Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170507

Chaos In New Polynomial Discrete Logistic Maps With Fractional Derivative And Applications For Text Encryption

Kalsouabe Zoukalne [1,3,4], *Ahamat Mahamat Hassane*[1,3,4], *Mahamoud Youssouf Khayal*[4] *and Paul Woafo*[1,2,*]

[1]Laboratory on Modelling and Simulation in Engineering, Biomimetics and Prototypes, and TWAS Research Unit, Faculty of Science, University of Yaounde I, Box 812, Yaounde, Cameroon
[2]Laboratory of Products Development and Entrepreneurship, Institut Superieur de l'Innovation et de Technologie, P.O. Box 8210 Yaounde, Cameroon
[3]Techno-pedagogy Unit, Virtual University of Chad, Box 5711, N'djamena, Chad
[4]Physics and Engineering Science Training, Sciences-Technology-Environment Doctoral School, University of N'Djamena, Box 1117, N'Djamena, Chad

Received: 8 Apr. 2023, Revised: 12 Jul. 2023, Accepted: 13 Jul. 2023
Published online: 1 Sep. 2023

Abstract: In this paper, we propose new polynomial discrete logistic equations based on the classical logistic map, which exhibit chaotic behavior as control parameters vary. We also explore versions with fractional derivatives. Using the chaotic sequence generated by these equations, we develop an encryption scheme for text. The scheme relies on initial conditions, control parameters, and a transformation of text characters into values between 0 and 1, followed by a transformation to discrete chaotic values for transmission

Keywords: Polynomial discrete maps; logistic equation; fractional order; chaos; text encryption

1 Introduction

Since the emergence of digital communications systems, telecommunication systems have evolved till the deployment of 5G. This technological evolution has facilitated the exchange of data through Internet, computer networks, USB keys, and many other devices. In this context of widespread information exchange, the security becomes a priority. This necessitates the development of new cryptographic algorithms to complement the existing ones such as DES (Data Encryption Standard)[1], AES (Advanced Encryptions Standard)[2], RSA (Rivest, Shamir, and Adleman)[3], RC4 (Rivest Cipher 4)[4]. Indeed, these existing algorithms have shown their limits in view of the exponential evolution of the volume of exchanges and the space of encryption keys. Encryption algorithms using chaotic attractor-based pseudo-random or quasi-random number generators came with the advantages of their fundamental properties such as sensitivity to the initial state or to the system parameter leading to best means of confusion, diffusion, and other encryption keys[5,6,7]. Since the introduction of chaos in cryptography, several research works have been carried out on the use of discrete time sequences[8,9,10,11,12]. Discrete chaotic systems are generally defined by the equation (1):

$$x_{n+1} = f(x_n, r). \tag{1}$$

where $x_n \in \mathbb{R}^n$,$\mathbb{R}^p$,n=1,2,3...,f is a vector function of its arguments and p designing the number of parameters r. The well-known and simple discrete maps leading to chaos was developed by the biologist Robert May in 1976[13]. It is described by the following equation (1):

$$x_{n+1} = rx_n(1 - x_n) \tag{2}$$

It is the discrete version of the logistic equation derived by Verhulst to describe the evolution of a population in a given environment where r is the control parameter[14, 15]. This simple logistic map was used for text encryption by Baptista[16] using a division of the interval in which the discrete values x_n belong. This was later improved

* Corresponding author e-mail: pwoafo1@yahoo.fr

© 2023 NSP
Natural Sciences Publishing Cor.

using modified versions[17,18]. In the same line, Xiao et al. proposed a dynamic lookup table using the logistic map to improve the security of the Baptista algorithm[19]. In 2019, another improvement was conducted by Kumar Verma et al.[20]. The idea of text encryption was also recently conducted by Charalampidis et al. using a new logistic map that they developed[21].

However, in spite of these advances, dynamic lookup table cryptosystems based on present logistic maps are not resistant to chosen and known plaintext attacks[22], and simple logistic maps are not very well adapted to secure communication[23]. Research investigations are therefore conducted with the aim to use more generalized logistic maps[24,25,26], or fractional maps[26,27] since the addition of an extra parameter allows to increase the number of keys. From the point of view of cryptography based on chaos theory, the increase of parameters allows the setup of more robust algorithms[28]. Moreover, the generalized and the fractional models can be developed using the properties of the classical logistic maps. This will facilitate their integration into cryptography applications[29,30].

The aim of this work is to propose new fractional generalized discrete logistic maps starting from the characteristic conditions of the classical logistic sequences and then use the new map to put in place a new algorithm for text cryptography. Section 2 presents the generalized maps or the polynomial discrete maps which have the same boundaries and maximal curve properties as the classical logistic map. Section 3 presents the discrete polynomial fractional maps and their bifurcation diagrams. In Section 4, a text encryption scheme is presented based on the transformation of text into its ASCII images which are then transformed into the correspondent numbers in the interval$[0,1]$. Then the discrete chaotic sequence whose values are enclosed in the interval $[0,1]$ are used to encrypt the text. The decryption stage follows the inverse scheme of the encryption. Finally, in the last section, the conclusion is presented.

2 Derivation of the polynomial discrete map and its chaotic behavior

To develop the new polynomial discrete equations, we use the properties of the classical logistic map. We take the map to have the following mathematical form

$$x_{n+1} = rf(x_n), \tag{3}$$

For the classical logistic map, one has $f(x_n) = x_n(1-x_n)$ and the following properties are known:

$$f'(\frac{1}{2}) = 0, f(\frac{1}{2}) = \frac{1}{4}, f(1) = 0, f(0) = 0 \tag{4}$$

$f(x_n)$ is symmetric about $x = \frac{1}{2}$

To obtain the polynomial or generalized maps based on the logistic map, we have taken

$$f(x_n) = \sum_{k=1}^{N} a_k x_n^k, \tag{5}$$

with the condition that it should satistfy the characteristics in (4). This leads to a set of linear algebraic equations satisfied by the coefficients a_k. The symmetry of the function about $x = \frac{1}{2}$ gives the possibility to generate the number of equations equal to the number of unknows a_k. Thus solving the set of algebraic equations, one obtains the mathematical expressions of the polynomial f(x) which can be rescaled in order to have the same first terms of the classical logistic equation or also the rescale of the value of the control parameter r. For instance, Table 1 presents the expressions of $f(x)$ for $N = 2$, 3 and 4.

Table 1: Discrete polynomial logistic equation

N	$f(x)$	**Discrete polynomial logistic equation**
2	$x(1-x)$.This is the classical logistic map equation	$x_{n+1} = rx_n(1-x_n)$
3	$\frac{1}{4}x - \frac{1}{8}x^2 - \frac{1}{8}x^3$	$x_{n+1} = \frac{r}{4}x_n(1 - \frac{1}{2}x_n - \beta x_n^2)$
4	$\frac{4}{5}x - \frac{8}{5}x^3 + \frac{4}{5}x^4$	$x_{n+1} = \frac{4}{5}rx_n(1 - 2x^2 + x^3)$

For the case $N = 3$, we have also introduced a new controlling parameter α which will also has impact on the bifurcation diagrams ($\beta = 0.5$ for the actual development). This can also be done for the case of $N = 4$ in order to increase the number of parameters of the system.
Figure 1 presents the chaotic sequences generated by the three polynomial logistic equations with the initial conditions $x_0 = 0.110$ and $x_0 = 0.11$. One finds that the three discrete equations generate chaotic discrete values belonging in the interval [0, 1].

In order to have a more general characterization of the polynomial discrete maps, bifurcation diagrams with the corresponding Lyapunov exponent have been plotted in Figure 2. For the three equations, the transition to chaos is through period-doubling sequence. In the classical model, chaos is observed from $r = 3.58$ to $r = 4$. After $r = 4$, an explosion occurs. For the third polynomial model, chaos is observed from $r = 10.5$ to $r = 12.5$. Explosion occurs after $r = 12.5$. And for the fourth polynomial model, one observes that chaos appears at $r = 3.58$ and remains till $r = 4$ where the explosion takes place. Let us however mention that in the chaos domain, there are some short intervals given place to periodic dynamics. It is also interesting to note that the Hopf bifurcation takes place at

© 2023 NSP
Natural Sciences Publishing Cor.

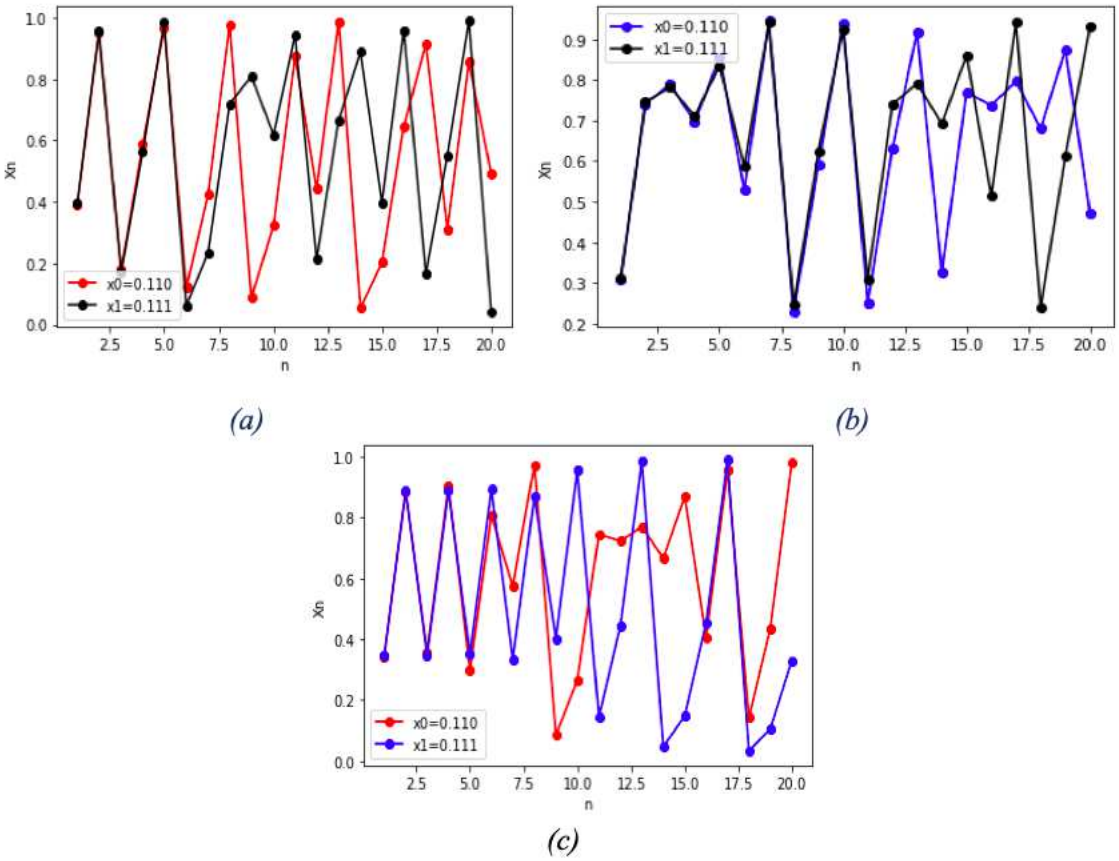

Fig. 1: Chaotic discrete sequences generated by the polynomial logistic equations and the sensitivity to initial conditions for $x_0 = 0.110$ and $x_0 = 0.11$ for (a) classical model with$r = 3.7$, (b) third order polynomial model (with $\beta = 0.5$ and $r = 11.7$) and (c) fourth order polynomial model with $r = 3.5$

r=1 for the three models and the first period-doubling bifurcation takes place at $r = 3$ for the classical model, at $r = 9.8$ for the third order polynomial model and at $r = 3$ for the fourth order polynomial model.

For the case $N = 3$, we have looked for chaos in the plane (r, β). Figure 3 presents what was found. The shaded area indicates where the couples of parameters (r, β) lead to chaos while the white area correspond to the domain where the discrete map generates periodic sequences and fixed values. This is obtained by using the positivity of the Lyapunov exponent. In the shaded area, some small isles of periodic behavhiors are present, appearing in a sort of concentric lines. It is also interesting to note that shade area presents several tails, some of which are long. Moreover, one also finds that the shaded area hars an arc disk shape.

3 Fractional order polynomial discrete map

To obtain the polynomial sequences of fractional order, we use the Grunwald-Letnikov difference of fractional order given by the relation [31]

$$\Delta^{\alpha} x(n) = \sum_{j=0}^{n} (-1)^j \binom{\alpha}{j} x(n-j) \tag{6}$$

where Δ^{α} is fractional order difference, $\alpha\mathbb{R}$ is the fractional order and its expansion gives

$$\Delta^{\alpha} x(n+1) = x(n+1) - \alpha x(n) + \sum_{j=2}^{n+1} (-1)^j \binom{\alpha}{j} x(n-j+1) \tag{7}$$

To simplify the equation7, we denote $m = j - 1$ and the equation becomes[32]

$$\Delta^{\alpha} x(n+1) = x(n+1) - \alpha x(n) + \sum_{m=1}^{n} (-1)^{m+1} \binom{\alpha}{m+1} x(n-m) \tag{8}$$

By fixing $C_m = (-1)^{m+1}\binom{\alpha}{m+1}$, we obtain the following fractional order difference expression:

$$\Delta^{\alpha} x(n+1) = x(n+1) - \alpha x(n) + \sum_{m=1}^{n} C_m x(n-m) \tag{9}$$

© 2023 NSP
Natural Sciences Publishing Cor.

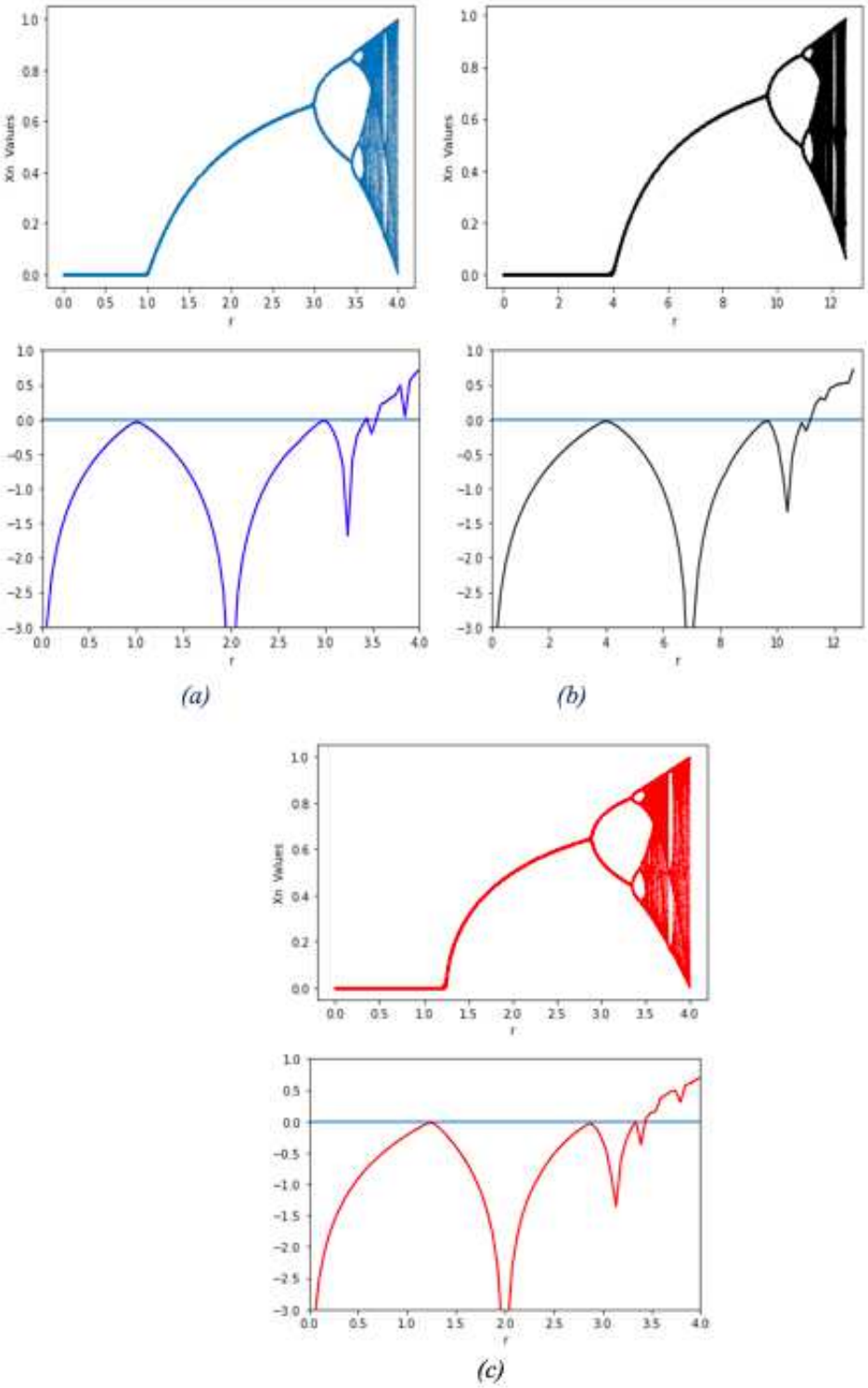

Fig. 2: Bifurcation diagrams and Lyapunov exponents as a function of r of the classical logistic sequence(a), the third order polynomial model (b) and the fourth order polynomial model(c)

© 2023 NSP
Natural Sciences Publishing Cor.

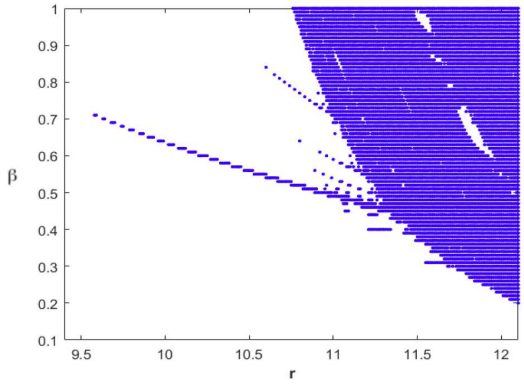

Fig. 3: Bifuraction diagram in the (r,β)plane for the third order discrete logistic map. The shaded area corresponds to the domain where a couple (r,β) leads to chaotic discrete sequences while the white area corresponds to periodic states

To have the fractional derivative of a discrete equation, we first need to define the integer difference of the same equation. Let us thus consider the discrete system of integer order defined by the following equation(10)

$$x(n+1) = f(x(n)). \tag{10}$$

where f is a nonlinear function
The difference of order 1 of the discrete system defined by relation 10 is given by:

$$\Delta^1 x(n+1) = x(n+1) - x(n) = f(x(n)) - x(n) \tag{11}$$

We can thus just operate the fractional derivative of equation 11 by replacing Δ^1 by Δ^α [31,33] to obtain the following equation 12:

$$\Delta^\alpha x(n+1) = f(x(n)) - x(n) \tag{12}$$

Then from equation (9), equation (12) leads to the following general equation(13 giving $x(n+1)$ when the fractional order derivative is applied.

$$x(n+1) = f(x(n)) + (\alpha-1)x(n) + \sum_{m=1}^{n} C_m x(n-m) \tag{13}$$

As the number of iterations increases, Cm decreases in value. This situation poses the problem of computational efficiency, the space required for each iteration and the storage of all the states of the system [33]. The solution to this problem is to use a finite truncation to approximate a discrete-time system of fractional order. The length of the truncation is denoted by **L**, which represents the size of the considered memory of the system [34]. Applying this principle to equation (13), we obtain the following approximation.

$$x(n+1) = f(x(n)) + (\alpha-1)x(n) + \sum_{m=1}^{L} C_m x(n-m) \tag{14}$$

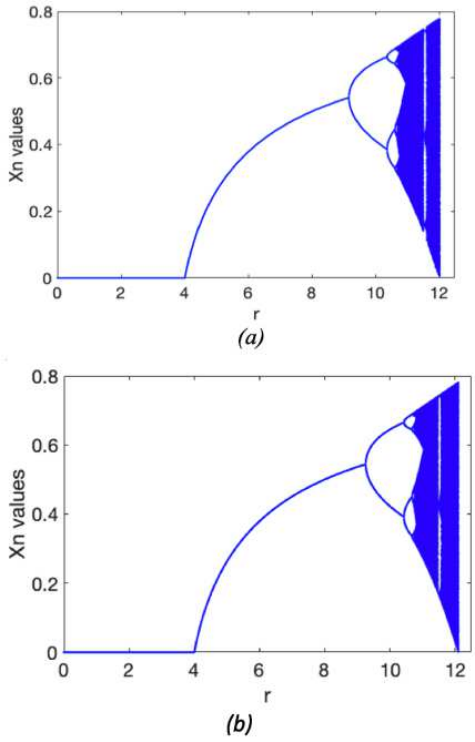

Fig. 4: Bifurcation diagram of the fractional polynomial map N=3 for $\alpha = 0.97$(a) and $\alpha = 1(b)$

By applying this formula to the discrete systems defined in Table 1 for $N = 3$ and $N = 4$, we obtain the polynomial sequences of fractional order recorded in Table 2.

Table 2: Fractional order discrete polynomial logistic equation

N	Fractional order discrete polynomial logistic equation
3	$x(n+1) = \frac{r}{4}x(n)(1-\frac{1}{2}x(n)-\beta x(n)^2) + (\alpha-1)x(n) + \sum_{m=1}^{L} C_m x(n-m)$
4	$x(n+1) = \frac{4}{5}rx(n)(1-2x(n)^2+x(n)^3) + (\alpha-1)x(n) + \sum_{m=1}^{L} C_m x(n-m)$

Figure 4 illustrates the behavior of the proposed fractional order polynomial sequences for N=3. From the bifurcation diagram (Figure 4 a), it is observed that the sequence with$\alpha = 0.97$ and $\beta = 0.5$ exhibits a period-doubling bifurcation and chaotic behavior for the range $r = 10.7$ to 12. Figure 4 b shows that the model with $\alpha = 0.97$ and $\beta = 0.5$ exhibits a chaotic behavior through a period-doubling bifurcation with one of periodic windows from $r = 10.5$ to 12.1.

In the same order, we plot the bifurcation of the fractional N=4 model when $\alpha = 0.98$ (Figure5a) and $\alpha = 1$ (Figure5b). For both cases, the factional order system exhibits a Hopf bifurcation when r=1 and a period

© 2023 NSP
Natural Sciences Publishing Cor.

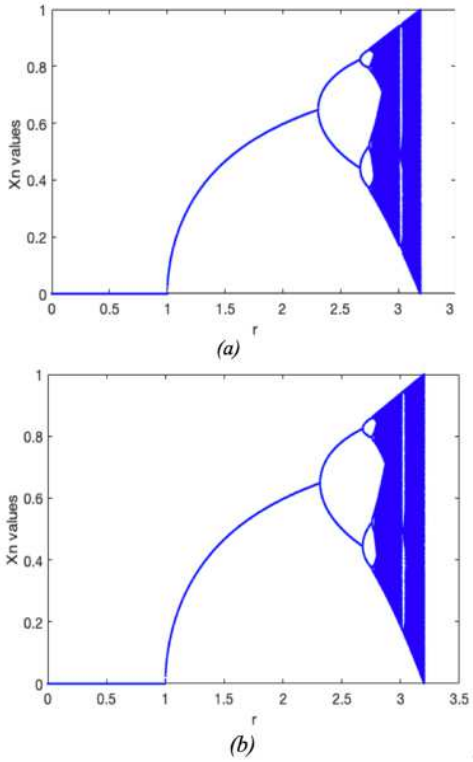

Fig. 5: Bifurcation diagram a of the fractional polynomial map N=4 for $\alpha = 0.98$(a) and $\alpha = 1(b)$

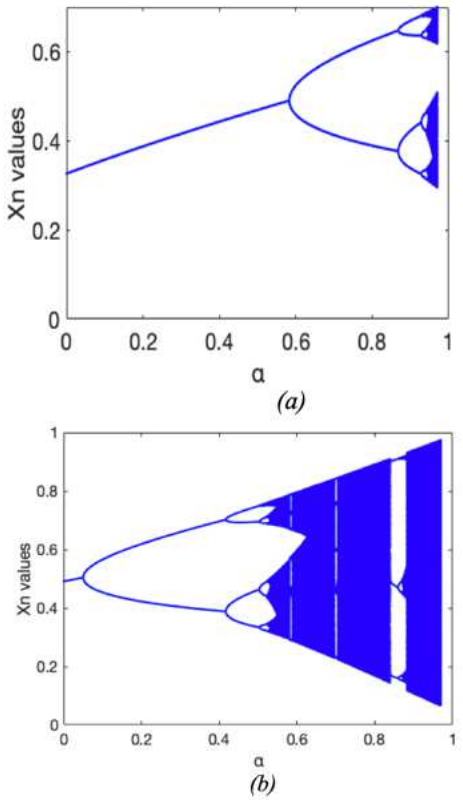

Fig. 6: Bifurcation diagram versus α for the fractional polynomial logistic maps for$N = 3$ (a) and $N = 4$(b)

doubling when r =2.3 for $\alpha = 0.98$ and $r = 2.4$ for $\alpha = 1$. The fractional map $\alpha = 0.98$ produces a chaotic behavior with a periodic window from $r = 2.7$ to3.2. For $\alpha = 1$, we observe a chaotic behavior with a periodic window from $r = 2.6$ to3.2. Thus the fractional order modifies the values of r for the bifurcation points.

4 Text Cryptography

In this section, we propose a text encryption algorithm based on three stages: conversion of the ASCII table in a table having values belonging to the interval [0,1]; transformation of a given message to its correspondence in this interval; mixing of the message with the chaotic sequence generated by the polynomial logistic map. We use here the third order polynomial model having the parameter β as another key. More details are given below.

4.1 Presentation of the encryption algorithm

As we indicated above, a new table of correspondence has been built between the text characters and the numerical values included in the interval [0,1] as the first step of the encryption process and then encrypt the clear message by the chaotic keys randomly generated. The different steps of the algorithm are as follows:

- –First, the ASCII value of each character, digit, and punctuation is divided by 256 leading to a new table. The ASCII value of each character using dedicated software (some of which are free online) ;
- –The plaintext message is converted to ASCII in the interval [0,1] by a simple set of indexing each character in the previously established correspondence table ;
- –The encryption keys are randomly generated by iterating n times the fractional generalized logistic sequence; n being the length of the plaintext message. This gives a set of disordered values included in the interval [0,1];
- –The product term by term of the encryption keys with the values of the plaintext messages in the interval [0,1] is then made to obtain the encrypted message.

The multiple keys of such a text encryption can be seen as being the following: the transformation of the ASCII in the interval [0,1], the initial conditions, the control parameters r and ?, the choice of the interval of iteration to obtain the n chaotic digits, the multiplication operation.

© 2023 NSP
Natural Sciences Publishing Cor.

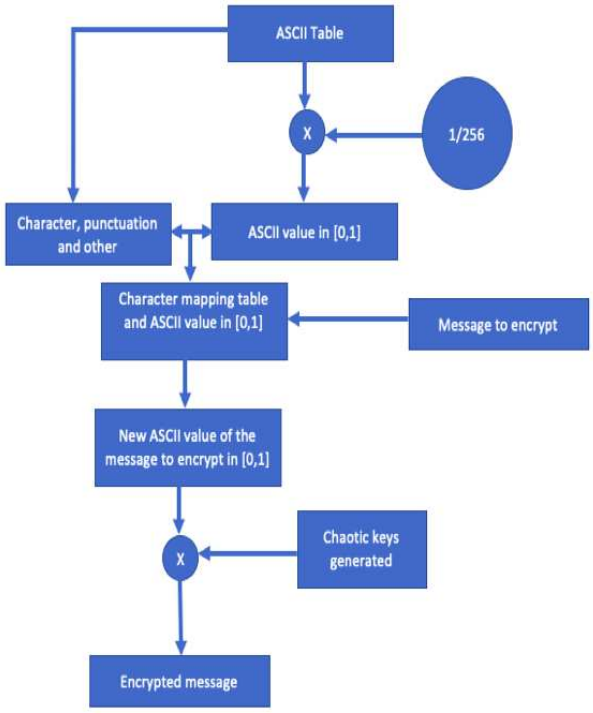

Fig. 7: Flowchart of the encryption process

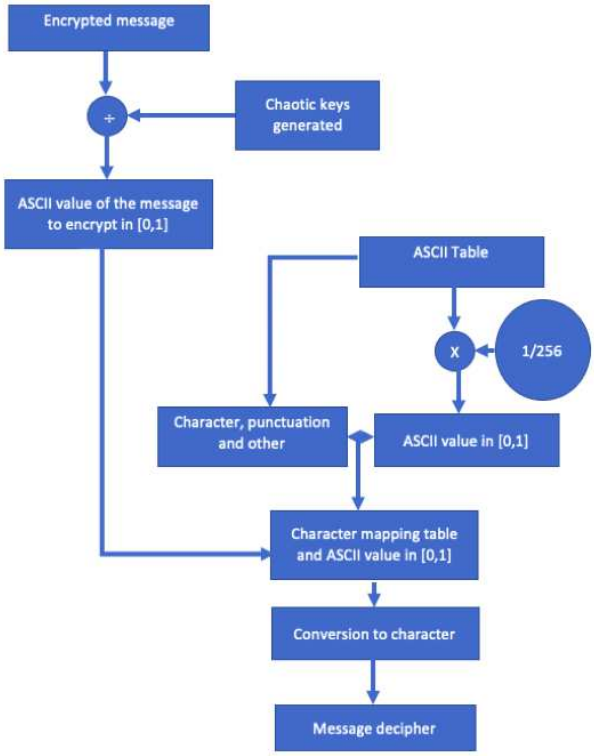

Fig. 8: Flowchart of the decryption process

Figure 7 summarizes the main steps of the encryption algorithm in a flowchart.

Text decryption is nothing else than the reverse operation of encryption. The symbols of the encrypted message are sequentially divided by the successive chaotic digits. The obtained values are then indexed in the correspondence table between the characters and the values included in [0,1], to display the corresponding characters. Figure 8 presents the flowchart of the decryption process.

The principle of the presented algorithm is close to that of Baptista's algorithm at the level of character matching with ASCII and interval division. In the Baptista's method, the interval [0,1] is divided into S subintervals of step ε where $\varepsilon = \frac{X_{max}-X_{min}}{256}$ and X_{max}, X_{min} the portion where the probability density is strong. The S characters in the text are associated to the corresponding subintervals by iterating the logistic sequence with the requirement the message to be encrypted belongs to the interval: $[X_{min} + \varepsilon_k * p, X_{min} + \varepsilon_k * (p+1)]$,$p$ is the ASCII value. At the end the encrypted message corresponds to the number of iterations M performed in the logistic equation[16].

4.2 Examples of encrypted and decrypted messages with correlation test

Example 1:

The first example of the message encrypted is ?Mummy goes to the market?. Its equivalent in the ASCII table is: 77, 117, 109, 109, 121, 32, 103, 111, 101, 115, 32, 116, 111, 32, 116, 104, 101, 32, 109, 97, 114, 107, 101, 116. Its correspondence in the interval [0,1] is:
0.30078125, 0.45703125, 0.42578125, 0.42578125, 0.47265625, 0.00390625, 0.40234375, 0.43359375, 0.39453125, 0.44921875, 0.00390625, 0.453125, 0.43359375, 0.00390625, 0.453125,0.40625,0.39453125,0.00390625, 0.45703125, 0.37890625, 0.4453125, 0.41796875, 0.39453125, 0.453125.
Using the following keys $r = 11.56$,$x_0 = 0.01$,$\alpha = 0.99$, $\beta = 0.75$, and undertaken the multiplication process with the M=24 discrete chaotic sequence starting at n=0 to 23, the encrypted message in the [0; 1] is:
0.008648463291015625,0.037408439951648165, 0.09609020968270764,0.23575723725122075 ,0.37303505612065113,0.001231495973435834, 0.2814690015711633,0.24822621966665498,0 .3054537274040361,0.16416555772221364 ,0.002958487147591067,0.18953714714160258,0.34 57470436658256,0.0011199901504932868, 0.29848984310723037,0.2669627762410615,0.260 41263578565954,0.0025574499897102806, 0.30367036184768254,0.24495587257470722,0.30 22670654248385,0.25832219885483165, 0.2850445231469722,0.2339405893224883.

© 2023 NSP
Natural Sciences Publishing Cor.

We remind that M=24 is the length of the message to be encrypted. Now undertaking the decryption process, the message received in the interval [0,1] is equal to the original message. Finally by using the correspondence between the interval [0,1] and the ASCII table, one obtains the good message in the ASCII format and finally the original message.

An interesting point was to find the correlation between the message transformed in the interval [0;1] and its encrypted correspondence in the same interval. We find a correlation value equal to 0.241.

Example 2: The second example we took is the text ¡¡qwerty¿¿. The ASCII transformation is 113, 119, 101, 114, 116, 121.

Its correspondence in the [0,1] interval is:
0.44140625, 0.46484375, 0.39453125, 0.4453125, 0.453125, 0.47265625.

Its encrypted version is:
0.012604067451171876,0.037527224030407764, 0.08727519256290914, 0.24107307073924983, 0.358711830064727, 0.1440712148331051.

The decryption process also leads to the original message.

5 Conclusion

In this work, we have proposed polynomial discrete maps derived from the classical logistic map with the requirements that the polynomial functions satisfy the boundary values and the symmetry of the classical logistic one. We have limited the expansion to polynomial of the fourth order. But the extension can be conducted for high order polynomials. The new polynomial discrete maps have shown transition to chaos in the same manner as the classical one with however different values for the bifurcation points. New control parameters can be introduced as the coefficients of each term of the polynomials as we did for the third order polynomial.

One of the new fractional discrete polynomial maps has been used to propose a new text encryption scheme based on three stages. The first consists of converting the ASCII table into a table of values belonging to the interval [0,1]. The second stage converts any text from its equivalent to its equivalent in the interval [0,1]. Then in the third stage, the message is multiplied by chaotic sequences of number generated from the logistic (with a size equal to the length of the text message). The number of keys gives some security for the encryption scheme. The chaos generated by the new polynomial logistic maps could be used for the encryption of other types of messages such as images and audio-videos messages, using the encryption scheme presented here or other chaos cryptography methods.

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] Federal Information Processing Standards Publication.*Data Encryption Standard (DES)*.NIST,U.S Publication 46 ,(1999).

[2] Federal Information Processing Standards Publication.*Advanced Encryption Standard (AES)*.NIST,U.S Publication 197 ,(2001).

[3] R .L. Rivest ,A. Shamir,L.M. Adleman.Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications.ACM* , **21**,120−126(1978).

[4] G.Gong,K.C. Gupta, M.Hell, Y.Nawaz,*Towards a General RC4-Like Keystream Generator* .**21**, Lecture Notes in Computer Science,162−174(2005).

[5] A. G.Radwan .On some generalized discrete logistic maps. *Journal of Advanced Research*, **4**,163−171(2013)

[6] R. R. Kumar ,R. Pandian,T.Prem Jacob, A.Pravin ,P. Indumathi. Cryptography Using Multiple Chaos. *Journal of Physics: Conference Series*, **1770** (2021).

[7] R. R. Kumar ,R. Pandian,T.Prem Jacob, A.Pravin ,P. Indumathi. Cryptography Using Chaos in Communication Systems. *Journal of Physics: Conference Series*,**1770**(2021).

[8] N.K.Pareek , Vinod Patidar ,K. K, Sud.Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation* ,**10**,715−723(2005).

[9] T.Xiang,K.Wong, Xiaofeng, X.Liao. An improved chaotic cryptosystem with external key, *Communications in Nonlinear Science and Numerical Simulation* ,**13**,1879−1887(2008).

[10] N.Singh, A.Sinha. Chaos-based secure communication system using logistic map. *Optics and Lasers in Engineering*, **48** 398–404 (2010).

[11] S.Agarwal ,Chaotic Dynamics of Complex Logistic Map in I-Superior Orbi. *International Journal of Information Technology and Computer Science* , **12** ,11−18 (2020).

[12] G.Makris , L.Antoniou.Cryptography with Chaos.*Chaotic Modeling and Simulation (CMSIM)* ,**1** ,169−178(2013).

[13] R.M .May,Simple mathematical models with very complicated dynamics, *Nature* ,**261**,459−467(1976).

[14] P.F.Verhulst.*Notice sur la loi que la population suit dans son accroissement*,Correspondence Mathematique et Physique (Ghent),**10** ,113−121(1838).

[15] N.Bacaer.*Verhulst and the logistic equation (1838)*,in A Short History of Mathematical Population Dynamics,Springer, London,35−39(2011).

[16] M.S. Baptista.Cryptography with chaos.*Physics Letters A* ,**240** ,50−54(1998).

[17] W.Wong, L.Lee, K.Wong.A modified chaotic cryptographic method. *Computer Physics Communications*,**3**, 234−236(2001).

[18] O.Datcu, R.Hobincu, M.Stanciu, R .A.Badea, Encrypting Multimedia Data Using Modified Baptista′s Chaos-Based Algorithm, In: Future Access Enablers for Ubiquitous and Intelligent Infrastructures. Ed. by Springer, Cham.,185−190(2018).

[19] D.Xiao, X.Liao , K.Wong. Improving the Security of a Dynamic Look-Up Table Based Chaotic Cryptosystem.*IEEE Transactions on Circuits and Systems*, **53**,502−506(2006).

[20] D.K.Verma, M.Rani, R.K.Tyagi, B.B Sagar.Baptista chaotic cryptosystem based on alternate superior dynamic lookup

© 2023 NSP
Natural Sciences Publishing Cor.

table.*Journal of Discrete Mathematical Sciences and Cryptography*,**22**,1383−1392(2019).
[21] N.Charalampidis, C.Volos, L.Moysis, A.V.Tutueva, D.Butusov, I.Stouboulos.*Text Encryption Based on a Novel One-Dimensional Piecewise Chaotic Map*, Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus),(2022).
[22] J.K.Pal,Administering a cryptology centre by means of scientometric indicators,*Collnet Journal of Scientometrics and Information Management* ,**10**,97−123(2016).
[23] D.Arroyo, G.Alverez, V.Fernandez,On the inadequacy of the logistic map for cryptographic applications. arXiv:0805.4355v1[nlin.CD] 28 May 2008.
[24] M.Stavroulaki,D.Sotiropoulos.The Energy of Generalized Logistic Maps at Full Chaos.*Chaotic Modeling and Simulation (CMSIM)* , **2** ,543−550(2012).
[25] W.Xingyuan, L. Yanpei. A new one-dimensional chaotic system with applications in image encryption.*Chaos, Solitons and Fractals* , **139**,(2020).
[26] Z.Ying-Qian, H.Jun-Ling, W.Xing-Yuan W.An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map. *IEEE Access*,**8**,54175−54188(2020).
[27] V.Sangavi, P.Thangavel, An Image Encryption Algorithm Based On Fractal Geometry, Procedia Computer Science, **165**,462−469(2019).
[28] S.K,Abd-El-Hafiz, A.G.Radwan, S.H.AbdEl-Haleem .Encryption Applications of a Generalized Chaotic Map. *Applied Mathematics and Information Sciences*, **9**,3215−3233(2015).
[29] M.Lawnik. Generalized logistic map and its application in chaos-based cryptography. *Journal of Physics Conference Series*, **936**,(2017).
[30] H.Natiq, N.M.G.Al-Saidi, S.J.Obaiys, M.N. Mahdi, A.K. Farhan.Image Encryption Based on Local Fractional Derivative Complex Logistic Map. *Symmetry*, **9**,(2022).
[31] A.A.Kilbas, H.M,Srivastava, J.J.Trujillo, J.J,Theory and Applications of Fractional Differential Equations, Elsevier B V, Amsterdam, (2006)
[32] O.Megherbi, H.Hamiche, S.Djennoune, M.Bettayeb,A new contribution for the impulsive synchronization of fractional-order discrete-time chaotic systems. *Nonlinear Dynamics*,**90**,1519−1533(2017).
[33] A.A.Khennaoui, A.Ouannas, S.Momani, O.A.Almatroud, M.M.Al-Sawalha MM, Boulaaras, V.T. Pham. Special Fractional-Order Map and Its Realization. *Mathematics* ,**10**4474(2022).
[34] X. Liao, Z. Gao, H. Huang. *Synchronization control of fractional-order discrete-time chaotic systems*, In European Control Conference (ECC), Zurich, Switzerland, (2013)

Kalsouabe Zoukalne received the M.S degree in Telecommunication from National Institute of Science and Technology of Abeché, Chad, in 2019, where his currently pursuing the Ph.D. He is currently investigating the discrete chaotic systems and their application in cryptography.

Ahamat Mahamat Hassanreceived the M.S degree in Telecommunication from National Institute of Science and Technology of Abeché, Chad, in 2019, where his currently pursuing the Ph.D. He is currently investigating the synchronization of multi-layer nonlinear discrete oscillator networks and their application to data security.

Mahamoud Youssouf Khayal is Professor of Energy and Electrical Engineering at University of N'djamena, Chad. He is currently Director of National Research Center for Development, N'djamena, Chad. He received the Ph.D. in Technical Sciences from the Belarus Polytechnic Institute. His main research interests are : Energy losses in the structural elements of enclosures for complete distribution systems, Estimation of the accuracy of the mathematical model used to describe the magnetisation of ferromagnetic plates by a variable field of currents.

© 2023 NSP
Natural Sciences Publishing Cor.

Paul Woafo received the Ph.D. degree in physics from the University of Yaoundé I, in 1992, and the Doctorat d'Etat degree in physics in 1997. He is Full Professor at the University of Yaoundé I since 2005, and heads the Laboratory of Modelling and Simulation in Engineering, Biomimetics and Prototypes (LAMSEBP). He is also an external member of the Applied Physics Group, Vrije Universiteit Brussel, Belgium. He is authors of 280 refereed articles in international journals. He was awarded the TWAS Prize for Young Scientists in 2004. His research interests involve the nonlinear dynamics in optoelectronics, electromechanics, electronic, biological and chaos cryptography systems. He was a member of the International Union of Pure and Applied Physics (IUPAP) Commission for statistical physics (C3). He was awarded the 2020 medal of the IUPAP Commission of Physics for development. He is a Founding Member and the former President of the Cameroon Physical Society (CPS), member of the board of the African Physical Society (AfPS), and the Dean of the College of Mathematics and Physical Sciences, Cameroon Academy of Sciences. He was an Associate member (junior, regular and senior) of the Abdus Salam International Center for Theoretical Physics (1995-2013). He is Georg Forster Fellow of the Humboldt Foundation, Germany.

© 2023 NSP
Natural Sciences Publishing Cor.