Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN NO. 2320-5407
Article DOI: 10.21474/IJAR01/xxx
DOI URL: http://dx.doi.org/10.21474/IJAR01/xxx

RESEARCH ARTICLE

New one-dimensional (1D) chaotic card for data encryption

Manuscript Info

Manuscript History
Received: xxxxxxxxxxxxxxx
Final Accepted: xxxxxxxxxxx
Published: xxxxxxxxxxxxxxx

Key words:-
Chaotic Map, pseudo-random number generator; Cryptography,1D-PEC, chaos

Abstract

In this paper, we present a new one-dimensional polynomial exponential chaotic map, named 1D-PEC. The dynamic properties of the new map are investigated as a function of different parameters. The set of areas in parameter space where the map exhibits periodic, constant, and chaotic dynamics is also determined. The cryptographic performance of the 1D-PEC map is successfully analyzed using initial condition and parameter sensitivity tests, key space, and histogram analyses. The new chaotic card has a larger key space, making cryptanalysis more difficult.

Introduction:-

With the rapid development of information and switching technologies, the dissemination of information is becoming increasingly simple thanks to computer networks. At the same time, the ways in which information can be distorted or manipulated have increased dramatically in recent decades.

To guarantee the protection and authenticity of information, a great deal of research has gone into developing the best encryption techniques, such as DES, AES and RSA. However, despite the effectiveness of traditional encryption systems, they are no longer adapted to today's realities, characterised in particular by the dissemination of digital images and videos (Li et al, 2007). To solve this problem, researchers have proposed several new image encryption methods based on the use of chaotic systems (Wang et al, 2010, Liu et al 2010, Alexan et al 2023, Hu et 2020), optical modification (Shao et al 2020, Ritika et al 2017, Faragallah et al 2019), grid variation (Chen et al , 2012, Francis et al, 2024), DNA coding (Xuejing et al 2020, Wang et al 2024) and quantum theory (Zhou et al 2024, Gao et al 2022).

Chaotic systems have several interesting characteristics, such as the ability to provide several different keys, ergodicity, unpredictability and high sensitivity to initial conditions and system parameters (Maqableh et al 2008). These characteristics thus increase the security and confidentiality of information hiding algorithms (Azzaz et al, 2013, Hasheminejad et al, 2019). Despite its advantages, chaotic maps have some flaws that make them vulnerable to chosen and known plaintext attacks (Pal,J.K., 2016). The flaws found in the logistic map include the presence of periodic windows in the chaotic area, the irregular distribution of data and the small size of the chaotic area. In addition, chaotic maps have few parameters, confined to small intervals. To solve these problems, several new discrete maps with good cryptographic performance have been developed in recent decades. For example, Yicong Zhou et al (Yicong Zhou et al,2013) presented a new one-dimensional discrete chaotic system for image encryption. The new map is obtained by combining two chaotic maps in parallel. Some chaotic properties of this map, such as distribution uniformity and sensitivity to changing conditions, are excellent. The bifurcation of this map has no periodic and blank windows on the interval from 0 to 4. I. Xie et al proposed in (Xie et al,2009) an image encryption algorithm based on a new logistic map with excellent characteristics. This contribution solved several problems of the classical logistic map, with the weak exception of the chaotic zone. The problems solved include stable windows, empty windows, uneven distribution of sequences and bifurcation control parameters. Zhongyun Hua et al (Zhongyun et al,2019) proposed cosine transform-based chaotic maps (CTBCS), using existing chaotic maps. The proposed maps exhibit complex behaviors and a very small chaotic region with no periodic window. More recently, F. Ullah et al (Ullah et al) developed a new non-

linear system called the chaotic cosine equation (CCE) for image encryption. The proposed map has a larger key space, a regular and random distribution, highly sensitive to initial conditions and chaotic over the entire domain of definition of the control parameter. However, the map has several stable or blank windows in the chaotic range.

As we have seen in the previous paragraphs, some of the weaknesses of the logistic map are present in the new maps. The presence of weaknesses such as stable windows in the chaotic zone and the key range opens the way to cryptanalysis. The objective of this contribution is to propose new polynomial maps that have a large chaotic range without stable windows and generate quasi-random numbers and then use the new map to develop a new image encryption algorithm. The rest of the paper is structured as follows: in section 1, the dynamic behavior of the new map is analyzed, in section 3 the cryptographic performance is evaluated and the last section presents the conclusion.

2. New 1D chaotic map

2.1. Logistics map

The classical logistic map is a non-linear iterated map developed by the biologist Robert May in 1976 (May, 1976). It is often presented as an example of the complexity that can generate simple chaotic behavior. It represents the discrete-time solution of the Verhulst model (Killmann and Schindler, 2001) and is defined by the relation 1 .

$$x_{n+1} = r x_n (1 - x_n) \quad (1)$$

In the logistic map, x_n represents the initial population number and r the control parameter. These two variables are defined in the intervals [0,1] and [0,4] respectively. The overall dynamic behavior of this map is summarized in Figure 1 by means of the bifurcation diagram and the corresponding Lyapunov exponent.

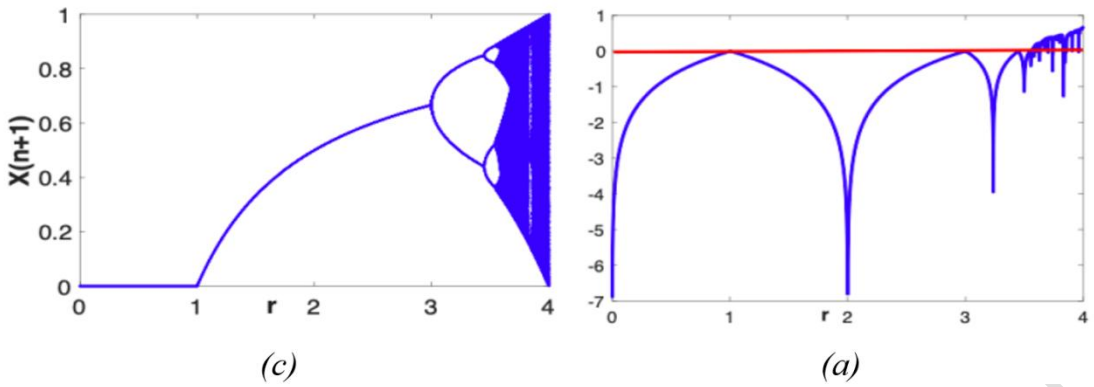

Fig. 1 : Bifurcation diagram as a function of r for the classical logistic map (a) and the corresponding Lyapunov exponent (b)

2.2. Analysis of the dynamic behavior of the 1D-PEC card

The new one-dimensional (1D) chaotic map called 1D-PCE has a much larger key space than the traditional logistics map. The proposed model is a simple structure defined as follows:

$$x_{n+1} = r x_n e^{r x_n} + \frac{1}{x_n{}^{\alpha}} mod 1 \qquad (2)$$

Where r and α are the control parameters, is the initial condition, and mod1 is the modulus operator that imposes that the output of the map is between 0 and 1. r is the main control parameter and its domain of definition is the interval [0,25]. On the other hand, the parameter takes its values in the interval]-,3.5]. To highlight the properties of the news, we evaluate the map through the main metrics for confirming the presence of chao in a system.

2.2.1. Evaluation of the phase diagram and trajectory

The phase diagram, also known as the attractor, is the curve representing all the trajectories of a system obtained from different initial conditions in phase space. To better observe the dynamic states of the 1D-PEC map, we have plotted its phase spectra and those of the classical logistic map in 2D and 3D planes in Fig. 2. We note that the chaotic sequences generated by the 1D-PEC map are distributed homogeneously over the entire 2D and 3D phase diagram, whereas those of

the logistic map are parabolic and undulating. This property solves the problems of the classical logistic map, such as periodic windows, empty windows or irregular outputs.

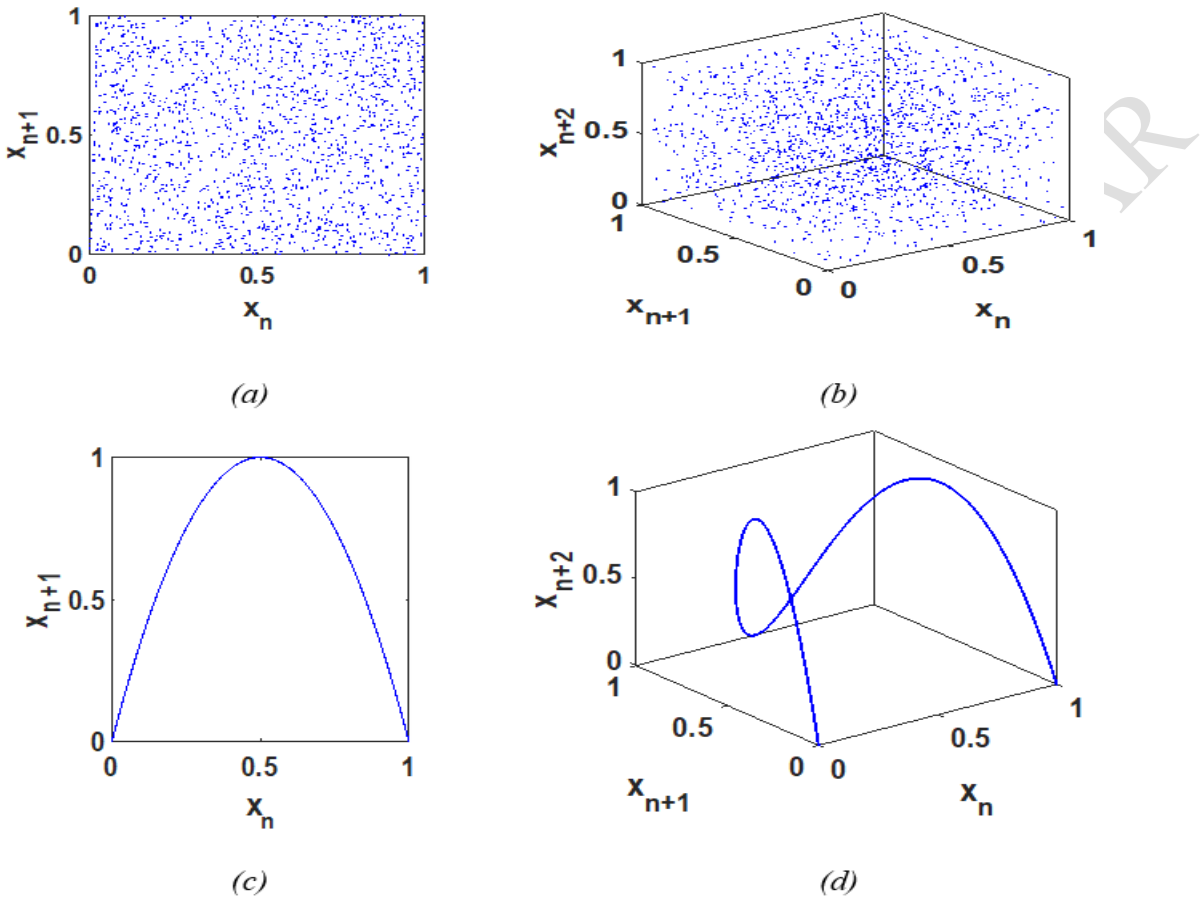

Fig. 2: Comparison between the phase portrait of the classic logistics map and 1D-PEC. (a), (b) phase portrait of the new map and (c), (d) phase portrait of the classic logistics map.

In the same vein, to further visualize the behavior of the new map, we have analyzed and presented the cobweb diagrams of the 1DPCE map and the logistics map in Fig. 3a and b. The cobweb diagram drawn shows that for a given initial condition, the system generates a set of non-repeating iterative trajectories, confirming the chaotic nature of the new map. Furthermore, the orbit of the 1DPCE map fills the entire output rectangle space unlike the orbit of the classical logistic map which does not, despite its chaotic behavior. This situation reinforces the idea that the new map is more efficient than the old logistics map.

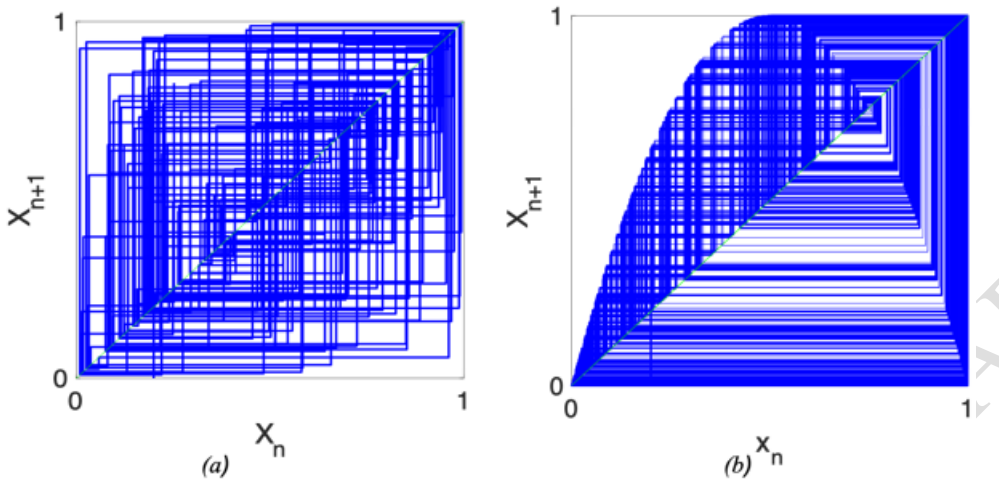

Fig.3: Cobweb diagram of the (a) 1D-PEC and (b) conventional logistics map

2.2.2. Evaluation of the bifurcation and the Lyapunov exponent

The bifurcation diagram is a graphical representation of all the qualitative changes observed in the study of a dynamic system as a function of a parameter. The Lyapunov exponent is a metric used to identify the presence of temporal chaos or the sensitivity of a discrete system to initial conditions. For a discrete system defined by an application f with initial condition x0, the Lyapunov exponent is defined by :

$$\lambda(x_0) = \lim_{n\to+\infty} \frac{1}{n} \left|\frac{df^n(x_0)}{dx}\right| = \lim_{n\to+\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln f'(x_i) \quad (2)$$

When the Lyapunov exponent (λ) is positive, this reflects the presence of chaotic behavior, the divergence between two neighboring trajectories increases greatly with time. Fig. 4 a, b and c show the bifurcation diagram and the Lyapunov exponent of the 1D-PEC map as a function of the parameters r, and a fixed. As we can see in Figure 4 a, when α is medium, the proposed map is periodic for 0.1<r< 0.28, then chaotic with stable windows for 0.29<r<0.4 and beyond 0.4, the system becomes totally chaotic. The map shows several periodic and fixed windows on the bifurcation diagram when α takes its largest value (3.5), as shown in Fig. 4 b. Finally, when a is small (α<-0.5), we observe completely chaotic dynamics over the whole domain of parameter r (Fig. 4 c) and the exponent becomes larger and larger.

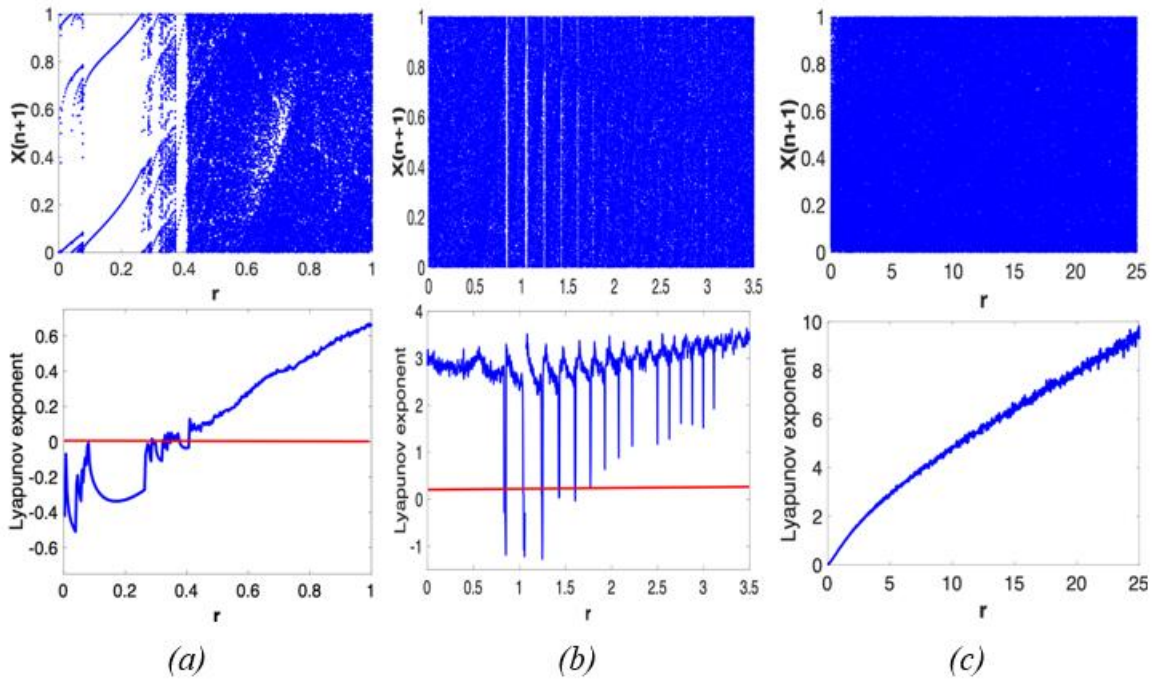

Fig. 4: Bifurcation plot as a function of r and the corresponding Lyapunov exponent of the 1D-PCE map in the cases(a) α =-0.1,(b) α =3.5 and (c) α = -1

In the same order, the bifurcation diagram and the exponent of the system as a function of the parameter α and fixed r are plotted in figures 5 a, b, and c. Fig. 5a shows the evolution of the system for r=0.15. The map is initially chaotic, then chaotic with periodic and fixed when -0.65<a<-0.2. The map is first chaotic, then chaotic with periodic and fixed when -0.65 < a < -0.2. It is then periodic when -0.2 < a < 0.4 and becomes chaotic when a > 0.4. When r is medium (r = 1.5), the system exhibits complex behaviour punctuated by alternating chaotic, periodic, and stable line windows, as illustrated in Fig. 5b. Finally, for large r, the new map exhibits complex behaviour over the entire interval where a takes its values (Figure 5 c).

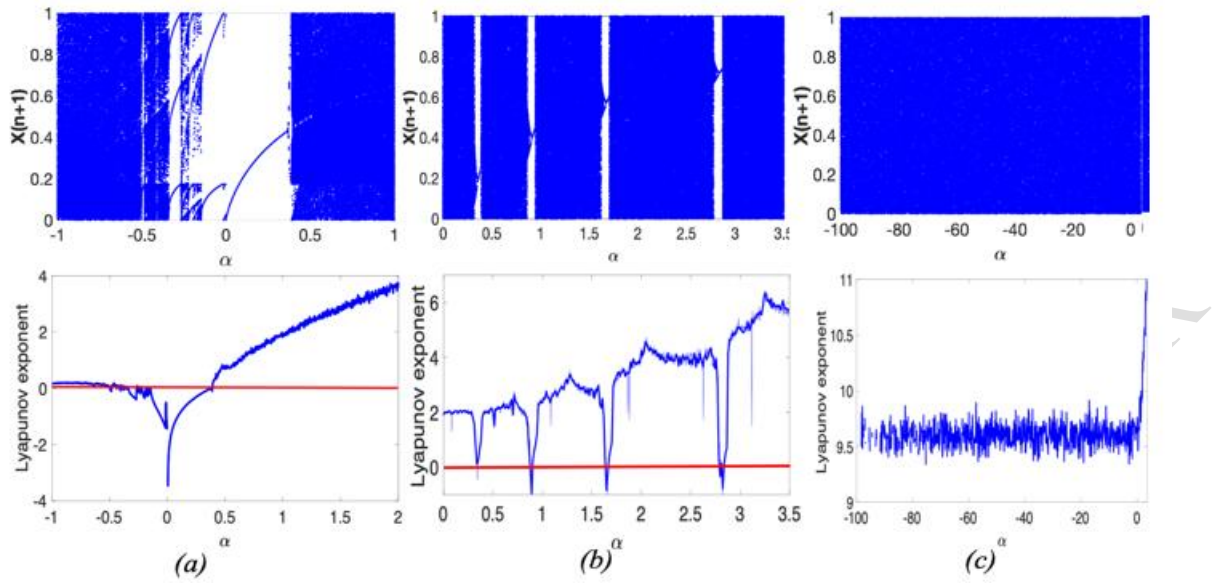

Fig. 5: Bifurcation plot as a function of α and the corresponding Lyapunov exponent of the 1D-PCE map in the case(a) r=0.15,(b) r=1.5 and (c) r=8.

3. Cryptographic performance analysis

3.1. Sensitivity analysis of initial conditions and parameters

The sensitivity of initial conditions and parameters is an important characteristic of chaotic systems. To highlight this property, diagrams of time series with a change in initial conditions and parameters are plotted. Fig 6a and b illustrate the values of the two chaotic sequences with a difference in initial conditions of 10^{-16} . As we can see, the time series of the 1DPCE map diverges after only four iterations (Fig. 6 a), whereas those of the logistic map diverge after forty iterations (Fig. 6 b).

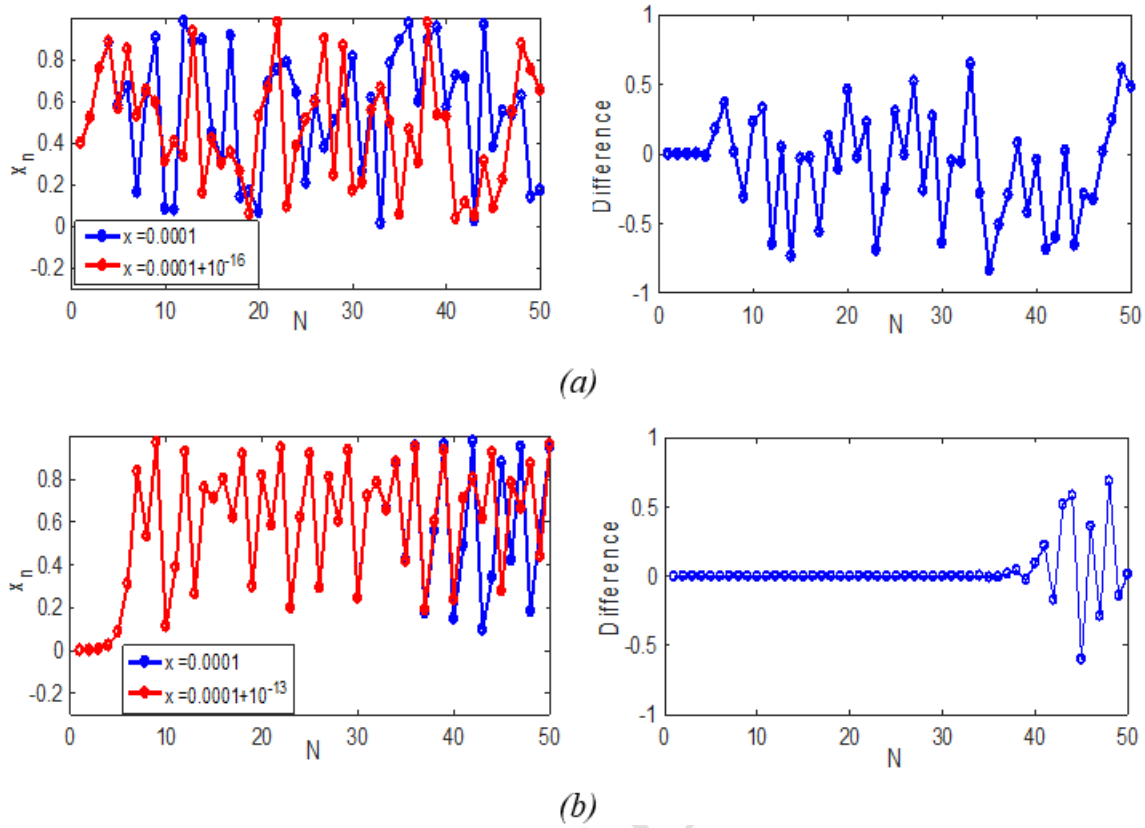

Fig. 6: Analysis and graphical comparison of chaotic sequences managed with modification and without modification of X0 in the case of (a) the classic 1D-PCE map and (b) the classic logistic map.

In Fig. 7, we show the sensitivity to the parameters with a difference of 10^{-16} and 10^{-14} respectively, for the alpha and beta parameters. As shown, the sequences of states of the new map (Fig. 7a and b) diverge very quickly, whereas those of the logistic map diverge after several iterations (Fig. 7c). Throughout the sensitivity analysis, the figures on the right show the difference between the values of the states of two-time traces. It is clear that our proposed map is very sensitive to initial conditions and parameters. Therefore, this map is a good candidate for cryptography.

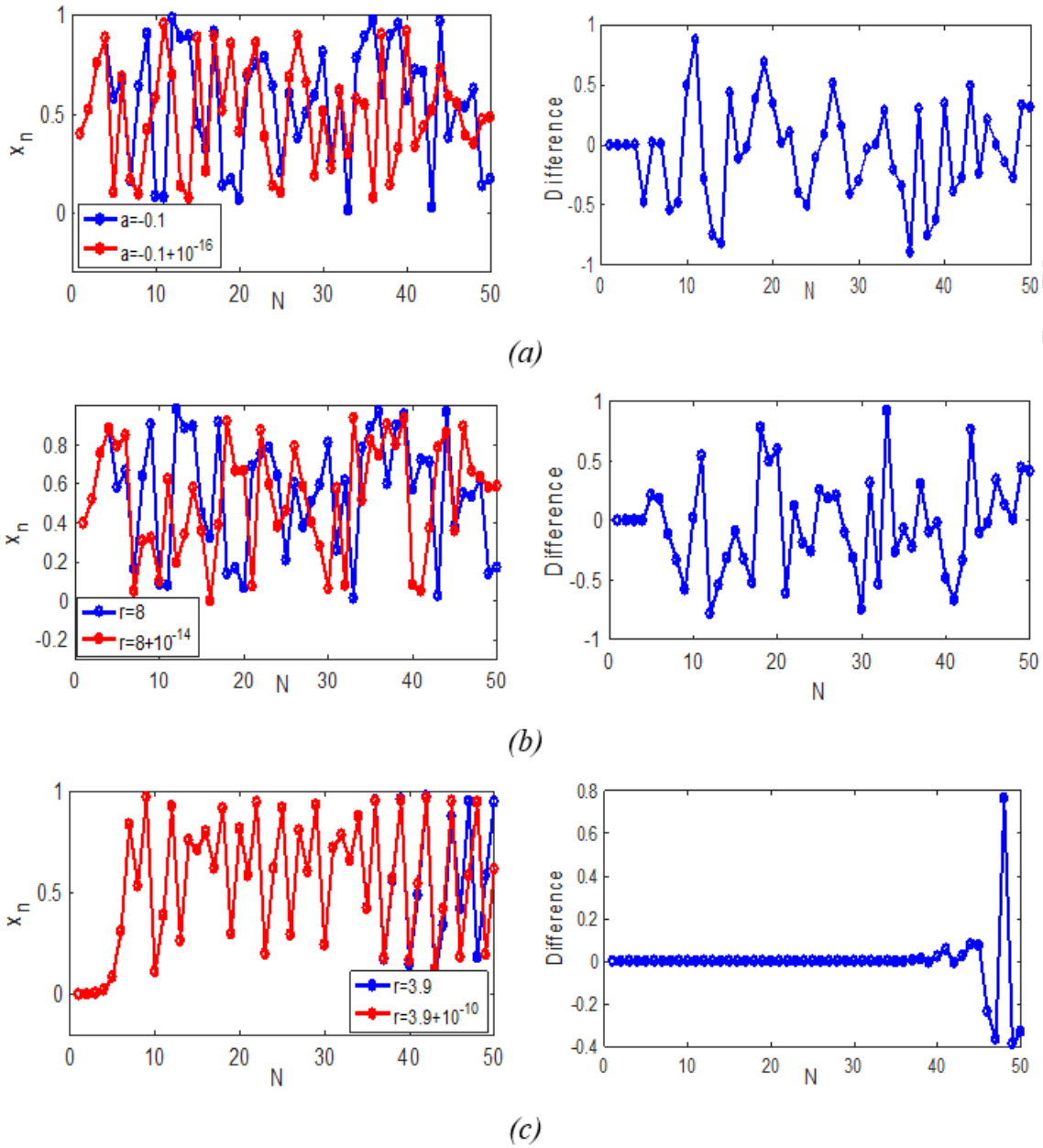

Fig. 7: Analysis and graphical comparison of the chaotic sequences generated with and without modification of the r parameters in the case of (a) the classic 1D-PCE map and (b) the classic logistic map.

3.2. Histogram analysis

The histogram is a very important metric for assessing whether the distribution of a random number generator is uniform over the desired interval. A system with a dense, uniform distribution is a system with unpredictable dynamic behaviour. The figure below shows the

sequences generated by the classic logistic map and the new map. Fig. 8 (a) shows the distribution of the logistic map. As we can see, the sequences generated are not uniformly distributed, and some sequences appear to be distributed around 0 and 1. In Fig. 8 (b) we see that the sequences generated by the new chaotic map are uniformly distributed in the interval [0, 1]. It is clear that the proposed 1D-PCE map has a more complex dynamic behaviour than the classical logistic map.

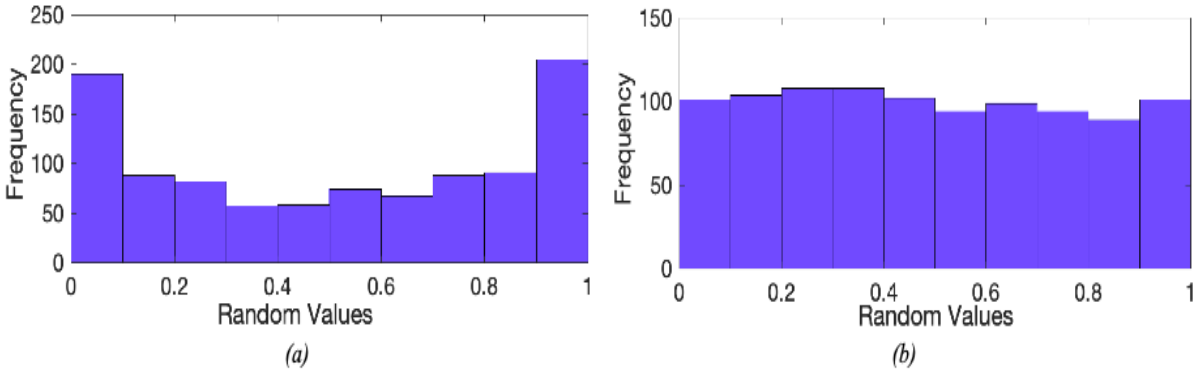

Fig. 8: Analysis and comparison of the histogram of the classic logistic map (a) 1D-PCE classic map (b).

3.3.Key space analysis

The cryptographic system space based on chaotic maps is made up of all the initial conditions and parameters. It is used as an indicator to assess resistance to brute force attacks. The new chaotic map introduces a new control parameter, which means that the entire key space is (α, r, and x0), whereas for the logistic map it is only 2.

4.CONCLUSION

In this manuscript, we have proposed a new chaotic scheme for cryptographic applications. The dynamic behaviour of the 1D-PCE card has been studied in terms of chaos domains and regular behaviour domains to evaluate the performance in random sequence generation. The new card has a sufficiently large key space, uniformly distributed chaotic sequences, and is very sensitive to initial conditions. The map performs much better than the logistic map.

5. Reference

1. A. Retia, A., Xing, Y. Quant, C., (2017). Optical image encryption using radon transform," 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL), Singapore, 2017, pp. 1235-1238
2. Alexa, W., Elkandoz, M., Mashaly, M., E. Azab, E., A. Aboshousha, E., (2023) Color Image Encryption through Chaos and KAA Map. IEEE Access,11, 11541-11554
3. Aziz, M. S., C. Tanougast, C, Sadoudi, S, Bouridane, A., (2013). Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption. Commun Nonlinear Sci Numer Simul, 18 (8), 2035–2047.
4. Borūjen, S. E., Ehsani, M. S., (2015). Modified Logistic Maps for Cryptographic Application. Appl. Math, 6 (5), 773–782.
5. Chen,T.H, Tsao,K.H, Lee,Y.S. Y, (2012). Multiple-image encryption by rotating random grids. Signal Process, 92(9):2229–37.
6. Faragallah O. S. et al (2019). Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding. IEEE Access,7,4184-4194
7. Francis, N., Lisha, A. & Monoth, T. (2024). Exploring recent advances in random grid visual cryptography algorithms. *J Supercomput* **80**, 23205–23224 (2024).
8. Gao, Y., Xie, H., Zhang, J., Zhang, H., (2022). A novel quantum image encryption technique based on improved controlled alternated quantum walks and hyper chaotic system. Physica A: Statistical Mechanics and its Applications, 598,127334
9. Hasheminejad, A., Rostami, M., (2019), A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map, Optik 184 (2019) 205–213.
10. Hu,X., Wei,L.,Chen,W., Chen.Q, Y. Guo,Y., (2020). Color image encryption algorithm based on dynamic chaos and matrix convolution. IEEE Access, 8, 12452-12466.
11. Li,S.,Chen,G.,Cheung,A.,Bhargava,B.,Lo,K-T.(2007). On the design of perceptual MPEGVideo encryption algorithms. IEEE Trans Circuits Syst Video Technol. 17 (2):214–23
12. Liu, H.J, Wang X.Y., (2010). Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl . 59(10):3320–7.
13. Maqableh, M., Samsudin, A., Alia, M. A., (2008). New hash function based on chaos theory (CHA-1). Int. J. Comput. Netw. Secur, 8 (2), 20–26.

14. Oravec, J., Lubos O.,Jan P.,(2021). An Image Encryption Algorithm Using Logistic Map with Plaintext-Related Parameter Values, Entropy 23(11)1373.
15. Pal J.K, (2016). Administering a cryptology center by means of scientometric indicators. Collnet Journal of Scientometrics and Information Management,10(1),97–123
16. Ramezanipour, N., Moattar, M.H., (2024). A secure and robust images encryption scheme using chaos game representation, logistic map and convolutional auto-encoder. Multimed Tools Appl 83, 74413–74440.
17. Shao, Z., Liu, X., Yao, Q., Qi, N., Shang, Y., Zhang, J.,(2020). Multiple- image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain. Sig. Process. Image Commun. 80, 115662
18. Ullah F., Faheem, Z.M., Hashmi, M. A., Aqeel-Ur-Rehman , Bashir, R. N., Khan, A. R.(2024). A Novel 1-Dimensional Cosine Chaotic Equation and Digital Image Encryption Technique.IEEEAcess, 12 , 118857-118874.
19. Wang, C., Chong, Z., Zhang H., Ma, P., Dong, W., (2024), Color image encryption based on discrete memristor logistic map and DNA encoding. Integration, 96, 2024
20. Wang,X.Y., Yang,L., Liu,R., Kadir,A.(2010). A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. 62(3), 615–21.
21. Xie.J,Yang,C.,Xie Q.,Tian. L., (2009),An Encryption Algorithm Based on Transformed Logistic Map, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China,111-114.
22. Xuejing, K., Zihui, G., (2020). A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Processing: Image Communication, 80, 115670
23. Yicong Z., Bao,L.,Philip Chen,C.L., A new 1D chaotic system for image encryption, Signal Processing,97,2014,172-182
24. Zhang, B., Lingfeng ,L (2023). Chaos-Based Image Encryption: Review, Application, and Challenges" Mathematics 11,11: 2585
25. Zhongyun H., Yicong Z., Hejiao H., (2019). Cosine-transform-based chaotic system for image encryption. Information Sciences,480, 403-419.
26. Zhou, N.R., Wu, J.W., Chen, M.X. et al. (2024), A Quantum Image Encryption and Watermarking Algorithm Based on QDCT and Baker map. Int J Theor Phys 63, 100