Applied Mathematics, 2015, 6, 773-782
Published Online May 2015 in SciRes. http://www.scirp.org/journal/am
http://dx.doi.org/10.4236/am.2015.65073

Scientific Research Publishing

Modified Logistic Maps for Cryptographic Application

Shahram Etemadi Borujeni, Mohammad Saeed Ehsani

Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran
Email: etemadi@eng.ui.ac.ir, ehsani@eng.ui.ac.ir

Received 13 October 2014; accepted 7 May 2015; published 12 May 2015

Abstract

In this paper, definition and properties of logistic map along with orbit and bifurcation diagrams, Lyapunov exponent, and its histogram are considered. In order to expand chaotic region of Logistic map and make it suitable for cryptography, two modified versions of Logistic map are proposed. In the First Modification of Logistic map (FML), vertical symmetry and transformation to the right are used. In the Second Modification of Logistic (SML) map, vertical and horizontal symmetry and transformation to the right are used. Sensitivity of FML to initial condition is less and sensitivity of SML map to initial condition is more than the others. The total chaotic range of SML is more than others. Histograms of Logistic map and SML map are identical. Chaotic range of SML map is fivefold of chaotic range of Logistic map. This property gave more key space for cryptographic purposes.

Keywords

Chaotic Map, Modified Logistic Map, FML Map, SML Map

1. Introduction

In order to explain simple chaotic dynamical systems, one-dimensional map is used. Tent, Bernoulli and Logistic maps are common examples of them. The return map of Tent and Bernoulli are linear, while Logistic map is nonlinear [1]-[3].

One dimensional map is simple as far as hardware implementation is concerned. In the other hand, security of nonlinear maps is usually more than linear functions. Logistic map is generally used in most of cryptosystems and pseudo random generators. It is used in chaos-based secure communication system and for generations of binary numbers. Li, Mou, and Cai proposed statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding [4]. Addabbo proposed performance analysis and optimized design of piecewise linear chaotic maps such as digital saw-tooth and tent maps as a source of pseudo-

How to cite this paper: Etemadi Borujeni, S. and Ehsani, M.S. (2015) Modified Logistic Maps for Cryptographic Application. *Applied Mathematics*, **6**, 773-782. http://dx.doi.org/10.4236/am.2015.65073

random bits generators [5] [6]. Pareek used chaotic maps for random bit generator [7]. Shastry, Nagaraj, and Vaidya proposed a generalization of Logistic map, and its applications in generating pseudo-random numbers [8]. Basios, Forti, and Gilbert proposed statistical properties of time-reversible triangular maps of the square [9]. The key element of the cryptosystems is key space. The key space is corresponding to chaotic range. Since chaotic range of logistic map is small, its key space is also small.

In this paper, with the aim of expanding chaotic range of Logistic map, two modified versions of Logistic map are proposed. Definition and properties of Logistic map are reviewed in Section 2. The first and second modified versions of Logistic map are proposed in Section 3. Return maps, orbit diagrams, bifurcation diagrams and Lyapunov exponents were also concerned. Comparison of the modified map with Logistic with respect to their sensitivity to initial conditions, their chaotic range and histograms is considered in Section 4. Finally, conclusion and references are integrated.

2. Logistic Map

Logistic map is one-dimensional map which uses to model simple nonlinear discrete systems. Logistic map explain by a recursive function as follows:

$$x_{n+1} = L\left(r, x_n\right) = r \cdot x_n \cdot \left(1 - x_n\right) \tag{1}$$

where r is its parameter and $x_n \in [0,1]$. Consider Logistic map $L : [0,1] \to [0,1]$, given by Equation (1), the parameter r lies in interval $[0,4]$. The return map of Logistic function is given in **Figure 1** for $r = 4$.

Sensitivity of Logistic map to initial condition could be observed by plotting orbit diagrams with respect to two initial conditions with small difference. The corresponding orbit diagrams with respect to two initial conditions 0.350 and 0.351 for fixed values of $r = 4$ is drawn in **Figure 2**. There is suitable sensitivity to initial condition.

In order to view chaotic properties of Logistic map, bifurcation diagram and Lyapunov exponent of it should be calculated and plotted. Bifurcation diagram of Logistic mapwith respect to "r" are calculated and plotted in **Figure 3**.

Lyapunov exponent of Logistic mapwith respect to "r" are also calculated and plotted in **Figure 4**. Regarding **Figure 3** and **Figure 4**, Logistic map is chaotic when parameter "r" lies in interval [3.6, 4].

First, confirm that you have the correct template for your paper size.

3. Modified Logistic Maps

A discrete dynamic process is said to be two-segmental if there exists a partitioning point. The general equation

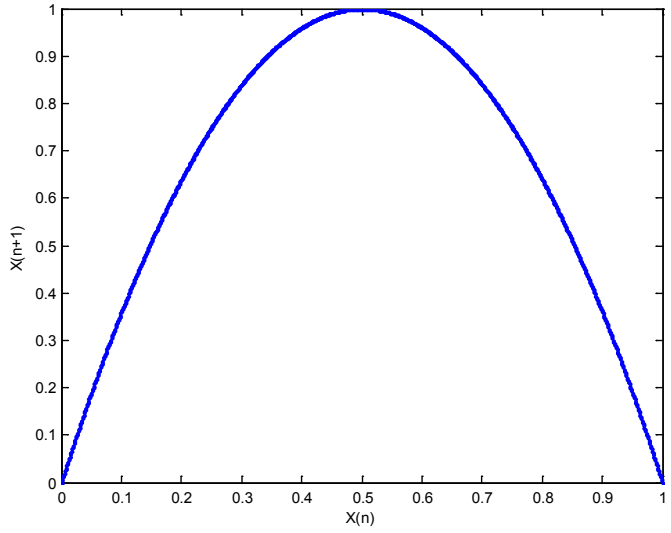

Figure 1. Return map of logistic map with respect to r = 4.

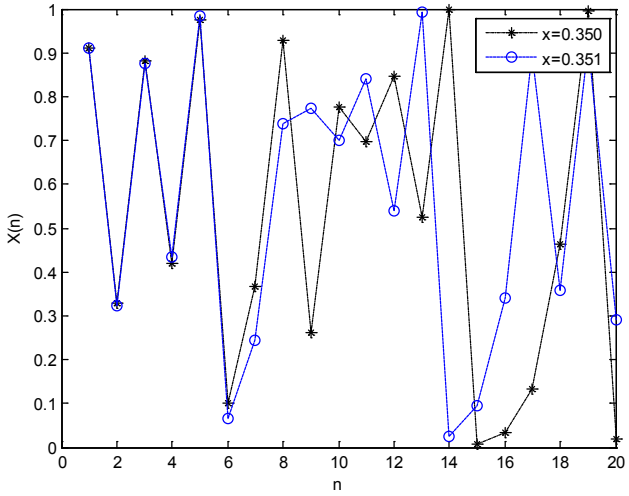

Figure 2. Orbit diagrams of logistic map with respect to two initial conditions 0.350 and 0.351 ($r = 4$).

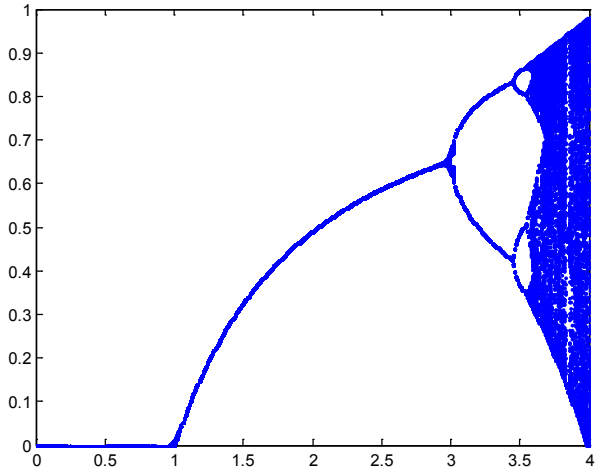

Figure 3. Bifurcation diagram of logistic map with respect to r.

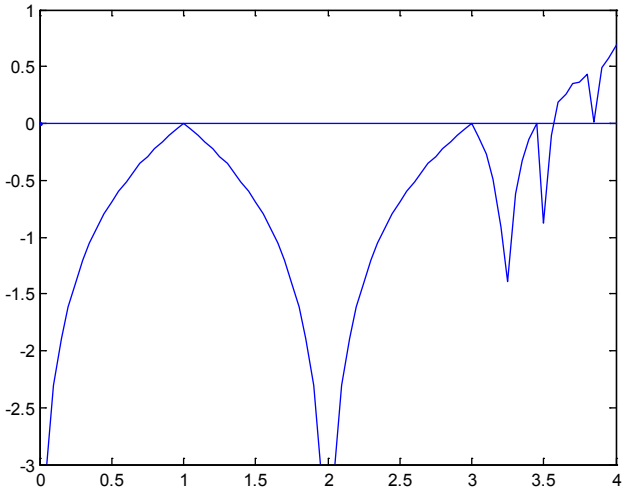

Figure 4. Lyapunov Exponent of Logistic map with respect to r.

of the process could be defined as depicted in Equation (2), such that $g(x)$ and $h(x)$ are the left and right hand side functions, respectively [10] [11].

$$x_{n+1} = f(x_n) = \begin{cases} g(x_n), & x_n < a; \\ h(x_n), & x_n \geq a. \end{cases} \tag{2}$$

where $x_n \in [0,1]$ and $a \in (0,1)$.

The necessary condition for a two segmental function $f = \{g, h\}$ to be a Lebesgue process is that the absolute value of slops must be greater than unity all over the domain [12]. That is, the absolute of derivatives of two branches over the range must be greater than one, Equation (3).

$$|f'(x)| > 1 \quad \text{for}: x \in [0,1] \tag{3}$$

As far as Logistic map is concerned, its equation could be separated as follows with respect to $a = 0.5$:

$$x_{n+1} = L(r, x_n) = \begin{cases} g(x_n) = r \cdot x_n \cdot (1 - x_n), & x_n < a; \\ h(x_n) = r \cdot x_n \cdot (1 - x_n), & x_n \geq a. \end{cases} \tag{4}$$

Considering Equation (4), the derivatives of $g(x)$ is exceeding unity, but this is not true for $h(x)$. To solve this problem, we use symmetry and transform properties to modify $h(x)$. Actually, we modified second part of Logistic map in order to improve chaotic range of Logistic map in two manners.

3.1. First Modified Logistic (FML) Map

We modified Logistic map, by obtaining vertical symmetry of $g(x)$ around $y = r/8$, then transform the result to right for $x = 0.5$, to generate a new $h(x)$. The recursive equation of First Modified Logistic (FML) map is defined in Equation (5), where *n* is a time index, x_0 is the initial value, and *r* is the control parameter.

$$x_{n+1} = \mathrm{FML}(r, x_n) = \begin{cases} g(x_n) = r \cdot x_n \cdot (1 - x_n), & x_n < 0.5; \\ h(x_n) = r \cdot (x_n - 0.5) \cdot (x_n - 1.5) + r/4. & x_n \geq 0.5. \end{cases} \tag{5}$$

where $x_n \in [0,1]$, $r \in (0,4]$. The return map of the result is drawn in **Figure 5** for $r = 4$.

Orbit diagrams of FML map with respect to two initial conditions 0.350 and 0.351 for fixed values of $r = 4$ are drawn in **Figure 6**. Sensitivity of FML map to initial condition is observed in the graph. There is not suitable sensitivity to initial condition.

Bifurcation diagram of FML map with respect to "*r*" are calculated and plotted in **Figure 7**. Lyapunov exponent of FML map with respect to "*r*" are calculated and plotted in **Figure 9**. According to **Figure 7** and **Figure 8**, FML map is chaotic when parameter "*r*" lies in intervals [2.6, 2.9] or [3.2, 4].

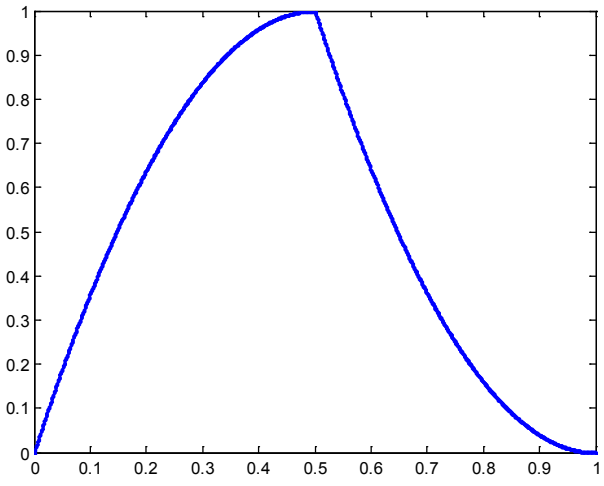

Figure 5. Return map of FML map with respect to *r* = 4.

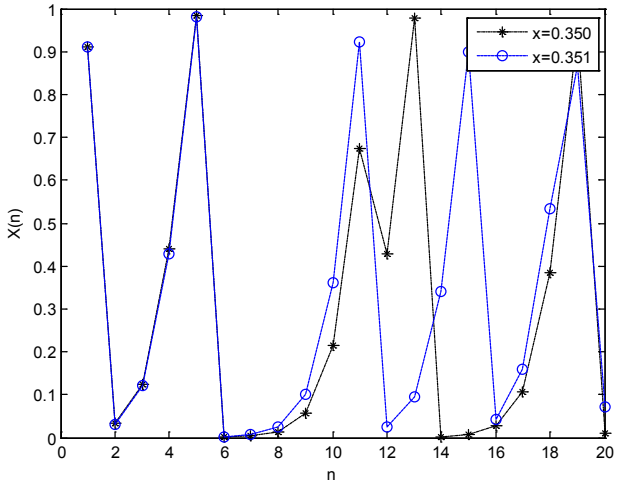

Figure 6. Orbit diagrams of FML map with respect to initial conditions 0.350 and 0.351 ($r = 4$).

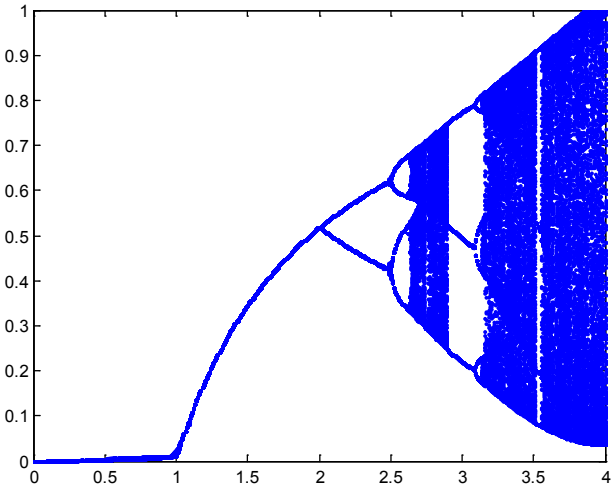

Figure 7. Bifurcation diagram of FML map with respect to r.

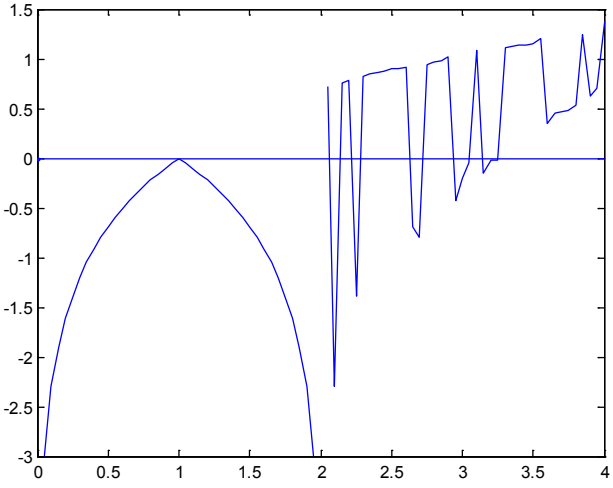

Figure 8. Lyapunov exponent of FML map with respect to r.

3.2. Second Modified Logistic (SML) Map

We make another modification to $h(x)$ by symmetries and transformation. Here, we find vertical symmetry of $g(x)$ with axis of symmetry $y = r/8$ and horizontal symmetry of the result with axis of symmetry $x = 0.25$. Then transformation of the result to right with $x = 0.25$ is performed. Therefore, recursive equation of Second Modified Logistic (SML) map is forming by modifying $h(x)$, and is defined in Equation (6):

$$x_{n+1} = \mathrm{SML}(r, x_n) = \begin{cases} g(x) = r \cdot x_n \cdot (1 - x_n), & x_n < 0.5; \\ h(x) = r \cdot x_n \cdot (x_n - 1) + r/4, & x_n \geq 0.5. \end{cases} \quad (6)$$

where n is a time index, x_0 is the initial value, $x_n \in [0,1]$ and the control parameters $r \in [0,1]$.

In order to explain the performance of Equation (6), the return map of the result is drawn in **Figure 9**.

The orbit diagrams of SML map with respect to two initial conditions 0.350 and 0.351 for fixed value of $r = 4$ are drawn in **Figure 10**. Sensitivity of SML map to initial condition is observed in the figure. There is superior sensitivity to initial condition.

Bifurcation diagram of SML map with respect to 'r' are calculated and plotted in **Figure 11**. Lyapunov exponent of SML map with respect to parameter 'r' are calculated and plotted in **Figure 12**. According to **Figure 11** and **Figure 12**, SML map is chaotic when parameter 'r' lies in intervals [2, 4].

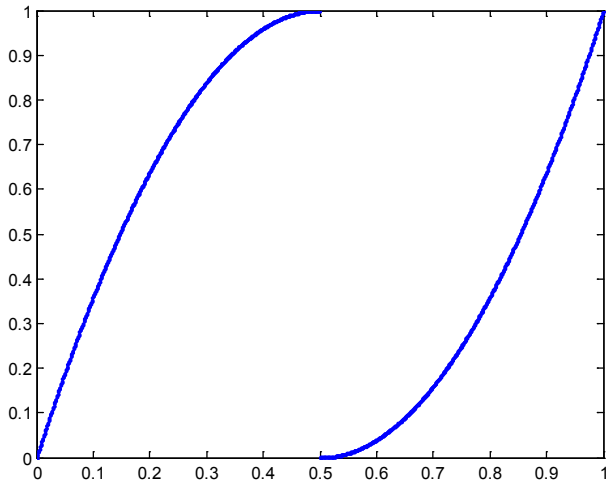

Figure 9. Return map of SML with respect to r = 4.

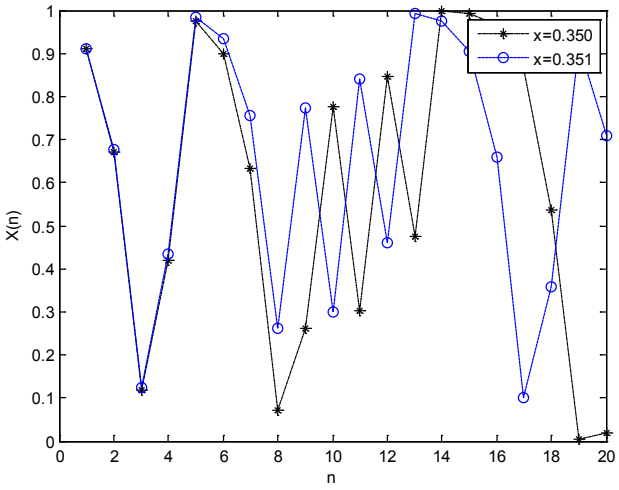

Figure 10. Orbit Diagrams of SML map with respect to initial conditions 0.350 and 0.351 (r = 4).

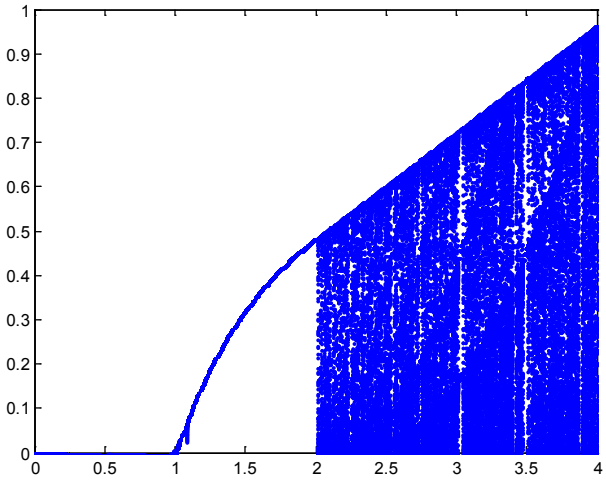

Figure 11. Bifurcation diagram of SML map with respect to *r*.

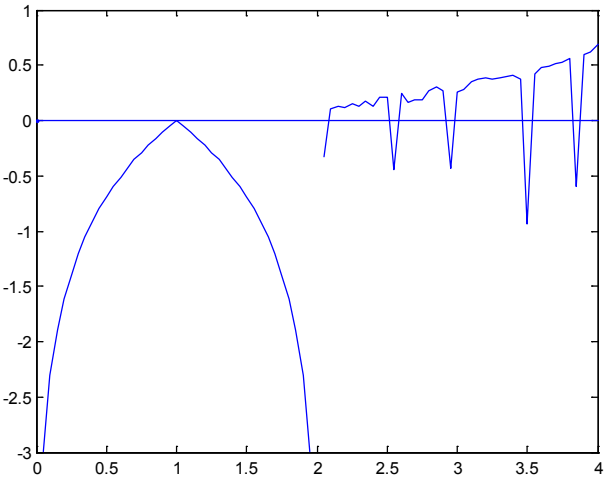

Figure 12. Lyapunov exponent of SML map with respect to *r*.

4. Comparison

With the purpose of expanding chaotic range, two modified version of Logistic map are proposed. In order to compare the performance of the proposed maps with respect to applications, orbit diagrams, bifurcation diagram, Lyapunov exponent and histogram of outputs are considered. Orbit diagram shows the sensitivity of the map to initial conditions. Bifurcation diagram and Lyapunov exponent is used to evaluate chaotic behavior of the maps. Histogram of outputs which could be plotted by observing outputs of large number of iterations, simulate probability density function of the maps.

4.1. Sensitivity to Initial Condition (Orbit Diagram)

In order to compare the sensitivity of the proposed maps, FML and SML, with Logistic map to initial condition, their orbit diagrams with respect to two initial conditions with small difference are considered. They are shown in **Figure 2**, **Figure 6** and **Figure 10**, respectively. As it explained earlier, sensitivity of FML to initial condition is less and sensitivity of SML map to initial condition is more than the others.

4.2. Chaotic Range (Bifurcation Diagram, Lyapunov Exponent)

Bifurcation diagram and Lyapunov exponent of Logistic mapwith respect to "*r*" are plotted in plotted **Figure 3** and **Figure 4**, respectively. Meanwhile, bifurcation diagram and Lyapunov exponent of FML map are also plot-

ted in **Figure 7** and **Figure 8**. Bifurcation diagram and Lyapunov exponent of SML map are also plotted in **Figure 11** and **Figure 12**. Regarding the related figures, Logistic map is chaotic for $r \in [3.6, 4]$, FML map is chaotic for intervals [2.6, 2.9] and [3.2, 4]. In addition, SML map is chaotic for range of $r \in [2, 4]$. Therefore, the total chaotic range of SML is more than the others. The comparison of these values is depicted in **Table 1**. Chaotic range of SML map is fivefold of chaotic range of Logistic map.

4.3. Statistical Characteristics (Histogram)

Simulation of probability density function could be performed to show the statistical characteristics of the map. This simulation is run for 10,000 iterations on the map and draws its histogram. **Figure 13** shows the histogram result of Logistic map for fixed parameter value of $r = 4$.

The probability density function of the SML map is also simulated with 10,000 iterations on SML map. **Figure 14** shows the histogram of SML map for fixed value of $r = 4$.

It is appearing that histograms of Logistic map and SML map are identical, while FML map could not perform acceptable result.

5. Conclusions

In order to evaluate the performance of Logistic map, after considering definition and properties of it, orbit diagrams, Lyapunov exponent and histogram of Logistic map were considered. Orbit diagram showed that the sensitivity of Logistic map to initial condition was medium. Bifurcation diagram and Lyapunov exponent were used to evaluate chaotic properties of the map and recognize the range of parameters. The total chaotic range of Logistic map was small.

With the purpose of expanding chaotic range, two modified versions of Logistic map are proposed. They are one-dimensional and two-segmental nonlinear maps. We called them First and Second Modified Logistic (FML & SML). We found vertical symmetry of first segment, transformed the result to right for the second segment, and called it FML map. Definition and properties of FML map were also considered. Sensitivity of FML map to

Table 1. Comparison of chaotic ranges.

Map	Chaotic range (out of 4)	Chaotic range ratio (%)
Logistic	0.4	10%
FML	1.2	36%
SML	2	50%

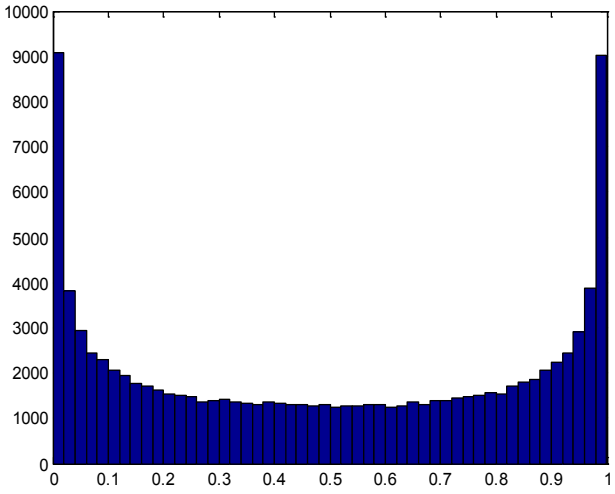

Figure 13. Histogram of logistic map iterations for $r = 4$.

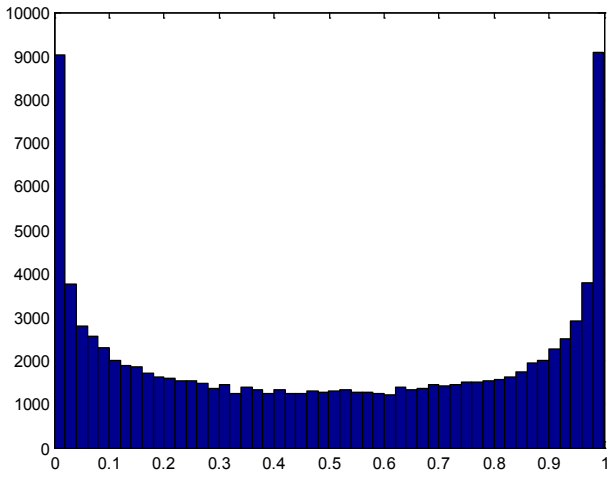

Figure 14. Histogram of SML map iterations for $r = 4$.

initial condition is not suitable. However, FML map is chaotic when parameter "r" lies in intervals [2.6, 2.9] or [3.2, 4] according to the graphs of bifurcation diagram and Lyapunov exponent. To define a second version-modified Logistic map, we found vertical and horizontal symmetry of its first segment and transformed the result to right. Recursive equation of Second Modified Logistic (SML) map is forming. Sensitivity of SML map to initial condition is observed in the figure. There is superior sensitivity to initial condition. According to **Figure 11** and **Figure 12**, SML map is chaotic when parameter "r" lies in intervals [2, 4].

It was concluded that sensitivity of FML to initial condition was less and sensitivity of SML map to initial condition was more than the others. Histograms of Logistic map and SML map are identical, while FML map cannot perform acceptable results. The total chaotic range of SML is more than the others. Chaotic range of SML map is fivefold of chaotic range of Logistic map. This property expands key space for cryptographic purposes.

References

[1] Alligood, K., Sauer, T. and Yorke, J. (1996) Chaos: An Introduction to Dynamical Systems. Springer-Verlag, New York.

[2] Strogatz, S. (1994) Nonlinear Dynamics and Chaos. Perseus Books, Cambridge.

[3] Schuster, H.G. and Just, W. (2005) Deterministic Chaos: An Introduction. 4th Edition, WILEY-VCH Verlag GmbH, Weinheim. http://dx.doi.org/10.1002/3527604804

[4] Li, S., Li, Q., Li, W., Mou, X. and Cai, Y. (2001) Statistical Properties of Digital Piecewise Linear Chaotic Maps and Their Roles in Cryptography and Pseudo-Random Coding. *Cryptography and Coding*, **2260**, 205-221. http://dx.doi.org/10.1007/3-540-45325-3_19

[5] Addabbo, T., Alioto, M., Bernardi, S., Fort, A., Rocchi, S. and Vignoli, V. (2004) The Digital Tent Map: Performance Analysis and Optimized Design as a Source of Pseudo-Random Bits. *Proceedings of the* 21*st IEEE Instrumentation and Measurement Technology Conference*, *IMTC* 04, **2**, 1301-1304.

[6] Addabbo, T., Alioto, M., Bernardi, S., Fort, A., Rocchi, S. and Vignoli, V. (2004) Hardware-Efficient PRBGs Based on 1-D Piecewise Linear Chaotic Maps. *Proceedings of the* 11*th IEEE International Conference on Electronics*, *Circuits and Systems*, *ICECS* 2004, 13-15 December 2004, 242-245.

[7] Pareek, N., Patidar, V. and Sud, K. (2010) A Random Bit Generator Using Chaotic Maps. *International Journal of Network Security*, **10**, 32-38.

[8] Shastry, M., Nagaraj, N. and Vaidya, P. (2006) The B-Exponential Map: A Generalization of the Logistic Map, and Its Applications in Generating Pseudo-Random Numbers. eprint arXiv.org:cs/0607069.

[9] Basios, V., Forti, G.L. and Gilbert, T. (2009) Statistical Properties of Time-Reversible Triangular Maps of the Square. *Journal of Physics A*: *Mathematical and Theoretical*, **42**, 1-13. http://dx.doi.org/10.1088/1751-8113/42/3/035102

[10] Huang, W. (2005) Characterizing Chaotic Processes That Generate Uniform Invariant Density. *Chaos*, *Solitons & Fractals*, **25**, 449-460. http://dx.doi.org/10.1016/j.chaos.2004.11.016

[11] Anikin, V., Arkadaksky, S., Kuptsov, S., Remizov, A. and Vasilenko, L. (2008) Lyapunov Exponent for Chaotic 1D Maps with Uniform Invariant Distribution. *Bulletin of the Russian Academy of Sciences*: *Physics*, **72**, 1684-1688. http://dx.doi.org/10.3103/S106287380812023X

[12] Huang, W. (2005) Constructing an Opposite Map to a Specified Chaotic Map. *Nonlinearity*, **18**, 1375-1391. http://dx.doi.org/10.1088/0951-7715/18/3/022