airplane	512x512	Color	0.003589	99.6109	49.80392
Lake	512x512	Color	0.006071	99.61052	49.77341
Tank	512x512	Gray	0.005092	99.6137	49.86115
Boat	512x512	Gray	0.007045	99.60467	49.82948
Man	1024x1024	Gray	0.002656	99.60988	49.81775

Table III: 16 bit block cipher analysis with pixel shuffling

Description	Size	Type	Correlation Coefficient	NPCR	UACI
House	256x256	Color	0.0180891	99.61853	49.61395
Tree	256x256	Color	0.012239	99.6226	49.68414
Moon	256x256	Gray	0.010066	99.60378	49.67194
Clock	256x256	Gray	0.011693	99.61813	49.77875
Girl(Lena)	512x512	Color	0.004269	99.6081	49.90273
Airplane	512x512	Color	0.0039	99.60531	49.82681
Lake	512x512	Color	0.003523	99.61764	49.78333
Tank	512x512	Gray	0.005695	99.60721	49.7036
Boat	512x512	Gray	0.00429	99.60899	49.85352
Man	1024x1024	Gray	0.003186	99.6054	49.80297

C. Key-Space analysis

To stop brute force attack it is important to have large key space. The proposed image algorithm has 280 distinct combinations of the secret key. In the proposed scheme, two chaotic maps are used.

D. Time analysis

The proposed scheme is applied on many coloured and gray scale images. The time analysis has been done on I 5 system with 8 GB RAM. The average encryption and decryption time taken by the proposed algorithm for images of different size are shown in Table IV.

Table IV: Average Encryption and Decryption time

	8-bit	16-bit	32-bit	64-bit	128-bit	256-bit
Size of File	**Average Encryption Time**					
(256, 256)	0.4036	0.358203	0.41423	0.34034	0.39311	0.3399
(512, 512)	1.32849	1.1628	1.35723	1.149056	1.248128	1.160772
(1024, 1024)	5.3209	4.66877	5.563	4.585	4.9029	4.645002
	Average Decryption Time					
(256, 256)	0.3896	0.321	0.441	0.3441	0.3587	0.3039
(512, 512)	1.3289	1.02488	1.488347	1.1755	1.18733	1.058788
(1024, 1024)	5.1849	4.23874	5.85833	4.700233	4.291865	4.2918

V. CONCLUSION

Real time cryptography is the most demanded for network and information security. Due to unpredictable nature of chaotic map, data transfer is more secure and is difficult to predict by analytical methods without knowing the secret keys (initial conditions or the parameters). The proposed chaotic model has the advantage of secure communication because of no key exchange between hosts. So, the above model is highly applicable for transferring high confidential data in two-party and multi-party scenario.

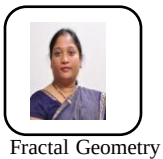
REFERENCES

1. G. Alvarez, F. Montoya, M. Romera and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher" in Phys. Lett. A, Vol. 31, Issue 2, 2003, pp. 172-179.
2. G. Alvarez, F. Montoya, M. Romera and G. Pastor, "Cryptanalysis of dynamic look-up table based chaotic cryptosystems", in Phys. Lett. A,Vol. 326, Issue 3, 2004, pp. 211-218.
3. G. Alvarez, F. Montoya, M. Romera and G. Pastor, "Cryptanalysis of a chaotic secure communication system", in Phys. Lett. A,Vol. 306, Issue 4, 2003, pp. 200-205.
4. G. Alvarez, F. Montoya, M. Romera and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key" in Phys. Lett. A, Vol. 319 Issue, 2003, pp. 334-339.
5. M. Ausloos and M. Dirickx, "The logistic map and the route to chaos. From the beginnings to modern applications", Springer-Verlag, Berlin, 2006. MR2202732 Zbl pre05018776
6. M. S. Baptista, "Cryptography with chaos", Vol. 240, Issue 1, Phys. Lett. A,1998, pp. 50-54.
7. Armin Bunde and Shlomo Havlin, "Fractals in science", Springer-Verlag, Berlin, 1994. MR1290340
8. Richard M. Crownover, "Introlduction to fractals And chaos", Jones & Barlett Publishers, 1995.

9. P. Garcia and J. Jimenez, "Communication through chaotic map systems" in Phys. Lett. A,Vol. 298, Issue, 2002, pp. 35-40.
10. Richard A. Holmgren, "A first course in discrete dynamical systems", Springer-Verlag, 1996 MR1410752
11. Palacios and H. Juarez, "Cryptography with cycling chaos" in Phys. Lett. A,,Vol. 303, Issue 5,2002 , pp. 345-351.
12. L. M. Pecora and T.L. Crroll, "synchronization in chaotic systems", Physical review letters Vol. 64,1997, pp. 821.
13. Heinz-Otto Peitgen, Hartmut Jürgens and Dietmar Saupe, " Fractals for the classroom. Part 2: Complex systems and Mandelbrot set", Springer-Verlag, Berlin, 1992, Zbl 0785.58001
14. Peitgen, Jurgens and Saupe, "Chaos and Fractals" in Springer-Verlag, New York, Inc., 2006.
15. Mamta Rani and Rashi Agarwal, "A new experimental approach to study logistic map", in Chaos Soliton and fractals, Vol. 41 Elsevier 2009, pp. 2062-2066.
16. Mamta Rani and Rashi Agarwal, "Generation of fractals from complex logistic map", Chaos Soliton and fractals, Vol. 42 , Elsevier, 2009, pp. 447-452
17. Mamta Rani and Rashi Agarwal, "Effect of stochastic noise on superior Julia sets", Journal of mathematical imaging and vision, springer. DOI: 10.1007/s10851-009-0
18. Mamta Rani, Ph.D. Thesis "Iterative procedure in Fractals and Chaos", Gurukala Kangri Vishwavidyalaya, Hardwar, India, 2002.
19. Mamta Rani and Vinod Kumar, "Superior Julia set", J Korea Soc Math Edu Series D: Research in Math Edu, 2004, pp. 261–277.
20. Mamta Rani and Vinod Kumar, "Superior Mandelbrot set", J Korea Soc Math Edu Series D: Research in Math Edu, , 2004, pp. 279–291.
21. Mamta Rani and Vinod Kumar, "A new experiment with the logistic function", J. Indian Acad. Math., 2005, pp. 143-156. MR2224669
22. W. K. Wong, L. P. Lee and K. W. Wong, "Keystream cryptanalysis of a chaotic cryptographic method", in Computer Physics Communications, Vol. 15, Issue 2 ,2004, pp. 208.
23. K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table" in Phys. Lett. A, Vol. 298 Issue 4, 2002, pp. 238-242. MR1918066
24. Xie, G.B., Wang, T "A new bit-scrambling hyperchaotic image encryption algorithm",in Microelectron. Comput, Vol. 33 Issue 7, 2016 pp. 28-32.
25. Xu, L., Gou, X., Li, Z., et al "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion" Opt. Lasers Eng. Vol. 91, 2017 pp: 41–52

AUTHORS PROFILE

Supriya Khaitan is B.Tech & M.Tech in Computer Science & Engineering. Her Research interests are Network Security, Data mining. She has published number of research papers in International Journals and conferences. She has 15 year of experience in teaching graduate and post graduate students



Dr. Rashi Agarwal is at present Professor in the Department of Master of Computer Applications in Galgotia College of Engineering and Technology. Dr. Rashi did Ph.D.(Computer Science) from Gautum Budth Technical University, Lucknow in 2011. Her area of Research is Fractal Geometry and Its applications in computer science, in which she has been guiding M.Tech. and Ph.D. students. She has published number of research papers in International Journals and conferences. Her publication focussed on stability of fractals under different type of perturbations. She has 18 year of experience in teaching graduate and post graduate students.

Dr. Mandeep Kaur is working as an **Associate Professor at the Department of Computer Science & Engineering**, Sharda University. She has completed her B.Tech in CSE from UPTU, M.Tech in CSE from PTU & completed Ph.D from Sharda University. Her topic of research was "Thought Recognition: Knowledge Discovery from EEG Signals and Classifying by Classifier Ensemble". She is M.Tech (Project & Dissertation) Coordinator cum Mentor and guiding research investigations for under-graduate, post-graduate engineering students & Ph.D scholars in the areas including Image & Signal Processing, Machine Learning, Neural Networks etc. She has 13 years of Teaching .She has published 03 book chapters in Springer & WSEAS Press and also authored more than 40 research papers in various reputed International / National Journal and Conferences and attended more than 20 FDPs, Workshops, Seminars and Conferences.