Pseudo-Random Number Generation Based on Generalized Delayed Logistic Map

Samar M. Ismail[1], Lobna A. Said[1], A. G. Radwan[2,3], A. H. Madian[3,4], M. F. Abu-ElYazeed[5]

[1]Faculty of IET, German University in Cairo (GUC), Egypt.
[2]Dept. of Engineering Mathematics and Physics, Cairo University, Egypt.
[3]NISC Research Center, Nile University, Cairo, Egypt.
[4]Radiation Engineering Dept., NCRRT, Egyptian Atomic Energy, Authority.
[5]Electronics and comm. Eng. Dept., Cairo University, Egypt.

Abstract

A pseudo-random sequence generator is a basic block in image encryption algorithms. Logistic maps are recently used for pseudo-random number generation because of their randomness, yet deterministic and easily reproducible. The generalization of a delayed version of the logistic map is presented in this paper. The addition of two general parameters offers the option of having three different maps; vertical, zooming and general map. The dynamic behavior of the proposed maps is analyzed. The study of the fixed points, stability ranges and bifurcation diagram of the delayed logistic map at hand is detailed in this work. The flow of the system behavior from stability to chaos is also presented with its transient response as well as its phase plane portraits. The use of these general parameters offers the option of designing any specific map. This is validated by some design examples. Moreover, the added general parameters offer increased randomness with controllability of the map design, making it more suitable for designing pseudo-random sequence generators.

1. Introduction

Chaotic systems have been of great interest for many researchers in the past few decades. Such systems are known to be sensitive dependent on their initial conditions. Any parameter small perturbation can cause different responses of the system. Some of these systems are continuous while others are shown in a discrete form. Of the most well-known discrete forms is the logistic map [1].The iterated logistic maps have proved great importance in both the modeling and information processing in many fields. Examples of such fields are population biology [2], chemistry [3], encryption [4], communication [5] and ecology [6]. They are also used to model the dynamics of a single species, for example the dynamics of tumor cells [7]. There has been a lot of work studying the stability and bifurcation of the logistic map, but mostly the conventional continuous or discrete logistic models without delays. Time delays offers a better description of real processes [8]. The stability and bifurcation of the discrete time Cohen-Grossberg neural networks with delays was studied in [9], while the stability and bifurcation for a discrete-time model of Lotka-Volterra type with delay was studied in [10], also, the Neimark-Sacker bifurcation in delayed logistic map in [11].

Hutchinson is considered to be the first ecologist to investigate the role of explicit delays in ecological models in 1948 [6]. He studied the differential-delay logistic equation with delay T. This equation can be described as follows: $(dx/dt) = x(t)\big(1 - x(t - T)\big)$. In this equation, it is assumed that the density of species at time t depends on their density at an earlier time by a delay of T. A lot of ecologists as well as mathematicians are interested in Hutchinson's work, the delay differential equations ever since.

The reproductive rate r may depend not only on the population density at the present time, but also on the population density in the past. In modeling seasonally breeding populations whose generations do not overlap, it is sufficient to keep track of the population once every generation [12]. Thus, the change in the population can be expressed with a difference equation of the form $x_{n+1} = R$, where x_n is the population size of the n^{th} generation and R is the reproductive rate. Now, following the assumption in [12], r can be written as $R = r(1 - x_{n-1})$. Hence, a discrete version of the delay differential equation is introduced in [12] as follows:

$$x_{n+1} = rx_n(1 - x_{n-1}) \tag{1}$$

Where the variables x_{n+1}, x_n and x_{n-1} is the density of population at generation $n + 1$, n and $n - 1$, respectively. The intrinsic growth rate of the population is symbolized by the parameter r.

This equation is like the famous logistic map except that the factor regulating the population growth contains a time delay of one generation. To follow the rate of a population, the density of the first two generations must be known. Equation (1) is called the delayed version of the logistic map. Such equation is proved to be of such a great interest to researchers as shown in [13-14].The dynamics of this model will be discussed as the value of this valuable parameter r is varied. Studying the behavior of this system as r increases, it is found that a smooth invariant circle transforms itself into a strange attractor. Investigating when the circle loses its integrity, no unique parameter value is found to divide the normal behavior to a strange one. On the contrary, parameter intervals are discovered for which the attractor transforms itself. This is to be discussed in details later on.

This paper is organized as follows: Section 2 introduces the generalization of the delayed logistic map. The dynamics of generalized map including the fixed points and the stability analysis are discussed in section 3. Section 4 presents two special case of the proposed delayed logistic map which are zooming with constant area with parameter b=1, and the other case which is the vertical scaling map. Different design problems for the generalized map are presented in section 5, to validate the flexibility and generality provided the added two parameters (a, b). Finally, section 6 concludes the work.

2. Generalized delay Logistic Map

The generalization of the conventional logistic map and the design of this map under certain constraints, is introduced in [15]. Adopting this idea of generalization, we propose the generalized form of the delayed logistic map as follows:

$$x_{n+1} = rx_n(a - bx_{n-1}) \quad (2)$$

where a & b are the generalization parameters. First, the generalized case is discussed where a, $b \in R^+$, then two special cases a=1 & b=1, are investigated. The analysis of the proposed map with its fixed points, range, and the bifurcation diagrams where $r \in R^+$, are presented with respect to all system parameters.

Special applications such as communication security including the transfer of images and the copyright of original pictures aroused a unique field of research. A lot of effort was exerted in this topic over the past decades to modify traditional image encryption algorithms. One of the mostly used schemes for encryption is based on chaotic signals. The characteristics of chaotic systems have made them most favorable in the field of information security for their sensitivity to initial conditions and control parameters, ergodicity, randomness and unpredictability, yet deterministic and easily reproducible. All these properties made chaotic systems most suitable in the security of communications transmission [4] as well as encryption [16]. These characteristics have encouraged a lot of cryptographers to develop new encryption algorithms. A cryptosystem is an algorithm used to transform an original message, known as plain text into a scrambled message, known as cipher text and then the message is recovered back to its original form. The process of transforming the plain text to the cipher text is known as the encryption process, and reversing the operation is called the decryption process. Both ways are controlled by a key stream, using a pseudo-random sequence generator to produce the cipher text.

Among all the chaotic systems, referring to the previously mentioned logistic map random characteristics and its easy way of implementation, it is most widely used to generate pseudo-random bit sequences [16-18]. Some research proposed methods to modify the logistic map for this purpose, such as mixing two or more logistic maps [19], or using a parameter-varied logistic map, or proposing a different kind of pseudo-random bit generator based on varying time-delayed logistic map [20].

In order to improve the security of logistic map-based pseudo-random bit generator, in this paper, a kind of pseudo-random bit generator based on generalized time-delayed logistic map is proposed. The extra added general parameters into the original map add more control, give wider range of randomness and provide more secure key streams suitable for pseudo-random bit generators. Possible generalization of mixed logistic maps for cryptanalysis techniques for pseudo-random sequence generation can be an open subject for future work.

3. Dynamics of the generalized map

This section describes the dynamics of the map which includes its fixed points, periodic attractors and the range r and the maximum value of the function x_{max}, the bifurcation point r_b,as well as the value of the function at the bifurcation point x_b.

For the ease of mathematical analysis of (2), it is converted to a system of first order equations (3). A new variable is introduced to be $y_{n+1} = x_n$.

Now, the difference equations (2) can be expressed as the following pair:

$$\begin{aligned} x_{n+1} &= rx_n(a - by_n) \\ y_{n+1} &= x_n \end{aligned} \quad (3)$$

For this pair of first order system of nonlinear equations, obtaining the Jacobian matrix J(p) at the fixed points p of such system as it is the way of linearization of these equations in the vicinity of its fixed points. Studying the stability of the fixed points, one should obtain the eigenvalues λ first. According to λ, one can confirm the stability of the fixed point. If the magnitude of each eigenvalue λ is less than 1, then p is a sink, else then p is a source.

3.1. Fixed points

The fixed points are calculated by $f(x,y) = (x,y)$, hence $x^* = rx^*(a - by^*)$ &$y^* = x^*$,where the fixed points of the 2D-map are:

$$(x^*, y^*) = (0,0) \;\&\; \left(\frac{a}{b} - \frac{1}{br}, \quad \frac{a}{b} - \frac{1}{br}\right) \quad (4)$$

The Jacobian matrix:

$$J = \begin{bmatrix} r(a - by) & -brx \\ 1 & 0 \end{bmatrix} \quad (5)$$

The Jacobian matrix is calculated for each fixed point, then the eigen values $|J - \lambda I| = 0$ are extracted for each Jacobian matrix. The first fixed point $(0,0)$:

$J = \begin{bmatrix} ra & 0 \\ 1 & 0 \end{bmatrix}$ and the eigen values are $\lambda_1 = 0$, $\lambda_2 = ra$.

3.2. Stability Analysis

From the stability criteria, the origin is asymptotically stable as long as $0 < r < 1/a$.

For the second fixed point $\left(\frac{a}{b} - \frac{1}{br}, \frac{a}{b} - \frac{1}{br}\right)$:

$J = \begin{bmatrix} 1 & 1 - ar \\ 1 & 0 \end{bmatrix}$ and the eigen values are $\lambda_{1,2} = \frac{1}{2} \pm \sqrt{(5/4) - ar}$.

So, from the stability criteria, the fixed point is asymptotically stable if $(1/a) < r \leq (5/4a)$ and the eigen values are complex conjugates for $r > (5/4a)$, to maintain stability $|\lambda_1| = |\lambda_2| < 1$, which happens at $r < (2/a)$, where which the bifurcation occurs at $r_b = (2/a)$. For $r > (2/a)$, it is unstable. Table 1 discusses the range of r for stable and unstable behaviors. Table 2 illustrates the system transient response for 150 iterations and the phase plane portraits for different values of r, with a=1, which matches with Table 1. For r = 0.8 shown in Table 2, part I, the origin is stable and the second fixed point is unstable and the system behavior is monotone approach to the origin. For r= 1.1, in part II, the first fixed point lost its stability , while the second fixed point is asymptotically stable with real eigenvalues, and the system shows monotone approach towards the second fixed point. While, for part III, r= 1.8, the second fixed point is stable with complex eigenvalues and the solutions start near it exhibit damped oscillations while approaching the second fixed point. For r = 2.1, part IV, both fixed points have lost their stability and they show oscillations as illustrated in Table 2.

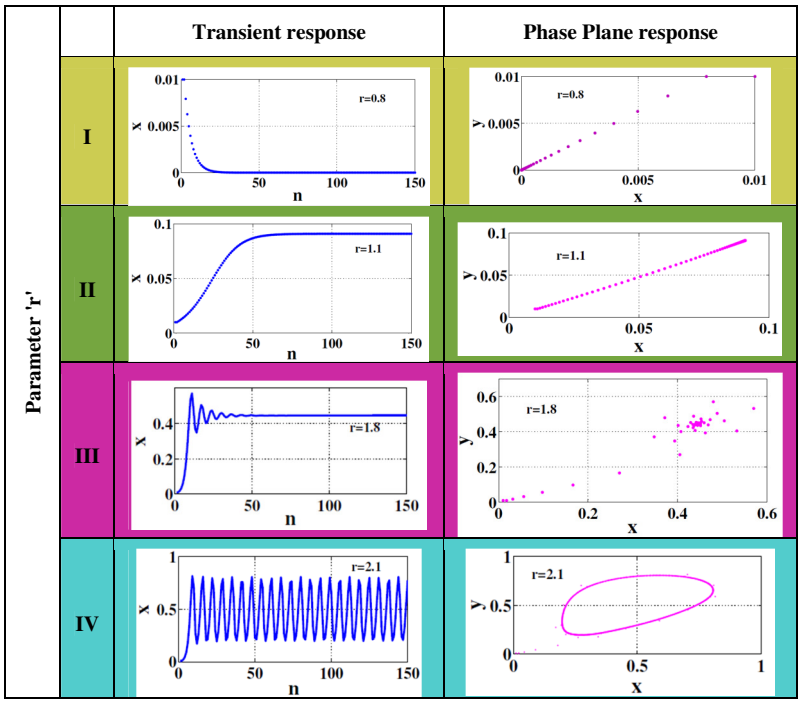
The dynamics of the delayed logistic map undergo complicated variations with respect to r. However, the phase plane reveals lots of its features. Figure 1 shows the phase plane with different values of r where in the case the eigenvalues are complex conjugate and of unit moduli. As r increases, the eigenvalues move off the unit circle, the generic result is that the appearance of closed invariant curve in the phase plane portrait. Inspecting the different graphs flow of Fig.1, it can be seen that attractor transforms itself as r increases as specially described in Fig.1(c), till r=2.27, after which the system turn chaotic with no special pattern to be shown as it is clear in Fig.1(d).

In one parameter families, like the conventional logistic map, the transition from simple to chaotic behavior is quite complicated. An effective way to follow the visible attractors as the parameter r is increased is to generate a bifurcation diagram. For a precise statement of this bifurcation, the delayed logistic map undergoes Poincare-Andoronov-Hopf Bifurcation as the parameter passes through r = 2. Using such diagrams, the effect of the generalization parameters a and b, added to the normal delayed logistic map (4) is illustrated.

Table 1. Summary of stability versus r

	Range of *r*	**First fixed point** (0,0)	**Second fixed point** $(\frac{a}{b}-\frac{1}{br},\frac{a}{b}-\frac{1}{br})$	**System Behavior**
I	$\mathbf{0 < r < \frac{1}{a}}$	stable	unstable	Real eigen values, Monotone approach to (0,0)
II	$\mathbf{\frac{1}{a} < r < \frac{5}{4a}}$	unstable	stable	Real eigen values, Monotone approach to the second fixed point
III	$\mathbf{\frac{5}{4a} < r < \frac{2}{a}}$	unstable	stable	complex eigenvalues, Damped oscillations
IV	$\mathbf{\frac{2}{a} < r < \frac{2.27}{a}}$	unstable	unstable	complex eigenvalues, Bifurcate till reaching chaos

Table 2. Transient response and Phase plane of different ranges of r for a=1, for 150 iterations



The function value at the bifurcation point x_b is calculated by substituting with the values of r_b , x^*, y^*in the 2D map which yields, $x_b = (a/2b)$ While the maximum value of the function is calculated as follows: $rx(a - by) > 0$ so $x > 0$ & $y < (a/b)$ and hence $x_{max} = (a/b)$. In next section, two special cases a=1 & b=1, are displayed, followed by a design section of the general case with both a and b parameters have values.

4. Special Maps

4.1. The zooming with constant area delayed logistic map b=1

The zooming map is described by:

$$x_{n+1} = rx_n(a - y_n)$$
$$y_{n+1} = x_n \qquad (6)$$

Where the parameter b, is set into 1 in the general map (3), with r & a are the controlling parameters of the map.

The fixed points of this map are equal to:

$$(x^*, y^*) = (0,0) \;\&\; \left(a - \frac{1}{r},\; a - \frac{1}{r}\right) \qquad (7)$$

Figure 2 shows the bifurcation diagram of the zooming map, for different values of a. As shown in the figure, the value of the parameter a affects the vertical axis parameters x_{max} , $x_b$as well as the horizontal axis parameters r_{max} and r_b, verifying that the effect of a is a zooming effect on the map. The relations binding all the map parameters with the variable parameter a is summarized in Table 3.

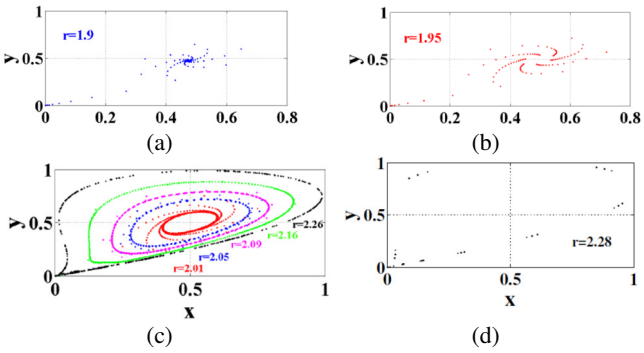


Fig. 1. Phase plane portraits for different $1.8 < r < 2.3$.

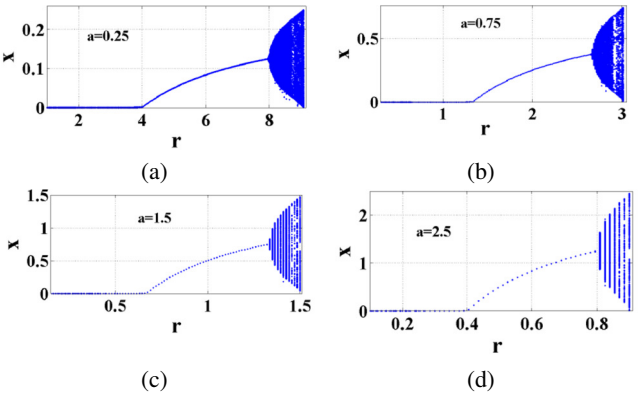


Fig. 2. Bifurcation diagrams for the zooming map.

4.2. The vertical scaling map a=1

The vertical scaling map is described by:

$$\begin{aligned} x_{n+1} &= r x_n (1 - b y_n) \\ y_{n+1} &= x_n \end{aligned} \qquad (8)$$

Where the parameter a, is set into 1 in the general map (3), with r& b are the parameters controlling the map.

Figure 3 show the bifurcation diagram of the vertical scaling map, for different values of b. As shown in the figure, the value of the parameter b only affects the vertical axis parameters x_{max} , x_b. It has no effect on the horizontal axis parameters r_{max} and r_b. Table 3 summarizes the relations binding up all the map parameters with the variable parameter b. Figure 4 is the 3D representation of the bifurcation diagrams versus the control parameters a for the zooming map as shown in Fig.4(a) and versus the control parameter b for the vertical scaling map in Fig.4(b).

5. Design of the generalized delayed logistic map

In this section, the design of a logistic map with predetermined parameters is investigated. According to the equations previously derived, one can specify the place of the bifurcation point r_b , the function value at which the bifurcation x_b takes place, the maximum value of the function x_{max}, at r_{max} , Table 3 discuss the relation between the design parameters, while Table 4 illustrates the different design problems chosen. Four design cases are studied, the required logistic map specifications are set, and using the equations derived in section II, the generalized map parameters (a,b) are calculated. Fig.5 shows the bifurcation diagrams of each design problem according to Table 4.

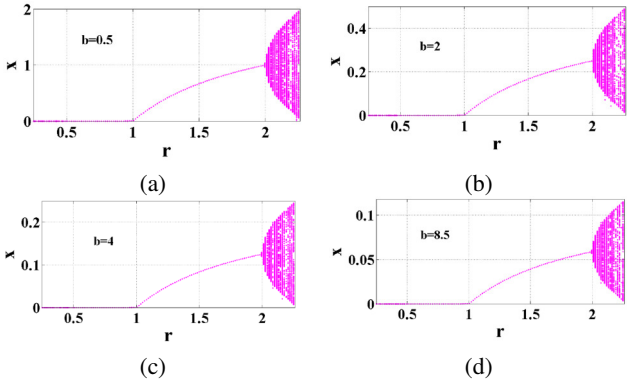


Fig.3. Bifurcation diagrams for the vertical scaling map.

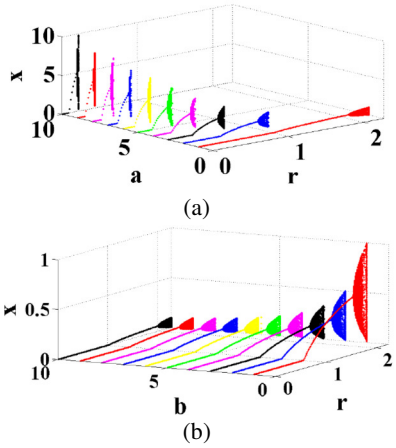


Fig.4. 3D-bifurcation diagram for (a) the zooming map (b=1), (b) the vertical scaling map (a=1).

6. Conclusion

In this paper, a generalization of the delayed logistic map is proposed. The effect of the generalization parameters a and b, is illustrated in the map. A general map is analyzed, then two special cases are introduced which are the vertical scaling map and the zooming map. The dynamics of the proposed maps is studied with respect to their stability and bifurcation points, as well as the different behaviors of the system from stability to

chaotic regions. Then, different designs are shown possible altering all the parameters proposed, showing the flexibility of the map design to fit for any specific application. The proposed general delayed map is more suitable for pseudo-random sequence generators which are used in image encryption algorithms and in secure communication transfer. Possible generalization of mixed logistic maps for cryptanalysis techniques for pseudo-random sequence generation can be an open subject for future work.

Table 3. Summary of all the design parameters for all the proposed logistic maps.

Parameters	General Map	Vertical Map	Zooming Map
$\mathbf{x_{max}}$	$\frac{a}{b}$	$\frac{1}{b}$	a
$\mathbf{x_b}$	$\frac{a}{2b}$	$\frac{1}{2b}$	$\frac{a}{2}$
$\mathbf{r_{max}}$	$\frac{2.27}{a}$	2.27	$\frac{2.27}{a}$
$\mathbf{r_b}$	$\frac{2}{a}$	2	$\frac{2}{a}$

Table 4. Design cases of the delayed logistic map.

	Required design	Equivalent parameters $(\mathbf{a}, \mathbf{b})$
Design a	$\mathbf{r_b = 2, x_{max} = 8}$	(1, 0.1250)
Design b	$\mathbf{r_{max} = 4, x_{max} = 15}$	(0.5675, 0.0378)
Design c	$\mathbf{r_b = 4, x_b = 6}$	(0.5, 0.0417)
Design d	$\mathbf{r_{max} = 2, x_b = 3}$	(1.1350, 0.1892)

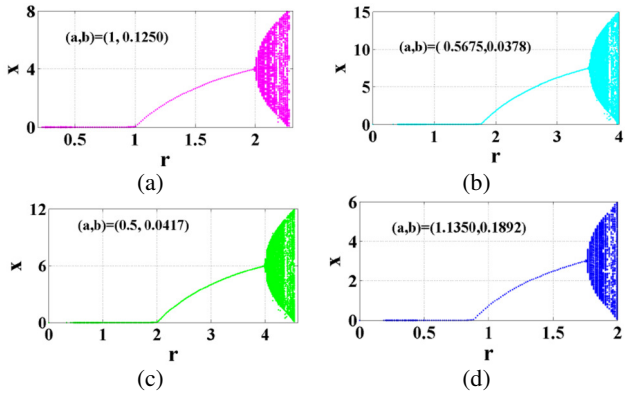


Fig. 5. Bifurcation diagrams versus r for the design problems in Table 4.

7. References

[1] M. Ausloos and M. Dirickx,"The logistic map and the route to chaos from the beginnings to modern applications", Springer, 2006.

[2] T. Kinnunen and H. Pastijn,"The chaotic behavior of growth Processes", *ICOTA*,1987.

[3] K. Malek and F. Gobal,"Application of chaotic logistic map for the interpretation of anion-insertion in poly-ortho-aminophenol films", *Synthetic Metals*,vol.113,pp.167-171,2000.

[4] 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.

[5] 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.

[6] G. E. Hutchinson, "Circular casual systems in ecology", *Annals of the New York Academy of Sciences*, vol. 50, pp. 221-246, 1948.

[7] J. C. Panetta, "A logistic model of periodic chemotherapy with drug resistance", *Applied Mathematics Letters*, vol. 10, no. 1, pp.123–127, 1997.

[8] M. Bodnar and U. Forys, "Three types of simple DDE's describing tumour growth", *Journal of Biological Systems*, vol. 15, no. 4, pp. 1–19, 2007.

[9] Q.Liu, R.Xu, and Z.Wang, "Stability and bifurcation of a class of discrete-time Cohen-Grossberg neural networks with delays", *Neural Processing Letters*, vol. 40, no. 3, pp. 289-300, 2014.

[10] W. Han and M. Liu, "Stability and bifurcation analysis for a discrete-time model of Lotka-Volterra type with delay", *Applied Mathematics and Computation*, vol. 217, no. 12, pp. 5449–5457, 2011.

[11] H. Sarmahi, M. Chandra and T. Baishya, "Neimark-Sacker bifurcation in delayed logistic map", *International Journal of Applied Mathematics & Statistical Sciences*, vol. 3, no. 1, pp.19-34, 2014.

[12] J. Maynard-Smith, " Mathematical Ideas in Biology", Cambridge University Press, 1968.

[13] D. Wu, H. Zhang, J. Cao and T. Hayat, "Stability and Bifurcation Analysis of a Nonlinear Discrete Logistic Model with Delay", *Discrete Dynamics in Nature and Society*, 2013.

[14] J. Arino, L. Wang and G. S. K. Wolkowicz, "An alternative formulation for a delayed logistic equation", *Journal of Theoretical Biology*, vol. 241, pp.109 - 119, 2006.

[16] A. G. Radwan, "On some generalized discrete logistic maps, ", *Journal of Advanced Research* , vol.4, pp. 163-171, 2013.

[17] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm", *Physics Letters*, vol.A 289, pp. 199–206, 2001.

[18] D. Sunder Swami and K. Kumar Sarma, "A Chaos based PN Sequence Generator for Direct-Sequence Spread Spectrum Communication System", *International journal of circuits, systems and signal processing*, vol. 8, 2014.

[19] R. Senkerik, M. Pluhacek, Ivan Zelinka and Zuzana Kominkova Oplatkova, "Utilization of the Discrete Chaotic Systems as the Pseudo Random Number Generators", *Advances in Intelligent Systems and Computing*,vol.285,pp 155-164, 2014.

[20] A. Kanso and N. Smaoui , "Logistic chaotic maps for binary numbers generations", *Chaos, Solitons and Fractals*, vol.40, pp.2557–2568, 2009.

[21] L. Liu, S. Miao, H. Hu and Y. Deng, "Pseudorandom bit generator based on varying time-delayed logistic map", *Applied mechanics and materials*, vols. 513-517, pp. 1727-1730, Switzerland, 2014.