A Study of Period Doubling in Logistic Map for Shift Parameter

H.B.Kekre[#1], Tanuja Sarode[*2], Pallavi N.Halarnkar[#3]

[#]*Sr.Professor & Computer Engineering Department & NMIMS University*
Vile Parle (w), Mumbai , India

[*]*Associate Professor & Computer Engineering Department & Mumbai University*
Bandra (w), Mumbai , India

[#] *Assistant Professor & Computer Engineering Department & NMIMS University*
Vile Parle (w), Mumbai , India

***Abstract*— Securing Images is very important. The traditional methods available for data security are sometimes not feasible for securing images as images have large amount of data. To secure images chaotic sequences are useful. In this paper the traditional logistic map is shifted, the shifting operation results in a wide range of chaotic sequences, which may be used for encrypting images and making them more robust.**

***Keywords*— Chaotic, Logistic Map, Period Doubling, Image Encryption**

I. INTRODUCTION

Edward Lorenz, a MIT Meteorologist, invented the chaos theory. He came across this chaos behavior in mathematical modeling of weather systems. The analysis observed by him, was that a small difference in a dynamic system such as a model of atmosphere would result in a vast amount of difference and unexpected results.

Garnet Williams tamed chaos theory [4].Chaos is a mathematical theory. It happens only in deterministic, nonlinear dynamical systems. The term deterministic refers to behavior of the system that is entirely predictable based on certain initial condition and inputs. Non-linearity means output is not proportional to input, or the system as a whole is less than or greater than the sum of its parts. A dynamical system is the one that changes with time.

Chaos in deterministic system is discussed [5] by Carlos Gershenson. Two most important characteristic of the chaotic system is that it is sensitive to initial condition, a small change in the initial condition will result in a varying output. The other characteristics is that Chaotic systems are strange attractors, the dynamics of this systems follow a pattern in which the states will not repeat itself. These states are in a well determined area of state space. The attractors are self affine and hence they are fractals.

An example considered for explaining the chaos behavior is a simple logistic function which is used in population dynamics. In this logistic function, the parameter a represents the fertility or growth rate. A detailed study of this logistic map for varying initial conditions and growth rate is given in the same.

Chaos theory has found a wide variety of applications. One such is "*Advising the undecided Students*" by using the chaos theory as a metaphor. This study has been done by Amy beck [1]. A few concepts explored for the study are sensitive dependence on initial condition, strange attractors, emergent behavior in complex system and fractals.

Another application of chaos includes cryptography with chaos. George Makris et al. has investigated how cryptography with chaos is done using three torus automorphisms , Baker map, the Horseshoe map and the Cat map [9]. The proposed method was used for encrypting images as well as text. The experimental results prove that the degree of security is high. An extension of these methods over text was provided. The key used is completely independent of the length of the block that is encrypted and is very small. In the developed system , the key is not operable if a small part of the document is lost. The only disadvantage of all the systems of symmetric cryptography is the safe transmission of key.

Christopher wood presented a study on overview of chaotic dynamics and its use in symmetric key cryptography from theoretical as well as practical point of view [11]. An introduction to chaos based on logistic map and Lorenz attractor plotted on a 3D plot is been given. Chaos theory is mapped to cryptography in which a discussion of how chaos can be used for cryptography is discussed. The different issues regarding cipher design and its evaluation is considered. Security analysis of a cryptographic technique from both theoretical as practical point of view is also been discussed.

Zhang hong et al. discussed about chaos theory and its application to Modern Cryptography [6]. The paper analyzed the relationship between chaos and cryptography, based on this study some approaches and their framework for chaotic cryptography system are proposed in the same. A detailed study on how to choose chaotic system and their parameters in digital encryption is also given.

LEI Li-hong et al. proposed a new image encryption algorithm using Logistic map and Hyper-chaos [8]. In the proposed method , key 1 is generated using logistic map which has better randomness, key 2 is generated using hyper-chaos. The overall encryption process has two rounds using the two keys produced. Experimental results shows that the

proposed method has high efficiency, good statistical characteristics and differential characteristics.

Jiu-Lun FAN et al. proposed an image encryption algorithm based on chaotic system [3]. The proposed algorithm overcomes the drawback of noise and shear transformation. Traditional algorithms proposed are not robust against these attacks. The presented algorithm is based on location transformation. A variation on magic –square matrix method is also presented, the proposed variation gives far better efficiency then the original magic-square matrix method. Experimental results obtained after introducing the attacks are good.

C.L.Philip Chen et al. proposed a combined chaotic system for image encryption [2]. The proposed method shows better results when compared to traditional techniques. In the proposed method , the Logistic map and Sine map are combined together. MOD operator is used in the process of encryption. The proposed method's bifurcation diagram and trajectory shows random like behavior and its high sensitivity to initial condition. This proves its adaptability to cryptographic applications.

A new color Image encryption algorithm based on chaotic sequences ranking is proposed by Meng Jian-liang et al. [7]. The image is first scrambled then a one to one relationship is set between image pixels and chaotic sequence generated using Lorenz map. The row and column image ranking is guided by chaotic sequence ranking. On this basis the color image pixel values are shuffled. The R , G and B pixel values interchange based on the guided chaotic sequence which results in image encryption. Experimental results show that the proposed method has good encryption effect.

LU Shong-dong et al. proposed an image scrambling algorithm using chaotic sequence [10]. Based on the size of the image, a chaotic sequence is generated which is 3 times the original image size. Using this sequence a corresponding subscript sequence is generated by sorting the chaotic sequence. The image pixels are transformed based on the subscript generated. This results in image scrambling. Evaluation index is used to analyze the scrambling effect and security. The proposed method has a large key space, a good scrambling effect, statistical characteristics and security.

Wang Yanlin proposed an image scrambling algorithm using chaotic sequence and image mirror mapping [12]. Using the logistic map, a chaotic sequence is generated. Using this sequence a bit XOR operation is applied to pixel values and chaotic sequence. Encrypted image is obtained by applying mirror mapping. Experimental results show that the proposed method is easy and feasible. The method can not only scramble the image pixel positions but also change the pixel values.

II. LOGISTIC MAP

A Logistic function is a population dynamics. It is given as follows

$$F(z)= a*z*(1-z) \quad (1)$$

Where a is the growth rate of population.

It is represented as a simple parabola as can be seen in the figure 1. below, intersecting the 45 degree line at 0.75.

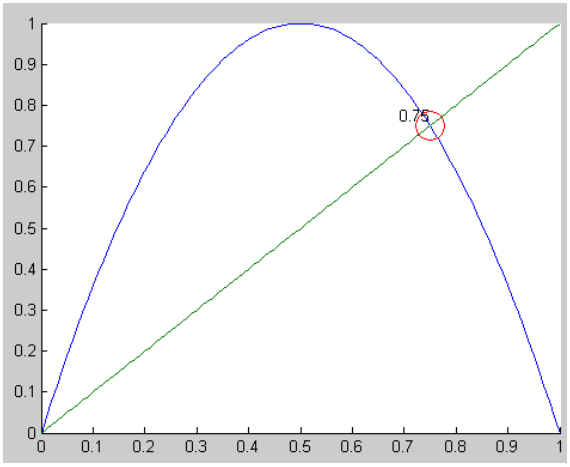


Figure 1. Logistic Map

III. LOGISTIC MAP SHIFTING

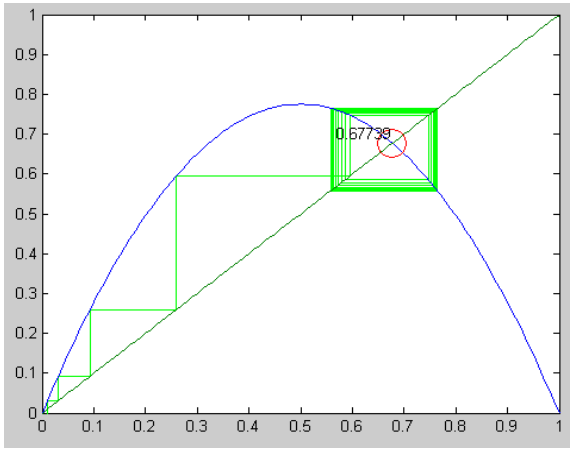
In this paper, a study has been conducted for left shift of Logistic Map, which is one of the most widely used map for chaotic sequence generation.

In the shifting operation, the logistic map is shifted left by a value of 0.1 so that the intersection point of the map with 45 degree line varies and this would result in a different range of chaotic sequence. A total of 9 different shifts have been analyzed and the results obtained for the same are shown in the experimental results.

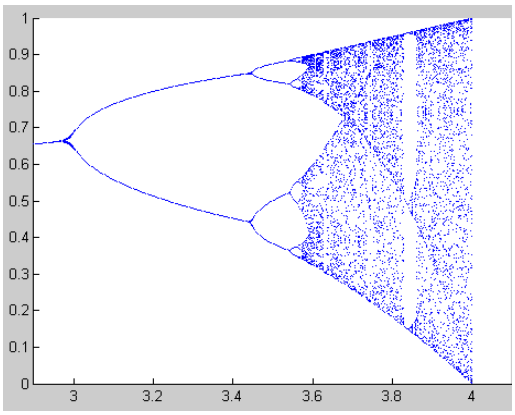
IV. EXPERIMENTAL RESULTS

In this paper, a study on shifting of Logistic map is done. The experimental results displayed below are all the different cases considered shift =0.1 to 0.9.

A. Logistic Map without any shift



(a) Parabola with a=3.1, iterations =100

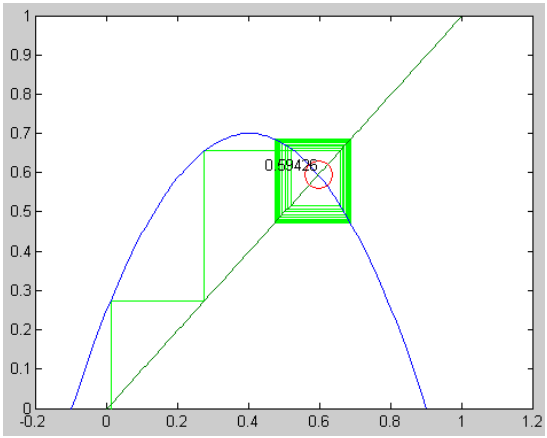


(b) Bifurcation Diagram for Original Logistic Map

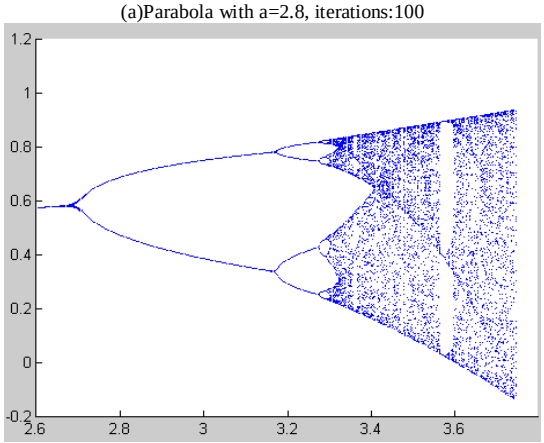
Figure 2. Original Logistic Map

Figure 2(a) shows the parabola of the original logistic Map with the value of growth rate as 3.1 with 100 iterations, Figure 2(b) shows the bifurcation diagram for the original Logistic Map

B. Case 1. Shift =0.1



(a)Parabola with a=2.8, iterations:100

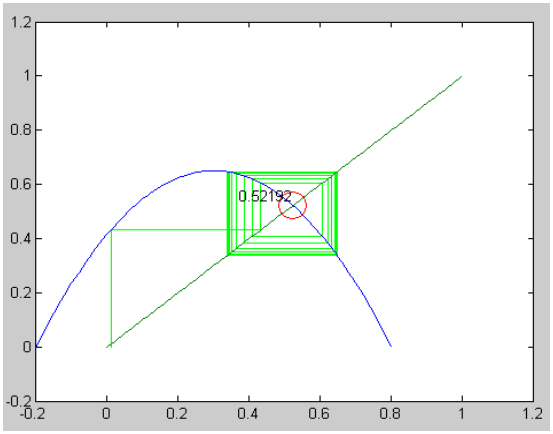


(b)Bifurcation Diagram for Logistic Map shift=0.1

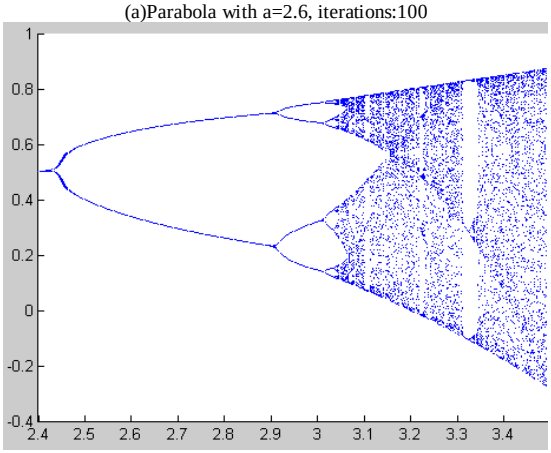
Figure 3. Logistic Map with shift =0.1

Figure 3(a) shows the parabola of the Logistic Map with shift value =0.1 and the value of growth rate as 2.8 with 100 iterations, Figure 3(b) shows the bifurcation diagram for the Logistic Map shift =0.1

C. Case 2. Shift =0.2



(a)Parabola with a=2.6, iterations:100

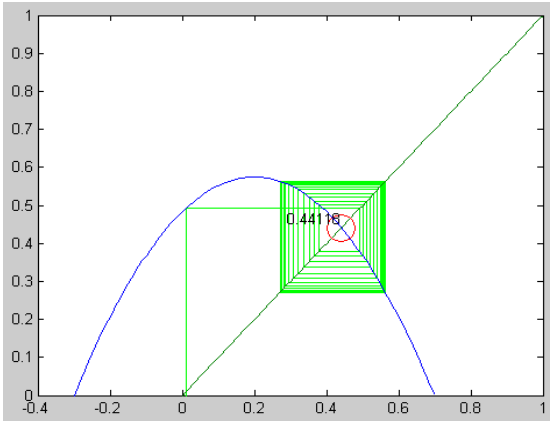


(b)Bifurcation Diagram for Logistic Map shift=0.2

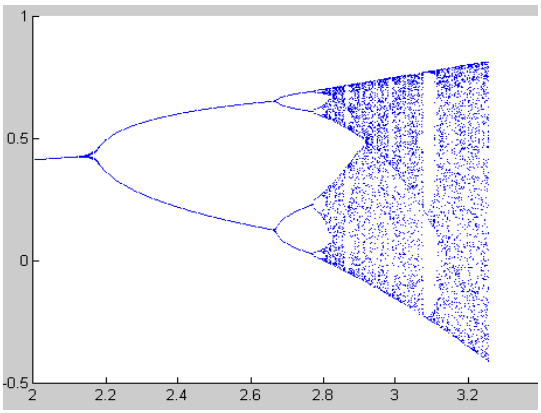
Figure 4. Logistic Map with shift =0.2

Figure 4(a) shows the parabola of the Logistic Map with shift value =0.2 and the value of growth rate as 2.6 with 100 iterations, Figure 4(b) shows the bifurcation diagram for the Logistic Map shift =0.2

D. Case 3. Shift =0.3



(a) Parabola with a=2.3, iterations:100

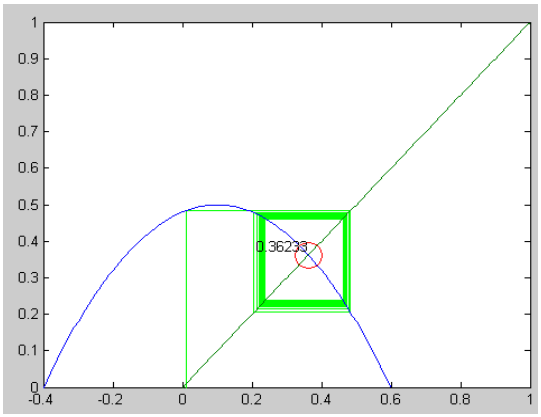


(b)Bifurcation Diagram for Logistic Map shift=0.3

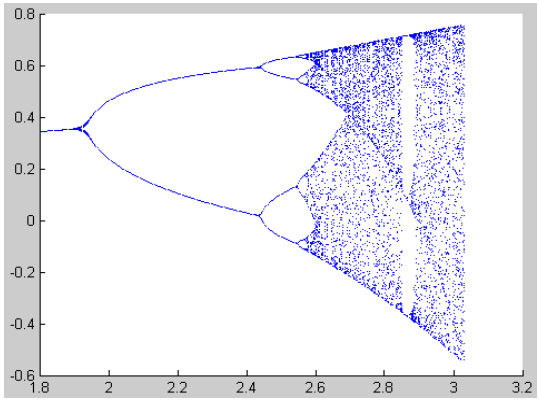
Figure 5. Logistic Map with shift =0.3

Figure 5(a) shows the parabola of the Logistic Map with shift value =0.3 and the value of growth rate as 2.3 with 100 iterations, Figure 5(b) shows the bifurcation diagram for the Logistic Map shift =0.3

E. Case 4. Shift =0.4



(a)Parabola with a=2.0, iterations:100

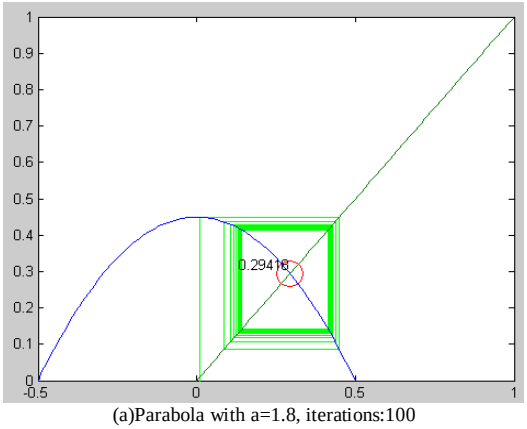


(b)Bifurcation Diagram for Logistic Map shift=0.4

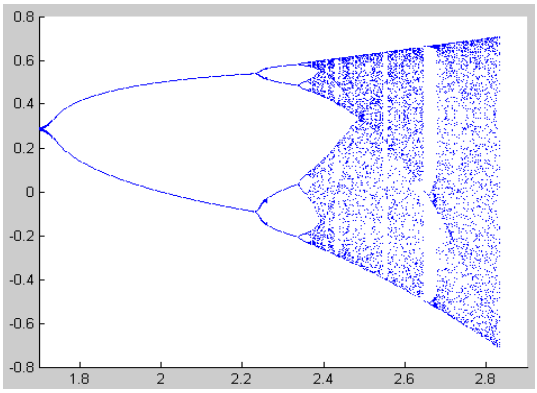
Figure 6. Logistic Map with shift =0.4

Figure 6(a) shows the parabola of the Logistic Map with shift value =0.4 and the value of growth rate as 2.0 with 100 iterations, Figure 6(b) shows the bifurcation diagram for the Logistic Map shift =0.4

F. Case 5. Shift 0.5



(a)Parabola with a=1.8, iterations:100

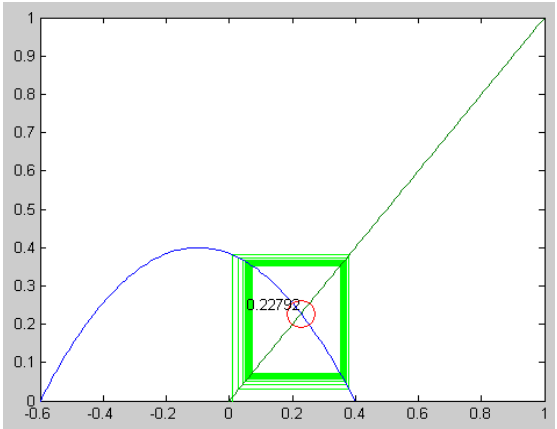


(b)Bifurcation Diagram for Logistic Map shift=0.5

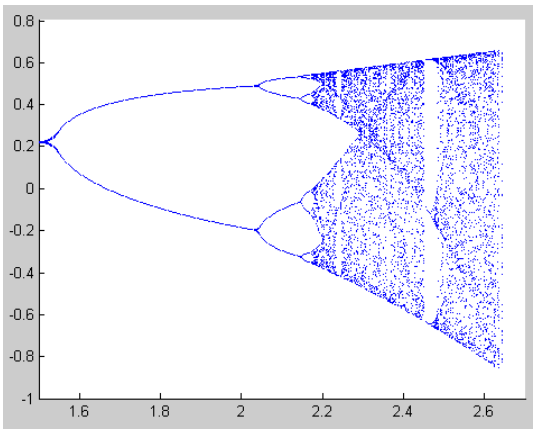
Figure 7. Logistic Map with shift =0.5

Figure 7(a) shows the parabola of the Logistic Map with shift value =0.5 and the value of growth rate as 1.8 with 100 iterations, Figure 7(b) shows the bifurcation diagram for the Logistic Map shift =0.5

G. Case 6. Shift =0.6



(a) Parabola with a=1.6, iterations:100

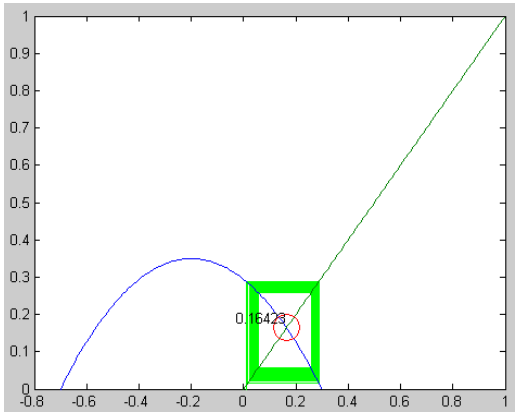


(b)Bifurcation Diagram for Logistic Map shift=0.6

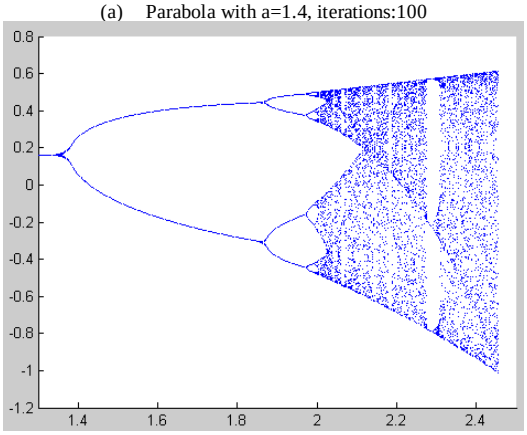
Figure 8. Logistic Map with shift =0.6

Figure 8(a) shows the parabola of the Logistic Map with shift value =0.6 and the value of growth rate as 1.6 with 100 iterations, Figure 8(b) shows the bifurcation diagram for the Logistic Map shift =0.6

H. Case 7: shift =0.7



(a) Parabola with a=1.4, iterations:100

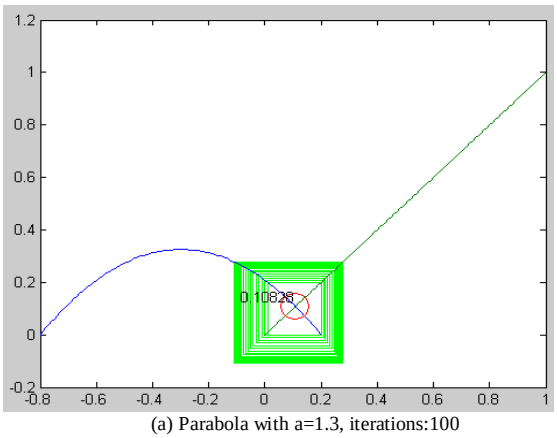


(b)Bifurcation Diagram for Logistic Map shift=0.7

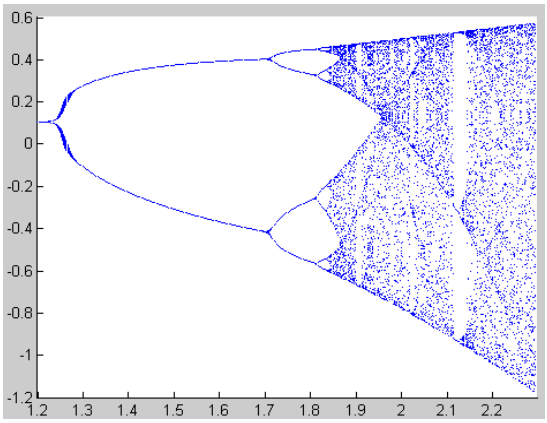
Figure 9. Logistic Map with shift =0.7

Figure 9(a) shows the parabola of the Logistic Map with shift value =0.7 and the value of growth rate as 1.4 with 100 iterations, Figure 9(b) shows the bifurcation diagram for the Logistic Map shift =0.7

I. Case 8 : shift =0.8



(a) Parabola with a=1.3, iterations:100

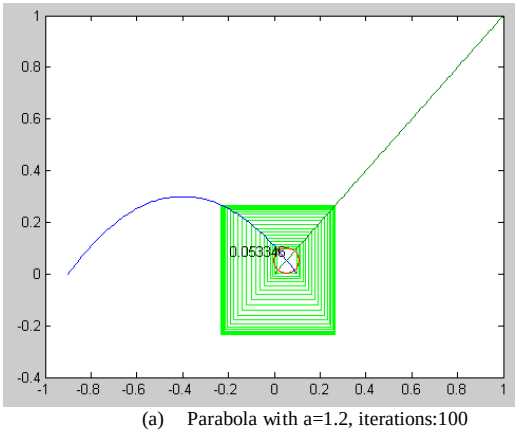


(b)Bifurcation Diagram for Logistic Map shift=0.8

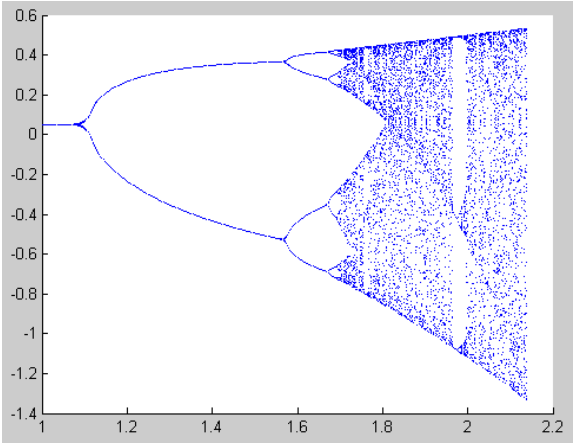
Figure 10. Logistic Map with shift =0.8

Figure 10(a) shows the parabola of the Logistic Map with shift value =0.8 and the value of growth rate as 1.3 with 100 iterations, Figure 10(b) shows the bifurcation diagram for the Logistic Map shift =0.8

J. Case 9: shift=0.9



(a) Parabola with a=1.2, iterations:100



(b)Bifurcation Diagram for Logistic Map shift=0.9

Figure 11. Logistic Map with shift =0.9

Figure 11(a) shows the parabola of the Logistic Map with shift value =0.9 and the value of growth rate as 1.2 with 100 iterations, Figure 11(b) shows the bifurcation diagram for the Logistic Map shift =0.9

TABLE NO I.
TYPE OF LOGISTIC MAP, INTERSECTION POINT OF PARABOLA AND 45 DEGREE LINE, MIN VALUE OF GROWTH RATE WHERE THE PERIOD DOUBLING STARTS, MAX VALUE OF GROWTH RATE AND RANGE.

Type of Logistic Map	Intersection Point	Min Value (a)	Max value (a)	Range
Original Map	0.67	3	4	1
Shift =0.1	0.59	2.7	3.7	1
Shift =0.2	0.52	2.5	3.5	1
Shift =0.3	0.44	2.2	3.2	1
Shift =0.4	0.36	1.9	3.1	1.2
Shift =0.5	0.29	1.7	2.9	1.2
Shift =0.6	0.22	1.5	2.7	1.2
Shift =0.7	0.16	1.4	2.5	1.1
Shift =0.8	0.10	1.2	2.3	1.1
Shift =0.9	0.05	1.1	2.1	1

Table No I gives the values of different intersection points obtained for all the cases of Logistic Map Shifting. The different cases considered are from shift =0.1 till shift =0.9. The intersection is considered between the parabola of Logistic Map and the 45 degree line. The Min value (a) represents the minimum value of growth rate where the Logistic Map starts diverging (Period doubling) , Max value (a) represents the limit of growth rate and the range for Minimum to maximum for all the shifts.

V. CONCLUSION

The properties of logistic map are studied for different left shifts of function. It has been observed that the point at which period doubling case starts varies with the shift. However the range is more or less independent of the shift which means all the maps from 0.1 to 0.3 & 0.9 shift have same range, shifts from 0.4 to 0.6 have the same range, shifts from 0.7 to 0.8 have the same range. Using the shift function it is possible to generate large sets of chaotic sequences which can be used for Image Encryption. Thus making it more robust and untractable. Our future work includes using all these variations for robust image encryption.

REFERENCES

[1] Beck, Amy, "Advising undecided students: Lessons from chaos theory", *NACADA Journal* 19,1 45-49, 1999.

[2] Chen, C. P., Zhang, T., & Zhou, Y., "Image Encryption Algorithm based on a New Combined Chaotic System". *International Conference on Systems, Man, and Cybernetics (SMC),* 2500-2504., 2012

[3] Fan, J. L., & Zhang, X. F., "Image Encryption Algorithm based on Chaotic System". *7th International Conference on Computer-Aided Industrial Design and Conceptual Design. CAIDCD'06.* 1-6., 2006

[4] Garnett, Williams P., "Chaos theory tamed". Taylor & Francis Ltd., 405, 1997

[5] Gershenson, Carlos "Introduction to chaos in deterministic systems." *Working paper. University of Sussex, Brighton, UK.,2003*

[6] Hong, Z., & Ji-xue, D., "Chaos theory and its application in modern cryptography". *International Conference on Computer Application and System Modeling ,ICCASM*. 7,. 332-334, 2010

[7] Jian-liang, M., Hui-jing, P., & Wan-qing, G. "New color image encryption algorithm based on chaotic sequences ranking". *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP'08* , 1348-1351, 2008

[8] Li-Hong, L., Feng-Ming, B., & Xue-Hui, H. "New Image Encryption Algorithm Based on Logistic Map and Hyper-Chaos". *Fifth International Conference on Computational and Information Sciences (ICCIS),* 713-716.,2013

[9] Makris, G., & Antoniou, I. "Cryptography with Chaos". *Chaotic Modeling and Simulation (CMSIM), 1,* 169-178.,2013

[10] Shou-Dong, L., "A New Color Digital Image Scrambling Algorithm Based on Chaotic Sequence". *International Conference on Computer Science & Service System (CSSS),* 922-925., 2012

[11] Wood, C. A. , "Chaos-Based Symmetric Key Cryptosystems". *In other words, 1,* 3, 1-9.,2011.

[12] Yanling, W. " Image scrambling method based on chaotic sequences and mapping". *First International Workshop on Education Technology and Computer Science, ETCS'09.* 3, 453-457., 2009.