Journal of Software Engineering and Applications, 2015, 8, 635-659
Published Online December 2015 in SciRes. http://www.scirp.org/journal/jsea
http://dx.doi.org/10.4236/jsea.2015.812059

A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map

Mahmoud Maqableh

Management Information Systems, Faculty of Business, The University of Jordan, Amman, Jordan
Email: maqableh@ju.edu.jo

Received 27 November 2015; accepted 28 December 2015; published 31 December 2015

Abstract

Chaos theory attempts to explain the result of a system that is sensitive to initial conditions, complex, and shows an unpredictable behaviour. Chaotic systems are sensitive to any change or changes in the initial condition(s) and are unpredictable in the long term. Chaos theory are implementing today in many different fields of studies. In this research, we propose a new one-dimensional Triangular Chaotic Map (TCM) with full intensive chaotic population. TCM chaotic map is a one-way function that prevents the finding of a relationship between the successive output values and increases the randomness of output results. The tests and analysis results of the proposed triangular chaotic map show a great sensitivity to initial conditions, have unpredictability, are uniformly distributed and random-like and have an infinite range of intensive chaotic population with large positive Lyapunov exponent values. Moreover, TCM characteristics are very promising for possible utilization in many different study fields.

Keywords

Chaos, Chaotic Maps, Triangular Chaotic Map, Logistic Map, Lyapunov Exponent

1. Introduction

Over the last few years, many researchers have studied chaos theory in several fields, such as electronic systems, fluid dynamics, lasers, weather and climate [1]-[5]. Chaos theory is implementing today in many different fields of studies such as: engineering, computer science, mathematics, physics, geology, microbiology, biology, economics, finance, algorithmic trading, meteorology, philosophy, politics, population dynamics, psychology, and robotics [6]. Moreover, Chaos theory has attracted the cryptography field due to its characteristics, such as its

How to cite this paper: Maqableh, M. (2015) A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map. *Journal of Software Engineering and Applications*, **8**, 635-659.
http://dx.doi.org/10.4236/jsea.2015.812059

deterministic nature, unpredictability, random-look nature and its sensitivity to initial value [7].

Cryptographers have utilized dynamic chaotic maps to develop new cryptographic primitives by exploiting chaotic maps, such as logistic maps, Henon maps, and Tent maps. There are similarities and differences between cryptography algorithms and chaotic maps [8]. The parameters in chaotic maps are meaningful, if they are real numbers, which can be used in the cryptographic algorithms as encryption and decryption keys. Chaotic systems are sensitive to any change or changes in the initial condition(s) and are unpredictable in the long term, thus representing the diffusion in cryptographic encryption algorithms. Iterations of a chaotic map lead to the spreading of the initial region over the entire phase space, and this can be achieved in cryptographic algorithms by designing the algorithm based on rounds. The main difference between chaos and cryptography is that encryption transformations are defined on finite sets, whereas chaos has meaning only in real numbers.

Since 1990, many studies on digital chaotic cryptography have been proposed to provide secure communications based on chaotic maps including chaotic block ciphers [9]-[34], chaotic cryptography hash functions [7] [31] [35]-[49], and chaotic pseudorandom number generators [11] [50]-[65]. In general, chaos theory has been proved a secure algorithm against known cryptanalysis techniques. Recently, various studies have been conducted on chaotic cryptographic algorithms [7] [66]-[87]. Some of the proposed chaotic cryptographic algorithms that have been analysed have had weak internal designs and incorrect exploitation of chaotic maps. In this research, we propose novel triangular chaotic map.

The rest of this research paper is organized as follows. Section 2 introduces chaos theory. The details of chaotic maps are discussed in Section 3. Section 4 describes details of Logistic map and Lyapunov exponent. In Section 5, details of the new Triangular Chaotic map are given. Finally, the conclusion is given in Section 6.

2. Chaos Theory

Chaos is derived from a Greek word "Χαος", meaning a state without order or predictability [2]. A chaotic system is a simple, non-linear, dynamical, and deterministic system that shows completely unpredictable behaviour and appears random [88]. Moreover, it is a deterministic system with great sensitivity to initial conditions, such that a computer system can give an amazingly different result when the value of an input parameter is changed. On the other hand, in classical science small changes in an initial value might generate small differences in the result [89] [90]. A system is called a chaotic system if it is sensitive to initial conditions, topology mix, and if periodic orbits are dense.

According to Alligood *et al*. (1996), a dynamical system contains all the possible states and regulations that control the next state from the current state. On the other hand, the deterministic regulations are those that determine the current state uniquely from the previous states, whereas there is always a mathematical equation to determine the system evolution [91]. From the previous definitions of deterministic and dynamical systems, we cannot say that the randomness is not allowed. The bifurcation in dynamic differential equation changes the number of solutions as the parameters is changed [92].

In 1890, Poincaré published his article [89] (on the equations of the dynamics and the three-body problem) of 270 pages, which simplified the way of looking at the complicated continuous trajectories from differential equations [2]. Then, in 1898, Hadamard observed the sensitivity to initial conditions and unpredictability of special systems, calling this the geodesic flow [2]. Later, in 1908, Poincaré noted that chaos sensitivity depends on initial conditions and gives unpredictable results [90] [93]. Later on, Edward Lorenz (1963) examined chaos theory and described a simple mathematical model of weather prediction [91]. Lorenz's model was the first numerical model to detect chaos in a non-linear dynamical system [3] [94]. Lorenz's findings were very interesting in that some equations rise to some surprisingly complex behaviour and chaos behaviour dependent on the initial condition [2]. In 1975, Li and Yorke were the first to introduce the word 'chaos' into mathematical literature, where system results appear random [1]-[5] [95] [96].

Chaotic maps have been the subject of an extremely active research area due to their characteristics, such as sensitivity to the initial value, complex behaviour, and completely deterministic nature. The chaotic behaviour can be observed in many different systems, such as electronic systems, fluid dynamics, lasers, weather, climate and economics [2] [88] [89] [97]. Our intuition tells us that a small change in input parameters should give a small change in output, but chaotic systems show us that this is not necessarily the case. Usually, chaotic maps define infinitely large fields of real numbers. The most important characteristics of chaotic systems are as follows:

1. Apparently random behaviour but completely deterministic: The behaviour of chaotic systems seems to be random but actually it is purely deterministic. Hence, if we run the chaotic system many times with the same initial value, we will obtain the same set of output values. Furthermore, the chaotic systems are dynamical systems that are described by differential equations or iterative mappings, and the next state is specified from the previous state (see Equation 3-1 [5] [98] [99]).

$$\frac{\mathrm{d}}{\mathrm{d}t}x_i = F_i\left(x_1,\cdots,x_n\right) \quad i=1,2,\cdots,n \tag{1}$$

2. Sensitivity dependence on the initial conditions (The state from which the system starts): Dynamical systems evolve completely differently over time with slight changes in the initial state [88] [90].

3. Unpredictable (difficult or impossible to predict the behaviour in the long term): In chaotic maps, even if one knows the current state of the chaotic system it is useless trying to predict the next state of the system. In other words, it is very difficult to predict the future states of the chaotic system in the long term [89] [100].

3. Chaotic Maps

According to Alligood *et al*. (1996), a chaotic map is a function of its domain and range in the same space, and the starting point of the trajectory is called the initial value (condition) [101]. Chaotic dynamics have a unique attribute that can be seen clearly by imagining the system starting twice with slightly different initial conditions [102]. Chaos theory attempts to explain the result of a system that is sensitive to initial conditions, complex, and shows unpredictable behaviour. Chaotic dynamical systems increase communication security with higher dimensions and more than one positive Lyapunov exponent [91]. A Lyapunov exponent is used to help select the initial parameters of chaotic maps that fall in chaotic areas. A chaotic system exhibits some chaotic behaviour and often occurs in the study of dynamical systems. In the following subsections, we will give a brief induction to some chaotic systems: Logistic map, Lorenz attractors, Rossler attractors, Henon map, Tent map, and Piecewise linear chaotic map.

3.1. Logistic Map

In 1845, Pierre Verhulst proposed a logistic map, which is a simple non-linear dynamical map. A logistic map is one of the most popular and simplest chaotic maps [103]. Logistic maps became very popular after they were exploited in 1979 by the biologist Robert M. May [89]. The logistic map is a polynomial mapping, a complex chaotic system, the behaviour of which can arise from very simple non-linear dynamical equations, as shown in **Figure 1** [104]. The logistic map equation is written as:

$$g\left(x_n\right) = x_{n+1} = r \times x_n \times \left(1 - x_n\right) \tag{2}$$

where x_n is a number between zero and one, x_0 represents the initial population, and r is a positive number between zero and four.

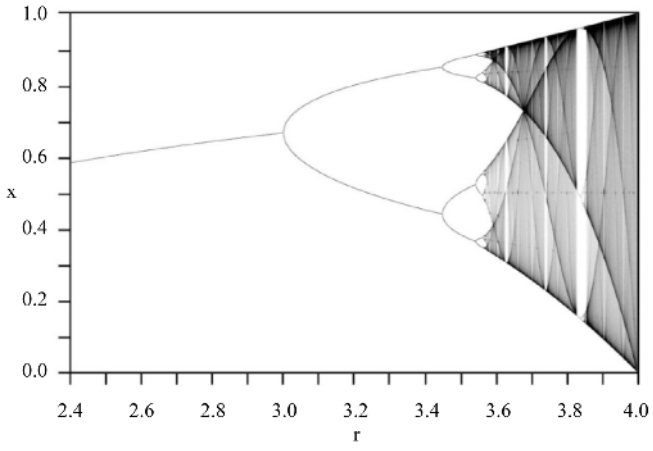

Figure 1. Bifurcation diagram of the Logistic map [105].

The logistic map is one of the simplest chaotic maps; it is highly sensitive to change in its parameter value, where a different value of the parameter r will give a different map f [89]. Its transformation function is F: $[0,1] \to [0,1]$ which is defined in the above equation. From the onset of chaos, a seemingly random jumble of dots, the behaviour of the logistic map depends mainly on the values of two variables (r, x_0); by changing one or both variables' values we can observe different logistic map behaviours. The population of a logistic map will die out if the value of r is between 0 and 1, and the population will be quickly stabilized on the value $(1-r)/r$ if the value of r is between 1 and 3 [89]. Then, the population will oscillate between two values if the value of parameter r is between 3 and 3.45. After that, with values of parameter r between 3.45 and 4 the periodic fluctuation becomes significantly more complicated. Finally, most of the values after 3.57 show chaotic behaviour.

In the logistic map $g(x_n) = r \times x_n \times (1-x_n)$, the function result depends on the value of parameter r, where different values of r will give quite different pictures. We can note that $g(x_1) = x_2$ and $g(x_2) = x_1$, that mean $g(g(x_1)) = x_2$ and $g(g(x_2)) = x_1$. According to Alligood *et al*. (1996) the periodic fluctuation between x_1, x_2 is steady and attracts orbits (trajectories). Therefore, there are a minimum number of iterations of the orbit to repeat the point. There are obvious differences between the behaviour of the exponential model and the logistic model's behaviour. To show the difference between the two functions, we take an example of the exponential function $f(x_{n+1}) = 2x_n$ and an example of logistic function $g(x_{n+1}) = 4x_n(1-x_n)$; the initial value for both functions is 0.0090, and we then calculate the population for n = 0, 1, 2, ⋯, 10 resulting in an accuracy of five decimal places. We can notice that the output values of the exponential function are always increasing as time progresses, while the output values of the logistic function are fluctuating with a finite limited size between zero and one [88] [89] [93].

3.2. Lorenz Attractor

The Lorenz attractor is one of the most popular three-dimensional chaotic attractors; it was examined and introduced by Edward Lorenz in 1963 [2]. He showed that a small change in the initial conditions of a weather model could give large differences in the resulting weather. This means that a slight difference in the initial condition will affect the output of the whole system, which is called sensitive dependence to the initial conditions. The non-linear dynamical system is sensitive to the initial value and is related to the system's periodic behaviour [90]. Lorenz's dynamic system presents a chaotic attractor, whereas the word chaos is often used to describe the complicated manner of non-linear dynamical systems [106]. Chaos theory generates apparently random behaviour but at the same time is completely deterministic, as shown in **Figure 2**. The Lorenz attractor is defined as follows:

$$\begin{aligned} dx/dt &= a*(y-x) \\ dy/dt &= r*x - y - x*z \\ dz/dt &= x*y - b*z \end{aligned} \tag{3}$$

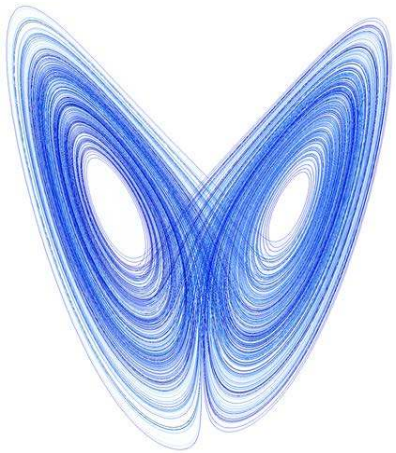

Figure 2. A plot of the trajectory of the Lorenz system, (modified from [107])

3.3. Rossler Attractors

In 1976 [88] [89], O. Rossler created a chaotic attractor with a simple set of non-linear differential equations [88]. Rossler attempted to write the simplest dynamical system that exhibited the characteristics of a chaotic system [89] [108]. The Rossler attractor was the first widely-known chaotic attractor from a set of differential equations; defined by a set of three non-linear differential equations, the system exhibits a strange attractor for $a = b = 0.2$ and $c = 5.7$ (see Equation (4)) [108]. The Rossler attractor is a rather nice but not famous attractor, which draws a nifty picture of a non-linear three-dimensional deterministic dynamical system, as shown in **Figure 3**.

$$\begin{aligned} \mathrm{d}x/\mathrm{d}t &= -y - z \\ \mathrm{d}y/\mathrm{d}t &= x + Ay \\ \mathrm{d}z/\mathrm{d}t &= B + xz - Cz \end{aligned} \tag{4}$$

A, B, and C are constants.

3.4. Henon Attractors

The Henon map is one of the dynamical systems that exhibit chaotic behaviours. The Henon map is defined by two equations; the map depends on two parameters a, b, and the system exhibits a strange attractor for $a = 1.4$ and $b = 0.3$ (see Equation (5)). A Henon map takes one point (x, y) and maps this point to a new point in the plane, as shown in **Figure 4** [108].

$$\begin{aligned} x_{n+1} &= y_n + 1 - ax_n^2 \\ y_{n+1} &= bx_n \end{aligned} \tag{5}$$

3.5. Tent Map

A Tent map is an iterated function of a dynamical system that exhibits chaotic behaviours (orbits) and is governed by Equation (6). It has a similar shape to the logistic map shape with a corner (**Figure 5** and **Figure 6**)

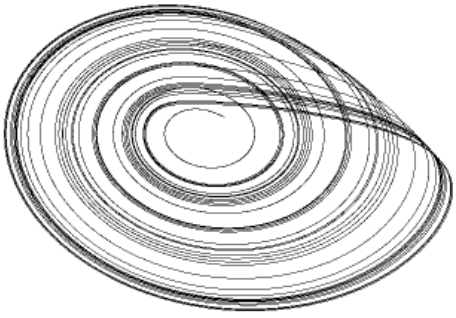

Figure 3. Rossler attractor [89].

Figure 4. Henon attractor for $a = 1.4$ and $b = 0.3$ [89].

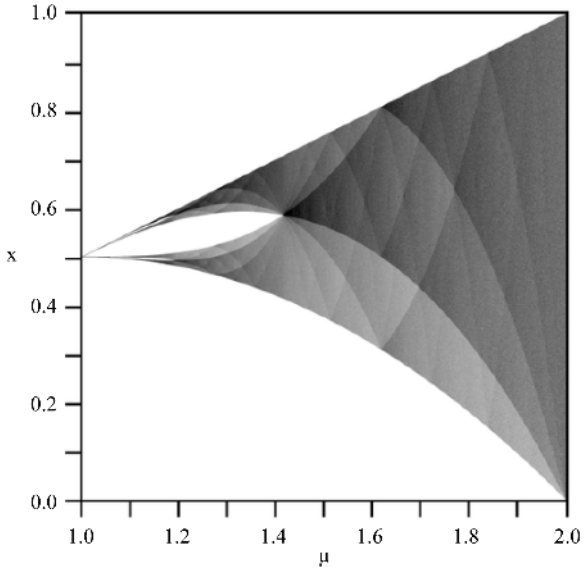

Figure 5. Bifurcation diagram for the tent map [110].

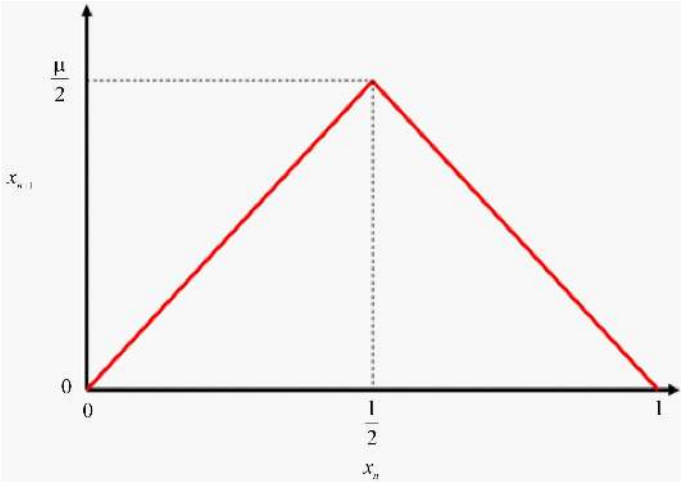

Figure 6. Graph of tent map function.

[109]. The Tent map exhibits the Lyapunov exponents on the unit interval $T(x) \in [0,1]$ and $\mu \in [0,2]$. It is a simple one-dimensional map generating periodic chaotic behaviour similar to a logistic map.

$$T_\mu(x) = \begin{cases} \mu x, & x \le 1/2 \\ \mu(1-x), & 1/2 \le x \end{cases} \tag{6}$$

3.6. Piecewise Linear Chaotic Maps

Piecewise linear chaotic maps (PWLCMs) are simple non-linear dynamical systems with large positive Lyapunov exponents. In [111], they are shown to have several brilliant chaotic properties that can be exploited in chaotic cryptographic algorithms. PWLCM has perfect behaviour and high dynamical properties such as invariant distribution, auto-correlation function, periodicity, large positive Lyapunov exponent, and mixing property [112]. Iterations of PWLCM with initial value and control parameters generate a sequence of real numbers between 0 and 1, which is called an orbit. A large positive Lyapunov exponent means that the system shows chaotic behaviour over large orbits [110]. The periodicity property indicates that the system behaviour is average over time and space. Correlation functions are a very important test of the correlation over time and space be-

tween random variables at two different points, thus indicating correlation statistical properties [2].

PWLCMs are the simplest kind of chaotic systems, which need one division and few additions. A skew Tent map is a PWLCM defined by a generalized form of Tent map that is very similar to a Tent map with small differences (see Equation (7)). A more complex example of PWLCMs is defined by Equation (8). It is very clear from Equation (8) that $f(0, p) = 0$, $f_2(0.5, p) = 0$, $f_3(1, p) = 0$ for any $P \in (0, 0.5)$. Thus, we should avoid those values as initial parameters of x_n.

$$x_{n+1} = f(x_n, p) = \begin{cases} x_n / p, & x_n \in [0, p) \\ (1 - x_n)/(1 - p), & x_n \in [p, 1] \end{cases} \tag{7}$$

$$x_{n+1} = f(x_n, p) = \begin{cases} x_n / p, & x_n \in [0, p) \\ (x_n - p)/(0.5 - p), & x_n \in (p, 0.5] \\ f(1 - x_n, P), & x_n \in [0.5, 1] \end{cases} \tag{8}$$

where x_0 is the initial condition value, P is the control parameter, $x_n \in [0, 1]$, and $P \in (0, 0.5)$.

4. Logistic map and Lyapunov Exponent

Chaos theory is a simple non-linear dynamical system that shows completely unpredictable behaviour [88]. A chaotic system is a deterministic system with great sensitivity to initial conditions that can give amazingly different results on a computer when one or both input parameters' values are changed. In contrast, small changes in the initial value of classical science equations tend to generate small differences in the result [7]. Chaotic maps have been an active research area due to their characteristics such as deterministic nature, unpredictability, random-look nature, and sensitivity to initial value [7] [11] [19] [34] [52] [53] [55] [113]-[123]. In the last decade, researchers have noticed a relationship between chaos theory and cryptography. Chaotic systems' properties are analogous to some cryptography systems' properties; for example, sensitivity to initial conditions is analogous to diffusion, iterations are analogous to rounds in encryption systems, and chaotic system complexity is analogous to complexity of cryptography algorithms. Cryptographers have utilized dynamical chaotic maps to develop new security primitives by exploiting some chaotic maps [89] [100]. Some of the well-known chaotic maps are Logistic map, Tent map and Henon map.

A Lyapunov number is the divergence rate average of very close points along an orbit and it is the natural algorithm of the Lyapunov exponent (see Equation (9) [91]). Therefore, the Lyapunov exponent is used with chaotic behaviour to measure the sensitivity dependence on the initial condition [88]. This means that, in one-dimensional chaos maps, the Lyapunov numbers are used to measure separation rates of nearby points along the real line. The Lyapunov exponent is used to help in choosing the initial parameters of chaotic maps that fall in chaotic areas. The Lyapunov exponent has three different cases of dynamics as follows [89]:

1. If all Lyapunov exponents are less than zero, there is a fixed point behaving like an attractor.
2. If some of the Lyapunov exponents are zero and others are less than zero, there is an ordinary attractor, which is simpler than a fixed point.
3. If at least one of the Lyapunov exponents is positive, the dynamical system is not stable (chaotic) and vice versa.

$$h(x_1) = \lim_{n \to \infty} (1/n) \left[\ln \left| f'(x_1) \right| + \cdots + \ln \left| f'(x_n) \right| \right] \tag{9}$$

A logistic map shows a chaotic behaviour that can arise from very simple non-linear dynamical equations (see **Figure 7** [124]). Logistic map behaviour seems to be a random jumble of dots and mainly depends on two parameters (x_0 and r). We can observe different logistic map behaviours by changing the value(s) of one or both of these parameters. The general idea of a logistic map was built based on an iterations function, where the next output value depends on the previous output value (see Equation (1)). **Figure 8** shows the calculated Lyapunov exponent value of a logistic map with different values of parameter $r \in [0, 4]$. In a logistic map equation, x_0 and r represent the initial conditions, $x_0 \in [0, 1]$ and $r \in [0, 4]$. Chaotic behaviour is exhibited with $3.57 > r \geq 4$, but it shows non-chaotic behaviour with some values of parameter r (see **Figure 9** and **Figure 10**). In this section, we refer to x_0 and r parameters as the initial conditions of a logistic map.

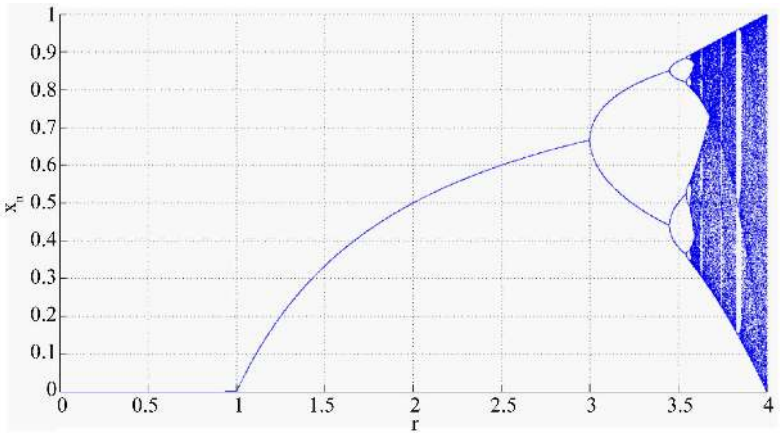

Figure 7. Bifurcation diagram of logistic map.

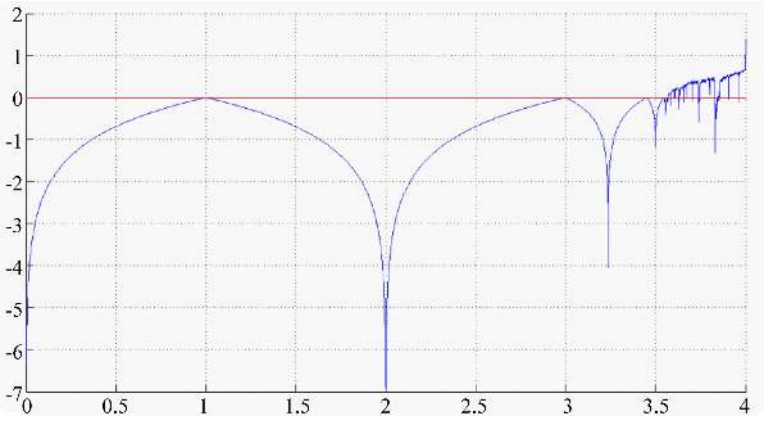

Figure 8. Lyapunov exponent of Logistic map with $t \in [0, 4]$.

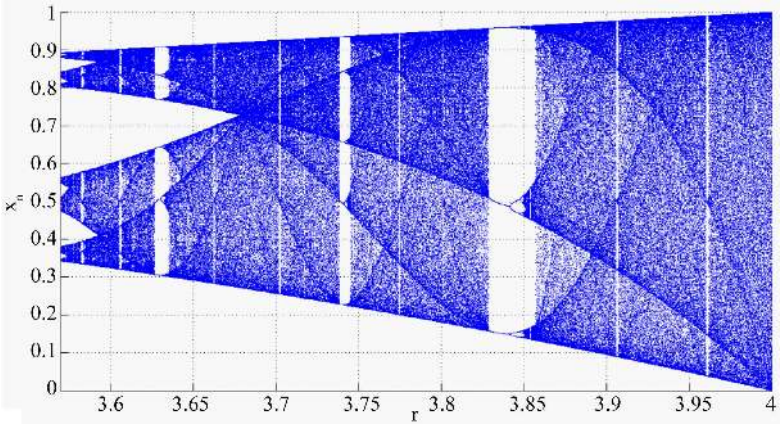

Figure 9. Logistic map bifurcation diagram of a periodic window.

A small range of logistic map parameters are consider as valid values to show chaotic behaviour [69]. In general, chaotic behaviour is exhibited with values of parameter r greater than 3.57 and less than or equal to 4. It is very clear from **Figure 9** that the logistic map periodic window becomes significantly complicated with $3.57 > r \geq 4$. In **Figure 9** and **Figure 10**, we plotted a portion of logistic map bifurcation and its Lyapunov exponent, respectively, using MATLAB software, to give a clear picture of the chaotic areas. There are non-chaotic areas with some values of parameter r over the chaotic interval, which are called stability or islands. It is very clear

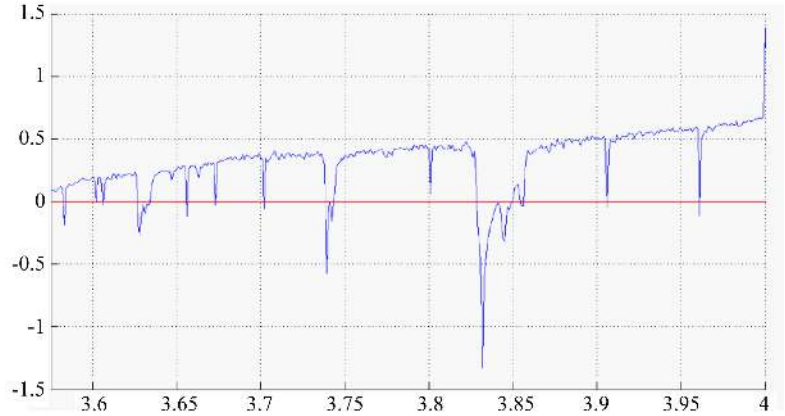

Figure 10. Lyapunov exponent of Logistic map with $t \in [3.575, 4]$.

that there is a 3-periodic window between 3.828429 and 3.841037 [69]. The value of $r = 3.840$ falls in the 3-periodic window and the value of $r = 3.845$ fall in the 6-periodic window. Therefore, after a small number of iterations with different initial values of x, (x_0) will end up in one of these periodic. The cryptosystems fall within the 3-perodic and the 6-periodic windows with $r = 3.840$ and 3.845, respectively, and were utilized for the purpose of attacking them [125]. Moreover, the logistic map population will cover the full interval of x, ([0,1]), only with $r = 4$.

5. Novel Triangular Chaotic Map (TCM)

In this section, a novel Triangular Chaotic map (TCM) is proposed. TCM is a one-dimensional chaotic map of degree two with full chaotic population over infinite interval of parameter t values (see Equation (10)). The Triangular Chaotic Map behaviour mainly depends on the initial values of parameters y_0 and t. TCM behaviour seems to be a random jumble of dots, and depends on initial conditions (y_0 and t). The y_0, y_n are positive real numbers between 0 and 1, $y_n \in [0, 1]$, and t can be any positive real number $t \in [0, \infty]$. **Figure 11** shows a TCM map bifurcation diagram and Figure 11 shows the calculated Lyapunov exponent value over $r \in [0, 4]$. It is very clear from the figures that TCM shows perfect chaotic behaviour over the full interval. **Figure 12** shows a TCM diagram with initial value of t very close to zero and random number of y_0, iterating TCM map many times, and then plotting the t series of values of y_n using MATLAB software. In other words, we plotted corresponding points of y_n to a given value of t and increased t to the right. TCM is very sensitive to any change(s) in one or both initial conditions and is unpredictable in the long term, as shown in **Figure 11** and **Figure 12**. In this paper, we refer to y_0 and t parameters as the initial conditions of TCM map.

$$f(y_n) = y_{n+1} = \begin{cases} \left(t \times y_n \times \left(1 - y_n\right)\right) \% 1 & n \% 2 = 0 \\ \left(\pi \times y_n \times \beta\right) \% 1 & n \% 2 ! = 0 \end{cases} \tag{10}$$

where y_n is a number between zero and one, y_0 represents the initial population, t is a positive real number, n is a number of iterations, β: is a positive odd number between 3 and 99.

The general idea of a TCM map was built based on an iteration function. The result of the next output value (y_{n+1}) in TCM depends on the previous output value (y_n) (see Equation (3)). A TCM map over a different range of parameter t values will give different f maps. To show TCM sensitivity we plotted the behaviour of three nearby initial values of y_0 and three nearby initial values of t. Three nearby initial values of y_0 (0.990000, 0.990001, and 0.990002) for $t = 1$ started at the same time and rapidly diverged exponentially over time with no correlation between each of them (see **Figure 13**). Moreover, we plotted populations of three slightly different parameter values of t (4.000000, 4.000001, and 4.000002) and $y_0 = 0.5$ to show great sensitivity to initial conditions of the TCM map (see **Figure 14**).

TCM diagram and population distribution histograms have been plotted for population of TCM over the $t \in [32, 36]$. TCM iterated 43686 times with initial conditions values of $t_0 = 32$ and $y_0 = 0.5$. We draw the TCM diagram by plotting corresponding points of y_n to a given value of t and increasing t to the right (see **Figure 15**).

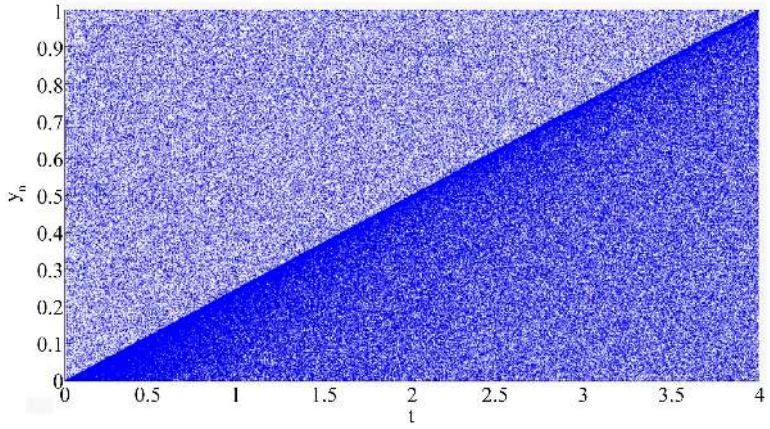

Figure 11. TCM chaotic map bifurcation diagram with $t \in [0, 4]$.

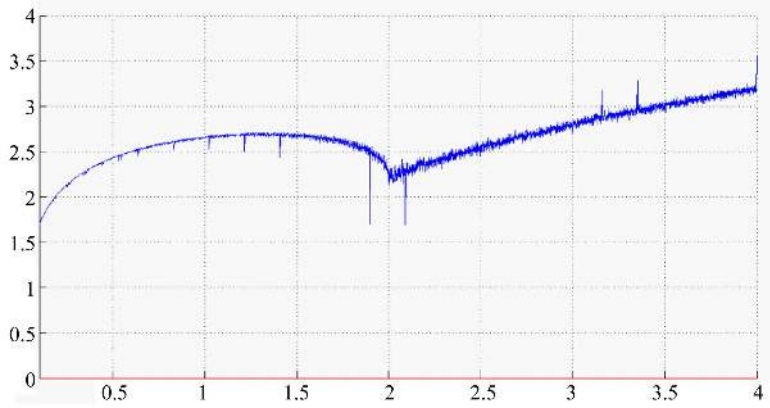

Figure 12. Lyapunov exponent of TCM chaotic map with $t \in [0, 4]$.

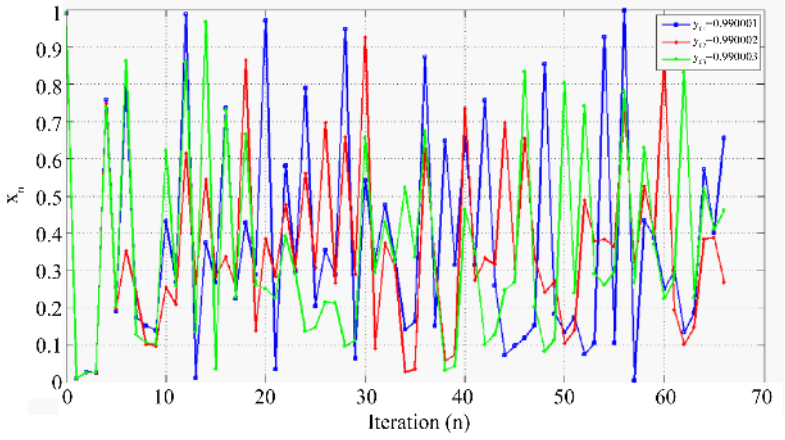

Figure 13. TCM iterations with $t = 1$ and three different initial values of y_0.

TCM population interval, [0, 1], is divided into 10 equal sub-intervals and the number of points in each interval has been counted for each sub-interval and plotted (see **Figure 16**). It is very clear from **Figure 15** and **Figure 16** that TCM population is uniformly distributed over the interval [0, 1] with $t \in [32, 36]$. We draw the TCM diagram and population distribution histogram with different initial t values (0, 4, 8, 12, ⋯ etc.) and the overall results confirm that the TCM population distributions are uniformly distributed with $t \geq 12$ and interval size 4. In conclusion, TCM is a new one-dimensional chaotic map with perfect chaotic behaviour over infinite interval,

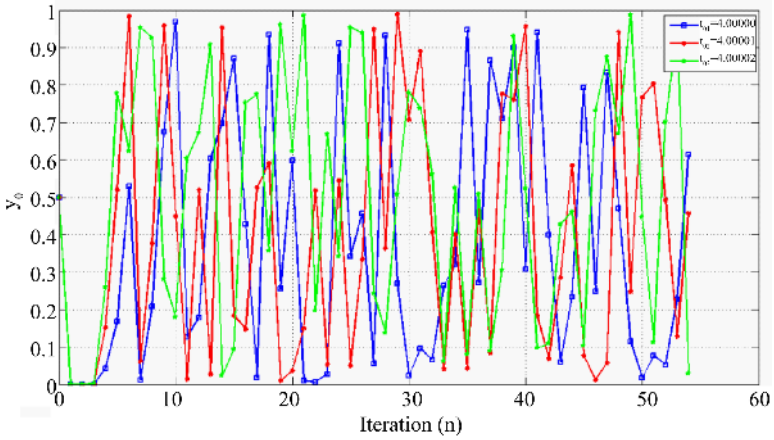

Figure 14. TCM iterations with $y_0 = 0.5$ and three different initial values of t.

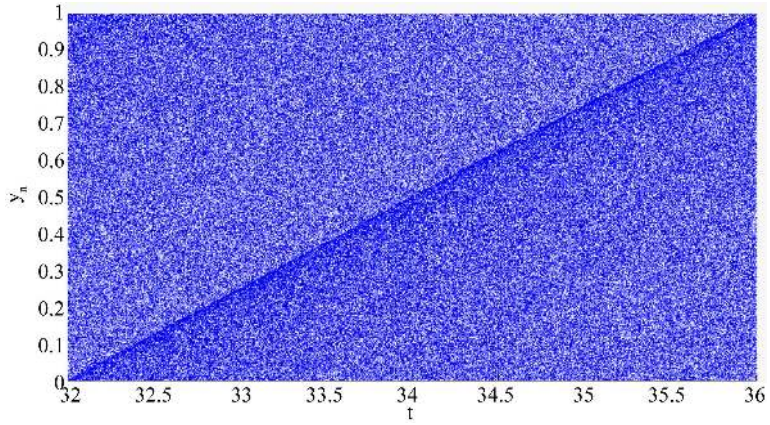

Figure 15. TCM chaotic map bifurcation diagram with $t \in [32, 36]$.

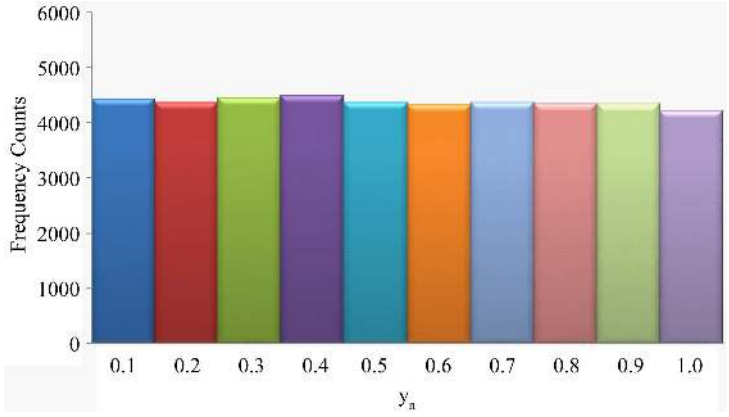

Figure 16. TCM distribution of y_n values over $t \in [32, 36]$.

high positive Lyapunov exponent value, uniform distribution, and great sensitivity to any change(s) in the initial condition or the control parameter.

As we explained earlier, a small range of logistic map parameters are considered valid values to show chaotic behaviour $r > 3.57 \geq 4$. In addition, the logistic map population will cover the full interval of x, $x_n \in [0, 1]$, only with $r = 4$. Therefore, we propose to use a modified version of the logistic map defined in Equation (8). We used the remainder of dividing the logistic map by 1 to ensure that all the output values will be between zero and one,

$x_n \in [0, 1]$, and we added a small real number ($\beta \leq 0.001$) to ensure $x_n \neq 0$ or 1. Consequently, in the modified version the value of parameter r can be any value greater than 0, $r \in [0, \infty]$. We plotted the modified version of logistic map bifurcation and its Lyapunov exponent over different intervals using MATLAB software (see **Figure 17** and **Appendix A**). It is very clear from **Figure 18** that the modified version has bigger intervals of chaotic behaviour and it covers the full x interval over many different values of parameter r. Unfortunately, it still shows non-chaotic areas over different values within the intervals: [0, 4], [4, 8], [8, 12] and [12, 16], which are known as stability or islands. In contrast, the TCM map shows perfect chaotic behaviour and covers the entire range of y for every value of t (see **Figure 18** and **Appendix B**). In other words, in the Triangular Chaotic Map at every value of $f(x)$ there is at least one image value, but in the logistic map and modified logistic map there are no image values.

6. Conclusion

In this research, we propose a new Triangular Chaotic Map (TCM) with high-intensity chaotic areas over infinite interval. The tests and analysis results of the proposed chaotic map show that it has very strong chaotic properties such as very high sensitivity to initial conditions, random-like, uniformly distributed population, deterministic nature, unpredictability, high positive Lyapunov exponent values, and perfect chaotic behaviour over infinite positive interval. TCM chaotic map is a one-way function that prevents the finding of a relationship between the successive output values, which increases sophistication and randomness of the proposed chaotic map. Therefore, TCM is considered as an ideal chaotic map with perfect and full population chaotic behaviour over the full interval. TCM characteristics are promising for possible utilization in many different fields of study to optimize exploitation chaotic maps.

Acknowledgements

This research work was conducted at the School of Engineering and Computer Sciences in Durham University,

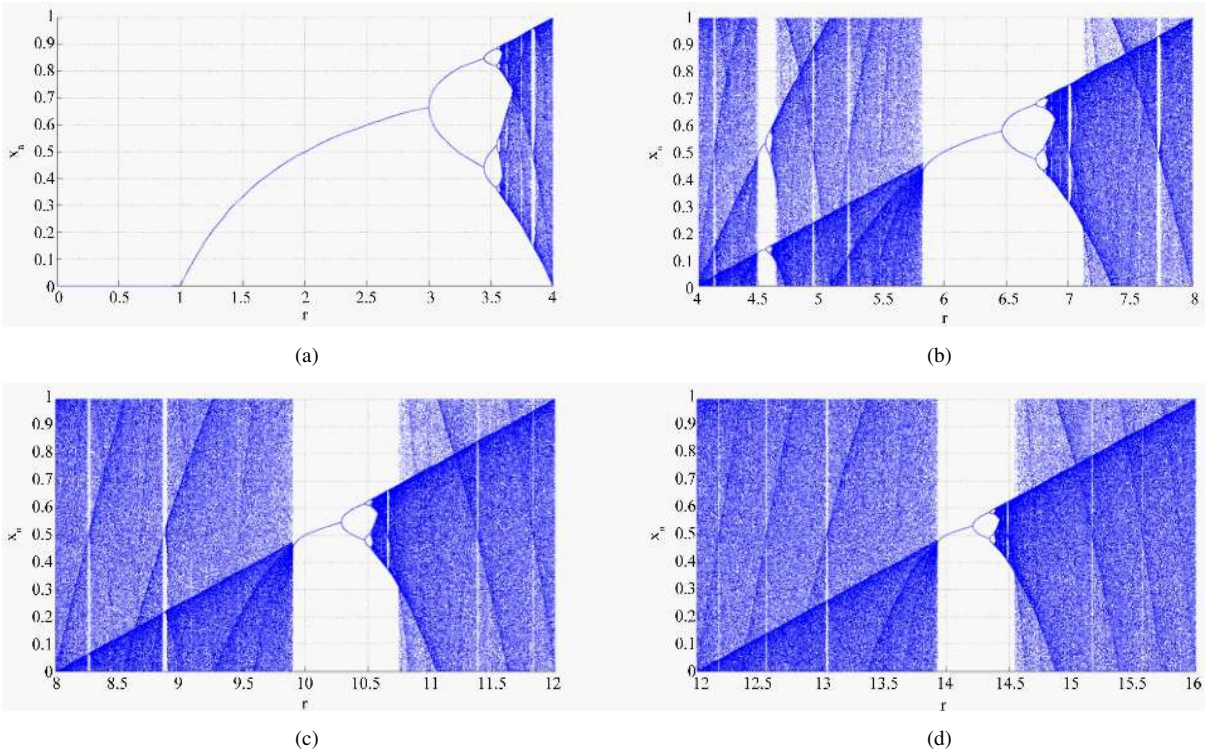

Figure 17. Modified logistic map bifurcation diagrams over different intervals. (a) Modified logistic map diagram for $a \in [0, 4]$; (b) Modified logistic map diagram for $r \in [4, 8]$; (c) Modified logistic map diagram for $a \in [8, 12]$; (d) Modified logistic map diagram for $r \in [12, 16]$.

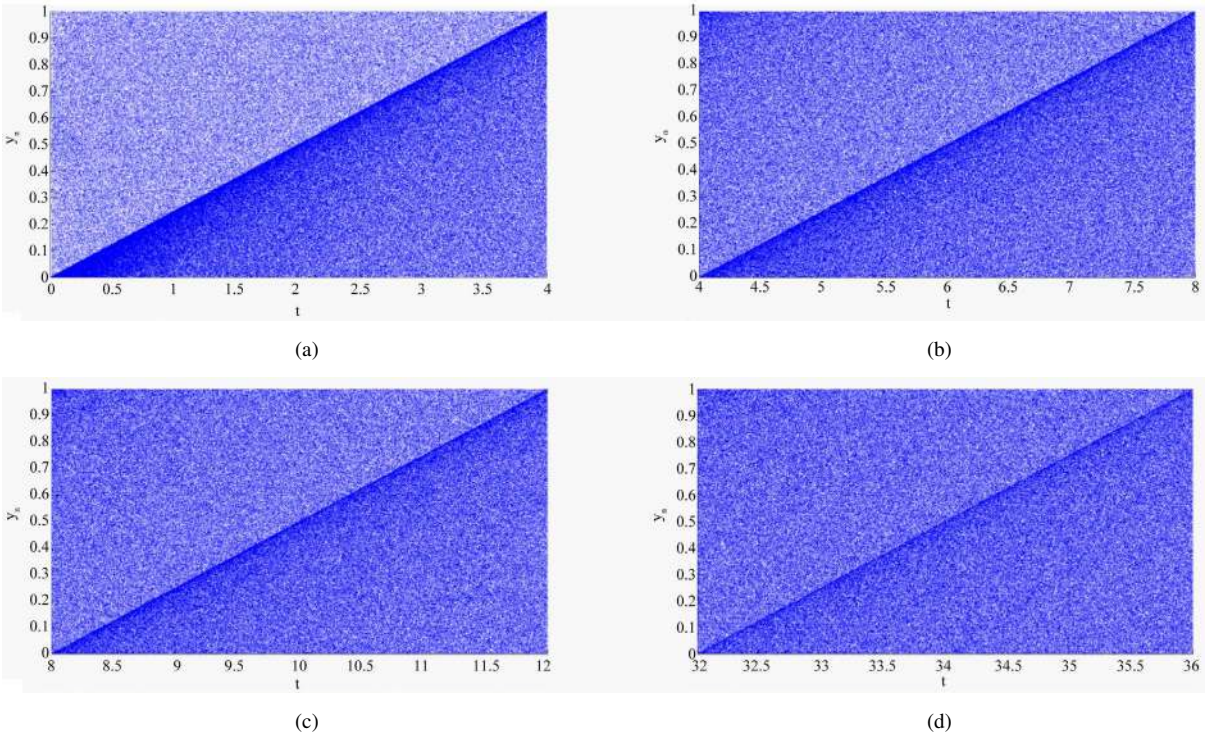

Figure 18. TCM map bifurcation diagrams over different intervals. (a) TCM diagram for $t \in [0, 4]$; (b) TCM diagram for $t \in [4, 8]$; (c) TCM diagram for $t \in [8, 12]$; (d) TCM diagram for $t \in [12, 16]$.

Durham—UK.

References

[1] Sneyers, R. (1997) Climate Chaotic Instability: Statistical Determination and Theoretical Background. *Environmetrics*, **8**, 517-532. http://dx.doi.org/10.1002/(SICI)1099-095X(199709/10)8:5<517::AID-ENV267>3.0.CO;2-L

[2] Zeng, X., Pielke, R.A. and Eykholt, R. (1993) Chaos Theory and Its Application to the Atmosphere. *Bulletin of the American Meteorological Society*, **74**, 631-639. http://dx.doi.org/10.1175/1520-0477(1993)074<0631:CTAIAT>2.0.CO;2

[3] Wikipedia. Chaos Theory. Cited 17 January 2009. http://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=264934743

[4] Serletis, A. and Gogas, P. (2000) Purchasing Power Parity, Nonlinearity and Chaos. *Applied Financial Economics*, **10**, 615-622. http://dx.doi.org/10.1080/096031000437962

[5] Serletis, A. and Gogas, P. (1997) Chaos in East European Black Market Exchange Rates. *Research in Economics*, **51**, 359-385. http://dx.doi.org/10.1006/reec.1997.0050

[6] Wikipedia (2015) Chaos Theory. https://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=693847517

[7] Maqableh, M., Samsudin, A.B. and Alia, M.A. (2008) New Hash Function Based on Chaos Theory (CHA-1). *IJCSNS International Journal of Computer Science and Network Security*, **8**, 20-26.

[8] Kocarev, L. (2001) Chaos-Based Cryptography: A Brief Overview. *IEEE Circuits and Systems Magazine*, **1**, 6-21. http://dx.doi.org/10.1109/7384.963463

[9] Pareek, N.K., Patidar, V. and Sud, K.K. (2003) Discrete Chaotic Cryptography Using External Key. *Physics Letters A*, **309**, 75-82. http://dx.doi.org/10.1016/S0375-9601(03)00122-1

[10] Pareek, N.K., Patidar, V. and Sud, K.K. (2005) Cryptography Using Multiple One-Dimensional Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **10**, 715-723. http://dx.doi.org/10.1016/j.cnsns.2004.03.006

[11] Xiang, T., Liao, X.F., Tang, G.P., Chen, Y. and Wong, K.W. (2006) A Novel Block Cryptosystem Based on Iterating a

Chaotic Map. *Physics Letters A*, **349**, 109-115. http://dx.doi.org/10.1016/j.physleta.2005.02.083

[12] Chen, S., Zhong, X.X. and Wu, Z.Z. (2008) Chaos Block Cipher for Wireless Sensor Network. *Science in China Series F*: *Information Sciences*, **51**, 1055-1063. http://dx.doi.org/10.1007/s11432-008-0102-5

[13] Peng, J., You, M.Y., Yang, Z.M. and Jin, S.Z. (2007) Research on a Block Encryption Cipher Based on Chaotic Dynamical System. 3*rd International Conference on Natural Computation*, *ICNC* 2007, Haikou, 24-27 August 2007, 744-748. http://dx.doi.org/10.1109/ICNC.2007.612

[14] Yang, H.Q., Liao, X.F., Wong, K.W., Zhang, W. and Wei, P.C. (2007) A New Block Cipher Based on Chaotic Map and Group Theory. *Chaos*, *Solitons & Fractals*, **40**, 50-59. http://dx.doi.org/10.1016/j.chaos.2007.07.056

[15] Peng, J., Jin, S.Z., Chen, G.R., Yang, Z.M. and Liao, X.F. (2008) An Image Encryption Scheme Based on Chaotic Map. 4*th International Conference on Natural Computation*, *ICNC* '08, Jinan, 18-20 October 2008, 595-599. http://dx.doi.org/10.1109/icnc.2008.227

[16] Lian, S. (2009) A Block Cipher Based on Chaotic Neural Networks. *Neurocomputing*, **72**, 1296-1301. http://dx.doi.org/10.1016/j.neucom.2008.11.005

[17] Wang, F.J., Zhang, Y.P. and Cao, T.J. (2009) Research of Chaotic Block Cipher Algorithm Based on Logistic Map. 2*nd International Conference on Intelligent Computation Technology and Automation*, 2009, *ICICTA* '09, Changsha, 10-11 October 2009, 678-681. http://dx.doi.org/10.1109/ICICTA.2009.169

[18] Peng, J., Jin, S.Z., Liu, H.L. and Liu, Y.G. (2009) A Block Cipher Based on a Hybrid of Chaotic System and Feistel Network. 5*th International Conference on Natural Computation*, *ICNC* '09, Tianjin, 14-16 August 2009, 427-431. http://dx.doi.org/10.1109/icnc.2009.663

[19] Amin, M., Faragallah, O.S. and Abd El-Latif, A.A. (2010) A Chaotic Block Cipher Algorithm for Image Cryptosystems. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 3484-3497. http://dx.doi.org/10.1016/j.cnsns.2009.12.025

[20] Huang, J.-H. and Liu, Y. (2010) A Block Encryption Algorithm Combined with the Logistic Mapping and SPN Structure. 2010 2*nd International Conference on Industrial and Information Systems* (*IIS*), Dalian, 10-11 July 2010, 156-159. http://dx.doi.org/10.1109/indusis.2010.5565655

[21] Zhao, G., Chen, G.R., Fang, J.Q. and Xu, G. (2011) Block Cipher Design: Generalized Single-Use-Algorithm Based on Chaos. *Tsinghua Science & Technology*, **16**, 194-206. http://dx.doi.org/10.1016/S1007-0214(11)70030-X

[22] Masuda, N., Jakimoski, G., Aihara, K. and Kocarev, L. (2006) Chaotic Block Ciphers: From Theory to Practical Algorithms. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **53**, 1341-1352. http://dx.doi.org/10.1109/TCSI.2006.874182

[23] Habutsu, T., Nishio, Y., Sasase, I. and Mori, S. (1991) A Secret Key Cryptosystem by Iterating a Chaotic Map. In: Davies, D.W., Ed., *Advances in Cryptology—EUROCRYPT* '91, Springer, Berlin, 127-140. http://dx.doi.org/10.1007/3-540-46416-6_11

[24] Gutowitz, H.A. (1993) Cryptography with Dynamical Systems, in Cellular Automata and Cooperative Phenomena. Kluwer Academic Press, Dordrecht. http://dx.doi.org/10.1007/978-94-011-1691-6_21

[25] Kotulski, Z. and Szczepanski, J. (1997) Discrete Chaotic Cryptography (DCC). *Annalen der Physik*, **6**, 381-394. http://dx.doi.org/10.1002/andp.19975090504

[26] García, P. and Jiménez, J. (2002) Communication through Chaotic Map Systems. *Physics Letters A*, **298**, 35-40. http://dx.doi.org/10.1016/S0375-9601(02)00382-1

[27] Masuda, N. and Aihara, K. (2002) Cryptosystems with Discretized Chaotic Maps. *IEEE Transactions on Circuits and Systems I*: *Fundamental Theory and Applications*, **49**, 28-40. http://dx.doi.org/10.1109/81.974872

[28] Baptista, M.S. (1998) Cryptography with Chaos. *Physics Letters A*, **240**, 50-54. http://dx.doi.org/10.1016/S0375-9601(98)00086-3

[29] Wong, W.-K., Lee, L.-P. and Wong, K.-W. (2001) A Modified Chaotic Cryptographic Method. *Computer Physics Communications*, **138**, 234-236. http://dx.doi.org/10.1016/S0010-4655(01)00220-X

[30] Alvarez, E., Fernández, A., García, P., Jiménez, J. and Marcano, A. (1999) New Approach to Chaotic Encryption. *Physics Letters A*, **263**, 373-375. http://dx.doi.org/10.1016/S0375-9601(99)00747-1

[31] Wong, K.W. (2002) A Fast Chaotic Cryptographic Scheme with Dynamic Look-Up Table. *Physics Letters A*, **298**, 238-242. http://dx.doi.org/10.1016/S0375-9601(02)00431-0

[32] Machado, R.F., Baptista, M.S. and Grebogi, C. (2004) Cryptography with Chaos at the Physical Level. *Chaos*, *Solitons & Fractals*, **21**, 1265-1269. http://dx.doi.org/10.1016/j.chaos.2003.12.094

[33] Guan, Z.-H., Huang, F. and Guan, W. (2005) Chaos-Based Image Encryption Algorithm. *Physics Letters A*, **346**, 153-157. http://dx.doi.org/10.1016/j.physleta.2005.08.006

[34] Gao, T. and Chen, Z. (2008) Image Encryption Based on a New Total Shuffling Algorithm. *Chaos*, *Solitons & Fractals*, **38**, 213-220. http://dx.doi.org/10.1016/j.chaos.2006.11.009

[35] Wong, K.W. (2003) A Combined Chaotic Cryptographic and Hashing Scheme. *Physics Letters A*, **307**, 292-298. http://dx.doi.org/10.1016/S0375-9601(02)01770-X

[36] Xiao, D., Liao, X. and Deng, S. (2005) One-Way Hash Function Construction Based on the Chaotic Map with Changeable-Parameter. *Chaos*, *Solitons & Fractals*, **24**, 65-71. http://dx.doi.org/10.1016/S0960-0779(04)00456-4

[37] Lian, S.G., Liu, Z.X., Ren, Z. and Wang, H.L. (2006) Hash Function Based on Chaotic Neural Networks. 2006 *IEEE International Symposium on Circuits and Systems*, *ISCAS* 2006, Island of Kos, 21-24 May 2006. http://dx.doi.org/10.1109/iscas.2006.1692566

[38] Peng, F. and Qiu, S.-S. (2007) One-Way Hash Functions Based on Iterated Chaotic Systems. *International Conference on Communications*, *Circuits and Systems*, *ICCCAS* 2007, Kokura, 11-13 July 2007, 1070-1074. http://dx.doi.org/10.1109/ICCCAS.2007.4348231

[39] Khan, M.K., Zhang, J. and Wang, X. (2008) Chaotic Hash-Based Fingerprint Biometric Remote User Authentication Scheme on Mobile Devices. *Chaos*, *Solitons & Fractals*, **35**, 519-524. http://dx.doi.org/10.1016/j.chaos.2006.05.061

[40] Xiao, D., Liao, X. and Deng, S. (2008) Parallel Keyed Hash Function Construction Based on Chaotic Maps. *Physics Letters A*, **372**, 4682-4688. http://dx.doi.org/10.1016/j.physleta.2008.04.060

[41] Song, Y.R. and Jiang, G.P. (2008) Hash Function Construction Based on Chaotic Coupled Map Network. *The 9th International Conference for Young Computer Scientists*, *ICYCS* 2008, Hunan, 18-21 November 2008, 2753-2758. http://dx.doi.org/10.1109/ICYCS.2008.134

[42] Deng, S., Xiao, D., Li, Y.T. and Peng, W.B. (2009) A Novel Combined Cryptographic and Hash Algorithm Based on Chaotic Control Character. *Communications in Nonlinear Science and Numerical Simulation*, **14**, 3889-3900. http://dx.doi.org/10.1016/j.cnsns.2009.02.020

[43] Guyeux, C. and Bahi, J.M. (2010) Topological Chaos and Chaotic Iterations Application to Hash Functions. *The* 2010 *International Joint Conference on Neural Networks* (*IJCNN*), Barcelona, 18-23 July 2010, 1-7. http://dx.doi.org/10.1109/ijcnn.2010.5596512

[44] Huang, Z. (2011) A More Secure Parallel Keyed Hash Function Based on Chaotic Neural Network. *Communications in Nonlinear Science and Numerical Simulation*, **16**, 3245-3256. http://dx.doi.org/10.1016/j.cnsns.2010.12.009

[45] Wang, Y., Wong, K.-W. and Xiao, D. (2011) Parallel Hash Function Construction Based on Coupled Map Lattices. *Communications in Nonlinear Science and Numerical Simulation*, **16**, 2810-2821. http://dx.doi.org/10.1016/j.cnsns.2010.10.001

[46] Yi, X. (2005) Hash Function Based on Chaotic Tent Maps. *IEEE Transactions on Circuits and Systems II*: *Express Briefs*, **52**, 354-357. http://dx.doi.org/10.1109/TCSII.2005.848992

[47] Zhang, J., Wang, X. and Zhang, W. (2007) Chaotic Keyed Hash Function Based on Feedforward-Feedback Nonlinear Digital Filter. *Physics Letters A*, **362**, 439-448. http://dx.doi.org/10.1016/j.physleta.2006.10.052

[48] Amin, M., Faragallah, O.S. and Abd El-Latif, A.A. (2009) Chaos-Based Hash Function (CBHF) for Cryptographic Applications. *Chaos*, *Solitons & Fractals*, **42**, 767-772. http://dx.doi.org/10.1016/j.chaos.2009.02.001

[49] Xiao, D., Shih, F.Y. and Liao, X. (2010) A Chaos-Based Hash Function with both Modification Detection and Localization Capabilities. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 2254-2261. http://dx.doi.org/10.1016/j.cnsns.2009.10.012

[50] Kocarev, L. and Jakimoski, G. (2003) Pseudorandom Bits Generated by Chaotic Maps. *IEEE Transactions on Circuits and Systems I*: *Fundamental Theory and Applications*, **50**, 123-126. http://dx.doi.org/10.1109/TCSI.2002.804550

[51] Tong, X.-J., Cui, M.-G. and Jiang, W. (2006) The Production Algorithm of Pseudo-Random Number Generator Based on Compound Non-Linear Chaos System. *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2006, *IIH-MSP* '06, Pasadena, 18-20 December 2006, 685-688. http://dx.doi.org/10.1109/IIH-MSP.2006.265094

[52] Chen, S. and Zhong, X.-X. (2007) Chaotic Block Iterating Method for Pseudo-Random Sequence Generator. *The Journal of China Universities of Posts and Telecommunications*, **14**, 45-48. http://dx.doi.org/10.1016/s1005-8885(07)60054-5

[53] Zheng, F., Tian, X.-J., Song, J.-Y. and Li, X.-Y. (2008) Pseudo-Random Sequence Generator Based on the Generalized Henon Map. *The Journal of China Universities of Posts and Telecommunications*, **15**, 64-68. http://dx.doi.org/10.1016/S1005-8885(08)60109-0

[54] Qi, A.X., Han, C.Y. and Wang, G.Y. (2010) Design and FPGA Realization of a Pseudo Random Sequence Generator Based on a Switched Chaos. *International Conference on Communications*, *Circuits and Systems* (*ICCCAS*), Chengdu, 28-30 July 2010, 417-420. http://dx.doi.org/10.1109/ICCCAS.2010.5581965

[55] Yoon, J.W. and Kim, H. (2010) An Image Encryption Scheme with a Pseudorandom Permutation Based on Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 3998-4006. http://dx.doi.org/10.1016/j.cnsns.2010.01.041

[56] Dabal, P. and Pelka, R. (2011) A Chaos-Based Pseudo-Random Bit Generator Implemented in FPGA Device. 2011 *IEEE* 14*th International Symposium on Design and Diagnostics of Electronic Circuits & Systems* (*DDECS*), Cottbus, 13-15 April 2011, 151-154. http://dx.doi.org/10.1109/ddecs.2011.5783069

[57] Forré, R. (1991) The Hénon Attractor as a Keystream Generator. In: Davies, D.W., Ed., *Advances in Cryptology—EUROCRYPT* '91, Springer, Berlin, 76-81.

[58] Matthews, R.A.J. (1989) On the Derivation of a "Chaotic" Encryption Algorithm. *Cryptologia*, **13**, 29-42. http://dx.doi.org/10.1080/0161-118991863745

[59] Li, S., Mou, X. and Cai, Y. (2001) Improving Security of a Chaotic Encryption Approach. *Physics Letters A*, **290**, 127-133. http://dx.doi.org/10.1016/S0375-9601(01)00612-0

[60] Wolfram, S. (1985) Cryptography with Cellular Automata. In: Williams, H.C., Ed., *Advances in Cryptology—CRYPTO* '85 *Proceedings*, Lecture Notes in Computer Science, Spinger-Verlag, Berlin, 429-432.

[61] Lee, P.-H., Pei, S.-C. and Chen, Y.-Y. (2003) Generating Chaotic Stream Ciphers Using Chaotic Systems. *Chinese Journal of Physics*, **41**, 559-581.

[62] Sang, T., Wang, R. and Yan, Y. (2000) Constructing Chaotic Discrete Sequences for Digital Communications Based on Correlation Analysis. *IEEE Transactions on Signal Processing*, **48**, 2557-2565. http://dx.doi.org/10.1109/78.863058

[63] Kwok, H.S. and Tang, W.K.S. (2007) A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation. *Chaos*, *Solitons & Fractals*, **32**, 1518-1529. http://dx.doi.org/10.1016/j.chaos.2005.11.090

[64] Patidar, V., Pareek, N.K. and Sud, K.K. (2009) A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **14**, 3056-3075. http://dx.doi.org/10.1016/j.cnsns.2008.11.005

[65] Patidar, V., Pareek, N.K., Purohit, G. and Sud, K.K. (2010) Modified Substitution-Diffusion Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 2755-2765. http://dx.doi.org/10.1016/j.cnsns.2009.11.010

[66] Biham, E. (1991) Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91. In: Davies, D.W., Ed., *Advances in Cryptology—EUROCRYPT* '91, Springer, Berlin, 532-534. http://dx.doi.org/10.1007/3-540-46416-6_49

[67] Wheeler, D.D. (1989) Problems with Chaotic Cryptosystems. *Cryptologia*, **13**, 243-250. http://dx.doi.org/10.1080/0161-118991863934

[68] Alvarez, G., Montoya, F., Romera, M. and Pastor, G. (2000) Cryptanalysis of a Chaotic Encryption System. *Physics Letters A*, **276**, 191-196. http://dx.doi.org/10.1016/S0375-9601(00)00642-3

[69] Alvarez, G., Montoya, F., Romera, M. and Pastor, G. (2003) Cryptanalysis of a Discrete Chaotic Cryptosystem Using External Key. *Physics Letters A*, **319**, 334-339. http://dx.doi.org/10.1016/j.physleta.2003.10.044

[70] Wei, J., Liao, X.F., Wong, K.W. and Zhou, T. (2007) Cryptanalysis of a Cryptosystem Using Multiple One-Dimensional Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **12**, 814-822. http://dx.doi.org/10.1016/j.cnsns.2005.06.001

[71] Li, C.Q., Li, S.J., Alvarez, G., Chen, G.R. and Lo, K.-T. (2008) Cryptanalysis of a Chaotic Block Cipher with External Key and Its Improved Version. *Chaos*, *Solitons & Fractals*, **37**, 299-307. http://dx.doi.org/10.1016/j.chaos.2006.08.025

[72] Wang, X. and Yu, C. (2009) Cryptanalysis and Improvement on a Cryptosystem Based on a Chaotic Map. *Computers & Mathematics with Applications*, **57**, 476-482. http://dx.doi.org/10.1016/j.camwa.2008.09.042

[73] Yang, J., Xiao, D. and Xiang, T. (2011) Cryptanalysis of a Chaos Block Cipher for Wireless Sensor Network. *Communications in Nonlinear Science and Numerical Simulation*, **16**, 844-850. http://dx.doi.org/10.1016/j.cnsns.2010.05.005

[74] Álvarez, G., Montoya, F., Romera, M. and Pastor, G. (2004) Keystream Cryptanalysis of a Chaotic Cryptographic Method. *Computer Physics Communications*, **156**, 205-207. http://dx.doi.org/10.1016/S0010-4655(03)00432-6

[75] Jakimoski, G. and Kocarev, L. (2001) Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms. *Physics Letters A*, **291**, 381-384. http://dx.doi.org/10.1016/S0375-9601(01)00771-X

[76] Li, S.J., Mou, X.Q., Ji, Z., Zhang, J.H. and Cai, Y.L. (2003) Performance Analysis of Jakimoski-Kocarev Attack on a Class of Chaotic Cryptosystems. *Physics Letters A*, **307**, 22-28. http://dx.doi.org/10.1016/S0375-9601(02)01659-6

[77] Çokal, C. and Solak, E. (2009) Cryptanalysis of a Chaos-Based Image Encryption Algorithm. *Physics Letters A*, **373**, 1357-1360. http://dx.doi.org/10.1016/j.physleta.2009.02.030

[78] Maqableh, M.M. and Dantchev, S. (2009) Cryptanalysis of Chaos-Based Hash Function (CBHF). 1*st International Al-*

ternative Workshop on Aggressive Computing and Security—iAWACS, Laval, 23-25 October 2009, 20-30.

[79] Yang, Q.-T., Gao, T.-G., Fan, L. and Gu, Q.-L. (2009) Analysis of One-Way Alterable Length Hash Function Based on Cell Neural Network. 5*th International Conference on Information Assurance and Security*, *IAS* '09, Xi'an, 18-20 August 2009, 391-395. http://dx.doi.org/10.1109/ias.2009.87

[80] Xiao, D., Liao, X. and Wang, Y. (2009) Improving the Security of a Parallel Keyed Hash Function Based on Chaotic Maps. *Physics Letters A*, **373**, 4346-4353. http://dx.doi.org/10.1016/j.physleta.2009.09.059

[81] Deng, S., Li, Y. and Xiao, D. (2010) Analysis and Improvement of a Chaos-Based Hash Function Construction. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 1338-1347. http://dx.doi.org/10.1016/j.cnsns.2009.05.065

[82] Li, C.Q., Li, S.J., Chen, G.R. and Halang, W.A. (2009) Cryptanalysis of an Image Encryption Scheme Based on a Compound Chaotic Sequence. *Image and Vision Computing*, **27**, 1035-1039. http://dx.doi.org/10.1016/j.imavis.2008.09.004

[83] Rhouma, R., Solak, E. and Belghith, S. (2010) Cryptanalysis of a New Substitution-Diffusion Based Image Cipher. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 1887-1892. http://dx.doi.org/10.1016/j.cnsns.2009.07.007

[84] Li, C., Li, S. and Lo, K.-T. (2011) Breaking a Modified Substitution-Diffusion Image Cipher Based on Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **16**, 837-843. http://dx.doi.org/10.1016/j.cnsns.2010.05.008

[85] Maqableh, M.M. (2011) Fast Parallel Keyed Hash Functions Based on Chaotic Maps (PKHC). *Western European Workshop on Research in Cryptology*, Weimar, 20-22 July 2011, 33-40.

[86] Maqableh, M.M. (2010) Secure Hash Functions Based on Chaotic Maps for E-Commerce Application. *International Journal of Information Technology and Management information System* (*IJITMIS*), **1**, 12-19.

[87] Maqableh, M.M. (2010) Fast Hash Function Based on BCCM Encryption Algorithm for E-Commerce (HFBCCM). 5*th International Conference on e-Commerce in Developing Countries*: *With Focus on Export*, Le Havre, 15-16 September 2010, 55-64.

[88] Bertuglia, C.S. and Vaio, F. (2005) Nonlinearity, Chaos & Complexity: The Dynamics of Natural and Social Systems. Oxford University Press.

[89] Alligood, K.T., Sauer, T.D. and Yorke, J.A. (1996) Chaos an Introduction to Dynamical Systems. Springer-Verlag, New York.

[90] Solari, H.G., Natiello, M.A. and Mindlin, G.B. (1996) Nonlinear Dynamics A Two-Way Trip from Physics to Math. Institute of Physics Publishing, Bristol.

[91] Baker, G.L. and Gollub, J.P. (1990) Chaotic Dynamics an Introduction. Press Syndicate of the University of Cambridge, New York.

[92] Poincaré, J.H. (1890) Sur le problème des trois corps et les équations de la dynamique. Divergence des séries de M. Lindstedt. *Acta Mathematica*, **13**, 1-270.

[93] Lorenz, E.N. (1963) Deterministic Nonperiodic Flow. *Journal of Atmospheric Sciences*, **20**, 130-141. http://dx.doi.org/10.1175/1520-0469(1963)020<0130:dnf>2.0.co;2

[94] Pritchard, J. (1996) The Chaos Cookbook. Butterworh-Heinemann, Oxford.

[95] Rahimi, A., Mohammadi, S. and Rahimi, R. (2009) An Efficient Iris Authentication Using Chaos Theory-Based Cryptography for E-Commerce Transactions. *International Conference for Internet Technology and Secured Transactions* (*ICITST* 2009).

[96] Serletis, A. and Gogas, P. (1999) The North American Natural Gas Liquids Markets Are Chaotic. *The Energy Journal*, **20**, 83-103. http://dx.doi.org/10.5547/ISSN0195-6574-EJ-Vol20-No1-5

[97] Gilmore, R. (2004) Chaos and Attractors. Encyclopedia of Mathematical Physics, EMP MS 93.

[98] Tullaro, N.B., Abbott, T. and Reilly, J.P. (1992) An Experimental Approach to Nonlinear Dynamics and Chaos. Vol. 1, Addison-Wesley, Boston.

[99] Parker, T.S. and Chua, L.O. (1989) Practical Numerical Algorithms for Chaotic Systems. Springer-Verlag, New York. http://dx.doi.org/10.1007/978-1-4612-3486-9

[100] Schmitz, R. (2001) Use of Chaotic Dynamical Systems in Cryptography. *Journal of the Franklin Institute*, **338**, 429-441. http://dx.doi.org/10.1016/S0016-0032(00)00087-9

[101] Maqableh, M.M. (2012) Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce. Doctoral Thesis, Durham University, Durham.

[102] Grassi, G. and Mascoio, S. (1999) Synchronizing Hyperchaotic Systems by Observer Design. *IEEE Transactions on*

Circuits and Systems II: *Analog and Digital Signal Processing*, **46**, 478-483. http://dx.doi.org/10.1109/82.755422

[103] May, R.M. (1976) Simple Mathematical Models with Very Complicated Dynamics. *Nature*, **261**, 459-467. http://dx.doi.org/10.1038/261459a0

[104] Wikipedia. Logistic Map. Cited 20 February 2009. http://en.wikipedia.org/w/index.php?title=chaotic_maps&oldid=261864353

[105] Naess, A. (2000) Chaos and Nonlinear Stochastic Dynamics. *Probabilistic Engineering Mechanics*, **15**, 37-47. http://dx.doi.org/10.1016/S0266-8920(99)00007-7

[106] Contributors, W. (2005) Chaos Theory. http://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=264934743

[107] Rössler, O. (1976) An Equation for Continous Chaos. *Physics Letters A*, **57**, 397-398. http://dx.doi.org/10.1016/0375-9601(76)90101-8

[108] Ho, A. (2006) Chaos Introduction. http://www.zeuscat.com/andrew/chaos/chaos.html

[109] Wikipedia. Tent Map. Cited 25 February 2009. http://en.wikipedia.org/w/index.php?title=Tent_map&oldid=186656075

[110] Li, S., Chen, G. and Mou, X. (2005) On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps. *International Journal of Bifurcation and Chaos*, **15**, 3119-3151. http://dx.doi.org/10.1142/S0218127405014052

[111] Jun, P., Jin, S.Z., Liu, Y.G., Yang, Z.M., You, M.Y. and Pei, Y.J. (2008) A Novel Scheme for Image Encryption Based on Piecewise Linear Chaotic Map. 2008 *IEEE Conference on Cybernetics and Intelligent Systems*, Chengdu, 21-24 September 2008, 1012-1016.

[112] Rhouma, R., Arroyo, D. and Belghith, S. (2009) A New Color Image Cryptosystem Based on a Piecewise Linear Chaotic Map. 6*th International Multi-Conference on Systems*, *Signals and Devices*, 2009, *SSD* '09, 23-26 March 2009, 1-6. http://dx.doi.org/10.1109/SSD.2009.4956666

[113] Yang, H.Q., Wong, K.-W., Liao, X.F., Zhang, W. and Wei, P.C. (2010) A Fast Image Encryption and Authentication Scheme Based on Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 3507-3517. http://dx.doi.org/10.1016/j.cnsns.2010.01.004

[114] Yang, H.Q., Wong, K.-W., Liao, X.F., Wang, Y. and Yang, D.G. (2009) One-Way Hash Function Construction Based on Chaotic Map Network. *Chaos*, *Solitons & Fractals*, **41**, 2566-2574. http://dx.doi.org/10.1016/j.chaos.2008.09.056

[115] Lian, S., Sun, J. and Wang, Z. (2005) A Block Cipher Based on a Suitable Use of the Chaotic Standard Map. *Chaos*, *Solitons & Fractals*, **26**, 117-129. http://dx.doi.org/10.1016/j.chaos.2004.11.096

[116] Li, P., Li, Z., Halang, W.A. and Chen, G.R. (2007) A Stream Cipher Based on a Spatiotemporal Chaotic System. *Chaos*, *Solitons & Fractals*, **32**, 1867-1876. http://dx.doi.org/10.1016/j.chaos.2005.12.021

[117] Ali-Pacha, A., Hadj-Said, N., M'Hamed, A. and Belgoraf, A. (2007) Lorenz's Attractor Applied to the Stream Cipher (Ali-Pacha Generator). *Chaos*, *Solitons & Fractals*, **33**, 1762-1766. http://dx.doi.org/10.1016/j.chaos.2006.03.009

[118] Tong, X. and Cui, M. (2008) Image Encryption with Compound Chaotic Sequence Cipher Shifting Dynamically. *Image and Vision Computing*, **26**, 843-850. http://dx.doi.org/10.1016/j.imavis.2007.09.005

[119] Gao, H., Zhang, Y.S., Liang, S.Y. and Li, D.Q. (2006) A New Chaotic Algorithm for Image Encryption. *Chaos*, *Solitons & Fractals*, **29**, 393-399. http://dx.doi.org/10.1016/j.chaos.2005.08.110

[120] Chee, C.Y. and Xu, D. (2006) Chaotic Encryption Using Discrete-Time Synchronous Chaos. *Physics Letters A*, **348**, 284-292. http://dx.doi.org/10.1016/j.physleta.2005.08.082

[121] Gao, T. and Chen, Z. (2008) A New Image Encryption Algorithm Based on Hyper-Chaos. *Physics Letters A*, **372**, 394-400. http://dx.doi.org/10.1016/j.physleta.2007.07.040

[122] Sun, F. and Liu, S. (2009) Cryptographic Pseudo-Random Sequence from the Spatial Chaotic Map. *Chaos*, *Solitons & Fractals*, **41**, 2216-2219. http://dx.doi.org/10.1016/j.chaos.2008.08.032

[123] Li, P., Li, Z., Halang, W.A. and Chen, G.R. (2006) A Multiple Pseudorandom-Bit Generator Based on a Spatiotemporal Chaotic Map. *Physics Letters A*, **349**, 467-473. http://dx.doi.org/10.1016/j.physleta.2005.09.060

[124] Arroyo, D., Li, C.Q., Li, S.J. and Alvarez, G. (2009) Cryptanalysis of a Computer Cryptography Scheme Based on a Filter Bank. *Chaos*, *Solitons & Fractals*, **41**, 410-413. http://dx.doi.org/10.1016/j.chaos.2008.01.020

[125] Kanso, A. and Smaoui, N. (2009) Logistic Chaotic Maps for Binary Numbers Generations. *Chaos*, *Solitons & Fractals*, **40**, 2557-2568. http://dx.doi.org/10.1016/j.chaos.2007.10.049

Appendix A

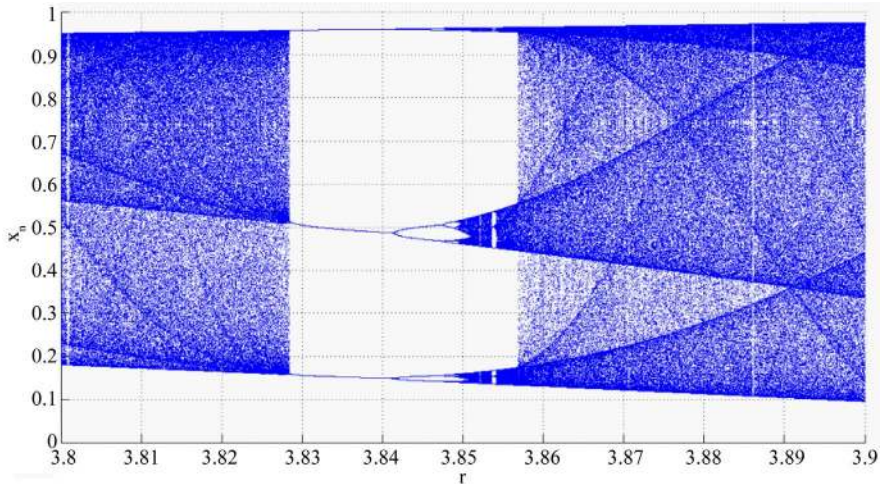

Figure A1. Logistic map bifurcation diagram with $t \in [3.8, 3.9]$.

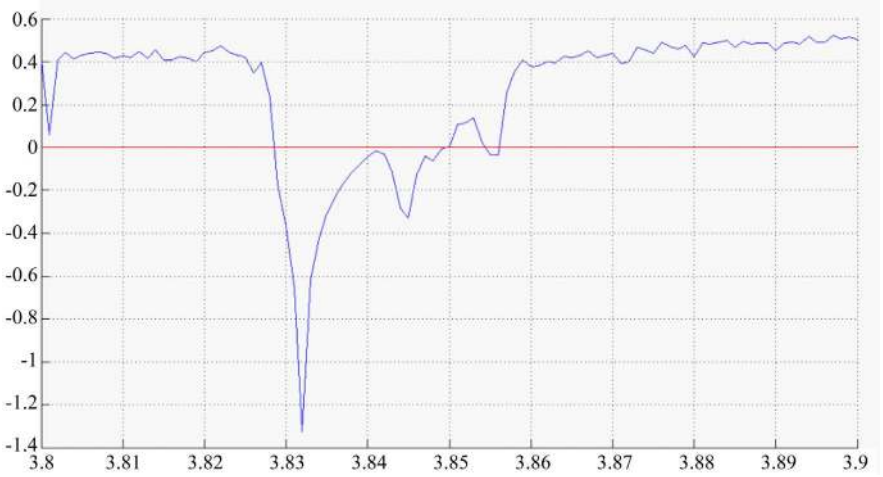

Figure A2. Lyapunov exponent of logistic map with $t \in [3.8, 3.9]$.

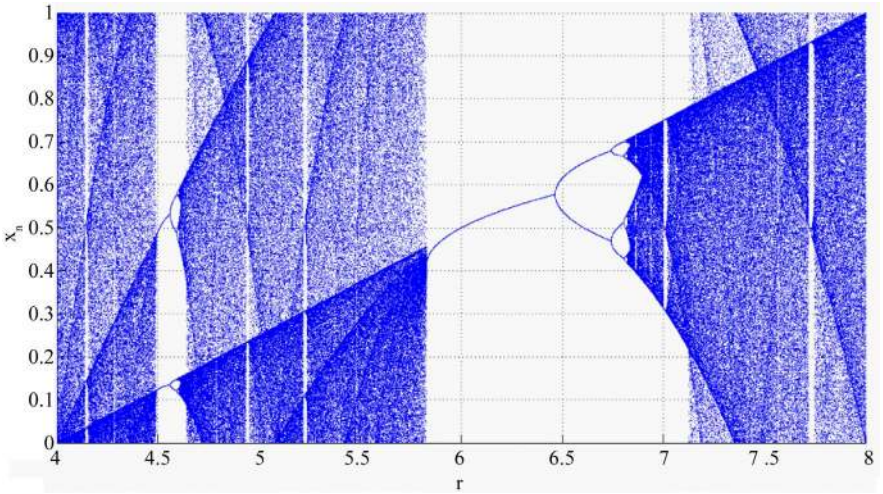

Figure A3. Modified logistic map bifurcation diagram with $t \in [4, 8]$.

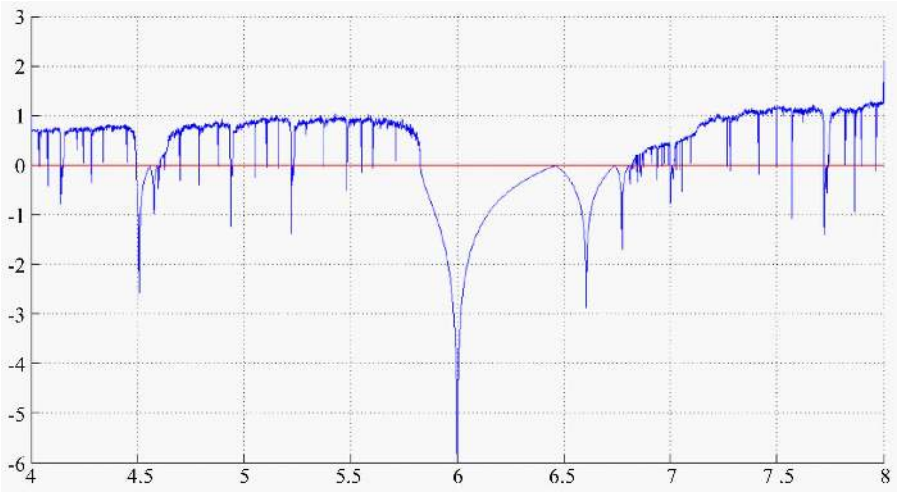

Figure A4. Lyapunov exponent of modified logistic map with $t \in [4, 8]$.

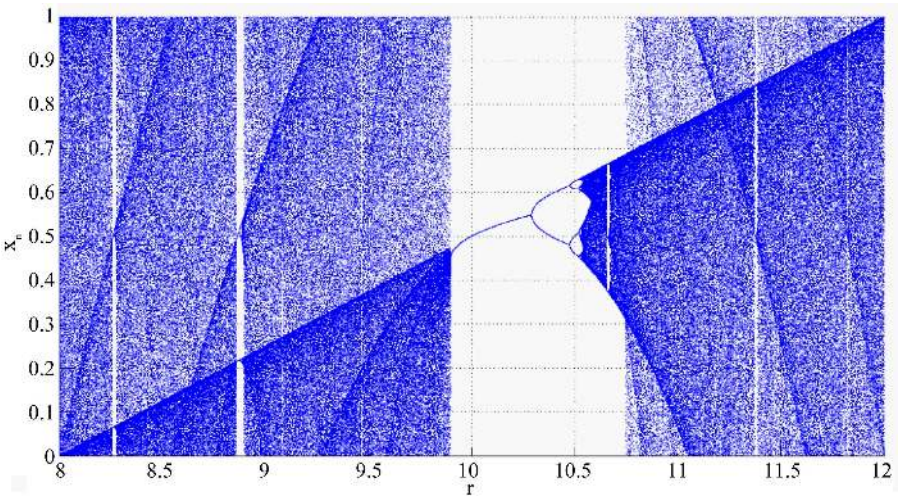

Figure A5. Modified logistic map bifurcation diagram with $t \in [8, 12]$.

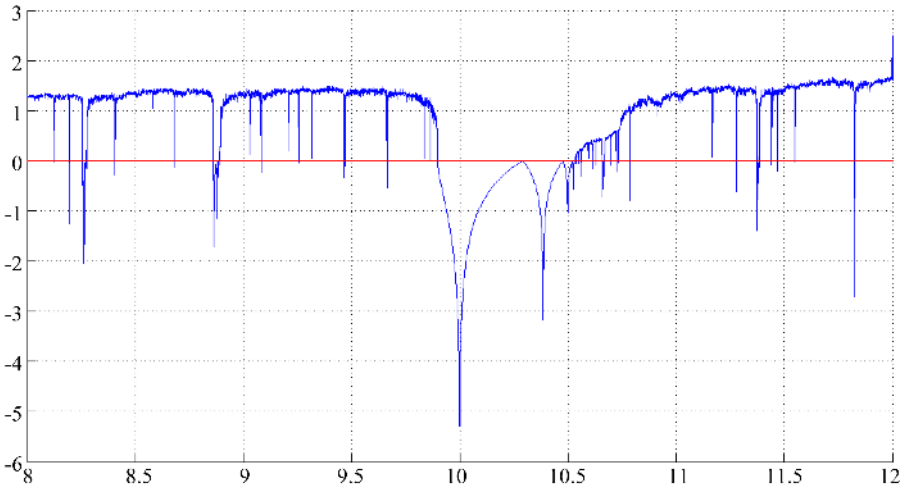

Figure A6. Lyapunov exponent of modified logistic map with $t \in [8, 12]$.

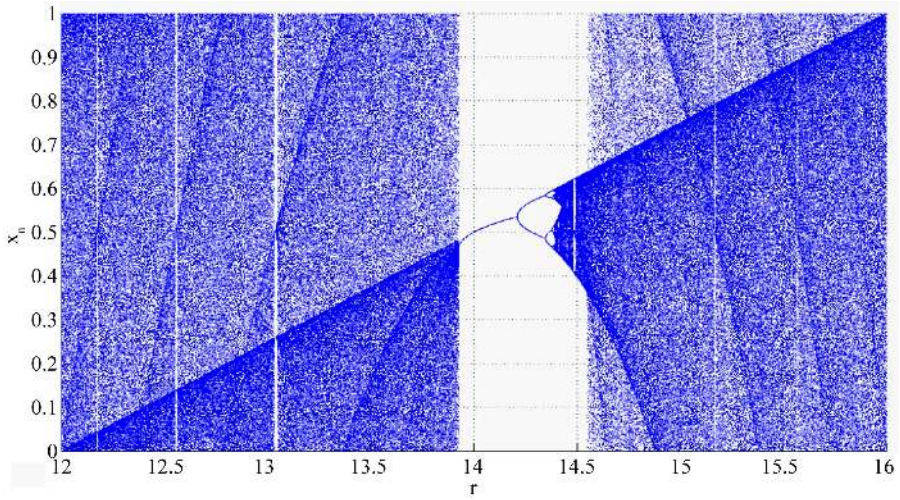

Figure A7. Modified logistic map bifurcation diagram with $t \in [12, 16]$.

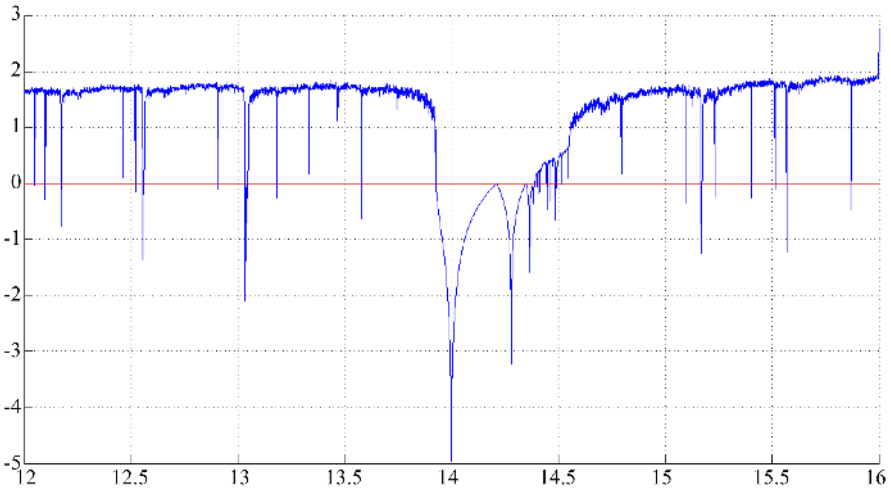

Figure A8. Lyapunov exponent of modified logistic map with $t \in [12, 16]$.

Appendix B

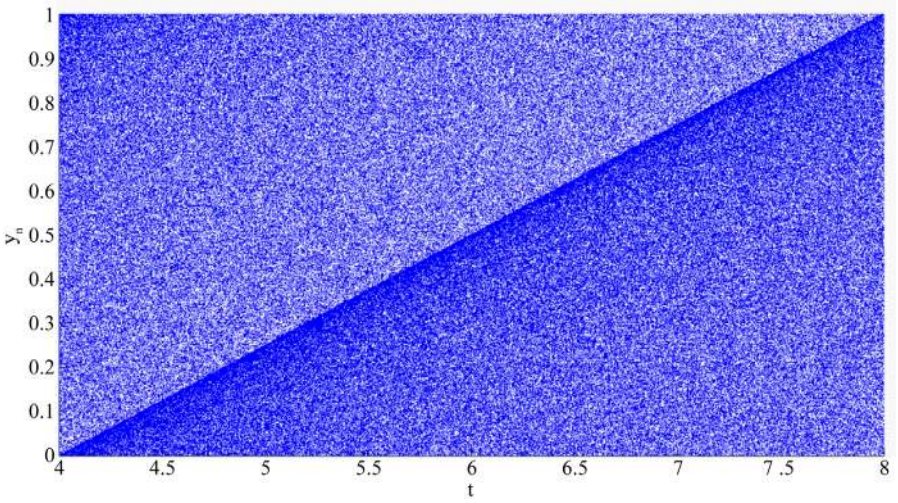

Figure B1. TCM chaotic map bifurcation diagram with $t \in [4, 8]$.

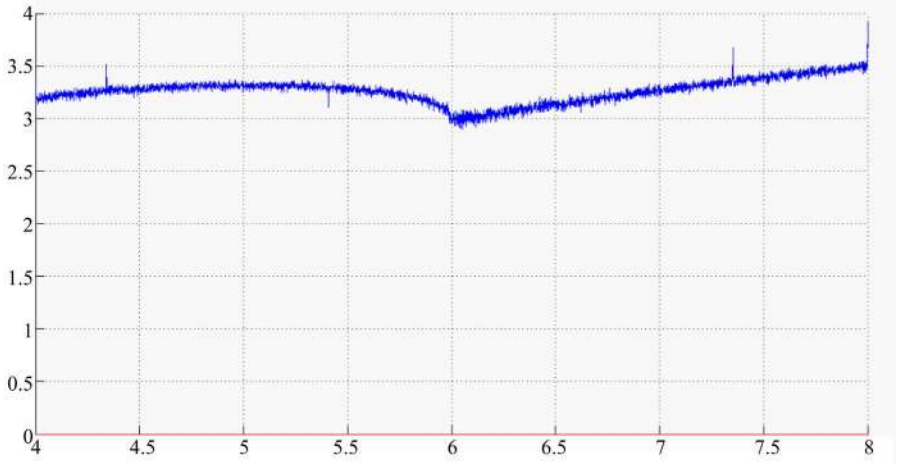

Figure B2. Lyapunov exponent of TCM chaotic map with $t \in [4, 8]$.

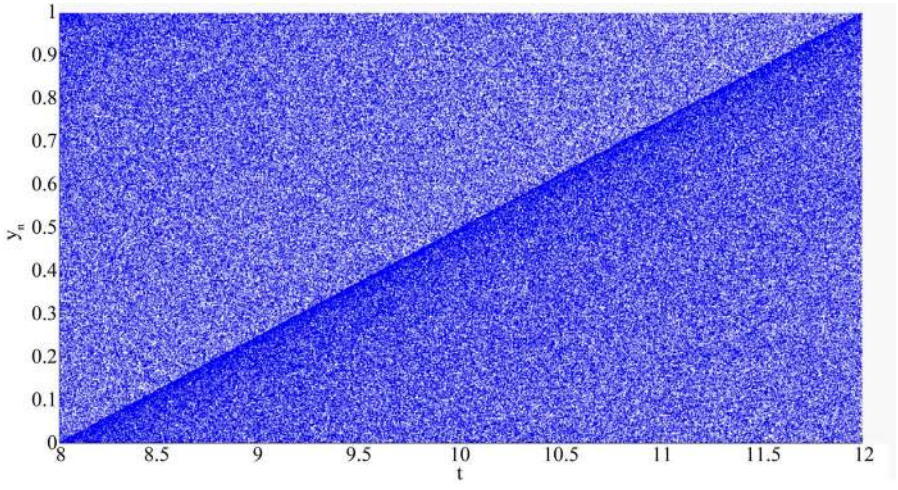

Figure B3. TCM chaotic map bifurcation diagram with $t \in [8, 12]$.

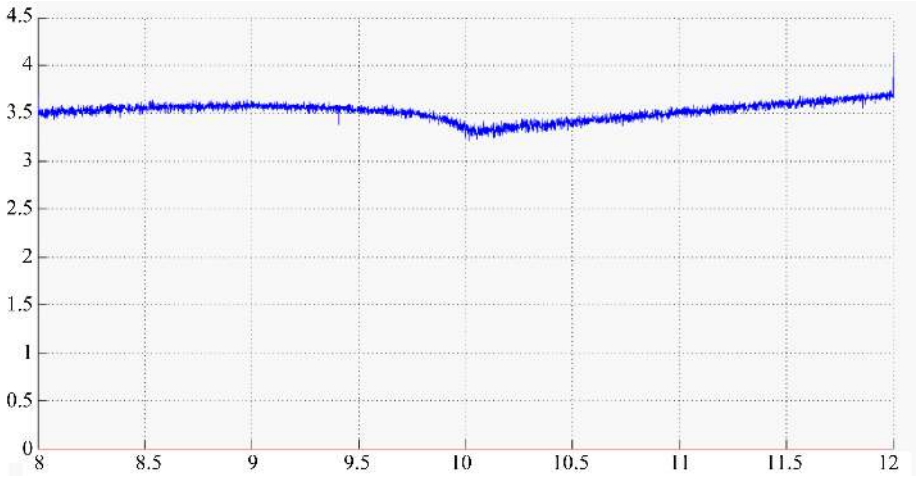

Figure B4. Lyapunov exponent of TCM chaotic map with $t \in [8, 12]$.

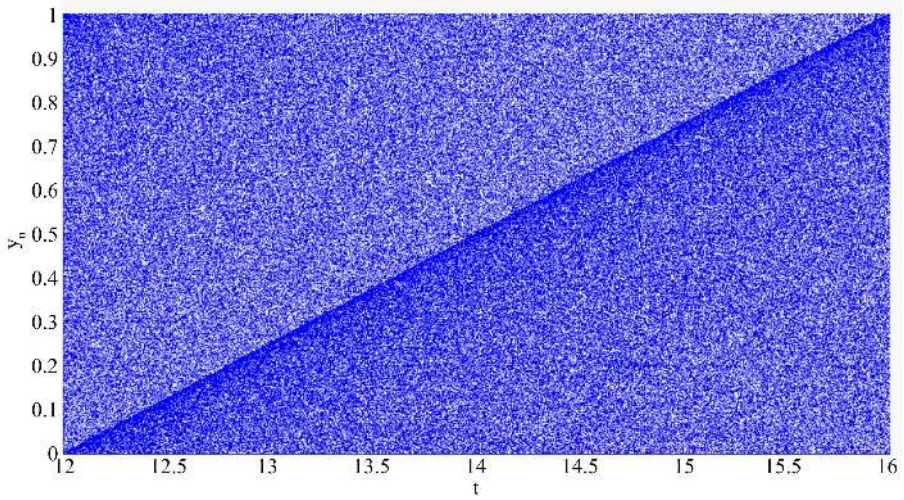

Figure B5. TCM chaotic map bifurcation diagram with $t \in [12, 14]$.

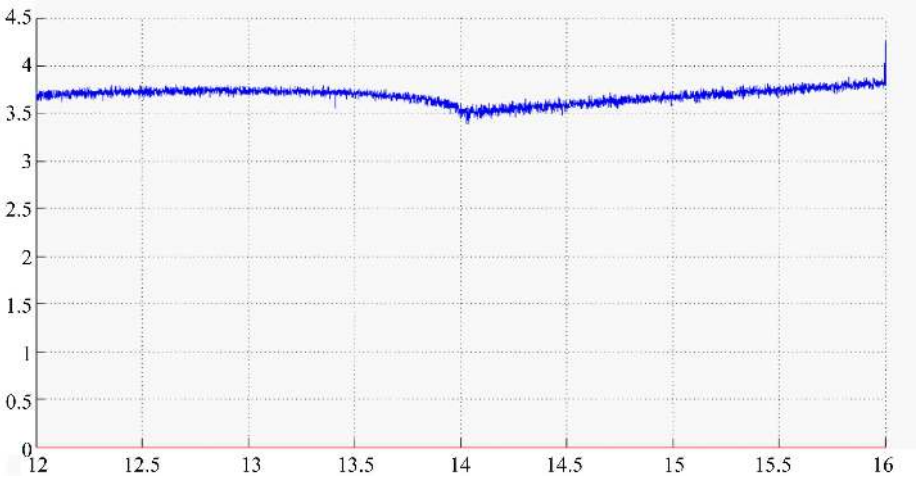

Figure B6. Lyapunov exponent of TCM chaotic map with $t \in [12, 14]$.

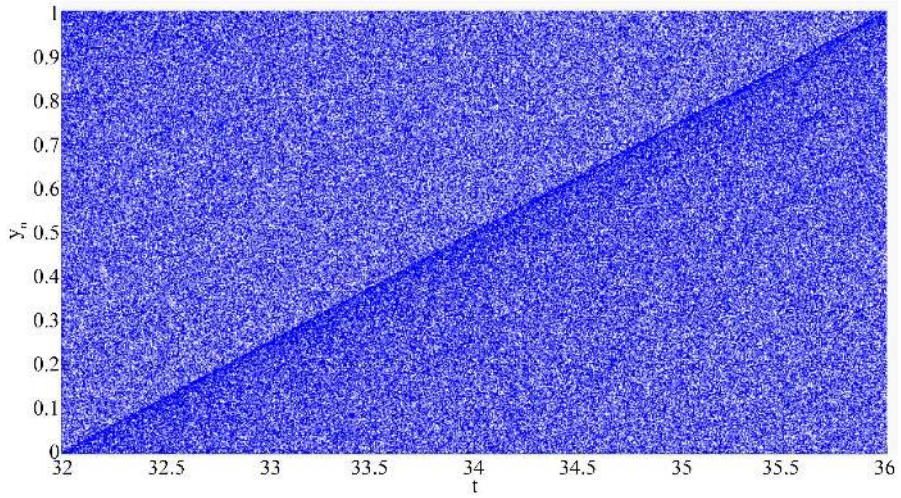

Figure B7. TCM chaotic map bifurcation diagram with $t \in [32, 36]$.

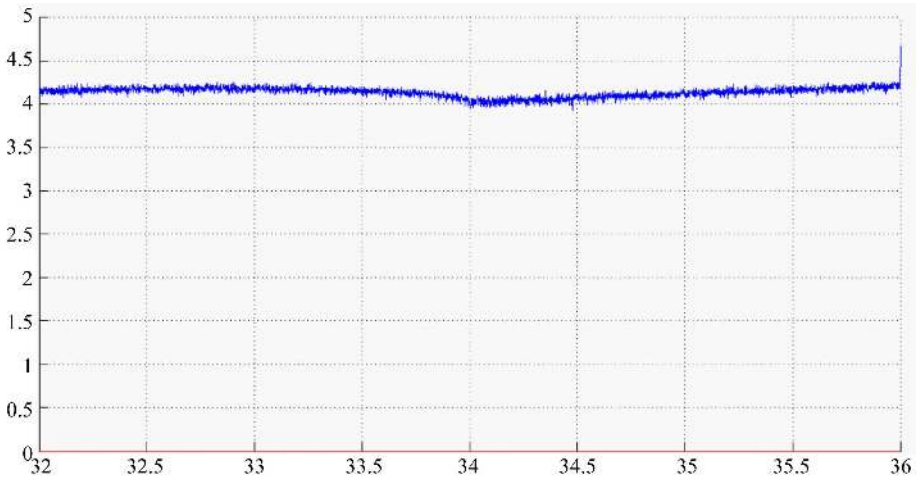

Figure B8. Lyapunov exponent of TCM chaotic map with $t \in [32, 36]$.

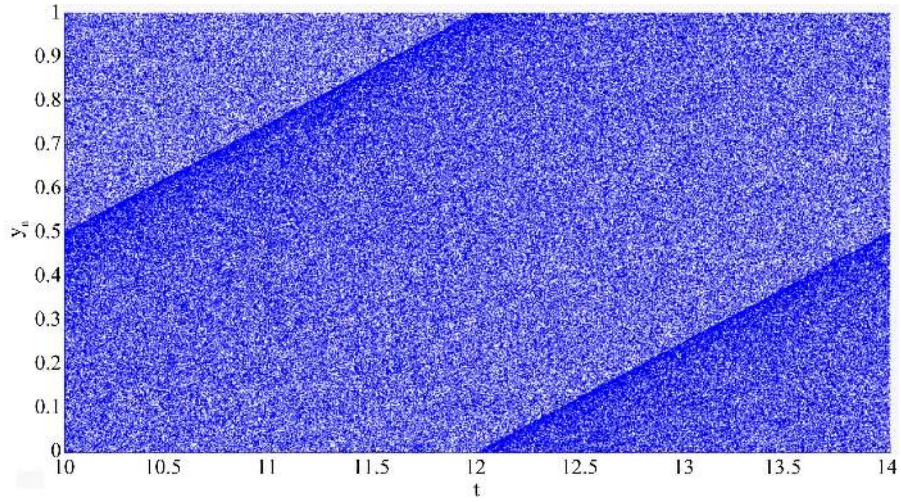

Figure B9. TCM chaotic map bifurcation diagram with $t \in [10, 14]$.

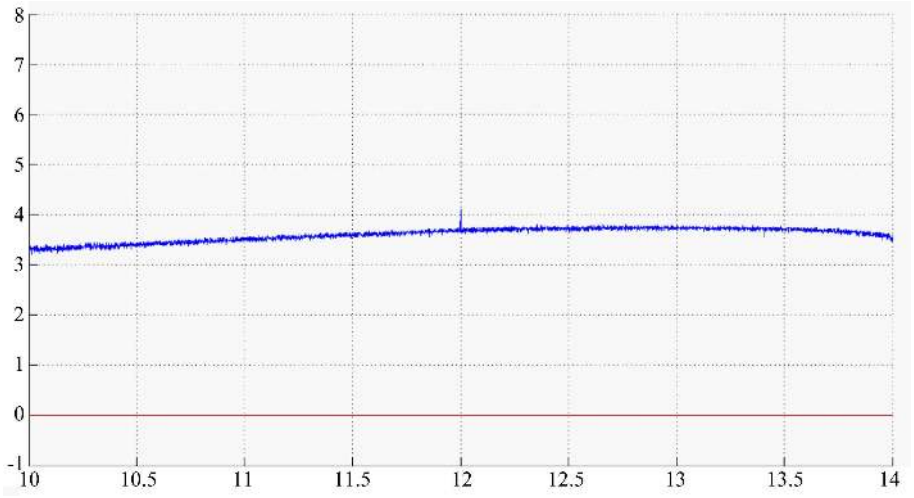

Figure B10. Lyapunov exponent of TCM chaotic map with $t \in [10, 14]$.