Hindawi
Complexity
Volume 2017, Article ID 8692046, 21 pages
https://doi.org/10.1155/2017/8692046

Research Article

Finite Precision Logistic Map between Computational Efficiency and Accuracy with Encryption Applications

Wafaa S. Sayed,[1] Ahmed G. Radwan,[1,2] Ahmed A. Rezk,[2] and Hossam A. H. Fahmy[3]

[1] *Engineering Mathematics and Physics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt*
[2] *Nanoelectronics Integrated Systems Center, Nile University, Cairo 12588, Egypt*
[3] *Electronics and Communication Engineering Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt*

Correspondence should be addressed to Wafaa S. Sayed; wafaa.s.sayed@eng.cu.edu.eg

Received 30 July 2016; Revised 8 October 2016; Accepted 4 December 2016; Published 12 February 2017

Academic Editor: Alicia Cordero

Chaotic systems appear in many applications such as pseudo-random number generation, text encryption, and secure image transfer. Numerical solutions of these systems using digital software or hardware inevitably deviate from the expected analytical solutions. Chaotic orbits produced using finite precision systems do not exhibit the infinite period expected under the assumptions of infinite simulation time and precision. In this paper, digital implementation of the generalized logistic map with signed parameter is considered. We present a fixed-point hardware realization of a Pseudo-Random Number Generator using the logistic map that experiences a trade-off between computational efficiency and accuracy. Several introduced factors such as the used precision, the order of execution of the operations, parameter, and initial point values affect the properties of the finite precision map. For positive and negative parameter cases, the studied properties include bifurcation points, output range, maximum Lyapunov exponent, and period length. The performance of the finite precision logistic map is compared in the two cases. A basic stream cipher system is realized to evaluate the system performance for encryption applications for different bus sizes regarding the encryption key size, hardware requirements, maximum clock frequency, NIST and correlation, histogram, entropy, and Mean Absolute Error analyses of encrypted images.

1. Introduction

Chaos theory is a branch of mathematics which precisely describes many of the dynamical systems that exhibit unpredictable, yet deterministic, behavior. Chaotic generators can be classified into discrete time maps and continuous time differential equations. The remarkable importance of chaotic iterated maps in both modeling and information processing in many fields explains the need for their hardware analog and digital realizations, for example, [1–4]. Digital realizations are generally more immune to the imperfections of real electronic systems and more secure due to the easiness of encryption and exhibit greater noise immunity. Moreover, they are composed of digital circuit components which are cheap and easily produced on a single chip. Since early 1990s, a new class of Pseudo-Random Number Generators (PRNGs) based on the digitization of chaotic maps has gained an increasing interest. Discrete time chaotic maps are easier to implement on digital platforms and their generalized forms [5, 6] could be fully utilized to fit multiple applications. This paper is concerned with one of the most famous one-dimensional discrete time chaotic maps: the logistic map.

The conventional logistic map is a quadratic nonlinear map [7] given by

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

where x_n is the iterated variable of the map and λ is a control parameter. Despite the simplicity of its mathematical relation that uses simple and computationally fast operators, it is highly rich in information and indications that are very useful in the field of chaos theory and chaotic systems. It has also found its way, among other chaotic generators, to many practical applications such as biology, physics, chemistry [8–10], pseudo-random number generation [11], secure data and image transfer techniques [12–17] with recent security

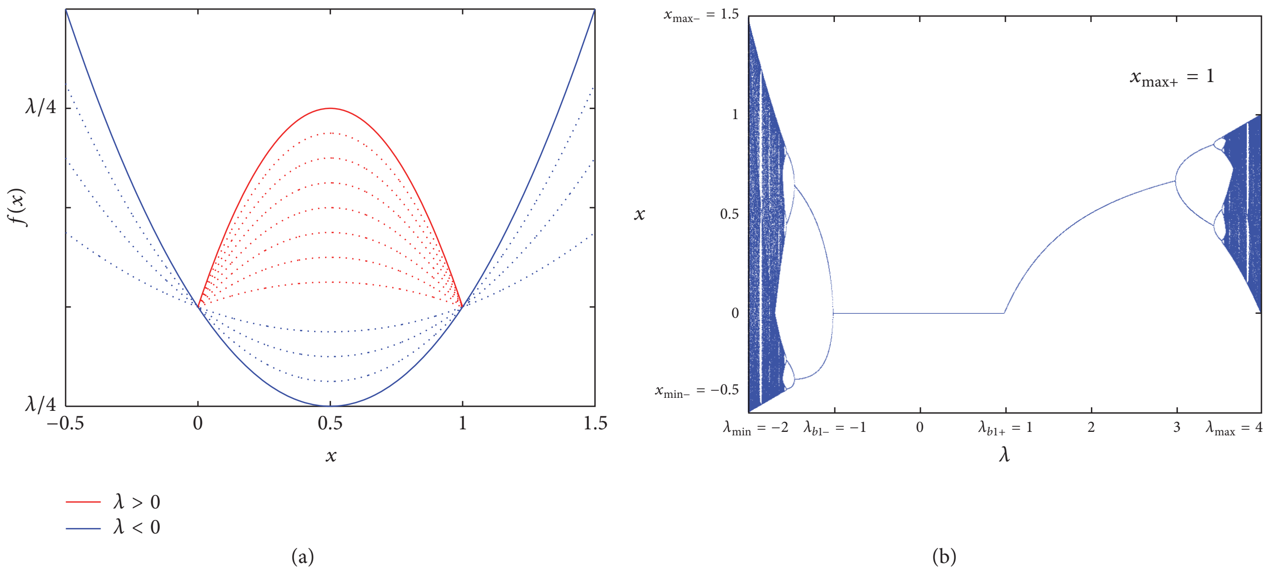


Figure 1: (a) Graph of $f(x) = \lambda x(1 - x)$. (b) Bifurcation diagram of $f(x)$ versus the control parameter λ.

reevaluation of some of them such as in [18], and financial modeling [19, 20].

Generalized logistic map with signed parameter in which the bifurcation diagram extends in both positive and negative control parameter sides has been analyzed in [6]. It has been shown that period doubling route to chaos occurs for convex maps as well as concave maps. This is shown in Figure 1(a) for different values of the control parameter λ. The output in negative control parameter side, called mostly positive map, has a wider range that extends asymmetrically with alternating sign as shown in Figure 1(b) with suggested applications in [6]. The key-points of the bidirectional bifurcation diagram are illustrated in Figure 1(b) including bifurcation points and output ranges in both sides which may be listed as follows:

(i) For $\lambda > 0$, the first bifurcation point in the positive side $\lambda_{b1+} = 1$, where the type of the first nonzero solution is a fixed point. In addition, the upper bound on the output $x_{\max+} = 1$ which takes place at $\lambda_{\max} = 4$.

(ii) For $\lambda < 0$, the first bifurcation point in the negative side $\lambda_{b1-} = -1$, where the type of the first nonzero solution is period-2. In addition, the lower and upper bounds on the output are $x_{\min-} = -0.5$ and $x_{\max-} = 1.5$, respectively, which take place at $\lambda_{\min} = -2$.

Unseen behavior lies between the analytical study of chaos and its digital representation where the effect on dynamical properties is inevitable. Several methods of digitization could come to mind such as the following: software implementations in floating-point arithmetic formats, simulations in fixed-point formats, hardware realizations either in ASIC or in FPGAs, and other digital implementations. Software simulations of digital chaotic maps are criticized for being unsuitable for direct application to hardware FPGAs which imply specific assumptions.

In this paper, a hardware oriented analysis of finite precision logistic map using fixed-point arithmetic is presented accompanied by a digital hardware implementation of PRNG. The basic operations constituting the map are executed individually in a sequential manner with the truncation step implemented between them. Throughout our discussion, four factors which affect the finite precision logistic map are considered. Two of them are explicit and not new which are the control parameter λ and the initial point x_0; however, finitude adds up to their known effects. The other two factors are introduced by the digital representation which are the precision or bus size p and the order of execution $f(x)$. A slight perturbation in any of these factors can yield massively different responses with varied properties in low and intermediate precisions. The effect of varying precision on several properties of the generalized logistic map with signed parameter and the differences from the analytical model are discussed comparing positive and negative parameter cases. A basic stream cipher system based on the PRNG is downloaded on FPGA and tested with text and image encryption applications.

The rest of this paper is organized as follows. First, digital representation of chaotic systems and a literature survey on previous related works are presented in Section 2. Then, Section 3 discusses how the one-dimensional logistic map can be represented in digital hardware realizations such that it can work for either positive or negative parameter cases. The assumptions required to simulate this representation in software environments are also discussed. Different versions of the map are proposed based on the order of execution of the operations constituting its expression. In Section 4, two of these versions are chosen primarily to conduct various experiments and demonstrate results including the following: the bifurcation diagram, its key-points, time series, periodicity of the generated sequence, and maximum Lyapunov exponent (MLE). The effects of varying precision, initial condition, and order of execution on the type of solution are statistically analyzed comparing positive and negative parameter cases.

Section 5 presents a hardware realization of a stream cipher system for text and image encryption applications based on the conventional logistic map as a Pseudo-Random Number Generator. The encryption performance, speed, and implementation area are evaluated at different bus sizes. NIST randomness tests, correlation, histogram, entropy, and Mean Absolute Error analyses of encrypted images are carried out for different bus sizes. Finally, Section 6 summarizes the contributions of this paper.

2. Digital Representation of Chaotic Systems

In the field of chaos-based communication and for practical considerations, a design guide of a computationally efficient PRNG using chaotic systems with finite precision is needed. The reason why chaos-based PRNGs are suggested frequently without paying attention to the effect of finite precision could be owed to the β-shadowing lemma. This lemma ensures that there exists an exact chaotic orbit close to the pseudoorbit with only a small error [21]. However, there is an argument with strong evidences that this lemma cannot be applied to digital chaos. Previous research efforts have attempted either to come up with a theoretical formulation of the problem and its consequences or to experimentally obtain results and analyze them in the aim of acquiring full understanding of the problem. In this experimental approach, several properties of chaotic systems are used as indicators that can be used to uncover security weakness hidden inside some digital chaotic ciphers.

There are two aspects of regarding digitally implemented chaos, either redefining the equation in a digital form and confining outputs to the integer domain [22, 23] or digitally implementing it in finite precision [24–30]. Since we are concerned with digital implementations, a review of several studies about the effect of finite precision on the properties of chaotic systems is presented. The problem of simulating or implementing digital chaos is composed of two parts: finite time and finite precision. Sentences like steady state or the limit as the number of discrete time steps approaches infinity no longer carry the same meaning. The behavior of a limited number of time samples can be recorded for some finite precision; that is, there is no practical implementation that is equivalent to infinite time or precision.

2.1. Continuous Time Chaotic Systems. Corless in [24] discussed numerical simulations, with finite time and precision, of chaotic dynamical systems and how much they should be trusted. He suggested that the computed orbit and the accompanied value for MLE could be falsely interpreted as chaotic (or nonchaotic). This could be owed to the ill-conditioned nature of chaotic dynamical systems where small errors in initial conditions or involved operations are exponentially amplified with time. Consequently, no measure exists of how much the actual response obtained shall deviate from the expected behavior, and this deviation cannot be tracked as time progresses.

Several recent studies for the effect of limited precision on the properties of digitally implemented continuous time chaotic systems have been conducted. For example, in [27, 28], fully digital implementations of several 3rd-order ODE-based chaotic systems have been studied. The threshold minimum precision required for chaos has been decided to be in the range of 8 to 11 fractional bits.

It is expected in advance that simpler systems with less dynamics such as one-dimensional discrete time logistic map needs a higher threshold minimum precision. The variation in the response is expected to be slower with varying the used precision.

2.2. Discrete Time Chaotic Systems. Li et al. in [25] studied digitization of one-dimensional piece-wise linear chaotic maps (PWLCM) and suggested several ways to reduce its negative effect. The effect of finite precision on the periodicity of a PRNG based on the logistic map has been explored in [26]. The algorithm employs truncation in a single-precision floating-point environment after converting the binary32 format to a denormalized binary fraction. Truncation takes place only after the execution of the whole expression, considering the subtraction followed by two multiplication operations in (1) as a single operation. However, this is not suitable for a fixed-point arithmetic FPGA implementation.

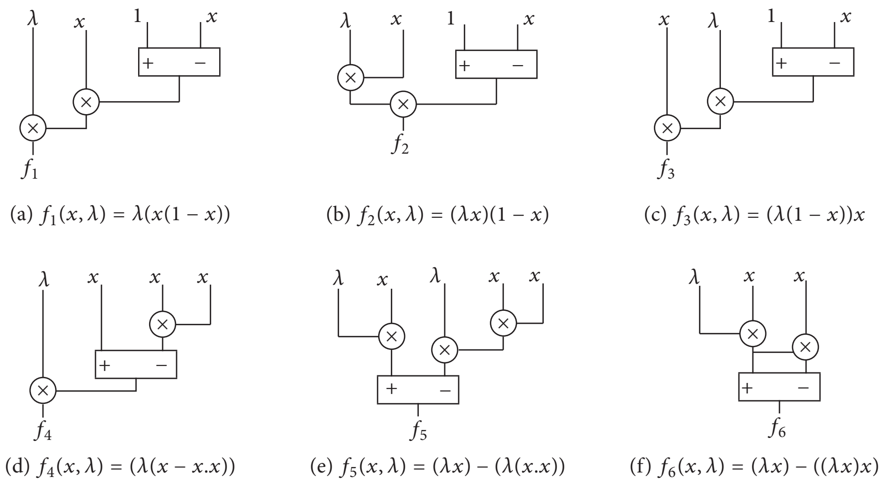
3. Fixed-Point Representation of the Logistic Map

Fixed-point representation uses integer hardware operations controlled by a given convention about the location of the fractional point. Our discussion focuses on computationally efficient fixed-point implementations of chaos, specifically one-dimensional logistic map. The reason is that fixed-point arithmetic is significantly faster and less expensive than an equivalent floating-point hardware implementation. In addition, most commercial arithmetic logic unit (ALU) hardware, for example, FPGAs, is based on it. Such hardware buses typically offer between 8 and 64 bits of precision.

3.1. Assumptions of Fixed-Point Binary Representation. Using finite precision fixed-point binary system, the evaluation of the logistic map function is carried out in a similar manner to a microprocessor instruction set; that is, it is subdivided into a sequence of basic operations. MATLAB fixed-point toolbox is used to simulate digital representation of the logistic map on FPGA.

The integer parts of the included ranges, $\lambda \in [-2, 4]$ and $x \in [-0.5, 1.5]$, are totally representable in 4 bits in two's complement coding. These ranges correspond to the two maps: positive logistic map and mostly positive logistic map as illustrated before in Figure 1. It is guaranteed that the resulting value $x \in [-0.5, 1.5]$ is bounded; that is, no extra bits are needed for handling overflow conditions. The total number of bits, or bus size, is denoted by p for precision which is represented as p_i integer bits and p_f fractional bits such that $p = p_i + p_f$.

Values of p starting from a lower bound of 8 correspond to the least bus size offered by FPGAs, that is, 4 bits in both the integer and the fractional parts. A reasonable upper bound $p = 27$ resembles the equality of the number of fractional bits $p_f = 23$ to the number of bits in the



(a) $f_1(x,\lambda) = \lambda(x(1-x))$ (b) $f_2(x,\lambda) = (\lambda x)(1-x)$ (c) $f_3(x,\lambda) = (\lambda(1-x))x$

(d) $f_4(x,\lambda) = (\lambda(x - x.x))$ (e) $f_5(x,\lambda) = (\lambda x) - (\lambda(x.x))$ (f) $f_6(x,\lambda) = (\lambda x) - ((\lambda x)x)$

Figure 2: Six different maps in fixed-point arithmetic.

fractional part f of the single-precision binary floating-point representation, which is the smallest precision used in most software implementations. Such upper bound is tentative and changes frequently in the rest of the paper according to the sensitivity of the studied property to precision. The following assumptions are made in simulating digital representation of the logistic map:

(i) The values of x and λ and the output of each basic operation are fixed-point variables stored in finite length Registers.

(ii) All operations are carried out assuming truncation.

(iii) Two's complement coding representation is used.

3.2. Different Maps in Fixed-Point Arithmetic. The result of the studied function given by (1) can be calculated in multiple ways in fixed-point arithmetic. For instance, consider the expressions shown in Figures 2(a), 2(b), and 2(c). Are they equivalent? Is the associativity property maintained in a fixed-point system? Moreover, the operations could be grouped such that suboperations are performed in different order as in Figures 2(d), 2(e), and 2(f). The six shown alternatives have been chosen to be considered. The hardware resources needed for executing each of them are also illustrated in the form of Registers and arithmetic units (adders, multipliers, etc.).

Throughout the rest of the discussion, all results are obtained by MATLAB starting at initial point $x_0 = 0.5$, discarding the first 1,000 iterations and considering the next 500 ones, except where stated otherwise. Figure 3 shows the bifurcation diagram versus the control parameter λ at $p = 9$, which is expected to exhibit different phases of behavior as those shown in Figure 1(b). However, it could be noticed that different orders of execution yield bifurcation diagrams that are different from those expected regarding the following: key-points, output range, transition between types of responses, and density of points at ranges that are supposed to exhibit chaotic behavior.

From the bifurcation diagrams, $f_3(x)$ and $f_6(x)$ exhibit smoother maps and a more similar behavior to that expected from the logistic map compared to the other studied alternatives. Hence, most of the following discussion concentrates on these two versions of the logistic map, the different properties that they exhibit, and how much they conform to the behavior expected from the mathematical analysis of the map.

Various properties that have been considered as facts in mathematical analysis of the one-dimensional discrete time logistic map are violated in finite precision environments. Several examples are detailed below.

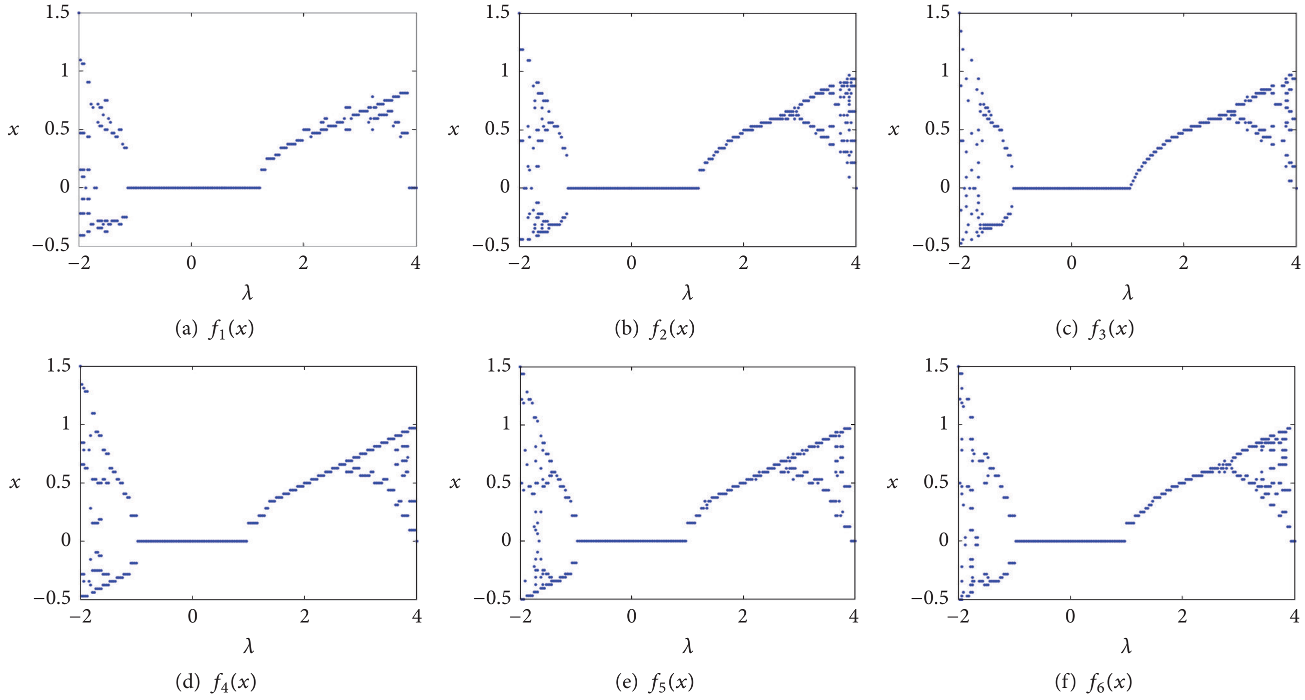
(i) Initial points with a "1" in the least significant bit only, that is, $x_0 = 2^{-p_f}$, could cause the response to die out. In addition, any quantity less than 2^{-p_f} will be considered zero after truncation to p_f fractional bits.

(ii) Analytically, it would be expected from (1) that two initial points with difference $= 1$ yield the same posttransient behavior, since they have the same orbit. However, this property is not always satisfied in finite precision case due to truncation effects.

(iii) The details of the bifurcation diagram over the whole range of λ might slightly alter starting at different initial points. Figure 4 shows that the bifurcation diagram differs from the previous case starting at different initial point $x_0 = 0.125$.

4. Properties of the Selected Maps

In order to study the effect of increasing the number of fractional bits and the impact of low precisions on the properties of logistic map, the bifurcation diagram of $f_3(x)$ versus the control parameter λ is plotted for different precisions in Figure 5, while that of $f_6(x)$ is shown in Figure 6, both starting at initial point $x_0 = 0.5$. The resulting diagrams reveal that the properties of the logistic map are so much affected by precision. These properties include the following: the key-points of the bifurcation diagram, the number of levels or the sequence of values at a fixed value of λ, and the degree



(a) $f_1(x)$

(b) $f_2(x)$

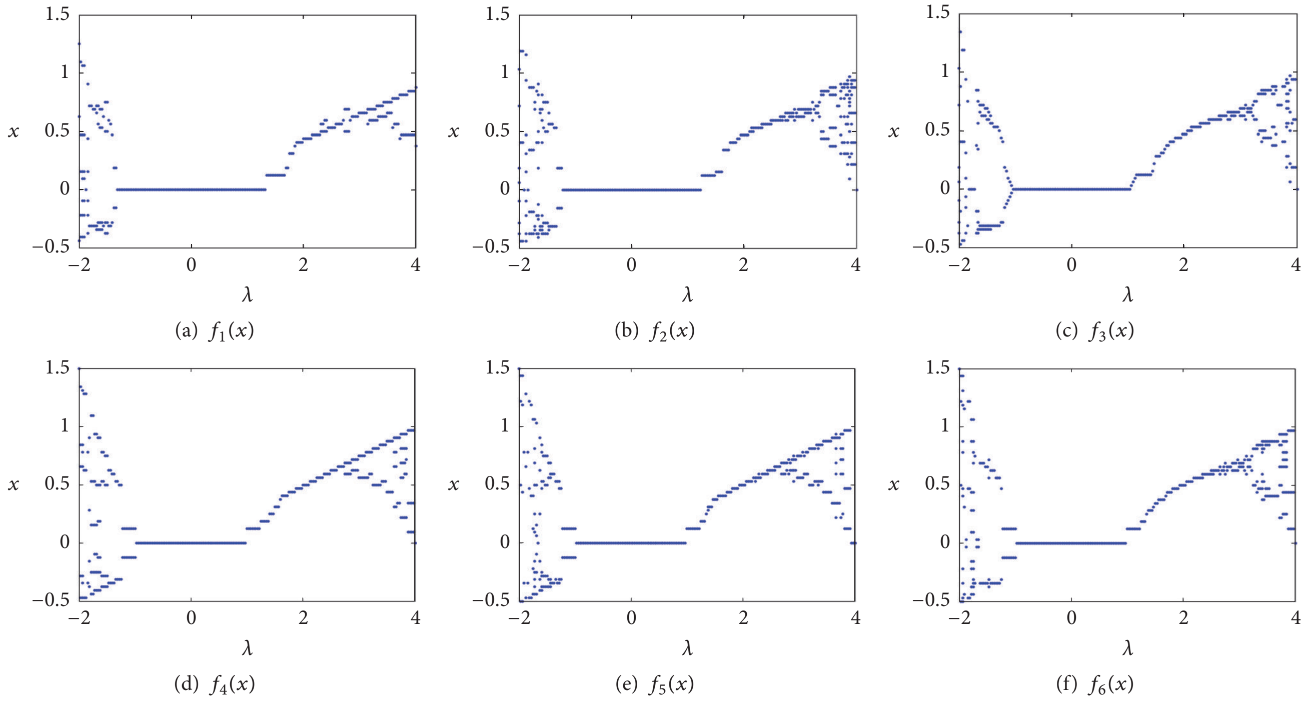
(c) $f_3(x)$

(d) $f_4(x)$

(e) $f_5(x)$

(f) $f_6(x)$

Figure 3: Bifurcation diagram versus the control parameter λ for six different orders starting at $x_0 = 0.5$ at $p = 9$ ($p_f = 5$ bits).



(a) $f_1(x)$

(b) $f_2(x)$

(c) $f_3(x)$

(d) $f_4(x)$

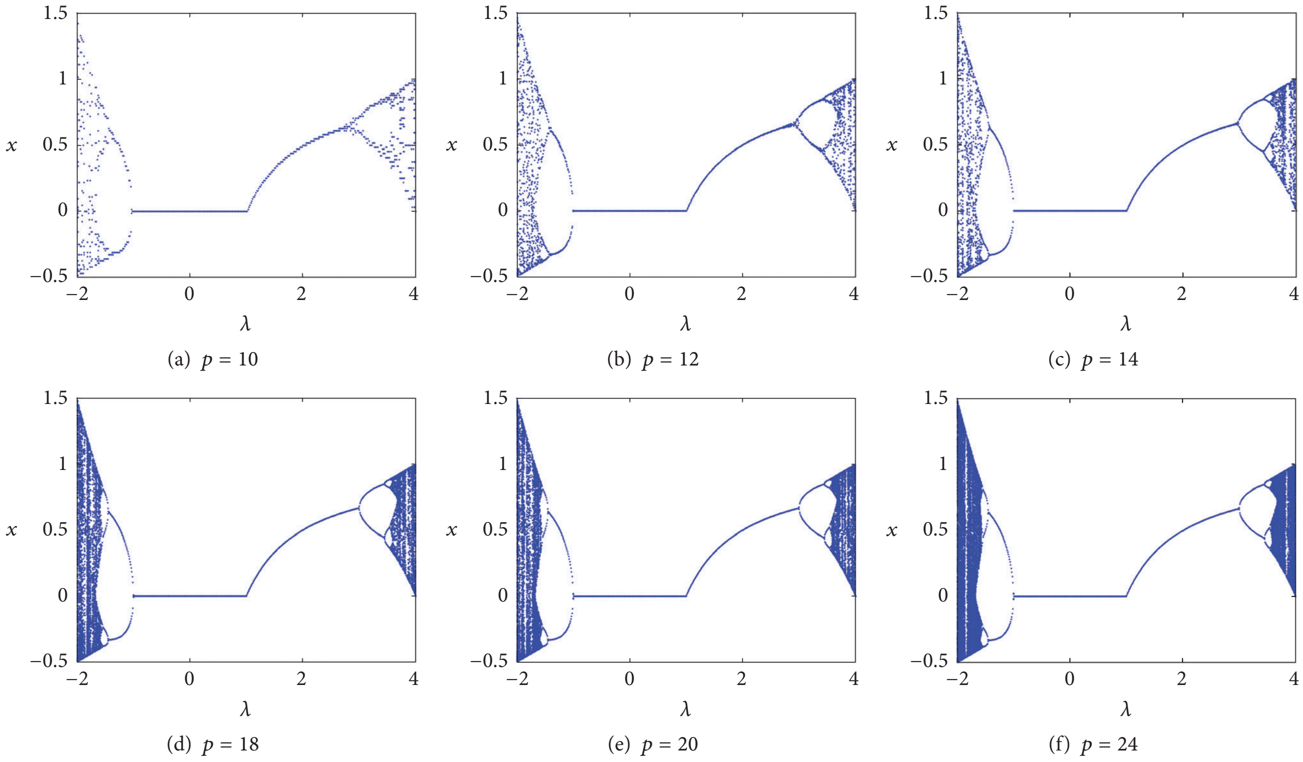
(e) $f_5(x)$

(f) $f_6(x)$

Figure 4: Bifurcation diagram versus the control parameter λ for six different orders starting at $x_0 = 0.125$ at $p = 9$ ($p_f = 5$ bits).

of chaos or how much chaotic is the behavior at values of λ near $\lambda_{\max}$ or $\lambda_{\min}$.

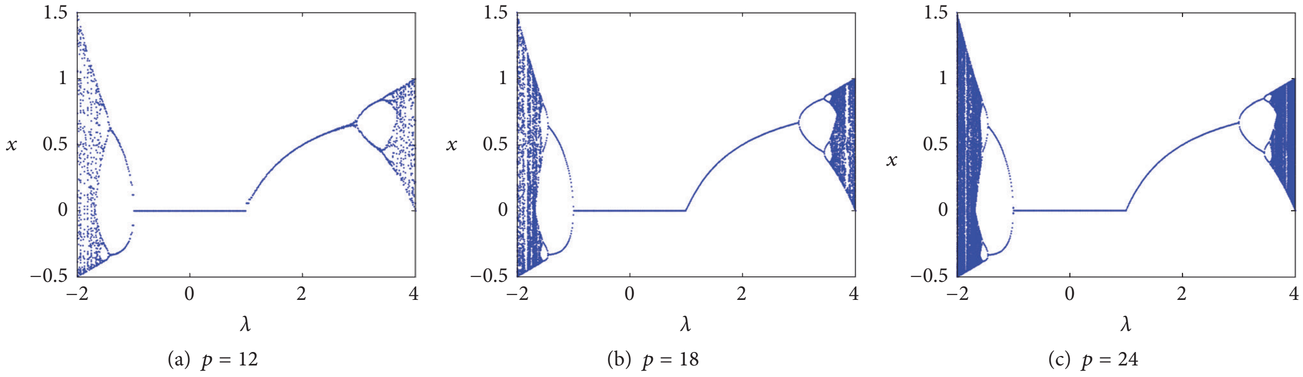
4.1. Key-Points of the Bifurcation Diagram. The key-points of the bifurcation diagram play an important role as design specifications of the logistic map utilized in various applications, specifically for generalized maps with extra parameters as those proposed in [5, 6] and others. These key-points differ for fixed-point representation from the analytical expected behavior defined in Section 1 due to truncation effects.



(a) $p = 10$ (b) $p = 12$ (c) $p = 14$

(d) $p = 18$ (e) $p = 20$ (f) $p = 24$

FIGURE 5: Bifurcation diagram of $f_3(x)$ versus the control parameter λ for different values of bus size starting at $x_0 = 0.5$.



(a) $p = 12$ (b) $p = 18$ (c) $p = 24$

FIGURE 6: Bifurcation diagram of $f_6(x)$ versus the control parameter λ for different values of bus size starting at $x_0 = 0.5$.

However, this difference decreases as p increases as discussed below.

4.1.1. Double-Precision Floating-Point. Using double-precision floating-point calculations, $\lambda_{b1+} = 0.969$, $x_{\max+} = 0.999738909465984$, $\lambda_{b1-} = -0.967$, $x_{\min-} = -0.49974730424707$, and $x_{\max-} = 1.5$. These values for λ are rounded to the third decimal digit after the point and obtained comparing with epsilon machine (defined in MATLAB as *eps*). The differences between the results of double-precision floating-point calculations and the expected results could be owed to their relative inaccuracy. They do not satisfy neither infinite precision nor infinite time conditions assumed analytically. Hence, floating-point arithmetic implementations of chaotic generators and their impact on the various properties need to be studied as well.

4.1.2. Fixed-Point Implementation. Using fixed-point map versions $f_3(x)$ and $f_6(x)$, let us consider the positive control parameter side at first. Figure 7(a) shows the values of λ_{b1+} for $8 \le p \le 26$ for various initial points $x_0 = \{0.125, 0.25, 0.375, 0.5\}$. For the map $f_3(x)$, Figure 7(a) shows that λ_{b1+} starts at values higher than its analytic value "1" at low precisions and then starts to decrease gradually approaching "1"; on the other hand, $f_6(x)$ seems insensitive to precision from the viewpoint of the value of λ_{b1+} for these four values of initial point. For output range, calculations are performed at multiple initial points and then the average of these different

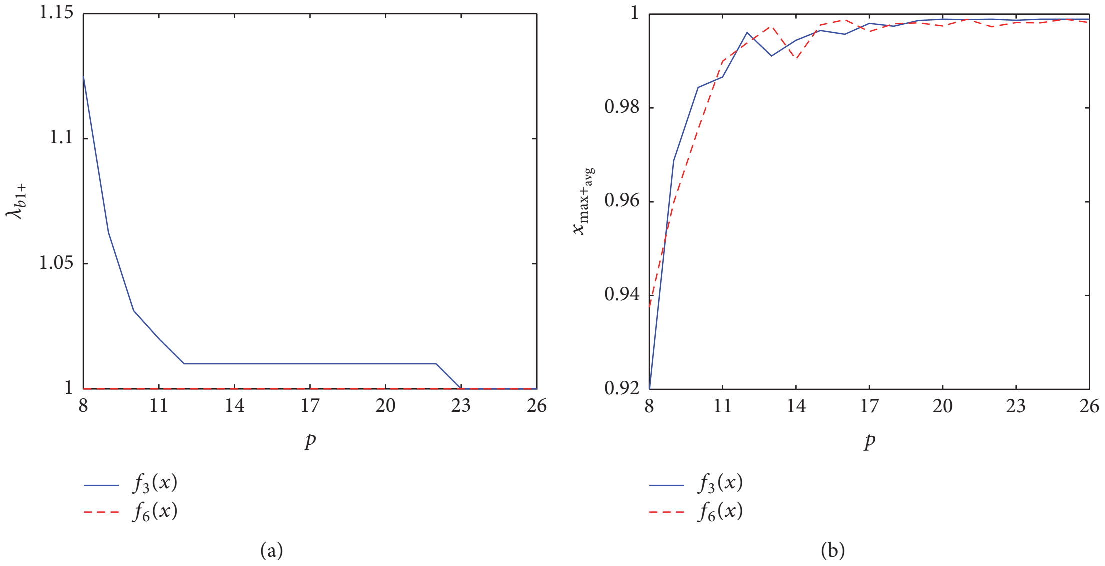


FIGURE 7: The key-points of the bifurcation diagram for the two positive control parameter map versions $f_3(x)$ and $f_6(x)$ at different precisions. (a) The first bifurcation point. (b) The average maximum value.

results is considered. Figure 7(b) shows the average value of the upper bound $x_{\max+_{\text{avg}}}$ on responses starting at multiple initial conditions versus different precisions. For both maps, $x_{\max+_{\text{avg}}}$ starts at values lower than its analytic value "1" at low precisions, then starts to increase gradually, with some fluctuations, approaching "1."

Similarly, the key-points of the bifurcation diagram in the negative control parameter side are studied. Figure 8(a) shows the values of λ_{b1-} where similar comments to the positive control parameter case could describe the plot but for the absolute value $|\lambda_{b1-}|$ instead. Figure 8(b) shows the values of $x_{\min-_{\text{avg}}}$ at different precisions, whereas Figure 8(c) shows the values of $x_{\max-_{\text{avg}}}$. The map $f_6(x)$ seems to be less sensitive to precision variation than $f_3(x)$. The average minimum value $x_{\min-_{\text{avg}}}$ starts at low precisions with absolute values which are lower than 0.5, whereas $x_{\max-_{\text{avg}}}$ starts with values which are lower than 1.5. As precision increases, the key-points approach their analytical values.

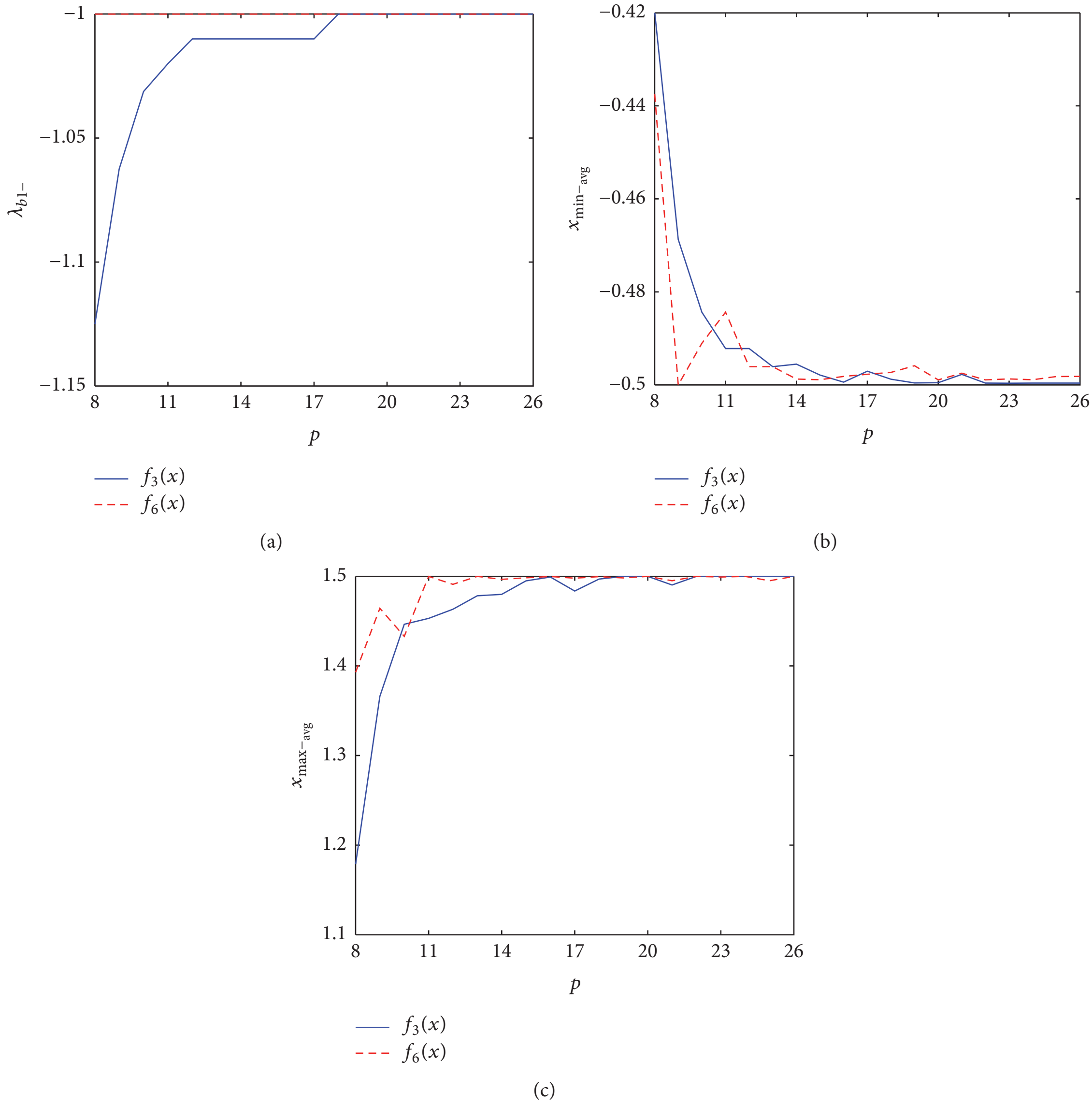
4.1.3. Sensitivity to Initial Conditions. From Figures 7(a) and 8(a), the values of λ_{b1+} and λ_{b1-} seem insensitive to the value of initial point x_0. On the other hand, the effect of initial point on the values of $x_{\max+}$, $x_{\min-}$, and $x_{\max-}$ cannot be avoided in finite precision implementations especially at low precisions. The value $x_{\max+}$ occurs at $\lambda = 4$, whereas $x_{\min-}$ and $x_{\max-}$ occur at $\lambda = -2$. Both values of λ exhibit maximum chaotic behavior, where sensitivity to initial conditions is a basic characteristic of the bifurcation diagram. Analytically, the "infinite" sequence generated at maximum chaotic behavior has lower and upper bounds which "must" be reached. Yet, in finite precision implementations, the length of the generated sequence is limited by both finite precision and time. Thus, it is not guaranteed whether its lower and upper bounds shall coincide with the analytical values or not, especially at low precisions.

4.1.4. Precision Threshold. By precision threshold, we mean the precision below which the properties of the map severely deteriorate and above which changes become less significant. It does not mean that the behavior becomes exactly as the analytical approach. From Figures 7 and 8, it is clear that the values of the key-points derived through mathematical analysis are the asymptotes that finite precision values approach as $p \to \infty$. The threshold minimum precision for key-points can be chosen as $p = 23$ for $f_3(x)$ and $p = 20$ for $f_6(x)$, for instance.

4.2. Time Series. A chaotic posttransient response should have a new value generated at each discrete time instant such that no periodicity can be recognized. In this section, the time series at values of λ that are supposed to be chaotic are studied in finite precision. The effects of varying the used precision and the initial point at which the orbit starts are explained.

Values near $\lambda = 4$ or $\lambda = -2$ which exhibit the widest chaotic response rich in applications are chosen. Figures 9 and 10 show the time series at $\lambda = 3.9375$ of the maps $f_3(x)$ and $f_6(x)$, respectively, starting at different initial conditions for different precisions. This specific value corresponds to an exactly representable fixed-point number with four fractional bits, corresponding to $p = 8$ the narrowest precision that is examined in our study. Generally, very low precisions exhibit undesirable periodic behavior for almost all initial conditions, and high precisions exhibit relatively long periods for some or most of the initial conditions. Time series at some combinations of p and x_0 analytically expected to be chaotic are periodic instead, for example, Figure 10(b).

For example, to study the reason behind the strange result obtained in Figure 10(b), the cobweb plot is shown



(a)

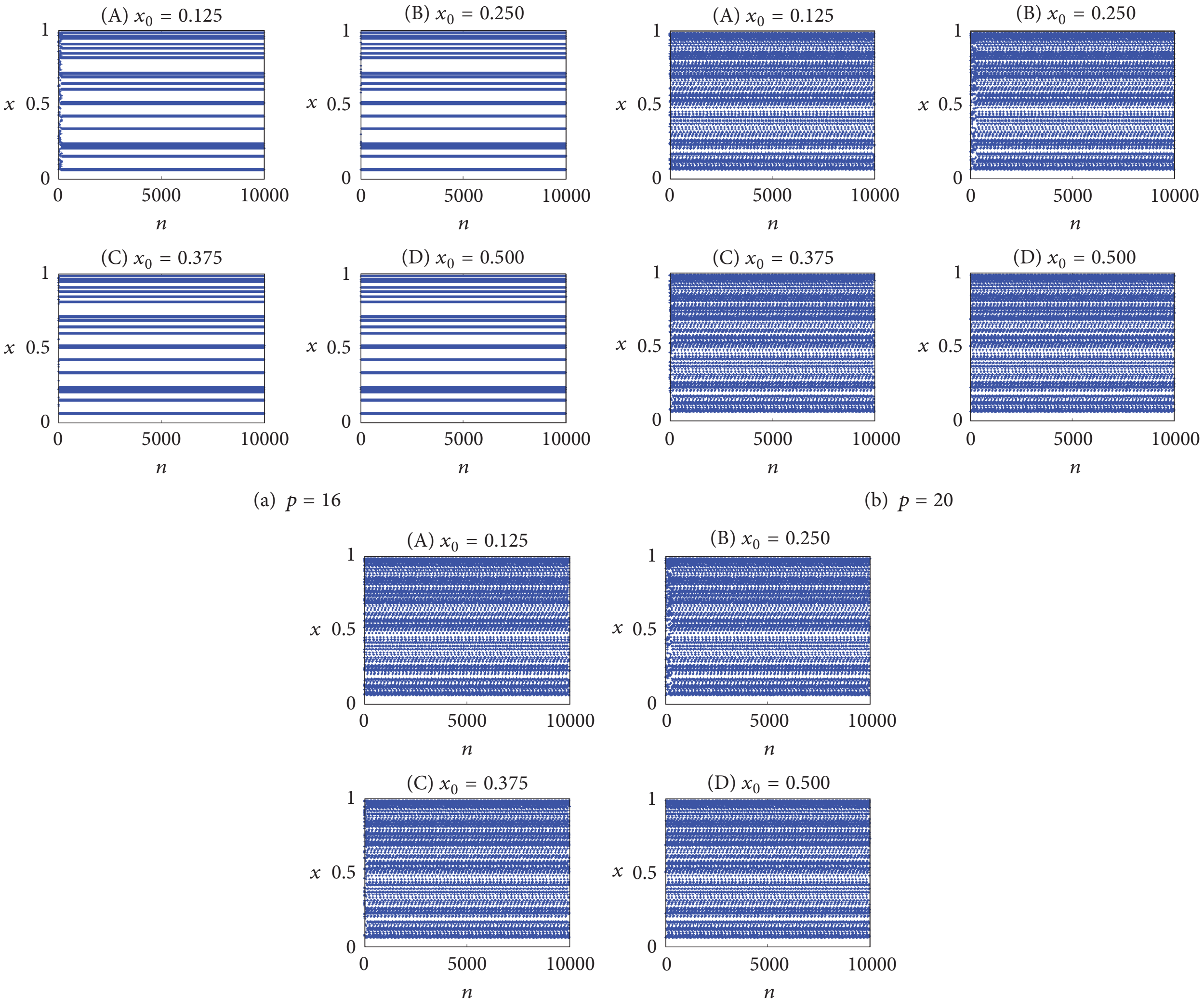
(b)

(c)

Figure 8: The key-points of the bifurcation diagram for the two negative control parameter map versions $f_3(x)$ and $f_6(x)$ at different precisions. (a) The first bifurcation point. (b) The average minimum value. (c) The average maximum value.

in Figure 11 which is a rough plot for the orbit of x starting at different initial points x_0, where the graph of the map function is sketched together with the diagonal line $y = x$. Although the four cobweb plots seem different, the posttransient solution, colored in red and blue, in case of $x_0 = 0.125$ or 0.25 is the same as the plot in case of $x_0 = 0.5$ which fluctuates between six different values, that is, period-6. The output states are as follows (these are the decimal equivalents of the binary sequences represented in the used fixed-point representation at $p = 20$, i.e., 16 fractional bits): 0.5 $\rightarrow$ 0.984375 $\rightarrow$ 0.0605621337890625 $\rightarrow$ 0.2240142822265625 $\rightarrow$ 0.6844635009765625 $\rightarrow$ 0.85040283203125 $\rightarrow$ 0.5009307861328125 $\rightarrow$ 0.984375.... Any orbit, at the same p and λ, including one of these six values, consequently the others, will converge to the same sequence of period-6. On the other hand, the case $x_0 = 0.375$ exhibits a much longer sequence that could be considered "chaotic." Assuming infinite precision, period-6 solution could be obtained through solving $f^6(x_p) = x_p$ along with the stability analysis of the periodic point; $|(f^6)'(x_p)| = 1$. This would yield value(s) for λ at which period-6 solution starts to appear and the corresponding values for x. According to [31], the value $\lambda = 3.9375$ is close to one of these values.

For further illustration, Figure 12 shows the time series for $\lambda = 3.984375$ which is representable in $p \geq 10$. Although the neighborhood of this value does not contain near values that generate periodic sequences, some combinations of p, and x_0 could also yield faulty periodic response. Figure 13 shows the time series at $\lambda = -1.984375$ at different combinations of $f(x)$, p, and x_0 to illustrate the impact of finitude on mostly positive logistic map too. Calculations could be tracked



(a) $p = 16$

(b) $p = 20$

(c) $p = 24$

Figure 9: Time series of $f_3(x)$ at $\lambda = 3.9375$ starting at different initial conditions and various precisions.

similarly to illustrate how the recurrence settles to a specific periodic sequence instead of the chaotic behavior expected from mathematical analysis.

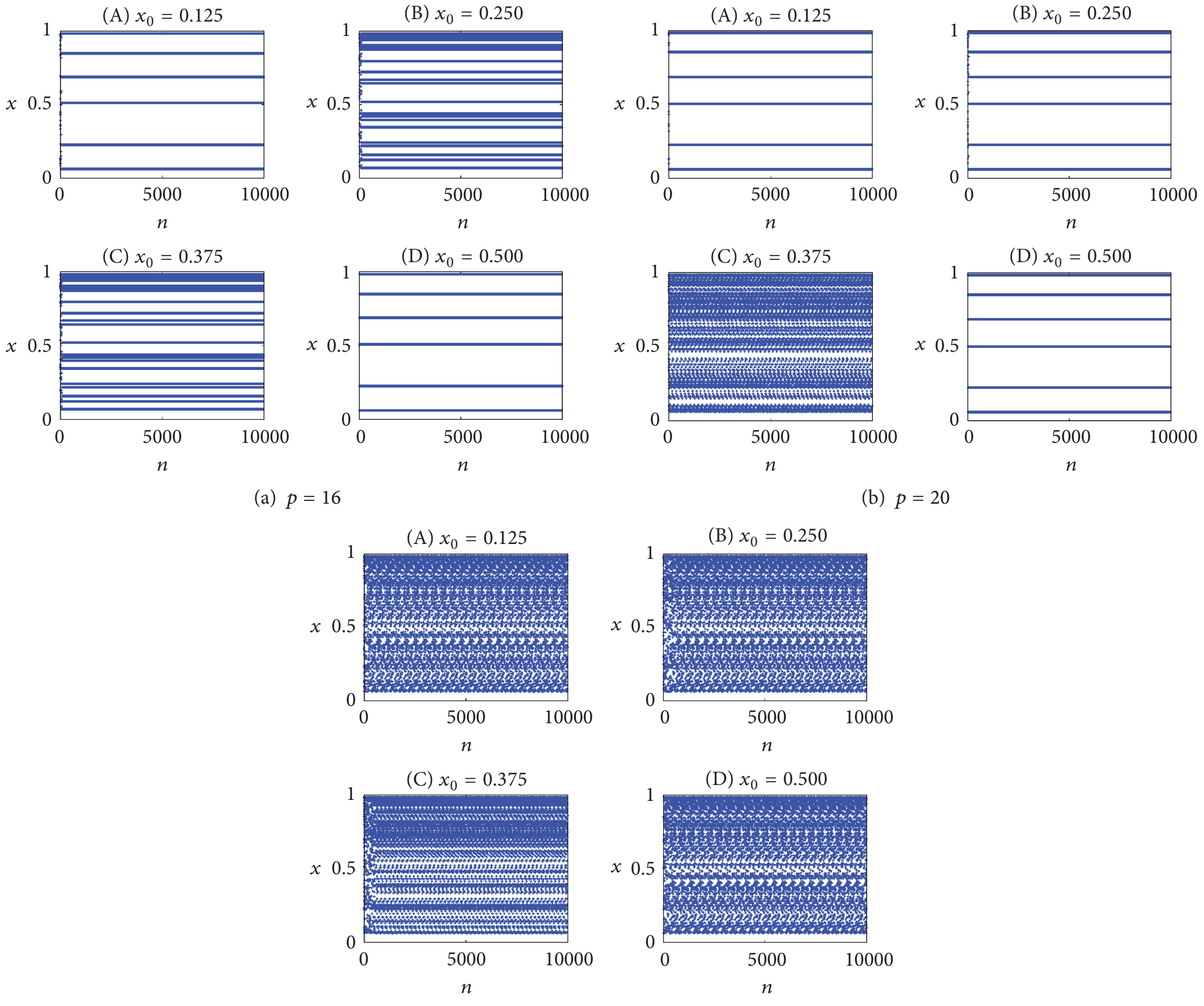
Consequently, the best expectation from the finite precision logistic map is a pseudo-random sequence with long enough period. The cases with significantly short periods depend on the combination of λ, p, and x_0, which might drive us away from the expected chaotic behavior. The phenomenon of deviation from chaotic behavior does not appear in a continuous manner along with varying precision. The solution could be chaotic at a certain precision p and then become periodic at the next precision $p + 1$. The same note could be used to describe the case fixing the used precision and varying the initial point. Moreover, all the studied orders of execution are subjected to these truncation effects in low precisions that yield output sequences with rather short period.

This section emphasizes the dependence of the type of posttransient response on the initial conditions in low and intermediate precisions. The effects of using $p + 1$ instead of p, $x_0 + \delta$ instead of x_0 (for small δ), and any of the orders $f_i(x)$, $i \in \{1, 2, 3, 4, 5, 6\}$ are illustrated more in Section 4.3. It is expected that, at relatively high precisions, x_0 and $x_0 + \delta$ mostly yield the same type of posttransient solution except for some cases in which truncation accidentally drives the solution into a shorter period. This is not to be confused with the property of sensitivity to initial conditions and whether they are two different posttransient solutions or not which is discussed in [29].

From the previous discussion and visually inspecting further time series, we could define the threshold minimum precision, according to the time series, as the precision at which the response "appears" chaotic for most of the initial points allowed by precision. Values close to those suitable for bifurcation diagrams and key-points can be suggested.

4.3. *Periodicity of the Generated Sequence.*

The sequences corresponding to different parameters (p, $f(x)$, λ, and x_0)



(a) $p = 16$

(b) $p = 20$

(c) $p = 24$

Figure 10: Time series of $f_6(x)$ at $\lambda = 3.9375$ starting at different initial conditions and various precisions.

which are generated by finite precision logistic map do not follow an identified, continuous manner as detailed in the previous subsection. It would be quite useful to point out which combinations of the parameters yield responses other than those expected through mathematical analysis. Reaching such combinations could be described as an attempt to solve the inverse problem where the value of x_{n+1} is known and the question is as follows: what is the value of x_n that had yielded it?, for given values of p and λ, as well as an order of execution $f(x)$. The answer to such a question is not straightforward, because successive values of x are held in a finite length Register. Consequently, the real number, possibly irrational, yielded by solving the inverse problem should be mapped to finite precision fixed-point arithmetic. However, the nonlinearity of the relation representing the logistic map makes it hard to decide whether the mapped value should be lower or higher than the analytical solution. The number of steps above or below in the used precision cannot be easily decided either.

The type of posttransient response of the recurrence is obtained in terms of the length of the period formed by the successive solutions. A posttransient sequence of k unique values is described as "period-k" which is affected by the four factors (p, f, λ, x_0). For example, at $\lambda = 4$ and $p = 8$, our experiments yield period lengths of 1 for the 15 available initial points using orders f_1, f_4, f_5, and f_6. However, they yield the same results as [26] with period lengths of either 1 or 3 at the same corresponding initial points using f_2 and f_3. Moreover, lower values of λ which were not considered by [26] are found out to yield longer period length of 4 at several combinations of λ, x_0, and f emphasizing how the introduced factors affect the period length.

Figure 14(a) shows the maximum period, or k, obtained with different orders of execution plotted versus precision for λ from 3.8125 to 4 in steps of 2^{-p_f} and all initial points allowed by the precision. It seems that $f_3(x) = (\lambda(1 - x))x$ yields relatively higher periods. Some other orders are acceptable where the best are $f_2(x)$, $f_3(x)$, and $f_6(x)$ as

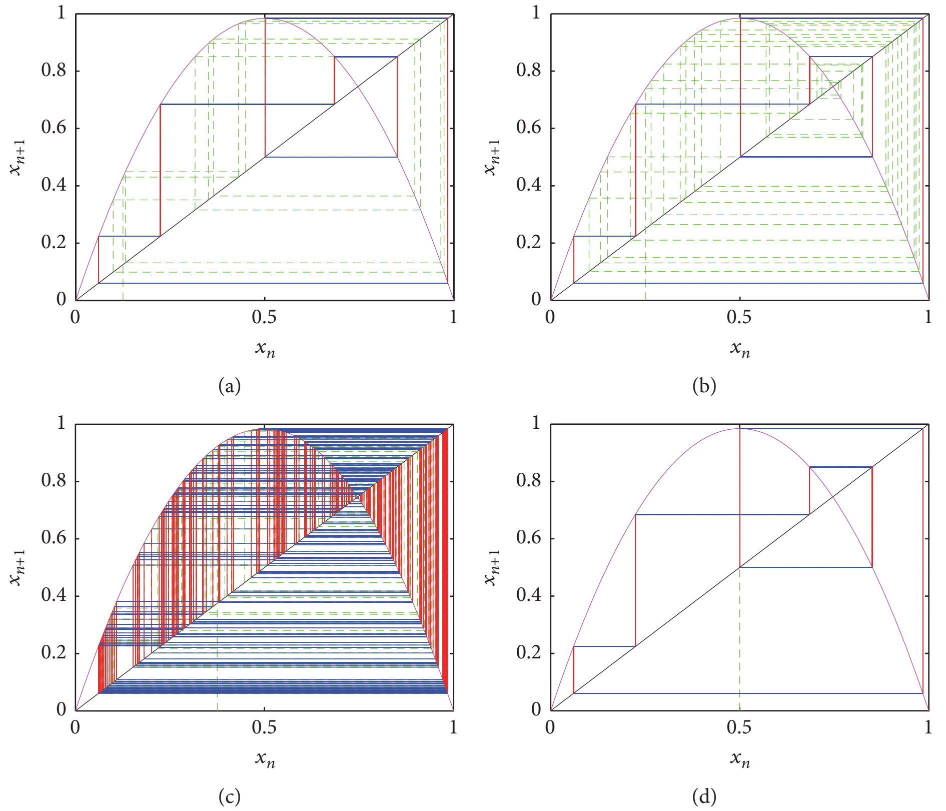


FIGURE 11: Cobweb plots of $f_6(x)$ at $\lambda = 3.9375$ and $p = 20$ starting at different initial conditions: (a) $x_0 = 0.125$, (b) $x_0 = 0.25$, (c) $x_0 = 0.375$, and (d) $x_0 = 0.5$.

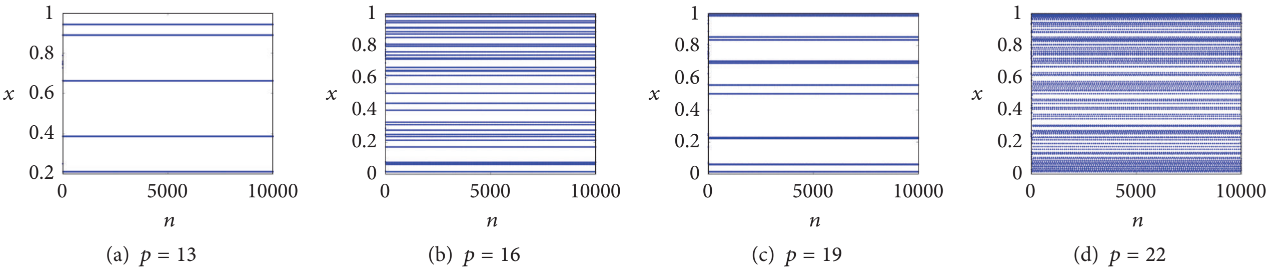
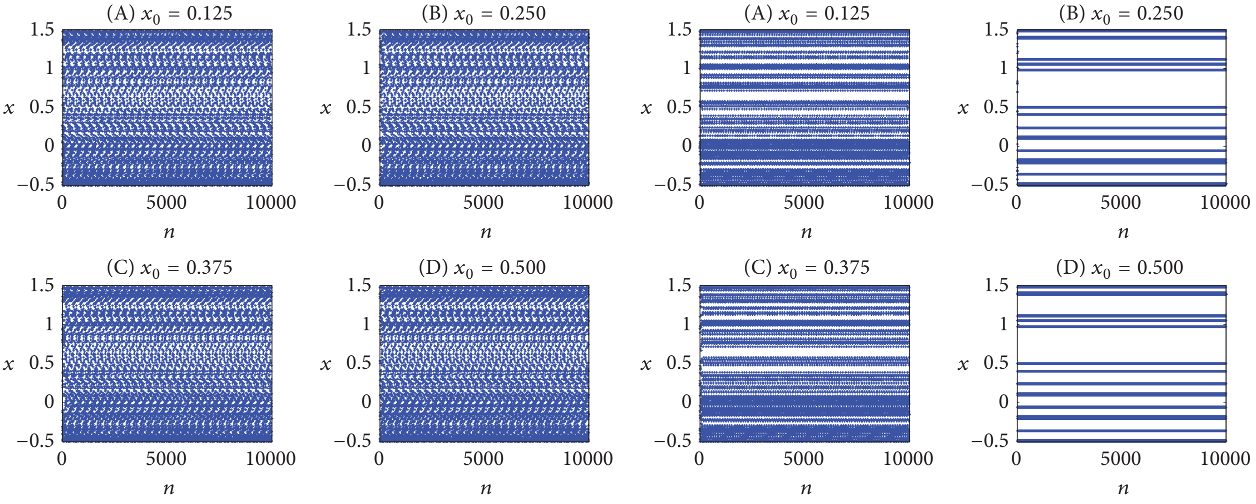


FIGURE 12: Time series of $f_3(x)$ at $\lambda = 3.984375$ starting at $x_0 = 0.25$ and various precisions.

decided before from the bifurcation diagrams in Section 3. It could be noticed that higher precisions provide more levels among which the solution(s) could take their values allowing higher values for k. Figure 14(b) for λ from -2 to -1.8125 shows how the logistic map with negative control parameter exhibits longer periods than that with positive control parameter and at lower precisions. In addition, for selected combinations of the factors, mostly positive map exhibits more alternatives for unique values of k with a longer maximum period, for example, f_1 and f_6 at $p = 11$. This indicates some merits of the logistic map with negative control parameter over the conventional logistic map with positive control parameter.

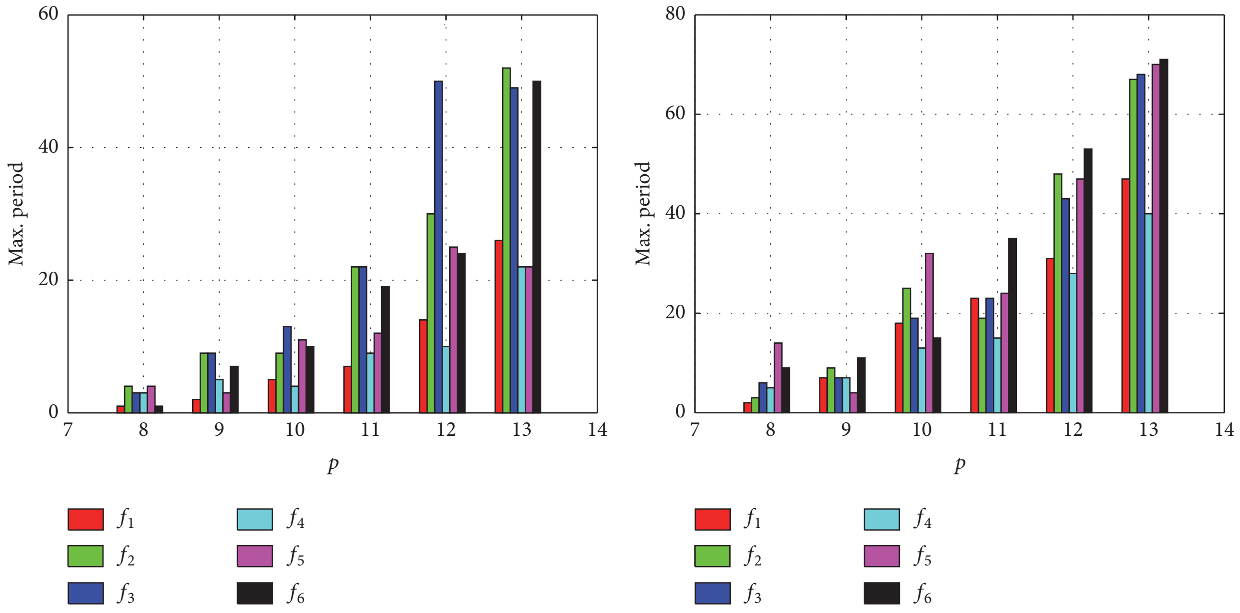
It would be expected that the sequence period is governed by the maximum number of levels allowed by the chosen precision, for example, 2^{p_f} for $\lambda > 0$. Yet, this factor represents a rather loose upper bound imposed by the used precision. The behavior of the studied map and whether its output sequence covers all the allowed levels or not are another important point to consider which has been discussed in [26]. For instance, consider $p = 13$, and the hypothetical maximum number of levels equal $2^9 = 512$ levels. However, experimental results show that the maximum achievable period or number of distinct levels before repeating the sequence is roughly 50 for positive logistic map and 70 for mostly positive logistic map. Hence, the dependence of the



(a) $p = 19$, $f_3(x)$

(b) $p = 19$, $f_6(x)$

Figure 13: Time series of mostly positive finite precision logistic map at $\lambda = -1.984375$ for different combinations of its parameters.



(a)

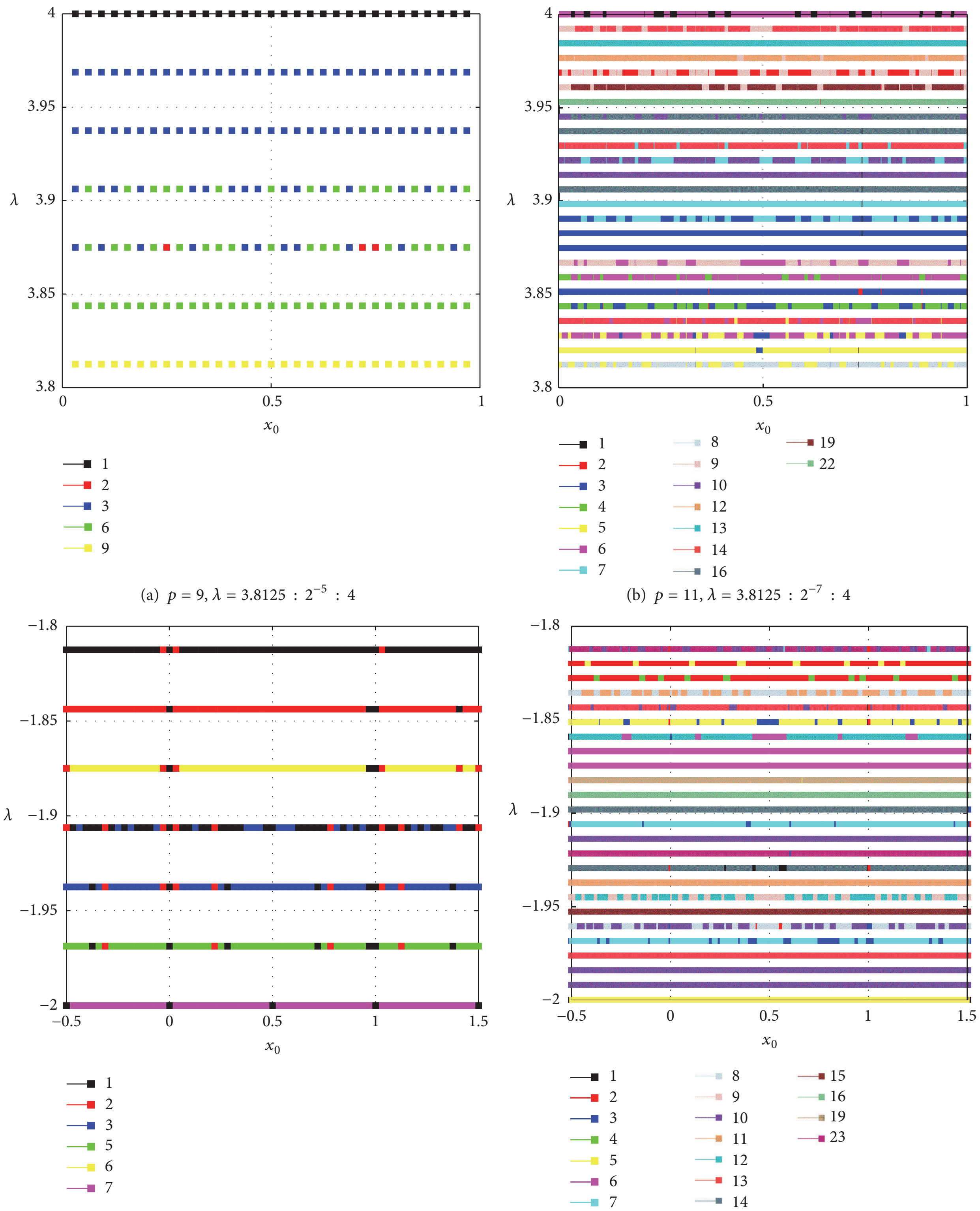
(b)

Figure 14: Maximum period obtained with different orders of execution plotted versus precision $p = 8 \rightarrow 13$ for (a) $\lambda = 3.8125 : 2^{-p_f} : 4$ and (b) $\lambda = -2 : 2^{-p_f} : -1.8125$ and all initial points allowed by p.

obtained period length on the used precision p does not follow a linear scale. The efficiency of filling the allowed levels is still insufficient in rather low and intermediate precisions.

Figure 15 shows all unique periods obtained at a given precision for $f_3(x)$. The legend shows the different colors corresponding to a given period k. Figure 15 illustrates that increasing the used precision provides more combinations of the parameter λ and the initial point x_0 as expected. As precision p increases, the number of alternatives for (f, x_0, λ) increases exponentially and the statistics are limited by huge processing time and memory requirements. In addition, the number of obtained unique periods of output sequence increases with each bit of precision increased for low and intermediate precisions. After reaching a high enough precision threshold, it is expected that the number of obtained unique periods approaches settling. Values close to these obtained before in [29] may result from some combinations, while other combinations may uncover surprising findings.

4.4. Maximum Lyapunov Exponent. Maximum Lyapunov exponent (MLE) is an indication whether the system exhibits chaotic behavior or not as it measures the rate of divergence of



(a) $p = 9, \lambda = 3.8125 : 2^{-5} : 4$

(b) $p = 11, \lambda = 3.8125 : 2^{-7} : 4$

(c) $p = 9, \lambda = -2 : 2^{-5} : -1.8125$

(d) $p = 11, \lambda = -2 : 2^{-7} : -1.8125$

Figure 15: All the generated period lengths in the studied ranges of parameter λ and all initial points allowed by p for $f_3(x)$ and different precisions.

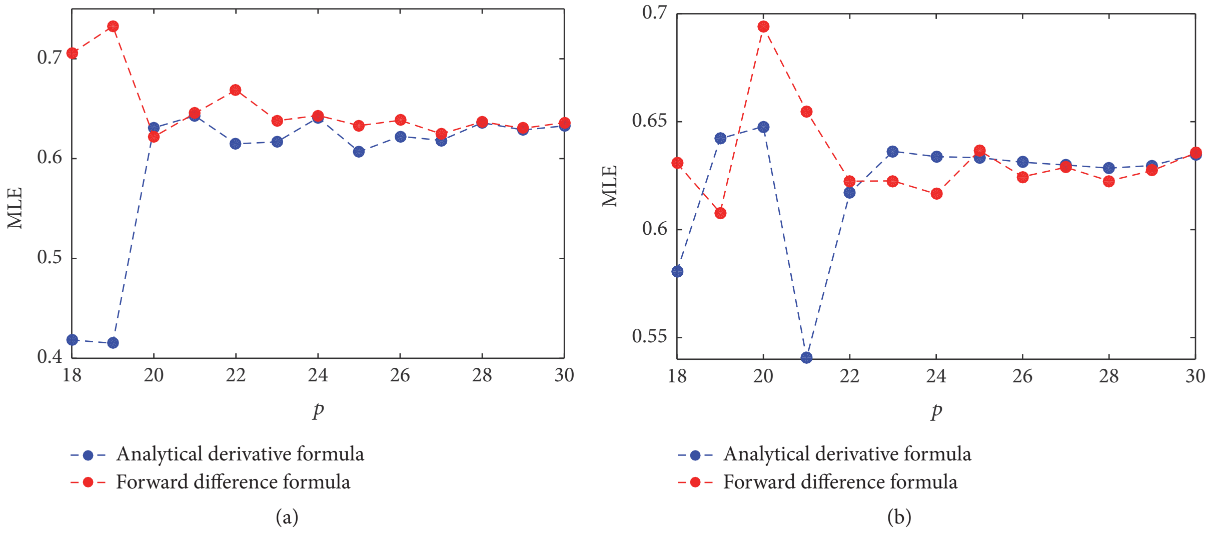


Figure 16: MLE evaluation in two different methods using $f_3(x)$ starting at $x_0 = 0.125$ at (a) $\lambda = 3.984375$ and (b) $\lambda = -1.984375$.

nearby initial points. Two suggested methods for calculating MLE in finite precision are explained in the next two subsections.

4.4.1. Analytical Derivative Formula. MLE for discrete time maps [7] is given by

$$\text{MLE} = \lim_{n\to\infty}\left(\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right), \tag{2}$$

where ln is the natural logarithm and $f'(x_i)$ is the first derivative of the map equation with respect to x at $x = x_i$, in addition to choosing n large enough; for example, $n = 50{,}000$ for MLE value to reach its steady state. In the analytical derivative formula, we calculate MLE of the finite precision logistic map as follows:

$$\text{MLE} = \frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\lambda\left(1-2x_i\right)\right|. \tag{3}$$

4.4.2. Numerical Approximation of First Derivative. The following discussion attempts to investigate whether the numerical approximations for first derivative are more compatible with a discrete map than continuous differentiation rules yielding $f'(x_i) = \lambda(1-2x_i)$. Consider the forward difference approximation of the first derivative

$$f'(x_i) = \frac{f(x_i+\Delta) - f(x_i)}{\Delta}. \tag{4}$$

Substituting (4) in (2) and using the properties of logarithm, we get

$$\text{MLE} = \frac{1}{n}\sum_{i=0}^{n-1}\ln\frac{\left|f(x_i+\Delta) - f(x_i)\right|}{\Delta}, \tag{5a}$$

$$\text{MLE} = \left[\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f(x_i+\Delta) - f(x_i)\right|\right] - \ln\Delta, \tag{5b}$$

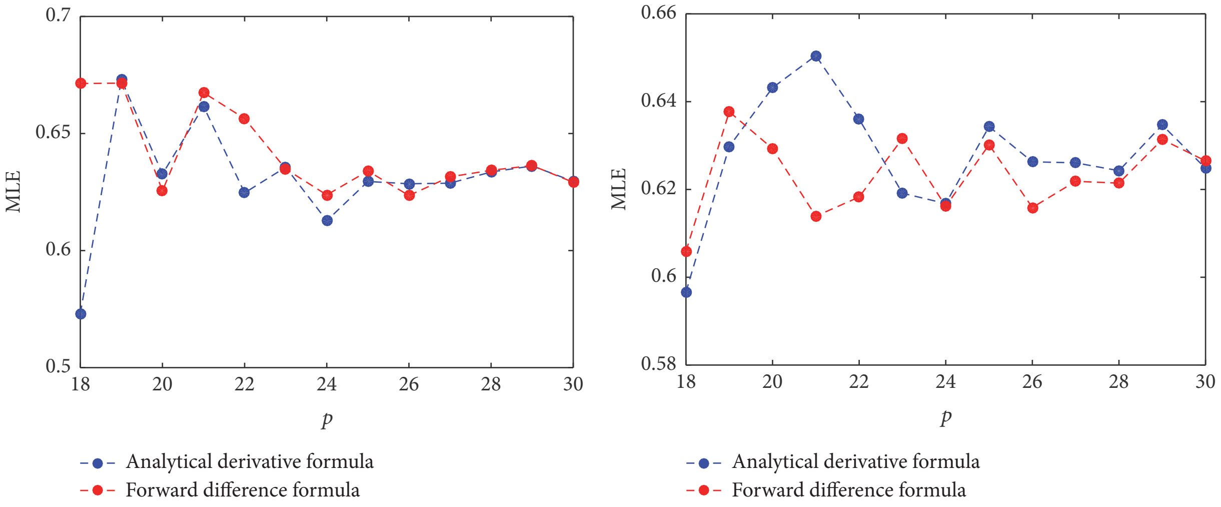
where the minimum value for Δ theoretically equals 2^{-p_f} which is the minimum representable value. However, for practical issues and to avoid overflow, Δ is set to a quite higher value. Both (5a) and (5b) were found to be equivalent in double-precision floating-point and match the analytical method for relatively high precisions. Applying the one-dimensional time series to MLE calculation tools such as [32] used in [27, 28] can be considered as a third approach.

A threshold minimum precision of $p \geq 22$ from the viewpoint of MLE calculation can be suggested as illustrated by Figures 16 and 17. However, results obtained in low precisions make us doubt the validity of both approaches for calculating MLE in rather low precisions and the reliability of the numbers computed through them in deciding how much chaotic a system is. However, the problems in calculating MLE using both methods are barely noticed at quite higher precisions and dominate only at relatively low precisions $p < 22$ as previously mentioned.

We conclude that, at rather low precisions, MLE cannot be used as a standalone indicator of chaotic behavior without considering the corresponding sequence length. The value of MLE calculated through either of the two methods could be falsely positive while the output sequence is clearly periodic. This result comes in accordance with the discussion presented in [24, 25].

5. Encryption Applications

A Pseudo-Random Number Generator (PRNG) is realized using the conventional logistic map (1), as shown in Figure 18. The inputs of the system are the clock, Reset, λ, and x_0. The arithmetic unit is used to compute x_{n+1} using x_n and λ. The Register is used to provide x_n to the arithmetic unit. The value of x_n is updated with Multiplexer's output every clock cycle (iteration). In case of Reset (Reset = 1), the Multiplexer will provide x_0 to the Register. Otherwise, the Multiplexer will pass x_{n+1} to the Register. This unit is realized using VHDL



(a)

(b)

FIGURE 17: MLE evaluation in two different methods using $f_6(x)$ starting at $x_0 = 0.125$ at (a) $\lambda = 3.984375$ and (b) $\lambda = -1.984375$.

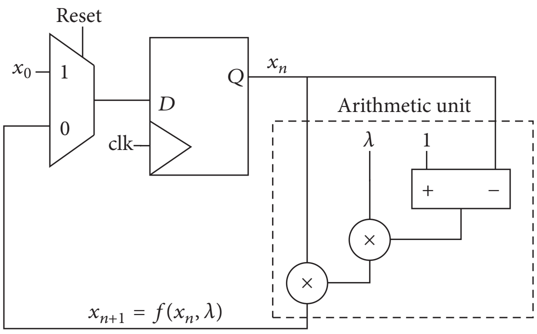


FIGURE 18: Hardware realization of Pseudo-Random Number Generator.

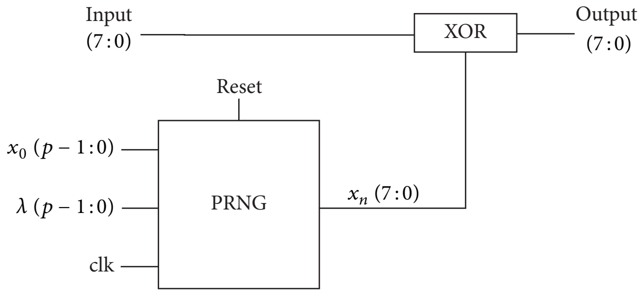


FIGURE 19: Stream cipher system for encryption applications.

and synthesized on Xilinx using XC5VLX50T as the target FPGA. Table 1 shows the hardware implementation area and the maximum clock frequency for different bus sizes.

A basic stream cipher system is realized as shown in Figure 19. The ciphering process is based on Xoring the input data with a stream of random numbers. The PRNG, presented in Figure 18, is used to output the random numbers, where λ and x_0 are used as the encryption key. Hence, the keyspace is 2^{2p}. Every clock cycle the system generates a new random number (RN), captures a new byte from the input data, and Xores the 8 least significant bits of the generated RN with the input byte. The system is realized using VHDL and synthesized on Xilinx using XC5VLX50T. Table 2 summarizes the synthesis results for different bus sizes. The system's performance, regarding the speed and implementation area, improves by decreasing the size of the bus. Unfortunately, decreasing the size of the bus leads to a reduction in the size of the encryption key which makes the system vulnerable to brute force attacks. Thus, the size of the bus must be adjusted to satisfy the security level, speed, and hardware resources.

The stream cipher system is downloaded on FPGA and tested with a text encryption application. The system displays the input word on the first line of the Kit's LCD screen, encrypts the word using the input key, and displays the encrypted word on the second line of the screen. Figure 20 shows the results of the prototype for different bus sizes and encryption keys. The system succeeds in encrypting the input word (Hello World 2016), for all test cases. However, in Figures 20(b) and 20(d), there is a relation between the input text and the ciphered text which leads to poor encryption. In (b), the characters "l"; "space"; and "o" are always transformed to "d"; "("; and "g," respectively. Similarly, in (d), the characters "l"; "space"; and "o" are always transformed to " }"; "1"; and "→," respectively. This is due to the fact that for $\lambda = 2$ the solution of the logistic map does not bifurcate as illustrated previously in Figure 3. Thus, in order to improve the encryption performance, the values of λ must be close to 4.

Moreover, Table 3 shows the encryption results for a famous quote by Mahatma Gandhi [33] using 27-bit bus size and two different keys, $(x_{01}, \lambda_1) = (0.5078741312, 3.7501969337)$ and $(x_{02}, \lambda_2) = (0.7578741312, 3.7501969337)$. The number of different bits between

Table 1: Synthesis results for the logistic map using different bus sizes.

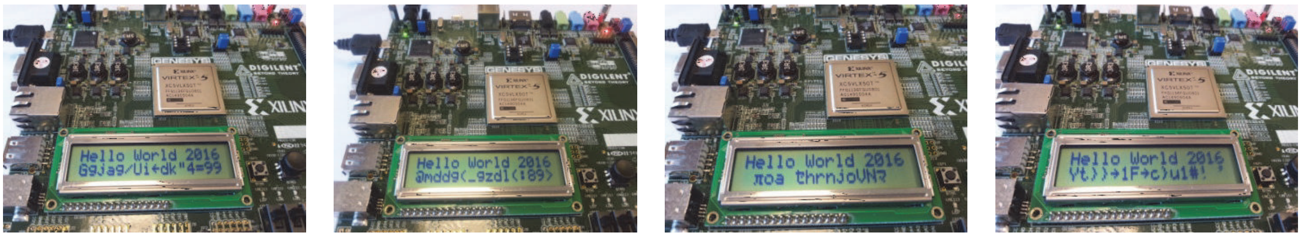
Bus size	Slice Registers (28800)	Slice LUTs (28800)	DSP48Es (48)	Maximum clock frequency
10	10	21	2	104.716 MHz
14	14	29	2	104.251 MHz
18	18	37	2	103.873 MHz
20	20	183	2	79.590 MHz
27	27	253	4	61.812 MHz

Table 2: Synthesis results of the stream cipher system.

Bus size	Slice Registers (28800)	Slice LUTs (28800)	DSP48Es (48)	Maximum clock frequency
10	10	31	2	104.716 MHz
14	14	37	2	104.251 MHz
18	18	45	2	103.873 MHz
20	20	191	2	79.590 MHz
27	27	261	4	61.812 MHz

Table 3: Encryption results for a famous quote using a bus size of 27 bits and two different keys.

Plain text	Live as if you were to die tomorrow. Learn as if you were to live forever. . .
Ciphertext (x_{0_1}, λ_1)	²□ÜÓ3yTy{□@O[fBÑHºõ¬õÈh9Á)§1 ×ì¬□ç¡× ÿG©Ç"XVñîíëÛÕz¤ÊnÇg¾&«¡ DXÌâ
Ciphertext (x_{0_2}, λ_2)	Ý#õ|Áû3äCF□; Ü Õvc! 1´C7Y□$²Ø□Ï#âD¿.` =¡ Ät = æsÕ½ütÚÏ□LalëI□6äÿmíÙEºÐ ÷



Bus size = 8 bits
$\lambda = 3.75$
$x_0 = 0.5$

(a)

Bus size = 8 bits
$\lambda = 2$
$x_0 = 0.5$

(b)

Bus size = 27 bits
$\lambda = 3.750008464$
$x_0 = 0.500061512$

(c)

Bus size = 27 bits
$\lambda = 2.000008464$
$x_0 = 0.500061512$

(d)

Figure 20: Results of the prototype for different bus sizes and encryption keys.

these two keys is reduced to one bit only in order to test the system's key sensitivity. The results show that the encrypted sentences are totally different which imply that the key sensitivity is high.

The randomness of the PRNG is usually tested by the standard NIST suite [34] in order to ensure high security performance. Accordingly, a VHDL test bench has been implemented to interface the Xilinx with the NIST suite. This test bench is used to generate a text file which includes the 8 LSBs of 125000 successive iterations. The PRNG must pass all the NIST tests in order to be considered as true random source. The results of the NIST test, for 8-bit bus size up to 45-bit bus size, are summarized in Table 4. For all tests the initial point x_0 is set to $0.5 + 2^{-13}$ while λ is set to $4 - 2^{-p_f}$, where p_f is the number of fractional bits. The threshold bus size for passing all the NIST tests is 45 bits. As the bus size is decreased below this threshold, the number of reported failures starts to increase until the PRNG fails in all the tests for 8-bit bus size. The system succeeds in all the NIST tests for any bus size greater than 45 bits.

Moreover, the system has been tested with an image encryption application as shown in Table 5. The standard gray color Lena (256 × 256) has been supplied to the stream cipher system in Figure 19. Three bus sizes, 11 bits, 12 bits, and 45 bits, have been used in the analysis.

The vertical, horizontal, and diagonal pixel correlation coefficients ρ are calculated using (6a), (6b), and (6c), where N is the total number of pixels selected from the image and

Table 4: NIST results for different bus sizes.

NIST test (sample: 1000000 bits in length)	8 bits	27 bits	34 bits	36 bits	38 bits	40 bits	42 bits	45 bits' P value
System parameters (λ, x_0)	$(4-2^{-4}, 0.5)$	$(4-2^{-23}, 0.5+2^{-13})$	$(4-2^{-30}, 0.5+2^{-13})$	$(4-2^{-32}, 0.5+2^{-13})$	$(4-2^{-34}, 0.5+2^{-13})$	$(4-2^{-36}, 0.5+2^{-13})$	$(4-2^{-38}, 0.5+2^{-13})$	$(4-2^{-41}, 0.5+2^{-13})$
Frequency	✗	✗	✗	√	√	√	√	0.788699 √
Block frequency (m = 128)	✗	✗	√	√	√	√	√	0.880935 √
Cusum-Forward	✗	✗	✗	√	√	√	√	0.321183 √
Cusum-Reverse	✗	✗	✗	√	√	√	√	0.511427 √
Runs	✗	✗	√	√	√	√	√	0.950620 √
Long runs of one	✗	✗	✗	√	√	√	√	0.301448 √
Rank	✗	✗	√	√	√	√	√	0.178158 √
Spectral DFT	✗	✗	✗	✗	✗	√	√	0.581909 √
Nonoverlapping templates	✗	✗	✗	✗	✗	✗	✗	0.645372 √
Overlapping templates (m = 9)	✗	✗	✗	√	√	√	√	0.566886 √
Universal	✗	√	√	√	√	√	√	0.725132 √
Approximate entropy (m = 10)	✗	✗	✗	✗	✗	√	√	0.877618 √
Random excursions	✗	✗	✗	✗	✗	✗	✗	0.970335 √
Random excursions variant	✗	✗	✗	✗	✗	✗	√	0.125786 √
Linear complexity (M = 500)	✗	√	√	√	√	√	√	0.113062 √
Serial (m = 16)	✗	✗	✗	✗	✗	√	√	0.115512 √

Table 5: Image encryption analysis.

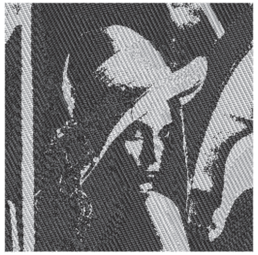
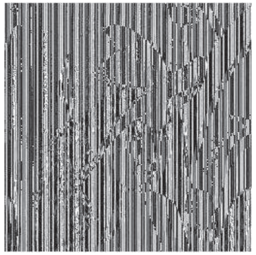
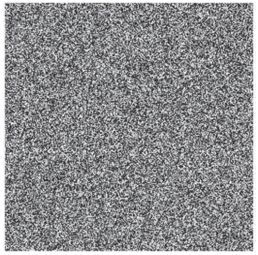
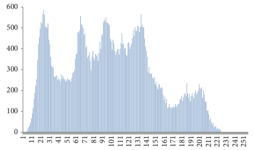
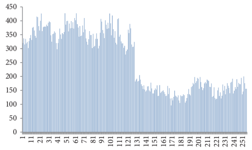
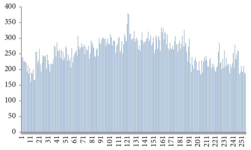
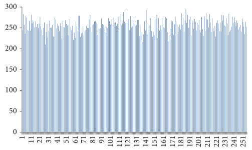
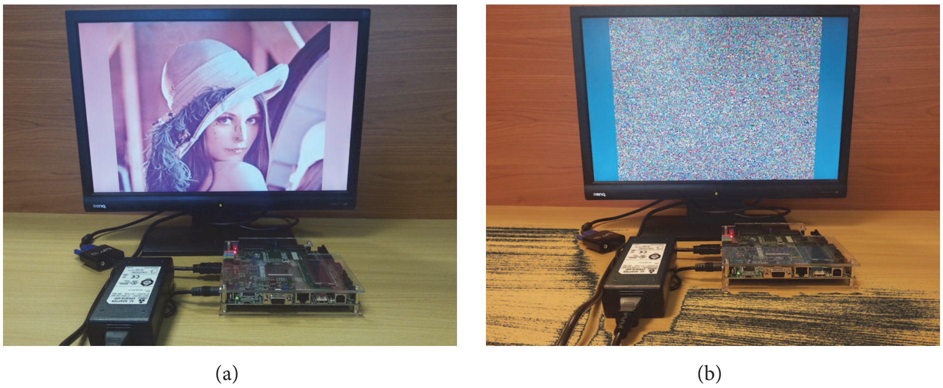
Analysis	Lena 256 × 256	Encrypted Image 11-bits	Encrypted Image 12-bits	Encrypted Image 45-bits
Keyspace	NA	2^{22}	2^{24}	2^{90}
Key parameters	NA	$\lambda = 4 - 2^{-7}$ $x_0 = 0.5$	$\lambda = 4 - 2^{-8}$ $x_0 = 0.5$	$\lambda = 4 - 2^{-41}$ $x_0 = 0.5 + 2^{-13}$
Image				
Vertical correlation	0.9693	0.6565	0.8988	0.0037
Horizontal correlation	0.9400	0.6482	0.0043	0.00073799
Diagonal correlation	0.9276	0.5858	−0.0027	−0.0051
Histogram y-axis: observed count. x-axis: color intensity				
Entropy	NA	7.8737	7.9823	7.9973
MAE	NA	41.3697	68.8534	77.8117

Table 6: Synthesis results of the 45-bit stream cipher system.

Resource	Stream cipher system	Stream cipher system with HDMI
Slice Registers (28800)	45	278
Slice LUTs (28800)	326	936
DSP48Es (48)	20	20
Maximum clock frequency	43.530 MHz	43.513 MHz


(a)

(b)

Figure 21: Standalone image encryption system. (a) Decrypted image. (b) Encrypted image.

$(x(i,j)$ and $y(i,j))$ are two adjacent pixels. For highly secured image ρ must be very close to zero.

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{j=1}^{N}x_j\right)\left(y_i-\frac{1}{N}\sum_{j=1}^{N}y_j\right), \quad (6a)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{j=1}^{N}x_j\right)^2, \quad (6b)$$

$$\rho=\frac{\operatorname{cov}(x,y)}{\sqrt{(D(x))}\sqrt{(D(y))}}. \quad (6c)$$

The histogram analysis is used to observe the distribution of the pixel's color intensity. For highly secured image the observed count for each of 2^8 color levels must be the same over the entire image.

The entropy of the ciphered image is calculated using (7) where $p(s_i)$ is the probability of symbol s_i. $p(s_i)$ is computed by dividing the observed count of s_i in the ciphered image by the size of the image. For highly secured image the entropy must be close to 8.

$$\text{Entropy}=-\sum_{i=1}^{2^8}p(s_i)\log_2 p(s_i), \quad (7)$$

The Mean Absolute Error (MAE) between the original image P and the ciphered image C is calculated using (8), where i and j are the pixel indices and M and N are the width and height of the image, respectively.

$$\text{MAE}=\frac{1}{M\times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left|P(i,j)-C_1(i,j)\right|. \quad (8)$$

The encryption analysis in Table 5 shows poor results for the 11-bit bus size. Fortunately, as the bus size increases, ρ coefficient approaches 0, the pixels' intensity distribution becomes flat, entropy approaches 8, and MAE increases. The best encryption result is achieved by setting the bus size to 45 bits which is identified previously in the NIST analysis.

Table 6 shows synthesis results of the 45-bit stream cipher system in addition to standalone encryption system that displays the encrypted and decrypted image on a screen through an HDMI connector. The "Lena" image is stored in the internal RAM of the FPGA. Figure 21 shows the proposed standalone image encryption system.

The proposed stream cipher system, with 8-bit up to 27-bit bus size, was acceptable in the text encryption application due to the small amount of input data. However the NIST and image encryption analysis have showed that it is necessary to extend the bus size to 45 bits in order to successfully encrypt large amount of data. The performance can be further enhanced through feedback, delay elements, nonlinear blocks, and permutation stages as well as postprocessing techniques to get better results for security and sensitivity analyses.

6. Conclusions

In this paper, a methodology for fixed-point simulation of the generalized one-dimensional logistic map with signed parameter and an equivalent hardware realization were presented. Criteria for choosing the bus size for digitally implemented chaotic systems and specifying the number of integer bits were suggested. Various numerical simulations for the properties of the finite precision map over the available precisions, orders of execution, parameter, and initial point were carried out in comparison with those obtained through mathematically analyzing the map over the infinite real field. These factors were shown to affect several properties including the following: the bifurcation diagram, its key-points, periodicity of the generated sequence, and maximum Lyapunov exponent for positive and negative control parameter cases. Moreover, a hardware realization of a stream cipher system for text and image encryption applications based on the conventional logistic map as a Pseudo-Random Number Generator was presented. Encryption results show the trade-off between security level, on the one hand, and speed and hardware resources on the other hand. The longer period lengths provided by mostly positive map suggest its use as one remedy for the problem of short cycles of finite precision chaotic maps compared with other PRNGs. It can be an additional enhancement beside using higher finite precisions, cascading multiple chaotic systems, and using perturbation based systems for either the control parameter or the iterated variable with different configurations. Scaling factors can further provide wider output ranges and hence increase period lengths. Moreover, we recommend that future implementations of chaotic systems on digital platforms consider the listed factors and their effects on various properties and then provide their implementation details for reproducibility. For example, we have shown that different orders of execution and parameter values yield different period lengths. For finite precision systems, we do not guarantee that $\lambda = 4$ or which order of execution yields the longest period. Hence, the different alternatives need to be considered similar to how initial conditions effect is considered. The procedure presented in this paper can be carried out for other generalized versions of the logistic map and other chaotic systems according to the allowed ranges of different parameters in order to study the impact of finite precision fixed-point implementation on their properties.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physical Review Letters*, vol. 71, no. 1, pp. 65–68, 1993.

[2] S. Mandal and S. Banerjee, "Analysis and CMOS implementation of a chaos-based communication system," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1708–1722, 2004.

[3] A. Radwan, A. Soliman, and A. S. Elwakil, "1-D digitally-controlled multiscroll chaos generator," *International Journal of Bifurcation and Chaos*, vol. 17, no. 1, pp. 227–242, 2007.

[4] M. A. Zidan, A. G. Radwan, and K. N. Salama, "Controllable V-shape multiscroll butterfly attractor: system and circuit implementation," *International Journal of Bifurcation and Chaos*, vol. 22, no. 6, Article ID 1250143, 2012.

[5] S. K. Abd-El-Hafiz, A. G. Radwan, and S. H. AbdEl-Haleem, "Encryption applications of a generalized chaotic map," *Applied Mathematics & Information Sciences*, vol. 9, no. 6, pp. 3215–3233, 2015.

[6] W. S. Sayed, A. G. Radwan, and H. A. H. Fahmy, "Design of positive, negative, and alternating sign generalized logistic maps," *Discrete Dynamics in Nature and Society*, vol. 2015, Article ID 586783, 23 pages, 2015.

[7] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos—An Introduction to Dynamical Systems*, Textbooks in Mathematical Sciences, Springer-Verlag, New York, NY, USA, 1997.

[8] E. Schöll, *Nonlinear Spatio-Temporal Dynamics and Chaos in Semiconductors*, vol. 10, Cambridge University Press, 2001.

[9] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, Westview Press, 2014.

[10] R. K. Upadhyay and P. Roy, "Disease spread and its effect on population dynamics in heterogeneous environment," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 26, no. 1, Article ID 1650004, 27 pages, 2016.

[11] L. Liu and S. Miao, "The complexity of binary sequences using logistic chaotic maps," *Complexity*, vol. 21, no. 6, pp. 121–129, 2016.

[12] S. C. Phatak and S. S. Rao, "Logistic map: a possible random-number generator," *Physical Review E*, vol. 51, no. 4, pp. 3670–3678, 1995.

[13] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," *Physics Letters A*, vol. 289, no. 4-5, pp. 199–206, 2001.

[14] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[15] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.

[16] V. Patidar, K. K. Sud, and N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, no. 4, pp. 441–452, 2009.

[17] N. Singh and A. Sinha, "Chaos-based secure communication system using logistic map," *Optics and Lasers in Engineering*, vol. 48, no. 3, pp. 398–404, 2010.

[18] Y. Liu, H. Fan, E. Y. Xie, G. Cheng, and C. Li, "Deciphering an image cipher based on mixed transformed logistic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 25, no. 13, Article ID 1550188, 9 pages, 2015.

[19] D. A. Hsieh, "Chaos and nonlinear dynamics: application to financial markets," *The Journal of Finance*, vol. 46, no. 5, pp. 1839–1877, 1991.

[20] N. Basalto, R. Bellotti, F. De Carlo, P. Facchi, and S. Pascazio, "Clustering stock market companies via chaotic map synchronization," *Physica A: Statistical Mechanics and Its Applications*, vol. 345, no. 1-2, pp. 196–206, 2005.

[21] R. Bowen and J. Chazottes, *Equilibrium States and the Ergodic Theory of Anosov Diffeomorphisms*, vol. 470, Springer, 1975.

[22] P. H. Borcherds and G. P. McCauley, "The digital tent map and the trapezoidal map," *Chaos, Solitons & Fractals*, vol. 3, no. 4, pp. 451–466, 1993.

[23] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "The digital tent map: performance analysis and optimized design as a low-complexity source of pseudorandom bits," *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 5, pp. 1451–1458, 2006.

[24] R. M. Corless, “What good are numerical simulations of chaotic dynamical systems?” *Computers & Mathematics with Applications*, vol. 28, no. 10–12, pp. 107–121, 1994.

[25] S. Li, G. Chen, and X. Mou, “On the dynamical degradation of digital piecewise linear chaotic maps,” *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[26] K. J. Persohn and R. J. Povinelli, “Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation,” *Chaos, Solitons & Fractals*, vol. 45, no. 3, pp. 238–245, 2012.

[27] A. S. Mansingka, A. G. Radwan, M. A. Zidan, and K. N. Salama, “Analysis of bus width and delay on a fully digital signum nonlinearity chaotic oscillator,” in *Proceedings of the 54th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS ’11)*, pp. 1–4, IEEE, Seoul, Republic of Korea, August 2011.

[28] A. S. Mansingka, M. Affan Zidan, M. L. Barakat, A. G. Radwan, and K. N. Salama, “Fully digital jerk-based chaotic oscillators for high throughput pseudo-random number generators up to 8.77 Gbits/s,” *Microelectronics Journal*, vol. 44, no. 9, pp. 744–752, 2013.

[29] İ. Öztürk and R. Kiliç, “Cycle lengths and correlation properties of finite precision chaotic maps,” *International Journal of Bifurcation and Chaos*, vol. 24, no. 9, Article ID 1450107, 14 pages, 2014.

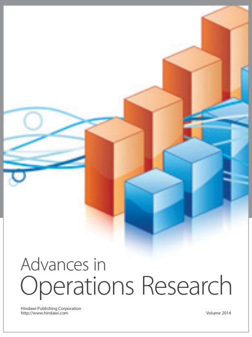
[30] H. Wang, B. Song, Q. Liu, J. Pan, and Q. Ding, “FPGA design and applicable analysis of discrete chaotic maps,” *International Journal of Bifurcation and Chaos*, vol. 24, no. 4, Article ID 1450054, 2014.

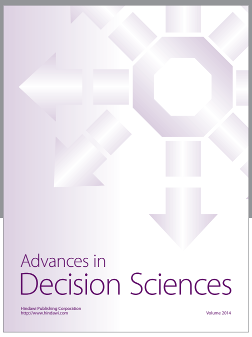
[31] E. W. Weisstein, Logistic map. From MathWorld-A Wolfram Web Resource, 2014, http://mathworld.wolfram.com/Logistic-Map.html.

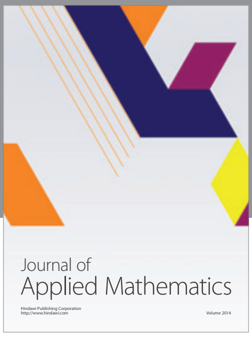
[32] M. Perc, “User friendly programs for nonlinear time series analysis,” 2010, http://www.matjazperc.com/ejp/time.html.

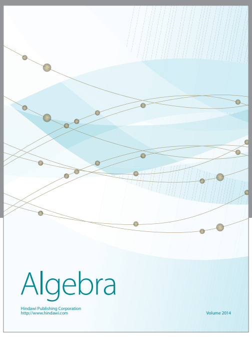
[33] https://en.wikiquote.org/wiki/Mahatma_Gandhi.

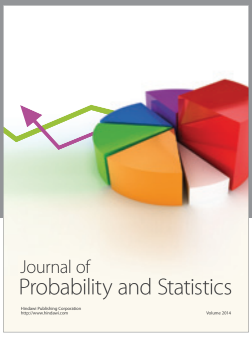
[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Tech. Rep., DTIC Document, 2001.


Advances in
Operations Research

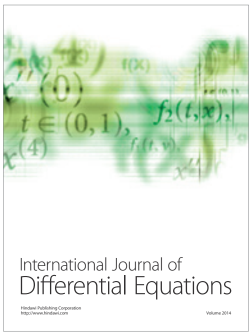

Advances in
Decision Sciences


Journal of
Applied Mathematics

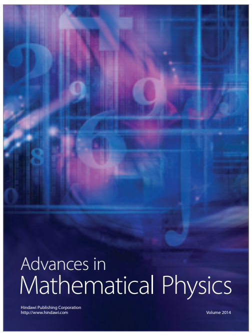

Algebra

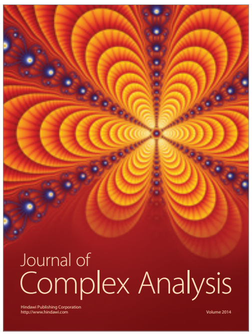

Journal of
Probability and Statistics

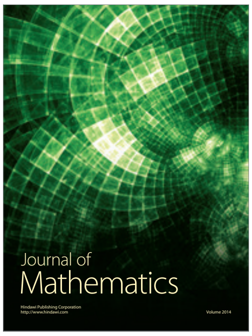
The Scientific
World Journal

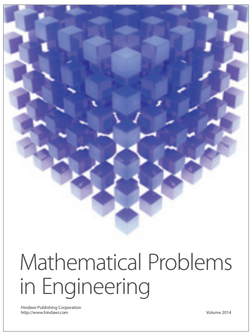

International Journal of
Differential Equations

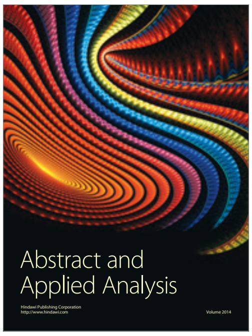
International Journal of
Combinatorics

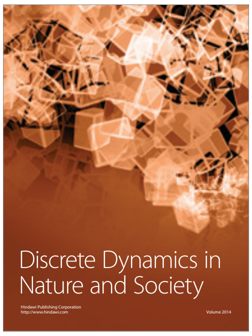

Advances in
Mathematical Physics

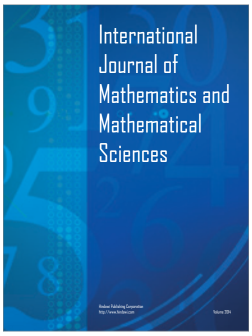

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

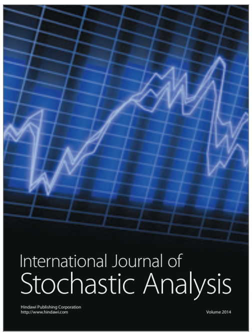

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization