Chaotic Modeling and Simulation (CMSIM) 4: 415-420, 2018

The Effects on Performance of Using Chaotic Systems in Entropy Source of Deterministic Random Number Generators

Fatih Özkaynak[1]

[1] Firat University Department of Software Engineering 23119 Elazig, Turkey
(E-mail: ozkaynak@firat.edu.tr)

Abstract. The concept of randomness is needed both in science and engineering applications. One of the main design approaches of random number generators is the deterministic random number generators. The deterministic random number generator starts with a seed value and generates algorithmically random numbers. Deterministic random number generators have many advantages. It is low cost, does not require a devoted device and can be implemented in software. But there are also disadvantages. The output can be determined completely from the kernel value. The output sequences are not really independent. A strong entropy or noise source is needed to solve these problems.

The most prominent application areas of chaotic systems are random number generators. Because chaotic systems are a powerful entropy or noise source. This strong relationship between the two disciplines is based on the precise dependence of the chaotic systems on the initial conditions and the control parameters.

In this study, chaos based deterministic random number generators are investigated. New designs have been obtained by using chaotic systems as entropy sources of designs commonly known in the literature. Statistical tests have been used to analyse the performance of new modified designs. Analysis result shows that output of this designs have been used as may application area such statistics, game theory, cryptography, and so on

Keywords: Cryptography, Chaos, Randomness.

1 Introduction

Chaos theory ia an exciting title of science. This theory has many applications in science and engineering [1]. One of the most successful applications in computer science is the random number generator [2-12]. The applications of random numbers have an important place in science and engineering [4]. Therefore, the relationship between these two topics is one of the hot topics on the agenda of the researchers.

In this study, chaos based deterministic random number generators are investigated. New designs have been obtained by using chaotic systems as

Received: 12 July 2018 / Accepted: 26 October 2018

ISSN 2241-0503

entropy sources of designs commonly known in the literature. Statistical tests have been used to analyze the performance of new modified designs. Analysis result shows that output of this designs have been used as may application area such statistics, game theory, cryptography, and so on

The rest of the work has been organized as follows. In the second section, the details of the chaotic system used in the study are given. In the third section, the details of the method used to examine the effects of chaotic system used as a source of entropy on randomness are introduced. The results obtained in the fourth section are presented. The results are discussed and the study is summarized in the last section.

2 Logistic Chaotic Map

It is one of the simplest and most widely used chaotic maps [1]. This emerged in the nonlinear dynamics of biological populations showing chaotic behavior. The logistic map is given in equation (1)

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

In this equation, n indicates the number of iterations, X_n value represents the n. chaotic number. When X_0 (0, 1) is the initial value, it changes in the range of X_n (0, 1).

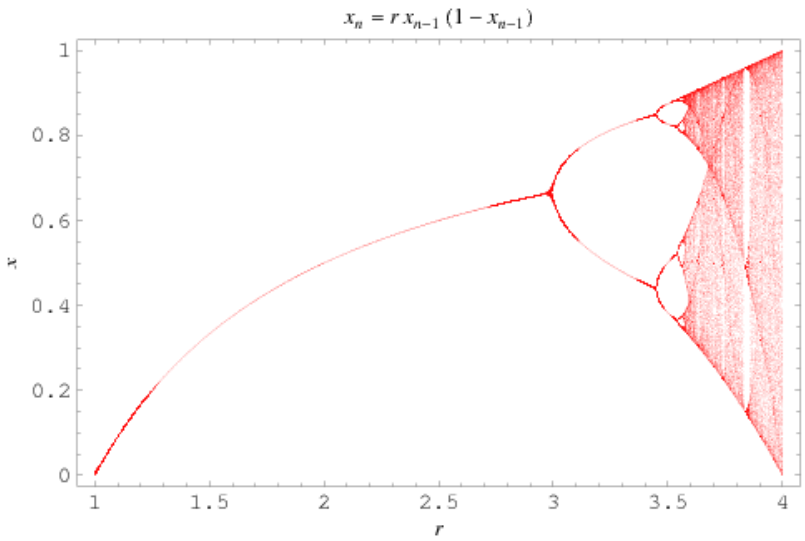

Fig. 1. Phase space diagrams of the Logistic map chaotic system

3 Proposed Analysis System

In the generation of random numbers, the following steps have been used.

- An X_0 initial value in the range (0.1) is selected.
- A value of r is selected in the range (3.5, 4).
- Calculate the X_n value using Equation (1).
- A threshold value is selected. In the study, the threshold value was determined as 0.5.
- if X_n is less than the threshold value, 0 is generated. 1 is produced in the opposite.
- The steps above are continued until a desired number of random sequences are reached.

The chaotic values produced using this method are shown in Figure 2.

X0	A	U0	U1	TP0	TP1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0,9999999	3,9999999	12	18	500019	499981	15507	15547	15754	15761	15593	15856	15689	15645	15462	15815	15610	15562	15578	15510	15588	15523
0,999	3,999	5	17	482787	517213	10456	15549	15613	15796	15606	15799	15224	16617	15457	15781	16155	16166	15397	16315	16886	17183
0,999	3,998	5	18	486583	513417	8848	15821	16258	16485	16666	15487	16061	16015	15763	16939	15839	15696	15922	16028	16462	15710
0,999	3,997	4	20	474686	525314	6551	15347	15258	16537	15818	15509	17465	16524	15243	16404	16470	16722	16148	17151	16021	16832
0,999	3,996	4	21	464914	535086	5960	14870	15338	15723	15684	16195	14876	17608	14719	16261	16392	16834	15314	17349	17928	18949
0,999	3,995	4	17	480594	519406	5901	15767	16991	15977	16218	16968	15366	16854	15706	17279	16294	16411	16749	15729	16684	15106

Fig. 2. Produced chaotic values

4 Analysis Results

In order to examine the effect of the selected initial condition and the control parameter value on the entropy source in the study, both the initial condition and the control parameter were increased by 0.001 within the defined range and chaotic outputs were obtained. these output values were converted to a sequence of 0/1.

1000000 bit sequence has been produced in order to examine whether the generated numbers have a uniform distribution. This bit sequence was divided into 4 bit lengths and converted to 0-15 numbers. The distribution of these numbers is shown in Figure 3.

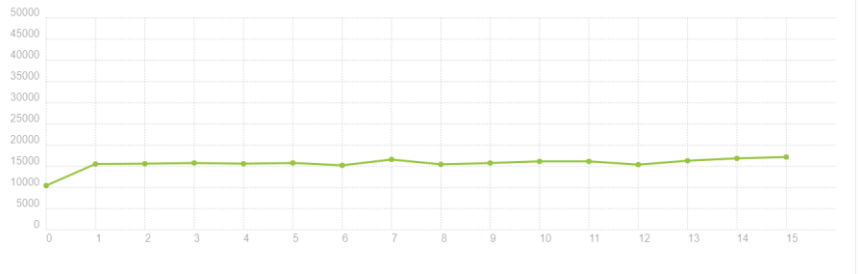

Fig. 3. Distribution of produced random numbers

One of the most important problems of the chaotic systems in computer implementations is the numerical deterioration caused by computational limitations. Two different analysis scenarios have been used to examine the effects of the numerical deterioration. These analyzes include calculations for 3

and 7 digits after the comma. According to the results of the analysis obtained from the 3 digits after the comma, the best results (smooth distribution) were obtained for the values of 3.991, 3.992, 3.993, 3.994, 3.995, 3.996, 3.997, 3.998, 3.999. These results are shown in Figure 4. The most appropriate values among 3-digit numbers after a comma are $X_n = 0.323$ and $r = 3.998$

X0	A	U0	U1	TP0	TP1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.999	3.991	4	25	474427	525573	2546	16683	16010	17763	16982	15131	17344	16152	16768	16887	16161	15965	16876	16470	16003	16259
0.998	3.991	4	18	474972	525028	2641	16857	15711	17922	16873	14954	17419	16104	17267	16876	15822	15789	16841	16506	16217	16201
0.997	3.991	4	21	474908	525092	2528	16995	16252	17825	16604	15156	17600	16194	16720	16883	15801	15707	17012	16551	16077	16095
0.996	3.991	4	20	474395	525605	2548	16880	16087	17705	16646	15059	17392	16265	16701	17059	16013	15593	17130	16716	15971	16235
0.995	3.991	4	20	475281	524719	2597	16800	16150	17751	16646	15196	17512	15973	16983	16869	16099	15787	17087	16402	15966	16182
0.994	3.991	4	20	475139	524861	2642	16610	15904	17866	16935	15171	17445	16105	16830	17107	16113	15687	16972	16518	16076	16019
0.993	3.991	4	20	474509	525491	2660	16770	15880	17644	16985	15271	17185	16056	16798	16907	15971	15728	16877	16695	16381	16192
0.992	3.991	4	18	474085	525915	2502	16636	16065	17922	16883	14805	17548	16192	16762	17102	15873	15870	16901	16495	16180	16264
0.991	3.991	4	19	474432	525568	2559	16850	15974	17547	16755	14907	17201	16126	16967	17274	16166	15669	16857	16683	16176	16289
0.989	3.991	4	20	474709	525291	2480	16754	16039	17856	16998	15203	17432	16293	16852	16725	15759	15878	17040	16603	16056	16032
0.988	3.991	4	19	475649	524351	2598	16981	15872	17694	16965	15230	17515	15987	17014	17024	16104	15709	16809	16352	15961	16185

Fig. 4. Best generated random numbers for 3 digits after the comma

When we increase the digit values after a comma to a 7-digit number, it is observed that the results produced are better than the 3-digit numbers after the comma. The best value obtained for the calculations made by taking 7 digits after the comma is shown in Figure 5. Best result values within 7-digit values after a comma are $X_n = 0.9999999$ and $r = 3.9999999$.

Xn	A	Uzun0	Uzun1	Tp0	Tp1	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15
0,10000001	3,999999	10	22	499070	500930	15443	15676	15572	15568	15742	15708	15549	15647	15650	15511	15492	15745	15505	15670	15650	15872
0,10000001	3,9999991	10	21	499422	500578	15421	15692	15568	15521	15615	15709	15682	15661	15692	15677	15590	15769	15646	15499	15458	15800
0,10000001	3,9999992	10	19	498551	501449	15256	15462	15673	15865	15527	15492	15459	15615	15669	15493	15673	15844	15814	15614	15869	15675
0,10000001	3,999999	10	22	499070	500930	15443	15676	15572	15568	15742	15708	15549	15647	15650	15511	15492	15745	15505	15670	15650	15872
0,10000001	3,9999993	10	21	499140	500860	15432	15744	15394	15709	15675	15651	15548	15827	15584	15502	15467	15472	15908	15692	15660	15735
0,10000001	3,9999991	10	21	499422	500578	15421	15692	15568	15521	15615	15709	15682	15661	15692	15677	15590	15769	15646	15499	15458	15800
0,10000001	3,9999994	10	18	499031	500969	15288	15728	15460	15780	15653	15556	15806	15810	15430	15778	15732	15641	15679	15377	15576	15706
0,10000001	3,9999992	10	19	498551	501449	15256	15462	15673	15865	15527	15492	15459	15615	15669	15493	15673	15844	15814	15614	15869	15675
0,10000001	3,9999995	11	19	499535	500465	15563	15395	15422	15734	15782	15584	15635	15682	15689	15615	15494	15494	15854	15755	15656	15646
0,10000001	3,9999993	10	21	499140	500860	15432	15744	15394	15709	15675	15651	15548	15827	15584	15502	15467	15472	15908	15692	15660	15735
0,10000001	3,9999996	11	22	500518	499482	15623	15685	15692	15606	15605	15540	15772	15668	15716	15393	15755	15679	15692	15477	15592	15505
0,10000001	3,9999994	10	18	499031	500969	15288	15728	15460	15780	15653	15556	15806	15810	15430	15778	15732	15641	15679	15377	15576	15706
0,10000001	3,9999997	11	22	500356	499644	15637	15874	15677	15617	15440	15703	15736	15467	15537	15476	15788	15581	15635	15569	15697	15566
0,10000001	3,9999995	11	19	499535	500465	15563	15395	15422	15734	15782	15584	15635	15682	15689	15615	15494	15494	15854	15755	15656	15646
0,10000001	3,9999998	11	18	499989	500011	15456	15723	15570	15668	15661	15580	15593	15529	15631	15769	15692	15517	15602	15820	15736	15453
0,10000001	3,9999996	11	22	500518	499482	15623	15685	15692	15606	15605	15540	15772	15668	15716	15393	15755	15679	15692	15477	15592	15505
0,10000001	3,9999999	12	20	500381	499619	15673	15581	15632	15469	15534	15942	15808	15558	15722	15582	15709	15611	15470	15581	15572	15556
0,10000001	3,9999997	11	22	500356	499644	15637	15874	15677	15617	15440	15703	15736	15467	15537	15476	15788	15581	15635	15569	15697	15566
0,10000002	3,999999	10	20	499419	500581	15402	15460	15729	15602	15696	15719	15685	15567	15646	15792	15558	15662	15536	15793	15412	15741
0,10000001	3,9999998	11	18	499989	500011	15456	15723	15570	15668	15661	15580	15593	15529	15631	15769	15692	15517	15602	15820	15736	15453
0,10000002	3,9999991	10	18	499953	500047	15557	15670	15592	15568	15638	15643	15656	15682	15761	15504	15729	15536	15531	15510	15752	15671
0,10000001	3,9999999	12	20	500381	499619	15673	15581	15632	15469	15534	15942	15808	15558	15722	15582	15709	15611	15470	15581	15572	15556
0,10000002	3,9999992	10	24	499411	500589	15377	15700	15617	15951	15559	15445	15534	15698	15665	15570	15693	15756	15658	15504	15620	15653
0,10000002	3,999999	10	20	499419	500581	15402	15460	15729	15602	15696	15719	15685	15567	15646	15792	15558	15662	15536	15793	15412	15741
0,10000002	3,9999993	10	18	499673	500327	15470	15834	15644	15608	15677	15544	15580	15621	15537	15471	15582	15750	15807	15593	15569	15713

Fig. 5. Best generated random numbers for 7 digits after the comma

Some statistical information about the numbers produced for $X_n = 0.9999999$ and $r = 3.9999999$ are given below.

- Number of 0-bit: 500.019
- Number of 1-bit: 499.981
- Longest run length of 0-bit: 12
- Longest run length of 0-bit: 18
- The desired number for each of the numbers 0-15: 15.625
- Number of 0: 15507
- Number of 1: 15547
- Number of 2: 15754
- Number of 3: 15761
- Number of 4: 15593
- Number of 5: 15856
- Number of 6: 15689
- Number of 7: 15645
- Number of 8: 15462
- Number of 9: 15815
- Number of 10: 15610
- Number of 11: 15562
- Number of 12: 15578
- Number of 13: 15510
- Number of 14: 15588
- Number of 15: 15523

Figure 6 shows the analysis result showing that the random numbers produced for the best values have a uniform distribution.

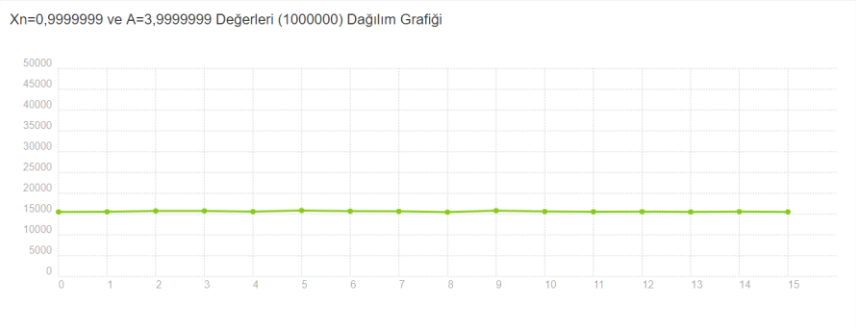

Fig. 6. Distribution of produced random numbers for X_n = 0.9999999 and r = 3.9999999

5 Conclusions

The most distinctive feature of chaotic systems is its dependence on initial conditions and control parameters. In this study, the effects of the initial

conditions and control parameters selected for random number generators, which are an application area of chaotic systems, were investigated.

In the study, logistic map is used as a source of entropy. Logistic maps is the most common known chaotic system and it has simple structure. The most appropriate initial condition and control parameter for the logistics map were analyzed. The calculation sensitivity was taken into account when performing these analyzes. The results of the analysis showed that the most appropriate deterministic random numbers are generated for X_n = 0.9999999 and r = 3.9999999.

Acknowledgment

This study is supported by the Firat University Scientific Research Project (TEKF.18.02).

References

1. J. Sprott, Elegant Chaos Algebraically Simple Chaotic Flows. World Scientific, 2010.
2. A. J. Menezes, P. C. Oorschot, S. A. Vanstone. Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, USA, 1997.
3. W. Schindler: Random Number Generators for Cryptographic Applications. C .K. Koc (ed.): Cryptographic Engineering. Springer, Signals and Communication Theory, Berlin, 2009.
4. F. Özkaynak, Cryptographically secure random number generator with chaotic additional input, Nonlinear Dynamics, November 2014, Volume 78, Issue 3, pp 2015–2020.
5. P. Gauravaram, L. R. Knudsen, K. Matusievicz, F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen. Grøstl - a SHA-3 candidate (October 31, 2008). Available online at http://www.groestl.info/Groestl.pdf
6. T. Stojanovski, L. Kocarev, Chaos-based random number generators – Part I: Analysis, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (2001) 281-288.
7. X. Wang, X. Qin, A new pseudo-random number generator based on CML and chaotic iteration, Nonlinear Dynamics 70 (2012) 1589–1592.
8. S. M. R. Farschi, H. Farschi, A novel chaotic approach for information hiding in image, Nonlinear Dyn (2012) 69:1525–1539
9. X. Wang •X. Bao, A novel block cryptosystem based on the coupled chaotic map lattice, Nonlinear Dyn (2013) 72:707–715
10. N. Liu, D. Guo, G. Parr, Complexity of chaotic binary sequence and precision of its numerical simulation, Nonlinear Dyn (2012) 67:549–556
11. P. Gong, P. Li, W. Shi, A secure chaotic maps-based key agreement protocol without using smart cards, Nonlinear Dyn (2012) 70:2401–2406
12. L. Kocarev. G. Jakimoski, Pseudorandom bits generated by chaotic maps, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 50 (2003) 123-126.