Data Encryption Based on Generalized Fractional 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

Logisitic maps are recently used in the generation of secret keys for data encryption. This paper presents a generalized form of the fractional logistic map. Two general parameters a and b are added to the classical fractional logistic equation. The combination of the added extra parameters a and b in addition to the system parameter ρ and the initial condition x_0, as well as the fractional order parameter α makes the proposed generalized fractional logistic map the most favorable in constructing more efficient encryption keys. The effect of such parameters with the fractional order parameter α offers an extra degree of freedom increasing the design flexibility and adding more design controllability. The vertical and the zooming map are two special maps that arise as a result of the added parameters. Moreover, some design problems are presented in this work. This shows that any application specific map can be designed, highlighting the flexibility and integrity of the map design.

1. Introduction

Chaotic systems have been able to catch the eye of so many researchers in the past few decades. A very well-known example of discrete chaotic systems is the iterated logistic map [1, 2]. Such maps have proved great importance in both the modeling and information processing in many fields such as population biology [3], medical applications [4], communication [5], and encryption [6].

The fractional calculus has allowed the operations of integration and differentiation to be used in wide spread applications rather than being restricted to integer order only. Recently, fractional-order differential equations have been of great interest to many researchers in many areas of science and engineering [7]. Such equations are widely studied by analytical and numerical methods. Inspired by the discretization of the Riemann-Liouville and the Caputo operators, the fractional difference equations is a relatively new field to tackle. Some research recently introduced the fractional discrete derivatives as in [8-9], offering great opportunities to study the dynamics of such discrete systems powerfully, as well as their chaotic behaviours.

Several studies concerning the discretization of the fractional logistic map and its chaotic behavior are studied in [10-13]. A method of generalizinig logistic equations is introduced in [14-15], by adding general parameters which affect the logistic map greatly. Similarly, this work presents the generalization of the discrete fractional logistic map exploring the effects of the extra general parameters added to the equation in combination with the extra degree of freedom offered by the fractional order parameter α.

This paper is organized as follows: Section 2 introduces the fractional order logistic map. The proposed generalized fractional logistic map is discussed in section 3, where the generalized derivations of the fixed points and stability analysis of the proposed map is analyzed. The two new special maps are also discussed in section 3. Section 4 offers different design problems of the proposed maps. Section 5 concludes this work.

2. Fractional order logistic map

The fractional calculus is the generalization of integer calculus. This leads to similar concepts with wider generality and applicability. The fractional calculus allowed the operations of integration and differentiation to be applied upon any fractional-order.

The basic definition of the Riemann-Liouville notation of fractional integral of order $\alpha > 0$ is given by:

$$J^{\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_0^t (t-\tau)^{\alpha-1}\ f(\tau) d\tau \tag{1}$$

where J^{α} represents the fractional integral operator of order $\alpha \in R^{+}$, $f(t)$ is a causal function and Γ is the gamma function.

The fractional order parameter α adds extra degree of freedom which increases the design flexibility and adds more control on design.

The discretization process can be explained as follows:

Consider the fractional-order logistic differential equation given by:

$$D^{\alpha} x(t) = \rho x(t)\big(1 - x(t)\big), \qquad t > 0 \tag{2}$$

Where $x(0) = x_o$ is the initial condition.

The study of chaotic behavior of logistic equations with piecewise constant arguments is discussed in [16-18]. The process of discretization with piecewise constant arguments is shown as:

$$D^{\alpha} x(t) = \rho x\left(\left[\frac{t}{r}\right] r\right) \left(1 - x\left(\left[\frac{t}{r}\right] r\right)\right) \tag{3}$$

Where $x(0) = x_o$ is the initial condition.

The steps of the discretization process used in this work is detailed in [10], reaching the final discrete fractional logistic equation (4) , where α is the fractional-order parameter.

$$x_{n+1} = x_n + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho x_n (1 - x_n) \quad (4)$$

3. Generalized discrete fractional logistic map

The fractional logistic equation (4) is proposed in [10], whereas a general study of the logistic map and how to design this map under certain constraints, is introduced in [15,16].

The proposed general fractional logistic equation is:

$$x_{n+1} = x_n + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho x_n (a - b x_n) \quad (5)$$

Where (a,b) are the generalization parameters. First, the general case is discussed then two special cases are displayed. The two cases are for (a,1),(1,b),where a, $b \in R^+$. The next section will introduce the three proposed maps with their fixed points, range, and the bifurcation diagrams with respect to all system parameters.

3.1. Generalized Derivations

The general logistic map is to be analyzed (5), having r, ρ, α, a and b as parameters. Having $f(x, r, \rho, \alpha, a, b)$, let us define the range ρ and the maximum value of the bifurcation x_{max}, the bifurcation point ρ_b, as well as the value of the function at the bifurcation point x_b.

3.1.1. Fixed points

The fixed points of the map are defined as the points where $x^* = f(x^*, r, \rho, \alpha, a, b)$.

$$x^* = x^* + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho x^* (a - b x^*) \quad (6)$$

Therefore, $\rho x^*(a - b x^*) = 0$. This gives two fixed points which are $x_1^* = 0$ and $x_2^* = a/b$.

3.1.2. Range of ρ

Discussing the positive side of the bifurcation diagram, x_n is positive for all iterations, that is

$$x_n + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho x_n (a - b x_n) > 0 \quad (7)$$

Putting $k = r^\alpha \rho / \Gamma(1+\alpha)$,

$$x_n < \frac{a}{b} + \frac{1}{bk} \quad (8)$$

therefore $x_n \in [0, \frac{a}{b} + \frac{1}{bk}]$ indicating that

$$x_{max} = \frac{a}{b} + \frac{1}{bk} \quad (9)$$

The critical point x_c is the point at which there will the function has a maximum, it is calculated by solving the derivative of the function $dx_{n+1}/dx_n = 0$, i.e.

$$\frac{dx_{n+1}}{dx_n} = 1 + k(a - 2bx_c) = 0 \quad (10a)$$

This gives the value of x_c to be:

$$x_c = \frac{a}{2b} + \frac{1}{2bk} = \frac{x_{max}}{2} \quad (10b)$$

Substituting by x_c in (5):

$$f(x_c, r, \rho, \alpha, a, b) = \frac{a}{2b} + \frac{1}{4bk} + \frac{a^2 k}{4b} \quad (11a)$$

This value should be less than $x_{max} = \frac{a}{b} + \frac{1}{bk}$,

$$\frac{a}{2b} + \frac{1}{4bk} + \frac{a^2 k}{4b} < \frac{a}{b} + \frac{1}{bk} \quad (11b)$$

Neglecting the negative term, $k < \frac{3}{a}$.

Substituting by the value of k gives an inequality for ρ:

$$\therefore \rho < \frac{3\Gamma(1+\alpha)}{a\, r^\alpha} \quad (12)$$

Therefore, $(x_{max}, \rho_{max}) = (\frac{a}{b} + \frac{1}{bk}, \frac{3\Gamma(1+\alpha)}{a\, r^\alpha})$.

3.1.3. Stability conditions

Stability is studied at the fixed points of the map. This is done by finding the first derivative of the function. The fixed points will be stable if $|f'(x^*, r, \rho, \alpha, a, b)| < 1$, and will be a saddle point if $|f'(x^*, r, \rho, \alpha, a, b)| > 1$.
Finding the first derivative of the function.

$$f'(x_n, r, \rho, \alpha, a, b) = 1 + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho (a - 2bx_n) \quad (13)$$

At $|f'(x^*, r, \rho, \alpha, a, b)| = 1$, at the fixed points, this is where bifurcation takes place.

At $x_1^* = 0$, $|f'(x^*, r, \rho_b, a, b)| = \left|1 + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho_b a\right| = 1$, i.e. $-2 < (r^\alpha \rho_b a / \Gamma(1+\alpha)) < 0$,which is out of our studied range. At $x_2^* = \frac{a}{b}$, $|f'(x^*, r, \rho_b, a, b)| = \left|1 + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho_b (a - 2b\frac{a}{b})\right| = 1$,i.e. the map will bifurcate at $-2 < -ka < 0$, i.e. $0 < k < \frac{2}{a}$.

$$\therefore 0 < \rho_b < \frac{2\Gamma(1+\alpha)}{a r^\alpha} \quad (14)$$

Substituting with this value of ρ_b, yields x_b ,the function value at the bifurcation point.

Now, two special cases are to be discussed. The first one, when a=1 , and the second case is when b=1.

3.2. Vertical Scaling Map:

As shown in the vertical scaling map equation (15),we set the parameter $a = 1$,in (5), and we have r, b, ρ and α as parameters.

$$x_{n+1} = x_n + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho x_n (1 - b x_n) \quad (15)$$

Following the same steps done in section 3.1, and substituting for a=1, we get the following equations for fixed points, range of ρ and the stability conditions.

There are two fixed points which are $x_1^* = 0$ and $x_2^* = 1/b$.

$$x_{max} = \frac{1}{b} + \frac{1}{bk} \quad (16)$$

$$x_c = \frac{1}{2b} + \frac{1}{2bk} \qquad (17)$$

$$\rho < \frac{3\Gamma(1+\alpha)}{r^{\alpha}} \qquad (18)$$

Therefore, $(x_{max}, \rho_{max}) = \left(\frac{1}{b} + \frac{1}{bk}, \frac{3\Gamma(1+\alpha)}{r^{\alpha}}\right)$.

$$0 < \rho_b < \frac{2\Gamma(1+\alpha)}{r^{\alpha}} \qquad (19)$$

Figure 1 shows the bifurcation diagrams of (15) versus ρ, for different values of α and b. The figures show how α affects the shift of bifurcation point ρ_b according to (19) with fixed value of b, with different values of $\alpha = 0.6$ and 0.8. While for fixed value of $\alpha = 0.5$,with different values of b, as shown in Fig.2, the effect of b on the vertical scaling of the map is shown, according to (18), where x_{max} is inversely proportional to b.

Figure 3 shows the bifurcation diagrams of (15) versus α for fixed $\rho = 3.7$, and different values of b. Figure 4 shows the changes of of ρ_{max} and ρ_b versus α, for fixed $r = 0.25$. Taking $\alpha = 0.8$ as an example, for r=0.25, $\rho_{max} = 8.47$ and $\rho_b = 5.647$, as confirmed by Fig.1(c) & (d).

How x_{max} behaves versus b is shown in Fig. 5, according to (16). This proves that b controls the vertical scaling of the bifurcation diagram by controlling the value of x_{max}. Taking Fig.2(a) as an example, where b=0.25, we can find that $x_{max} = 5.33$.with increasing b to 4, as in Fig.2(b), the value of x_{max} decreased to 0.3299. Comparing Fig.1 (a)&(c) and Fig.1 (b)&(d) it is so clear that changes in the value of b only affects the vertical scaling of the map, with no changes in the horizontal axis. Ten snapshots of bifurcation diagrams are plotted versus ρ for fixed b=5 , in Fig.6 (a), and versus b for fixed $\alpha = 0.4$, in Fig.6 (b).

3.3. Zooming map

Equation (20) describes the other special case where b=1 in (5), and we have r, a, ρ and α as parameters.

$$x_{n+1} = x_n + \frac{r^{\alpha}}{\Gamma(1+\alpha)} \rho x_n (a - x_n) \qquad (20)$$

Following the same steps done in section 3.1, and substituting for a=1, we get the following equations for fixed points , range of ρ and the stability conditions.

The two fixed points for this case are $x_1^* = 0$ and $x_2^* = a$.

$x_n \in [0, a + \frac{1}{k}]$ indicating that

$$x_{max} = a + \frac{1}{k} \qquad (21)$$

$$x_c = \frac{a}{2} + \frac{1}{2k} \qquad (22)$$

$$\rho < \frac{3\Gamma(1+\alpha)}{a\, r^{\alpha}} \qquad (23)$$

Therefore, $(x_{max}, \rho_{max}) = \left(a + \frac{1}{k}, \frac{3\Gamma(1+\alpha)}{a\, r^{\alpha}}\right)$.

We also have $\alpha < \frac{3}{k}$. Rendering a value of

$$a_{max} = \frac{3\Gamma(1+\alpha)}{\rho r^{\alpha}} \qquad (24)$$

$$0 < \rho_b < \frac{2\Gamma(1+\alpha)}{a r^{\alpha}} \qquad (25)$$

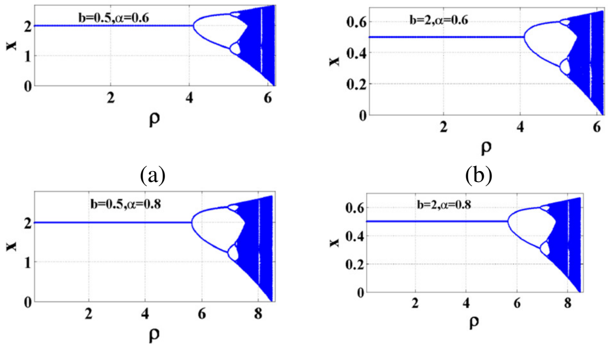


Fig.1. Bifurcation diagram x versus ρ at r=0.25.

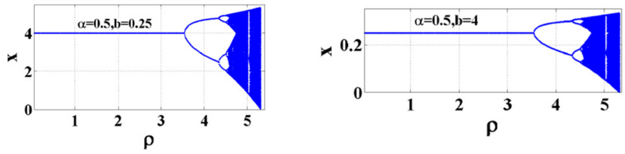


Fig.2. Bifurcation diagram x versus ρ at r=0.25.

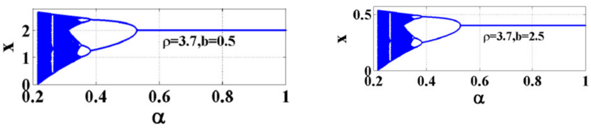


Fig.3. Bifurcation diagram x versus α at r=0.25, $\rho = 3.7$

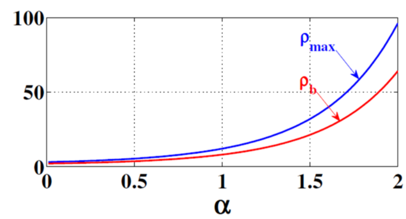


Fig.4. Changes of ρ_{max} and ρ_b versus α, for fixed r =0.25.

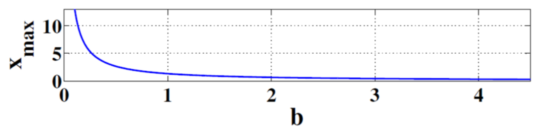


Fig.5. Changes of x_{max} versus b.

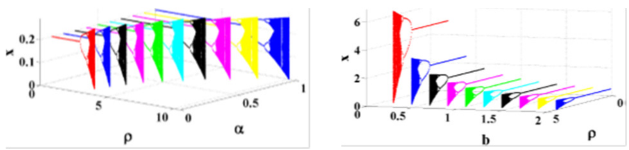


Fig.6. 3D Bifurcation diagrams x versus ρ, at $r = 0.3$,(a) versus α with $b = 5$, and (b) versus b with $\alpha = 0.4$.

Figure 7 (a) & (c) shows the bifurcation diagram of x versus ρ, for r=0.25,a=0.5,and initial condition =0.01 for different values of the fractional order $\alpha = 0.7$ and 0.9. While Fig.7 (b) & (d) shows the bifurcation diagram versus ρ for also r=0.25, with a=2, for the same values of $\alpha = 0.7$ and 0.9, to highlight the effect of a on the diagrams. It is clear that a has a horizontal shift effect on the bifurcation points, as it is inversely proportional to ρ_b (25), with also a vertical offset on the vertical axis as it appears as an added term in the values of x (21). So, the parameter a effect is like a general zooming effect on the map. Figure 8 illustrates the bifurcation diagram versus ρ with fixed parameters r=0.25, α =0.5 for different values of a ,while

Figure 9 (a) shows some snapshots of the bifurcation diagrams versus α for r=0.3 and a=2 for different values of ρ, while the bifurcation diagrams versus ρ for r=0.3, $\alpha = 0.4$ for different values of a are plotted in Fig. 9 (b).

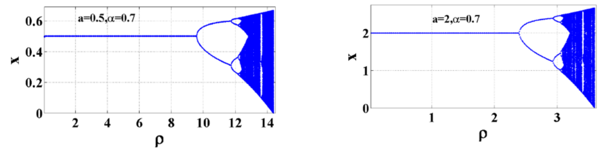
The changes of ρ_{max} and ρ_b versus a, for fixed $r = 0.25$ and fixed $\alpha = 0.7$ are shown in Fig.10(a).For example, for $a = 0.5$, $\rho_{max} = 14.39$ and $\rho_b = 9.592$,which agrees with the results shown in Fig.7(a). Also, for $a = 2$, the value of $\rho_{max} = 3.597$ and $\rho_b = 2.398$, which also coincides with the results shown in Fig.7 (b). Investigating Fig.10 (b), for $r = 0.25$ and $a = 2$, taking $\alpha = 0.9$, as an example, we find that $\rho_{max} = 5.024$ and $\rho_b = 3.349$, which agrees with the results depicted in Fig.7(d).

As shown in Fig. 11, x_{max} increases linearly with the parameter a, following the equation (21). Comparing Fig.11 with one of the graphs obtained previously, for example, Fig.8(a),where a=0.25,the value of x_{max} is found to be 0.346. Whereas,Fig.8(b),with increasing a to 2, x_{max} increases to 2.67. Combining this effect of a on x_{max},with the effect on a on ρ_{max} and ρ_b , explained in Fig. 10a, this proves that the parameter a has a vertical as well as horizontal scaling on the map calling it the zooming effect on the logistic map bifurcation diagram.

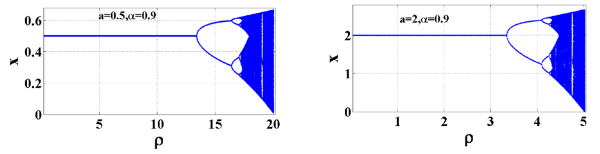
From the previous discussed two special cases, we are able to scale the bifurcation map with dependent axes by using an extra parameter, b for the first case, a for the second case, with the extra fractional order parameter α .

4. Design of the proposed map

In this section, different logistic maps are being designed showing the possibility of controlling the map parameters easily to fit any specific application. According to the equations previously derived, the place of the bifurcation point ρ_b and the value x_b , correspondingly, as well as the maximum value of the rate ρ_{max} and the corresponding maximum value of the function x_{max} are set. All these parameters can be specified and the general parameters a and b are to be calculated to realize the predefined parameters. The extra degree of freedom provided by the fractional order α gives the flexibility of achieving the designs at different values of α. Four design cases are illustrated in Table 1 as examples to the design flexibility provided. As an example to this, in the first design, the values of ρ_{max} and x_{max} are specified, and then the values of the parameters a and b are calculated fitting the specifications required. Figure 12, shows the bifurcation diagrams of each design problem in Table 1. Figure 13 is a graphical verification of the values of x_{max} specified in the first two designs in Table 1, where x_{max} relation with the parameters a and b is clarified. Whereas, the values of ρ_{max}andρ_b, throughout the designs are proven correct according to Fig.10.

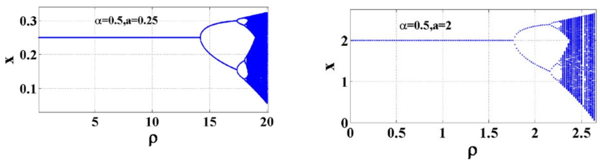


(a) (b)



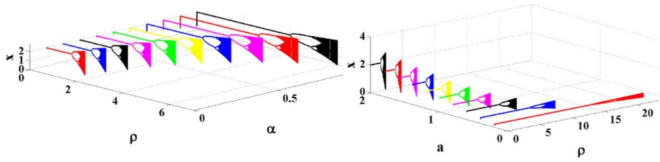
(c) (d)

Fig.7. Bifurcation diagram versus ρ for r=0.25 & a=0.5 & a=2 for different α.



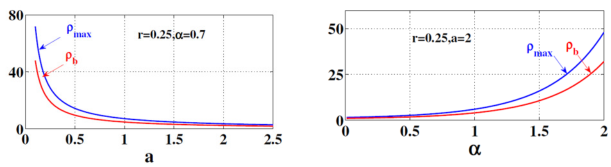
(a) (b)

Fig.8. The bifurcation diagram versus ρ for r=0.25, α =0.5.



(a) (b)

Fig.9. The 3D bifurcation diagram (a) x versus ρ versus α for r=0.3,a=2, (b) x versus ρ versus a for r=0.3, $\alpha = 0.4$.



(a) (b)

Fig.10. Changes of ρ_{max} and ρ_b (a) versus a , for fixed r and fixed α , (b)versus α, for fixed r and fixed a.

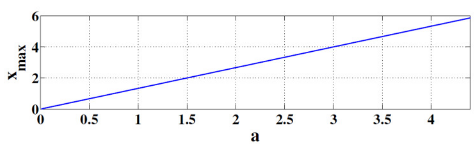


Fig.11. Changes of x_{max} versus a.

Table 1. Different design cases

	Required design	Equivalent parameters
Design 1	$\rho_{max} = 6, x_{max} = 10$	a=0.8862 , b= 0.1182
Design 2	$\rho_b = 3, x_{max} = 6$	a= 1.1816, b= 0.2626
Design 3	$\rho_{max} = 5, x_b = 3$	a= 1.2317, b=0.4106
Design 4	$\rho_b = 7, x_b = 7$	a= 0.8067 , b= 0.1152

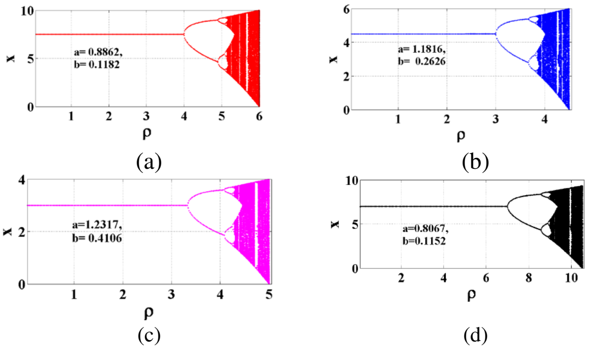


Fig.12. Bifurcation diagram versus ρ corresponding to Table 1.

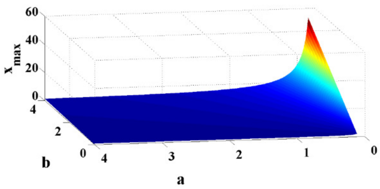


Fig.13. Relation of x_{max} versus a and b.

Chaotic maps are known of their high sensitivity on initial conditions, as well as being deterministic and easily reproducible. These characteristics made them very suitable for pseudorandom sequences generation, which are used in many applications such as data encryption [6,19]. Xoring the characters of the plaintext with the output sequence of the map produces what is called the ciphertext. The successive iterations of the chaotic system makes the ciphertext less dependent on the plaintext. The combination of the added extra parameters a and b in addition to the system parameter ρ and the initial condition x_0 , as well as the fractional order parameter α makes the proposed generalized fractional logistic map the most favorable in constructing more efficient encryption keys.

5. Conclusion

A generalization of the fractional logistic map is proposed in this work. The effect of the generalization parameters a and b, in scaling the map horizontally and vertically is shown. This scaling effect resulted in two types of maps, the vertical and the zooming map. The fractional order parameter α added an extra degree of freedom in the design of the proposed map. Some design examples are illustrated showing the controllability of the map as well as the design flexibility to fit any specific application such as data encryption. The mixing of the generalized parameters, the map parameter ρ and the initial condition x_0, as well as the fractional order parameter α offers a great variety for constructing more efficient encryption keys.

6. References

[1] S. Banerjee, "Dynamics for engineers," Wiley, 2005.
[2] M. Ausloos, M. Dirickx, "The logistic map and the route to chaos from the beginnings to modern applications," Springer, 2006.
[3] T. Kinnunen, H. Pastijn,"The chaotic behavior of growth Processes," *ICOTA*,1987.
[4] J. C. Panetta, "A logistic model of periodic chemotherapy with drug resistance," *Applied Mathematics Letters*, vol. 10, no. 1, pp.123–127, 1997.
[5] N. Singh, A. Sinha, "Chaos-based secure communication system using logistic map, " *Optics and Lasers in Engineering*,vol.48,no.3,pp.398–404,2010.
[6] N. K. Pareek, V. Patidar, K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*,vol.24, no.9, pp.926–934,2006.
[7] I. Podlubny, "Fractional Differential Equations," *Mathematics in Science and Engineering*, vol. 198,USA, 1999.
[8] F. M. Atici, P. W. Eloe, "Initial value problems in discrete fractional calculus," *American Mathemathical Society*, vol.137, pp.981–989, 2009.
[9] F. M. Atici, S. Senguel,"Modeling with fractional difference equations," *Journal of Mathematical Analysis and Applications*, vol. 369,no.1,pp. 1–9, 2010.
[10] Z. F. El Raheem, S.M. Salman , "On a discretization process of fractional order logistic differential equation," *Journal of the Egyptian Mathematical Society*, vol. 22,pp. 407–412, 2014.
[11] J. Munkhammar,"Chaos in a fractional order logistic map," *Fractional Calculus and Applied Analysis*, vol.16, no.3, pp.511–519, 2013.
[12] G. Wu, D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dynamics*, vol.75, no.1-2, pp.283–287, 2014.
[13] A. El-Sayed, A. El-Mesiry, H. EL-Saka," On the fractional-order logistic equation," *Applied Mathematics Letters*,vol. 20,pp.817–823, 2007.
[14] A. G. Radwan," On some generalized discrete logistic maps," *Journal of Advanced Research* ,vol.4,pp. 163–171.2013.
[15] 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*, 2015.
[16] A. M. A. El-Sayed, S. M. Salman, "Chaos and bifurcation of the Logistic discontinuous dynamical systems with piecewise constant arguments," *Malaya Journal of Matematik*, vol. 3 no.1,pp. 14–20,2013.
[17] M. U. Akhmet,"Stability of differential equations with piecewise constant arguments of generalized type," *Nonlinear Analysis*, vol.68 ,no. 4.pp. 794–803,2008.
[18] A. M. A. El-Sayed, S. M. Salman, "On a discretization process of fractional-order Riccati differential equation," *Journal of Fractional Calculus and Applications*, vol.4,no. 2,pp. 251–259,2013.
[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.