ISSN: 2687 - 4539

CHAOS
THEORY AND APPLICATIONS

IN APPLIED SCIENCES AND ENGINEERING

VOLUME 3, ISSUE 1, JUNE 2021

AN INTERDISCIPLINARY JOURNAL OF NONLINEAR SCIENCE

ISSN: 2687 - 4539

CHAOS

THEORY AND APPLICATIONS

IN APPLIED SCIENCES AND ENGINEERING

Chaos Theory and Applications (CHTA)
Volume: 3 – Issue No: 1 (June 2021)
https://dergipark.org.tr/tr/pub/chaos/issue/56378

Editorial Advisory Board Members

Language Editors

Technical Coordinator

ISSN: 2687 - 4539

CHAOS

THEORY AND APPLICATIONS

IN APPLIED SCIENCES AND ENGINEERING

Chaos Theory and Applications (CHTA)
Volume: 3 – Issue No: 1 (June 2021)
https://dergipark.org.tr/tr/pub/chaos/issue/56378

Contents

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
EDITORIAL
Vol.3 / No.1 / 2021 / pp.1-2

Chaos Theory and Applications: A New Trend

Guanrong Chen *,1
*Department of Electrical Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, Hong Kong.

It is amazing and also exciting to see a new journal **Chaos Theory and Applications** established recently. After chaos was coined with a precise model, the Lorenz system, more than half a century ago Lorenz (1963), there have already been many well-known journals on chaos Sprott (2010) such as, to name just a few specialized ones, Chaos, Chaos Solitons and Fractals, International Journal of Bifurcation and Chaos, Nonlinear Dynamics, and several Physical Review journals. Therefore, on the one hand, organizing a new journal on chaos needs a lot of courage and planning, and on the other hand, one can see that the chaos is still an ever-young subject for scientific research today.

Typically, a subject with linearity by nature would last for one or two decades of active research before it turns to be mature or even becomes a toolbox for efficient applications, whereas a subject of nonlinear-ity in essence could last for much longer time or forever. Chaos is one example. The Lorenz system has been an icon of the subject for study, which is simple in form as a three-dimensional, autonomous, second-order polynomial system with three equilibria, but has extremely complex dynamics. Notably, it never exclude other possible chaotic models to be developed. Rössler system Rössler (1976) was another icon that is even simpler with only two equilibria, followed by yet an engineering model, Chua's circuit Matsumoto *et al.* (1985), which is a simple piecewise linear system, not to mention many others (e.g. the generalized Lorenz systems family Chen *et al.* (2020)).

Great progress notwithstanding, all that were not the end of the chaos story. Recently, it was found that there are many Lorenz-like chaotic systems, namely three-dimensional autonomous second-order polynomial systems, however without equilibrium, or with one stable equilibrium, or with two stable foci, or with infinitely many equilibria on a curve or a surface in the three-dimensional phase space Chen *et al.* (2020). They were classified to be systems with hidden chaotic attractors Wang *et al.* (2021); Leonov and Kuznetsov (2013). In these systems, the traditional bifurcation analysis is inapplicable, since even eigenvalues of Jacobians at equilibria do not exist or cannot be well defined, thereby the familiar bifurcation analysis cannot be performed to characterize chaos, or to find a route to chaos, in such unusual non-hyperbolic systems. This poses great challenges to theorists in the field of bifurcation and chaos.

It is our expectation, therefore, that the new journal **Chaos Theory and Applications** could contribute more to this new direction of chaos research, along with other traditional topics.

Manuscript received: 16 August 2020,
Accepted: 17 August 2020.

[1] eegchen@cityu.edu.hk (**Corresponding author**)

LITERATURE CITED

Chen, G. *et al.*, 2020 Generalized lorenz systems family.arXiv preprint arXiv:2006.04066 .

Leonov, G. A. and N. V. Kuznetsov, 2013 Hidden attractors in dynamical systems. from hidden oscillations in hilbert–kolmogorov, aizerman, and kalman problems to hidden chaotic attractor in chua circuits. International Journal of Bifurcation and Chaos 23:1330002.

Lorenz, E. N., 1963 Deterministic nonperiodic flow. Journal of the atmospheric sciences 20: 130–141.

Matsumoto, T., L. Chua, and M. Komuro, 1985 The double scroll. IEEE Transactions on Circuits and Systems 32: 797–818.

Rössler, O. E., 1976 An equation for continuous chaos. Physics Letters A 57: 397–398.

Sprott, J. C., 2010, Journals with chaos and related papers. http://sprott.physics.wisc.edu/chaostsa/journals.htm.

Wang, X., N. V. Kuznetsov, and G. Chen (Editors), 2021 Chaotic systems with multistability and hidden attractors. (An edited book to be published)

How to cite this article: Chen, G. Chaos Theory and Applications: A New Trend. Chaos Theory and Applications, 3(1), 1-2, 2021.

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / No.1 / 2021 / pp.3-10
https://doi.org/10.51537/chaos.717432

A Chaos-Based Encryption Application for Wrist Vein Images

Ömer Faruk Boyraz [*,1], Murat Erhan Çimen [*,2], Emre Güleryüz [*,3] and Mustafa Zahid Yıldız [*,4]
[*] Department of Electrical & Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54187 Serdivan, Sakarya, Turkey.

ABSTRACT In this study, the images of the wrist vein taken from the individuals were subjected to various preprocessings and then encrypted with random numbers obtained from the chaotic system. Before encryption, random numbers were generated using a chaotic system. The random numbers produced have successfully passed the NIST 800-22 tests. Images encrypted with random numbers were subjected to security analysis such as correlation, NPCR, UACI and histogram analysis. With the study carried out, it has been shown that wrist vein patterns that can be used in authentication systems can be safely stored in the database.

KEYWORDS
Wrist vein image
Chaotic system
Random number generator
Encryption
Security analysis

INTRODUCTION

Biometrics allows individuals to classify individuals based on different physiological and behavioral characteristics, such as fingerprints, iris, manner of walking, and patterns of movement. While physiological features such as fingerprints, palm prints, iris are linked to the form of the body, behavioral features such as voice, handwriting signature, and walking are linked to the model of behavior of the person. (Lee *et al.* 2010). The near infrared wavelength is absorbed by the hemoglobin in the blood, and the region of vein near the skin are displayed darker with the infrared camera. Identification process from the vein pattern; It can be performed on various images such as dorsal hand vein pattern (Yildiz and Boyraz 2019), finger vein pattern (Cho *et al.* 2012), palm vein pattern (Raut *et al.* 2017) and wrist vein pattern (Niyaz *et al.* 2017).

Among the four different types of vascular patterns, the wrist vein pattern provides a clear view due to its close proximity to the outer skin and its intensive presence.

Wrist vascular biometry has not been studied much in the literature. In their study, Akhloufi and colleagues obtained the vascular network structures in the forearm wrist region through a CCD infrared camera. Anisotropic diffusion process was applied to improve the contrast of the images obtained, and then segmented the vascular network structures using morphological processes (Akhloufi and Bendada 2008).

Thanks to the lighting system and infrared camera platform designed by Pascual et al., they collected hand-wrist vein images and showed that these images are clear enough to be used for identification (Pascual *et al.* 2010).

Wrist vein are used in the process of personal identification. The advantage of performing touchless wrist vein recognition processes over other pattern recognition systems (touch based fingerprint, palm, finger vein, etc.) is the ability to conduct touchless identification and verification operations during image acquisition. In this way, in a more sterile setting, identification is achieved. Such advantages make touchless wrist vein recognition technology a more accurate and promising system that attracts increasing attention in security systems, hospitals, courthouses, banks, public institutions and industry.

Manuscript received: 9 April 2020,
Revised: 31 August 2020,
Accepted: 24 September 2020.

[1] oboyraz@subu.edu.tr (**Corresponding Author**)
[2] muratcimen@subu.edu.tr
[3] emre.guleryuz1@ogr.sakarya.edu.tr
[4] mustafayildiz@subu.edu.tr

Consequently, it is a crucial issue to secure fingerprint image transmission over the internet and its access in the open network environment. Therefore, it is very important to protect and store touchless wrist vein images by encrypting them.

Several technologies have been developed to secure and store various groups of images so far. Among these technologies, the chaos-based encryption method is the most intuitive and effective way to turn images into unrecognizable (Chai *et al.* 2017). Several image encryption algorithms have recently been proposed that can be used to preserve images at a high level of protection (Hua and Zhou 2017).

Dzwonkowski et al. presented an encryption scheme that uses quaternion to protect the image of DICOM (Digital Imaging and Communications in Medicine) (Dzwonkowski *et al.* 2015). Hsiao et al. Encrypted their contact fingerprint images using 2 different chaotic systems (Hsiao and Lee 2015). Random numbers produced using multiple chaotic system passed NIST SP 800-22a test. Zhang et al. proposed a medical image encryption and compression algorithm using the compression detection and pixel permutation approach. This algorithm will simultaneously encrypt and compress medical images. (Zhang *et al.* 2015).

Yildiz et al., In their study, encrypted the hand vein images that converted into 1 bit with a new encryption algorithm and stored them in the database (Yildiz *et al.* 2019).The SURF matching algorithm was used in the encrypted images.

In this study, wrist vein images taken from people with the help of infrared camera were subjected to various preprocesses on the microcomputer and it was aimed to store the vein images safely in the database since it is a personal data. After the wrist vein images were pretreated, they were encrypted by eXclusive OR (XOR) processing with random numbers obtained using the chaotic system.

MATERIAL AND METHOD

Material

Right and left hand wrist vein images obtained from a total of 50 volunteers from 20 females and 30 males used in the study were collected by the device shown in Figure 1. Volunteers were asked to place their wrists on the hand placement platform illuminated by infrared power leds with 850 nm wavelength and images were taken via an infrared camera.

The obtained images were transferred to the microcomputer environment and were subjected to image preprocessing and encryption algorithms, respectively. The encrypted images are securely stored in the database in the microcomputer environment.

Method

The block diagram of encryption of wrist vein images in microcomputer environment is shown in Figure 2. Hand-wrist vein images taken with the help of infrared camera were subjected to gray level conversion and contrast limited adaptive histogram equalizition processes, respectively. These images were then encrypted using random numbers obtained using the chaotic system.

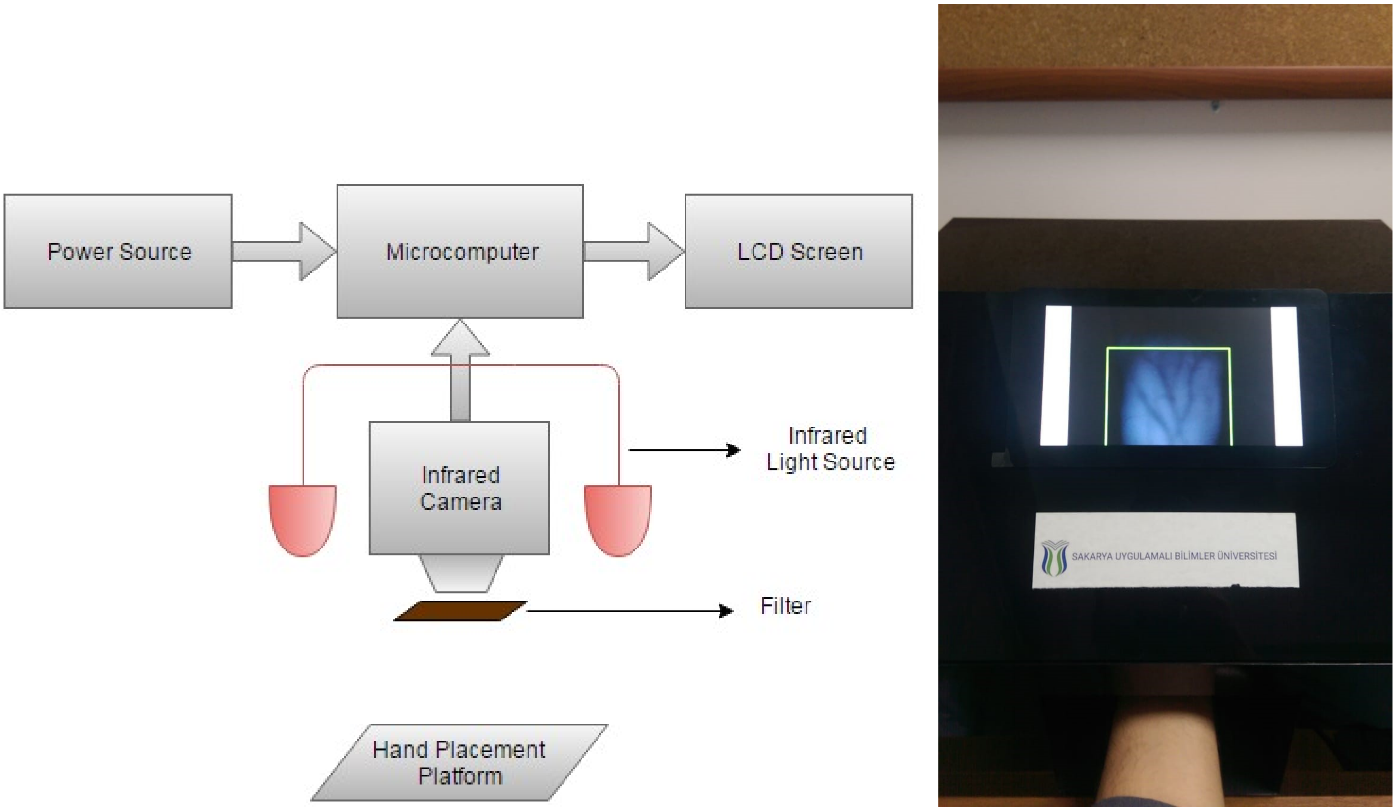
In this research, the chaotic system used is a continuous time, a chaotic 3-dimensional balance point system (Akgül *et al.* 2020). The system consists of 3 different differential equations as given in equation 1. There are three state variables in the system: x, y, z, and a total of four parameters: a, b, c, d. In order for the system to be chaotic, initial conditions are determined as x(0) = 0.4, y(0) = 0.1, z(0) = 0.

$$\begin{aligned}\dot{x} =& ax\\ \dot{y} =& -x + byz\\ \dot{z} =& -x - cxy - dxz\end{aligned} \tag{1}$$

For the system given in Equation 1, the parameters show a chaotic feature when a = 1.9, b = 1.1, c = 11.5 and d = 0.7. In Equation 2, the parameters of the chaotic system are shown.

$$\begin{aligned}\dot{x} =& 1.9y\\ \dot{y} =& -x + 1.1yz\\ \dot{z} =& -x - 11.5xy - 0.7xz\end{aligned} \tag{2}$$

There are several techniques of research to understand whether or not a system is chaotic. The analysis of the system's behavior (time series), phase portraits, lyapunov exponentials, bifurcation diagrams over a certain period of time are some of these analysis methods. As a result of these analyzes, the system has been shown to exhibit chaotic behavior (Akgül *et al.* 2020).



(a)

(b)

Figure 1 a)Block diagram of system (Boyraz and Yildiz 2016) b)Collection of hand-wrist images from volunteers

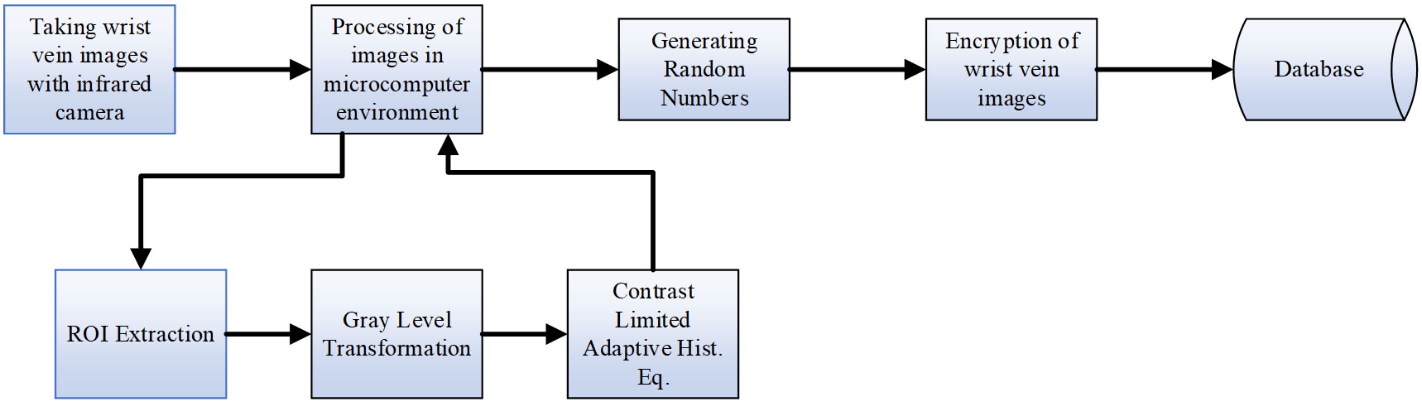

Taking wrist vein images with infrared camera
Processing of images in microcomputer environment
Generating Random Numbers
Encryption of wrist vein images
Database
ROI Extraction
Gray Level Transformation
Contrast Limited Adaptive Hist. Eq.

Figure 2 Block diagram of encryption of Hand-Wrist Vein images

PRE-PROCESSING OF WRIST IMAGES

Contrast improvement is aimed in the pre-processing process. The target area was removed from the wrist images taken with the help of the infrared camera, and then the contrast-limited adaptive histogram equalization was performed to make the vascular areas more visible.

The acquired images were first converted to gray level, and the areas of the vein were clarified by applying contrast-limited histogram equalization (CLAHE) method (Stimper *et al.* 2019). This method is used both on noise reduction and on medical images to eliminate the edge shadow effects in homogeneous areas. Figure 3 shows the vascular area, which has been converted to a gray level and the contrast has been improved with the CLAHE method. As a result of these processes, the stage before the 8-bit level encryption has been reached.

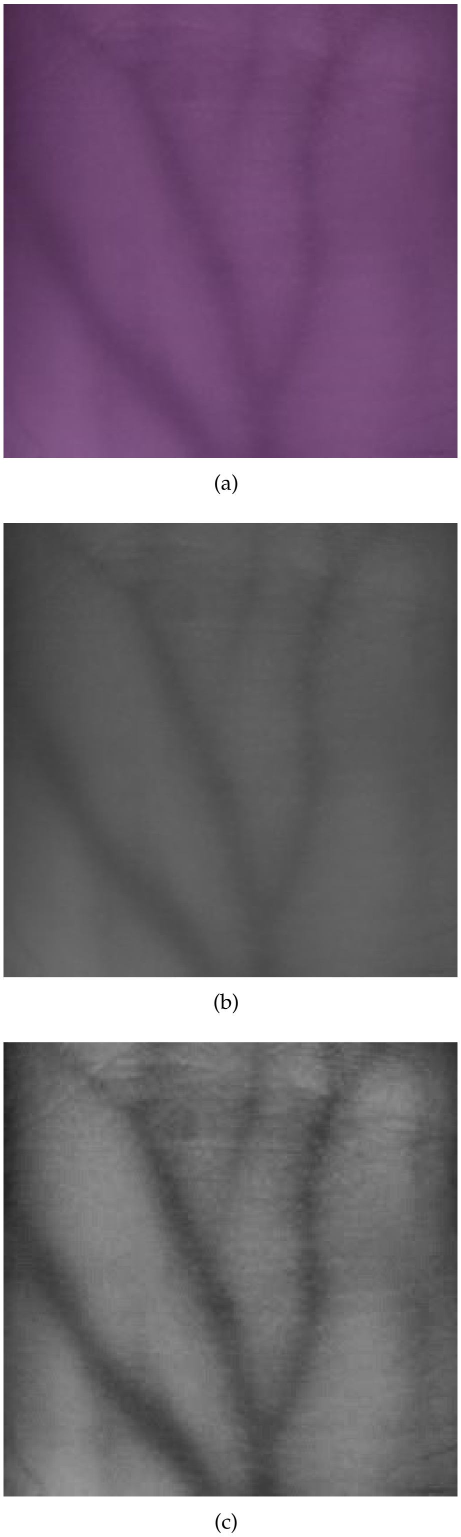
In Table 2 NPCR and UACI analyzes between the encrypted image and the 8-bit wrist image are given. According to the analysis, it is concluded that almost all the pixels of the 8-bit wrist image are changed and the image that is encrypted using random numbers produced from the chaotic 1system is formed. UACI results express the density of the changing pixels.

NIST 800-22 TESTS FOR RANDOMNESS

NIST-800-22 test was used to perform randomness tests of the produced numbers. The NIST-800-22 test bit sequence must pass all of these tests successfully to be considered successful. The NIST-800-22 test contains 16 different statistical tests which define the randomness of the bit sequences (Akgül *et al.* 2019). As all the numbers passed the test, it was concluded, according to Table 1. Randomness was obtained by random numbers created from the last 8 bits of the x, y and z values.

ENCRYPTION OF WRIST VEIN IMAGES

The flow chart showing the encryption of 8-bit vein images using random numbers produced is given in Figure 4. The wrist vein images taken are given to the system for encryption first. Then the dimensions of this image are calculated. Pixel values in each coordinate are converted to an 8-bit binary level. Number sequences converted into 8-bit binary level are subjected to XOR processing with random numbers generated from the chaotic system. After this process, the values formed are converted to decimal system and the pixel values of the encrypted image are obtained.



(a)

(b)

(c)

Figure 3 a) Raw image b) Gray Level c) CLAHE

Table 1 NIST-800-22 test results

Statistical Tests	P-value (X_8bit)	P-value (Y_8bit)	P-value (Z_8bit)	Results
The Frequency Test	0.3547	0.5425	0.4879	Successful
Frequency Test within a Block	0.4578	0.7421	0.6444	Successful
The Cumulative Sums Test	0.5412	0.3478	0.3789	Successful
The Runs Test	0.2879	0.3456	0.4785	Successful
Tests for the Longest-Run-of-Ones in a Block	0.6789	0.3127	0.1987	Successful
The Binary Matrix Rank Test	0.7214	0.4879	0.3414	Successful
The Discrete Fourier Transform Test	0.1754	0.1424	0.4232	Successful
The Non-overlapping Template Matching Test	0.7543	0.0425	0.1074	Successful
The Overlapping Template Matching Test	0.1987	0.7562	0.3412	Successful
Maurer’s Universal Statistical Test	0.7521	0.4017	0.3478	Successful
The Aproximate Entropy Test	0.1789	0.3485	0.6147	Successful
The Random Excursions Test (x = -4)	0.6755	0.3478	0.1977	Successful
The Random Excursions Variant Test (x = -9)	0.6478	0.3974	0.2476	Successful
The Serial Test-1	0.7213	0.3456	0.4102	Successful
The Serial Test-2	0.7620	0.4397	0.3157	Successful
The Linear Complexity Test	0.3024	0.3789	0.4987	Successful

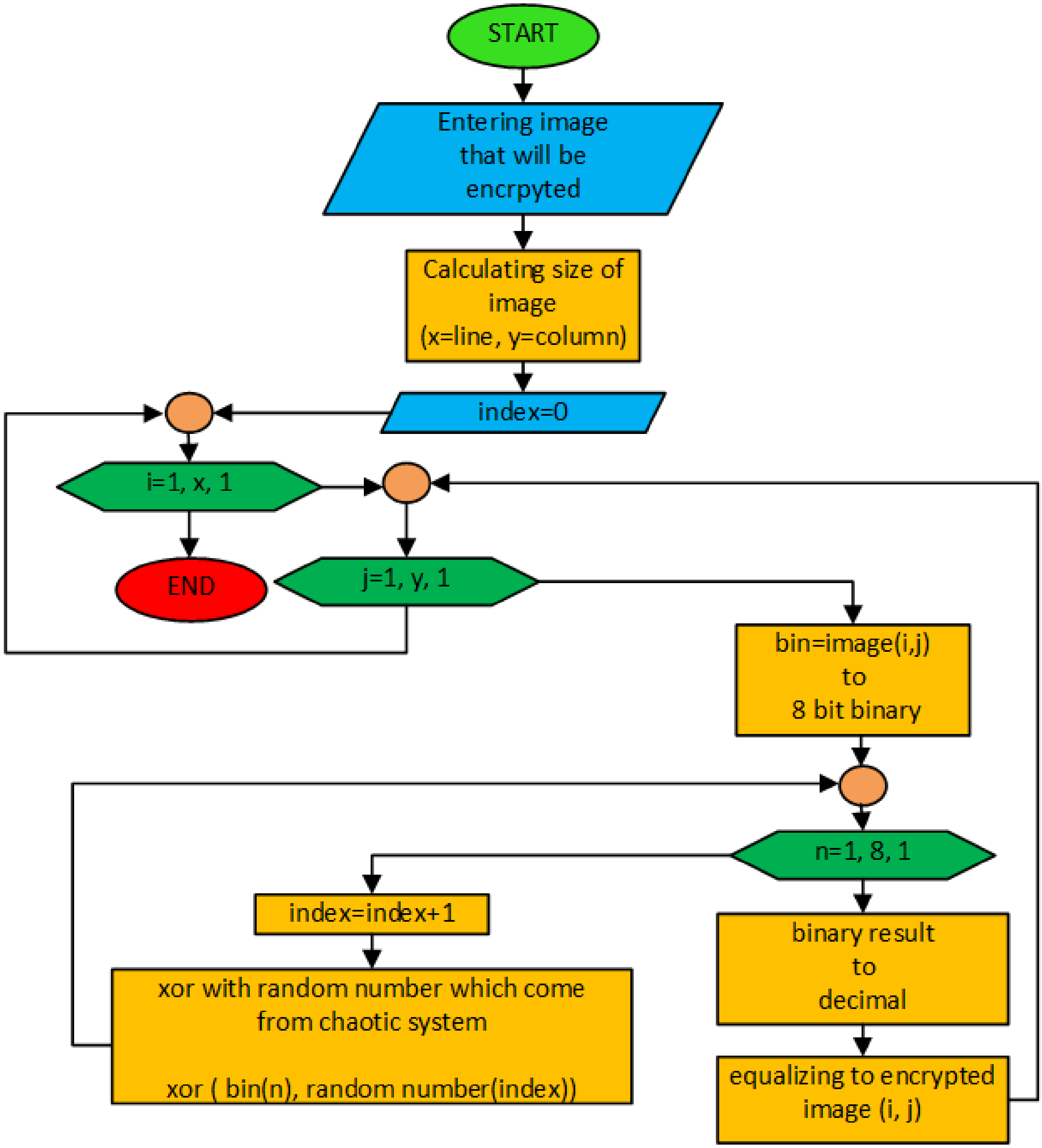
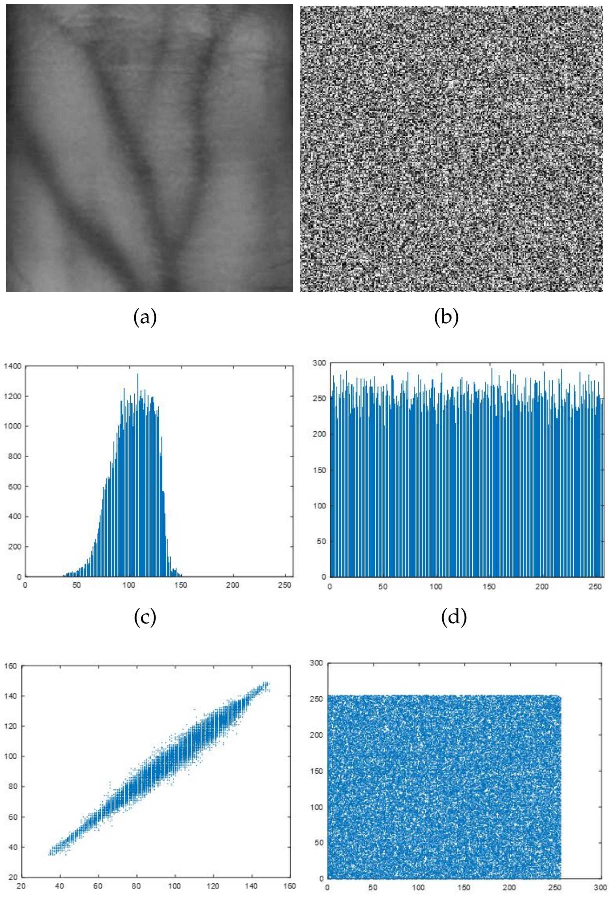

START
Entering image that will be encrpyted
Calculating size of image (x=line, y=column)
index=0
i=1, x, 1
END
j=1, y, 1
bin=image(i,j) to 8 bit binary
n=1, 8, 1
index=index+1
xor with random number which come from chaotic system
xor (bin(n), random number(index))
binary result to decimal
equalizing to encrypted image (i, j)

Figure 4 The Encryption Algorithm flowchart

SECURITY ANALYSIS

In this section, encryption operations are realized with random numbers produced from the chaotic system. The system's security analysis was performed using entropy, differential attack (NPCR, UACI), correlation and histogram methods after encryption. Figure 5 shows histogram analysis and correlation analysis of the encrypted wrist image. As a result of encryption, the correlation and histogram distributions of the images are homogeneous, indicating that the encryption is successful.



(a) (b) (c) (d) (e) (f)

Figure 5 a) Wrist vein image b) Encrypted wrist image c) Histogram distributions of Wrist vein d) Encrypted histogram distributions of Wrist vein e) Correlation map of wrist vein image f) Correlation map of encrypted wrist image

Table 2 Security analysis for sample images

Sample Images	NPCR	UACI
1. Encrypted image	99.7894	29.4785
2. Encrypted image	100	28.9789
3. Encrypted image	99.8974	29.7454

CONCLUSION

In this article, the wrist vein images taken from people with the help of infrared camera are transferred to microcomputer, passed through various preprocesses, encrypted as chaos-based and security analysis are performed. Vein images vary from individual to individual, much like fingerprints. Hiding these data is therefore very necessary for the protection of the biometric recognition system. These images are encrypted and stored in the database to ensure the system's protection. Random numbers produced from the x, y and z phases of the chaotic system have successfully passed the internationally accepted NIST-800-22 tests Rukhin *et al.* (2001) and have been found to provide randomness in all 3 phases. In the encryption part, the encryption process was performed with random numbers generated. The images obtained after encryption and the pretreated vein images were analyzed by histogram, correlation, entropy, NPCR and UACI analysis and the encryption was successful.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Akgül, A., C. Arslan, and B. Arıcıoğlu, 2019 Design of an interface for random number generators based on integer and fractional order chaotic systems. Chaos Theory and Applications **1**: 1–18.

Akgül, A., M. Z. Yıldız, Ö. F. Boyraz, E. Güleryüz, S. Kaçar, *et al.*, 2020 Doğrusal olmayan yeni bir sistem ile damar görüntülerinin mikrobilgisayar tabanlı olarak şifrelenmesi. Journal of the Faculty of Engineering & Architecture of Gazi University **35**.

Akhloufi, M. and A. Bendada, 2008 Hand and wrist physiological features extraction for near infrared biometrics. In *2008 Canadian Conference on Computer and Robot Vision*, pp. 341–344, IEEE.

Boyraz, Ö. F. and M. Z. Yildiz, 2016 Mobil damar görüntüleme cihazı tasarımı. In *4th International Symposium on Innovative Technologies in Engineering and Science (ISITES2016) 3-5 Nov 2016 Alanya/Antalya-Turkey*.

Chai, X., Z. Gan, Y. Chen, and Y. Zhang, 2017 A visually secure image encryption scheme based on compressive sensing. Signal Processing **134**: 35–51.

Cho, S. R., Y. H. Park, G. P. Nam, K. Y. Shin, H. C. Lee, *et al.*, 2012 Enhancement of finger-vein image by vein line tracking and adaptive gabor filtering for finger-vein recognition. In *Applied Mechanics and Materials*, volume 145, pp. 219–223, Trans Tech Publ.

Dzwonkowski, M., M. Papaj, and R. Rykaczewski, 2015 A new quaternion-based encryption method for dicom images. IEEE Transactions on Image Processing **24**: 4614–4622.

Hsiao, H.-I. and J. Lee, 2015 Fingerprint image cryptography based on multiple chaotic systems. Signal Processing **113**: 169–181.

Hua, Z. and Y. Zhou, 2017 Design of image cipher using block-based scrambling and image filtering. Information Sciences **396**: 97–113.

Lee, E., H. Jung, and D. Kim, 2010 Infrared imaging based finger recognition method. In *Proceedings of International Conference on Convergence and Hybrid Information Technology*, pp. 228–230.

Niyaz, O., Z. G. Cam, and T. Yildirim, 2017 Wrist vein recognition by ordinary camera using phase-based correspondence matching. In *Modelling, Identificat. Control*, pp. 89–93.

Pascual, J. E. S., J. Uriarte-Antonio, R. Sanchez-Reillo, and M. G. Lorenz, 2010 Capturing hand or wrist vein images for biometric authentication using low-cost devices. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 318–322, IEEE.

Raut, S. D., V. Humbe, and A. V. Mane, 2017 Development of biometrie palm vein trait based person recognition system: Palm vein biometrics system. In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, pp. 18–21, IEEE.

Rukhin, A., J. Soto, J. Nechvatal, M. Smid, and E. Barker, 2001 A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-allen and hamilton inc mclean va.

Stimper, V., S. Bauer, R. Ernstorfer, B. Schölkopf, and R. P. Xian, 2019 Multidimensional contrast limited adaptive histogram equalization. IEEE Access **7**: 165437–165447.

Yildiz, M. Z., O. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, 2019 A novel encryption method for dorsal hand vein images on a microcomputer. IEEE Access **7**: 60850–60867.

Yildiz, M. Z. and Ö. F. Boyraz, 2019 Development of a low-cost microcomputer based vein imaging system. Infrared Physics & Technology **98**: 27–35.

Zhang, L.-b., Z.-l. Zhu, B.-q. Yang, W.-y. Liu, H.-f. Zhu, *et al.*, 2015 Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. Mathematical Problems in Engineering **2015**.

How to cite this article: Boyraz, O. F., Cimen, M. E., Guleryuz, E. and Yildiz, M. Z. A Chaos-Based Encryption Application for Wrist Vein Images. Chaos Theory and its Application, 3(1), 3-10, 2021.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / No.1 / 2021 / pp.11-19
https://doi.org/10.51537/chaos.835222

Designing a Pseudo-Random Bit Generator Using Generalized Cascade Fractal Function

Shafali Agarwal *,1
*Independent Researcher, 9600 Coit Road, Plano, TX 75025, USA.

ABSTRACT A cascade function is designed by combining two seed maps that resultantly has more parameters, high complexity, randomness, and more unpredictable behavior. In the paper, a cascade fractal function, i.e. cascade-PLMS is proposed by considering the phoenix and lambda fractal functions. The constructed cascade-PLMS exhibits the required fractal features such as fractional dimension, self-similar structure, and covering entire phase space by the data sequence in addition to the chaotic properties. Due to the chaotic behavior, the proposed function is utilized to generate a pseudo-random number sequence in both integer and binary format. This is the result of an extreme scalability feature of a fractal function that can be implemented on a large scale. A sequence generator is designed by performing the linear function operation to the real and imaginary part of a cascade-PLMS, cascade-PLJS separately, and the iteration number at which the cascade-PLJS converges to the fixed point. The performance analysis results show that the given method has a large key space, fast key generation speed, high key sensitivity, and strong randomness. Therefore, the scheme can be efficiently used further to design a secure cryptosystem with the ability to withstand various attacks.

KEYWORDS
Mandelbrot set
PRNG
Cascade phoenix lambda fractal
Key security analysis
Dynamic behavior

INTRODUCTION

An internet era extends the security requirement of the digital information transmitted over the unsecured network. Cryptography is one of the most prominent ways to protect the data from illegitimate users (SI 1998). Since the last few years, a chaotic system has attracted researchers to utilize it in the field of cryptography. The dynamical properties of a non-linear chaotic system such as unpredictability, randomness, sensitivity to the minute change in its initial value, ergodicity, complex structure and deterministic dynamics lead it to a secure cryptosystem design. The abovementioned properties encourage to construct of a chaotic system having increased security and high complexity (Devaney 2018).

A fractal is a graphical representation of a chaotic function with complex structure and infinite scaling in each direction. In addition to chaotic behavior, a fractal function possesses more features such as construction in a complex domain, fractional dimension, self-similarity, etc. (Devaney *et al.* 1989; Mandelbrot and Mandelbrot 1982). A hybrid fractal function exhibits the characteristics of seed functions with more controlling parameters. Recently, a composite fractal function has been proposed by the author and discussed the suitability of the function in an image cryptosystem design (Agarwal 2020). Even many hybrid chaotic maps and their applicability in a pseudo-random generator, cryptography, s-box design have been studied by the researchers (Artuğer and Özkaynak 2020; Bai *et al.* 2020; Hua *et al.* 2018; Lynnyk *et al.* 2015; Moysis *et al.* 2020a). Additionally, fractal geometry is widely utilizing in user authentication (Motỳl and Jašek 2011), medical image analysis (Dey *et al.* 2018), and image hashing (Khelaifi and He 2020). Unpredictable behavior and extreme sensitivity towards the change in initial values prefer a fractal function to design a pseudo-random number sequence (PRNG).

Manuscript received: 3 December 2020,
Revised: 1 February 2021,
Accepted: 3 February 2021.

[1] shafali.agarwal@gmail.com

A pseudo word indicates a random sequence calculated using a deterministic system. According to mathematical theory, a deterministic system is predictable. A complex sequence generator including the process to select a seed value can help to enhance the security and reduce the correlation in the generated sequence. A PRNG has a wide range of applicability in various fields such as in the game industry, artificial intelligence, cryptography, statistical simulation, and many more. On the other hand, a true random number sequence is produced by the author by visualizing spontaneous chaotic oscillation of the current through semiconductor superlattices (Bonilla *et al.* 2016).

Recently, Barnsley's chaos game rules were utilized to generate a pseudo-random sequence (Ayubi *et al.* 2020). A complex Newton fractal function was used to generate a secure PRNG due to the strong statistical characteristics and a random phase space (Barani *et al.* 2020). An additional advantage of the map is to have a PRNG in an integer as well as a complex form. A modified logistic map was utilized to generate PRNG in two phases, including initial pseudo-random sequence and normal pseudo-random sequence using the value obtained in the previous phase (Wang and Cheng 2019). Another modified logistic map was successfully applied to generate random bit sequences by performing a comparison between maps, XOR, and bit reversal (Moysis *et al.* 2020b). An original logistic map was coupled with a piecewise map to implement a chaotic pseudo-random number generator (Sahari and Boukemara 2018). To overcome the chaotic degradation that arises due to the computational accuracy, a self-perturbed hyperchaotic system based PRN generator is proposed. The used hyperchaotic map is derived using the classical Lorenz three-dimensional chaotic system (Zhao *et al.* 2019). A similar Lorenz-like Chen chaotic system (Chen and Ueta 1999) was utilized by the author to generate a complex pseudo-random number generator (Hamza 2017). Earlier a PRN generator was proposed using the time series obtained from the generalized Lorenz chaotic map (Lynnyk *et al.* 2015). The author proposed a method in (Moysis *et al.* 2020a) to generate a PRNG by extracting around 8 bits per iteration from the decimal part of the chaotic map. The method was tested on various one-dimensional maps including the logistic map, sine map, Renyi map, Chebyshev map, cubic map, cubic logistic map.

In this paper, the cascading of two fractal functions is proposed with the applicability of the function in the design of a pseudo-random number generator. The emergence of the chaotic characteristics of two maps provides a more complex environment to produce a PRNG. The change in any single parameter realizes to a completely new data sequence, which is the foremost requirement of a secure PRNG. The main contribution in the paper can be summarized as follows:

1. A cascade structure of the fractal function is implemented using Phoenix and lambda fractal functions.
2. The dynamical behavior of the proposed cascade-PLMS is thoroughly investigated by analyzing its dimension, self-similar structure, trajectory, and cobweb diagram.
3. A method to generate a pseudo-random number sequence is proposed by using a combination of a cascade-PLMS, cascade-PLJS fractal function, and a fixed-point value resultant the execution of a particular cascade-PLJS.
4. The randomness and security of the generated PRNG are verified with various tests such as key space, key sensitivity, correlation value, autocorrelation analysis, information entropy, etc.

The rest of the paper is organized as follows. The structure of the proposed cascade-PLMS, and cascade PLJS and their dynamical properties are studied in section 2. In section 3, the generated fractal functions are applied to produce a pseudo-random bit sequence. In section 4, the randomness and security performance of the generated PRNG are analyzed. Finally, the paper is concluded with a discussion of future work direction in section 5.

A CASCADE FRACTAL FUNCTION AND IT'S DYNAMICAL BEHAVIOR ANALYSIS

A cascade fractal function (Cascade-FF) is designed by considering two seed functions (for example $F_1(x)$ and $F_2(x)$) connected in the series. For each iteration, the output of $F_1(x)$ is fed into the $F_2(x)$ as input, and the output of $F_2(x)$ is fed as an input to the $F_1(x)$. A repetitive output value feeding to each other until the number of iteration limit gets over (Zhou *et al.* 2014). Mathematically, for functions $F_1(x)$ and $F_2(x)$, a cascade-FF is defined as follows:

$$x_{n+1} = F_1(F_2(x_n)) \tag{1}$$

where $F_1(x)$ and $F_2(x)$ two seed functions which can be the same or different. A function is known as a cascade with itself if the same functions are using in the cascade-FF design. In that case, the function definition will be:

$$x_{n+1} = F_1(F_1(x_n)) \tag{2}$$

A cascade-FF has the ability to exhibit different structures while changing the order of contributed seed functions. Such as:

$$x_{n+1} = F_1(F_2(x_n)) \tag{3}$$

and

$$x_{n+1} = F_2(F_1(x_n)) \tag{4}$$

The paper focuses on the single aspect of designing a cascade-FF using phoenix and lambda fractal function. Let's recall the mathematical definition of the phoenix fractal and lambda fractal functions respectively (Peitgen *et al.* 2006):

$$\begin{aligned} z_{(n+1)} &= z_n^a + z_n^b c + p z_{(n-1)} \\ z_{(n+1)} &= c z_n (1 - z_n)^{(w-1)} \end{aligned} \tag{5}$$

where $c \in C$, and $-1 < p < 1$ with $z_0 \neq 0$. The fractal images generated by executing both functions are shown in Figure 1.

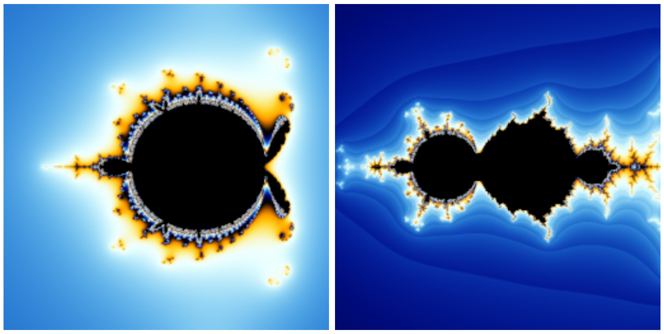


Figure 1 a) Phoenix fractal b) Lambda fractal.

Cascade-PLMS and Cascade-PLJS

A cascade-PLMS function is proposed to have a more complicated chaotic structure that is controlled by many parameters as compared to an individual. Too many parameters give the flexibility to have a more random and unpredictable output sequence by varying its value. By considering the phoenix fractal as $F_1(x)$ and lambda fractal as $F_2(x)$), a cascade-PLMS is defined as follows:

$$\begin{aligned} tempz &= z_n^a + z_n^b c + pz_{(n-1)} \\ z_{(n+1)} &= c * tempz(1 - tempz)^{(w-1)} \end{aligned} \tag{6}$$

All variables have their usual meaning except tempz. It represents an intermediate value of the phoenix function which has fed to the lambda function as input. The cascade-PLMS function is a set of c values for which the orbit of starting value i.e. z_n remains bounded under the function iteration. The proposed cascade-PLMS function is utilized to generate a pseudo-random number sequence with the parameter values $z_0 = 0.09$, $p = -0.03$, $a = 2$, $b = 1$, and $w = 3$.

A cascade phoenix lambda Julia set (cascade-PLJS) is nothing but a fractal image of the same function for a fixed c value starting with a nonzero z value. The paper has shown a cascade-PLJS image for $c = (0.7444196429, 0.6863839286)$. Both fractal images are plotted for the above-given parameter values using the UltraFractalTM and shown in Figure 2. A repetitive execution of the function with a fixed c value makes it converge to a fixed-point attractor, depending on whether the c value lies inside the cascade-PLMS image or outside of it. The convergence rate of the function varies for different c values. The iteration number at which the cascade-PLJS converges will be utilized in the pseudo-random number generation method.

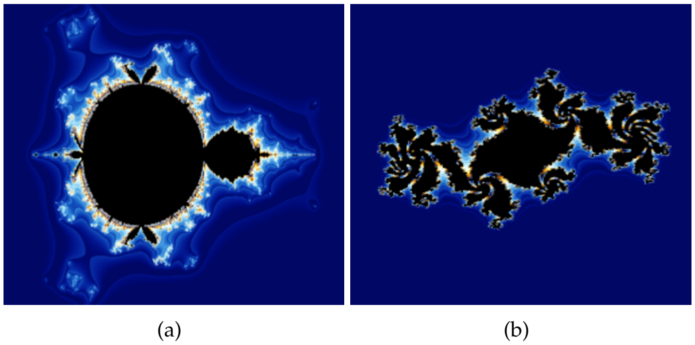


Figure 2 a) Cascade-PLMS b) Cascade-PLJS.

Dynamical Properties Analysis of Cascade-PLMS

Self-Similar Structure A fractal image is well-known to have a self-similar structure at a wide range of different scales. The beauty of a Mandelbrot set is to have infinite information on a small area of interest. As you zoom into the set, you will get newer fascinating images. A new cascade-PLMS is supposed to create an artistically appealing fractal image that also exhibits new patterns upon further exploration. Figure 3 shows randomly selected fractal images obtained by zooming the cascade-PLMS function.

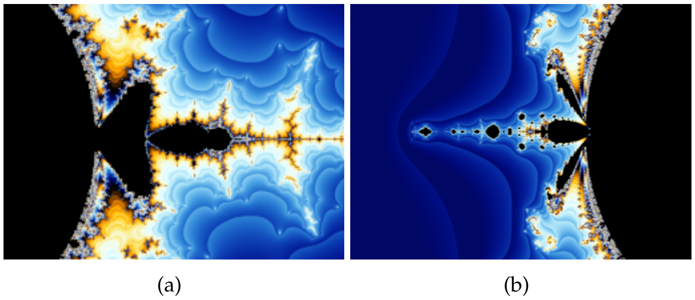


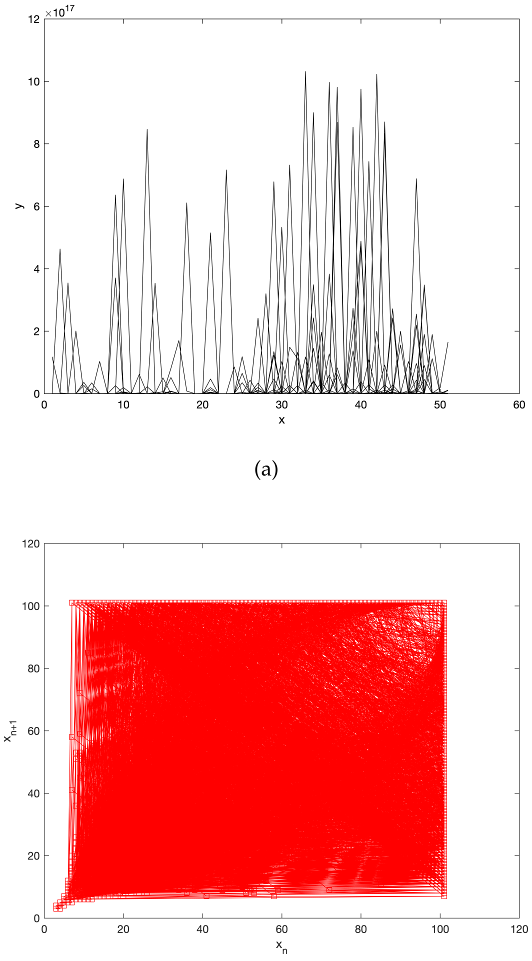
Figure 3 (a)-(b) Zoomed version of cascade-PLMS

Fractal dimension According to Felix Hausdorff (Czyz 1994), rough and broken fractal images should have an "in-between" dimension. This is a common way to measure the complexity of a fractal image boundary. A non-regular two-dimensional fractal image is supposed to have a dimension value between one and two. Recently, the author developed a user interface to calculate the fractal dimension using the box-counting method (Çimen *et al.* 2020). If a fractal image is superimposed by a grid of N squares to occupy the E number of edges, the fractal dimension can be calculated as:

$$\dim = \frac{\log N}{\log E} \tag{7}$$

The fractal dimension for several cascade-PLMS was calculated to verify the fractional structure of the proposed system. The obtained results were able to satisfy the requirement of a fractal function. The fractal dimension of the proposed cascade-PLMS function for the above-discussed parameters is 1.1535.

Trajectory and Cobweb diagram A cobweb and trajectory diagrams are used to display the successive iterations of a function. The only difference is that a cobweb diagram presents the function behavior of a one-dimensional map whereas a trajectory diagram is used to show the path of the generated number sequence of the multi-dimensional map. The chaotic behavior of a function can be justified by distributing the generated sequence over time in the entire phase space. A cascade-PLMS fractal image is generated based on the number of iterations required to bound the initial value within the image. At the same time, a sequence of a complex number is also generated on the execution of the function for each initial value. Therefore, the below Figure 4 shows a cobweb diagram to show the occupancy of the space by the iteration values and also a trajectory diagram to present the relationship between real and imaginary values. It can be stated that the produced data covers the entire phase space in both diagrams.



(a)

(b)

Figure 4 a) Trajectory diagram b) Cobweb diagram.

APPLICATION TO PSEUDO-RANDOM BIT GENERATION

The pseudo-random number generator is implemented by considering the above proposed cascade-PLMS and its corresponding cascade-PLJS functions. All randomness tests verify the suitability of the proposed cascade functions to generate an unpredictable number sequence. A pictorial representation of the proposed method can be seen in Figure 5.

The process starts by executing both the functions using the initial values set within the respective value range. Here, the cascade-PLMS function generates a sequence by considering initial values (z_0, a, b, c, p, w) as $(0.09, 2, 1, 0, -0.03, 3)$ while the c value is considered $(0.7444196429, 0.6863839286)$ in cascade-PLJS assuming other values same as in cascade-PLMS. The detailed method of the proposed technique is described as follows:

Step 1: *Calculate zdataMS and zdataJS as a set of a complex number after executing the cascade-PLMS and cascade-PLJS using the above-mentioned initial values set respectively.*

Step 2: *Calculate the fixed point of the cascade-PLJS function for a given c value and record the maximum iteration number (Itr) at which the fixed point is obtained.*

Step 3: *Separate real and imaginary parts of the zdataMS into zdataMSreal and zdataMSimg and convert it into a one-dimensional array.*

Step 4: *Repeat step 3 using $zdataJS$ and obtained $zdataJSreal$ and $zdataJSimg$ in a one-dimensional vector.*

Step 5: *Perform the linear function operation on the real number sequence of both the functions and Itr as follows:*

$$updatedRealSeq = zdataMSreal * Itr + zdataJSreal \tag{8}$$

Step 6: *Perform the same linear function operation on the imaginary number sequence of both the functions and Itr as follows:*

$$updatedImgSeq = zdataMSimg * Itr + zdataJSimg \tag{9}$$

Step 7: *Convert float numbers to an integer by executing the given function separately for real sequence and imaginary sequence as follows:*

$$\begin{aligned} IntRealSeq &= round((updatedrealSeq * 2^{14}) mod 256) \\ IntImgSeq &= round((updatedImgSeq * 2^{14}) mod 256) \end{aligned} \tag{10}$$

Step 8: *At last, a pseudo-random sequence is computed by concatenating both the sequences obtained prior using the following function:*

$$\begin{aligned} PRNG(2j) &= IntRealSeq(i) \\ PRNG(2j+1) &= IntImgSeq(i) \end{aligned} \tag{11}$$

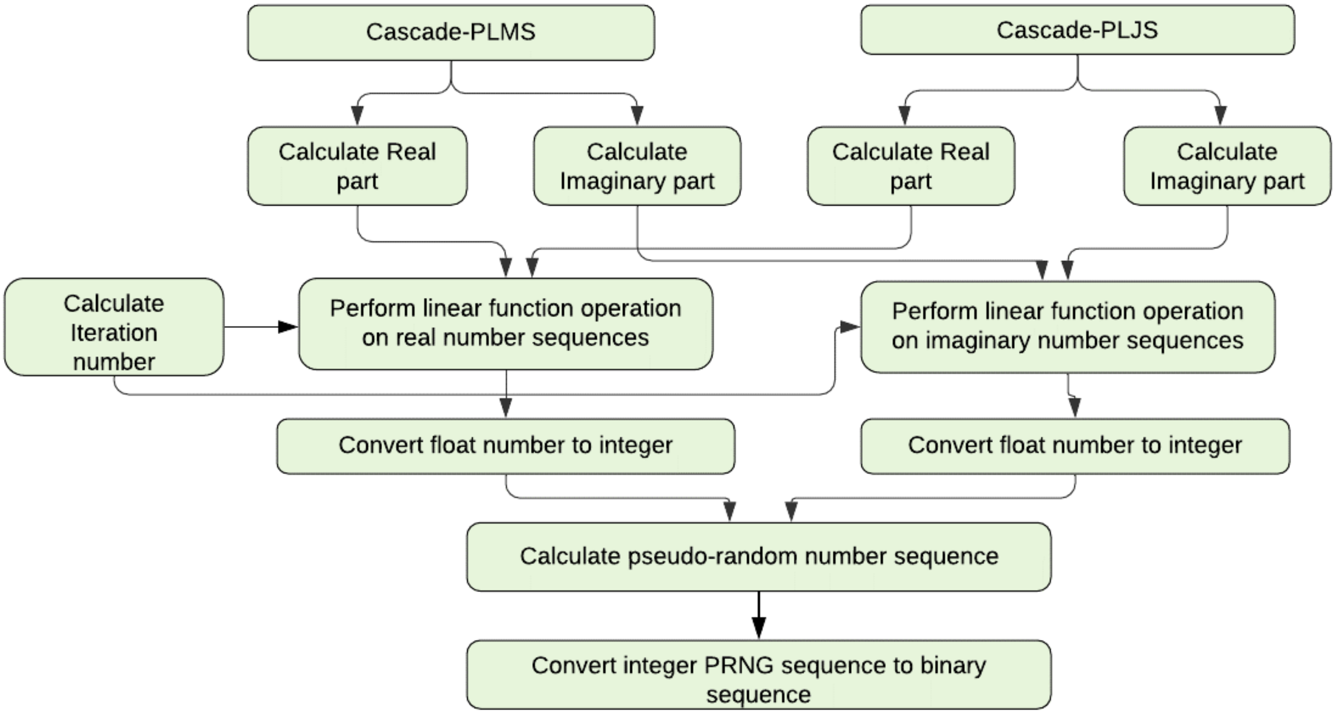

Cascade-PLMS
Cascade-PLJS
Calculate Real part
Calculate Imaginary part
Calculate Real part
Calculate Imaginary part
Calculate Iteration number
Perform linear function operation on real number sequences
Perform linear function operation on imaginary number sequences
Convert float number to integer
Convert float number to integer
Calculate pseudo-random number sequence
Convert integer PRNG sequence to binary sequence

Figure 5 Block diagram of proposed PRNG method

where $i = 1, 2, \ldots, 500000$ and initialize j=0. As a result, an integer sequence of length 10^6 is obtained. After converting it into binary form, an 8-bit binary sequence of length $8 * 10^6$ is produced. Hence, eight different binary random number sequences can be generated by combining the digits column-wise. To have a more random outcome, intermediate 500000 values of each real and imaginary data are considered while concatenating the sequence to get a pseudo-random number sequence.

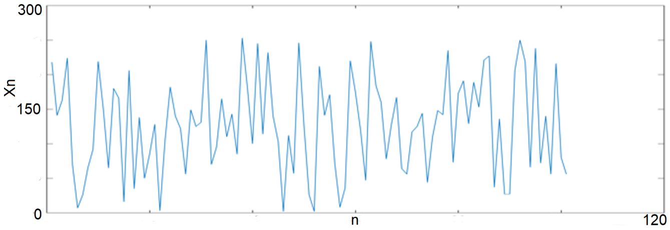


Figure 6 Visual path of generated number sequence

RANDOMNESS AND SECURITY ANALYSIS

Visual Representation of PRN Sequence

A trajectory diagram is used to display the path followed by the sequence generated upon the execution of the function for a particular set of initial values. A non-linear pixel path distributed over the entire phase space represents the chaotic behavior of the map. By selecting an appropriate set of initial values set can lead to producing a random number sequence that does not show the periodic or closed curve behavior. Figure 6 displays a trajectory diagram of randomly selected 500 pixels.

Key Space

Key space is an important index to indicate a secure cryptosystem. The generator uses a cascade fractal function having a set of initial values and control parameters to generate a pseudo-random sequence. As per the function requirement, a set of values includes (z_0, a, b, c, p, w) and a previous z value. According to the IEEE floating-point standard, a computational precision of a double datatype number is about 10^{15}. Therefore, the possible key space is calculated as $\left(10^{15}\right)^7 = 10^{105} \approx 2^{320}$. Thus, the available key space is large enough than the prescribed range of 2^{100} that is required to resist the brute-force attack (Alvarez and Li 2006).

Key Generation Speed

The proposed PRNG method is implemented on MATLABTM with a MacBook Pro having system configuration 2.6 GHz 6-Core Intel Core i7, and 16 GB memory. The approximate time to produce a random key sequence of size $1000 * 1000$ is 0.2084 sec.

Key Sensitivity using NBCR Analysis

A key sensitivity test analysis is done to evaluate the impact of the slight change in the input value to its corresponding output value. The sensitiveness of the proposed pseudo-random number generator is tested by executing two tests: 1) visual criterion, 2) the number of bit change rate (NBCR).

To evaluate the visual impact of two sequences, a control parameter value of the function is increased by 10^{-14} and others remain constant. Figure 7 shows the reaction of both the sequences generated through initial values and the small perturbed data set. It can be concluded from the figure that the generated number sequence is completely different even by making a small change in the control parameter value. The other test calculates the number of changed bits between two sequences. It is calculated as follows:

$$NBCR = \frac{Ham\_dis(x,y)}{bit\_len} \tag{12}$$

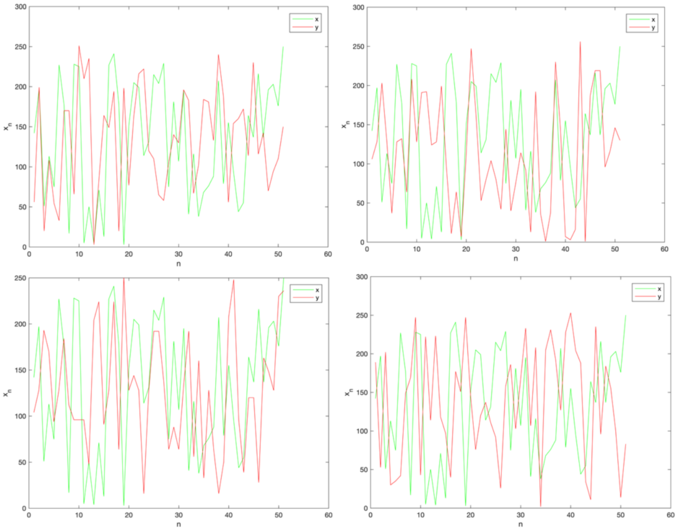


Figure 7 Graphical representation of key sensitivity analysis of generated sequence produced using original values and altered values

The number of the bit change rate of two different number sequences is expected to be close to 50%. NBCR result in Table 1 indicates that the initially generated pseudo-random sequence is different from the sequence generated after increasing a control parameter value slightly. Therefore, the generated sequences prove the key sensitiveness of the proposed pseudo-random number generator.

Entropy Analysis

An information entropy concept was introduced by Shannon to describes the randomness and uncertainty in the information system (Shannon 1949). It can be computed using the given function:

$$H(s) = -\sum_{i=0}^{(2^n-1)} p(x_i) log_2[p(x_i)] \tag{13}$$

Table 1 NBCR value of generated sequence produced using original values and altered values

Changed Parameter	NBCR Value
Change in initial value z (Seq1)	49.90
Change in distortion (Seq2)	49.95
Change in power 'a' (Seq3)	50.01
Change in power 'w' (Seq4)	50.04

where $p(x_i)$ denotes the probability of occurrence of a symbol x_i in the pseudo-random sequence. If n number of bits are required to represent a symbol, the entropy of the information system is supposed to be close to n. A binary sequence requires only one bit to show the symbol, i.e. either zero or one. Therefore, an entropy value of a binary sequence equals to one is considered as ideal value to exhibit the randomness of the sequence.

Correlation Analysis

A correlation coefficient is calculated to analyze the relationship between the two pseudo-random number sequences. A value close to zero depicts no relationship between the two sequences whereas strongly related sequences have *a* correlation coefficient value near to one. Due to the cascading of the two functions, many parameters are involved in the pseudo-random number generator. Therefore, the correlation analysis is done by varying *a* key at *a* time and keeping constant the other parameters. For two sequences x and y, the correlation coefficient is calculated using the given equation:

$$CC(x,y) = \frac{N\sum_{i=1}^{N}(x_i y_i) - \sum_{i=1}^{N}(x_i)\sum_{i=1}^{N}(y_i)}{\sqrt{N\sum_{i=1}^{N}(x_i)^2 - \left(\sum_{i=1}^{n}(x_i)^2\right)\left(N\sum_{i=1}^{N}(y_i)^2 - \left(\sum_{i=1}^{n}(y_i)^2\right)\right)}} \tag{14}$$

Table 2 displayed the effect of changing parameters in terms of correlation coefficient value. Each time a new sequence, i.e. y is generated by adding $\varepsilon = 10^{-14}$ to the previous parameter value and also keeping others as same as before. The process is executed for every parameter in the same way and calculated the corresponding correlation value. The obtained values indicate the high sensitivity of the sequence towards the minute change in the parameter value.

Table 2 Correlation coefficient value of generated sequence produced using original values and altered values

Changed Parameter	Correlation coefficient
Change in initial value z (Seq1)	0.0034
Change in distortion (Seq2)	0.0024
Change in power ’a’ (Seq3)	-0.0003
Change in power ’w’ (Seq4)	0.0005

Autocorrelation Analysis

Autocorrelation analysis is carried out to measure the similarity between a sequence OS and its corresponding shifted sequence OSS. The formula to calculate autocorrelation of a sequence with size N is given as:

$$AC = \frac{M1 - M2}{N} \tag{15}$$

where $M1$ and $M2$ refer to the number of matches and mismatches between the OS and OSS respectively. A value that falls in a range $[-1, 1]$ depicts a highly random number sequence with a small correlation with itself. A graphical view of pixel autocorrelation can be seen in Figure 8.

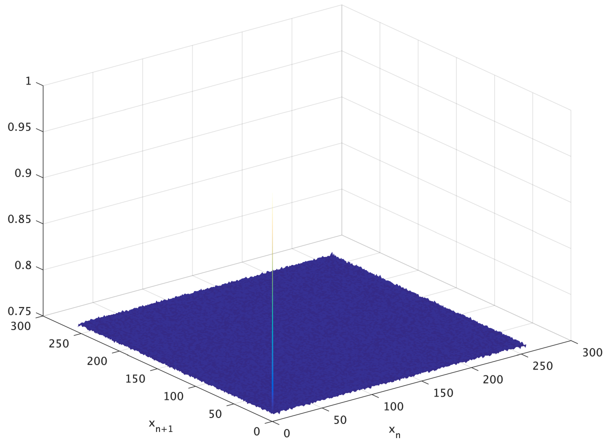


Figure 8 Autocorrelation analysis of number sequence

Performance Comparison with Existing Encryption Algorithms

A comparative analysis of the proposed scheme with the other existing PRNG methods is discussed in the section. The comparison is mainly focused on the evaluation parameters such as key space, entropy, number of bit change rate, and adjacent pixels correlation. Table 3 listed the data of various considered PRNG methods along with the proposed scheme to show a relative view of obtained results. The performance parameters considered in the table proved good agreement of the proposed PRNG algorithm from a highly efficient and security view.

CONCLUSION

A cascade fractal function can be designed by combining any two existing fractals. The paper analyzed the dynamical behavior of cascade-PLMS function by considering phoenix and lambda fractals. The benefit of combining two nonlinear functions is to have a more complex structure that is further utilized to propose a pseudo-random number generator. A linear function operation was applied to the cascade-PLMS, cascade-PLJS, and the number of iterations got as a result of obtaining a fixed point of the cascade-PLJS. It is of interest to generate a PRNG which is an integer and is convertible to the 8-bit binary sequence. By considering the arrangement of the column-wise bit of the data, eight simultaneous binary number sequences can be utilized in further application. Aiming at the security of the generated PRNG, a slight change in any system parameter leads to a completely new pseudo-random number sequence.

The proposed concept of a new cascade fractal function opens the door for the researchers to analyze the feasibility of the model using the other existing fractal functions. The choice of fractal surely affects the complexity outcome based on the corresponding function combination. Further, the obtained PRNG can be applied to the cryptographic application including creating watermarks, casinos, encoding digital contents, and many more. It’s also aiming to study how fast a bitstream can be generated so that it can be utilized in the hardware implementation.

Table 3 Performance comparison of the proposed PRNG method with the existing methods

Encryption Algorithm	Key Space	Entropy	NBCR	Correlation Coefficient
Proposed	2^{320}	7.9864	49.97	0.0016
Ref. (Zhao *et al.* 2019)	2^{70}	7.9896	49.74	-
Ref. (Barani *et al.* 2020)	2^{588}	7.9937	50.13	0.0003
Ref. (Ayubi *et al.* 2020)	2^{232}	-	-	0.0586
Ref. (Wang and Cheng 2019)	variable	7.9692	51.92	-
Ref. (Agarwal 2018)	2^{145}	-	-	0.0041

CONFLICTS OF INTEREST

The author declares that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Agarwal, S., 2018 Cryptographic key generation using burning ship fractal. In *Proceedings of the 2nd International Conference on Vision, Image and Signal Processing*, pp. 1–6.

Agarwal, S., 2020 A new composite fractal function and its application in image encryption. Journal of Imaging **6**: 70.

Alvarez, G. and S. Li, 2006 Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos **16**: 2129–2151.

Artuğer, F. and F. Özkaynak, 2020 A novel method for performance improvement of chaos-based substitution boxes. Symmetry **12**: 571.

Ayubi, P., S. Setayeshi, and A. M. Rahmani, 2020 Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. Journal of Information Security and Applications **52**: 102472.

Bai, S., L. Zhou, M. Yan, X. Ji, and X. Tao, 2020 Image cryptosystem for visually meaningful encryption based on fractal graph generating. IETE Technical Review pp. 1–12.

Barani, M. J., P. Ayubi, M. Y. Valandar, and B. Y. Irani, 2020 A new pseudo random number generator based on generalized newton complex map with dynamic key. Journal of Information Security and Applications **53**: 102509.

Bonilla, L. L., M. Alvaro, and M. Carretero, 2016 Chaos-based true random number generators. Journal of Mathematics in Industry **7**: 1–17.

Chen, G. and T. Ueta, 1999 Yet another chaotic attractor. International Journal of Bifurcation and chaos **9**: 1465–1466.

Çimen, M. E., Z. GARİP, Ö. F. Boyraz, I. Pehlivan, M. Z. YILDIZ, *et al.*, 2020 An interface design for calculation of fractal dimension. Chaos Theory and Applications **2**: 3–9.

Czyz, J., 1994 *Paradoxes of measures and dimensions originating in Felix Hausdorff's ideas*. World Scientific.

Devaney, R., 2018 *An introduction to chaotic dynamical systems*. CRC Press.

Devaney, R. L., J. A. Yorke, L. Keen, K. T. Alligood, M. F. Barnsley, *et al.*, 1989 *Chaos and Fractals: The Mathematics Behind the Computer Graphics: The Mathematics Behind the Computer Graphics*, volume 1. American Mathematical Soc.

Dey, N., A. S. Ashour, H. Kalia, R. Goswami, and H. Das, 2018 *Histopathological image analysis in medical decision making*. IGI Global.

Hamza, R., 2017 A novel pseudo random sequence generator for image-cryptographic applications. Journal of Information Security and Applications **35**: 119–127.

Hua, Z., F. Jin, B. Xu, and H. Huang, 2018 2d logistic-sine-coupling map for image encryption. Signal Processing **149**: 148–161.

Khelaifi, F. and H. He, 2020 Perceptual image hashing based on structural fractal features of image coding and ring partition. Multimedia Tools and Applications pp. 1–20.

Lynnyk, V., N. Sakamoto, and S. Čelikovskỳ, 2015 Pseudo random number generator based on the generalized lorenz chaotic system. IFAC-PapersOnLine **48**: 257–261.

Mandelbrot, B. B. and B. B. Mandelbrot, 1982 *The fractal geometry of nature*, volume 1. WH freeman New York.

Motỳl, I. and R. Jašek, 2011 Advanced user authentication process based on the principles of fractal geometry. In *Proceedings of the 11th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial Vision (ISCGAV'11)*, pp. 109–112.

Moysis, L., A. Tutueva, K. Christos, and D. Butusov, 2020a A chaos based pseudo-random bit generator using multiple digits comparison. Chaos Theory and Applications **2**: 58–68.

Moysis, L., A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, *et al.*, 2020b A two-parameter modified logistic map and its application to random bit generation. Symmetry **12**: 829.

Peitgen, H.-O., H. Jürgens, and D. Saupe, 2006 *Chaos and fractals: new frontiers of science*. Springer Science & Business Media.

Sahari, M. L. and I. Boukemara, 2018 A pseudo-random numbers generator based on a novel 3d chaotic map with an application to color image encryption. Nonlinear Dynamics **94**: 723–744.

Shannon, C. E., 1949 Communication theory of secrecy systems. The Bell system technical journal **28**: 656–715.

SI, W. S., 1998 Cryptography and network security: Principles and practice.

Wang, L. and H. Cheng, 2019 Pseudo-random number generator based on logistic chaotic system. Entropy **21**: 960.

Zhao, Y., C. Gao, J. Liu, and S. Dong, 2019 A self-perturbed pseudo-random sequence generator based on hyperchaos. Chaos, Solitons & Fractals: X **4**: 100023.

Zhou, Y., Z. Hua, C.-M. Pun, and C. P. Chen, 2014 Cascade chaotic system with applications. IEEE transactions on cybernetics **45**: 2001–2012.

How to cite this article: Agarwal, S. *Designing a Pseudo-Random Bit Generator Using Generalized Cascade Fractal Function*. Chaos Theory and Applications, 3(1), 11-19, 2021.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / **No.**1 / 2021 / **pp.**20-28
https://doi.org/10.51537/chaos.783548

FPGA-based Dual Core TRNG Design Using Ring and Runge-Kutta-Butcher based on Chaotic Oscillator

Murat Alcin [*,1], **Murat Tuna** [β,2], **Pakize Erdogmus** [γ,3] **and Ismail Koyuncu** [§,4]
[*]Department of Mechatronics Engineering, Faculty of Technology, Afyon Kocatepe University, Afyon, 03200, Turkey, [β]Department of Electrical, Technical Sciences Vocational School, Kırklareli University, Kırklareli, 39000, Turkey, [γ]Department of Computer Engineering, Faculty of Engineering, Düzce University, Düzce, 81620, Turkey, [§]Department of Electrical Electronics Engineering, Faculty of Technology, Afyon Kocatepe Uni., Afyon, 03200, Turkey.

ABSTRACT Despite the fact that chaotic systems do not have very complex circuit structures, interest in chaotic systems has increased considerably in recent years due to their interesting dynamic properties. Thanks to the noise-like properties of chaotic oscillators and the ability to mask information signals, great efforts have been made in recent years to develop chaos-based TRNG structures. In this study, a new chaos-based Dual Entropy Core (DEC) TRNG with high operating frequency and high bit generation rate was realized using 3D Pehlivan-Wei Chaotic Oscillator (PWCO) structure designed utilizing RK5-Butcher numerical algorithm on FPGA and ring oscillator structure. In the FPGA-based TRNG model of the system, 32-bit IQ-Math fixed-point number standard is used. The developed model is coded using VHDL. The designed TRNG unit was synthesized for Virtex-7 XC7VX485T-2FFG1761 chip produced by Xilinx. Then, the statistics of the parameters of FPGA chip resource usage and unit clock speed were examined. The data processing time of the TRNG unit was achieved by using the Xilinx ISE Design Tools 14.2 simulation program, with a high bit production rate of 437.043 Mbit/s. In addition, number sequences obtained from FPGA-based TRNG were subjected to the internationally valid statistical NIST 800-22 Test Suite and all the randomness tests of NIST 800-22 Test Suite were successful.

KEYWORDS
Chaotic systems
Ring oscillator
RK5-Butcher
Dual core TRNG
FPGA

INTRODUCTION

The term chaos is used to describe the dynamic behavior of simple dynamical systems, which appears to be complex and very different from what was predicted (Akgul *et al.* 2016b; Tuna and Fidan 2018). The behavior of these systems has a non-periodic property and can easily be confused with random behavior (Akkaya *et al.* 2018; Rivera-Blas *et al.* 2019). Chaotic systems are sensitive to initial conditions, complex and irregular in appearance, and occur in deterministic nonlinear time-dependent systems (Dursun and Kaşifoğlu 2018; Tuna *et al.* 2019a; Bonny and Elwakil 2018). Although chaotic systems do not have very complex circuit structures, since they have interesting dynamical properties, the interest in chaotic systems has been increased in recent years (Alçın *et al.* 2016; Koyuncu *et al.* 2019; Öztürk and Kiliç 2014). The basic structure to be used in chaos-based engineering applications is a chaos generator that produces the necessary chaotic signal (Adiyaman *et al.* 2020; Akgul *et al.* 2016a; Li *et al.* 2005). Thus, secure communication, cryptographic and random number generators, in which chaotic signals are used as entropy sources, have been proposed (Taskiran and Sedef 2020; Akgul *et al.* 2019; Benkouider *et al.* 2020; Bonny *et al.* 2019).

Ring oscillators are the oscillators consisting of an odd number of NOT gates connected cascade (Koyuncu *et al.* 2020). The output of each gate is connected to the input of the next gate, and the output of the last gate is connected to the input of the first gate. Ring oscillators generate a square

Manuscript received: 22 August 2020,
Revised: 25 December 2020,
Accepted: 27 January 2021.

[1] muratalcin@aku.edu.tr (**Corresponding Author**)
[2] murattuna@klu.edu.tr
[3] pakizeerdogmus@duzce.edu.tr
[4] ismailkoyuncu@aku.edu.tr

wave having a frequency depending on the delay of the ring (Koyuncu *et al.* 2020; Tuncer 2016). Therefore, the frequency of the obtained square wave varies according to the static and dynamic factors in the elements forming the ring. That is, the frequencies of the signals produced by two equally arranged oscillators will not be the same. This shows that ring oscillators can be used to generate random bits that differ in the frequencies of the signals they produce (Tuna *et al.* 2019b). Most of the integrated circuit (I.C.) applications and Field Programmable Gate Array (FPGA) based True Random Number Generators (TRNG) use the ring oscillator structures as the source of randomness (Kaya 2020; Buchovecka *et al.* 2017; Garipcan and Erdem 2019; Yoo *et al.* 2010; Avaroglu and Tuncer 2020; Bonny and Nasir 2019).

Systems that do not have autocorrelation at their output using hardware or software methods and produce numbers that are statistically independent from each other are called Random Number Generators (RNG) (Coskun *et al.* 2019; Gupta *et al.* 2019; Prakash *et al.* 2020). These generators are structures that can generate outputs at the level of randomness, where the next data cannot be predicted with the help of previous data. Because of these features, RNG is used in many different areas. TRNG is a device that produces a sequence of numbers such that they cannot be predicted. The random numbers produced by TRNG is a safe method since it is difficult to generate the same numbers. For this reason, considerable efforts are being made in the field of developing hardware-based random number generation structures with FPGA and general purpose microprocessors (Koyuncu and Özcerit 2017; Öztürk and Kılıç 2019). FPGA is a programmable integrated circuit (IC) whose internal structure can be changed any number of time with respect to desired function (Koyuncu and Özcerit 2017; Alcin 2020). So, FPGA is used for rapid prototype development. FPGA is commonly used nowadays because it presents great flexibility in the design stage, and it has parallel processing capability. The advantages of faster implementation and having higher density, make FPGAs possible to implement complex systems including numerical calculations. Programmable FPGA chips have an important potential to improve information security capacity in applications such as cryptology and secure communication, which require high performance and processing power, due to their high speed and capacity (Hagras and Saber 2020; Alcin *et al.* 2019; Koyuncu and Şeker 2019).

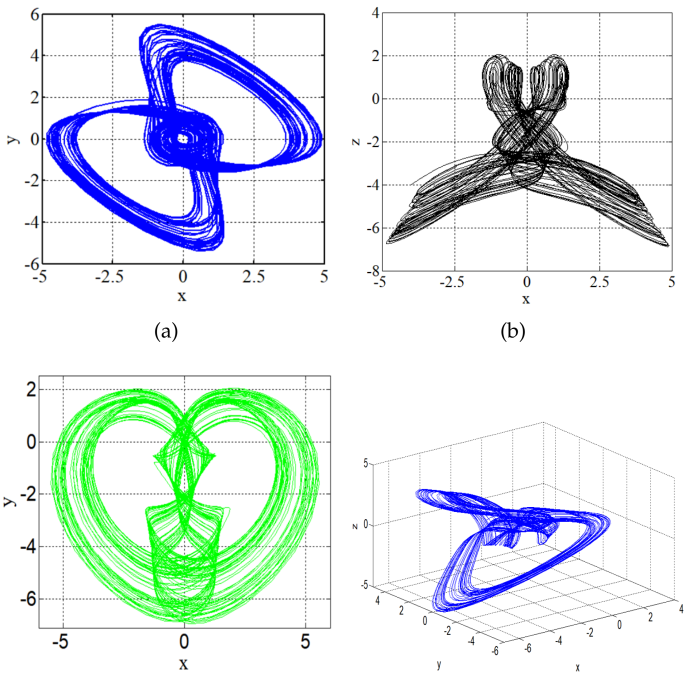
In the second part of the study, two and three dimensional phase portraits obtained from the modeling of the 3D PWCO system, one of the chaotic oscillators presented to the literature, using Runge-Kutta-Butcher algorithm (RK5-Butcher) are presented. In the third chapter, Dual Entropy Core (DEC) TRNG design using Ring and RK5-Butcher based PWCO on FPGA and the results obtained from the design are given. In the last part, the results obtained from the study are discussed.

THE 3D PWCO SYSTEM

Chaotic systems are expressed using differential equations. The differential equation for the continuous-time 3D PWCO system is given in Eq. (1) (Koyuncu *et al.* 2014).

$$\begin{aligned} \dot{x} &= y(1-z) \\ \dot{y} &= y(1+z) - \alpha x \\ \dot{z} &= \alpha - xy - y^2 \end{aligned} \tag{1}$$

Here α is the system parameter for PWCO. The change of this value greatly changes the dynamic behavior of the system. In this study, α has been set to 2.1 for the PWCO modeled using the RK5-Butcher algorithm. Initial conditions are needed for the system to work. In this study, the initial conditions for PWCO modeled by using the RK5-Butcher algorithm are taken as $x(0) = -3.9, y(0) = 0.90$, and $z(0) = -4.1$. Two-dimensional $x-y, x-z, y-z$ and three-dimensional $x-y-z$ phase portraits for the PWCO oscillator modeled using the RK5-Butcher algorithm are presented in Figure 1.



(a) (b)

(c) (d)

Figure 1 2D a) x-y, b) x-z, c) y-z and d) x-y-z phase portraits of RK5-Butcher based 3D PWCO

PWCO AND RING BASED DEC TRNG ON FPGA

In this section, the DEC TRNG design, which is implemented utilizing PWCO oscillator that created using Fifth Order Runge-Kutta Butcher Algorithm (RK5-B) numerical algorithm and Ring oscillator on FPGA, has been implemented. The discretized mathematical model of PWCO using the RK5-Butcher algorithm is given in Eq. 2. Here, the expansion of variables $\kappa_1 \ldots\ \kappa_6$, $\lambda_1 \ldots\ \lambda_1$ and $\xi_1 \ldots\ \xi_1$ is given in Eq. 3. Although the RK5-B has a similar structure with the RK4 (Fourth Order Runge-Kutta Algorithm) algorithm, this algorithm also produces more precise solutions than the RK4 and Euler algorithms since it has fifth and sixth order terms (Tlelo-Cuautle *et al.* 2015; Pano-Azucena *et al.* 2018; Sambas *et al.* 2020).

$$
\begin{aligned}
&x(k+1) = x(k) + \tfrac{1}{90}\Delta h\,[7\kappa_1(k) + 32\kappa_3(k) + 12\kappa_4(k) + 32\kappa_5(k) + 7\kappa_6(k)]\\
&y(k+1) = y(k) + \tfrac{1}{90}\Delta h\,[7\lambda_1(k) + 32\lambda_3(k) + 12\lambda_4(k) + 32\lambda_5(k) + 7\lambda_6(k)]\\
&z(k+1) = z(k) + \tfrac{1}{90}\Delta h\,[7\xi_1(k) + 32\xi_3(k) + 12\xi_4(k) + 32\xi_5(k) + 7\xi_6(k)]
\end{aligned}
\tag{2}
$$

$$
\begin{aligned}
&\kappa_1 = f(x(k), y(k), z(k))\\
&\lambda_1 = g(x(k), y(k), z(k))\\
&\xi_1 = \delta(x(k), y(k), z(k))\\
&\kappa_2 = f(x(k) + \tfrac{1}{4}\Delta h\kappa_1, y(k) + \tfrac{1}{4}\Delta h\lambda_1, z(k) + \tfrac{1}{4}\Delta h\xi_1)\\
&\lambda_2 = g(x(k) + \tfrac{1}{4}\Delta h\kappa_1, y(k) + \tfrac{1}{4}\Delta h\lambda_1, z(k) + \tfrac{1}{4}\Delta h\xi_1)\\
&\xi_2 = \delta(x(k) + \tfrac{1}{4}\Delta h\kappa_1, y(k) + \tfrac{1}{4}\Delta h\lambda_1, z(k) + \tfrac{1}{4}\Delta h\xi_1)\\
&\kappa_3 = f(x(k) + \tfrac{1}{8}(\Delta h(\kappa_1 + \kappa_{2)}, y(k) + \tfrac{1}{8}(\Delta h(\lambda_1 + \lambda_{2)}, z(k) + \tfrac{1}{8}(\Delta h(\xi_1 + \xi_{2)})\\
&\lambda_3 = g(x(k) + \tfrac{1}{8}(\Delta h(\kappa_1 + \kappa_{2)}, y(k) + \tfrac{1}{8}(\Delta h(\lambda_1 + \lambda_{2)}, z(k) + \tfrac{1}{8}(\Delta h(\xi_1 + \xi_{2)})\\
&\xi_3 = \delta(x(k) + \tfrac{1}{8}(\Delta h(\kappa_1 + \kappa_{2)}, y(k) + \tfrac{1}{8}(\Delta h(\lambda_1 + \lambda_{2)}, z(k) + \tfrac{1}{8}(\Delta h(\xi_1 + \xi_{2)})\\
&\kappa_4 = f(x(k) - \tfrac{1}{2}\Delta h\kappa_2 + \Delta h\kappa_3, y(k) - \tfrac{1}{2}\Delta h\lambda_2 + \Delta h\lambda_3, z(k) - \tfrac{1}{2}\Delta h\xi_2 + \Delta h\xi_3)\\
&\lambda_4 = g(x(k) - \tfrac{1}{2}\Delta h\kappa_2 + \Delta h\kappa_3, y(k) - \tfrac{1}{2}\Delta h\lambda_2 + \Delta h\lambda_3, z(k) - \tfrac{1}{2}\Delta h\xi_2 + \Delta h\xi_3)\\
&\xi_4 = \delta(x(k) - \tfrac{1}{2}\Delta h\kappa_2 + \Delta h\kappa_3, y(k) - \tfrac{1}{2}\Delta h\lambda_2 + \Delta h\lambda_3, z(k) - \tfrac{1}{2}\Delta h\xi_2 + \Delta h\xi_3)\\
&\kappa_5 = f(x(k) + \tfrac{3}{16}\Delta h\kappa_1 + \tfrac{9}{16}\Delta h\kappa_4, y(k) + \tfrac{3}{16}\Delta h\lambda_1 + \tfrac{9}{16}\Delta h\lambda_4, z(k) + \tfrac{3}{16}\Delta h\xi_1 + \tfrac{9}{16}\Delta h\xi_4)\\
&\lambda_5 = g(x(k) + \tfrac{3}{16}\Delta h\kappa_1 + \tfrac{9}{16}\Delta h\kappa_4, y(k) + \tfrac{3}{16}\Delta h\lambda_1 + \tfrac{9}{16}\Delta h\lambda_4, z(k) + \tfrac{3}{16}\Delta h\xi_1 + \tfrac{9}{16}\Delta h\xi_4)\\
&\xi_5 = \delta(x(k) + \tfrac{3}{16}\Delta h\kappa_1 + \tfrac{9}{16}\Delta h\kappa_4, y(k) + \tfrac{3}{16}\Delta h\lambda_1 + \tfrac{9}{16}\Delta h\lambda_4, z(k) + \tfrac{3}{16}\Delta h\xi_1 + \tfrac{9}{16}\Delta h\xi_4)\\
&\kappa 6 = f(x(k) - \tfrac{3}{7}\Delta h\kappa_1 + \tfrac{2}{7}\Delta h\kappa_2 + \tfrac{12}{7}\Delta h\kappa_3 - \tfrac{12}{7}\Delta h\kappa_4 + \tfrac{8}{7}\Delta h\kappa_5, y(k) + -\tfrac{3}{7}\Delta h\lambda_1 + \tfrac{2}{7}\Delta h\lambda_2 +\\
&\tfrac{12}{7}\Delta h\lambda_3 - \tfrac{12}{7}\Delta h\lambda_4 + \tfrac{8}{7}\Delta h\lambda_5, z(k) - \tfrac{3}{7}\Delta h\xi_1 + \tfrac{2}{7}\Delta h\xi_2 + \tfrac{12}{7}\Delta h\xi_3 - \tfrac{12}{7}\Delta h\xi_4 + \tfrac{8}{7}\Delta h\xi_5)\\
&\lambda 6 = g(x(k) - \tfrac{3}{7}\Delta h\kappa_1 + \tfrac{2}{7}\Delta h\kappa_2 + \tfrac{12}{7}\Delta h\kappa_3 - \tfrac{12}{7}\Delta h\kappa_4 + \tfrac{8}{7}\Delta h\kappa_5, y(k) + -\tfrac{3}{7}\Delta h\lambda_1 + \tfrac{2}{7}\Delta h\lambda_2 +\\
&\tfrac{12}{7}\Delta h\lambda_3 - \tfrac{12}{7}\Delta h\lambda_4 + \tfrac{8}{7}\Delta h\lambda_5, z(k) - \tfrac{3}{7}\Delta h\xi_1 + \tfrac{2}{7}\Delta h\xi_2 + \tfrac{12}{7}\Delta h\xi_3 - \tfrac{12}{7}\Delta h\xi_4 + \tfrac{8}{7}\Delta h\xi_5)\\
&\xi 6 = \delta(x(k) - \tfrac{3}{7}\Delta h\kappa_1 + \tfrac{2}{7}\Delta h\kappa_2 + \tfrac{12}{7}\Delta h\kappa_3 - \tfrac{12}{7}\Delta h\kappa_4 + \tfrac{8}{7}\Delta h\kappa_5, y(k) + -\tfrac{3}{7}\Delta h\lambda_1 + \tfrac{2}{7}\Delta h\lambda_2 +\\
&\tfrac{12}{7}\Delta h\lambda_3 - \tfrac{12}{7}\Delta h\lambda_4 + \tfrac{8}{7}\Delta h\lambda_5, z(k) - \tfrac{3}{7}\Delta h\xi_1 + \tfrac{2}{7}\Delta h\xi_2 + \tfrac{12}{7}\Delta h\xi_3 - \tfrac{12}{7}\Delta h\xi_4 + \tfrac{8}{7}\Delta h\xi_5)
\end{aligned}
\tag{3}
$$

The top level block diagram of the designed structure is given in Figure 2. Random number sequences with high throughput and high operating frequency obtained from the proposed structure; they can be used in cryptography and secure communication areas that require fast, secure and intensive processing. The designed chaotic DEC TRNG unit was synthesized for the Virtex-7 VC707 chip produced by Xilinx, and the statistics of the parameters of FPGA chip resource usage and the clock speeds of the units were analyzed. The data processing time of TRNG units was obtained using Xilinx ISE Design Tools 14.2 simulation program.

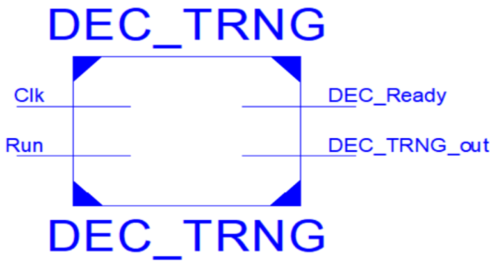


Figure 2 The top-level block diagram of the FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO.

Figure 3 shows the block diagram of the proposed FPGA-based DEC TRNG unit. RK5-Butcher-based TRNG unit designed on FPGA consists of 5 parts: $x3mux$, $PWKS_RK5$ oscillator, Quantization unit, Ring oscillator and Art unit. In the design, the $x3mux$ unit is basically a multiplexer (MUX) structure developed for the control of the start signals required by the $PWKS_RK5$ unit, which has 3 dependent variables.

Quantization process was realized by taking the last 23 bits of the fractional part of each 32-bit number in the fixed point number standard produced by the fixed point number based chaotic oscillator unit. The RN signals obtained from the output of this unit are the signals that carry random numbers. The sh signal indicates that random signals are received from the unit output. These two signals are transmitted to the ART unit. Post processing is applied for the signals obtained here.

In the presented study, XOR process was applied as the post process and the results obtained were sent to the output of the system. The random numbers produced by the ring oscillator and the random numbers produced by the RK5-Butcher algorithm based PWCO-based TRNG unit are subjected to XOR processing in the $ART - PROCESSING$ unit.

In TRNG structures subjected to XOR process presented in the literature, as a result of the XOR process, the bit production rate is reduced by half. However, unlike the studies presented in the literature, in the XOR process presented in this study, since random numbers are generated from two different sources and subjected to the XOR process, there is no decrease in the bit production rate in the high speed DEC TRNG using Ring and RK5-Butcher algorithm based 3D PWCO on FPGA design.

In Fig. 4, the third level block diagram of high speed DEC TRNG using Ring and RK5-Butcher based on PWCO on FPGA is presented.

Here, the structure of the $PWKS_RK5$ unit is given in more detail. The $PWKS_RK5$ oscillator generates the chaotic signals that TRNG needs and transfers these values to 32-bit x_out, y_out and z_out signals. When the chaotic oscillator produces an output, the 1-bit RNG_Ready signal becomes "1" and sends the values produced by the 3D PWCO to the Quantization unit. All units used in these designs such as multiplier, adder, and subtractor were created using the IP Core generator developed with Xilinx ISE Design Tools.

FPGA-based DEC TRNG Design using Ring and RK5-Butcher based on PWCO unit is synthesized and tested for Xilinx Virtex-7 XC7VX485T-2FFG1761 FPGA chip. Figure 5. presents the test bench results for the FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit, whose code was written in VHDL.

FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit has been synthesized and then after the Place-Route processes, XC7VX330T-2-FFG-1157 FPGA chip statistics have been obtained. As can be observed from the chip statistics in the Table 1, the maximum clock frequency of the FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit reaches 437.043 MHz.

As can be observed from the literature, it is necessary to examine and to test the randomness and statistical properties of the random numbers produced by random number generators (Rezk *et al.* 2019; Murillo-Escobar *et al.* 2017). For this purpose, various statistical tests developed in the literature are used. At this stage, the new chaotic DEC TRNG developed on FPGA has been subjected to the NIST 800-22 statistical tests in order to be used safely in cryptographic applications (Etem and Kaya 2020). This test itself consists of 16 separate subtests. In order for the tested bit stream to be accepted as successful, it must pass all tests successfully. The orders in which the 16 tests in the NIST 800-22 test are run is completely optional. However, the Frequency Test is recommended to be applied first as it gives basic clues about the existence of nonrandom regions in a sequence. If this test fails, it is likely that other tests will also fail. The most complex test in terms of time criteria is the Linear Complexity test.

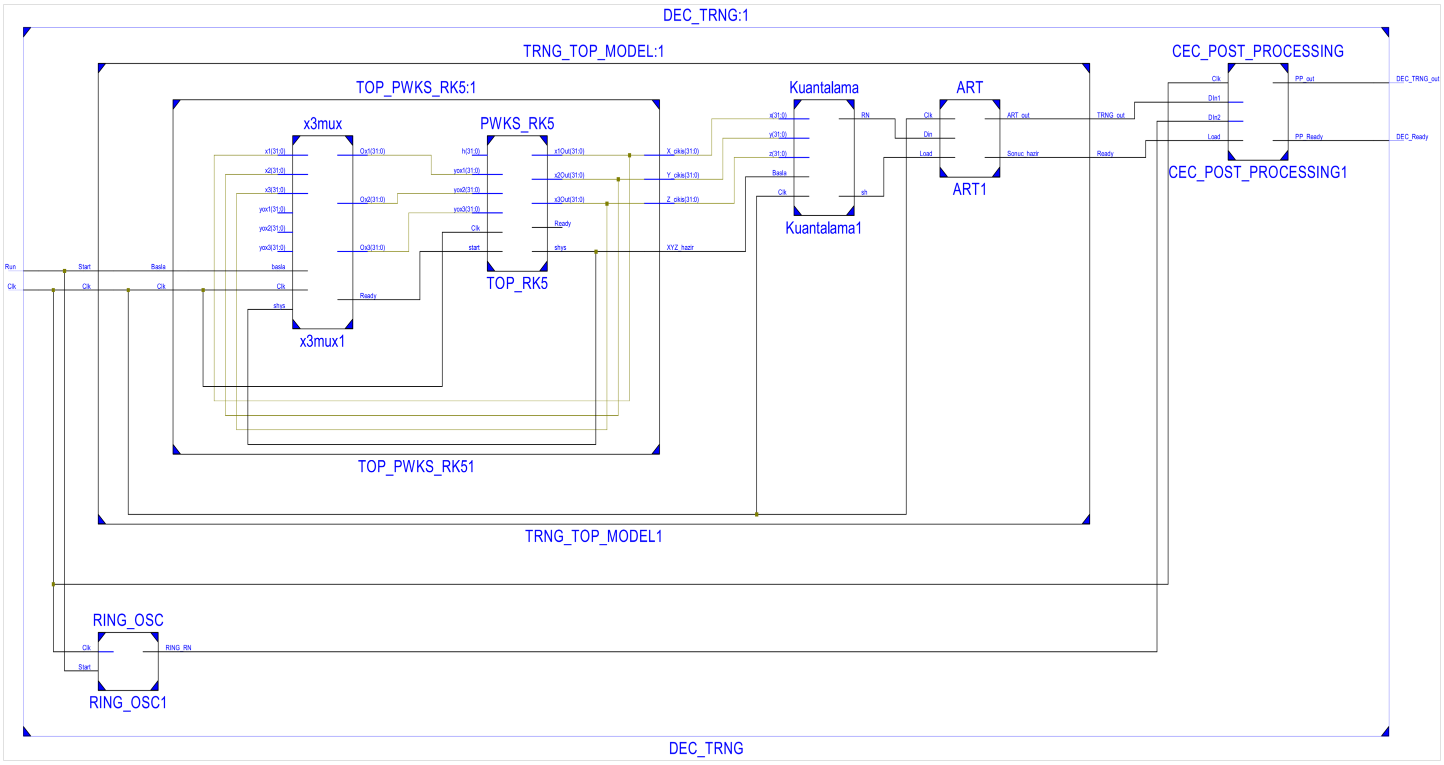


Figure 3 The second level block diagram of the FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO.

Table 1 The area utilization report of FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit on Virtex-7.

Utilization for 7VX485TFFG1761-2 Device	Used	Available	Utilization %
Number of Slice Registers	85.763	607.200	14
Number of Slice LUTs	85.294	303.600	28
Number of fully used LUT-Flip Flop Pairs	69.011	102.046	67
Number of Inputs/Outputs	4	700	1
Number of BUFG/BUFGCTRLs	1	32	3
Latency (ns)	702	-	-
Min. clock period (ns)	2.288	-	-

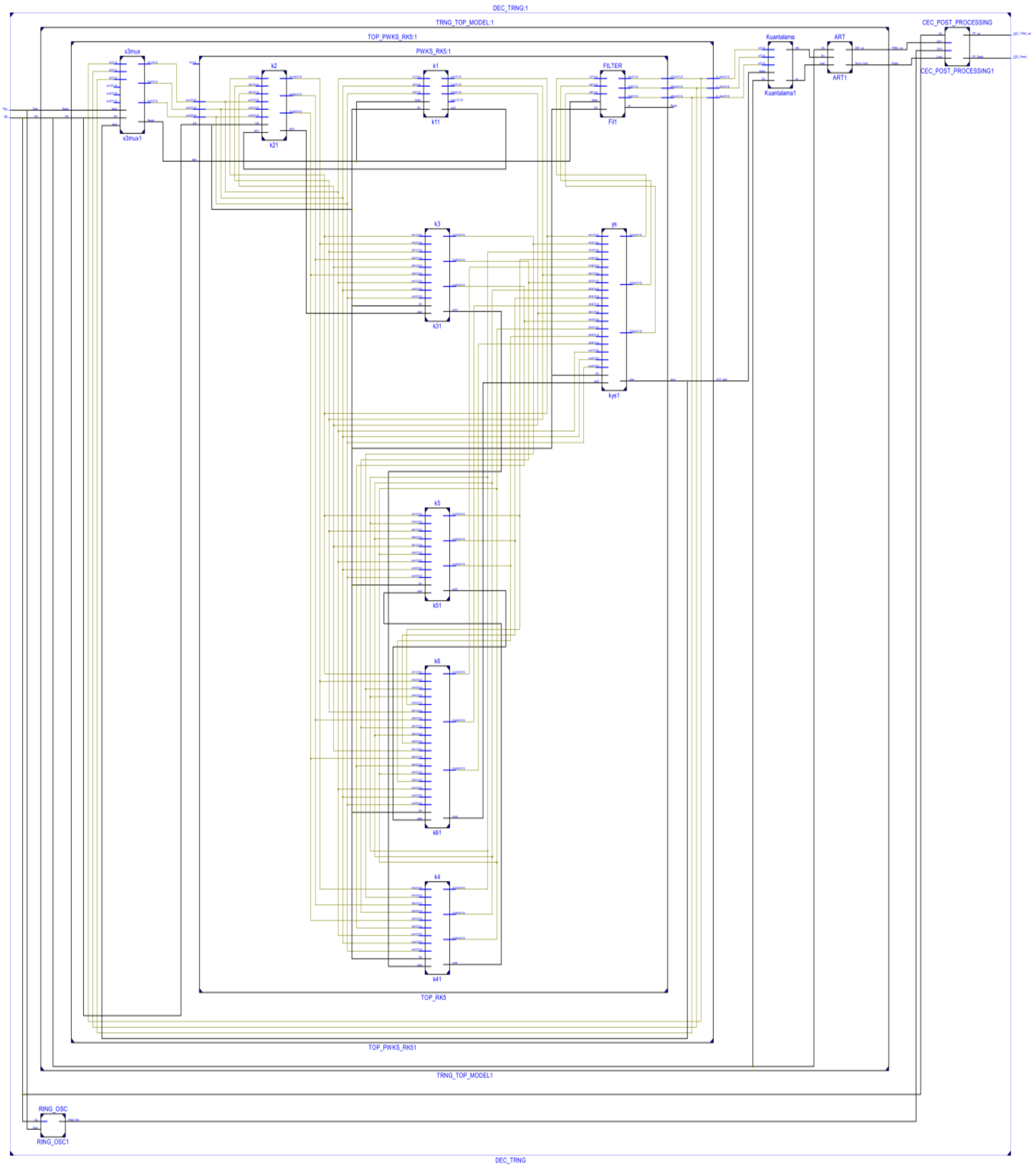


Figure 4 The third level block diagram of FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO.

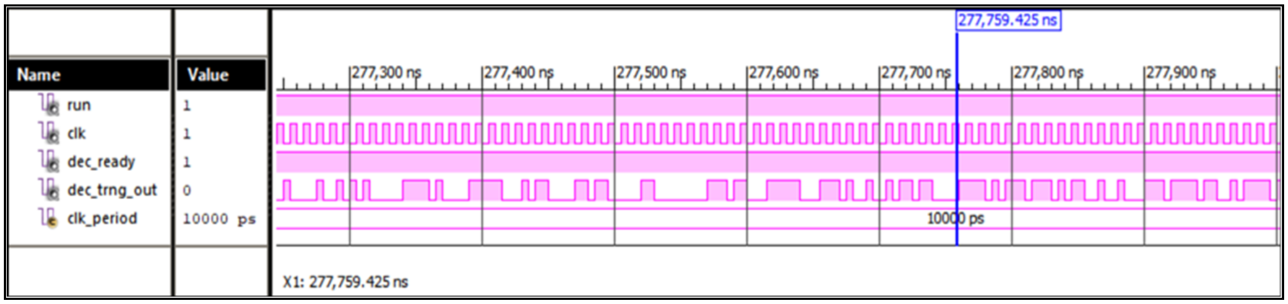


Figure 5 The operation timing diagram of FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit obtained from Xilinx ISE Simulator.

Table 2 TThe NIST test results of FPGA-based DEC TRNG design using Ring and RK5-Butcher based on PWCO unit.

NIST 800-22 Statistical Tests	P-value	Result
Frequency Test	0.80568	Successful
Block Frequency Test	0.33645	Successful
Runs Test	0.75218	Successful
Longest Runs of One's Test	0.834183	Successful
Binary Matrix Rank Test	0.73924	Successful
Discrete Fourier Transform (FFT) Test	0.48553	Successful
Non-Overlapping Template Matching Test	0.47564	Successful
Overlapping Template Matching Test	0.26366	Successful
Maurer's "Universal Statistical" Test	0.67244	Successful
Linear Complexity Test	0.21416	Successful
Serial Test 1	0.33020	Successful
Serial Test 2	0.68817	Successful
Approximate Entropy Test	0.40933	Successful
Cumulative Sums (Forward) Test	0.87979	Successful
Random Excursions Test (for x=-3)	0.33195	Successful
Random Excursions Variant Test (for x= 3)	0.28495	Successful

1 million bits of data were collected and saved in a file for the system designed for testing. Then the bit file was subjected to 16 tests in the NIST Test Suite and all the sequences obtained were successful in all the randomness tests. In this test, some parameters of the random bit stream to be tested can be determined externally. P-value, which is one of the most important parameters in these tests, is accepted as a measure of the randomness of the random sequences subjected to the test. If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random. A significance level (α) can be chosen for the tests. Typically, the, α is chosen in the range $[0.001, 0.01]$. For this study, α parameter has been choosen as 0.01. As can be seen from the test results in Table 2, since the P-value $\geq$ 0.01, the obtained sequences are accepted randomly.

CONCLUSION

This paper presents a novel FPGA based Dual Core TRNG unit implemented in discrete time. In this direction, in the first stage, 3D PWCO has been modeled with RK5-Butcher numerical method and chaos analyses were performed by examining the dynamic behavior of the systems. Then, the PWCO was modeled on FPGA using the hardware description language as VHDL in accordance with the 32 bit IQ-Math fixed point number standard. RK5-Butcher numerical method was used in the modeling phase. The ring oscillator and PWCO designs were harvested in the post processing unit and the proposed TRNG design was implemented on FPGA. The proposed TRNG is capable of producing a high throughput of 437.043 Mbit/s after post-processing. Apart from the studies presented in the literature, post- processing has been performed without the decrease in the bit production rate. In the last part, number streams acquired from the presented TRNG unit have been applied to NIST 800-22 Test Suite. The test results have shown that the proposed TRNG unit can be used in the cryptographic systems. In addition, when this study is compared with other studies and methods presented in the literature, it offers very successful results in terms of both operating frequency and throughput.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Adiyaman, Y., S. EMİROGLU, M. K. UÇAR, and M. YILDIZ, 2020 Dynamical analysis, electronic circuit design and control application of a different chaotic system. Chaos Theory and Applications **2**: 10–16.

Akgul, A., C. ARSLAN, and B. ARICIOĞLU, 2019 Design of an interface for random number generators based on integer and fractional order chaotic systems. Chaos Theory and Applications **1**: 1–18.

Akgul, A., H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbullu, 2016a Chaos-based engineering applications with a 3d chaotic system without equilibrium points. Nonlinear dynamics **84**: 481–495.

Akgul, A., S. Hussain, and I. Pehlivan, 2016b A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications. Optik **127**: 7062–7071.

Akkaya, S., İ. Pehlivan, A. Akgül, and M. Varan, 2018 Yeni bir kaos tabanlı rasgele sayı üreteci kullanan banka şifrematik cihazı tasarımı ve uygulaması. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi **33**: 1171–1182.

Alcin, M., 2020 The runge kutta-4 based 4d hyperchaotic system design for secure communication applications. Chaos Theory and Applications **2**: 23–30.

Alcin, M., I. Koyuncu, M. Tuna, M. Varan, and I. Pehlivan, 2019 A novel high speed artificial neural network–based chaotic true random number generator on field programmable gate array. International Journal of Circuit Theory and Applications **47**: 365–378.

Alçın, M., İ. Pehlivan, and İ. Koyuncu, 2016 Hardware design and implementation of a novel ann-based chaotic generator in fpga. Optik **127**: 5500–5505.

Avaroglu, E. and T. Tuncer, 2020 A novel s-box-based post-processing method for true random number generation. Turkish Journal of Electrical Engineering & Computer Sciences **28**: 288–301.

Benkouider, K., T. Bouden, and M. E. Yalcin, 2020 A snail-shaped chaotic system with large bandwidth: dynamical analysis, synchronization and secure communication scheme. SN Applied Sciences **2**: 1–15.

Bonny, T., R. Al Debsi, S. Majzoub, and A. S. Elwakil, 2019 Hardware optimized fpga implementations of high-speed true random bit generators based on switching-type chaotic oscillators. Circuits, Systems, and Signal Processing **38**: 1342–1359.

Bonny, T. and A. S. Elwakil, 2018 Fpga realizations of high-speed switching-type chaotic oscillators using compact vhdl codes. Nonlinear Dynamics **93**: 819–833.

Bonny, T. and Q. Nasir, 2019 Clock glitch fault injection attack on an fpga-based non-autonomous chaotic oscillator. Nonlinear Dynamics **96**: 2087–2101.

Buchovecka, S., R. Lórencz, F. Kodỳtek, and J. Buček, 2017 True random number generator based on ring oscillator puf circuit. Microprocessors and Microsystems **53**: 33–41.

Coskun, S., I. Pehlivan, A. AKGÜL, and B. GÜREVİN, 2019 A new computer-controlled platform for adc-based true random number generator and its applications. Turkish Journal of Electrical Engineering & Computer Sciences **27**: 847–860.

Dursun, M. and E. Kaşifoğlu, 2018 Design and implementation of the fpga-based chaotic van der pol oscillator. International Advanced Researches and Engineering Journal **2**: 309–314.

Etem, T. and T. Kaya, 2020 A novel true random bit generator design for image encryption. Physica A: Statistical

Mechanics and its Applications **540**: 122750.

Garipcan, A. M. and E. Erdem, 2019 Implementation and performance analysis of true random number generator on fpga environment by using non-periodic chaotic signals obtained from chaotic maps. Arabian Journal for Science and Engineering **44**: 9427–9441.

Gupta, R., A. Pandey, and R. K. Baghel, 2019 Fpga implementation of chaos-based high-speed true random number generator. International Journal of Numerical Modelling: Electronic Networks, Devices and Fields **32**: e2604.

Hagras, E. A. and M. Saber, 2020 Low power and high-speed fpga implementation for 4d memristor chaotic system for image encryption. Multimedia Tools and Applications **79**: 23203–23222.

Kaya, T., 2020 A true random number generator based on a chua and ro-puf: design, implementation and statistical analysis. Analog Integrated Circuits and Signal Processing **102**: 415–426.

Koyuncu, İ., M. Alçin, M. Tuna, İ. Pehlivan, M. Varan, *et al.*, 2019 Real-time high-speed 5-d hyperchaotic lorenz system on fpga. International Journal of Computer Applications in Technology **61**: 152–165.

Koyuncu, I. and A. T. Özcerit, 2017 The design and realization of a new high speed fpga-based chaotic true random number generator. Computers & Electrical Engineering **58**: 203–214.

Koyuncu, I., A. T. Ozcerit, and I. Pehlivan, 2014 Implementation of fpga-based real time novel chaotic oscillator. Nonlinear Dynamics **77**: 49–59.

Koyuncu, İ. and H. İ. Şeker, 2019 Implementation of dormand-prince based chaotic oscillator designs in different iq-math number standards on fpga. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi **23**: 859–868.

Koyuncu, I., M. Tuna, I. Pehlivan, C. B. Fidan, and M. Alçın, 2020 Design, fpga implementation and statistical analysis of chaos-ring based dual entropy core true random number generator. Analog Integrated Circuits and Signal Processing **102**: 445–456.

Li, S., G. Chen, and X. Mou, 2005 On the dynamical degradation of digital piecewise linear chaotic maps. International journal of Bifurcation and Chaos **15**: 3119–3151.

Murillo-Escobar, M., C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, 2017 A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dynamics **87**: 407–425.

Öztürk, İ. and R. Kiliç, 2014 Cycle lengths and correlation properties of finite precision chaotic maps. International Journal of Bifurcation and Chaos **24**: 1450107.

Öztürk, I. and R. Kılıç, 2019 Higher dimensional baker map and its digital implementation with lsb-extension method. IEEE Transactions on Circuits and Systems I: Regular Papers **66**: 4780–4792.

Pano-Azucena, A., E. Tlelo-Cuautle, G. Rodriguez-Gomez, and L. De la Fraga, 2018 Fpga-based implementation of chaotic oscillators by applying the numerical method based on trigonometric polynomials. AIP Advances **8**: 075217.

Prakash, P., K. Rajagopal, I. Koyuncu, J. P. Singh, M. Alcin, *et al.*, 2020 A novel simple 4-d hyperchaotic system with a saddle-point index-2 equilibrium point and multistability: Design and fpga-based applications. Circuits, Systems, and Signal Processing pp. 1–22.

Rezk, A. A., A. H. Madian, A. G. Radwan, and A. M. Soliman, 2019 Reconfigurable chaotic pseudo random number generator based on fpga. AEU-international Journal of Electronics and Communications **98**: 174–180.

Rivera-Blas, R., S. A. Rodríguez Paredes, L. A. Flores-Herrera, and I. Adrián Romero, 2019 Design and implementation of a microcontroller based active controller for the synchronization of the petrzela chaotic system. Computation **7**: 40.

Sambas, A., S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. Abd El-Latif, *et al.*, 2020 A 3-d multi-stable system with a peanut-shaped equilibrium curve: Circuit design, fpga realization, and an application to image encryption. IEEE Access **8**: 137116–137132.

Taskiran, Z. and H. Sedef, 2020 Realization of memristor-based chaotic rossler circuit. J. Fac. Eng. Archit. Gazi Univ. **35**: 765–774.

Tlelo-Cuautle, E., J. Rangel-Magdaleno, A. Pano-Azucena, P. Obeso-Rodelo, and J. C. Nuñez-Perez, 2015 Fpga realization of multi-scroll chaotic oscillators. Communications in Nonlinear Science and Numerical Simulation **27**: 66–80.

Tuna, M., M. Alçın, İ. Koyuncu, C. B. Fidan, and İ. Pehlivan, 2019a High speed fpga-based chaotic oscillator design. Microprocessors and Microsystems **66**: 72–80.

Tuna, M. and C. Fidan, 2018 A study on the importance of chaotic oscillators based on fpga for true random number generating (trng) and chaotic systems .

Tuna, M., A. Karthikeyan, K. Rajagopal, M. Alcin, and İ. Koyuncu, 2019b Hyperjerk multiscroll oscillators with megastability: analysis, fpga implementation and a novel ann-ring-based true random number generator. AEU-International Journal of Electronics and Communications **112**: 152941.

Tuncer, T., 2016 The implementation of chaos-based puf designs in field programmable gate array. Nonlinear dynamics **86**: 975–986.

Yoo, S.-K., D. Karakoyunlu, B. Birand, and B. Sunar, 2010 Improving the robustness of ring oscillator trngs. ACM Transactions on Reconfigurable Technology and Systems (TRETS) **3**: 1–30.

How to cite this article: Alcin, M., Tuna, M., Erdogmus, P. and Koyuncu, I. FPGA-based Dual Core TRNG Design Using Ring and Runge-Kutta-Butcher based on Chaotic Oscillator. Chaos Theory and Applications, 3(1), 20-28, 2021.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / No.1 / 2021 / pp.29-33
https://doi.org/10.51537/chaos.850012

Chaos synchronization in chaotic current modulated VCSELs by bidirectional coupling

Nasr Saeed [*,1], **Alex Stephane Kemnang Tsafack** [β,2], **Hubert Malwe Boudoue** [γ,3] **and Sifeu Takougang Kingni** [§,4]
[*] Department of Physics, College of Education, Nyala University, P.O. Box: 155, Nyala, Sudan, [β] Research unit of Condensed matter of electronics and signal processing, Department of Physics, Faculty of Sciences, University of Dschang, P.O. Box 67, Dschang, Cameroon, [γ] Department of Physics, Faculty of Science, University of Maroua, P.O. Box 814 Maroua, Cameroon, [§] Department of Mechanical, Petroleum and Gas Engineering, Faculty of Mines and Petroleum Industries, University of Maroua, P.O. Box 46, Maroua, Cameroon.

ABSTRACT This paper reports on the synchronization proprieties in bidirectional coupled current modulated vertical cavity surface-emitting lasers (CMVCSELs) based on the combined model of Danckaert et al.. Regular pulse packages and chaotic behaviors are found in CMVCSEL during the numerical results. The suitable coupling strength leading to high quality of synchronization is determined by numerical analysis. The consequence of the parameter mismatch and the duration of the synchronization process are also highlighted.

KEYWORDS
VCSEL
Modulation current
Bidirectional coupling
Synchronization

INTRODUCTION

Many researchers have proved that in certain conditions, current modulated vertical cavity surface-emitting lasers (VCSELs) are able to exhibit not only periodic and chaotic behaviors (Masoller *et al.* 2007; Valle *et al.* 2007; Mbé *et al.* 2010; Kingni *et al.* 2012). but also pulse packages (Mbé *et al.* 2010; Kingni *et al.* 2012; Tabaka *et al.* 2006). The compact light sources of chaotic VCSELs are desirable and can be used in chaos-based secure communications (Colet and Roy 1994). The fact of hiding a message carrying information in a noise and exploiting the synchronization of the both (receiver with the output) to recover the information signal constituting the idea of chaotic secure communications. Work on chaos synchronization has been demonstrated in several lasers, notably Nd: YAG (Roy and Thornburg Jr 1994), CO2 (Sugawara *et al.* 1994), fiber laser (Vanwiggeren and Roy 1998) and semiconductor edge-emitting lasers (Goedgebuer *et al.* 1998; Bindu and Nandakumaran 2000; Kouomou and Woafo 2003; Argyris *et al.* 2005; Kingni *et al.* 2020).

By contrast, it should be noted that studies remain scarce concerning VCSELs coupled with the synchronization of chaos (Takougang Kingni *et al.* 2012; Li *et al.* 2007; Sciamanna *et al.* 2007; Zhong *et al.* 2008; Xie *et al.* 2016; Wang *et al.* 2020; Roy *et al.* 2019). Many researches on the synchronization of chaos in coupled VCSELs found in the literature have been done using a complex mathematical model of VCSELs, mostly the Spin-Flip Model (SFM) (Li *et al.* 2007; Sciamanna *et al.* 2007; Zhong *et al.* 2008). According to the knowledge of the authors, the synchronization of chaos in coupled CMVCSELs based on the combined model of Danckaert et al. is scare (Takougang Kingni *et al.* 2012). In (Takougang Kingni *et al.* 2012), synchronization properties and communications of unidirectional coupled VCSELs based on the combined model of Danckaert et al. (Danckaert *et al.* 2002) and driven by chaotic oscillators with wide spectral frequency bandwidth has been studied numerically. The results showed that best quality synchronization was achieved and message transmission by using the chaos shift keying technique has been demonstrated.

The purpose of this article is to analyze the chaos synchronization in bidirectional coupled CMVCSELs described by the combined model of Danckaert et al. (Danckaert *et al.* 2002). The bidirectional coupling is used to achieve synchro-

Manuscript received: 30 December 2020,
Revised: 26 February 2021,
Accepted: 21 March 2021.

[1] nasrsaeed19@yahoo.com
[2] alexstephanekemnang@gmail.com (**Corresponding Author**)
[3] malwehubert@yahoo.fr
[4] stkingni@gmail.com

nization between chaotic coupled CMVCSELs due to the fact that it leads to high quality of synchronization and it is robust to the parameter mismatch. The paper is subdivided in three sections. Section 2 discusses the examination of chaos synchronization in two CMVCSELs by bidirectional coupling. Conclusion is given in section 3.

CHAOS SYNCHRONIZATION OF BIDIRECTIONAL COUPLED CMVCSELS

The system of two bidirectional coupled CMVCSELs based on the combined model of Danckaert et al. (Danckaert *et al.* 2002) is described by the following equations:

$$\frac{dP_{x,j}}{dt} = \left(\eta_j - \varepsilon_{xx}P_{x,j} - \varepsilon_{xy}P_{y,j}\right)P_{x,j} + \frac{R_{sp}}{2} \tag{1a}$$

$$\begin{aligned} \frac{dP_{y,j}}{dt} &= \left\{\eta_j + G\left[j\left(t\right)\right] - \varepsilon_{yy}P_{y,j} - \varepsilon_{yx}P_{x,j}\right\}P_{y,j} \\ &+ \frac{R_{sp}}{2} + k\left(P_{y,i\neq j} - P_{y,j}\right)\, H\left(t - T_0\right), \end{aligned} \tag{1b}$$

$$\begin{aligned} \frac{d\eta_j}{dt} &= \rho^{-1}\left[gj\left(t\right) - 1 - P_{x,j} - P_{y,j}\right] - \eta_j \\ &- \left(\eta_j - \varepsilon_{xx}P_{x,j} - \varepsilon_{xy}P_{y,j}\right)P_{x,j} \\ &- \left(\eta_j - \varepsilon_{yy}P_{y,j} - \varepsilon_{yx}P_{x,j}\right)P_{y,j} \end{aligned} \tag{1c}$$

where t, P_x, P_y and η are the time, the photon density in x and y polarization modes (PMs) and the carrier density, respectively. The parameters $\varepsilon_{xx} = 4$ and $\varepsilon_{yy} = 4$ are the self-gain saturation coefficients while the parameters $\varepsilon_{xyx} = 8$ and $\varepsilon_{yx} = 8$ are the cross-gain saturation coefficients. The parameter $R_{sp} = 0.001$ is the mean of the spontaneous emission above threshold and the parameter $\rho = 0.001$ is the ratio of photon lifetime $\tau_p = 1\,ps$ to carrier lifetime $\tau_c = 1\,ns$. The modulation current is $j(t) = j_{dc} + j_m \sin(2\pi f_m \tau_c t)$, j_{dc} is the dc bias current,j_m is the modulation amplitude and f_m is the modulation frequency. The parameter $G\left[j(t)\right] = g\left[1 - j\left(t\right)/j_{sw}\right]$ is the relative gain difference between the two modes, the parameter $j_{sw} = 0.15$ is the switching current and the parameter $g = 10$ is a positive coefficient. The index i and j represent the VCSEL number (i, $j \in \{1, 2\}$). The parameter K is the coupling strength; the parameter T_0 is the onset of synchronization time process and the the Heaviside function $H\left(t - T_0\right)$ is defined as:

$$H\left(t - T_0\right) = \left\{ \begin{array}{ll} 0 & for\, t \prec\ T_0 \\ 1 & for\ t\ \geq T_0 \end{array} \right. . \tag{2}$$

The uncoupled CMVCSEL can exhibit regular pulse packages and chaotic attractors as shown in Fig. 1.

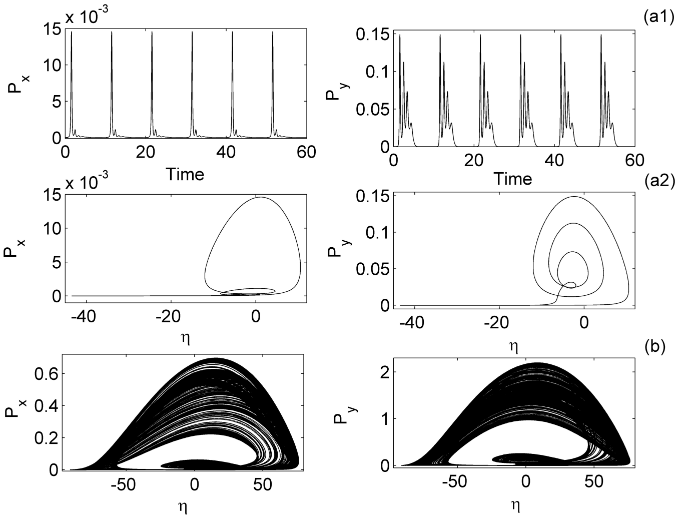


Figure 1 Pulse packages and chaotic attractors for given values of parameters j_{dc}, j_m, f_m: (a) $j_{dc} = 0.1$, $j_m = 0.005$, $f_m = 100\,MHz$ and (b) $j_{dc} = 0.12$, $j_m = 0.065$, $f_m = 3.2\,GHz$. The initial conditions are $\left(P_x\left(0\right), P_y\left(0\right), \eta\left(0\right)\right) = \left(0.01, 0.001, 0.1\right)$.

The photon densities display regular pulse packages in Fig. 1 (a) while in Fig. 1 (b) they exhibit chaotic attractors.

It is firstly assumed the case where the two coupled VCSELs are identical but with different initial conditions: $\left(P_{x1}\left(0\right), P_{y1}\left(0\right), \eta_1\left(0\right)\right) = \left(0.01, 0.001, 0.1\right)$ and $\left(P_{x2}\left(0\right), P_{y2}\left(0\right), \eta_2\left(0\right)\right) = \left(0.011, 0.001, 0.1\right)$. This means that the two VCSELs have the same threshold current, output power and relaxation oscillation frequency. In Figure 2, the higher synchronization error of both PMs as a function of coupling strength K in the chaotic regime are displayed.

In Fig. 2, when the maximal synchronization error of the absolute value of $\left(P_{x1,y1} - P_{x2,y2}\right)$ becomes equal to zero, this means that the two VCSELs are in a chaotic synchronization. This appears for $K \geq 1.33$ as shown in Fig. 2. The synchronization diagrams of photon densities of two coupled VCSELs are depicted in Fig. 3 in order to further emphasize the different synchronization properties found in Fig. 2.

For the coupling strength $K = 1$, there is no chaos synchronization between chaotic coupled CMVCSELs as seen in Fig. 3 (a) whereas in Fig. 3 (b) for $K = 1.4$, it is clear that CMVCSELs are well synchronized.

However, the high quality of synchronization mentioned here can only be achieved for the ideal condition. Regarding applications, parameters such as mismatch of device parameters, noise, coupling asymmetry, different bias current, etc. Moreover in a physical system, the parameters cannot remain constant in the course of its utilization. It may fluctuate due to the internal instabilities of the system or due to the perturbations from the environment. Fluctuations introduce parametric mismatches in coupled systems. Hence,

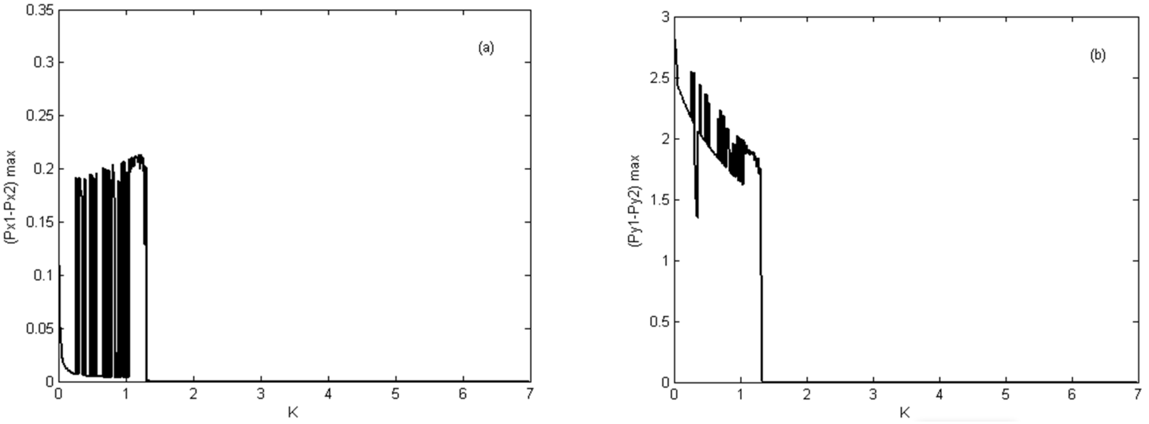


Figure 2 Variation of the maximal synchronization error of x-PM (a) and y-PM (b) versus the coupling strength K for $j_{dc} = 0.12,\ j_m = 0.065$, and $f_m = 3.2\,GHz$.

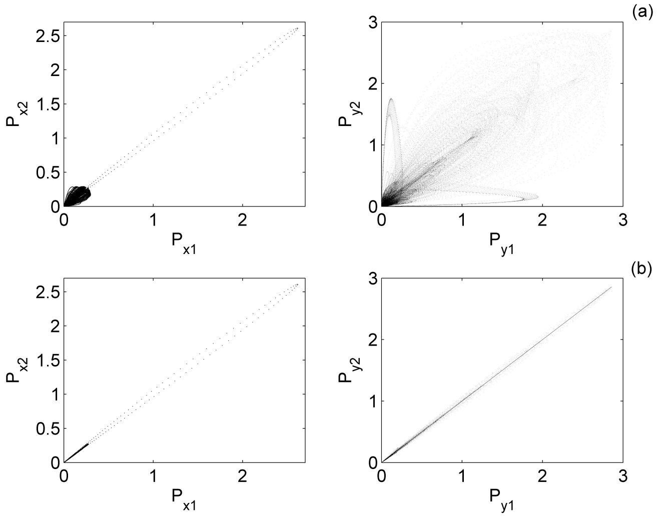


Figure 3 Synchronization diagrams for some values of the coupling strength : (a) $K = 1$ (b) $K = 1.4$ The initial conditions are $(P_{x1}(0), P_{y1}(0), \eta_1(0)) = (0.01, 0.001, 0.1)$ and $(P_{x2}(0), P_{y2}(0), \eta_2(0)) = (0.011, 0.001, 0.1)$.

it is relevant to check the robustness of synchronization in an environment where the parameters fluctuate. To analyze the influence of parameter mismatch, it is assumed that the parameters of VCSEL 2 are varied following the general rule:

$$a_2 = a_1\left[\alpha\,\%\,(2\xi - 1) + 1\right], \tag{3}$$

where ξ is a random number, a_1 is the parameter of the VCSEL 1 which in this case coincides with those used in Fig. 2, a_2 corresponds to the parameters of the VCSEL 2 and $\alpha\,\%$ is the percentage of parameter mismatch. By using this variation, the maximal synchronization error versus the coupling strength K for different percentages of parameter mismatch is plotted in Fig. 4.

Figure 4 shows that the maximal synchronization error of both PMs effectively increases with the parameter mismatch. Chaos synchronization is lost for a parameter mismatch of 1%. A severe degradation of synchronization is noticed in x-PM above 1% (see Fig. 4 (a) than in y-PM (see Fig. 4 (b)).

The synchronization time is the duration from the launching of the synchronization process to the time where the synchronization is attained. In secure communication technologies, the synchronization time plays a central role since the range of time during which the chaotic VCSELs are not synchronized corresponds to the range of time during which the coded message can unfortunately not be recovered or sent. This loss of information can prove to be damaging in some circumstances. Hence, it clearly appears that T_{syn} has to be minimized, so that the chaotic VCSELs synchronize as fast as possible. The synchronization time is given as (Woafo and Kraenkel 2002):

$$T_{syn} = t_{syn} - T_0, \tag{4}$$

where t_{syn} is the time instant at which the trajectories of VCSEL 1 and VCSEL 2 are close enough to be considered as synchronized. Here, synchronization is achieved when the deviation [ε_1 obeys the following synchronization criterion:

$$\varepsilon_1 = \left|P_{x1,y1} - P_{x2,y2}\right| \prec h\,,\ \forall t \succ t_{syn}, \tag{5}$$

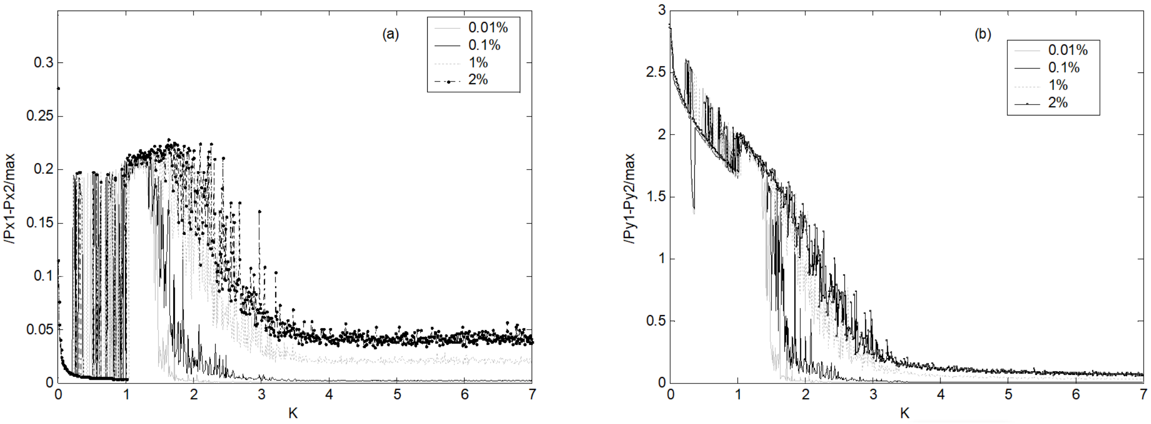


Figure 4 Variation of the maximal synchronization error of x-PM (a) and y-PM (b) versus the coupling strength K for different percentages of parameter mismatch.

where h is the synchronization precision or tolerance. The parameter T_{syn} is plotted versus the parameter K in Fig. 5.

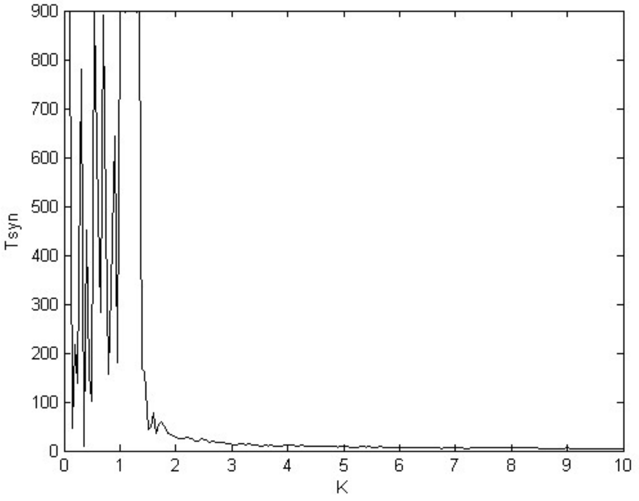


Figure 5 Synchronization time (T_{syn}) versus the coupling strength K in coupled CMVCSELs in the chaotic regime for synchronization precision $h = 10^{-6}$ and $T_0 = 100$.

It is noticed that for T_{syn} very close to the synchronization boundaries, its value is very large, however the coupling strength K approaches the limits, then T_{syn} decreases and for large K, it reaches a limit value of approximately about 4.0. Fig. 5 also shows that very large K values are not necessary to ensure the synchronization with approximately the minimum T_{syn}.

CONCLUSION

In this paper, the synchronization of two chaotic current modulated vertical cavity surface-emitting lasers based on the combined model of Danckaert et al. was carried out through a bidirectional coupling. A robust and quasi-perfect synchronization were found for a specific range of coupling strength. The quality of synchronization was influenced by parameter mismatch and it was found a severe degradation of synchronization for a parameter mismatch equal and above 1%. An asymptotic minimal value of the synchronization time was reached.

Acknowledgments

Authors would like to thank Doctor Foutse Momo (Université des Montagnes, Bangangté, Cameroun) for careful reading of the manuscript. S.T.K. thanks Professor Paul Woafo (Department of Physics, University of Yaounde I, Cameroon) and Doctor Jimmy Hervé Talla Mbe (Department of Physics, University of Dschang, Cameroon) for interesting discussions.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Argyris, A., D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, *et al.*, 2005 Chaos-based communications at high bit rates using commercial fibre-optic links. Nature **438**: 343–346.

Bindu, V. and V. Nandakumaran, 2000 Numerical studies on bi-directionally coupled directly modulated semiconductor lasers. Physics Letters A **277**: 345–351.

Colet, P. and R. Roy, 1994 Digital communication with synchronized chaotic lasers. Optics letters **19**: 2056–2058.

Danckaert, J., B. Nagler, J. Albert, K. Panajotov, I. Veretennicoff, *et al.*, 2002 Minimal rate equations describing polarization switching in vertical-cavity surface-emitting lasers. Optics Communications **201**: 129–137.

Goedgebuer, J.-P., L. Larger, and H. Porte, 1998 Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode. Physical Review Letters **80**: 2249.

Kingni, S., J. T. Mbé, and P. Woafo, 2012 Nonlinear dynamics in vcsels driven by a sinusoidally modulated current and rössler oscillator. The European Physical Journal Plus **127**: 1–10.

Kingni, S. T., C. Ainamon, V. K. Tamba, and J. C. OROU, 2020 Directly modulated semiconductor ring lasers: Chaos synchronization and applications to cryptography communications. Chaos Theory and Applications **2**: 31–39.

Kouomou, Y. C. and P. Woafo, 2003 Stability analysis for the synchronization of semiconductor lasers with ultra-high frequency current modulation. Physics Letters A **308**: 381–390.

Li, X., W. Pan, B. Luo, D. Ma, and W. Zhang, 2007 Nonlinear dynamics and localized synchronization in mutually coupled vcsels. Optics & Laser Technology **39**: 875–880.

Masoller, C., M. S. Torre, and K. A. Shore, 2007 Polarization dynamics of current-modulated vertical-cavity surface-emitting lasers. IEEE journal of quantum electronics **43**: 1074–1082.

Mbé, J. T., K. Takougang, and P. Woafo, 2010 Chaos and pulse packages in current-modulated vcsels. Physica Scripta **81**: 035002.

Roy, A., A. Misra, and S. Banerjee, 2019 Chaos-based image encryption using vertical-cavity surface-emitting lasers. Optik **176**: 119–131.

Roy, R. and K. S. Thornburg Jr, 1994 Experimental synchronization of chaotic lasers. Physical Review Letters **72**: 2009.

Sciamanna, M., I. Gatare, A. Locquet, and K. Panajotov, 2007 Polarization synchronization in unidirectionally coupled vertical-cavity surface-emitting lasers with orthogonal optical injection. Physical Review E **75**: 056213.

Sugawara, T., M. Tachikawa, T. Tsukamoto, and T. Shimizu, 1994 Observation of synchronization in laser chaos. Physical review letters **72**: 3502.

Tabaka, A., M. Peil, M. Sciamanna, I. Fischer, W. Elsäßer, *et al.*, 2006 Dynamics of vertical-cavity surface-emitting lasers in the short external cavity regime: Pulse packages and polarization mode competition. Physical Review A **73**: 013810.

Takougang Kingni, S., J. Hervé Talla Mbé, and P. Woafo, 2012 Semiconductor lasers driven by self-sustained chaotic electronic oscillators and applications to optical chaos cryptography. Chaos: An Interdisciplinary Journal of Nonlinear Science **22**: 033108.

Valle, A., M. Sciamanna, and K. Panajotov, 2007 Nonlinear dynamics of the polarization of multitransverse mode vertical-cavity surface-emitting lasers under current modulation. Physical Review E **76**: 046206.

Vanwiggeren, G. D. and R. Roy, 1998 Communication with chaotic lasers. Science **279**: 1198–1200.

Wang, H., T. Lu, and Y. Ji, 2020 Key space enhancement of a chaos secure communication based on vcsels with a common phase-modulated electro-optic feedback. Optics Express **28**: 23961–23977.

Woafo, P. and R. A. Kraenkel, 2002 Synchronization: Stability and duration time. Physical Review E **65**: 036225.

Xie, Y.-Y., J.-C. Li, C. He, Z.-D. Zhang, T.-T. Song, *et al.*, 2016 Long-distance multi-channel bidirectional chaos communication based on synchronized vcsels subject to chaotic signal injection. Optics Communications **377**: 1–9.

Zhong, D.-Z., G.-Q. Xia, Z.-M. Wu, and X.-H. Jia, 2008 Complete chaotic synchronization characteristics of the linear-polarization mode of vertical-cavity surface-emitting semiconductor lasers with isotropic optical feedback. Optics communications **281**: 1698–1709.

How to cite this article: Saeed, N., Kemnang Tsafack, A. S., Malwe Boudoue, H. and Kingni, S. T. Chaos synchronization in chaotic current modulated VCSELs by bidirectional coupling. Chaos Theory and Applications, 3(1), 29-33, 2021.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / No.1 / 2021 / pp.34-42
https://doi.org/10.51537/chaos.936679

Discrete Superior Hyperbolicity in Chaotic Maps

Ashish [*,1], **Jinde Cao** [β,2], **Fawaz Alsaadi** [‡,3] **and A. K. Malik** [§§,4]

[*]Department of Mathematics, Government College Satnali, Mahendergarh-123024, India, [β]School of Mathematics, Southeast University, Nanjing-210096, China, [β]Yonsei Frontier Lab, Yonsei University, Seoul-03722, South Korea, [‡]Department of Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, [§§]B. K. Birla Institute of Engineering and Technology, Pilani-333031, India.

ABSTRACT In the last few decades, the dynamics of one-dimensional chaotic maps have gained the tremendous attention of scientists and scholars due to their remarkable properties such as period-doubling, chaotic evolution, Lyapunov exponent, etc. The term hyperbolicity, another important property of chaotic maps is used to examine the regular and irregular behavior of the dynamical systems. In this article, we deal with the hyperbolicity and stabilization of fixed states using a superior two-step feedback system. Due to the superiority in the chaotic evolution of one-dimensional maps in the superior system we are encouraged to examine the hyperbolicity and stabilization in chaotic maps. The hyperbolic notion, hyperbolicity in periodic states of prime order, stabilization, and the hyperbolic set of the chaotic maps are studied. The numerical, as well as experimental simulations, are carried out, followed by theorems, examples, remarks, functional plots, and bifurcation diagrams.

KEYWORDS
Chaos
Hyperbolicity
Bifurcation plot
Chaotic maps

INTRODUCTION

Hyperbolicity, in short, is an effective and efficient tool that examines the regular and irregular behavior in nonlinear dynamical systems. In fact, it induces an invariant set for different parameter values which are responsible for the chaotic phenomena of a dynamical system. It was Poincare (1899) who first introduced the hypothesis of chaotic phenomena which is considered as an essential factor in the study of hyperbolicity and stabilization. Surprisingly, the standard chaotic map $\nu p(1-p)$, a model of population growth has a significant role in the simulation of hyperbolicity, invariant sets, and stability in chaos theory.

P. F. Verhlust (1845 and 1847) first established the chaotic map $\nu p(1-p)$ as a model of population growth, where the parameter ν varies in a certain range. But the dynamical appearance in any chaotic system leads to 2^n periodic cycles through a bifurcation plot. Finally, the bifurcation plot leads to a chaotic domain which gives a set of invariant measures and is known as a hyperbolic set. Further, for a detailed study on hyperbolicity and on its stability one may refer to, Robinson (1995), Holmgren (1994), Devaney (1948), Devaney (1992), Alligood *et al.* (1996), Martelli (1999), Chugh *et al.* (2012), etc..

In the last few decades, the hyperbolicity and the stabilization in fixed and periodic states have been studied by various academicians using standard chaotic systems. In 2001, Glendinning (2001) examined the hyperbolicity in the standard chaotic system $\nu p(1-p)$, for the parameter range $4 < \nu \leq 2+\sqrt{5}$ and also established a good estimation of the expansion rate on invariant sets. In 2003, Kraft (1999) studied some analytical results on the hyperbolicity of chaotic maps for $\nu > 4$ using Schwarzian derivative and shown that it is negative except for its critical states.

Robinson (1995) and Newhouse (1981) proved the repelling hyperbolicity on invariant sets using Schwarz Lemma for complex functions. Further, Guckenheimer (1979), Melo (1993) and Misiurewicz (1976) also described some analytical results using kneading theory and Schwarzian derivative. In 2003, Aulbach *et al.* (2004) using elementary calculus established that the invariant set Λ_ν is hyperbolic for $\nu > 4$ and also proved that for $\nu > 4$, the

Manuscript received: 13 May 2021,
Revised: 11 June 2021,
Accepted: 15 June 2021.

[1] akrmsc@gmail.com
[2] jdcao@seu.edu.cn
[3] fesalsaadi@kau.edu.sa
[4] ajender.malik@bkbiet.ac.in (**Corresponding Author**)

system is chaotic with the capacity of Bernoulli shift defined on $[0, 1]$.

In the twenty first century, the chaotic maps have played a crucial role in every branch of science such as in traffic control system (Ashish *et al.* 2018, 2019b), cryptography, (Wang 2017; Akgul 2013), secure communication (Baptista *et al.* 1998), etc. Further, for a detailed study one may refer to Adiyaman (2020), Andrecut (1998), Ausloos *et al.* (2006), Jonassen (2002), Saha (2009), Saha (2010), Sharkovsky *et al.* (1993), Kumar (2020), Volos (2018), etc.

Recently, in 2021, Ashish *et al.* (2021) introduced a modulated logistic system and reported superior chaos through period-doubling, period-three orbit, and Lyapunov exponent. Also, they examined the elementary properties for chaotic maps in Ashish *et al.* (2019a), controlling chaos with applications in the traffic control system in Ashish *et al.* (2019b) and irregularity in Ashish *et al.* (2018) using two-step feedback approach.

The article is arranged into five major sections. Section 1 accommodates essential literature review and Section 2 consists of elementary results. The results on hyperbolicity and stability of periodic states of prime order are described in Section 3. An experimental simulation for hyperbolic sets in the two-step superior system is described in Section 4. Finally, all the results are summarized in Section 5.

PRELIMINARIES

This section deals with some basic entities in chaos theory that are used in further sections to determine the hyperbolicity of the chaotic maps in a superior two-step feedback system.

Definition 1. (Hyperbolicity). Let $\tilde{p}$ be a periodic point of order $n \in N$, then $\tilde{p}$ is said to be hyperbolic for the map f if it satisfy $\mid (f^{(n)})'(\tilde{p}) \mid \neq 1$ (Devaney 1948).

Definition 2. (Periodic state). Let $\tilde{p} \in X$ be a point and f be a map defined on X. Then, $\tilde{p}$ is periodic of prime order n if $f^{(n)}(\tilde{p}) = \tilde{p}$ but $f^{(m)}(\tilde{p}) \neq \tilde{p}$ for $1 \leq m < n$ (Devaney 1992).

Definition 3. (Sink and stretch states). A point $\tilde{p} \in X$ for a map f is said to be sink if $|f'(p)| < 1$ and is said to be stretch if $|f'(p)| > 1$ (Devaney 1992).

Definition 4. (Superior two-step feedback system). For an initiator $p \in X$, the iterative sequence $\{p_n\}$ defined by $p_{n+1} = p_n - \alpha_n(p_n - f(p_n))$, where $0 \leq \alpha_n \leq 1$ is said to be superior iterative orbit and the complete process is known as superior two-step feedback system (Mann 1953).

Definition 5. (Hyperbolic set). Let Λ be an invariant set for the map f defined on X, that is, $f(\Lambda) = \Lambda$. Then, the invariant set Λ is said to be hyperbolic, if it satisfy $\mid (f^{(n)})'(p) \mid \geq K\theta^n$, for $p \in \Lambda$, $n \geq 1$, $\theta > 1$ and constant $K > 0$ (Devaney 1948).

HYPERBOLICITY AND STABILIZATION ANALYSIS

Throughout this section, we deal with the analytical as well as numerical simulations for hyperbolicity and stabilization of fixed and periodic states of chaotic maps in a superior two-step feedback system. The hyperbolicity and stabilization in fixed and periodic states is described, followed by some theorems, examples and remarks. Therefore, let us consider f_μ be a chaotic map defined on X. Then, from Definition 4, for the superior two-step feedback system, we can write

$$p_{n+1} = p_n - \alpha(p_n - f_\nu(p_n)) = S_{\alpha,\nu}(p). \quad \text{(say)} \qquad (1)$$

Then, for an initiator $p_0 \in X$ and using (1) we obtain the following iterative sequence,

$$SO^+(p_0) = \{p_0, p_1, p_2, ...\} \qquad (2)$$

and is said to be forward iterative sequence for an initiator p_0. Similarly, we get the relation

$$SO^-(p_0) = \{p_0, p_{-1}, p_{-2}, ...\} \qquad (3)$$

and is said to be backward iterative sequence for an initiator p_0. Then, from (2) and (3), we obtain the following complete iterative sequence

$$\begin{aligned} SO(p_0) &= \{p_0, p_{-1}, p_{-2}, ...\} \bigcup \{p_0, p_1, p_2, ...\}, \\ &= \{..., p_{-2}, p_{-1}, p_0, p_1, p_2, ...\}, \\ &= \{p_n : n \in Z\}. \end{aligned}$$

Also, for the n^{th} iterate of the chaotic map f_ν using (1) we obtain

$$p_{n+1} = (1-\alpha)p_n + \alpha f(f_\nu^{n-1}(p_0))_{n \in N} = S^{(n)}_{\alpha,\nu}(p). \qquad (4)$$

Thus, it is noticed that in a casual dynamical system the forward iterative sequence (2) is named as the superior orbit for an initiator $p_0 \in X$. Therefore, using the relation (4), first we introduce the definition of hyperbolicity followed by a few examples and then prove the stability results using a superior two-step feedback system.

Hyperbolicity

Hyperbolicity, another eminent property of chaotic maps is illustrated to examine the regular and irregular movements in nonlinear systems. Therefore, this subsection deals with the hyperbolicity in fixed and periodic states using a superior two-step feedback system.

Definition 6. Let $S_{\alpha,\nu}(p)$ be the superior two-step system and f_ν be a chaotic map defined on X. Then, the point $\tilde{p} \in X$ of prime order n is said to be superior hyperbolic of order-n if it satisfy $\mid (S^{(n)}_{\alpha,\nu})'(\tilde{p}) \mid \neq 1$, where $\alpha \in (0, 1)$, $n \in N$ and $\nu > 0$.

Example 1. *Let us consider $S_{\alpha,\nu}(p) = p - \alpha(p - f_\nu(p))$ be the superior two-step system and $f_\nu(p) = \nu p(1-p)$ be the chaotic map, where $\nu \in [0, 4.22]$. Then, determine the domain of parameter ν for which the fixed-point $\tilde{p} \in [0,1]$ admits hyperbolicity.*

Solution. Since $S_{\alpha,\nu}(p) = p - \alpha(p - f_\nu(p))$ and $f_\nu(p) = \nu p(1-p)$, where $\nu \in [0, 4.22]$. Then, from Definition 1 for superior hyperbolicity, we can say

$$\begin{aligned} \mid (S_{\alpha,\nu})'(p) \mid &= \mid 1 - \alpha + \alpha f_\nu'(p) \mid, \\ &= \mid 1 - \alpha + \alpha(\nu - 2\nu p) \mid . \end{aligned} \tag{5}$$

Also, the point $\tilde{p} = 0$ and $\tilde{p} = 1 - \frac{1}{\nu}$ are the two fixed points of prime order one of the system $S_{\alpha,\nu}(p)$. Therefore, substituting $\tilde{p}$ one by one in (5), we obtain

$$\mid (S_{\alpha,\nu})'(0) \mid = \mid 1 - \alpha + \alpha\nu \mid \tag{6}$$

and
$$\begin{aligned} \mid (S_{\alpha,\nu})'(1 - \frac{1}{\nu}) \mid &= \mid 1 - \alpha + \alpha(\nu - 2\nu(1 - \frac{1}{\nu}) \mid, \\ &= \mid 1 - \alpha + \alpha(2 + \nu - 2\nu) \mid, \\ &= \mid 1 + \alpha - \alpha\nu) \mid . \end{aligned} \tag{7}$$

Since the growth-rate parameter $\nu \in [0, 4.22]$ and $\alpha \in (0,1)$, therefore, it is clear from (6) and (7) that both the fixed states are hyperbolic when $\nu \neq 1$, that is, $\nu \in (0,1) \bigcup (1, 4.22]$. Figure 1, shows the hyperbolic behavior of the fixed states at $\nu = 1$. To understand more about the hyperbolicity of fixed and periodic states, the graphical plot of the trajectories for the functions $S_{\alpha,\nu}(p)$ and $S^2_{\alpha,\nu}(p)$ is drawn in Figures 1-4. It is interesting to see that all the fixed and periodic states shown in Figures 1-4 are satisfied by Definition 1 of hyperbolicity. Figure 1 shows the functional plot using the superior system $S_{\alpha,\nu}(p)$ for $\nu = 1$, $\nu > 1$ and $\nu < 1$. For $\nu = 1$, the diagram shows that the fixed point 0 is completely hyperbolic, that is, $\mid (S_{\alpha,1})'(0) \mid \neq 1$. While the bifurcation plot in Figure 2 shows that at $\nu = 1$ the trajectory approaches to the fixed point $1 - \frac{1}{\nu}$ and then again at $\nu = 3.2$ the fixed point $1 - \frac{1}{\nu}$ bifurcates into the hyperbolic periodic point of order 2. Further, Figure 3 shows the hyperbolicity of periodic points of order 2 for the system $S^2_{\alpha,\nu}(p)$. For $\nu = 3.2$, $\nu < 3.2$ and $\nu > 3.2$ it admits completely hyperbolic state, hyperbolic repelling state and hyperbolic attracting state, respectively. Moreover, the magnified Figure 4 represents the hyperbolicity in higher order periodic points.

Example 2. *Let us consider $S_{\alpha,\nu}(p) = p - \alpha(p - f_\nu(p))$ be the superior two-step system and $f_\nu(p) = \nu p(1-p)^m$, where $m > 1$ and $\nu > 0$ be a chaotic map. Then, determine the domain of parameter ν for which the fixed point $\tilde{p} \in [0,1]$ admits hyperbolicity.*

Solution. Since $S_{\alpha,\nu}(p) = p - \alpha(p - f_\nu(p))$ and $f_\nu(p) = \nu p(1-p)^m$. Then, from the above definition of hyperbolicity, we have

$$\begin{aligned} \mid (S_{\alpha,\nu})'(p) \mid &= \mid 1 - \alpha + \alpha f_\nu'(p) \mid, \\ &= \mid 1 - \alpha + \alpha(\nu(1-p)^m - \nu p m(1-p)^{m-1}) \mid . \end{aligned} \tag{8}$$

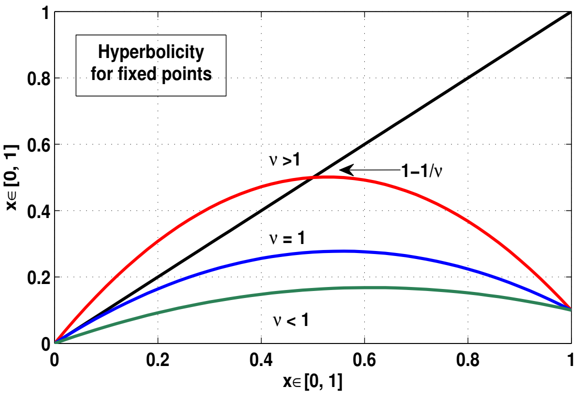


Figure 1 Functional plot for $\nu p(1-p)$ in $S_{\alpha,\nu}(p)$ for $\nu > 1$, $\nu < 1$ and $\nu = 1$

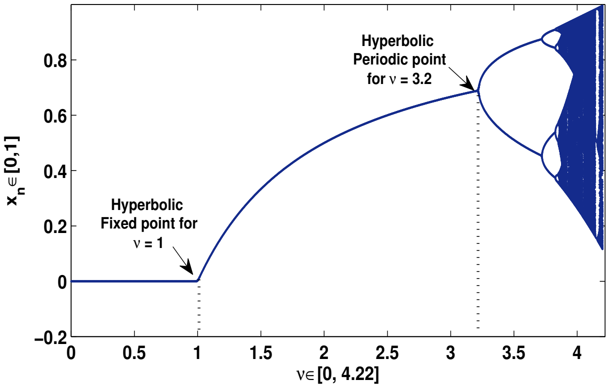


Figure 2 Bifurcation plot for $\nu p(1-p)$ in $S_{\alpha,\nu}(p)$ for $0 \leq \nu \leq 4.22$

Also, the point $\tilde{p} = 0$ and $\tilde{p} = 1 - \frac{1}{\sqrt[m]{\nu}}$ are the two fixed point of prime order one for the system $S_{\alpha,\nu}(p)$. Therefore, substituting $\tilde{p}$ one by one in (8), we obtain

$$\mid (S_{\alpha,\nu})'(0) \mid = \mid 1 - \alpha + \alpha\nu \mid \tag{9}$$

$$\begin{aligned} \mid (S_{\alpha,\nu})'(1 - \frac{1}{\sqrt[m]{\nu}}) \mid &= \mid 1 - \alpha + \alpha - \nu\alpha m(1 - \frac{1}{\sqrt[m]{\nu}})(\frac{1}{\sqrt[m]{\nu}})^{m-1}) \mid, \\ &= \mid 1 - \nu\alpha m(1 - \frac{1}{\sqrt[m]{\nu}})(\frac{1}{\sqrt[m]{\nu}})^{m-1}) \mid, \\ &= \mid 1 - \alpha m(\nu^{1/m} - 1) \mid . \end{aligned}$$

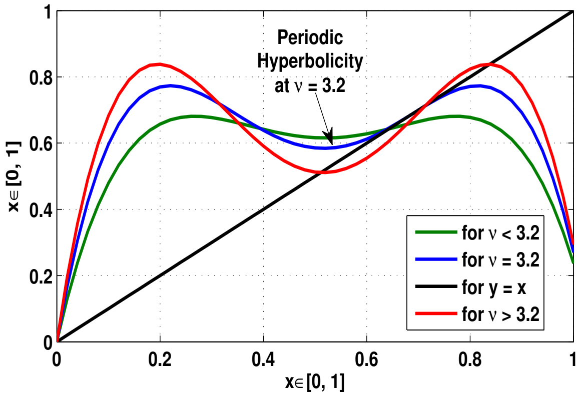


Figure 3 Periodic plot for $\nu p(1-p)$ in $S^2_{\alpha,\nu}(p)$ for $\nu = 3.2, \nu > 3.2, \nu < 3.2$

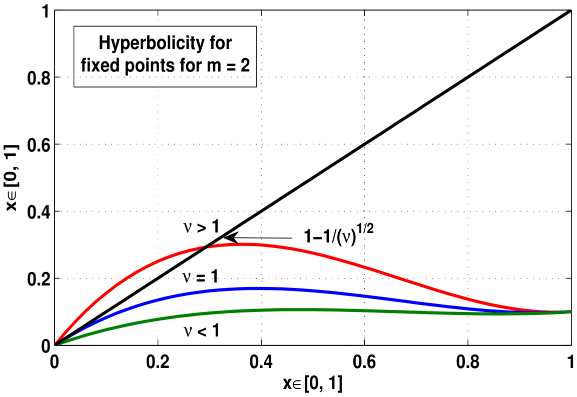


Figure 5 Functional plot for $\nu p(1-p)^2$ in $S_{\alpha,\nu}(p)$ for $\nu > 1, \nu < 1$ and $\nu = 1$

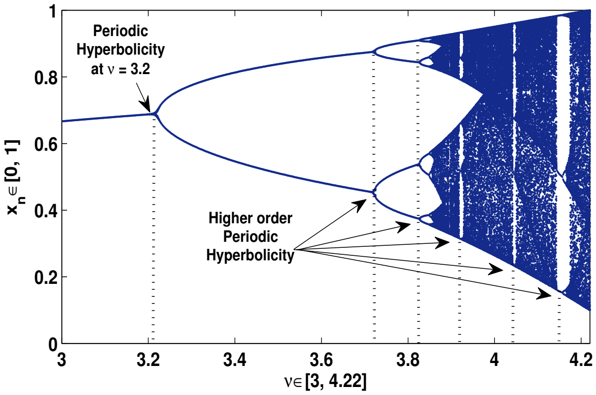


Figure 4 Hyperbolic periodic plot for $\nu p(1-p)$ in $S_{\alpha,\nu}(p)$ for $3 \leq \nu \leq 4.22$

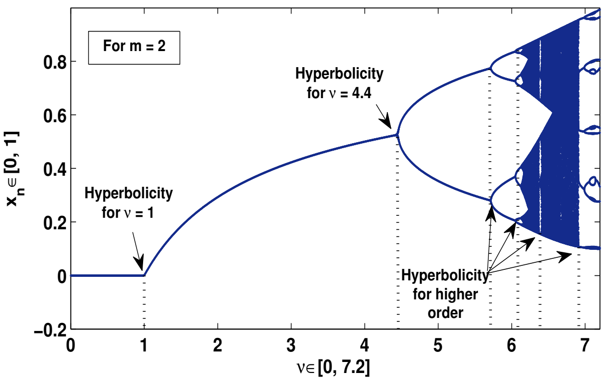


Figure 6 Hyperbolic periodic plot for $\nu p(1-p)^2$ in $S_{\alpha,\nu}(p)$ for $0 < \nu \leq 7.2$

Since the growth-rate parameter $\nu \in (0, \nu_{max}]$ and $\alpha \in (0,1)$, thus, it is clear from (8) and (9) that both the fixed point are hyperbolic when $\nu \neq 1$, that is, $\nu \in (0,1) \bigcup (1, \nu_{max}]$. In particular, for $m = 2$ and $\nu \in (0,1) \bigcup (1, 7.2]$, Figure 5 and 6, shows the hyperbolic fixed and periodic states. Figure 5 represents the functional plot for the quadratic map $\nu p(1-p)^2$ using superior system $S_{\alpha,\nu}(p)$ for $\nu = 1$, $\nu > 1$ and $\nu < 1$. For $\nu = 1$ it shows that the fixed state 0 is completely hyperbolic, that is, $\mid (S_{\alpha,1})'(0) \mid \neq 1$ for each $\alpha \in (0,1)$. While the Figure 6 shows that the at the hyperbolic state $\nu = 1$ the trajectory approaches to the fixed state $1 - \frac{1}{\sqrt[2]{\nu}}$ and then again at $\nu = 4.4$ the fixed state $1 - \frac{1}{\sqrt[2]{\nu}}$ bifurcates into the hyperbolic periodic fixed states of order 2. Further, as ν approaches through 4.4 the hyperbolic states for higher order periodic states also exists as shown in Figure 6.

Stabilization

In this subsection, we deal with the stabilization of hyperbolic fixed and periodic states for chaotic maps using a superior two-step feedback system. The main results are followed by corollaries and remarks:

Theorem 1. *Let $S_{\alpha,\nu}(p)$ be a superior recursive system and f_ν be a chaotic map defined on X. Also, let $\tilde{p}$ be a hyperbolic fixed state for f_ν such that $\mid (S_{\alpha,\nu})'(\tilde{p}) \mid < 1$. Then, for $\tilde{p} \in X$, there exists a neighbourhood Y such that for each $p \in Y$, we obtain*

$$S^n_{\alpha,\nu}(p) \to \tilde{p} \quad \textit{as} \quad n \to \infty,$$
$$\textit{or} \qquad \lim_{n\to\infty} S^n_{\alpha,\nu}(p) = \tilde{p}.$$

Proof. Let f_ν be a chaotic map defined on X with a hyperbolic fixed state $\tilde{p} \in X$. Then, there exists a number $\kappa > 0$, however small, such that

$$\begin{aligned} &\mid (S_{\alpha,\nu})'(p) \mid < 1, \quad \text{for} \quad p \in [\tilde{p} - \kappa, \tilde{p} + \kappa], \text{that is,} \\ &\mid (S_{\alpha,\nu})'(p) \mid < P < 1, \quad \text{for} \quad p \in [\tilde{p} - \kappa, \tilde{p} + \kappa]. \quad (10) \end{aligned}$$

Then, from the statement of Mean Value Theorem and using Definition 2 of periodic state, we can write

$$\begin{aligned}
\mid S_{\alpha,\nu}(p)-\tilde{p}\mid &=\mid S_{\alpha,\nu}(p)-S_{\alpha,\nu}(\tilde{p})\mid,\\
&=\mid (S_{\alpha,\mu})'(s)\mid\mid p-\tilde{p}\mid, \qquad s\in[p,\tilde{p}]\\
&< P\mid p-\tilde{p}\mid,\\
&\leq\mid p-\tilde{p}\mid, \qquad (\because P<1)\\
&\leq \kappa, \qquad (\because\mid p-\tilde{p}\mid<\kappa)
\end{aligned}$$

$$\text{that is,}\quad \mid S_{\alpha,\nu}(p)-\tilde{p}\mid\leq\kappa. \tag{11}$$

Thus, $S_{\alpha,\nu}(p)\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$, for each $p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$. Inductively, it is also clear that for each $p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$, we can say

$$S^{n}_{\alpha,\nu}(p)\in[\tilde{p}-\kappa,\tilde{p}+\kappa], \quad \text{for each} \quad n\in N. \tag{12}$$

Then, again using the statement of Mean Value Theorem for the n^{th} iterate of the system $S_{\alpha,\nu}(p)$, we obtain

$$\begin{aligned}
\mid S^{n}_{\alpha,\nu}(p)-\tilde{p}\mid &=\mid S^{n}_{\alpha,\nu}(p)-S^{n}_{\alpha,\nu}(\tilde{p})\mid, \qquad (13)\\
&=\mid (S^{(n)}_{\alpha,\nu})'(s)\mid\mid p-\tilde{p}\mid, \quad \text{for } s\in[p,\tilde{p}].
\end{aligned}$$

Now, from Devaney's (Devaney 1992) Definition for Chain rule of product along a cycle, we can write

$$\mid (S^{(n)}_{\alpha,\nu})'(p)\mid=\prod_{i=0}^{n-1}S'_{\alpha,\nu}(S^{i}_{\alpha,\nu}(p)), \tag{14}$$

for $p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$ and $n\in N$. Then, from (10) and (14), we get

$$\mid (S^{(n)}_{\alpha,\nu})'(p)\mid=\prod_{i=0}^{n-1}S'_{\alpha,\nu}(S^{i}_{\alpha,\nu}(p))<1,$$

$$\text{that is,}\quad \mid (S^{(n)}_{\alpha,\nu})'(p)\mid<P^{n}<1. \tag{15}$$

Then, from the relation (13) and (15), we find

$$\mid S^{n}_{\alpha,\nu}(p)-\tilde{p}\mid<P^{n}\mid p-\tilde{p}\mid<\kappa. \tag{16}$$

Thus, $S^{n}_{\alpha,\nu}(p)\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$, for each $p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$. Hence taking $n\to\infty$ in (16), we get the required result

$$\begin{aligned}
&\mid S^{n}_{\alpha,\nu}(p)-\tilde{p}\mid<P^{n}\mid p-\tilde{p}\mid\to 0,\\
\text{that is,}\quad &\lim_{n\to\infty}S^{n}_{\alpha,\nu}(p)=\tilde{p}.
\end{aligned}$$

Hence proved. □

Theorem 2. *Let $S_{\alpha,\nu}(p)$ be a superior recursive system and f_ν be a chaotic map defined on X. Let $\tilde{p}$ be a hyperbolic state of order n satisfying $\mid (S^{(n)}_{\alpha,\nu})'(\tilde{p})\mid<1$. Then, for $\tilde{p}\in X$, there exists a neighbourhood Y such that for each $p\in Y$, we have*

$$\begin{aligned}
&S^{(nk)}_{\alpha,\nu}(p)\to\tilde{p} \quad \textit{as} \quad k\to\infty.\\
\textit{or} \quad &\lim_{k\to\infty}S^{(nk)}_{\alpha,\nu}(p)=\tilde{p}.
\end{aligned}$$

Proof. Since $S_{\alpha,\nu}(p)$ is a superior system and $\tilde{p}$ is a periodic state of f_ν, then, there exists a number $\kappa>0$, however small, such that

$$\begin{aligned}
&\mid (S^{(n)}_{\alpha,\nu})'(p)\mid<1, \quad \text{for} \quad p\in[\tilde{p}-\kappa,\tilde{p}+\kappa], \text{that is,}\\
&\mid (S^{(n)}_{\alpha,\nu})'(p)\mid<P^{n}<1, \quad \text{for} \quad p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]. \qquad (17)
\end{aligned}$$

Similarly for an arbitrary $k\in N$, we can say

$$\mid (S^{(nk)}_{\alpha,\nu})'(p)\mid<P^{(nk)}<1. \tag{18}$$

Then, using Mean Value Theorem, for the system $(S^{(nk)}_{\alpha,\nu})'(p)$, we obtain

$$\begin{aligned}
\mid S^{(nk)}_{\alpha,\nu}(p)-\tilde{p}\mid &=\mid S^{(nk)}_{\alpha,\nu}(p)-S^{(nk)}_{\alpha,\nu}(\tilde{p})\mid,\\
&=\mid (S^{(nk)}_{\alpha,\nu})'(s)\mid\mid p-\tilde{p}\mid, \quad \text{for} \quad s\in[p,\tilde{p}],\\
&<P^{nk}\mid p-\tilde{p}\mid,
\end{aligned}$$

$$\text{that is,}\quad \mid S^{(nk)}_{\alpha,\nu}(p)-\tilde{p}\mid<\kappa. \tag{19}$$

Thus, $S^{(nk)}_{\alpha,\nu}(p)\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$, for each $p\in[\tilde{p}-\kappa,\tilde{p}+\kappa]$. Hence taking as $k\to\infty$ in (19), we obtain

$$\begin{aligned}
&\mid S^{(nk)}_{\alpha,\nu}(p)-\tilde{p}\mid<P^{nk}\mid p-\tilde{p}\mid\to 0,\\
\text{that is,}\quad &\lim_{k\to\infty}S^{(nk)}_{\alpha,\nu}(p)=\tilde{p}.
\end{aligned}$$

Hence proved.

Corollary 1. *Let $S_{\alpha,\nu}(p)$ be a superior recursive system and f_ν be a chaotic map defined on X. Also, let $\tilde{p}$ be a hyperbolic state for the map f_ν such that $\mid (S_{\alpha,\nu})'(\tilde{p})\mid<1$. Then, for $\tilde{p}\in X$, there exists a neighbourhood Y such that for each $p\in Y$, we have*

$$\begin{aligned}
&S^{(-nk)}_{\alpha,\nu}(p)\to\tilde{p} \quad \textit{as} \quad k\to\infty\\
\textit{or} \quad &\lim_{k\to\infty}S^{(-nk)}_{\alpha,\nu}(p)=\tilde{p}.
\end{aligned}$$

Proof. The proof may be illustrated by using Theorem 1 and 2. □

Remark 1. Let $S_{\alpha,\nu}(p)$ be the superior recursive system and $\tilde{p}$ be a hyperbolic periodic state for the map f_ν satisfying $\mid (S^{(n)}_{\alpha,\nu})'(p)\mid<1$. Then, $\tilde{p}\in X$ is said to be hyperbolic stable of order-n. For $0<\nu<1$, the fixed point $\tilde{p}=0$ is hyperbolic stable and for $0<\nu<3.2$, the periodic state $\tilde{p}$ is hyperbolic stable as shown in Fig. 1 and 3.

Remark 2. Let $S_{\alpha,\nu}(p)$ be the superior recursive system and $\tilde{p}$ be a hyperbolic periodic fixed point for the map f_ν satisfying $\mid (S^{(n)}_{\alpha,\nu})'(p)\mid>1$. Then, $\tilde{p}$ is said to be hyperbolic unstable of order-n.

HYPERBOLIC SET

In the earlier sections, the hyperbolicity of fixed states and their stability is described in chaotic maps using the superior two-step system. But this section deals with the hyperbolic sets in chaotic maps using the superior two-step system. Therefore, let us start with the chaotic map $\nu p(1-p)$ and the system $S_{\alpha,\nu}(p)$. Figure 7 shows the functional plot of the system $S_{\alpha,\nu}(p)$ which gives a parabola and intercept at $(0,0)$ and $(1,0)$. For $p=\frac{1}{2}$ the system $S_{\alpha,\nu}(p)$ approaches a maximum $\frac{\nu}{4.22}>1$ if and only if $\nu>4.22$. In 1992, Devaney (1992) introduced that quadratic map $\nu p(1-p)$ for $\nu>4$ admits the following Cantor set representation

$$\Lambda_\nu = \bigcap_{n=1}^{\infty} I_{i_0 i_1 \ldots . i_n}, \tag{20}$$

where $I_{i_0} \supset I_{i_0 i_1} \supset \ldots . \supset I_{i_0 i_1 \ldots . i_n}$ is a nested sequence of closed intervals. Afterward, Kraft (1999) and Aulbach *et al.* (2004) also examined that for $\nu>4$, the set Λ_ν is hyperbolic, since it satisfies $\mid f_\nu'(p) \mid > 1$ for $\nu>4$. Therefore, looking into the potential of superior system in dynamical systems, the future work of hyperbolic set is studied in this section.

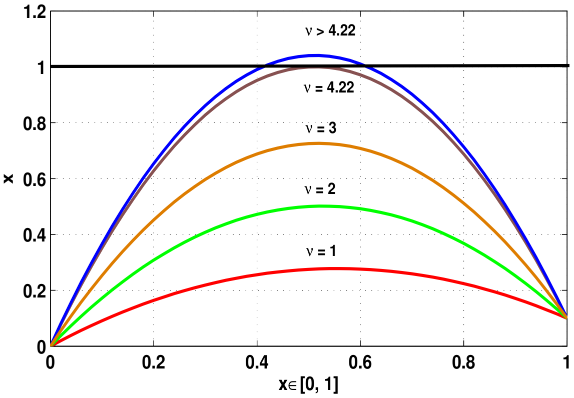


Figure 7 Functional plot for the system $S_{\alpha,\nu}(p)$ for $0<\nu\leq 4.22$ and $\nu>4.22$

Now, to examine hyperbolicity in $S_{\alpha,\nu}(p)$, let us take the quadratic map $\nu p(1-p)$, where $\nu>4.22$. Figure 7 shows the functional plot for the system $S_{\alpha,\nu}(p)$ for $\nu=1,2,3,4.22$ and 4.5 in different color radiations. It is observed that as the value of the growth-rate parameter ν lies in the closed interval $(0,4.22]$ the parameter $p\in[0,1]$. But as the value of ν approaches through 4.22, the functional plot also approaches beyond the closed interval $[0,1]$. That means, a Cantor set representation $\Lambda_{\alpha,\nu}$ admits a nested sequence of closed intervals which is hyperbolic for $\nu>4.22$. Moreover, it is examined that at $\nu=4.22$ all the higher order iterations of the system $S_{\alpha,\nu}(p)$ lies in $[0,1]$ as shown in Figure 8 for $S_{\alpha,\nu}(p)$, $S^2_{\alpha,\nu}(p)$ and $S^3_{\alpha,\nu}(p)$. But as ν approaches beyond 4.22, all the higher order iterations goes to $\pm\infty$ as shown in Figure 9. Also, from the Figure 10 it is analyzed that the bifurcation characteristic stops when $\nu=4.22$ and the hyperbolic set $\Lambda_{\alpha,\nu}$ exists for $\nu>4.22$.

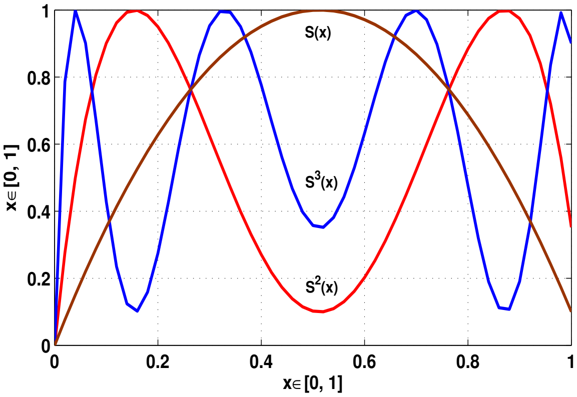


Figure 8 Functional plot $S_{\alpha,\nu}(p)$, $S^2_{\alpha,\nu}(p)$ and $S^3_{\alpha,\nu}(p)$ for $\nu=4.22$

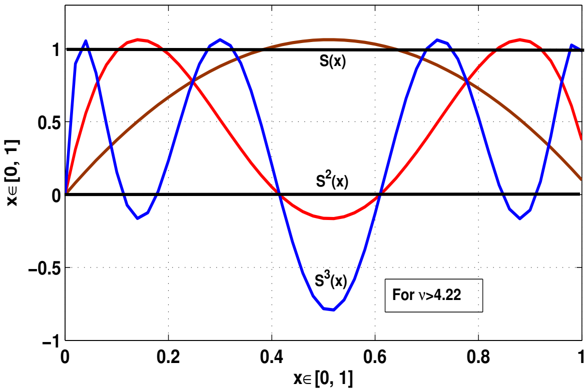


Figure 9 Functional plot $S_{\alpha,\nu}(p)$, $S^2_{\alpha,\nu}(p)$ and $S^3_{\alpha,\nu}(p)$ for $\nu>4.22$

Remark 3. From the above analysis it is noticed that as $\nu\in[0,4.22]$, $S^n_{\alpha,\nu}(p)\subset[0,1]$ and for $\nu>4.22$, $S^n_{\alpha,\nu}(p)\supset[0,1]$. For a particular value $\nu=4.5$, $S^n_{\alpha,\nu}(p)\to\infty$ as $n\to\infty$.

Remark 4. For $\nu>4.22$ the quadratic map $\nu p(1-p)$ in $S_{\alpha,\nu}(p)$ admits a compact invariant set $\Lambda_{\alpha,\nu}$ for $\nu>4.22$, which is hyperbolic for the system $S_{\alpha,\nu}(p)$.

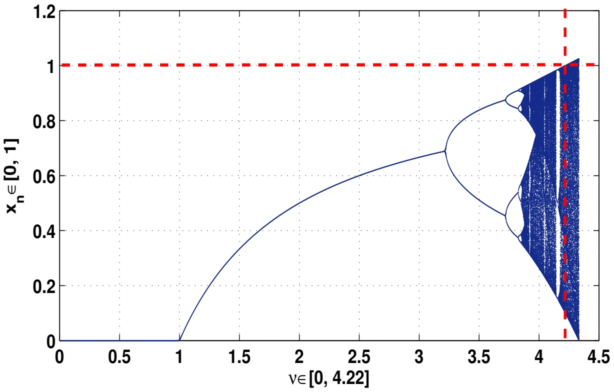


Figure 10 Bifurcation plot for the system $S_{\alpha,\nu}(p)$ for $0 \leq \nu \leq 4.5$

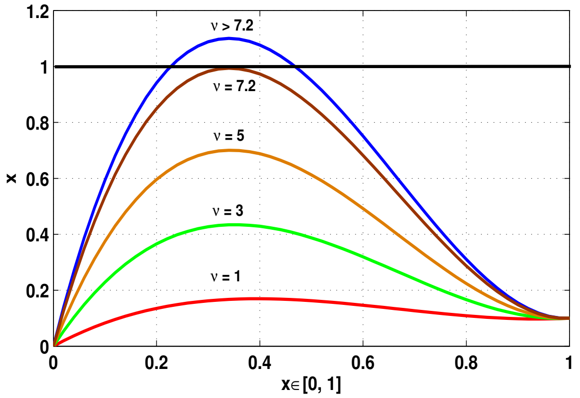


Figure 11 Functional plot for the system $S_{\alpha,\nu}(p)$ for $\nu \leq 7.2$ and $\nu > 7.2$

Similarly, we consider an another cubic map $f_\nu(p) = \nu p(1-p)^2$, where $\nu \in [0, 7.2]$ and $p \in [0, 1]$. Figure 11 shows the functional plot for the different parameter values of ν. Taking $\nu = 1, 3, 5$ and 7.2 the orbit of iteration $p_n \in [0, 1]$. But as the value of parameter ν is approached through 7.2 the functional plot of the map approaches outside the closed interval $[0, 1]$ as shown in Figure 11. Further, the Figure 12 shows that the functional plot of the higher order iterations such as $S^3(p)$, $S^2(p)$ and $S(p)$ also lies in $[0, 1]$ for each $\nu \in [0, 7.2]$. But as ν approaches beyond 7.2 the functional plot of higher order tends to $\pm\infty$ as $n \to \infty$ as shown in Figure 13. Moreover, from the bifurcation plot, Figure 14 it is clear that for $\nu > 7.2$ we obtain a compact invariant set $\Lambda_{\alpha,\nu}$ in which the function iteration approaches beyond the closed interval $[0, 1]$, that is, $S^n_{\alpha,\nu}([0, 1]) \supset [0, 1]$. Hence $\Lambda_{\alpha,\nu}$ is hyperbolic set for $\nu > 7.2$.

Remark 5. It is observed that for $\nu \in [0, 7.2]$ the functional iteration $S^n_{\alpha,\nu}([0, 1]) \subset [0, 1]$ and for $\nu > 7.2$, $S^n_{\alpha,\nu}([0, 1]) \supset [0, 1]$. Further, for $\nu > 7.2$, it is also determined that the interval of recursive sequence $S^n_{\alpha,\nu}(p)$ is not same as the interval of an initiator $p \in [0, 1]$ as shown in Figures 11-14.

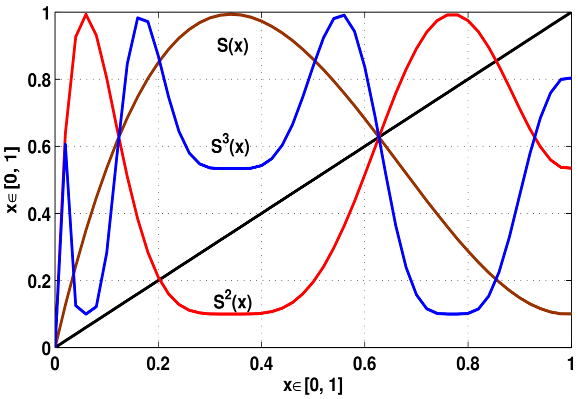


Figure 12 Functional plot $S_{\alpha,\nu}(p)$, $S^2_{\alpha,\nu}(p)$ and $S^3_{\alpha,\nu}(p)$ for $\nu = 7.2$

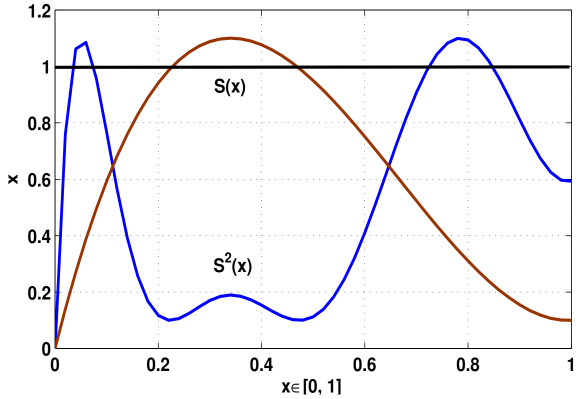


Figure 13 Functional plot $S_{\alpha,\nu}(p)$ and $S^2_{\alpha,\nu}(p)$ for $\nu = 7.2$

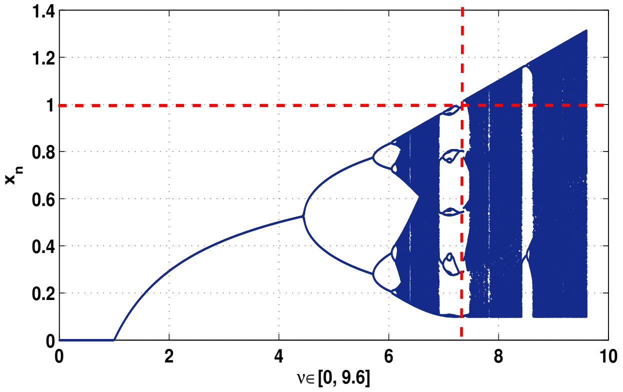


Figure 14 Bifurcation plot for the system $S_{\alpha,\nu}(p)$ for $0 \leq \nu \leq 10$

CONCLUSION

In this article, a two-step superior feedback approach is established to examine the hyperbolicity and the stabilization for one-dimensional chaotic maps. Throughout the study, a few mathematical results are derived and experimental simulations are carried out. Thus, we conclude the following results:

- In Section 3 the superior hyperbolic notions for the chaotic maps are derived using superior system. Definition 1, for the hyperbolic fixed and periodic states is introduced followed by the Example 1 and 2 for the chaotic maps. Further, the numerical simulations are also presented in each case.
- The hyperbolic control results for fixed and periodic state are described. Theorem 1, presents the stability in hyperbolic fixed states and Theorem 2 determines the stability in periodic states.
- In Section 4, the property of hyperbolic set is described using experimental analysis of the quadratic and cubic type maps in superior system. Moreover, it is studied that for the chaotic map $\nu p(1-p)$ the invariant sets $\Lambda_{\alpha,\nu}$ is hyperbolic for $\nu > 4.22$ and for the cubic map $\nu p(1-p)^2$ is hyperbolic for $\nu > 7.2$.

Further, it is emphasized that the hyperbolic property in superior system may lead to a strong interest in nonlinear systems. In the next article, we will present some applications on hyperbolicity.

Acknowledgments

This work was jointly supported by Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia under Grant no. FP-108-42.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Adiyaman, Y., S. Emiroglu, M. Ucar and M. Yildiz, 2020 Dynamical analysis, electronic circuit design and control application of a different chaotic system, Chaos Theory and Applications **02**: 10-16.

Akgul, A., Kaçar, S., Arıcıoğlu, B., and Pehlivan, I., Text encryption by using one-dimensional chaos generators and nonlinear equations. In 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), IEEE 320-323.

Alligood, K. T., T. D. Sauer and J. A. Yorke, 1996 Chaos : An Introduction to Dynamical Systems, Springer Verlag, New York Inc.

Andrecut, M., 1998 Logistic map as a random number generator, International Journal of Modern Physics B **12**: 101-102.

Ashish, J. Cao and R. Chugh, 2018 Chaotic behavior of logistic map in superior orbit and an improved chaos-based traffic control model, Nonlinear Dynamics **94**: 959-975.

Ashish and J. Cao, 2019a A novel fixed point feedback approach studying the dynamcial behaviour of standard logistic map, International Journal of Bifurcation and Chaos **29**: 1950010-16, 16 pages.

Ashish, J. Cao and R. Chugh, 2019b Controlling chaos using superior feedback technique with applications in discrete traffic models, International Journal of Fuzzy System **21**: 1467-1479.

Ashish, J. Cao and R. Chugh, 2021 Discrete chaotification in modulated logistic system, International Journal of Bifurcation and Chaos **31**: 2150065, 14 Pages.

Aulbach, B. and B. Kieninger, 2004 An elementary proof for hyperbolicity and chaos of the logistic maps, Journal of Difference Equations and Applications **10**: 1243-1250.

Ausloos, M. and M. Dirickx, 2006 The Logistic Map and the Route to Chaos : from the Beginnings to Modern Applications, Springer Verlag, New York Inc.

Baptista, M. S., 1998 Logistic map as a random number generator, Physics Letter A **240**: 50-54.

Chugh, R., M. Rani and Ashish, 2012 Logistic map in Noor orbit, Chaos and Complexity Letter **6**, 167-175.

Devaney, R. L., 1948 An Introduction to Chaotic Dynamical Systems, 2nd Edition (Addison-Wesley).

Devaney, R. L., 1992 A First Course in Chaotic Dynamical Systems: Theory and Experiment, (Addison-Wesley).

Glendinning, P., 2001 Hyperbolicity of the invariant set for the logistic map with $\mu > 4$, Nonlinear Analysis **47**: 3323-3332.

Guckenheimer, J., 1979 Sensitive dependence to initial conditions for one-dimensional maps, Communications in Mathematical Physics **70**: 133-160.

Holmgren, R. A., 1994 A First Course in Discrete Dynamical Systems, Springer Verlag, New York Inc.

Jonassen, T. M., 2002 On the Concept of Hyperbolicity, Oslo Univ. College Report Series **21**:, ISBN 82-579-4155-7.

Kraft, R. L., 1999 Chaos, cantor sets and hyperbolicity for the logistic maps, Transactions of the American Mathematical Society **106**: 400-408.

Kumar, V., Khamosh and Ashish, 2020 An empirical approach to study the stability og generalized logistic map in superior orbit, Advances In Mathematics: Scientific Journal **10**: 2094-2109.

Mann, W. R., 1953 Mean value methods in iteration, Proceedings of American Mathematical Society **04**: 506-510.

Martelli, M., 1999 Chaos : An Introduction to Discrete Dynamical Systems and Chaos, Wiley-Interscience Publication, New York Inc.

Melo, W. de. and S. J. van Strien, 1993 One-dimensional dynamics, Springer, Berlin.

Misiurewicz, M., 1976 Absolutely continuous measures for certain maps of an interval, Publications Mathematiques de l'Institut des Hautes Etudes Scientifiques, **261**: 459-475.

Newhouse, S. J., 1981 The abundance of wild hyperbolic set and non-smooth stable sets for diffeomorphism, Publications Mathematiques de l'Institut des Hautes Etudes Scientifiques, **53**: 17-51.

Poincare, H., 1899 Les Methods Nouvells de la Mecanique Leleste, Gauthier Villars, Paris.

Robinson, C., 1995 Dynamical Systems: Stabilily, Symbolic Dynamics, and Chaos, CRC Press.

Saha, L. M., L. Bharti and R. K. Mohanty, 2010 Study of bifurcation and hyperbolicity in discrete dynamical systems, Iranian Journal of Science and Technology, **34**: 1-12.

Saha, L. M., R. K. Mohanty and L. Bharti, 2009 Hyperbolicity and chaos in discrete systems, International Journal of Applied Mathematics and Mechanics, **05**: 48-56.

Sharkovsky, A. N., Y. L. Maistrenko and E. Y. Romanenko, 1993 Difference Equations and Their Applications, Kluwer Academic Publisher.

Volos, C. K., Akgul, A., Pham, V. T., and Baptista, M. S., 2018 Antimonotonicity, crisis and multiple attractors in a simple memristive circuit. Journal of Circuits, Systems and Computers, **27(02)**: 1850026.

Wang, X., Akgul, A., Cicek, S., Pham, V. T., and Hoang, D. V., 2017 A chaotic system with two stable equilibrium points: Dynamics, circuit realization and communication application. International Journal of Bifurcation and Chaos, **27(08)**: 1750130.

How to cite this article: Ashish, Cao, J., Alsaadi, F., and Malik, A. K. Discrete Superior Hyperbolicity in Chaotic Maps. Chaos Theory and Applications, 3(1), 34-42, 2021.