International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Chaotic Binary Sequence Generator based on Logistic Map

K. Chidananda Murthy, Mahalinga. V. Mandi, R. Murali

Abstract— Pseudorandom binary sequences find various applications in different areas such as security, communication, steganography and cryptography. The properties like sensitivity to initial condition, ergodicity, mixing property and dynamic behavior are used in the designing of random number generators known as chaotic systems. In this study, an efficient chaotic binary sequence generator using logistic map is proposed, implemented and analyzed. The proposed binary sequence generator generates 50 chaotic sequences by varying initial condition with fixed system parameter. Subsequently, the generated sequences are transformed to binary sequences using thresholding method. The output of binary sequences is statistically tested with FIPS 140-2 test suite in order to identify the specific properties expected for truly random binary sequences. The experimental results prove that the generated binary sequences possess identical characteristics of true random numbers and can pass all tests of FIPS 140-2 test suite.

Keywords: Chaotic map, chaotic binary sequence, logistic map, FIPS 140-2 and poker test.

I. INTRODUCTION

Communication technology and the popularity of the internet have expanded the field of data transmission and reception which leads to new challenges for securing user data from illegal access. Today, almost everyone across the globe is using internet for exchanging information. Hence, information security is of fundamental importance against unauthorized eavesdropping. Cryptographic techniques are the most popular and widely used methods to deal with the problems of information security. Several security systems make use of different cryptographic techniques to protect the data [1]. Various encryption methods are reported in literature. Amidst, pseudorandom binary sequence-based encryption method is utilized across various fields such as military, spread spectrum communications, watermarking and stochastic computation because of its execution speed, easy implementation and high security [2, 3, 4]. Many research efforts have been carried out on the generation of pseudo random numbers. Most of earlier methods depend on the linear congruential method, mid square method, linear and nonlinear feedback shift registers. However, these methods have limited security due to their fixed linear structure [5]. Further to this, these methods cannot satisfy the conventions of Golomb [6]. Hence, it is an interesting area of research to generate pseudorandom numbers with good statistical properties using cryptographic techniques.

Recently, nonlinear dynamical systems, chaos theory has caught more attention from researchers for generating random numbers. Chaotic systems are nonlinear deterministic, nonperiodic and non-converging in nature. The future importance of chaotic systems is dependent on their initial condition and system parameter. Properties of chaotic systems such as sensitivity to initial conditions, system or growth parameter, ergodicity, mixing property, flexibility of the length of sequences, good correlation properties, difficulty of interception and the multiple access capability [7] make the chaotic systems a potential candidate for spread spectrum communication. In addition to this, chaotic sequences are generated by deterministic systems, random like but they can be reproduced.

In this study, an efficient chaotic binary sequence generator using logistic map is proposed. 50 chaotic sequences are generated directly from the logistic map function by varying initial condition with discrete fixed system parameter. These analog chaotic sequences are converted to binary sequences using thresholding method. The randomness properties of the corresponding chaotic binary sequences are investigated. Statistical properties of the generated sequences are validated employing FIPS 140-2 test suite. Results reveal that the binary sequences pose good attributes of true random numbers, difficult to predict and stable.

The rest of the paper is structured as follows. Section 2 presents the review related works in this domain. Section 3 explains the logistic map function. Section 4 presents the functioning of the planned chaotic binary sequence generator. Section 5 provides numerical results and discussion. Section 6 concludes the paper followed by relevant references.

II. RELATED WORKS

Swami and Sarma [1] designed a pseudorandom number generator using logistic map function for spread spectrum communication.

Manuscript published on November 30, 2019.
* Correspondence Author
K. Chidananda Murthy*, Research Scholar, Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India.
Mahalinga. V. Mandi, Professor, Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India.
R. Murali, Professor, Department of Mathematics, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India.

Performance of the proposed generator was validated on a multipath environment with Rayleigh channel. Kanso et al. [2] proposed two different methods for binary sequence generation. The first method was proposed using 1D logistic map and the second method was proposed with two logistic map functions. Beker and piper's test suites were employed to detect the characteristics of the binary sequence.
Results showed that the 95% of binary sequences passed the tests. Pseudorandom number generator using non-stationary logistic map was presented by Liu et. al. in [3]. Statistical characteristics of the produced sequence was analyzed with Beker and Piper test suites. Experimental results showed that the generated sequences have good characteristics of true random numbers. Fatima and Ali [7] developed a chaotic binary sequence generator. The authors analyzed the autocorrelation of the generated binary sequence. Length of the generated sequence was compared with conventional sequences. Results demonstrated that the chaotic binary sequence outperforms the conventional sequences in several aspects such as multiple access, length and complexity. However, statistical properties of the generated sequence were not analyzed. In 2016, Falih et al., presented two binary sequence generators using feedback shift register and chaotic map function. Quality of the generated sequence was tested with FIPS 140-2 and visual test. FIPS 140-2 was used to detect the characteristics of the generated sequence and visual test was used to detect the patterns in the bit. Results proved that the chaotic based generator was better than shift register based generator in eradicating linearity. Mandi et al. proposed a sequence generator using chaotic map function. In literature, many researchers have designed chaotic binary sequence generator using logistic map function. Each generator has its own merits and demerits. An important property of the chaotic system is sensitivity to initial condition. Most of the researchers generated one or two chaotic binary sequences and analyzed their statistical properties. However, no author has attempted to generate 20 or more sequences. Keeping this in context, this study intends to generate 50 chaotic binary sequences with each of 200000-bit length and analyze the statistical properties of the generated binary sequences with FIPS 140-2 test suite.

III. LOGISTIC MAP

Chaotic systems have dynamic characteristics and can be used as a pseudo random generator. One of the simplest and most commonly used chaotic non-linear system is logistic map. In this study, logistic map is utilized for generating chaotic binary sequence.

Mathematically logistic map function can be stated as:

$$x_{n+1} = \lambda x_n(1 - x_n) \qquad (1)$$

Where, x_n is the state variable, [0,1], λ is the system or growth parameter [1,4] and n is the number of iterations, [0, ∞]. For any initial value x_n [0,1], the sequences are found to be non-linear and non-periodic. Fig.1 shows the sensitivity of the dynamical behavior of the logistic map changes with respect to two different initial conditions, x_n=0.01, x_n=0.02 with same bifurcation parameter λ= 3.9999. Both the curves start almost at the same point and eventually after 5 iterations the state will have completely different or unrelated patterns. It proves that with small difference in initial conditions, the resulting sequences are uncorrelated.

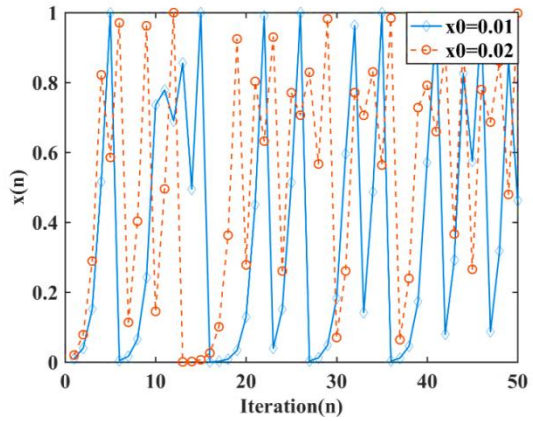

Figure.1 Sensitivity with respect to initial condition for first 50 iterations when λ =3.999

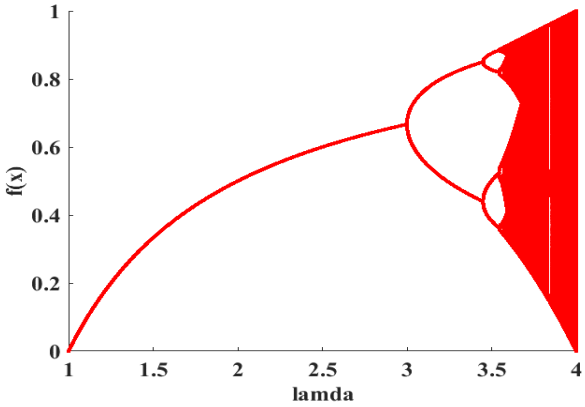

Figure.2 Bifurcation diagram

Fig.2 depicts the bifurcation diagram of logistic map as the system parameter λ is varied. Behavior of the logistic map is analyzed by varying system parameter from 1 to 4. As in Fig.2, the dynamical behavior of logistic map lies in the range [0,1]. The system has one steady value when system parameter is varied from 1 to 3. After increasing the value of the system parameter λ, almost from 3.1 to 3.59, the system will have two values. When the system parameter λ > 3.59, the system exhibits increase in periodicity and has many values.

IV. PROPOSED PSEUDORANDOM NUMBER GENERATOR

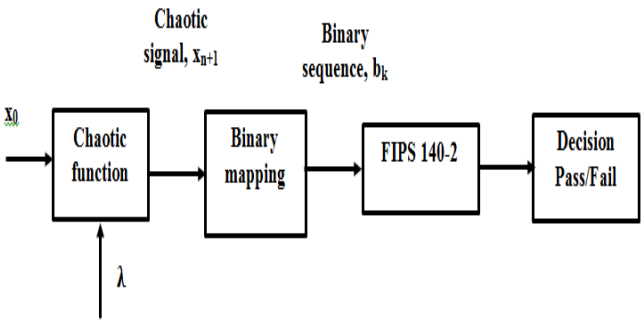

Figure.3 Framework of the proposed chaotic binary sequence generator

Fig.3 depicts the framework of the proposed chaotic binary sequence generator. The chaotic signal generator generates a random signal based on logistic map. The magnitude of the generated sequences heavily relies on the initial condition x_0 and system parameter λ value. Generating a chaotic signal from logistic map is described as:

$$x_{n+1} = \lambda x_n(1 - x_n) \quad (2)$$

The generated chaotic signal is converted to a digital signal by using a thresholding method.

$$b_k = f(x_n) = \begin{cases} 1 & if\ x_n > Th \\ 0 & otherwise \end{cases} \quad (3)$$

where, *Th* is a thresholding value, defined by experimentation. In this study, 50 chaotic binary sequences are generated by varying initial condition x_0 with fixed system parameter.

V. EXPERIMENTAL RESULTS AND DISCUSION

In the following section, simulation results of the proposed chaotic binary sequence generator are presented.

A. Simulation result

The proposed chaotic binary sequence generator using logistic map is implemented in MATALB2016a environment. 50 sequences, each of 200000 bits are generated by varying initial condition with fixed system parameter. Subsequently, the generated sequences are converted to binary sequences using thresholding method. Fig.4 illustrates the sample of the generated logistic map function f(x) as a function of x for x_0=0.1 and λ=3.9999.

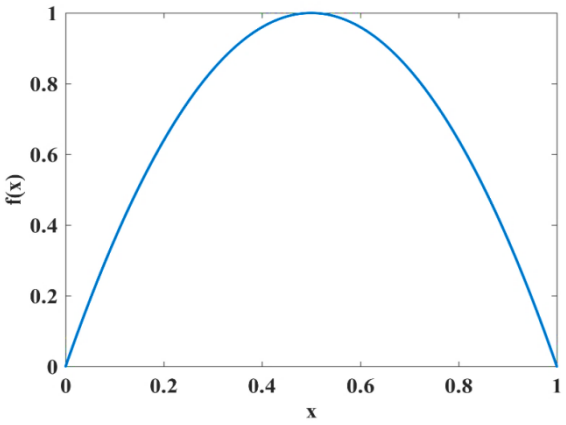

Figure.4 Logistic map function

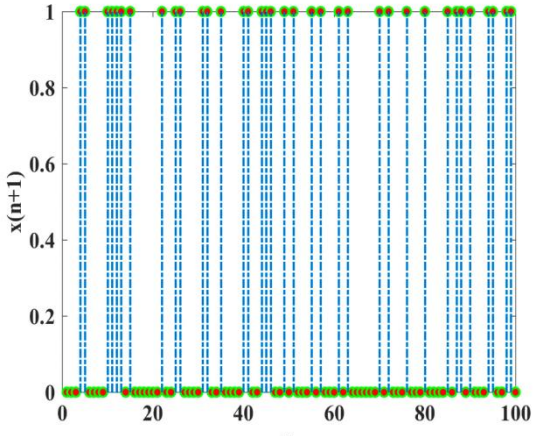

Figure.5 Sample of generated binary sequence (x0=0.01 and λ=3.9999)

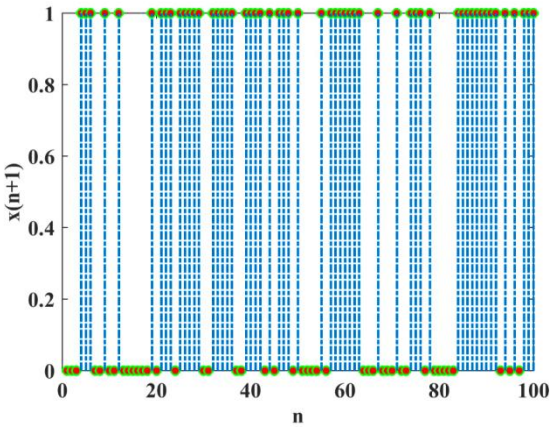

Figure.6 Sample of generated binary sequence (x0=0.02 and λ=3.9999)

Fig.5 and Fig.6 shows the sample of generated chaotic binary sequences for x_0=0.01 and x_0=0.02 respectively. From both figures, it is observed that the generated sequences are different which shows that a small difference in initial conditions results in uncorrelated sequences.

B. Statistical testing

The most popular test suits are (i) National Institute of Standards and Technology (NIST) (ii) Federal Information Processing Standard (FIPS) 140-2 (iii) Diehard and (iv) The Donald Knuth's Statistical test. In this study, FIPS 140-2 test is employed for testing the statistical characteristics of the generated binary sequences.

FIPS 140-2 TEST

The FIPS 140-2 test suite issued by NIST has been widely utilized for analyzing the statistical characteristics of the binary sequence generated by the Pseudo Random Number Generators (PRNGs). It is a statistical package comprising of four tests namely (i) monobit test (ii) poker test (iii) run test and (iv) long run test. These four tests are applied to verify the statistical properties. Each of these tests requires a single stream of 20,000 bits from the generated binary sequence under investigation. Any failure in one of these tests means that the generated binary sequence is not random.

The simulation results demonstrate that the required interval of the FIPS 140-2 monobit test corresponds to the confidence level with significant level $\alpha=10^{-4}$. The required interval of the FIPS 140-2 poker test corresponds to chi-square test with significant level $\alpha=10^{-6}$. The required intervals of the FIPS 140-2 run test corresponds to the confident interval with significant level $\alpha=1\ X10^{-7}$. FIPS 140-2 can be described as follows:

Monobit test

The main focus of the monobit test is to calculate the proportion of ones and zeros for the whole sequence. It is used to determine whether the number of zeros and ones in a sequence are approximately same. In monobit test, the number of ones or zeros is counted and stored in N. The test binary sequence is random or passed, if 9652>N<10,346. The

result of monobit test is reported in Table 1. From Table 1, it can be observed that the number of ones, N lies in the specified range for all the sequences. It is proved that the generated sequences are true random numbers. For example, when x_0=0.08, N=9938, monobit test passes.

Table 1. Monobit test result on the binary sequences for different initial conditions with λ=3.9999

Sl.No.	x_0	N	Results	Sl.No.	x_0	N	Result
1	0.01	10048	PASS	26	0.26	9935	PASS
2	0.02	10088	PASS	27	0.27	10061	PASS
3	0.03	10099	PASS	28	0.28	10068	PASS
4	0.04	10064	PASS	29	0.29	10032	PASS
5	0.05	10061	PASS	30	0.3	9996	PASS
6	0.06	10084	PASS	31	0.31	10013	PASS
7	0.07	10010	PASS	32	0.32	10064	PASS
8	0.08	9938	PASS	33	0.33	9989	PASS
9	0.09	10051	PASS	34	0.34	10089	PASS
10	0.1	10056	PASS	35	0.35	10120	PASS
11	0.11	10124	PASS	36	0.36	10114	PASS
12	0.12	10046	PASS	37	0.37	10093	PASS
13	0.13	10109	PASS	38	0.38	10006	PASS
14	0.14	10086	PASS	39	0.39	10093	PASS
15	0.15	10010	PASS	40	0.4	10134	PASS
16	0.16	10048	PASS	41	0.41	10173	PASS
17	0.17	10195	PASS	42	0.42	10108	PASS
18	0.18	10122	PASS	43	0.43	10078	PASS
19	0.19	9996	PASS	44	0.44	10038	PASS
20	0.2	10067	PASS	45	0.45	10031	PASS
21	0.21	10042	PASS	46	0.46	10015	PASS
22	0.22	9876	PASS	47	0.47	10128	PASS
23	0.23	10056	PASS	48	0.48	10025	PASS
24	0.24	10010	PASS	49	0.49	10048	PASS
25	0.25	10160	PASS	50	0.5	9971	PASS

Poker test

In poker test, the 20,000-bit sequence is divided into 5,000 contiguous 4-bit segments. The number of possible occurrences of each of the 16 possible 4-bit segment value is counted and stored in y(j), where 0<j<15. The poker test is evaluated by using Equation (4),

$$P = \left(\left(\frac{16}{5000}\right)\left(\sum_{j=0}^{15} y(j)^2\right)\right) - 5000 \qquad (4)$$

The test sequence is random or passed for poker test if 1.03<P<57.4. The outcome of the poker test is summarized in Table 2. From Table 2, it can be observed that the all the 50 chaotic binary sequences pass the poker test.

Table 2. Poker test result on the binary sequences for different initial conditions with λ=3.9999

Sl.No.	x_0	P	Results	Sl.No.	x_0	P	Result
1	0.01	13.8368	PASS	26	0.26	10.0608	PASS
2	0.02	20	PASS	27	0.27	19.424	PASS
3	0.03	20.1152	PASS	28	0.28	23.6032	PASS
4	0.04	14.1568	PASS	29	0.29	7.4432	PASS
5	0.05	10.9888	PASS	30	0.3	28.9216	PASS
6	0.06	5.7472	PASS	31	0.31	6.7328	PASS
7	0.07	15.072	PASS	32	0.32	23.2768	PASS
8	0.08	18.144	PASS	33	0.33	17.408	PASS
9	0.09	15.872	PASS	34	0.34	17.6832	PASS
10	0.1	18.7392	PASS	35	0.35	15.2	PASS
11	0.11	18.624	PASS	36	0.36	26.0032	PASS
12	0.12	12.6272	PASS	37	0.37	15.5648	PASS
13	0.13	15.2512	PASS	38	0.38	8.768	PASS
14	0.14	16.1664	PASS	39	0.39	20.5056	PASS
15	0.15	24.224	PASS	40	0.4	12.1792	PASS
16	0.16	21.6192	PASS	41	0.41	21.6448	PASS
17	0.17	17.6448	PASS	42	0.42	19.4752	PASS
18	0.18	21.7536	PASS	43	0.43	21.1968	PASS
19	0.19	13.472	PASS	44	0.44	7.5136	PASS
20	0.2	28.992	PASS	45	0.45	19.5968	PASS
21	0.21	12.4864	PASS	46	0.46	12.8768	PASS
22	0.22	20.0704	PASS	47	0.47	19.1616	PASS
23	0.23	17.2224	PASS	48	0.48	17.3056	PASS
24	0.24	16.4544	PASS	49	0.49	7.6224	PASS
25	0.25	19.5904	PASS	50	0.5	16.3456	PASS

Run test

The test sequence is passed if the number of runs of length 1,2,3,4,5 and longer than 5 lies in predefined interval tabulated in Table 3.

Table 3. The required interval of the FIPS 140-2 run test

Run length	Required interval
1	2267~2733
2	1079~1421
3	502~748
4	223~402
5	90~223
>=6	90~223

Sample of the run test of the generated binary sequences are tabulated in Table 4. From the Table 4, it is seen that the generated sequences are true random numbers.

Table 4. Sample outcome of the FIPS 140-2 run test for different initial conditions with fixed system parameter

Run length	Initial conditions					Result
	x_0=0.01	x_0=0.18	x_0=0.23	x_0=0.37	x_0=0.48	
1	2452	2544	2461	2482	2471	PASS
2	1271	1251	1248	1241	1276	PASS
3	640	641	650	668	634	PASS
4	314	297	311	319	330	PASS
5	153	178	145	148	141	PASS
>=6	71	82	83	92	92	PASS

Long run test

The test sequence passes the long run test if there are no runs of length equal to or greater than 34 bits. In this study, all the 50 chaotic binary sequences passed the long run test.

VI. CONCLUSION

In this paper, a chaotic binary sequence generator using logistic map is presented. Chaotic systems are sensitive to initial condition. 50 chaotic sequences, each of 200000 bits are generated by varying initial condition with fixed system parameter. The generated chaotic binary sequences are tested with FIPS 140-2 test suite, which consists of four independent statistical tests namely, monobit test, poker test, run test and long run test to identify the specific properties expected of true random sequences. The experimental results reveal that the proposed chaotic binary sequence has perfect specific characteristics of true random numbers and can be used for cryptographic applications.

REFERENCES

1. D S. Swami and K K. Sarma, 'A logistic map based PN sequence generator for direct sequence spread spectrum modulation systems', In: Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, 780 – 784.
2. A.Kanso and N. Smaoui, 'Logistic Chaotic maps for binary numbers generations', Chaos, Solitons and Fractals, 40, 2009, 2557 – 2568.
3. L. Liu, S.Miao, H. Hu and Y. Deng, ' Pseudorandom bit generator based on non-stationary logistic maps', IET Information Security, 10 (2), 2016, 87 – 94.
4. B. Liu and Q.Chen, 'A method of generating pseudorandom binary sequences based on 3D Chaotic mapping', In: Proceedings of the 3rd International conference on information Management, 2017.
5. S.F. Raza and V.R. Satpute, 'PRACTO: Pseudo random bit generator for cryptographic application', KSII Transactions on Internet and Information Systems, 12(12), 2018, 6162-6175.
6. S.W. Golomb, 'Sequences with randomness properties', Terminal Progress Report under Contract 639498, Baltimore, 1955.
7. C. Fatima and D. Ali, 'New chaotic binary sequences with good correlation property using logistic maps', IOSR Journal of Electronics and Communication Engineering, 5(3), 2013, 59-64.