IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 24-29
www.iosrjournals.org

Analysis and Comparison of One Dimensional Chaotic Map Functions

Tanu Wadhera[1], Gurmeet Kaur[2]
[1,2] *(Punjabi University, Patiala, Punjab, India)*

Abstract : *Chaotic functions because of their complexity and random nature are used in the cryptographic networks. Chaotic functions are one dimensional, two dimensional, three dimensional in nature. One dimensional chaotic functions are usually implemented in cryptographic algorithms. In this paper two chaotic one dimensional function have been analyzed and compared on the basis of Average, Standard Deviation and Entropy.*
Keywords: *Chaotic functions, Entropy, Logistic Map, One Dimensional Chaotic functions, Tent Map*.

I. INTRODUCTION

Chaotic term is coined from the word chaos. When the system is not in a proper order then it is said to exhibit chaos. Using chaotic function scientists projected a theory that can be mathematically explained known as chaos theory [1, 2]. The behavior of nonlinear dynamical systems has been described using chaotic functions and the behaviors shown are known as chaos [3]. Chaos based systems are deterministic in nature for some values but after certain value of control parameter their nature becomes random and they becomes unpredictable. Because of unpredictability and random nature of chaotic functions most of security and encryption algorithms use chaotic functions. The randomization of chaotic systems may also be valuable for structuring cryptographic functions, to implement them in symmetric key cryptography [4].

The properties of chaotic systems such as sensitivity to control parameter of the chaotic maps, sensitivity to initial conditions, ergodicity, system complexity, mixing property made their applicability in cryptosystems [4,5,6]. Sensitivity to initial condition means a minor change in input would lead to a significant change in output. Chaotic system produces different outputs even if the change in initial condition is after 3rd decimal place [5]. The mathematical equations showing the chaotic behavior are called chaotic functions [5]. Sensitivity to control parameter means the choice of control parameter value in the function equation must ensure chaotic behavior. There are one dimensional, two dimensional, three dimensional chaotic functions but the analysis of functions in this paper has been restricted to one dimensional only because owing to their simplicity these are implemented in cryptography algorithms.

The two chaotic functions discussed in this paper are Logistic map and Tent map function. In first section introduction to the functions has been given. In second section the parameters for analyzing chaotic function have been discussed. In third section the results and discussion of the functions has been given. In last section conclusion has been drawn.

II. DIFFERENT TYPES OF CHAOTIC FUNCTIONS

Carbon Chaotic functions construct good pseudorandom generators to develop most of the cryptographic algorithms with much more security. Various one dimensional chaotic functions used in Quantum cryptography and other algorithms are Logistic Map, Tent map, Piece wise linear map, Sawtooth map. Out of all these functions Logistic Map and Tent Map functions are the best known chaotic functions used in cryptographic algorithms [4]. Basic theory of these two chaotic functions is presented as under.

Logistic Map

The logistic map is one dimensional and the simplest map concerning its implementation in algorithms [4] and is given by:

$$X_{n+1}=A.X_n.(1-X_n) \quad (1)$$

where A is the control parameter such that $0<A<4$, X_n is the initial condition that can have values between 0 and 1 [5]. This function is iterating one, starting with initial condition X_0. The value of n depends upon the number of iterations required. The control parameter controls the behavior of the map. For the values of $A<3.7$ the graph will have the pattern accordingly and for values $3.7<A<4$ the system shows chaotic behavior [5].

Tent Map

Logistic map is topologically conjugate to tent-like map [7], [8], [9], [10], [11]. Tent map is a continuous piecewise-linear map having unit interval in it. Tent map can be given as :

$$X_{n+1}=r.(1-|1-2X_n|) \quad (2)$$

Where r is the control parameter such that $0<r<1$, X_n is the initial condition which can take values between 0 and 1[6]. For $r > 0.5$ the tent map shows sensitivity to the initial values. For $0.99<r<1$ the tent map will be chaotic in nature [6]. This function is iterating one with n number of iterations. Once the initial value is to be given between 0 and 1 then it will keep on taking values depending upon n.

III. PARAMETERS FOR ANALYSIS OF CHAOTIC FUNCTIONS

Energy There are different parameters for analyzing chaotic functions. The analysis of chaotic functions in terms of Average, Standard Deviation and Entropy has been done in this paper. The brief introduction to these parameters has been presented here.

Average

Average provides arithmetic mean of given values. It can be given by the equation:

$$\text{Average}(u)=\sum x/N \quad (3)$$

where $\sum x$ is the sum of values and N is the number of terms. It is calculated by dividing the sum of values with number of terms taken for summation. The expected value of average for sequence to be should be near 0.5[12]. The average shows the deviation of the function from expected value of the function. For a sequence to be random the calculated average value should lie near the expected value.

Standard Deviation

The standard deviation depicts the reliability of data [13]. Higher value of standard deviation depicts that data is stretched over much wider region so reliability of data decreases [13]. Its lower value depicts that data is not stretched and is in proximity of average value and hence data will be reliable in nature [13]. It can be given by the equation:

$$\text{S.D.}=\sqrt{1/(N-1)\sum(x-u)^2} \quad (4)$$

Where u is the average, x is the value calculated using function given by equation (1) and (2) and N is the number of terms taken for calculation. For random sequences it should be small, only then the data would be reliable in nature.

Entropy

Entropy provides the information on an average and is given by symbol H [14]. It is given mathematically by theexpression:

$$H = -\sum_{i=1}^{n} Pi.LogPi \quad (5)$$

Where Pi is the probability for 0 and 1 and the base for log should be 2. If random generators do not have sufficient entropy then intruders can hack security of long keys and sound algorithms [15]. The systems which have less entropy value are more susceptible to attacks as they can be predicted easily. A good pseudorandom generator should be unpredictable in nature [15]. Unpredictability can be calculated in terms of uncertainty. More the uncertainity value of the sequence, the more unpredictable it is [15].

IV. RESULTS AND DISCUSSION

The analysis of chaotic functions has been done based on Average, Standard deviation and Entropy. These parameters are calculated for different set of initial conditions chosen randomly and function is iterated for 10 values. The first set of initial conditions starting from 0.004 with an increment of 0.010 till 0.994 is taken for which the X_{n+1} is calculated for 10 points and then the average, standard deviation of X_{n+1} is calculated by directly using the formula given by equation (3) and (4). For entropy, chaotic functions iterated values X_{n+1} are converted in to sequence of 1's and 0's using [16]

$$b = \begin{cases} 0 \; if \; x(n+1) < 0.5 \\ 1 \; if \; x(n+1) \geq 0.5 \end{cases} \quad (6)$$

After getting binary sequence, entropy is calculated using formula given by equation (5).

The results obtained from analysis are shown graphically in figure 1 to11. After analysis, comparison of these two chaotic functions has been summarized in Table 1.

Analysis of Logistic Map has been given in figure 1,2,3,4 for different values of A. For Fig.1 all calculations has been done for same initial condition (X_n) with number of iterations equal to 20.

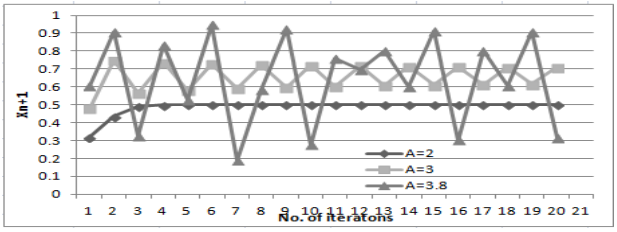

Fig.1: Comparison of logistic map for different values of control parameter (A).

For A=2; variation of X_{n+1} with number of iterations is increasing up to 3 iterations, after that it becomes constant. For A=3; plot shows some variations as opposed to the behavior for A=2. For A=3.8; behavior is chaotic. It can be concluded from the analysis of Fig.1 that variation of X_{n+1} with number of iterations is sensitive to system control parameter A. It can be inferred from Fig.1 that when A>3.7 map shows chaotic behavior.

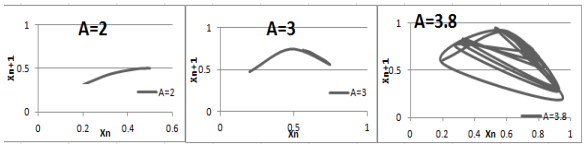

Fig.2: Comaprison of scatter plots for Logistic Map for different values of control parameter (A).

Fig. 2 gives the scatter plot with X_{n+1} and X_n for different values of A. The plot shows the behavior of map is monotonic for A=2, little oscillatory for A=3 and chaotic for A=4. Similar results have been plotted by S. V. Kartalopoulos [5].
Fig.3 shows variation of average with X_n. The rationale behind the calculation of average and standard deviation of values for different initial conditions is to analyze the performance of map.

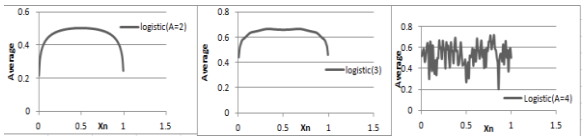

Fig.3: Comparison of Average for different values of control parameter (A).

For A=2, value of average is increasing initially then becomes constant and then it decreases the way it has increased. It is similar to logistic map's curve. For A=3, the curve show perturbations as opposed to A=2, shows chaotic behavior for A=4.

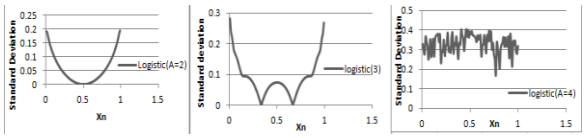

Fig.4: Comparison of Standard Deviation for different values of control parameter (A).

Fig.4 shows variation of standard deviation with X_n. For A=2, the curve is inverted logistic curve. For A=3 curve is similar to A=2 with little perturbation, shows chaotic behavior for A=4.
Analysis of Tent map has been shown in Fig. 5,6,7,8 for different values of r. For fig.5 calculations have been done for same X_n value with number of iterations equal to 20 for r=0.2, r=0.6 and r=0.993.

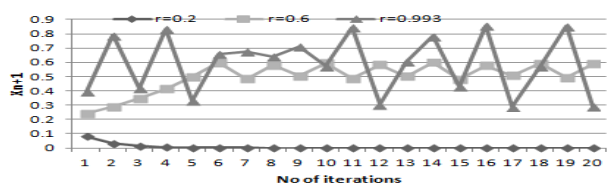

Fig.5: Comparison of Tent map for different values of control parameter (r).

Fig.5 shows the variation of X_{n+1} with number of iterations. For r=0.2 the variation of X_{n+1} with number of iterations has defined value up to 2 iterations after that it dies out. For r= 0.6 the curve shows more variations as compared to behavior for r=0.2, shows chaotic behavior for r=0.993.

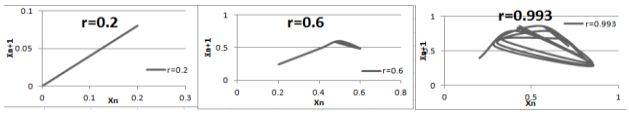

Fig.6: Comparison of scatter plots for Logistic Map for different values of control parameter (r).

Fig. 6 gives the scatter plot with X_{n+1} and X_n for different values of r. The plot shows the behavior of map is linear for r=0.2, perturbated from linear graph for r=0.6 and chaotic for r=0.993.

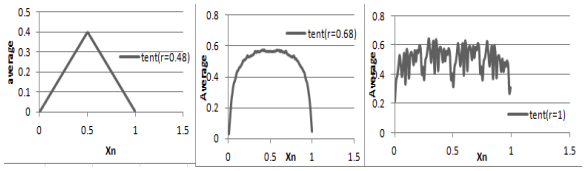

Fig7: Comparison of Average for different values of control parameter (r).

Fig.7 shows the variation of Average with X_n. For r=0.48, the plot shape is triangular as tent map curve. For r=0.68, the variation shows perturbations as compared to r=0.48 and chaotic for r=1.

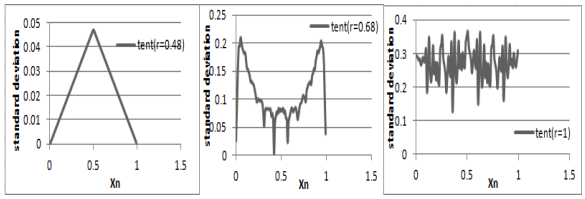

Fig8: Comparison of Standard Deviation for different values of control parameter (r).

Fig.8 shows plot of Standard deviation with X_n. For r=0.48; the variation is triangular similar to tent map curve, perturbated for r=0.68 as compared to behavior for r=0.48 and chaotic for r=1.
After independent analysis the comparison of these two functions have been shown in Fig. 9, 10, 11 based on average, standard deviation and entropy. These parameters are calculated for different X_n chosen randomly and function is iterated for 10 values. The first set of X_n starting from 0.009 with an increment of 0.010 till 0.999 is taken for which the X_{n+1} is calculated for 10 points and then average, standard deviation and entropy is calculated. Similarly values are calculated for different sets of X_n. Then average of calculated average values, standard deviation and entropy is computed.

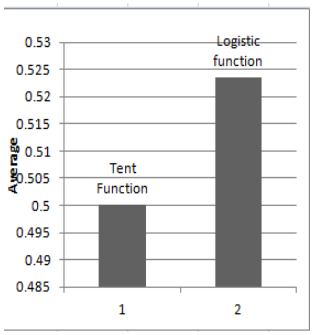

Fig.9: Comparison of Tent and Logistic map based on parameter Average.

Fig.9 shows the comparison of tent and logistic map based on the parameter average. The average value for tent map is 0.500101333 for logistic function the average is 0.523490667

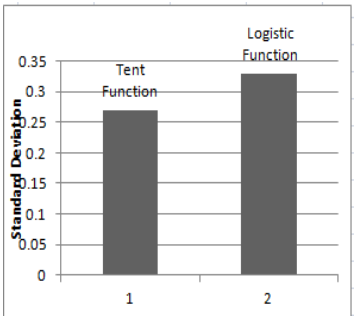

Fig.10: Comparison of Tent and Logistic map based on parameter Standard Deviation.

Fig.10 shows the comparison of two functions based on parameter standard deviation. The value for tent map is 0.269994167 and for logistic map is 0.330062667.

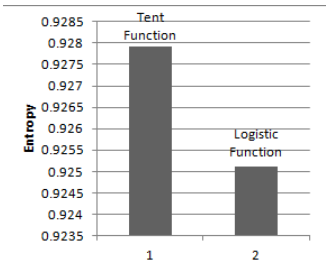

Fig.11: Comparison of Tent and Logistic map based on parameter Entropy.

Fig.11 shows the comparison of two functions based on parameter Entropy. The average entropy for tent map is 0.927911 and for logistic map is 0.92511.

Table1: Comparison of Tent and Logistic Map.

Initial Values	Tent Function			Logistic Function		
	Average	S.D.	Entropy	Average	S.D.	Entropy
0.009-0.999	0.500032	0.269984	0.92028	0.525544	0.327273	0.9145
0.008-0.998	0.500128	0.270242	0.93718	0.511273	0.336833	0.93669
0.007-0.997	0.50016	0.269157	0.92514	0.520897	0.331983	0.93325
0.006-0.996	0.500128	0.270299	0.93231	0.528843	0.328507	0.92586
0.004-0.994	0.500128	0.290299	0.93231	0.528843	0.327273	0.92586
0.001-0.991	0.500032	0.269984	0.92038	0.525544	0.330063	0.9145
Average	0.500101	0.269994	0.927917	0.523491	0.320063	0.92511

Based on the comparison given in table it can be concluded that tent map is showing better performance as compared to logistic map.

V. CONCLUSION

In this paper the two chaotic functions Tent map and Logistic map are analyzed and compared in terms of 3 parameters: average, standard deviation and entropy. Following conclusion have been drawn from the study: (i) For A>3.7 logistic map shows chaotic behavior. (ii) For r>0.99 tent map shows chaotic behavior. (iii)Comparing both functions shows Tent map is better than Logistic map. These functions can be combined to enhance their properties and can be analyzed in terms of these parameters

REFERENCES

[1] J. Gleick, Chaos, the Making of a New Science,Penguin Books Ltd, Harmondsworth, Middlesex, 1987.
[2] E. Ott, Chaos in Dynamical Systems, Cambridge University Press, 2002.
[3] X. Yu et. al, "Chaos Criterion on Some Quadric Polynomial Maps and Design for Chaotic Pseudorandom Number Generator", 2011 Seventh International Conference on Natural Computation, IEEE, 2011, 1373-1376.
[4] C. Rîncu, V. Iana, "S-Box Design Based on Chaotic Maps Combination" IEEE, 2014.
[5] S. V. Kartalopoulos,"Network Security: Synchronization in Chaotic Communication Systems",IEEE,2009.
[6] D. A. Cristina et. Al, "A New Pseudorandom Bit Generator Using Compounded Chaotic Tent Maps", IEEE, 2012, 339-342.
[7] J. Argyris, G. Faust, and M. Haase, "An exploration of chaos," in Texts on Computational Mathematics. New York: Elsevier , vol. VII, 1994.
[8] T. Kohda and A. Tsuneda, "Pseudonoise sequences by chaotic nonlinear maps and their correlation properties" IEICE Transaction Communication, vol.E76-B no. 8, 1993, 855–862.
[9] A. Lasota and M. C. Mackey, "Chaos fractals and noise" in Applied Mathematical Science 97, 2nd ed. New York: Springer Verlag, 1995.
[10] H-O. Peitgen, H. Jürgens, and D. Saupe, Chaos and Fractals. New Frontiers of Science. New York: Springer-Verlag, 1992.
[11] H. G. Schuster, Deterministic Chaos. An Introduction. Weinhem, Germany: VCH Verlagsgesellschaft, 1988.
[12] M.Jessa, "Statistical properties of number sequences generated by 1D chaotic maps considered as a potential source of pseudorandom-number sequences", IEEE, 2001, 449-459.
[13] http://sciece.halleyhosting.com/sci/soph/inquiry/standdev2.htm.
[14] K. Inayah and Rahmat Purwoko "Insertion Attack effects on standard PRNGs ANSI X9.17 and ANSI X9.31 based on Statistical Distance Tests and Entropy Difference Tests", International Conference on Computer, Control, Informatics and Its Applications, IEEE, 2013, 219-224.
[15] A. Vassilev and T. A. Hall, "The Importance of Entropy to Information Security", IEEE Computer Society, 2014, 78-81.
[16] R. Kadir and M. A. Maarof, "Randomness Analysis of Pseudorandom Bit Sequences", International Conference on Computer Engineering and Applications, IPCSIT vol.2, 2011, 390-394.