International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 1, February 2021, pp. 863~871
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i1.pp863-871

Low power pseudo-random number generator based on lemniscate chaotic map

Mohamed Saber[1], Marwa M. Eid[2]
[1]Department of Communications and Computers, Faculty of Engineering,
Delta University for Science and Technology, Egypt
[2]Department of Communications and Electronics, Delta Higher Institute of Engineering and Technology (DHIET), Egypt

Article Info

Article history:

Received Apr 1, 2020
Revised Jun 17, 2020
Accepted Jun 28, 2020

Keywords:

Chaotic map
FPGA
Lemniscate chaotic map
Random number generator
Read-only memory (ROM)

ABSTRACT

Lemniscate chaotic map (LCM) provides a wide range of control parameters, canceling the need for several rounds of substitutions, and excellent performance in the confusion process. Unfortunately, the hardware model of LCM is complex and consumes high power. This paper presents a proposed low power hardware model of LCM called practical lemniscate chaotic map (P-LCM) depending on trigonometric identities to reduce the complexity of the conventional model. The hardware model designed and implement into the field programmable gate array (FPGA) board, Spartan-6 SLX45FGG484-3. The proposed model achieves a 48.3% reduction in used resources and a 34.6% reduction in power consumption compared to the conventional LCM. We also introduce a new pseudo-random number generator based on a proposed low power P-LCM model and perform the randomization tests for the proposed encryption system.

Corresponding Author:

Mohamed Saber,
Department of Communications and Computers, Faculty of Engineering,
Delta University for Science and Technology,
Belkas, Dakahlia Governorate, Egypt.
Email: Mohamed.saber@deltauniv.edu.eg

1. INTRODUCTION

Pseudo chaotic random number generators (PCRNG) is a vital cryptography application of nonlinear chaotic systems. Many researchers present the software implementation of PCRNGs using MATLAB. The most common way to generate PCRNG is to use a feedback shift register method in different ways such as a linear feedback shift register, carry forward feedback shift register, and nonlinear feedback shift register [1-3]. Another technique used a coupled map lattice with time-varying delay [4].

The researchers in [5] proposed a PRNG based on Lorenz systems with FPGA implementation achieving an operating frequency of 78.149 MHz. In [6], the authors investigate the fixed-point arithmetic representation random effect, and they presented a PRNG based on coupled skew tent maps and provides its hardware implementation. The FPGA implementations of different PRNGs based on chaotic maps presented in [7]. In [8], A pseudo-random generator generated using a chaotic quadratic map with FPGA implementation. In [9], another idea used to make PRNG with a function based on ring oscillator and chaotic logistic map. Another design to PRNG based on a logistic map that changes its chaotic parameters presented and implemented with FPGA in [10]. In [11], a secured PRNG based on a piecewise linear chaotic map presented and implemented using FPGA.

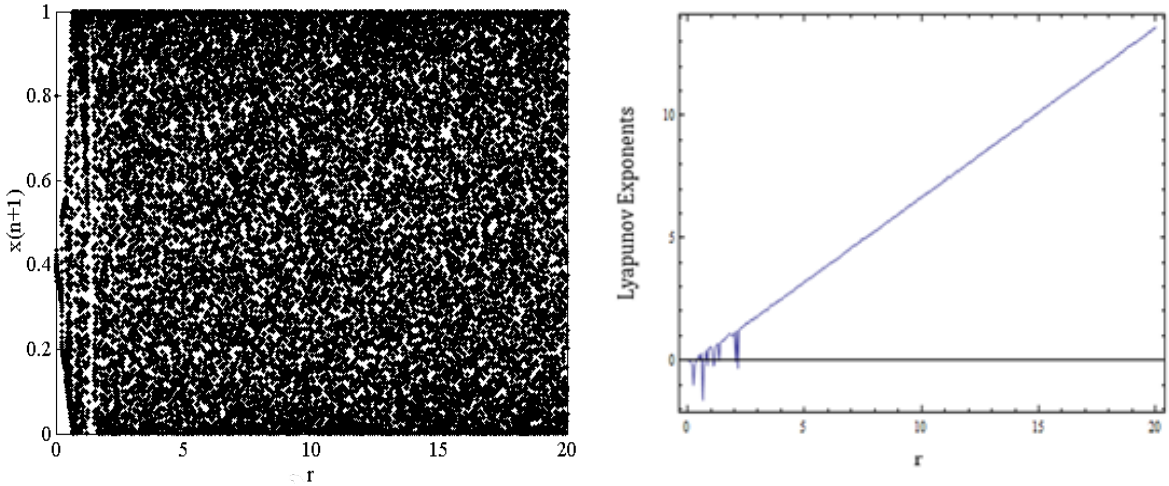
The sensitivity of the chaos-based encryption systems is affected by two factors; the first factor is the use of binary streams extracted from a single orbit of a chaotic map while the second factor is the use of

maps that have chaotic behavior only for small ranges of control parameters' values. Another issue that affects the chaos-based encryption systems is a low speed, which can be caused by the need for several rounds of permutation and/or substitution of the original image pixel [12]. The LCM whose cryptographic properties have been demonstrated to be very good in the confusion process, and eliminate the need for several rounds of substitutions of the pixels values and have a wide range of control parameter's values [13]. The basic equations of LCM are:

$$x(n+1) = \frac{\cos\left(2^r y(n)\right)}{1+\sin^2(2^r y(n))} \quad (1)$$

$$y(n+1) = \frac{2\sqrt{2}\sin\left(2^r x(n)\right)\cos(2^r)x(n)}{1+\sin^2\left(2^r x(n)\right)} \quad (2)$$

Where the initial conditions x_0 , y_0 are given from the intereval $[-1: +1]$ and $r_0 > 3$ for the hyperchaotic regime. In Figure 1, the bifurcation diagram and the Lyapunov exponents of LCM are shown in Figure 1 (a) that and Figure 1(b) respectively.



(a) (b)

Figure 1. Analysis of the lemniscate map's chaotic behavior, (a) Bifurcation diagram, (b) Lyapunov exponents

The equations of LCM have trigonometric functions (sin, cos), and it can be implemented in a hardware model by different methods such as; look-up table (LUT) based read-only memory (ROM), CORDIC algorithm, Taylor's series, and linear segmentation [14-16]. Since the total power consumption of a hardware model depends on the components used in the implementation, so any reduction for these components reduces the overall power consumption. In the LCM hardware model, the components LUT, ROM, consume more power so, the total power consumption reduction achieved by reducing the number of these components in the hardware model. The main idea of this paper is to present a low power implementation of the lemniscate hardware model. Three alternatives hardware models designed, explained, and implemented according to the mathematical equations of LCM. Furthermore, we present a PRNG based on the best low power FPGA architecture of the LCM with MATLAB simulations and FPGA simulation and implementation.

This paper organized as follows: Section 2 describes the mathematical analysis of three alternative models of LCM. In section 3, FPGA Implementations of the three hardware models of LCM are presented. The FPGA hardware implementation results provided in section 4. The hardware implementation of the PRNG based on the lowest power consumption hardware model is presented in section 5. Section 6 presents NIST SP800-22 randomization tests for a proposed PRNG. Section 7 presents a comparison between the proposed model and recent comparable models. Finally, this conclusion presented in section 8.

2. PROPOSED LCM MODELS

2.1. Modified model

The first alternative "Conventional" model achieved by using the basic mathematical equations of lemniscate chaotic map, which are (1-2). The second alternative "Modified" map uses two abbreviations to (1) and (2) using the trigonometric identities, which are:

$$\sin^2(t) + \cos^2(t) = 1 \tag{3}$$

$$2\sin(t)\cos(t) = \sin(2t) \tag{4}$$

Using (3) converts the denominator of (1) as follows:

$$1 + \sin^2\left(2^r y(n)\right) = 2 - \cos^2\left(2^r y(n)\right) \tag{5}$$

Also, using (4) converts the numerator of (2) as follows:

$$2\sqrt{2}\sin\left(2^r x(n)\right)\cos(2^r\, x(n)) = \sqrt{2}\ \sin\left(2 \times 2^r x(n)\right) \tag{6}$$

So, the second alternative "Modified" has the following equations

$$x(n+1) = \frac{\cos\left(2^r y(n)\right)}{2 - cos^2(2^r y(n))} \tag{7}$$

$$y(n+1) = \frac{\sqrt{2}\sin\left(2 \times 2^r x(n)\right)}{1 + \sin^2\left(2^r x(n)\right)} \tag{8}$$

2.2. Practical model

The third alternative "Practical" uses three abbreviations to (1) and (2); using the trigonometric identities in (3), (4), and the following identity:

$$\cos(2t) = \cos^2(t) - \sin^2(t) = 2\cos^2(t) - 1 = 1 - 2\sin^2(t) \tag{9}$$

$$\sin^2(t) = \frac{1}{2} - \frac{1}{2}\cos(2t) \tag{10}$$

In (3) converts (1) to be (5), while (4) converts (2) to (6), as done in "Modified" model. Substitute with (7) in (6) leads to

$$y(n+1) = \frac{\sqrt{2}\sin\left(2\ \times 2^r\ x(n)\right)}{1.5 - 0.5\cos\left(2 \times 2^r x(n)\right)} \tag{11}$$

Since

$$\frac{d}{dx(n)}\left(\sin\left(2 \times 2^r x(n)\right) = 2 \times 2^r \cos\left(2 \times 2^r x(n)\right)\right) \tag{12}$$

Rewriting (8)

$$y(n+1) = \frac{\sqrt{2}\sin\left(2 \times 2^r x(n)\right)}{1 + \sin^2\left(2^r x(n)\right)} \tag{13}$$

In discrete-time, the time differentiation is calculated using

$$\frac{d}{dn}x(n) = x(n) - x(n-1) \tag{14}$$

It means by only using a one-time delay and subtractor; we can obtain a time differentiator. So, the third alternative "practical" hardware model implements the following equations:

$$x(n+1) = \frac{\cos(2^r y(n))}{2 - \cos^2(2^r y(n))} \tag{15}$$

$$y(n+1) = \frac{\sqrt{2}\sin(2 \times 2^r x(n))}{1.5 - 2^r \times \frac{\mathrm{d}}{\mathrm{dx(n)}}(\sin(2 \times 2^r x(n)))} \tag{16}$$

3. FPGA IMPLEMENTATION OF PROPOSED LCM

The hardware models of the lemniscate architectures is designed using Xilinx system generator (XSG) [17-22]. In this paper, we implement the sine and cosine functions using LUT based ROM in the three hardware models. Table 1 indicates the number of LUT used in each alternative.

Table 1. No. of LUT in the three hardware models

Model	No. of LUTs
Conventional	4
Modified	3
Practical	2

The three alternatives of the LCM system are modelled using the XSG program in thirty two fixed-point formats, also the three architectures are implemented into the same FPGA board (Spartan-6 SLX45FGG484-3). The XSG conventional hardware architecture model which depend on (1-2) is shown in Figure 2. The "Modified" XSG model, which implement (7-8) is shown in Figure 3. The "Practical" XSG model which applies the (15-16) is shown in Figure 4.

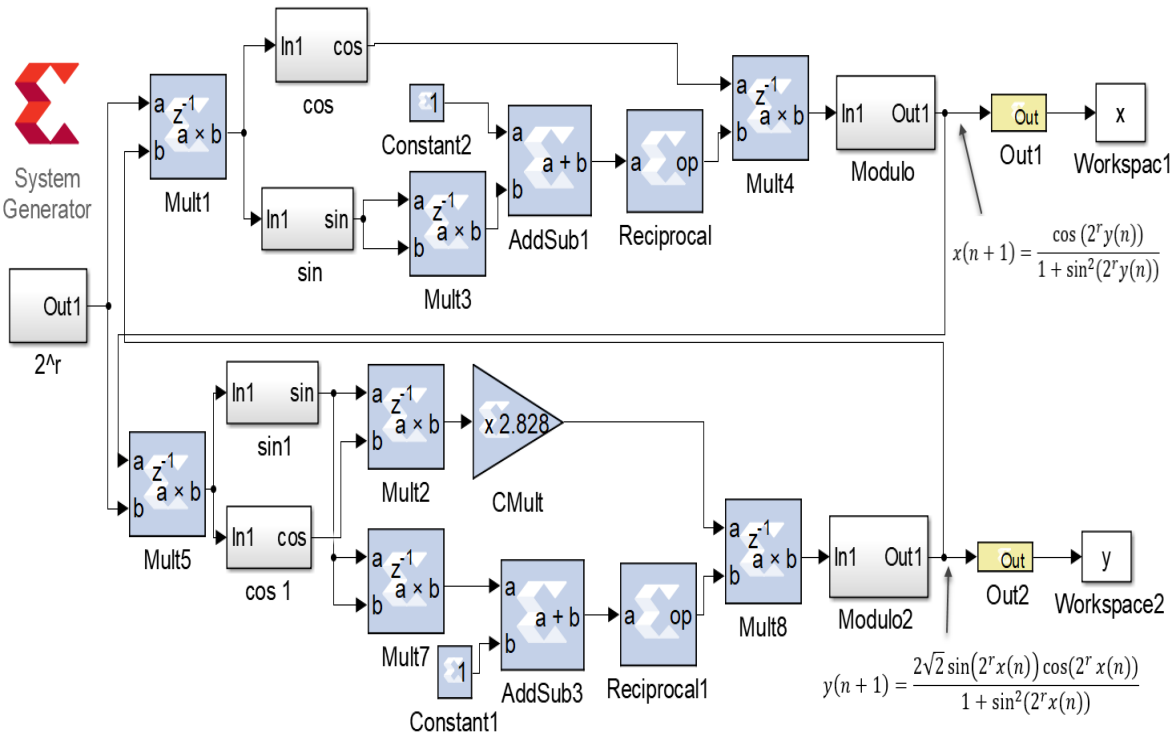


Figure 2. XSG model of "Conventional" LCM

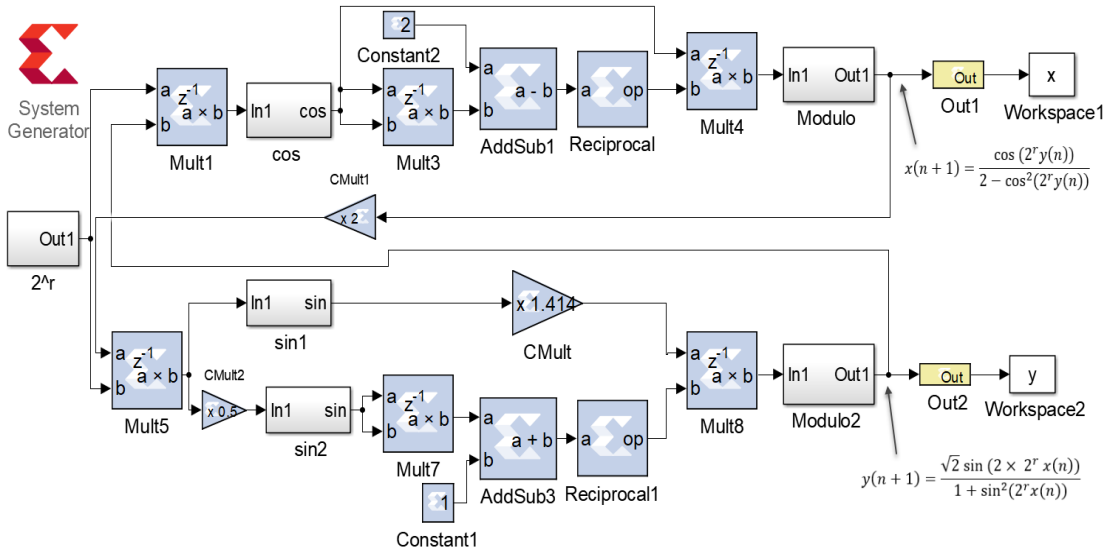


Figure 3. XSG model of "Modified" LCM

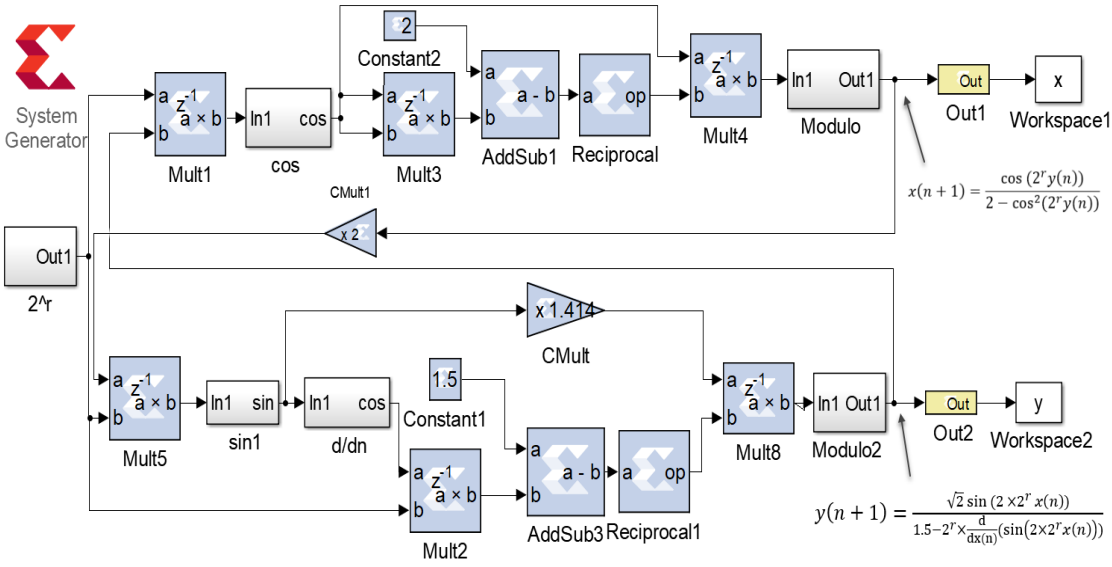


Figure 4. XSG model of "Practical" LCM

4. HARDWARE SIMULATION RESULTS

4.1. Bifurcation diagram

Table 2 shows a comparison between the bifurcation diagram for the three models generated by theoretical simulations using Matlab and bifurcation diagram generated by the hardware model. The difference between the two types of simulation because of the finite word length in the digital hardware models [23].

4.2. Implementation results

The implementation results for the three-hardware LCM models are presented in Table 3. Note that the maximum frequency is the same for the three hardware models because the maximum frequency is determined by the critical path, which is the longest path between the input and output signal. Since the steps of calculations are the same in the three hardware models, so the maximum frequency is the same.

Table 2. Comparison between Bifurcation diagrams generated by Matlab codes, and by hardware models

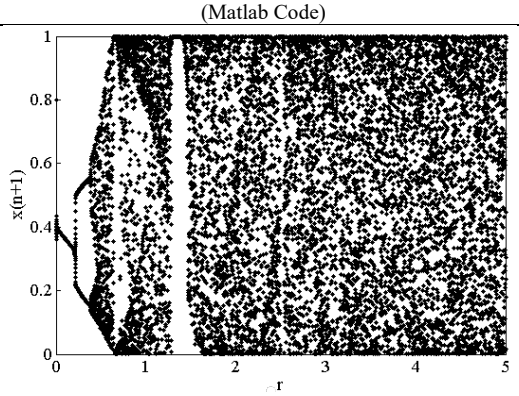
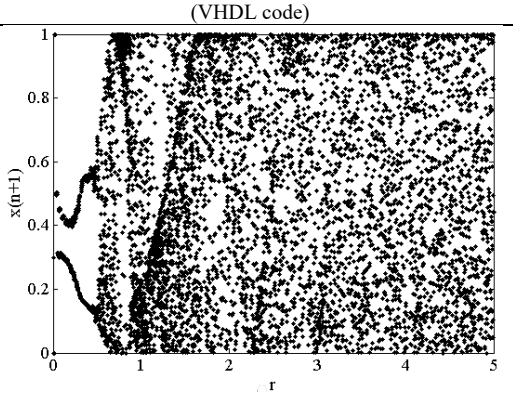
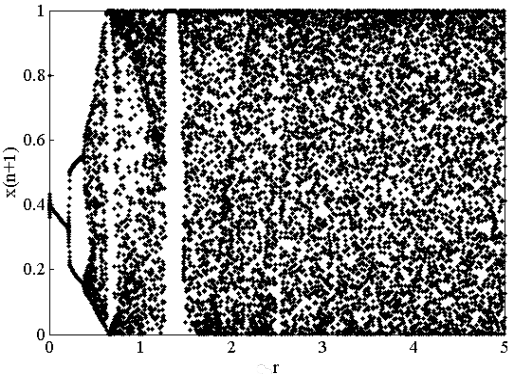
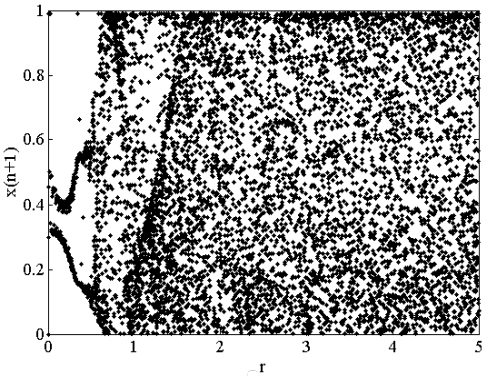
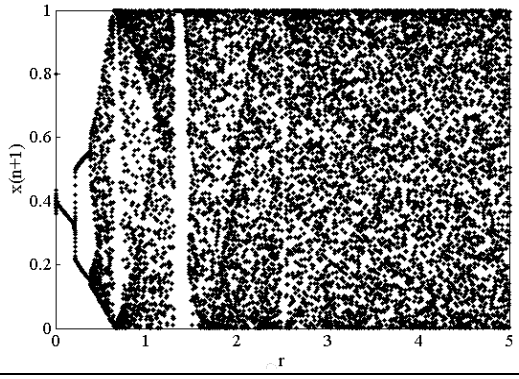
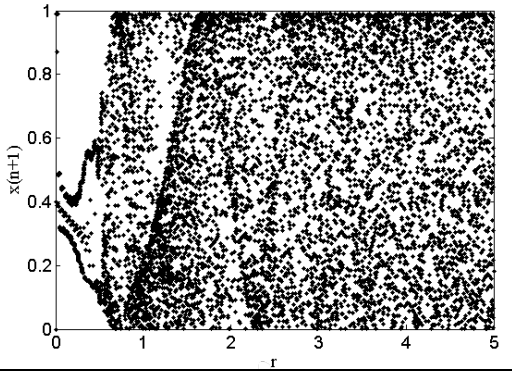
Model	Theoretical Simulation (Matlab Code)	Hardware Model Simulation (VHDL code)
Conventional		
Modified		
Practical		

Table 3. Hardware implementation results of LCM

Model	Slice Registers	LUTs	Frequency (MHz)	Power (mW)	Power reduction ratio Compared to Conventional
Conventional	1247	7614	80.592	367	---
Modified	1024	5806		300	18%
Practical	859	3329		240	34.6%

5. FPGA IMPLEMENTATION OF P-LCM RNG

An XSG hardware model of the random number generator is built by adding two threshold units and a multiplexer to the outputs of the "Practical" model (x,y) as shown in Figure 5. The threshold is a "Relational" block compares the input to a threshold value which is "0.5", if the input is a fraction higher than "0.5" then the output of the "Relational" block is "1", otherwise the output will be "0". Figure 6 shows a simulation for RNG. A random output number is a binary number "0" or "1" according to the "sel" signal which chooses between the inputs "d0" and "d1".

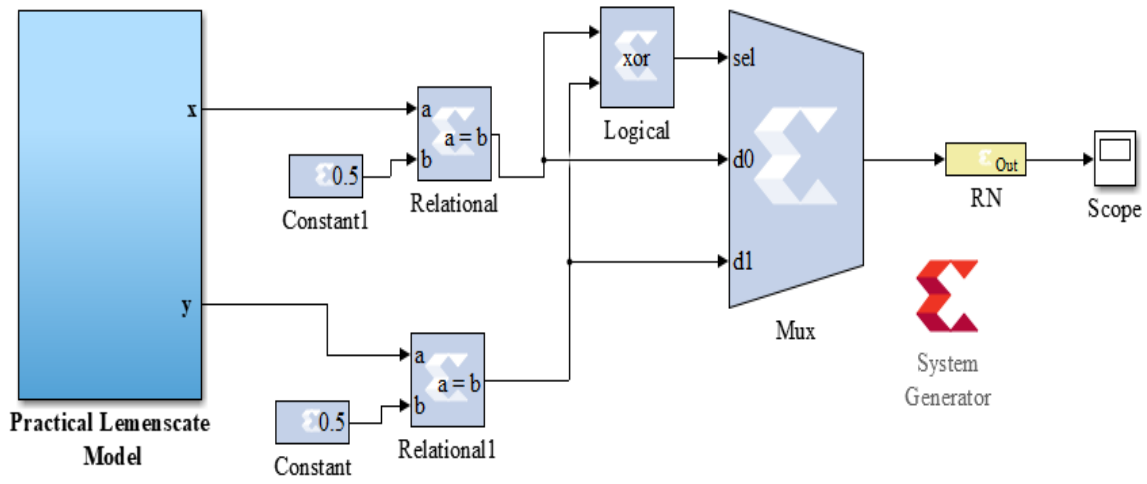


Figure 5. XSG model of random number generator hardware model based on P-LCM

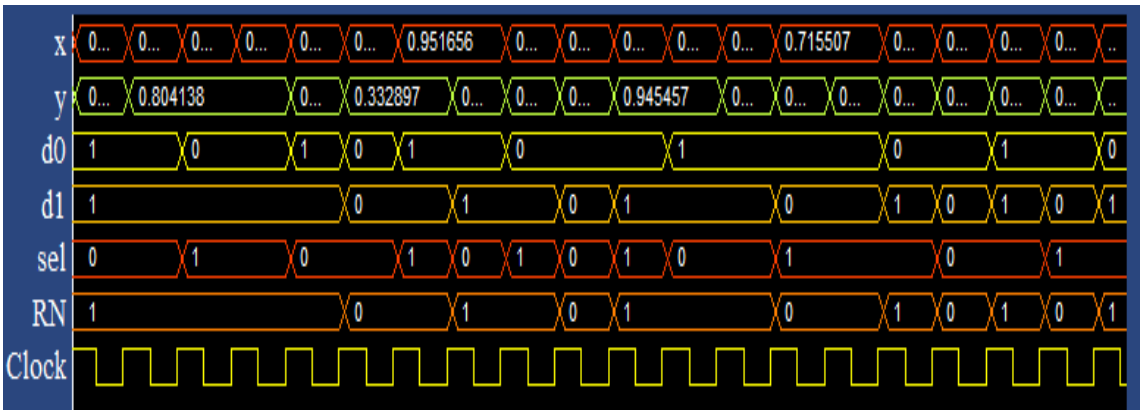


Figure 6. The output random number generator "RNG"

6. NIST SP800-200 RANDOMIZATION TESTS

A good encryption system should be able to assign plane images to randomly encoded images. It is, therefore, vital to test the randomization of the encrypted images obtained by the proposed image encryption algorithm [24]. The results given in Table 4 indicates that the P-LCM PRNG is suitable for cryptographic applications.

Table 4. SP 800-22 random and pseudo-random sequence test results

Statistic Tests	p value	Results
Runs test.	0.2219	Pass
Longest run of ones	0.6638	Pass
Binary matrix rank test	0.7214	Pass
FFT (spectral)	0.9293	Pass
Non-overlapping template	0.5495	Pass
Overlapping templates	0.6257	Pass
Universal statistical	0.6127	Pass
Linear complexity	0.8895	Pass
Serial test (1)	0.9428	Pass
Serial test (2)	0.7215	Pass
Approximate entropy	0.7621	Pass
Cumulative sums (Forward)	0.8164	Pass
Cumulative sums (Revere)	0.6845	Pass
Random excursions	0.6732	Pass
Random excursions variant	0.2765	Pass

7. COMPARISONS

In this section, the proposed encryption system compared to recent chaotic systems. Table 5 presents the security test results in the case of using the Lena image. As indicated in Table 5, the results of our encryption system are close to the recent systems. Another comparison between the three hardware models of LCM and other similar works based on chaotic maps are presented in Table 6.

Table 5 Security tests comparison

References	Entropy	Unified averaged changed intensity	Correlation	Number of changing pixel rate
Z. Hau [25]	7.9956	33.418	0.0209	99.630
Z. Tang [26]	7.990	33.390	0.0857	99.600
Z. Deng [27]	7.9931	33.365	0.0032	99.5995
Our System	7.9980	33.448	0.0014	99.661

Table 6. Hardware implementation comparisons

Reference		FPGA Resources			Maximum operating frequency (MHz)	Power (Milliwatts)
		Registers	Look Up Tables	Multipliers		
M. Azzaz [28]		1695	3251	78	38.86	321
S.Sadoudi [29]		1138	1969	40	22.850	-
E. Gerardo [30]		476	928	-	31.33	-
B. Karakaya[21]		165	311	22	59.492	-
Our work	Conventional	1247	7614	16		367
	Modified	1024	5806	14	80.592	300
	Practical	859	3329	12		240

8. CONCLUSION

A solution to the high-power consumption problem of the LCM hardware model is explained, analyzed, and implemented. Using trigonometric identities two alternatives hardware models; “Modified”, and “Practical” have been presented instead of the “Conventional” model. The implementation results indicate 18% reduction in power consumption in case of using the “Modified” model instead of “conventional” model. Also, implementation results indicate a 33% reduction in power consumption when using the “Practical” model instead of “conventional” model. We proposed a new Pseudo number generator based on a proposed “Practical” model. Also, statistical analysis has been used to determine the randomization tests. Finally, two comparisons are presented; the first between the security of the proposed encryption system and similar recent chaotic cryptosystems, while the second between the hardware implementation models of the proposed LCM systems and similar recent works.

REFERENCES

[1] L. Koncarev and S. Lian, "Chaos- Based Cryptography, " *Springer,* 2011.
[2] F. Arnault and T. P. Berger, "Design and properties of a new pseudorandom generator based on a filtered FCSR automaton," *IEEE Transaction on Computers,* vol. 54, pp. 1374–1383, 2005.
[3] S. Alomar, "Method of designing generators of pseudorandom sequences for information protection based on shift register with non-linear feedback function," *Journal of Information security,* vol. 5, pp. 218-227, 2014.
[4] X. Lv, Xiaofeng Liao, and Bo Yang., "A novel pseudo-random number generator from coupled map lattice with time-varying delay," *Nonlinear Dynamics,* vol. 94, pp 324-341, 2018.
[5] Rezk, et al., "Reconfigurable chaotic pseudo random number generator based on FPGA," *AEU-International Journal of Electronics and Communications,* vol. 98, pp. 174-180, 2019.
[6] Elmanfaloty and Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos Solitons & Fractals,* vol. 144, pp.118-134, 2019.
[7] L. Gerardo, et al., "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dynamics,* vol. 90, pp. 1661-1670, 2017.
[8] Hidayat an Mustafa, "FPGA Implementations of Chaotic Quadratic Map for Cryptographic Applications," *Turkish Journal of Science & Technology,* vol. 12, no. 2, pp. 113-119, 2017.
[9] Tuncer, "The implementation of chaos-based PUF designs in Field programmable gate array," *Nonlinear Dynamics,* vol. 86, pp. 975-986, 2016.
[10] Garcia, et al., "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Transactions on Instrumentation and Measurement,* vol. 68, pp. 291-293, 2019.

[11] A. Thane and R. Chaudhari, "Hardware Design and Implementation of Pseudorandom Number Generator Using Piecewise Linear Chaotic Map," *International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 456-459, 2018.
[12] R. Boriga, et al., "A New Fast Image Encryption Scheme Based on Chaotic Maps," *International Journal of Computer science,* vol. 41, pp. 249-258, 2014.
[13] A. Dăscălescu and R. Boriga, "A novel pseudo-random bit generator based on a new couple of chaotic systems," *Annals of Ovidius University - Economics Sciences Series*, vol. 11, pp. 553-558, 2011.
[14] P. Kumar, "FPGA Implementation of the Trigonometric Functions Using the CORDIC Algorithm," *5th International Conference on Advanced Computing & Communication Systems (ICACCS),* pp. 894-900, 2019.
[15] S. Nandi, et al., "Fixed point implementation of trigonometric function using Taylor's series and error characterization," *International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 442-446, 2016.
[16] M. Saber, et al., "Quadrature direct digital frequency synthesizer using FPGA," *IEEE International Conference on Computer Engineering and Systems,* pp. 14-18, 2006.
[17] Xilinx, Vivado " Design Suite User Guide: Model-Based DSP Design using System Generator," *UG897, v2016.1 ed., Xilinx,* 2018.
[18] R. Palanisamy, et al., "Switching pulse generator generation for DC-DC boost converter using using xilinx-ISE with FPGA processor," *International Journal od Electrical and Computer Engineering (IJECE),* vol. 10, no. 2, pp. 1722-1727, 2020.
[19] A. Stacul, "Filtering and acquisition of serial data frames using xilinx system generator," *International Journal of Reconfigurable and Embedded systems (IJRES),* vol. 9, pp. 1-11, 2020.
[20] L. Zhang, "Fixed point FPGA Model based design and optimization for Henon Map chaotic generator," *IEEE 8th Latin American Symposium on Circuit & systems,* pp. 1-4, 2017.
[21] Karakaya, et al., "Realizations of Delayed Cellular Neural Network Model on FPGA," *2018 Electric Electronics, Computer Science, Biomedical Engineering's' Meeting (EBBT),* 2018.
[22] Mohamed Saber and Esam A. Hagras, "Parallel multi-layer selector S-BOX based on lorenz chotic system with FPGA implementation," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 19, no. 2, pp. 784-792, 2020.
[23] D. Menard, et al., "Analysis of Finite Word-Length Effects in Fixed-Point Systems," *Springer Cham,* 2019.
[24] A Rukhin, et al., "A Statistical Test Suite for random and Pseduo-random Number Generator for Cryptographic Applications," *Booz-allen and hamilton inc mclean va,* 2010.
[25] Z. Hua, et al.,"Cosine-transform-based chaotic system for image encryption," *Information Sciences,* vol. 480, pp. 403-419, 2019.
[26] Z. Tang, et al., "Image Encryption with Double Spiral Scans and Chaotic Maps," *Security and Communication Networks,* vol. 2019, pp. 1-15, 2019.
[27] Z. Deng and S. Zhong,"A digital image encryption algorithm based on chaotic mapping," *Journal of Algorithms & Computational Technology,* vol. 13, pp 1–11, 2019.
[28] M.S. Azzaz, et al., "A new auto-switched chaotic system and its FPGA implementation," *Communications in Nonlinear Science & Numerical Simulation,* vol. 18, pp. 1792-1804, 2013.
[29] S. Sadoudi, et al., "An FPGA Real-time Implementation of the Chen‟s Chaotic System for Securing Chaotic Communications," *International Journal of Nonlinear Science,* vol. 7, pp. 1749-3889, 2009.
[30] L. Gerardo, et al., "Hardware Implementation of Pseudo-random number generator based on chaotic maps," *Nonlinear Dynamics,* vol. 90, pp. 1661-670, 2017.

BIOGRAPHIES OF AUTHORS

Mohamed Saber, he received Ph.D. Degree In Informatics and Communications, Kyushu University, Japan, 2012. He works as an assistant professor at Delta university for science and Technology, Mansoura, Egypt. His research interests are: Digital signal processing, Design and implement digital communication systems on FPGA and DSP circuits, Synchronization in digital receivers.

Marwa M. Eid received the Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2015. She worked as an assistant professor at Delta Higher Institute for Engineering & Technology since 2011 till now. Her current research interests are in image processing, encryption, wireless communication systems, and Field Programmable Gate Array (FPGA) applications.