Pseudorandom Bit Generator Based On Chaotic Parameter Hopping Chaos

Ahmed I. El-Naggary[#1], Karim H. Moussa [*2]
[#1] King Mariott Higher Institute of Engineering, Alexandria, Egypt.
[1] anaggary@gmail.com
[*2] Engineering Faculty, Horus University-Egypt, New Damietta 34518, Egypt.
[2] karim6684@gmail.com

***Abstract*—Pseudorandom bit generators which produce bit sequences have become a significant factor serving human's life in many fields, such as cryptography, spread spectrum wireless communication, computer simulations and error correcting coding. So far, the main source for producing pseudorandom binary sequences was the chaotic systems. Most of the used chaotic systems were stationary ones based on fixed logistic maps or code books. Accordingly, the pseudorandom binary sequences produced were almost stationary and insufficiently secured. In this paper, we propose a novel algorithm for generating pseudorandom codes based on a logistic map with a dynamic hopping parameter. While the main chaotic map is used to generate a chaotic sequence, another chaotic map is utilized to hop the chaotic parameter of the main map. The model numerical analysis, correlation behaviours and statistical tests showed that the proposed algorithm improved the statistical properties, robustness, security against phase space reconstruction methods, ideal correlation properties, and predictable behaviour for the generated bit sequence.**

Keyword - Pseudorandom, NIST, Chaotic, Hopping, Bifurcation

I. INTRODUCTION

Mobile telecommunications are exposing rapid growth and sensitive data interception which in turn necessitates the establishment of more secure media for such communication data. As a consequence continuous development and researches for data encryption algorithms and cryptography is pervasively growing(Clark 2000). The main aspect of the cryptographic system is to generate artificially unpredictable random numbers (RNs) as a source for key generation and encryption applications. Random number generators (RNGs) can be broadly classified as true RNGs (TRNGs), and pseudo RNGs (PRNGs). A TRNG is based on a source sequence emission using natural physical phenomena such as white noise, radioactive decay and chaotic systems (Gude 1985; Yalçın, Suykens, and Vandewalle 2004).

The pseudorandom bit generators (PRBGs) based on chaotic maps are very significant, due to its high security and random behaviour. A chaotic system for generating a pseudorandom sequence are proposed in (Oishi and Inoue 1982). Despite being more complex, but the time-varying chaotic sequence proved to be much better than a fixed one. Due to the non-stationary output behaviour, such type of encryption technique turns to be difficult in prediction and analysis. Constructing a time-varied chaotic system can be effectively done by changing the chaotic system parameters continuously.

In this paper, a novel PRBG which produce pseudorandom bit sequences utilizing a main logistic map with a dynamic hopping parameter. The hopping parameter is also generated in a pseudo-random behavior utilizing another different logistic map. The numerical analysis showed a great performance enhancement over previous bit generator versions considering the randomness and time-varying parameters which in turn leads to more security systems. In this paper, we propose a novel technique for generating a PRBS based on chaotic parameters that were generated using another hopped chaotic map. This dynamic hopping algorithm proved to make chaotic system parameters act in a random-like way which yields to more secure binary sequence generation. The statistical and experimental results show that the proposed dynamic hopping algorithm is hardly predictable and highly secured in terms of phase space reconstruction which makes it very competitive with other PRBS algorithms.

The rest of the paper is organized as follows: Previous related works in the same field are summarized in section II. Traditional logistic maps were briefly discussed in section III. In section IV we propose our PRBG model based on chaotic parameter hopping chaotic system. Experimental statistical tests results for our newly developed bit generator are depicted in section V. In section VI, the simulation results for the generated pseudorandom binary sequence obtained using both traditional and parameter hopped logistic maps are discussed. Finally, the conclusions for our simulation results and related future work are stated in section VII.

II. RELATED WORK

Our proposed algorithm was based on previous versions of bit sequence generators obtained through a survey done on related researches of chaotic PRBG as follows. True random bit generator based on one dimensional piecewise linear chaotic map was proposed in (Addabbo et al. 2006) [1].in (Xie, Wang, and Jiang 2007) [2], A proposed bit generator which changes the system parameter dynamically through a feedback control procedure [3]. A couple of chaotic systems was designed to generate an independent and identically distributed (i.i.d) sequence. The cryptographic analysis showed a random-like generated sequence. Zheng et al. proposed an algorithm for solving the non-uniformity distribution of the generated sequence obtained through the generalized Henon map [4]. The proposed algorithm was based on moving the decimal point of elements in the sequence to the right, cutting off the integer and finally quantifying it into a binary sequence (Zheng et al. 2008) [5].

A binary stream-cipher algorithm was proposed by Wang and Yang using dual one-dimensional chaotic maps to eliminate the degradation of dynamical properties caused by finite states of computer (Wang and Yang 2012) [6]. In order to avoid the non-uniform distribution of the sequence generated, Hu et al. proposed an algorithm based Chen chaotic system (Hu, Liu, and Ding 2013) [7]. Francois et al. developed an algorithm for generating multiple sequences of random codes obtained through mixing the chaotic maps obtained using input initial vector (Francois et al. 2013) [8]. Based on the non-stationary logistic map, Liu et al. proposed a scheme for generating a PRBG. The designed algorithm generated a random-like sequence (Liu et al. 2016) [9].

III. TRADITIONAL LOGISTIC MAP

Chaotic behaviour is mostly displayed mathematically using a 1D map (Lsota and Mackey 1994) [8]. One of the most commonly used 1D maps to generate pseudorandom binary sequences is the logistic map which can be produced through

$$x_{n+1} = f(x_n) = k\, x_n (1 - x_n), \qquad (1)$$

where k is the bifurcation parameter of the logistic map, $x_n = f^{(n)}(x_0) \in N$, $n = 0,1,2,\ldots N$ and f: $N \rightarrow N$, where N denotes an interval. For $3.6 \leq k \leq 4$, equation (1) turns to be chaotic. A real-valued sequence is obtained by using the above function and by iteration of an initial value x_0. The chaotic binary sequences b_n can be generated using

$$b_n = \begin{cases} 0 \text{ for } x_n \leq 0.5 \\ 1 \text{ for } x_n > 0.5 \end{cases} \quad n = 0,1,\ldots N. \qquad (2)$$

The main frame for pseudorandom bit generator based on a traditional chaotic logistic map based on the above equations is shown in Fig.1. Hence, some researches show that the binary sequences $\{b_n\}$ generated are not highly secure and with some weaknesses, as stated in (Alvarez et al. 2003, 2004) [10]. Accordingly, we suggest a new algorithm for generating varying hopping parameter based on another chaotic map as described in the following section.

IV. PARAMETER HOPPING LOGISTIC MAP

In this section, we describe a new algorithm to resolve the weakness of the bit sequence generated through a traditional logistic map. The major change in our new PRBG is based on changing the chaotic parameter from a fixed value to a variable value dependent on another logistic map.

The new variable chaotic parameter vector a_n with size N is generated by

$$a_n = 4 - y_n (4 - 3.6), \qquad (3)$$

$$y_{n+1} = f_r(y_n) = r\, y_n (1 - y_n), \qquad (4)$$

Where, y_{n+1} represent the newly generated chaotic value, based on the previous chaotic value y_n, while r represents the chaotic parameter and is set to 4. The initial value for y_0 is set to 0.1, yields a_n with$N$ length which is equal to 10000. Finally, the proposed new chaotic sequence with a hopped parameter will be generated through

$$x_{n+1} = a_n x_n (1 - x_n), \quad \text{where } n = 1,2,\cdots,\mathrm{N} \qquad (5)$$

The new proposed chaotic binary sequences b_n based on parameter hopping logistic map is shown in Fig.2 and can be generated applying equation (2) on the vector generated by equation (5).

$$\{x_n\}: \; x_0 \quad x_1 \quad x_2 \quad \cdots \quad x_n \quad x_{n+1} \quad x_{n+2} \quad \cdots \quad x_N$$
$$\downarrow \; \textit{Equation} \; (2)$$
$$\{b_n\}: \; b_0 \quad b_1 \quad b_2 \quad \cdots \quad b_n \quad b_{n+1} \quad b_{n+2} \quad \cdots \quad b_N$$

Fig. 1.Mainframe for generating pseudorandom bit sequence using traditional chaotic logistic map.

$$\{y_n\}: \; y_0 \quad y_1 \quad y_2 \quad \cdots \quad y_n \quad y_{n+1} \quad y_{n+2} \quad \cdots \quad y_N$$
$$\downarrow \; \textit{Equation} \; (3)$$
$$\{a_s\}: \; a_0 \quad a_1 \quad a_2 \quad \cdots \quad a_n \quad a_{n+1} \quad a_{n+2} \quad \cdots \quad a_N$$
$$\downarrow \; \textit{Equation} \; (5)$$
$$\{x_n\}: \; x_0 \quad x_1 \quad x_2 \quad \cdots \quad x_n \quad x_{n+1} \quad x_{n+2} \quad \cdots \quad x_N$$
$$\downarrow \; \textit{Equation} \; (2)$$
$$\{b_n\}: \; b_0 \quad b_1 \quad b_2 \quad \cdots \quad b_n \quad b_{n+1} \quad b_{n+2} \quad \cdots \quad b_N$$

Fig. 2.Mainframe for generating pseudorandom bit sequence using parameter hopping logistic map

TABLE 1. Nist Results ForPseudorandom Bit Generators

Type of Test	**Traditional logistic map**		**Parameter hopping logistic map**	
	P-Value	***Conclusion***	***P-Value***	***Conclusion***
1. Frequency Test (Monobit)	*0.18607170765703596*	*Random*	*0.40009192566536733*	*Random*
2. Frequency Test within a Block	*0.18740702062695833*	*Random*	*0.7716225139520125*	*Random*
3. Run Test	*0.04178826098333288*	*Random*	*0.9303878099370719*	*Random*
4. Longest Run of Ones in a Block	*0.0757358003744378*	*Random*	*0.9000797814444522*	*Random*
5. Binary Matrix Rank Test	*0.5700775353820208*	*Random*	*0.5298547388020864*	*Random*
6. Discrete Fourier Transform (Spectral) Test	*0.6970310032898969*	*Random*	*0.05559297481886976*	*Random*
7. Non-Overlapping Template Matching Test	*0.4273387391035214*	*Random*	*0.824474096897771*	*Random*
8. Overlapping Template Matching Test	*0.9074255762195176*	*Random*	*0.9542118108789912*	*Random*
9. Maurer's Universal Statistical test	*-1.0*	*Non-Random*	*-1.0*	*Non-Random*
10. Linear Complexity Test	*0.48837948546813037*	*Random*	*0.27946594555640825*	*Random*
11. Serial test	*0.040209811166077074*	*Random*	*0.7094555988015047*	*Random*
	0.47058098349498734	*Random*	*0.644376873918763*	*Random*
12. Approximate Entropy Test	*0.003805530444709128*	*Non-Random*	*0.9615888377028079*	*Random*
13. Cummulative Sums (Forward) Test	*0.2551001186976895*	*Random*	*0.6580393680308335*	*Random*
14. Cummulative Sums (Reverse) Test	*0.15657952373294165*	*Random*	*0.3650042967423617*	*Random*

TABLE 2. Random Excursions Tests ForPseudorandom Bit Generators

State	Traditional logistic map			Parameter hopping logistic map		
	Chi Squared	***P-Value***	***Conclusion***	***Chi Squared***	***P-Value***	***Conclusion***
-4	*5.694455541483566*	*0.3370937664420536*	*Random*	*3.8588562932586257*	*0.5699110443466062*	*Random*
-3	*12.209234285714285*	*0.032030582465855634*	*Random*	*3.4667623931623948*	*0.6284227621922605*	*Random*
-2	*13.634819853867473*	*0.018103288376204812*	*Random*	*4.602827899124195*	*0.4662443919661713*	*Random*
-1	*3.3346938775510204*	*0.6485343982583003*	*Random*	*1.4729344729344729*	*0.9161718766578935*	*Random*
+1	*2.9510204081632656*	*0.7075370181473756*	*Random*	*6.1737891737891735*	*0.28967395376965044*	*Random*
+2	*1.490904509952129*	*0.914117039024038*	*Random*	*11.866870669339805*	*0.03665820327809488*	*Random*
+3	*1.869916734693877*	*0.8668358298408736*	*Random*	*3.073599999999998*	*0.6886398502349407*	*Random*
+4	*2.5559537267635086*	*0.7680457568120757*	*Random*	*3.002812218555659*	*0.6995522471894431*	*Random*

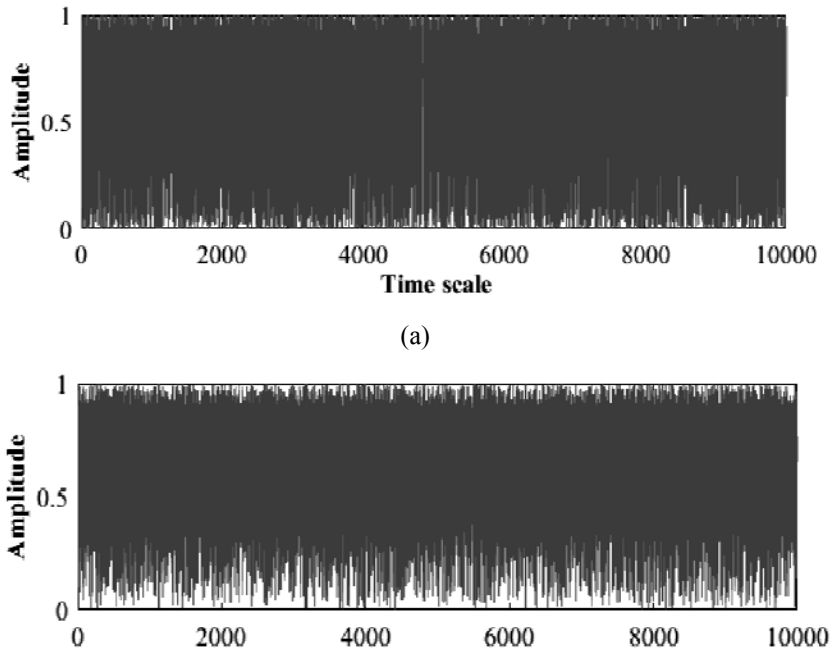
TABLE 3. Random Excursions Variant Tests ForPseudorandom Bit Generators

State	Traditional logistic map			Parameter hopping logistic map		
	Counts	***P-Value***	***Conclusion***	***Counts***	***P-Value***	***Conclusion***
-9.0	*343*	*0.2829343037511922*	*Random*	*322*	*0.7906523464874595*	*Random*
-8.0	*330*	*0.3214609495409527*	*Random*	*340*	*0.9146335044410514*	*Random*
-7.0	*333*	*0.2702064608148309*	*Random*	*391*	*0.6754235581650763*	*Random*
-6.0	*358*	*0.12376498707129498*	*Random*	*391*	*0.6489707595446188*	*Random*
-5.0	*364*	*0.07313979965890892*	*Random*	*351*	*1.0*	*Random*
-4.0	*381*	*0.020224405838067196*	*Random*	*296*	*0.43269151047244103*	*Random*
-3.0	*367*	*0.013710038072158832*	*Random*	*278*	*0.21788699527633115*	*Random*
-2.0	*321*	*0.04745305500706095*	*Random*	*300*	*0.266428582970169*	*Random*
-1.0	*280*	*0.11384629800665805*	*Random*	*327*	*0.36503027183830394*	*Random*
+1.0	*246*	*0.9639675060523949*	*Random*	*325*	*0.3264414887087018*	*Random*
+2.0	*287*	*0.27332167829229814*	*Random*	*321*	*0.5132919253032896*	*Random*
+3.0	*308*	*0.20309178757716784*	*Random*	*364*	*0.8263175463282955*	*Random*
+4.0	*324*	*0.17736881225787016*	*Random*	*373*	*0.7536443136180725*	*Random*
+5.0	*313*	*0.30584678887953964*	*Random*	*344*	*0.9298242261420541*	*Random*
+6.0	*269*	*0.743742417412888*	*Random*	*334*	*0.8466012275077377*	*Random*
+7.0	*266*	*0.7924600886080352*	*Random*	*351*	*1.0*	*Random*
+8.0	*267*	*0.7974773754253042*	*Random*	*364*	*0.8991888016018846*	*Random*
+9.0	*278*	*0.7176739776483174*	*Random*	*403*	*0.6340717432140395*	*Random*

V. STATISTICAL TESTS RESULTS

The National Institute of Standards and Technology (NIST) formulated some specific statistical tests to measure the randomness behavior for the pseudorandom number generators used in cryptographic applications (Rukhin et al. 2010) [12]. These statistical tests were chosen to measure the randomness of the generated binary sequence for both traditional and parameter hopping logistic maps. Classified into 14 statistical tests then categorized into parameterized and non-parameterized tests. The non-parameterized tests include runs test (longest runs of ones), frequency test, discrete Fourier transform test, rank test, random excursions test, cumulative sums test, and random excursions variant test. While the second category for parameterized tests includes; universal statistical test, approximate entropy test, linear complexity test, serial test, frequency test within a block, overlapping and non-overlapping template matching tests. The NIST set a level of 0.01 for each test. Achieving such a level means that 99% of the test samples for the generated sequence samples are truly random. Achieving a p-value ≥ 0.01 means that the generated sequence is truly random with a confidence of 0.99. In our case, 10000 binary sequences were generated, the resultant P-value from each test was calculated for both traditional and parameter hopping logistic maps and tabulated in Tables 1, 2, and 3. The test results show a significant improvement for the P-values obtained through our PRBG based on parameter hopping logistic maps compared to that obtained through traditional logistic maps, which leads to a better random and more secure generated binary sequence.

VI. SIMULATION RESULTS AND COMMENTS

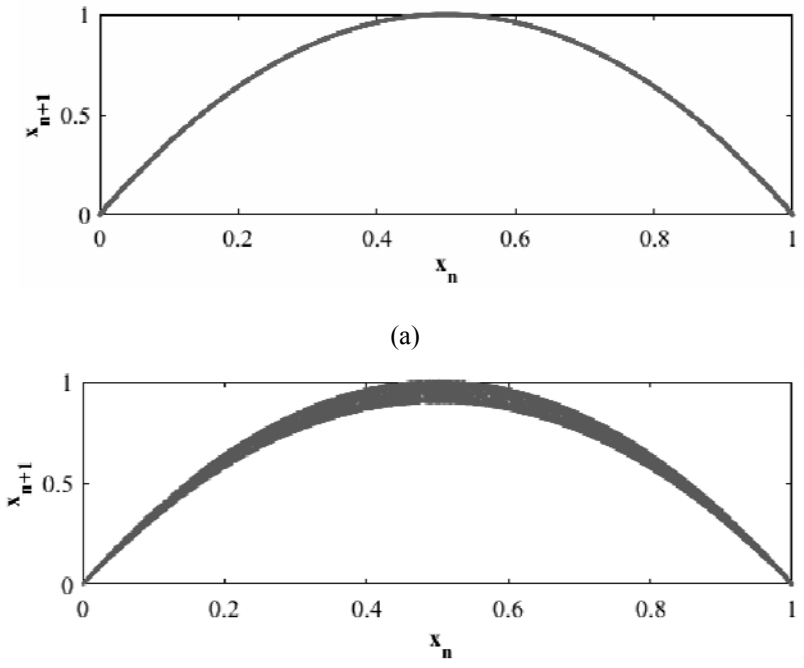


(a)

(b)

Fig. 3 Phase diagram (a) traditional logistic map, (b) parameter hopping logistic map

Fig.3. shows the phase diagram using 10000 successive points obtained by iteration of both (a) traditional logistic map and (b) parameter hopping logistic map. We could recognize that the fluctuations of successive points in Fig.3b are larger than that in Fig.3a which leads to improvement of the generator system robustness against known-system based attacks [14].

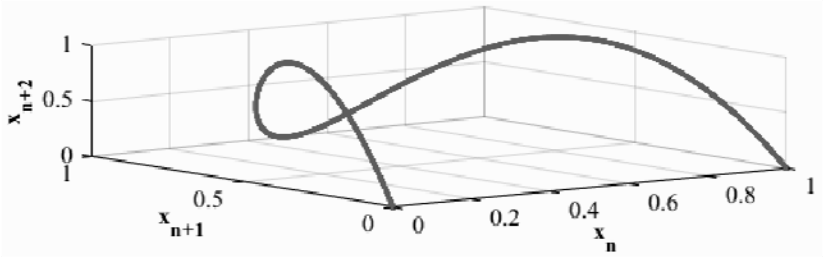


(a)

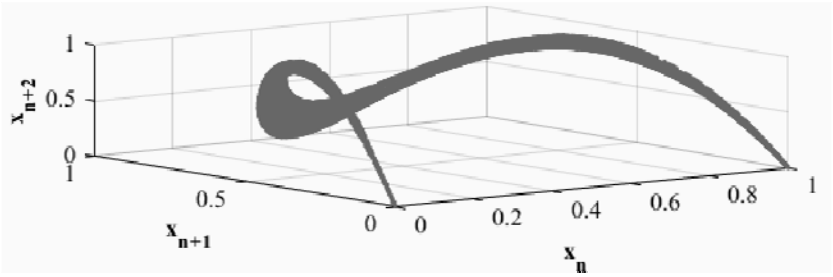
(b)

Fig. 4 Two-dimensional reconstructed phase space (a) traditional logistic map, (b) parameter hopping logistic map

Fig.4 shows a two-dimensional Poincaré plot of the logistic map's state space for $r = 4$, wherein Fig. 4a the quadratic curve for the traditional logistic map is obtained using the difference equation (1), while the quadratic curve in Fig.4b was obtained using (3-5) and an initial value of 0.1. A variation of the output of the logistic map based on parameter hopping is clearly shown in Fig.4b compared to that in Fig.4a. For each input (horizontal axis) of Fig.4b, there exists more than one output which is not the case in the traditional logistic map as shown in Fig.4a.



(a)



(b)

Fig. 5 Three-dimensional reconstructed phase space (a) traditional logistic map, (b) parameter hopping logistic map

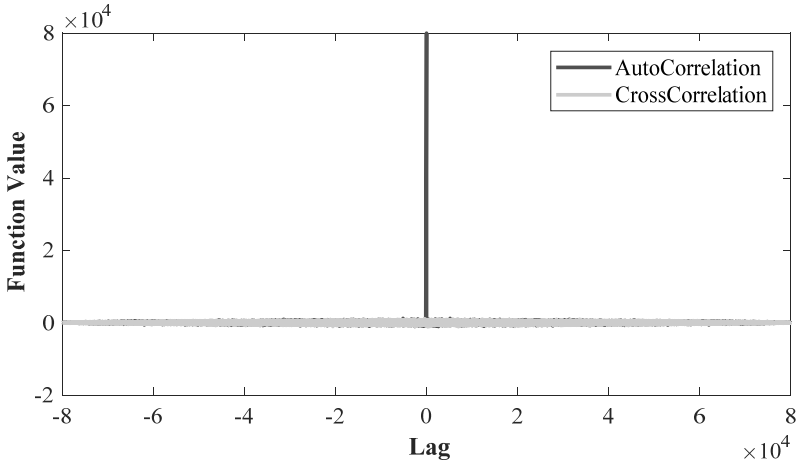


Fig. 6 Auto and cross-correlation resultsfor parameter hopping logistic map

Three-dimensional state space diagrams for both maps are illustrated in Fig.5. An exponential divergence of the sequences of iterates for both maps in Figs 5a, 5b respectively can be figured through the stretching-and-folding plots, producing a complex and unpredictable binary sequence. More state space for the generated output sequence can be clearly identified in Fig.5b than that produced in Fig.5a which in turn leads to a more secured output sequence [15]. Fig.6. shows the auto and cross-correlation functions for our PRBG based on parameter hopping logistic map. The auto-correlation plot indicates a pure delta function while the cross-correlation is zero which gives a clear indication about the ideal randomness of the generated binary sequence.

The bifurcation diagrams for both logistic maps are shown in Fig. 7. The horizontal axis represents the possible values of the parameter r while the vertical axis represents the PRBG output x_n values obtained using all initial conditions by iterating the logistic equations for both studied logistic maps. We can simply conclude from both maps that in Fig.7a the iteration converge to the attractor for values of the parameter r starting from 3.6 to 4, while for the parameter hopping logistic map in Fig.7b the converge to the attractor for values of the parameter r starting from 1 to 4, which gives a better indication about randomness, unpredictability and security for the generated binary sequence produced through this proposed map.

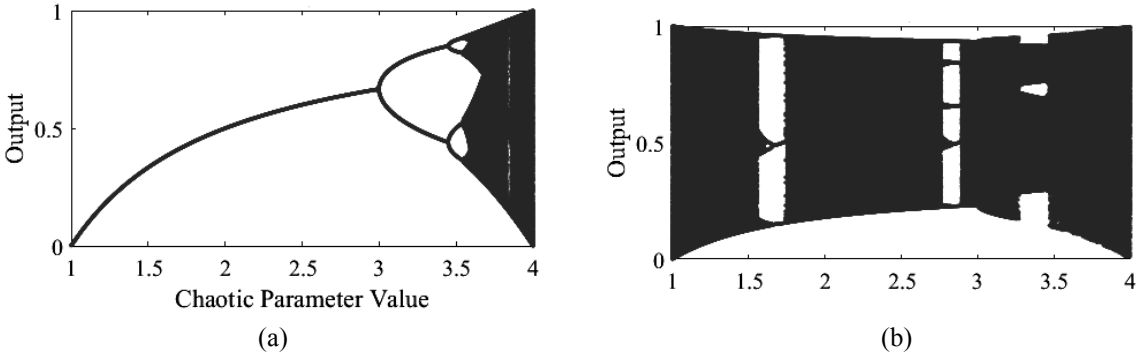


Fig. 7 Bifurcation diagram (a) traditional logistic map, (b) parameter hopping logistic map

VII. CONCLUSION

The pseudorandom bit generators based on a fixed parameter chaotic map that uses a codebook proved to be naturally insecure and showed weakness especially under phase space reconstruction techniques. Consequently, the generated bit sequence based on stationary logistic maps can be analyzed and attacked by means of statistical methods. To avoid such weakness, we proposed a pseudorandom bit generator based on a dynamic algorithm that is capable of generating a random-like chaotic parameter value. The generated pseudo number sequence proved to be unpredictable due to its dependency on the initial value conditions and dynamic behavior. The statistical analysis and tests results obtained showed that the generated sequences are truly random, having perfect correlation properties and are highly capable of withstanding different types of cryptographic attacks. The proposed pseudorandom generator also proofed to be suitable for all types of applications mentioned previously and especially cryptography applications.

REFERENCES

[1] Addabbo, Tommaso, Student Member, Massimo Alioto, and Ada Fort. 2006. "A Feedback Strategy to Improve the Entropy of a Chaos-Based Random Bit Generator." 53(2):326–37.
[2] Alvarez, Gonzalo, F. Montoya, M. Romera, and G. Pastor. 2004. "Keystream Cryptanalysis of a Chaotic Cryptographic Method." Computer Physics Communications 156(2):205--207.
[3] Alvarez, Gonzalo, Fausto Montoya, Miguel Romera, and Gerardo Pastor. 2003. "Cryptanalysis of an Ergodic Chaotic Cipher." Physics Letters A 311(2–3):172--179.
[4] Clark, David. 2000. "Encryption Advances to Meet Internet Challenges." Computer 33:20--24.
[5] Francois, Michael, Thomas Grosges, Dominique Barchiesi, and Robert Erra. 2013. "A New Pseudo-Random Number Generator Based on Two Chaotic Maps." Informatica 24(2):181--197.
[6] Gude, Micheal. 1985. "Concept for a High Performance Random Number Generator Based on Physical Random Phenomena." FREQUENZ 39:187–90.
[7] Hu, HanPing, LingFeng Liu, and NaiDa Ding. 2013. "Pseudorandom Sequence Generator Based on the Chen Chaotic System." Computer Physics Communications 184(3):765–68.
[8] Liu, Lingfeng, Suoxia Miao, Hanping Hu, and Yashuang Deng. 2016. "Pseudorandom Bit Generator Based on Non-Stationary Logistic Maps." IET Information Security 10(2):87--94.
[9] Lsota, A. and M. Mackey. 1994. Chaos, Fractals, and Noise.
[10] Oishi, Shinichi and Hajime Inoue. 1982. "Pseudo-Random Number Generators and Chaos." Transactions of the Institute of Electronics and Communication Engineers of Japan. Section E E65(9):534–41.
[11] Rukhin, Andrew, Juan Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, and Others. 2010. "NIST Special Publication 800-22rev1a: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, April 2010.
[12] Wang, Xing-Yuan and Lei Yang. 2012. "Design of Pseudo-Random Bit Generator Based on Chaotic Maps." International Journal of Modern Physics B 36(32):1250208-1–9.
[13] Xie, B., D. Wang, and X. Jiang. 2007. "On Pseudo-Random Bit Generator Based on Couple Chaotic Systems." Journal of Naval University of Engineering 19(5):51–55.
[14] Yalçın, Müstak, Johan Suykens, and JoosVandewalle. 2004. "True Random Bit Generation From a Double-Scroll Attractor." IEEE Transactions on Circuits and Systems-I:Regular Papers 51(7):1395–1404.
[15] Zheng, Fan, Xiao-jian Tian, Jing-yi Song, and Xue-yan LI. 2008. "Pseudo-Random Sequence Generator Based on the Generalized Henon Map." The Journal of China Universities of Posts and Telecommunications 15(3):64--6

AUTHOR PROFILE

Ahmed I. El Naggary received the B. Sc., M. Sc. from Arab Academy For Science & Technology & Maritime Transport, Alexandria Egypt, and Ph.D. degree from Alexandria University, Alexandria, Egypt, in 1999, 2003, and 2013respectively. He is currently Assistant Professor in Electronics & Communication Department at King Mariott Higher Institute for Engineering & Technology, Alexandria Egypt. His research interests include digital signal processing, data security, communication networks, mobile communication systems, multiuser MIMO systems, massive MIMO and engineering optimization.

Karim H. Moussa received the B. Sc., M. Sc., and Ph.D. degrees from Alexandria University, Alexandria, Egypt, in 2006, 2011, and 2016, respectively. He is currently assistant professor of computer, communications, and electronics in Engineering Faculty, Horus University in Egypt (HUE). Hisresearch interests include digital signal processing, multimedia, data security, communication networks, mobile communication systems, multiuser MIMO systems, massive MIMO and engineering optimization.