ISSN: 2687 - 4539

CHAOS
THEORY AND APPLICATIONS

IN APPLIED SCIENCES AND ENGINEERING

VOLUME 5, ISSUE 3, NOVEMBER 2023

AN INTERDISCIPLINARY JOURNAL OF NONLINEAR SCIENCE

ISSN: 2687-4539

Chaos Theory and Applications (CHTA)
Volume: 5 – Issue No: 3 (November 2023)
https://dergipark.org.tr/en/pub/chaos/issue/80150

Editorial Board Members

Honorary Editorial Board

Otto E. ROSSLER, University of Tuebingen, GERMANY, oeross00@yahoo.com
Julien C. SPROTT, University of Wisconsin–Madison, USA, csprott@wisc.edu
Guanrong CHEN, City University of Hong Kong, HONG KONG, eegchen@cityu.edu.hk
José A. Tenreiro MACHADO†, Polytechnic Institute of Porto, PORTUGAL, jtm@isep.ipp.pt
Ravi P. AGARWAL, Texas A&M University, USA, Ravi.Agarwal@tamuk.edu

Editor-in-Chief

Akif AKGUL, Hitit University, TURKEY, akifakgul@hitit.edu.tr

Associate Editors

Miguel A. F. SANJUAN, Universidad Rey Juan Carlos, SPAIN, miguel.sanjuan@urjc.es
Chunbiao LI, Nanjing University of Information Science & Technology, CHINA, goontry@126.com
Dumitru BALEANU, Cankaya University, TURKEY, dumitru.baleanu@gmail.com
Yeliz KARACA, University of Massachusetts Chan Medical School, USA, yeliz.karaca@ieee.org
J. M. MUÑOZ PACHECO, Benemérita Universidad Autónoma de Puebla, MEXICO, jesusm.pacheco@correo.buap.mx
Martin BOHNER, Missouri University of Science and Technology, USA, bohner@mst.edu
Nikolay V. KUZNETSOV, Saint Petersburg State University, RUSSIA, n.v.kuznetsov@spbu.ru
Sifeu T. KINGNI, University of Maroua, CAMEROON, stkingni@gmail.com
Fahrettin HORASAN, Kırıkkale University, TURKEY, fhorasan@kku.edu.tr
Vinod PATİDAR, School of Computer Science UPES, INDIA, vinod.patidar@ddn.upes.ac.in
Hijaz AHMAD, International Telematic University, ITALY, hijaz555@gmail.com
Eyyüp Ensari ŞAHİN, Nigde Omer Halisdemir University, TURKEY, ensarisahin@ohu.edu.tr

Editorial Board Members

Jun MA, Lanzhou University of Technology, CHINA, hyperchaos@lut.edu.cn
René LOZI, University Côte D'azur, FRANCE, Rene.LOZI@univ-cotedazur.fr
Herbert Ho-Ching LU, The University of Western Australia, AUSTRALIA, herbert.iu@uwa.edu.au
Praveen AGARWAL, Anand International College of Engineering, INDIA, goyal.praveen2011@gmail.com
Shaher MOMANI, Ajman University, UAE, shahermm@yahoo.com
Edmon PERKINS, North Carolina State University, USA, edmonperkins@gmail.com
Alexander PCHELINTSEV, Tambov State Technical University, RUSSIA, pchelintsev.an@yandex.ru
Yudong ZHANG, University of Leicester, UK, yudongzhang@ieee.org
Wesley Joo-Chen THIO, The Ohio State University, USA, wesley.thio@gmail.com
Yong WANG, Chongqing University of Posts and Telecommunications, CHINA, wangyong_cqupt@163.com
Mustafa Zahid YILDIZ, Sakarya University of Applied Sciences, TURKEY, mustafayildiz@sakarya.edu.tr
Anastasios (Tassos) BOUNTİS, University of Patras, GREECE, anastasios.bountis@nu.edu.kz
Marcelo MESSIAS, São Paulo State University, BRAZIL, marcelo.messias1@unesp.br
Sajad JAFARI, Ton Duc Thang University, VIETNAM, sajadjafari83@gmail.com
Jesús M. SEOANE, Universidad Rey Juan Carlos, SPAIN, jesus.seoane@urjc.es
G. Cigdem YALCIN, Istanbul University, TURKEY, gcyalcin@istanbul.edu.tr
Marcelo A. SAVI, Universidade Federal do Rio de Janeiro, BRAZIL, savi@mecanica.coppe.ufrj.br
Christos K. VOLOS, Aristotle University of Thessaloniki, GREECE, volos@physics.auth.gr
Charalampos (Haris) SKOKOS, University of Cape Town, SOUTH AFRICA, haris.skokos@uct.ac.za
Ihsan PEHLİVAN, Sakarya University of Applied Sciences, TURKEY, ipehlivan@sakarya.edu.tr
Olfa BOUBAKER, University of Carthage, TUNUSIA, olfa_insat@yahoo.com
Karthiekeyan RAJAGOPAL, Defence University, ETHIOPIA, rkarthiekeyan@gmail.com
Binoy Krishna ROY, National Institute of Technology Silchar, INDIA, bkr_nits@yahoo.co.in
Jacques KENGNE, Université de Dschang, CAMEROON, kengnemozart@yahoo.fr
Fatih KURUGOLLU, University of Sharjah, UAE, fkurugollu@sharjah.ac.ae
Denis BUTUSOV, Petersburg State Electrotechnical University, RUSSIA, butusovdn@mail.ru
Iqtadar HUSSAIN, Qatar University, QATAR, iqtadarqau@qu.edu.qa
Sundarapandian VAIDYANATHAN, Vel Tech - Technical University, INDIA, sundarvtu@gmail.com
Irene M. MOROZ, University of Oxford, UK, Irene.Moroz@maths.ox.ac.uk
Serdar CICEK, Tarsus University, TURKEY, serdarcicek@gmail.com
Zhouchao WEI, China University of Geosciences, CHINA, weizhouchao@163.com
Qiang LAI, East China Jiaotong University, CHINA, laiqiang87@126.com
Viet-thanh PHAM, Phenikaa University, VIETNAM, pvt3010@gmail.com
Günyaz ABLAY, Abdullah Gul University, TURKEY, gunyaz.ablay@agu.edu.tr
Jay Prakash SINGH, Rewa Engineering College, INDIA, jp4ssm@gmail.com

Yılmaz UYAROĞLU, Sakarya University, TURKEY, uyaroglu@sakarya.edu.tr
Shaobo HE, Central South University, CHINA, heshaobo_123@163.com
Esteban Tlelo CUAUTLE, Instituto Nacional de Astrofísica, MEXICO, etlelo@inaoep.mx
Dan-gheorghe DIMITRIU, Alexandru Ioan Cuza University of Iasi, ROMANIA, dimitriu@uaic.ro
Jawad AHMAD, Edinburgh Napier University, UK, jawad.saj@gmail.com
Metin VARAN, Sakarya University of Applied Sciences, TURKEY, mvaran@sakarya.edu.tr
Ashish ASHISH, Government College Satnali, INDIA, drashishkumar108@gmail.com
Murat TUNA, Kırklareli University, TURKEY, murat.tuna@klu.edu.tr
Orhan Ozgur AYBAR, Piri Reis University, TURKEY, oaybar@pirireis.edu.tr
Mehmet YAVUZ, Necmettin Erbakan University, TURKEY, mehmetyavuz@erbakan.edu.tr

Editorial Advisory Board Members

Ayhan ISTANBULLU, Balıkesir University, TURKEY, ayhanistan@yahoo.com
Ismail KOYUNCU, Afyon Kocatepe University, TURKEY, ismailkoyuncu@aku.edu.tr
Fatih OZKAYNAK, Firat University, TURKEY, ozkaynak@firat.edu.tr
Sezgin KACAR, Sakarya University of Applied Sciences, TURKEY, skacar@subu.edu.tr
Ugur Erkin KOCAMAZ, Bursa Uludag University, TURKEY, ugurkocamaz@gmail.com
Erdinc AVAROGLU, Mersin University, TURKEY, eavaroglu@mersin.edu.tr
Ali DURDU, Social Sciences University of Ankara, TURKEY, ali.durdu@asbu.edu.tr
Hakan KOR, Hitit University, TURKEY, hakankor@hitit.edu.tr

Language Editors

Muhammed Maruf OZTURK, Suleyman Demirel University, TURKEY, muhammedozturk@sdu.edu.tr
Mustafa KUTLU, Sakarya University of Applied Sciences, TURKEY, mkutlu@subu.edu.tr
Hamid ASADİ DERESHGİ, Istanbul Arel University, TURKEY, hamidasadi@arel.edu.tr
Emir AVCIOGLU, Hitit University, TURKEY, emiravciogluhitit.edu.tr

Managing Editor

Akif AKGUL, Hitit University, TURKEY, akifakgul@hitit.edu.tr

Technical Coordinator

Muhammed Ali PALA, Sakarya University of Applied Sciences, TURKEY, pala@subu.edu.tr
Murat Erhan CIMEN, Sakarya University of Applied Sciences, TURKEY, muratcimen@sakarya.edu.tr
Harun Emre KIRAN, Hitit University, TURKEY, harunemrekiran@hitit.edu.tr
Berkay EMİN, Hitit University, TURKEY, berkayeminn@gmail.com

ISSN: 2687-4539

Chaos Theory and Applications (CHTA)

Volume: 5 – Issue No: 3 (November 2023)
https://dergipark.org.tr/en/pub/chaos/issue/80150

Contents:

Are Chaotic Attractors just a Mathematical Curiosity or Do They Contribute to the Advancement of Science? (Editorial) 133-140
René LOZI

Estimating Optimal Synchronization Parameters for Coherent Chaotic Communication Systems in Noisy Conditions (Research Article) 141-152
Vyacheslav RYBİN, Ivan BABKİN, Dmitriy KVİTKO, Timur KARİMOV, Lucas NARDO, Erivelton NEPOMUCENO, Denis BUTUSOV

Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System (Research Article) 153-159
Berkay EMİN, Zabit MUSAYEV

A New Secure Communications Scheme Based on a Synchronisation of Hybrid Chaotic System (Research Article) 160-166
Manal MESSADİ, Karim KEMİH, Hamid HAMİCHE

A Secure Communication System of Synchronized Chua's Circuits in LC Parallel Coupling (Research Article) 167-177
Satya Prakash V, Narender Reddy S, Sadanandachary A

Lossless Image Encryption using Robust Chaos-based Dynamic DNA Coding, XORing and Complementing (Research Article) 178-187
Vinod PATİDAR, Gurpreet KAUR

Anomaly Detection in Cyber Security with Graph-Based LSTM in Log Analysis (Research Article) 188-197
Yusuf ALACA, Yuksel CELIK, Sanjay GOEL

A New Fractional-order Derivative-based Nonlinear Anisotropic Diffusion Model for Biomedical Imaging (Research Article) 198-206
Alka CHAUHAN, Santosh KUMAR, Yeliz KARACA

Analyzing Predator-Prey Interaction in Chaotic and Bifurcating Environments (Research Article) 207-218
Ansar ABBAS, Abdul KHALİQ

Analyses of Reconfigurable Chaotic Systems and their Cryptographic S-box Design Applications (Research Article) 219-232
Mangal Deep GUPTA, Rajeev Kumar CHAUHAN, Vipin Kumar UPADDHYAY

Chaos and Control of COVID-19 Dynamical System (Research Article) 233-241
Vivek MİSHRA, Sarit MAİTRA, Mihir DASH, Saurabh Kumar AGRAWAL, Praveen AGARWAL

Time-Varying Fractal Analysis of Exchange Rates (Research Article) 242-255
Baki ÜNAL

Analysis of Nonlinear Mathematical Model of COVID-19 via Fractional-Order Piecewise Derivative (Erratum) 256
Muhammad SİNAN, Kamal SHAH, Thabet ABDELJAWAD, Ali AKGUL

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
EDITORIAL
Vol.5 / No.3 / 2023 / pp.133-140

Are Chaotic Attractors just a Mathematical Curiosity or Do They Contribute to the Advancement of Science?

René Lozi[*,1]
[*]LJAD, CNRS, Université Côte d'Azur, F-06000 Nice, France.

ABSTRACT Since the seminal work of Henri Poincaré on the three-body problem, and more recent research dating back to the second half of the 20th century on chaotic dynamical systems, many applications have emerged in different domains (economics, electronic, cryptography, physics, etc). We try to describe the evolution of the last 50 years on the subject and to find out whether applications have compromised the purity and beauty of theoretical research.

KEYWORDS
Chaotic attractors
Optimization
Cryptography
Memristor
Economy

INTRODUCTION

Since the very beginning of their appearance in the history of humanity, research in mathematics has been guided by two different currents: theory and applications or in other words by beauty and utility. Around 5,000 years ago people in the Mesopotamia and Egypt began using arithmetic, algebra and geometry for commerce, trade, taxation and social activities. Later, in the 6th century BC, Greeks introduced mathematics as a "demonstrative discipline" (Heath 1931) (see (Høyrup J. 2011) for comparison between both approaches). This double current of research still functions today in competition-cooperation mode.

I had the immense privilege of being student of Jean Alexandre Dieudonné, one of the founding members of the Bourbaki group. For him, the only need to research mathematics for humanity was "for the honor of the human spirit" (as the great mathematician Karl Gustav Jacobi 1804-1851 said before him).

As a young student, I was imbued with this idea, but I was also attracted by research in physics and ultimately my university career was that of professor of numerical analysis. The subject of my doctoral thesis concerned the numerical analysis of bifurcations, which quickly led me to study chaotic dynamic systems from both aspects: theory and application. I was fortunate to see the birth of a new field of research in mathematics in the mid-1970s, that of chaotic attractors. I had the privilege of inventing one that, surprisingly, is still the subject of intensive research 50 years later. This is the reason why I often ask myself the question of the place of these attractors not only in mathematics, but also for the advancement of science.

It is widely accepted that the beginning of modern research on nonlinear dynamical systems is due to the initial work of Henri Poincaré on the three-body problem. Even if a real astronomical problem (will the Earth continue to orbit around the sun forever?) is at the origin of his reflection, no practical application of his "Méthodes nouvelles de la mécanique céleste" has guided his mind.

The "butterfly effect" reveled by Edward Lorenz in 1963 (Lorenz, E. N. 1963) and the "sexier" word "chaos" coined by James A. Yorke in 1975 (Li, T. Y. and Yorke, J. A. 1975) have brought global awareness of these concepts often not actually understood by the public. However, it is only at the beginning of 90′ that the applications of chaotic properties of dynamical systems were introduced with the pioneering idea of synchronization of two chaotic attractors of Louis M. Pecora and Thomas L. Carroll (Pecora, L. M. and Carroll, T. L. 1990). Such concept was soon used (and improved) to transmit encrypted messages.

Since then, many applications have emerged in electronics (Chua circuit and memristors), optimization for meta-heuristic algorithms (particle swarm optimization (PSO), differential evolution (DE), Self-Organizing Migrating Algorithm (SOMA),...), cryptography based chaos, generation of pseudo-random number, economy, etc.

Manuscript received: 28 September 2023,
Accepted: 28 September 2023.

---

[1] Rene.LOZI@univ-cotedazur.fr (**Corresponding author**)

Have these applications compromised the purity and beauty of theoretical research? We attempt to describe the evolution of the last 50 years on the subject from the perspective of this question.

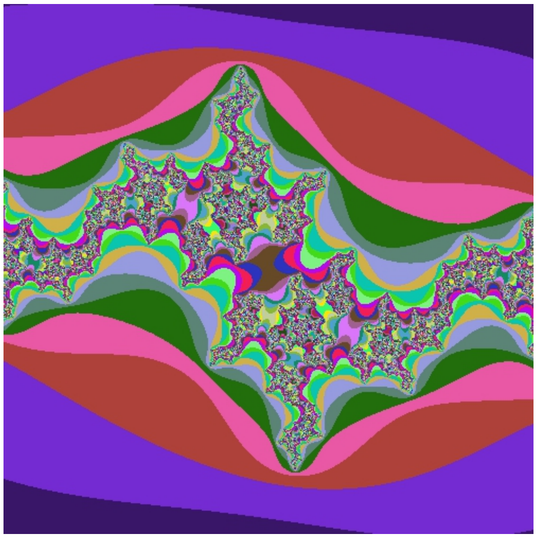


Figure 1 Example of Julia set.

THE DAWN OF CHAOTIC DYNAMICAL SYSTEMS

The study of the frighteningly complicated solutions discovered by Poincaré continued quietly for almost 80 years in several directions including conservative and dissipative dynamical systems, differential equations and difference equations. We can cite among many, the pioneer works of Pierre Fatou (1878-1929) and Gaston Julia (1893-1978) related to one-dimensional maps with a complex variable (see Figure 1), near a century ago; those of Cristian Mira and Igor Gumowski, who began their mathematical research in 1958 (the Gumowski-Mira map (1), see Figure 2), the fractals introduced in 1967 by Benoît Mandelbrot (1924-2010) (Mandelbrot 1967), and of course the continuous attractors of Lorenz (1963) (2) (Figure 3) and Rössler (1976) (Rössler 1976) (Rössler 2020), (3) (Figure 4); and the discrete attractors of Hénon (1976), Belykh (1976) (Belykh, V. N. *et al.* 2023) and Lozi (1977), among many others.

$$\begin{cases} x_{n+1} = f(x_n) + by_n \quad with \quad f(x_n) = ax + 2(1-a)\frac{x^2}{1+x^2}, \\ y_{n+1} = f(x_{n+1}) - x_n. \end{cases} \tag{1}$$

$$\begin{cases} \dot{x} = \sigma(y-x), \\ \dot{y} = rx - y - xz, \\ \dot{z} = xy - bz. \end{cases} \tag{2}$$

$$\begin{cases} \dot{x}_1 = -x_2 - x_3, \\ \dot{x}_2 = x_1 + ax_2, \\ \dot{x}_3 = b + x_3(x_1 - c). \end{cases} \tag{3}$$

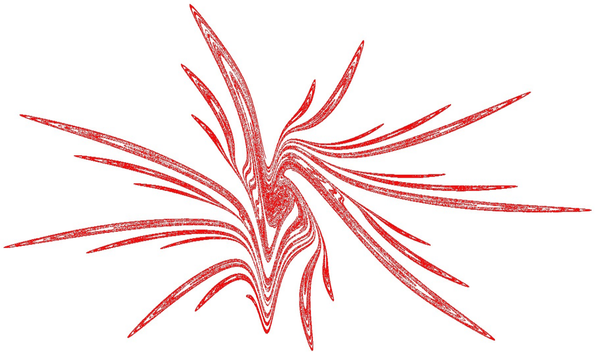


Figure 2 Gumowski-Mira attractor for $a = 0.93333$, $b = 0.92768$.

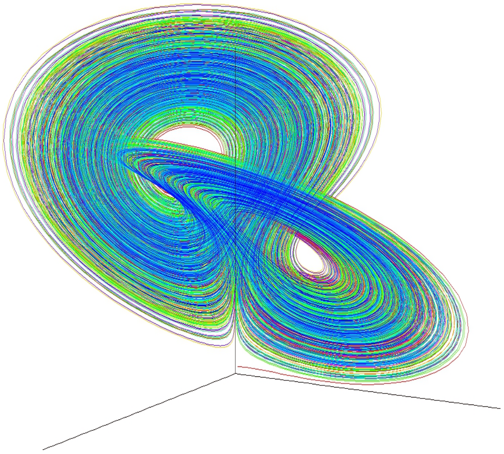


Figure 3 Lorenz attractor for $\sigma = 10$, $b = 8/3$ and $r = 27$.

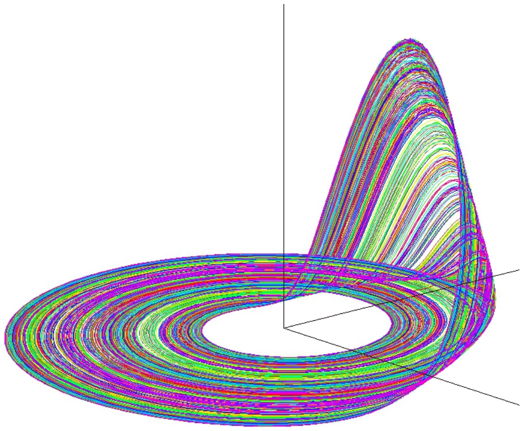


Figure 4 Rössler attractor for $a = 0.2$, $b = 0.2$ and $c = 5.7$.

The images produced by these fractal sets 40 years ago, astonished not only mathematicians accustomed to geometric figures drawn only with rulers and compas, but also the general public. Heinz-Otto Peitgen published a book containing dozens of figures generated by complex dynamic systems, coining the name "computer art" (Peitgen, H.-O. and Richter, P. H. 2011). Today, no one is surprised by the use of chaotic systems in cinema or advertising.

FIRST APPLICATIONS OF CHAOTIC DYNAMICAL SYSTEMS

Electric circuits

In Japan the Hayashi's School (with disciples like Ikeda, Ueda and Kawakami) in the same period, were motivated by simulation of chaotic dynamics by electric and electronic circuits. Chaotic mappings were used as models of behavior of electric circuits (the Ikeda map (4), see Figure 5).

$$\begin{cases} x_{n+1} = 1 + u(x_n cos(t_n) - y_n sin(t_n)) \quad with \quad t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}, \\ y_{n+1} = u(x_n sin(t_n) + y_n cos(t_n)). \end{cases} \tag{4}$$

In 1983, Leon Chua invented a very simple electric circuit producing chaos (5). The advantage of this circuit (see Figure 6 a)) was that the variables of the mathematical equations corresponded to voltage and current and could be viewed on the screen of an oscilloscope (see Figure 6 (b)).

$$\begin{cases} \dot{x} = \alpha(y - \Phi(x)), \\ \dot{y}_2 = x - y + z, \\ \dot{x}_3 = -\beta y. \end{cases} \tag{5}$$

with $\Phi(x) = m_1 x + \frac{1}{2}(m_0 - m_1)\left[|x+1| - |x-1|\right]$.

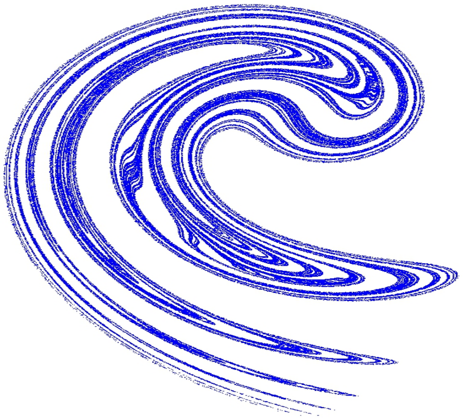
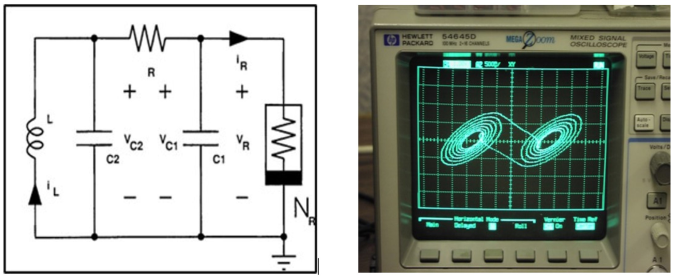


Figure 5 Ikeda attractor for $u = 0.9$.

Before 1990 computers were not as efficient as they are today. It is why many experimenters still used analog electrical systems to explore the behavior of chaotic maps. Rodriguez-Vasquez et al. (Rodriguez-Vazquez, A. *et al.* 1987) in 1987 presented a special-purpose analog computer made of switched-capacitor circuit for analyzing chaos and bifurcation phenomena in nonlinear discrete dynamical systems modeled by discrete maps. They published results for four maps: the logistic map, a piece-wise linear map, the Hénon map and the Lozi map (6). For this last map, they built a rather complicated circuit realization (see Figure 25 of (Rodriguez-Vazquez, A. *et al.* 1987)) and compared the attractor measured from this circuit with the corresponding numerical simulation and found good agreement between them. Even if this example is not strictly speaking an application of the Lozi map for electric purposes, it constitutes one of the first examples of solid realization. However, these works cannot be considered as real applications.



(a)

(b)

Figure 6 (a) Chua circuit. (b) Chua attractor on oscilloscope.

$$\mathcal{L}_{a,b}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 - a|x| + y, \\ bx. \end{pmatrix} \tag{6}$$

Secure communications

It was the discovery of the synchronization of chaotic electrical circuits by Pecora and Carroll (Pecora, L. M. and Carroll, T. L. 1990) in 1990 that sparked research into secure communications.

A first reported experimental secure communication system via chaotic synchronization using two Chua's circuits (one as master and one as slave) was built two years after. However, the signal recovered from this system which used the Chua circuit, contained some inevitable noise that degraded the fidelity of the original message. The system was soon improved in 1993, by cascading the output of the receiver in the original system, into an identical copy of this receiver (Lozi, R. and Chua, L. O. 1993) (see Figure 7). This cascading process was extended to multiple copies and analyzed using filtering theory (Lozi, R. 1995) in the case of a multi-tone signal.

In 2000, Dmitriev et al. (Dmitriev, A .S. *et al.* 2000) discussed a principle of multiple access, in satellite communication systems or cellular telephony based on fine structure of chaotic attractors, using control of special chaotic trajectories. They demonstrated the experimental verification of the proposed approach for asynchronous packet data transmission. In their approach they considered that a chaotic attractor can be treated as a number of countable sets of special trajectories: unstable periodic orbits (UPO) and transitions between these orbits. Instability of the periodic orbits and transient trajectories between them gives rise to irregular chaotic behavior. They used the set of the unstable

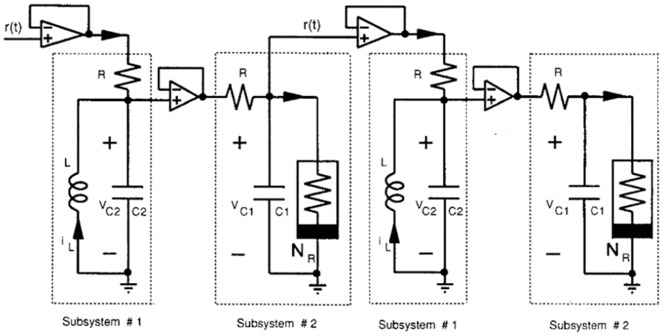


Figure 7 Cascade of Chua circuits.

"skeleton" periodic trajectories, constituting the structure of the strange attractor (or a part of this set), as a "reservoir" of potential codes for multi-user communication systems. They observed that the multitude of the codes from a certain "reservoir" for communications is practically infinite, i.e., the number of users provided with individual code sets is unlimited.

As an example of the realization of their method, they considered twenty period-16 (UPO) of the Lozi map (6) for $a = 1.7$ and $b = 0.5$. They displayed the switching between them in the Figure 2 of (Dmitriev, A .S. *et al.* 2000) and showed from this diagram that the forming of all successive cycles (10-times repeating) is practically instantaneous. Improving their initial method, they remarked that unstable periodic orbits can be utilized for not only encoding the entire transmitted information, but also for attributing it to this or that group of users, i.e., they play the role of "chaotic markers". The idea to use the system of unstable periodic orbits as markers was applied to the problem of asynchronous packet transmission of data from several users through a single common communication channel. They concluded that the generating and controlling of UPO may be realized in rather high frequency band, provided in by modern digital methods.

Memristors

In 1971, L.O. Chua predicted the existence of a missing fourth passive circuit element, in addition to the three classical ones: resistor, inductor and capacitor (Chua 1971). He called this new element "memristor" meaning it is a resistor with memory. It is characterized by a nonlinear constitutive relationship between the charge q and the flux φ. Such a physical device would not be reported until 2008, when a physical model of a two-terminal *hp* device behaving like a memristor was announced (Strukov, D. B. *et al.* 2008) sparkling intense research with thousands of papers published to date. A general Ohm's law for theorizing this device was published ten years ago (Abdelouahab, M.- S. *et al.* 2008).

Nowadays, discrete memristor model is known as a research hotspot. Many researchers have devoted themselves to the analysis of chaotic phenomena in discrete memristors. Recently, hidden attractors have also been discovered in some discrete memristors based maps (Zhang, L. P. *et al.* 2022). Wang et al. (Wang, J. *et al.* 2022) included a discrete-time memristor to create a memristive Lozi map. This new 3-D memristor-based Lozi map was established by coupling a discrete memristor to the original 2-D Lozi map (6).

$$\begin{cases} x_{n+1} = 1 - a\,|x_n| + y_n, \\ y_{n+1} = bx_n + ky_n sin(z_n), \\ z_{n+1} = y_n + z_n, \end{cases} \tag{7}$$

where k is a real valued control parameter coupling gain between the discrete-time memristor and the Lozi map. Since there are no fixed points but hyperchaos can emerge, the memristor-based Lozi map is a hidden hyperchaotic map.

For some specific control parameters, the 3-D memristor-based Lozi map can show heterogeneous and homogeneous hidden multistability. It should be noted that heterogeneous hidden multistability implies the coexisting behavior of multiple hidden attractors of different stability types, while homogeneous hidden multistability indicates the coexisting behavior of multiple hidden attractors of the same stability type but only in different dynamic intervals. In addition to the coexistence of these heterogeneous hidden attractors, the memristor-based Lozi map is very likely to produce the coexistence of homogeneous hidden hyperchaotic attractors, i.e., homogeneous hidden multistability. Therefore, the homogeneous hidden hyperchaotic attractors from the 3-D memristor based Lozi map can be robustly controlled by the memristor's initial conditions.

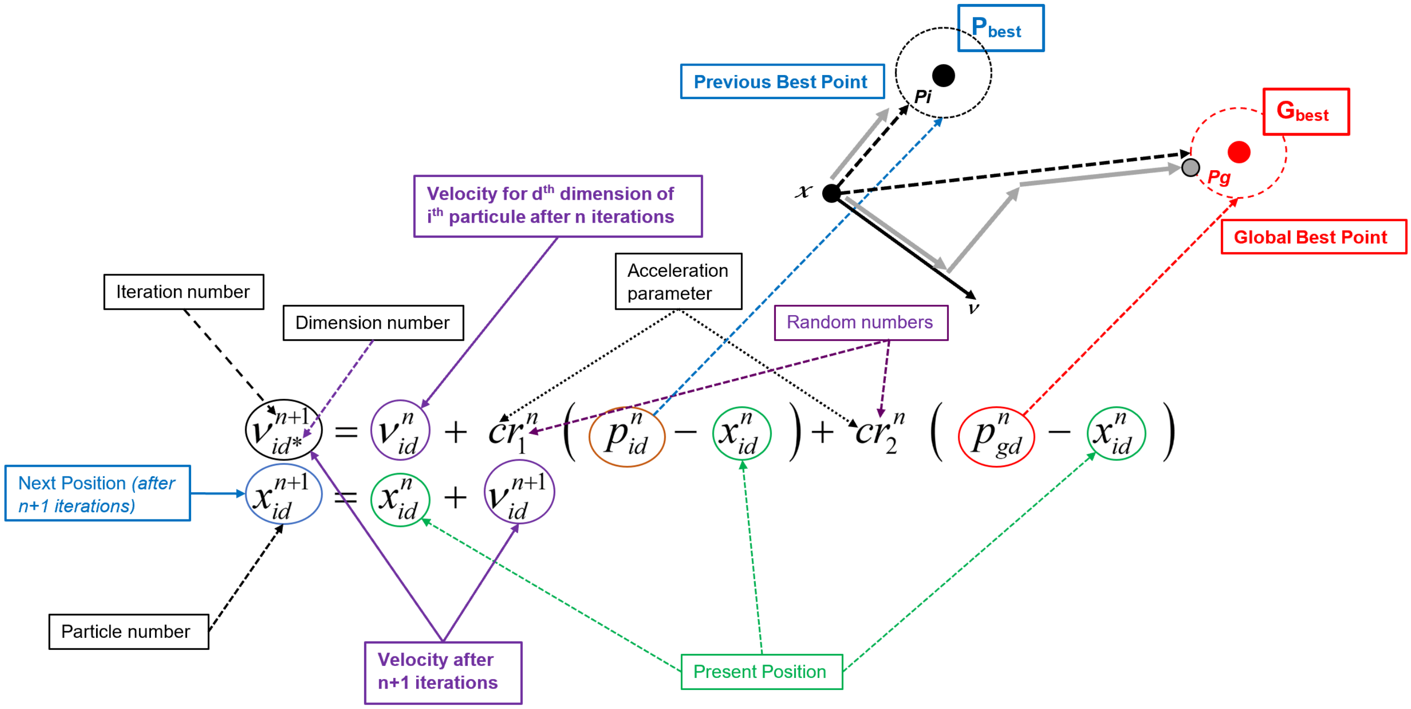
Additionally, Wang et al. implemented this memristor in a digital circuit based on a high-performance micro-controller. They physically obtained an image of the hyperchaotic hidden attractors using a digital oscilloscope. Eventually, a digital platform was exploited, and its experimental phase portraits were obtained to confirm the numerical portraits.

APPLICATIONS IN OTHER DOMAINS

Optimization

Most engineering problems can be defined as optimization problems, e.g. the finding of an optimal trajectory for a robot arm, the optimal thickness of steel in pressure vessels, the optimal set of parameters for controllers, optimal relations or fuzzy sets in fuzzy models, etc. Solutions to such problems are usually difficult to find their parameters which usually include variables of different types, such as floating point or integer variables.

Applications of chaotic maps in the now flourishing field of optimization took longer to appear than applications in electrical devices. The main reason comes from a paradigm shift in optimization algorithms: instead of using deterministic algorithms like gradient method or the steepest descent which are not efficient in high-dimensional problems optimization involving hundred or thousand of variables, heuristic algorithms based on an imitation of Darwin's theory of the evolution of species, were introduced a few decades ago. Such algorithms require easy access to random or chaotic numbers. This is why interest has only recently focused on chaotic attractors. It took three decades for this paradigm shift in the study of the chaotic maps (logistic, symmetric tent, Belykh, Hénon, Lozi, etc.). Instead of focusing on the theoretical study of their mathematical properties or on finding generalizations, Araujo and Coelho (Araujo and Coelho 2008) used them as a core for particle swarm optimization (PSO) (see Figure 8).



Pbest
Previous Best Point
Pi
Gbest
Pg
Global Best Point
x
v
Velocity for dth dimension of ith particule after n iterations
Acceleration parameter
Iteration number
Dimension number
Random numbers
$v_{id^*}^{n+1} = v_{id}^{n} + cr_1^n\left(p_{id}^n - x_{id}^n\right) + cr_2^n\left(p_{gd}^n - x_{id}^n\right)$
$x_{id}^{n+1} = x_{id}^{n} + v_{id}^{n+1}$
Next Position (after n+1 iterations)
Particle number
Velocity after n+1 iterations
Present Position

Figure 8 Geometric core of Particle Swarm Optimization (PSO) algorithm.

Optimization algorithms based on the chaos theory are methodologies for searching optimal solutions that differ from any of the existing traditional stochastic optimization techniques. Due to the wandering of chaos, it can carry out overall searches in the solution space at higher velocities when compared to stochastic ergodic searches, which has its computing based on probabilities. This remark has been done in the pioneering work of Caponetto et al. (Caponetto, R. *et al.* 2003), who, four years before Araujo and Coelho found that chaotic sequences improved the performance of evolutionary algorithms.

PSO method was used for many purpose like the control of the thermal-vacuum system used at the Brazilian National Institute for Space Research (INPE). The original controller was designed to control the temperature on the shroud (set of pipes) of a chamber where satellites are tested (Marinke, R. *et al.* 2005). This method was used by Pluhacek et al. (Pluhacek, M. *et al.* 2012) who considered a Partial-Integral-Derivative (PID) controller for a Direct-Current (DC) motor system in order to obtain optimal settings. A DC motor is any of a class of rotary electrical motors that converts direct current electrical energy into mechanical energy. Proportional-Integral-Derivative (PID) control is the most common control algorithm used in industry and has been universally accepted in industrial control.

The optimization process involving PSO algorithm was applied to minimize errors of the output transfer function that can indicate the quality of regulation of such controller.

Another evolutionary optimization algorithm called Differential Evolution (DE) was used by Davendra et al. (Davendra, D. *et al.* 2010) in the same goal, and by Senkerik et al. (Senkerik, R. *et al.* 2013) in the task of optimization of batch chemical reactor geometry.

In 2004, Zelinka in (Zelinka, I. 2004), introduced SOMA (Self-Organizing Migrating Algorithm), a new class of stochastic optimization algorithms. Evolutionary algorithms work on populations of candidate solutions that are evolved in generations (two parents create one new individual – the offspring) in which only the best-suited – or fittest – individuals are likely to survive. Instead SOMA which can also works on a population of individuals, is based on the self-organizing behavior of groups of individuals in a "social environment", e.g. a herd of animals looking for food.

A group of animals such as wolves or other predators may be a good example. If they are looking for food, they usually cooperate and compete so that if one member of the group is successful (it has found some food or shelter) then the other animals of the group change their trajectories towards the most successful member. If a member of this group is more successful than the previous best one (is has found more food, etc.) then again all members change their trajectories towards the new successful member. It is repeated until all members meet around one food source. This principle from the real world is of course strongly simplified. Yet even so, it can be said it is that competitive-cooperative behavior of intelligent agents that allows SOMA to carry out very successful searches.

Recently Zelinka et al. used SOMA (Zelinka, I. *et al.* 2023) for the design of quantum computing circuits for the future quantum computers.

Of course, we cannot present, within the limited extend of this editorial, all the dozens of algorithms using chaotic attractors (see (Lozi, R. 2023) for a survey).

Cryptography

Cryptography is the primary means of protecting communications in the cyber world in which mankind lives today. Modern technologies involve fast communication links between potentially billions of devices via complex networks (satellite, mobile phone, Internet, etc.). The primary concern posed by these complex and tangled networks is their protection against passive and active attacks that could compromise public safety and privacy. Cryptography has been around for over two thousand years with the famous Caesar code used by Emperor Julius Caesar. Today, the properties of chaotic attractors are recognized as being the basis of part of the methods of cryptography.

Among many algorithms based on chaotic dynamical systems, we can mention the image encryption algorithms, like the optical color image encryption scheme based on fingerprint key and three-step phase-shifting digital holography which was proposed by Su et al. (Su, Y. *et al.* 2021). In this scheme the fingerprint is served as secret key directly. The random phase masks generated from the fingerprint using secure hash algorithm (SHA-256) and the chaotic Lozi map are just used as interim variables. The fingerprint is served as secret key directly. With the help of the fingerprint-based random phase masks located in the linear canonical transform domain and the three-step phase-shifting digital holography, the primary color image that is hidden into a grey-scale carrier image can be encrypted into three noise-like holograms. In addition, the parameters of the chaotic Lozi map and linear canonical transform can also provide additional security to the proposed encryption scheme. Other examples of cryptography-based chaos can be found in (El Assad, S. *et al.* 2022).

Economy

Since twenty years, one can find application of chaotic dynamical systems in economy. For example Tang et al. (Tang, T. W. *et al.* 2004) carried out an analysis of Parrondo's games with different chaotic switching strategies. The performance of Parrondo's games was compared with random and periodic switching strategies. The main idea of Parrondo's paradox, exposed in 1996, is that two individually losing games can be combined to win via deterministic or non-deterministic mixing of games (Harmer, G. P. *et al.* 2001). In (Tang, T. W. *et al.* 2004) a fair way to compare random and chaotic Parrondo's games was generalized. The logistic, tent, sinusoidal and Gaussian 1-D maps were considered together with Hénon and Lozi maps.

To play chaotic Parrondo's games, one of these chaotic generator being chosen, we consider a sequence that it generates from an initial value. Then every n-th iterate of such sequence determines whether Game A or B is played. Of course the outcomes of Parrondo's game are affected by the different switching strategies applied and the initial value chosen. The proportion of Game A and B played is equal for all switching strategies for a fair comparison. In conclusion, the authors found that chaotic Parondo's games can give a higher rate of winning compared to random switching strategies. This result recalls the remark made by Caponetto et al. (Caponetto, R. *et al.* 2003) that chaotic sequences can improve the performance of evolutionary algorithms versus random sequences.

Another examples can be found in (Commendatore, P. *et al.* 2015) in which Commendatore et al. proposed a new economic geography model which describes spatial distribution of industrial activity in the long run across three identical regions depending on the balancing of agglomeration and dispersion forces. It is defined by a two-dimensional piecewise smooth map depending on four parameters. They discussed the emergence of the Wada basins of coexisting attractors leading to the so-called final state sensitivity (see Figure 9). And also, in (Sushko, I. *et al.* 2023, in progress) in which Sushko et al. studied the dynamics of a financial market model with trend-followers and contrarians proposed a 2D-piecewise linear discontinuous map F given by (8) (see Figure 10).

$$\begin{cases} x_{n+1} = (1-k_1-b)\,x_n + k_1 x_{n-1} \quad if\, |x_n - x_{n-1}| < k, \\ x_{n+1} = (1-k_2-b)\,x_n + k_2 x_{n-1} + m \quad if\, |x_n - x_{n-1}| > k. \end{cases} \tag{8}$$

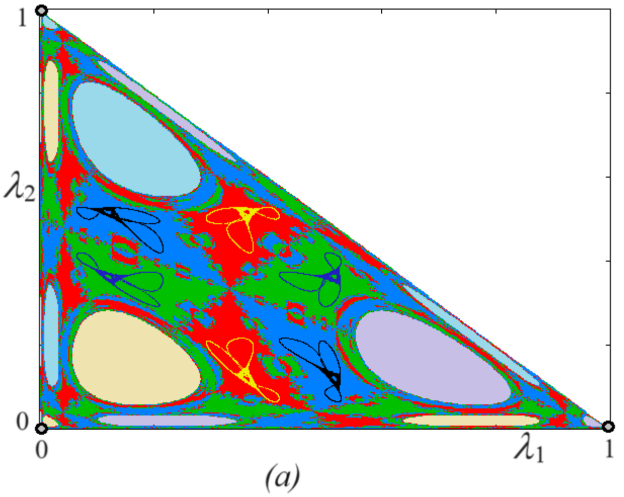


Figure 9 2D piecewise smooth map G governing dynamics of a three region New Economic Geography model. Basins of attraction of the fixed points $(0,0)$, $(1,0)$, $(0,1)$ (attracting in Milnor sense) and of the three 2-piece chaotic attractors.

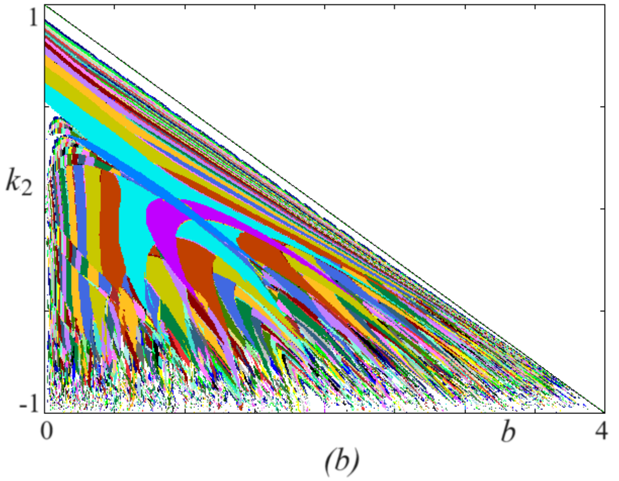


Figure 10 Periodicity regions (where different colors are related to attracting cycles of different periods) in the $(b;k2)$-parameter plane for $k1 = -1$, $m = 1.9$, $k = 0.1$.

THEORETICAL RESULTS

We have shown that chaotic attractors have been used for more than thirty years for applications in different fields. This does not mean that they did not advance pure mathematics.

It is difficult to list all the improvements in chaotic dynamical systems theory and bifurcation theory, so many have been made over the last half century. We can only name a few, such as the concepts of Smale'Axiom A and horseshoe, homoclinic bifurcation and Shilnikov attractors, border-collision bifurcation, ergodicity, hyperbolicity, symbolic dynamics and kneading sequences, Sinai-Bowen-Ruelle measures, fractal dimensions, general usage of fractional derivatives, fractional maps, topological entropy, etc.

I think the best example of a theory-practice-theory approach is that of chimeras. Following the discovery of the synchronized chaotic attractors (theory), research focused on network of attractors with several topologies for multiple purposes like the creation of Pseudo Random Number Generation for cryptography (Garasym, O. *et al.* 2017) (practice).

Describing the dynamical properties of synchronization of such networks, special solutions called "chimeras" and "solitary states" were highlighted (theory).

Rybalova et al. (Rybalova, E. *et al.* 2018) considered a complex system consisting of three coupled rings of nonlocally coupled chaotic maps. This multilayer network is described by the following equations:

$$\begin{cases} x^i_{n+1} = f(x^i_n, y^i_n) + \frac{\sigma_1}{2P}\sum_{j=i-P}^{j=i+P}\left[f(x^j_n, y^j_n) - f(x^i_n, y^i_n)\right] + \gamma_1 F^i_n, \\ y^i_{n+1} = b x^i_n, \\ u^i_{n+1} = f(u^i_n, v^i_n) + \frac{\sigma_2}{2R}\sum_{j=i-R}^{j=i+R}\left[f(u^j_n, v^j_n) - f(u^i_n, v^i_n)\right] + \gamma_2 G^i_n, \\ v^i_{n+1} = b x^i_n, \\ z^i_{n+1} = f(z^i_n, s^i_n) + \frac{\sigma_3}{2T}\sum_{j=i-T}^{j=i+T}\left[f(z^j_n, s^j_n) - f(z^i_n, s^i_n)\right] + \gamma_3 H^i_n, \\ s^i_{n+1} = b x^i_n, \end{cases} \tag{9}$$

The first system of equations in (9) specifies a ring network of nonlocally coupled Hénon maps with f defined by (10)

$$f(x_n, y_n) = 1 - a x_n^2 + y_n, \tag{10}$$

with $a = 1.4$, $b = 0.3$, $\sigma_1 = 0.72$ and and $P = 320$. The second pair of equations corresponds to the ring of nonlocally coupled Lozi maps with f defined by (11)

$$f(x_n, y_n) = 1 - a\,|x_n| + y_n, \tag{11}$$

and is analyzed for $a = 1.4$, $b = 0.3$, $\sigma_2 = 0.206$ and $R = 180$. The third pair of equations also determines the ring of nonlocally coupled Hénon maps with $a = 1.4$, $b = 0.3$, $\sigma_1 = 0.295$ and $T = 320$.

The first two rings are coupled inertially via the coupling functions $F^i_n = -G^i_n = u^i_n - x^i_n$ with the coupling coefficients γ_1 and γ_2. The third ring nodes is connected unidirectionally with the first ring units by the coupling term $\gamma_3 H^i_n$ where

$$H^i_n = f(x^i_n, y^i_n) - f(z^i_n, s^i_n), \tag{12}$$

defines the diffusive coupling with the coupling coefficient γ_3. N is the number of elements in the ensemble of coupled equations in each ring. The coupling parameters $\sigma_{1,2,3}$ characterize the coupling strength, and $2P, 2R, 2T$ are the number of neighbors on each ring (P (resp. R, T) neighbors on the either side of the ith element). The initial conditions are chosen to be randomly distributed in the interval $[-0.5, 0]$ for all the variables of the network (9).

Using numerical simulation they have demonstrated that the network of two symmetrically coupled ensembles of Hénon and Lozi maps can show a novel type of chimera state, a solitary state chimera (SSC), when the coupling between them is weak. This special structure emerges in the case if the Lozi ensemble exhibits a developed regime of solitary states. The SSC is fairly stable and is observed within a finite range of parameter variation. If the two layer network of nonlocally coupled Hénon and Lozi maps in the solitary state chimera is unidirectionally coupled to the third ring of nonlocally coupled Hénon maps, then the effect of external synchronization can be observed in a finite range of the coupling coefficient γ_3.

CONCLUSION

The first research on chaotic dynamic systems marked the mind of the public by the beauty of the images that these attractors made it possible to draw. Nowadays applications of chaotic attractors in several domains (see (Lozi, R. 2023) for a survey) is a flourishing domain of research since three decades and can nevertheless produce wonderful images (Figures 9, 10). In the mean time, theoretical research is still very much alive and offers new mathematical tools such as chimeras, fractional differential equations and fractional mappings which in turn will allow the development of new applications.

Chaotic attractors are definitely not a mathematical curiosity.

Acknowledgments

The author thanks Laura Gardini from University of Urbino (Italy) and Iryna Sushko from National Academy of Sciences of Ukraine, Kyiv (Ukraine) for drawing two special figures for this editorial.

Availability of data and material

Not applicable.

Conflicts of interest

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

LITERATURE CITED

Abdelouahab, M.- S., Lozi, R., and Chua, L. O., 2008 Memfractance: A mathematical paradigm for circuit elements with memory. Int. J. Bifurc. Chaos **24**: 1430023.

Araujo, E. and L. S. Coelho, 2008 Particle swarm approaches using lozi map chaotic sequences to fuzzy modelling of an experimental thermal-vacuum system. Applied Soft Computing **8**: 1354–1364.

Belykh, V. N., Barabash, N. V., and Grechko, D. A. , 2023 Existence proofs for strange attractors in piecewise-smooth nonlinear lozi-hénon and belykh maps. Journal of Difference Equations and Applications pp. 1–21.

Caponetto, R., Fortuna, L., Fazzino, S., and Xibilia, M. G., 2003 Chaotic sequences to improve the performance of evolutionary algorithms. IEEE Trans. Evol. Comput. **7**: 289–304.

Chua, L. O., 1971 Particle swarm approaches using Lozi map chaotic sequences to fuzzy modelling of an experimental thermal-vacuum system. IEEE Trans. Circuit Th. **18**: 507–519.

Commendatore, P., Kubin, I., and Sushko, I., 2015 Typical bifurcation scenario in a three region symmetric new economic geography model. Mathematics and Computers in Simulation **108**: 63–80.

Davendra, D., Zelinka, I., and Senkerik, R., 2010 Chaos driven evolutionary algorithms for the task of pid control. Computers and Mathematics with Applications **60**: 1088–1104.

Dmitriev, A .S., Panas, A. I., and Starkov, S. O., 2000 Multiple access communication based on control of special chaotic trajectories. Proceedings of 2nd International Conference. Control of Oscillations and Chaos(COC-2000), St. Petersburg, Russia **3**: 518–522.

El Assad, S., Lozi, R., and Puech, W., 2022 *Special Issue "Cryptography and Its Applications in Information Security"*. Applied Science, MDPI,.

Garasym, O., Lozi, J. P., and Lozi, R., 2017 How useful randomness for cryptography can emerge from multicore-implemented complex networks of chaotic maps. Journal of difference equations and applications **23**: 821–859.

Harmer, G. P., Abbott, D., Taylor, P. G., and Parrondo J. M. R., 2001 Brownian ratchets and parrondo's games. Chaos **11**: 705A–714.

Heath, T. L., 1931 *A Manual of Greek Mathematics*. Oxford University Press, Oxford.

Høyrup J., 2011 Mesopotamian calculation: Background and contrast to greek mathematics. Contribution to IX Congresso della Società Italiana di Storia della Matematica, Genova, 17–19 novembre .

Li, T. Y. and Yorke, J. A. , 1975 Period three implies chaos. The American Mathematical Monthly **82**: 985–992.

Lorenz, E. N., 1963 Deterministic nonperiodic flow. Journal of the Atmospheric Sciences **20**: 130–141.

Lozi, R., 1995 Secure communications via chaotic synchronization in chua's circuit and bonhoeffer-van der pol equation: numerical analysis of the errors of the recovered signal. IEEE international Symposium on circuits and systems **1**: 684–687.

Lozi, R., 2023 Algorithms using the chaotic lozi map for real applications or for applications exploring some new mathematical fields: a survey. Algorithms, To appear pp. 1319–1325.

Lozi, R. and Chua, L. O., 1993 Secure communications via chaotic synchronization ii: noise reduction by cascading two identical receivers. International Journal of Bifurcation and Chaos **3**: 1319–1325.

Mandelbrot, B., 1967 How long is the coast of britain? statistical self-similarity and fractional dimension. Science, New Series **156**: 1088–1104.

Marinke, R., Araujo, J. E., Coelho, L. S., and Matko, I., 2005 Particle swarm optimization (pso) applied to fuzzy modeling in a thermal-vacuum system. Proceedings of the 5th International Conference on Hybrid Intelligent Systems, Rio de Janeiro, Brazil pp. 67–72.

Pecora, L. M. and Carroll, T. L., 1990 Synchronization in chaotic systems. Phys. Rev. Lett. **64**: 821.

Peitgen, H.-O. and Richter, P. H., 2011 *The Beauty of Fractals: Images of Complex Dynamical Systems*. Springer Verlag, Berlin.

Pluhacek, M., Senkerik, R., Davendra, D., and Zelinka, I., 2012 Designing pid controller for dc motor system by means of enhaced pso algorithm with discrete lozi map. Proceedings 26th European Conference on Modelling and Simulation,ECMS 2012, Troitzsch, K. G.; Möhring, M.; Lotzmann, U. (Eds) pp. 405–409.

Rodriguez-Vazquez, A., Huertas, J. L., Perez-Verdu, B., and Chua, L. O. , 1987 Chaos from switched-capacitor circuits: Discrete maps. Proceedings of the IEEE **75**: 1090–1106.

Rössler, O. E., 1976 Chaotic behavior in simple reaction system. Zeitschrift für Naturforschung A **31**: 259–264.

Rössler, O. E., 2020 On the Rossler Attractor. Chaos Theory and Applications **2**: 1–2.

Rybalova, E., Semenova, N., and Anishchenko, V., 2018 Solitary state chimera: Appearance, structure, and synchronization. International Symposium on Nonlinear Theory and Its Applications NOLTA 2018, Tarragona, Spain pp. 601–604.

Senkerik, R., Davendra, D, Zelinka, I., Pluhacek, M., and Kominkova Oplatkova, Z., 2013 Chaos driven differential evolution with lozi map in the task of chemical reactor optimization. Lecture Notes in Computer Science **7895**.

Strukov, D. B., Snider, G. S., Stewart, D. R., and Williams, R. S., 2008 The missing memristor found. Nature **453**: 80–83.

Su, Y. , Xu, T. , Li, T. , Zhao, J. , and Liu, S. , 2021 Optical color image encryption based on fingerprint key and phase-shifting digital holography. Optics and Lasers in Engineering **140**: 106550.

Sushko, I. , Tramontana, F. , and Gardini, L. , 2023, in progress Optical color image encryption based on fingerprint key and phase-shifting digital holography. Working Papers Series in Economics, Mathematics and Statistics, University of Urbino .

Tang, T. W. , Allison, A., and Abbott, D. , 2004 Investigation of chaotic switching strategies in parrondo's games. Fluctuation and Noise Letters **4**: L585–L596.

Wang, J., Gu, Y., Rong, K., and Xu, Q.and Zhang, X., 2022 Memristor-based lozi map with hidden hyperchaos. Mathematics **10**: 3426.

Zelinka, I., 2004 Self-organizing migrating algorithm. Studies in Fuzziness and Soft Computing **141**: 167–217.

Zelinka, I., Kojecky, L., Lampart, M., Nowakova, M. J., and Plucar, J., 2023 isoma swarm intelligence algorithm in synthesis of quantum computing circuits. Applied Soft Computing **142**: 110350.

Zhang, L. P., Wei, Z. C., Jiang, H. B., Lyu, W. P., and Bi, Q. S., 2022 Extremely hidden multistability in a class of a two dimensional maps with a cosine memristor. Chin. Phys. **B 31**: 100503.

How to cite this article: Lozi, R. Are Chaotic Attractors just a Mathematical Curiosity or Do They Contribute to the Advancement of Science? *Chaos Theory and Applications*, 5(3), 133-140, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.141-152
https://doi.org/10.51537/chaos.1314803

Estimating Optimal Synchronization Parameters for Coherent Chaotic Communication Systems in Noisy Conditions

Vyacheslav Rybin [*,1], **Ivan Babkin** [*,2], **Dmitry Kvitko** [*,3], **Timur Karimov** [*,4], **Lucas Nardo** [α,5], **Erivelton Nepomuceno** [β,6] **and Denis Butusov** [*,7]

[*] Youth Research Institute at ETU LETI, ul. Professora Popova 5, 197022 St. Petersburg, Russian Federation, [α] Graduate Program in Electrical Engineering, Federal University of Minas Gerais, Av. Antônio Carlos, 6627, Pampulha, Belo Horizonte, 31270-901, Brazil, [β] Center for Ocean Energy Research, Department of Electronic Engineering, Maynooth University, Maynooth, Kildare, Dublin 7, W23 A3HY Ireland.

ABSTRACT It is known, that coherent chaotic communication systems are more vulnerable to noise in the transmission channel than conventional communications. Among the various methods of reducing the noise impact, such as extended symbol length and various digital filtering algorithms, the optimization of the synchronization coefficient may appear as a very efficient and simple straightforward approach. However, finding the optimal coefficient for the synchronization of two chaotic oscillators is a challenging task due to the high sensitivity of chaos to any disturbances. In this paper, we propose an algorithm for finding the optimal synchronization parameter K_{opt} for a coherent chaos-based communication system affected by various noises with different signal-to-noise ratios (SNR). It is shown, that under certain conditions, optimal K provides the lowest possible bit error rate (BER) during the data transmission. In addition, we show that various metrics applied to the message analysis and demodulation task propose different noise immunity to the overall system. In the experimental part of the study, we simulated and physically prototyped two chaotic communication systems based on well-known Rössler and Lorenz chaotic oscillators. The microcontroller-based prototype of a wire chaotic communication system was developed to investigate the influence of noise in the physical data transmission channel. The experimental results obtained with the designed hardware testbench are in good correspondence with the theoretical propositions of the study and preliminary simulation results. The suggested evaluation metrics and optimization algorithms can be used in the design of advanced chaos-based communication systems with increased performance.

KEYWORDS
Chaotic synchronization
Coherent chaotic communication
Covert communication
MCU
Chaos with noise

INTRODUCTION

Dynamical chaos and chaotic synchronization are essential phenomena in nonlinear dynamics. Recently, many chaos applications such as chaotic encryption (Volos *et al.* 2013), chaos-based sensors (Karimov *et al.* 2021a), and chaos-based communication systems were proposed. One of the most promising applications of chaotic synchronization is chaos-based communication systems, which possess a broadband channel for concealed data transfer. Chaotic communication systems (CCS) based on chaotic synchronization are called coherent (Kaddoum 2016).

Recent works include studies on optical coherent chaotic communication systems (Wang *et al.* 2020; Yang *et al.* 2020), digital data transfer systems for Internet of Things (IoT) applications (Babajans *et al.* 2023, 2022; Cirjulina *et al.* 2022), area- and power-efficient implementation of chaotic oscillators for coherent secure systems

Manuscript received: 19 June 2023,
Revised: 17 July 2023,
Accepted: 21 July 2023.

[1] vgrybin@etu.ru
[2] iababkin@stud.etu.ru
[3] dvkvitko@stud.etu.ru
[4] tikarimov@etu.ru
[5] nardo@ufmg.br
[6] erivelton.nepomuceno@mu.ie
[7] dnbutusov@etu.ru (**Corresponding Author**)

(Hedayatipour *et al.* 2022).

Coherent chaos-based communication systems assume achieving chaotic synchronization on the receiver side, which has prompted the development of various synchronization methods. Initially, this phenomenon was discussed in studies (Fujisaka and Yamada 1983) and (Afraimovich *et al.* 1986). However, the topic of chaotic synchronization gained great attention after the introduction of Pecora and Carroll's method. In their famous paper, these authors proposed to use a simple synchronization method in secure communications (Pecora and Carroll 1990). The Pecora-Carroll synchronization suggests a master-slave system architecture, represented by two identical chaotic oscillators with the same parameter set, where the signal from the master system is driving the other system dynamics (Pecora and Carroll 1990).

To transform the meaningful signal into chaotic carrier changes, various modulation and demodulation techniques were developed. The most popular modulation methods used in chaos-based communications are chaotic shift keying (CSK) (Dedieu *et al.* 1993; Dmitriev and Panas 2002), parametric modulation (PM) (Yang and Chua 1996; Koronovskii *et al.* 2009), and chaotic symbolic dynamics (Kaddoum 2016). Although some other modulation techniques have been proposed recently, they mainly involve variations or combinations of the aforementioned approaches (Kharel 2011). In the current study, we focus on parametric modulation (PM), as an easy-to-implement and highly secure common approach.

In classical studies, such as (Carroll and Pecora 1995) and (Willsey *et al.* 2011), as well as in more recent works, e.g. (Abib and Eisencraft 2015), scholars proposed the application of analog circuits to generate chaotic signals in communication systems. However, this approach possesses some disadvantages, e.g. the limited precision of the chaotic circuit components, conditional parameter drift, etc. In addition, as is known from several recent studies (Minati *et al.* 2017; Karimov *et al.* 2023; Emiroglu *et al.* 2022; Alexander *et al.* 2023), the behavior of analog circuits may significantly differ from the original mathematical models and vary between different implementations, which in the field of coherent chaotic communications may lead to difficulties in matching between transmitter and receiver parameters. Therefore, one can consider a completely digital communication system based on direct digital synthesis (DDS) as a prospective technology.

The DDS is a method of generating an analog signal using a digital-to-analog converter (DAC) and data from a digital processing unit (Liu *et al.* 2007). DDS can generate highly precise and stable waveforms, allowing one to use it in a wide variety of applications, such as telecommunications, signal processing, test, and measurement equipment (Cordesses 2004a,b). The DDS was also reported to be used for noise radar (Willsey *et al.* 2011), as well as for covert messaging in noisy conditions (Lukin and Zemlyaniy 2016) - tasks that are very closely related to chaotic messaging.

Latest developments have shown the opportunity for chaotic communication DDS systems to use modulation schemes where the discretization operator is varied to obtain different finite-difference equations. An example of such a technique is the symmetry coefficient modulation (SCM) (Karimov *et al.* 2021b). SCM operates by manipulating the numerical method parameter, called symmetry coefficient, and can be used to construct the digital chaotic messaging signal. Several papers (Rybin *et al.* 2022a, 2023) show that SCM may provide more covert messaging than traditional PM techniques.

As an alternative to coherent chaotic communication systems, so-called non-coherent systems have been researched and developed. Such systems do not use synchronization but are based on correlation or other matching methods. Recent works on the subject include digital underwater communication systems (Bai *et al.* 2019, 2018), systems based on chaotic oscillators with special properties for general applications (Rajagopal *et al.* 2018), and other techniques (Moysis *et al.* 2020; Lyu *et al.* 2015). Non-coherent communication systems are considered more resistant to noise while being also less resistant to attacks (Kaddoum *et al.* 2010; Kaddoum 2016). It should be noted, that low resistivity to noise is one of the key shortcomings of coherent CSS. Thus, considering their high-security level, especially when using DDS technology, it seems promising to develop some methods of improving their noise immunity.

Such methods can include denoising techniques for chaotic signals (Voznesensky *et al.* 2022), as well as various techniques for improving the reliability of communications with noisy input signals. One natural idea here is to find the optimal synchronization coefficient K (the proportion, in which the transmitter signal is mixed via the receiver signal to force its synchronization) for the given channel conditions. Our previous studies have shown that the synchronization coefficient value provides a noticeable impact on the quality of messaging in coherent systems without noise in the communication channel(Rybin *et al.* 2021, 2022b). Therefore, the current study aims to investigate the possibility of finding optimal K comprehensively. We consider different chaotic oscillators, various signal-to-noise ratios in the channel, and symbol lengths in order to experimentally validate the obtained results.

The main contributions of this study can be summarized as follows:

1. A model of a coherent chaos-based communication system with parameter modulation (PM) under various signal-to-noise (SNR) levels is considered. We choose classical Lorenz and Rössler systems for the CCS prototypes due to their well-known chaotic properties, and Gaussian white noise as typical interference noise.

2. Various metrics for synchronization error analysis were used to distinguish binary characters '0' and '1' in demodulating algorithms of the prototyped systems.

3. It was discovered that different metrics for synchronization error analysis at the receiver side provide different noise immunity to the overall system. The most effective metrics were found to be root-mean-square (RMS) and mean value calculation.

4. The suggestion that the optimal synchronization coefficients K depend on the noise level in channel and symbol length, and the form of this dependence is unique for a particular chaotic oscillator, is confirmed experimentally. For practical applications, the optimal K value can be approximated by a simple expression with sufficient accuracy, and then dynamically selected during communication based on an estimate of the noise level and the data transfer rate, which advances the architecture of the chaotic communication system.

5. A new algorithm for finding an array of optimal synchronization coefficients for an arbitrary chaotic oscillator under given parameters and certain conditions is proposed.

Summarizing, the reported research makes a significant step toward solving the problem of finding the optimal synchronization coefficient and further improving the design of coherent CCS. Being a simple and efficient technique, this approach could be

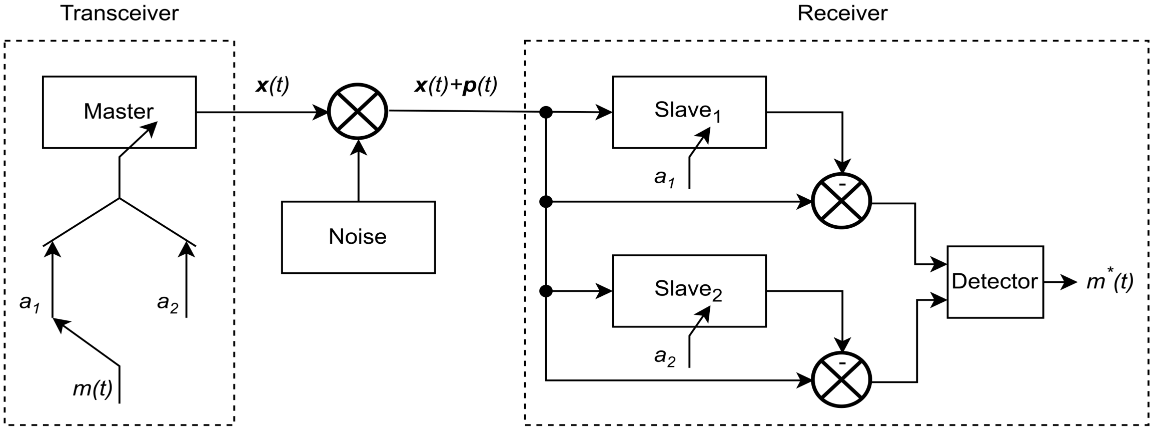


Figure 1 The scheme for a chaotic communication system based on parameter modulation.

considered alongside other noise-reducing methods to advance the development of robust and reliable communication systems.

The rest of the paper is organized as follows: in Section 2, the investigated chaotic systems and the architecture of the chaos-based communication system are described. The experimental setup, as well as the results of the experimental investigation, are presented in Section 3. Section 4 discusses the obtained results considering their practical applications, and Section 5 concludes the paper.

MATERIALS AND METHODS

This section provides a brief description of the chosen chaotic oscillators and the communication system under investigation, as well as the methods of analyzing the synchronization error on the receiver side.

Investigated chaotic systems

In previous works, we attempted to determine the optimal synchronization coefficients for chaotic communication systems based on Lorenz and Rössler systems (Rybin *et al.* 2021, 2022b). These canonical systems are used as chaos generators in the current study as well, providing a basis for chaotic communication systems under investigation.

The well-known Lorenz chaotic system (Liao 1998) is described by the following system of ordinary differential equations:

$$\begin{aligned} \dot{x} &= \sigma(y-x), \\ \dot{y} &= x(r-z)-y, \\ \dot{z} &= xy-bz, \end{aligned} \tag{1}$$

where $\sigma = 10$, $r = 28$, $b = \frac{8}{3}$.

Let us apply the Pecora-Carroll (Pecora and Carroll 1990) synchronization to system (1) to obtain the slave (receiver) oscillator system:

$$\begin{aligned} \dot{x} &= \sigma(y-x), \\ \dot{y} &= x(r-z)-y+K(y_M-y), \\ \dot{z} &= xy-bz, \end{aligned} \tag{2}$$

where K is the coupling strength coefficient, and y_M is the second variable of the master system. It is known (Rybin *et al.* 2021, 2022b) that the preferred synchronization variable for the Lorenz system is y and the approximate value of coupling strength $K \approx 40$ provides the fastest synchronization.

The Rössler system (Gaspard 2005) is described by the following system of ordinary differential equations:

$$\begin{aligned} \dot{x} &= -y-z, \\ \dot{y} &= x+ay, \\ \dot{z} &= b+z(x-c), \end{aligned} \tag{3}$$

where $a = 0.2$, $b = 0.2$ and $c = 5.7$. Applying the Pecora-Carroll synchronization to system (3), one can obtain the equations of the slave oscillator:

$$\begin{aligned} \dot{x} &= -y-z, \\ \dot{y} &= x+ay+K(y_M-y), \\ \dot{z} &= b+z(x-c), \end{aligned} \tag{4}$$

where K is a synchronization coefficient and y_M is the second variable of the master system, which is also the optimal synchronization variable for Rössler system. The value of coupling strength $K \approx 1.93$ provides the rapid synchronization process (Rybin *et al.* 2021, 2022b).

Chaotic communication system design

In the experimental part of the study, we considered a conventional coherent chaotic communication system with parametric modulation. It should be noted that all the methods used in this research can be used for improving the chaotic communication systems based on other modulation methods, for example, the recently proposed symmetry coefficient modulation (Karimov *et al.* 2021b; Tutueva *et al.* 2022). The investigated scheme for a chaotic communication system based on parameter modulation is shown in Figure 1.

The operating principle of the CCS based on parametric modulation can be described as follows. The desired digital signal $m(t)$ modulates parameter a of the chaotic oscillator on the transceiver side. Next, the signal passes through the simulated communication channel, where white Gaussian noise is added along with the noise of the DAC (digital-to-analog converter) and ADC (analog-to-digital converter) units. In our experiments, the bit depth of the DAC and ADC was 12 bits. One can observe that the generalized chaotic synchronization occurs on the receiver side, depending on the transmitted bit of the message. The message recovery $m^*(t)$ is performed by determining the lowest value of the synchronization error. The example of message transmission is shown in Figure 2.

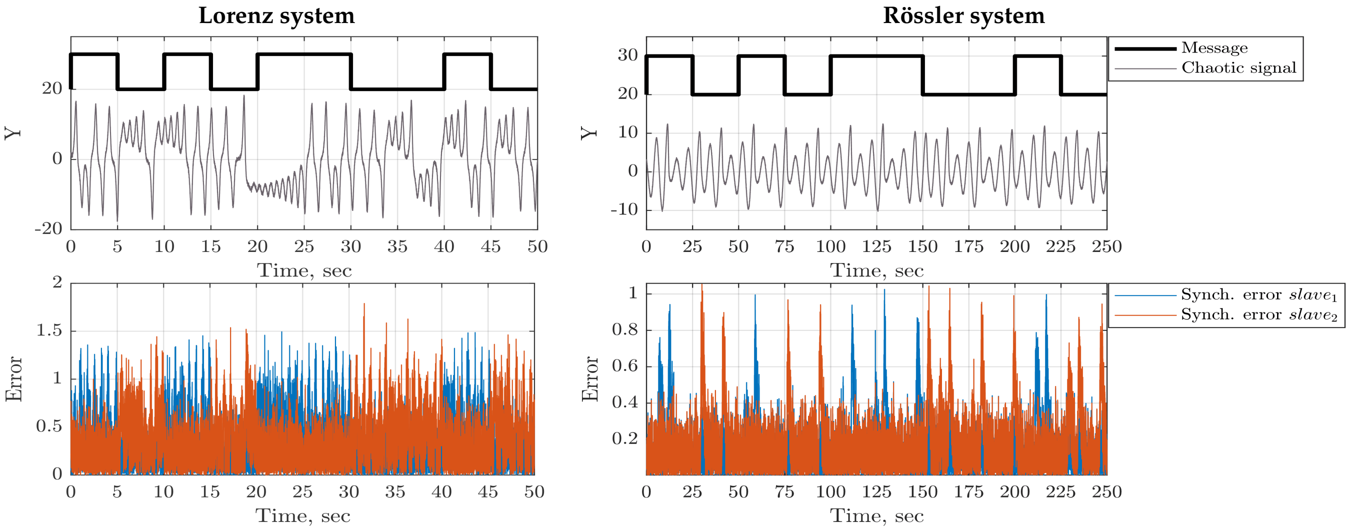


Figure 2 Transmission of message "1010110010" by chaotic communication system with parameter modulation based on Rössler and Lorenz system.

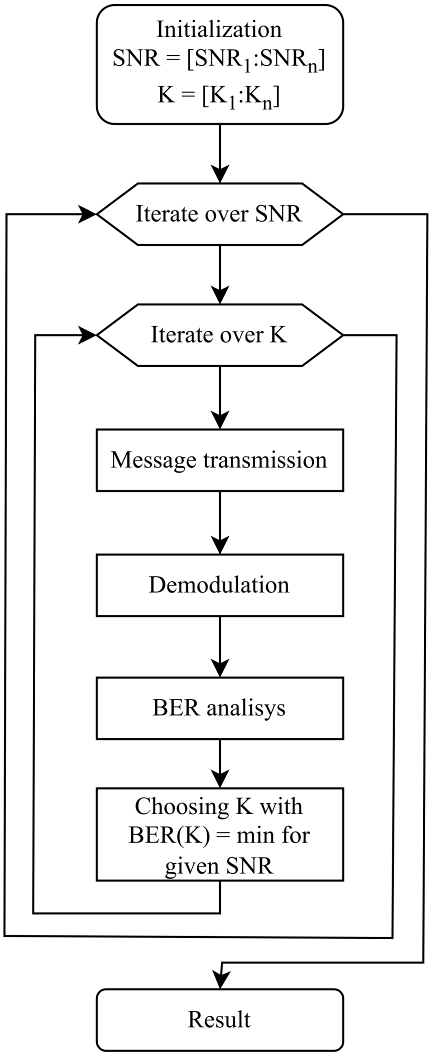


Figure 3 Scheme of an algorithm for the synchronization coefficient investigation.

As one can see from the Figure 2, the chaotic signal possesses no visible correlation with the transmitted message in both cases, especially being compared with the behavior of the synchronization error.

In some studies, the transmission of certain informational bits is determined by threshold (Rybin *et al.* 2023; Kaddoum 2016) and assumed post-processing of the resulting synchronization error. However, in the presence of noise in the communication channel, threshold detection can be inefficient. Thus, in the current paper, we have chosen and evaluated several comparative methods for estimating the difference in synchronization error.

Finding the optimal synchronization coefficient

To determine the optimal values of K for an arbitrary SNR range, one should set the optimization criterion first. Let us call the synchronization coefficient K optimal if the bit error rate (BER) of the communication system is minimal. The following algorithm was developed (see Figure 3) to solve the optimization task. First, the SNR range and the synchronization coefficient K are initialized. Then, an iterative enumeration of the SNR is performed, and K values for which the transmission process takes place are determined. Finally, the received message is demodulated and analyzed. The number of errors in the message at a chosen K and SNR is calculated, and the BER for a chosen K is compared to the minimum error value for a given SNR. The smallest of these two values is selected. Then the K value is iteratively increased, and all the abovementioned steps are repeated until the investigation range ends. Then, the SNR is iteratively increased, and the same process continues until all K values are determined for all SNR values. One can find optimal values of $K_{opt} = f(SNR)$ when BER = $f(K)$ is minimal. The final goal, namely, to get the minimal BER for the given SNR, can be achieved via selected $K = K_{opt}$.

RESULTS

Experimental setup

All numerical experiments were performed using the National Instruments LabVIEW 2021 environment. In all numerical experiments, the explicit Runge-Kutta method of accuracy order 2

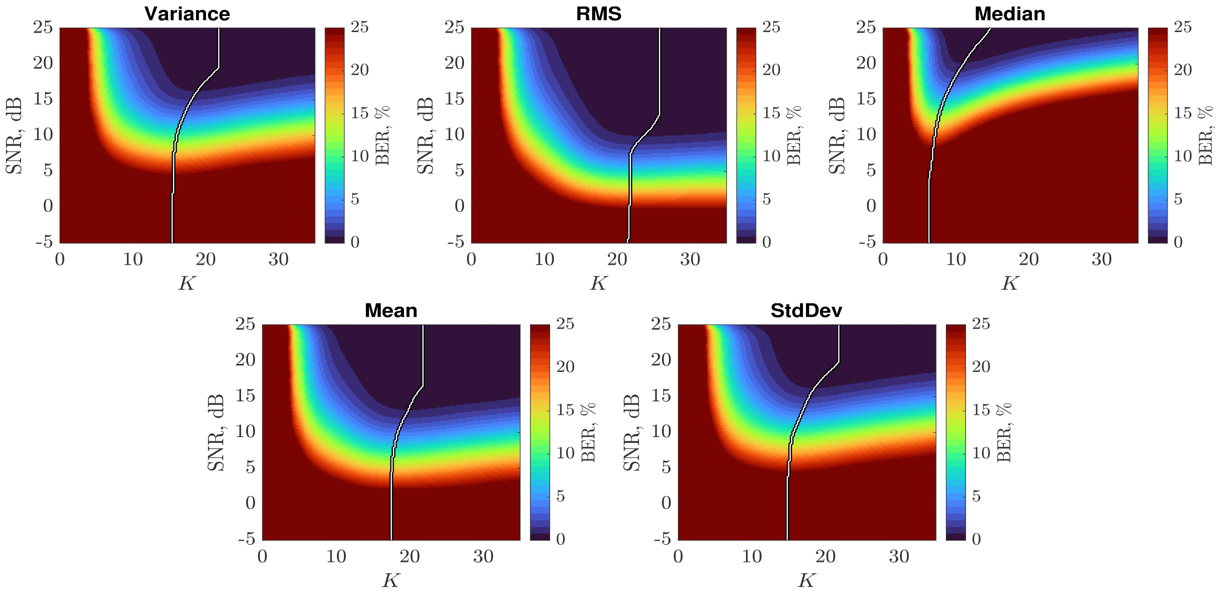


Figure 4 The dependence between BER, synchronization coefficient K, and SNR for Lorenz system. The black-and-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNR values.

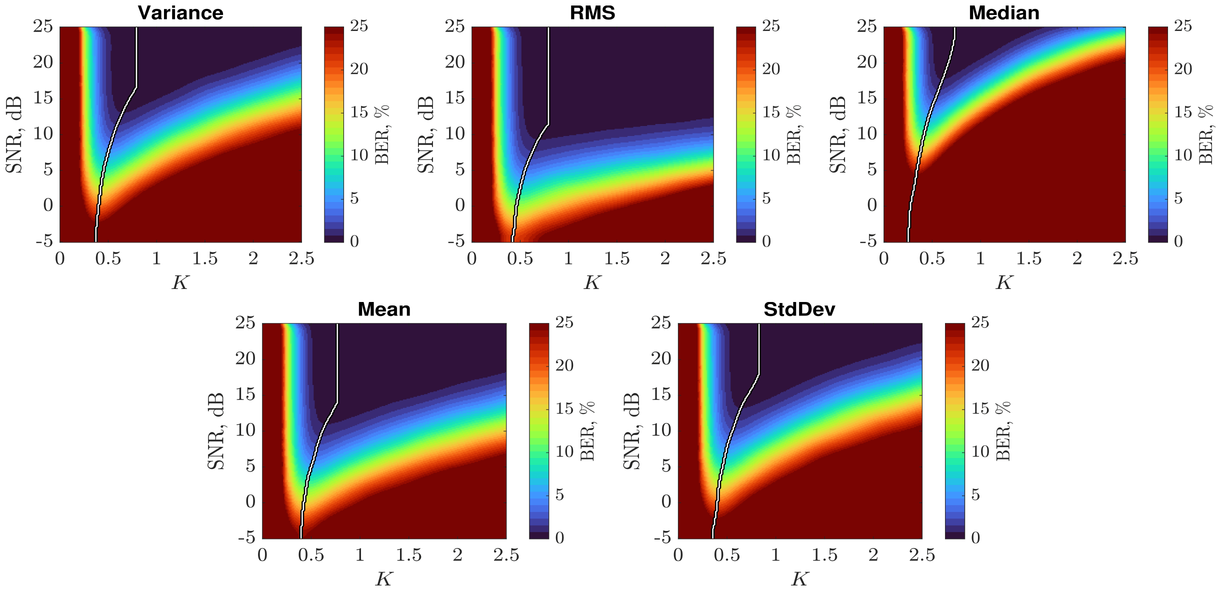


Figure 5 The dependence between BER, synchronization coefficient K, and SNR for Rössler system. The black-and-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNR values.

(RK2) was used to solve the ODEs of the investigated system. The choice of the RK2 method can be explained by the fact, that obtaining the highly accurate solution of ODE is not required for CCS construction purposes. In fact, one can use almost an arbitrary finite-difference model of the chosen continuous chaotic system because both sample systems are dissipative and do not require special geometrical integration procedures for long-term simulation. The benefit of choosing an explicit second-order integration method is the simplicity of its hardware implementation. To summarize, the RK2 method ensures the stable long-term generation of the chaotic signal, and switching the bifurcation parameters does not cause a stability loss.

The integration stepsize for the Lorenz system was chosen as $h = 0.005$ and for Rössler system was set as $h = 0.025$. The initial conditions for both systems were set as $(0.1, 0.1, 0.1)$. One should note, that in a real CCS, the initial conditions may be a part of the security key.

In this study, we use relative time units to characterize the length of the transmitted symbol for the Lorenz and Rössler systems. The reason is that these systems have different dynamics and variable change speeds when presented in a natural timescale given in seconds. The Lorenz system dynamics is faster than Rössler systems. Therefore, let us introduce pseudo-periods $N_{\tilde{T}}$ as time units for this study:

$$N_{\tilde{T}} = \vartheta \cdot T_s, \tag{5}$$

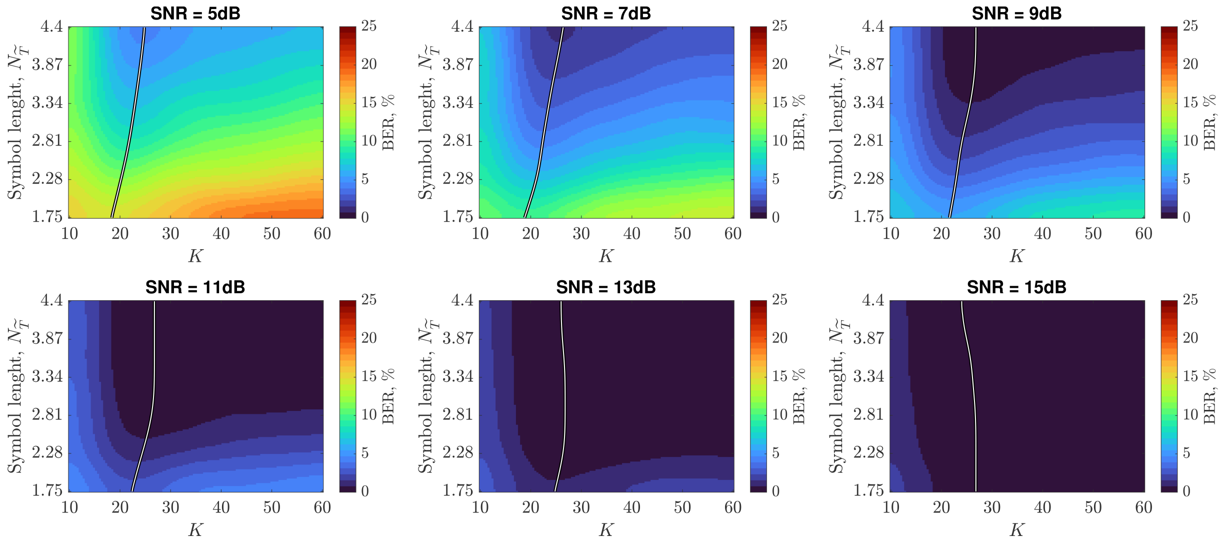


Figure 6 The dependence between BER, synchronization coefficient K, and symbol transmission length for various SNR values of Lorenz-based CCS system. The black-and-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNR values.

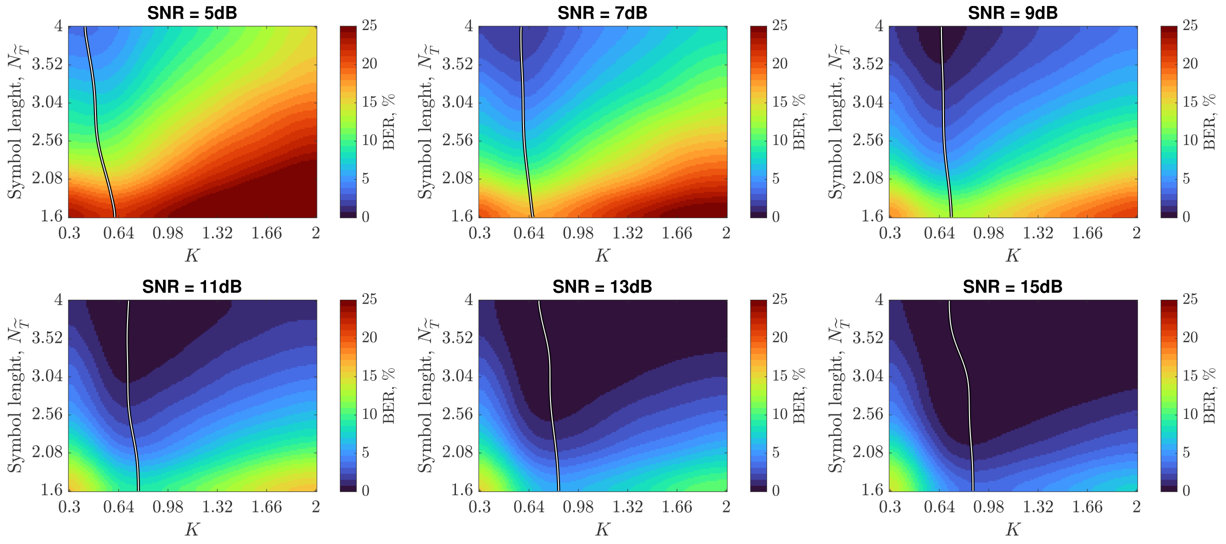


Figure 7 The dependence between BER, synchronization coefficient K and symbol transmission length with various SNR values for Rössler system. The black-and-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNR values.

where ϑ is the median frequency of the chaotic signal (Hz), and T_s is the symbol transmission time in seconds.

Obtaining the optimal synchronization coefficient using BER and SNR metrics

Let us vary the synchronization coefficient under different noise conditions and calculate the corresponding bit-error rate. Figure 4 shows the experimental results for the CCS based on the Lorenz system with parameter σ ($\sigma_1 = 9.5$ and $\sigma_2 = 10.5$) modulation.

Figure 5 shows the experimental results for the investigated CCS based on Rössler system with parameter a ($a_1 = 0.18$ and $a_2 = 0.22$) modulation.

Following the experimental results, one can conclude that the most efficient metric for estimating the synchronization error in coherent communication systems is root-mean-square (RMS) as it provides the lowest BER for a given SNR value in comparison to other metrics, which makes it a perfect candidate for optimization function. Thus, our further experiments on the chaotic communication systems' optimization will be performed using this metric as a key evaluator of the design quality.

Investigating the dependence between K and $N_{\tilde{T}}$

Let us estimate the dependence of BER on the synchronization coefficient and the length of the transmitted symbol for different levels of noise present in the communication channel. Figures 6 and 7 show the experimental results for Lorenz and Rössler systems, respectively.

One can see from Figures 6 and 7, that while the SNR in the communication channel increases, the symbol transmission time may be reduced by preserving the same BER level using the proper choice of the synchronization coefficient. Thus, it can be concluded, that it also can be used for increasing the data transfer rate while

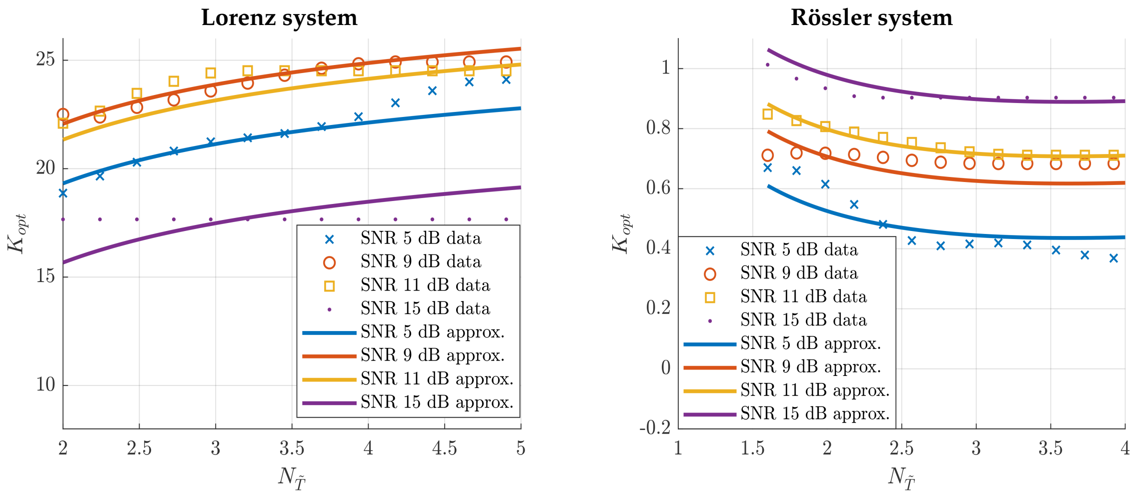


Figure 8 The behavior of optimal synchronization coefficient K while varying the symbol transmission length with various values of SNR for Lorenz and Rössler

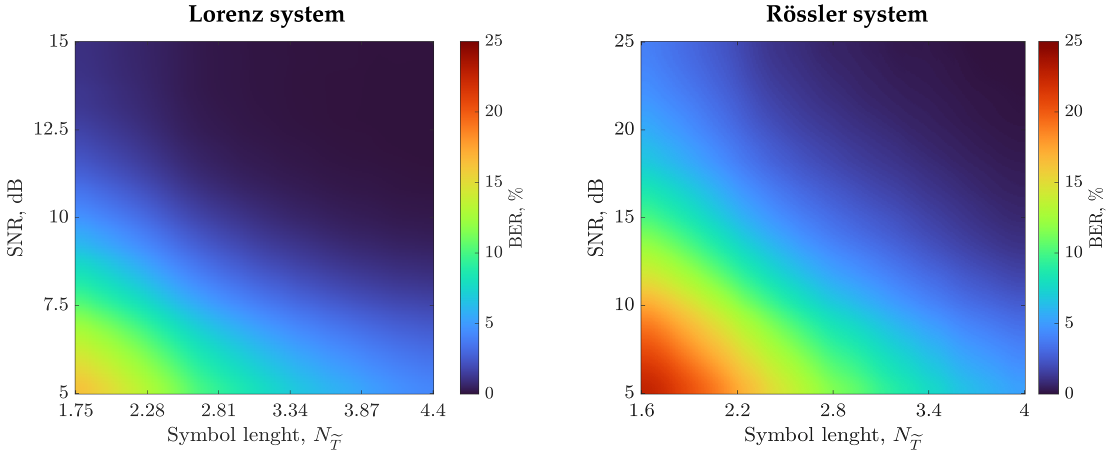


Figure 9 The dependence between BER, symbol transmission length, and SNR with variable synchronization coefficient K for Lorenz and Rössler systems.

preserving the same level of BER.

Approximation of optimal synchronization coefficient K

Using the results obtained in the previous subsection, let us obtain the equations for calculating the optimal synchronization coefficient depending on the symbol length and SNR.

The equation for optimal synchronization coefficient calculation for the Lorenz system is as follows:

$$K_L(N_{\tilde{T}},\varsigma) = a + bN_{\tilde{T}} + c\varsigma + d\varsigma^2 + e/N_{\tilde{T}}; \qquad (6)$$

where $N_{\tilde{T}}$ is a length of transmitted symbol in pseudo-periods, ς is a signal-to-noise ratio in dB, $a = 12.61$, $b = 0.1665$, $c = 3.141$, $d = -0.1753$, $e = -9.892$.

The equation for calculating the optimal synchronization coefficient for Rössler system is as follows:

$$K_R(N_{\tilde{T}},\varsigma) = a + bN_{\tilde{T}} + c\varsigma + d/(N_{\tilde{T}})^g; \qquad (7)$$

where $N_{\tilde{T}}$ is a length of transmitted symbol in pseudoperiods, ς is signal-to-noise ratio in dB, $a = -0.273$, $b = 0.06711$, $c = 0.04534$, $d = 0.886$, $g = 1.018$.

Figure 9 shows the estimation of BER in the proposed CCS with various symbol transmission lengths and SNR values, while K varies being obtained by equation 6 and 7. Experimental results confirm the linear dependence of the symbol's transmitted length on the various SNRs while maintaining the same BER value. Generally, this dependence is in direct correspondence with the Shannon theorem: when increasing the data transfer rate, the BER level will also increase (Shannon 1984).

Influence of the different CCS parameters on K

Table 1 shows the experimental results for the prototype chaotic communication systems based on Rössler and Lorenz systems, where modulated parameters are $a_0 = 0.18$ and $a_1 = 0.22$ for Rössler system, and $\sigma_0 = 9.5$ and $\sigma_1 = 10.5$ for Lorenz system.

Table 2 shows the experimental results for the CCS based on Lorenz and Rössler system with short symbol transmission length and parameter σ and a modulation, where $a_0 = 0.18$ and $a_1 = 0.22$,

Table 1 The optimal synchronization coefficient K value which provides a minimum SNR for BER = 0%

System	Rössler					Lorenz				
Method	Var	RMS	Med	Mean	StdDev	Var	RMS	Med	Mean	StdDev
Optimal K	0.6384	0.6816	0.5933	0.6394	0.6369	16.0754	22.1078	9.5615	19.1313	15.3134
Min SNR	12.7108	9.2169	17.0482	10.7831	12.8313	16.2371	10.5155	19.0206	13.7629	16.3918

Table 2 The optimal synchronization coefficient K value, providing a minimum SNR for BER = 0% for Rössler and Lorenz system for a short message.

System	Rössler					Lorenz				
Method	Var	RMS	Med	Mean	StdDev	Var	RMS	Med	Mean	StdDev
Optimal K	0.7541	0.8296	0.7148	0.7719	0.7694	14.4131	17.7306	7.8008	15.3437	14.1714
Min SNR	18.8285	14.5607	22.8452	16.318	18.7029	20.3614	14.4578	23.9759	17.4699	20.3614

Table 3 The optimal synchronization coefficient K value which provides the minimum SNR for BER = 0% while modulating a third parameter.

System	Rössler					Lorenz				
Method	Var	RMS	Med	Mean	StdDev	Var	RMS	Med	Mean	StdDev
Optimal K	0.5454	0.612	0.5104	0.552	0.5772	13.5907	19.0163	7.17294	15.3663	13.8238
Min SNR	11.2651	8.9759	15.4819	9.9398	11.506	10.7831	5.8434	13.5542	8.3735	10.6627

and $\sigma_0 = 9.5$ and $\sigma_1 = 10.5$.

Table 3 shows the experimental results for CCS based on Rössler and Lorenz system with parameter c modulation, where $c_0 = 5.7$ and $c_1 = 6.2$ for Rössler, and $b_0 = 2.3$ and $b_1 = 2.7$ for Lorenz system.

Note that in all experiments the RMS showed the highest performance, and the arithmetic mean performed slightly worse. However, the arithmetic mean can also be a potential candidate for coherent CCS implementation because of its computational simplicity, which is vital for such hardware as microcontrollers and FPGAs.

Another important conclusion from the repo experiments is that the value of optimal coefficient K depends also on the choice of parameters used for transmitting binary symbols '0' and '1'. Thus, the algorithm 3 should be executed for each parameter set in the CCS design.

Experiments with hardware prototype

BER values obtained by numerical simulation were validated using a physical prototype of a Lorenz-based chaotic communication system. We performed this experiment using the experimental CCS testbench developed by our team for research purposes (Rybin *et al.* 2023). The appearance of the experimental bench is shown in Figure 10.

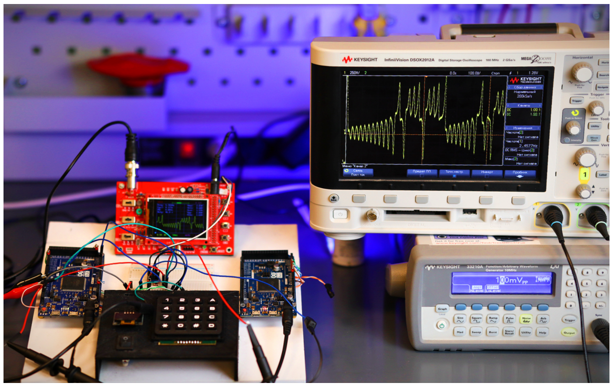


Figure 10 Experimental bench implementing MCU-operating chaotic communication system with a noisy channel based on Lorenz chaotic oscillator.

The suggested testbench consists of two microcontrollers (Arduino DUE) serving as transmitter and receiver, a wired communication channel with additive noise provided by a signal generator and op-amp-based mixer, a couple of oscilloscopes for acquiring and visualizing the signals, and a simple keyboard to input messages. In this experimental study, we used SNR levels of 5, 10, and 15 dB, and symbol lengths 2, 3, and 4 $N_{\tilde{T}}$. The optimal K values were calculated using the equation (6). The obtained results show that the numerical simulation allows us to predict most of the effects observed in the real CCS with high accuracy. The difference between the simulation and experiments using BER metrics appeared not to exceed 5%. This slight difference can be explained by statistical errors. For example, considering a data transfer rate of 6 bps, we transmitted only approximately 1000 symbols (bits) for each set of parameters. In addition, the experimental study is challenging in setting the required SNR level, as the noise admixing was performed in an analog way.

DISCUSSION

One may ask, is there a possibility that several optimal values of K exist? The Figures 4 and 5 clearly indicate that for all metrics for synchronization error analysis, the value of the optimal synchronization coefficient is unique in mathematical terms (note: this stands if the value of BER is greater than zero). In other words, if we consider K as a function of SNR, it is unimodal. For the cases with zero BER, one may find and choose the optimal synchronization coefficient which will provide the maximal transfer rate in the designed CCS.

Equations (6) and (7) may be combined with other noise estimation algorithms. Being a critical performance parameter that affects the reliability and throughput of both wire and wireless communications, the level of SNR is often estimated to dynamically adjust transmitter and receiver parameters. Many classical and recent works on the SNR estimation algorithms for communication systems indicate the high importance of the subject (Arslan and Reddy 2003; Hasan and Shongwe 2017; Khan *et al.* 2017; Türkben and Al-Akraa 2022). Having information about the current SNR level, the expression for calculating K_{opt} may be used for both selecting the symbol length at the transmitter side and for adjusting K at the receiver side.

CONCLUSION

The application of coherent chaotic communication systems is currently hampered by their insufficient performance when noise is present in the transmission channel. In the current study, we stepped towards solving this problem by analyzing test chaotic communication systems and finding an approach to estimating the optimal synchronization parameter K that allows researchers to significantly improve the noise immunity of CCS. We explicitly show that it is possible to find the optimal synchronization coefficient for an arbitrary coherent chaotic communication system when the minimum bit error rate (BER) will be achieved at the desired SNR level ς. This procedure requires taking into account other CCS parameters, such as the pair of modulation parameters for binary '0' and '1' representation (p_0 and p_1) and length of the symbol transmission $N_{\tilde{T}}$. Reducing the $N_{\tilde{T}}$, as expected, leads to a decrease in noise resistivity, and influences the value of the optimal synchronization coefficient as well.

In this study, we proposed the practically applicable algorithm for finding the optimal value of K, which takes into account all of the abovementioned factors, and constructed an empirical equation for the calculation of $K_{opt} = f(N_{\tilde{T}}, \varsigma)$ for a given modulation parameter set in a practical system.

We also investigated the efficiency of different techniques for analyzing synchronization errors that are commonly used in CCS design for distinguishing '0' and '1' symbols at the receiver side. We discovered that using arithmetic means and RMS allows us to achieve the lowest BER values. Besides, the arithmetic mean is easier to implement in microcontrollers and FPGAs, while the RMS makes it possible to choose a larger value of the synchronization coefficient, which potentially provides a higher data transfer rate.

As a practical result, we managed to increase the noise immunity of the test coherent communication system without changing its communication structure and without using any denoising or filtering algorithms. It is shown, that by choosing the proper K values and $N_{\tilde{T}}$, it is possible to achieve zero BER at a certain SNR value, while the non-optimal choice of K leads to bit errors at higher SNR levels. For both considered chaotic communication systems, we achieved nearly zero BER using K_{opt} at an SNR level of 3-5 dB, which is significantly lower in comparison to the CCS architectures with fixed synchronization coefficient values known from the literature.

As the direction of future research, we will consider noise level and noise color estimation algorithms for practical CCS implementation in FPGA, as well as combine the suggested approach with digital signal processing techniques.

Author contributions

Conceptualization: Denis Butusov and Vyacheslav Rybin; Formal analysis: Dmitriy Kvitko and Erivelton Nepomuceno; Funding acquisition: Denis Butusov; investigation: Ivan Babkin, Dmitry Kvitko and Vyacheslav Rybin; Methodology: Denis Butusov and Vyacheslav Rybin; project administration: Denis Butusov, Erivelton Nepomuceno and Vyacheslav Rybin; resources: Lucas Nardo and Timur Karimov; software: Dmitriy Kvitko, Ivan Babkin and Timur Karimov; supervision: Denis Butusov; validation: Timur Karimov and Lucas Nardo; visualization: Ivan Babkin and Vyacheslav Rybin; writing – original draft: Vyacheslav Rybin, Timur Karimov and Denis Butusov; writing – review and editing: all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Acknowledgments

This study was supported by Russian Science Foundation (RSF), project 20-79-10334.

Availability of data and material

The data collected in this study are available from the corresponding author upon reasonable request.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

APPENDICES

Methods for synchronization errors analysis during messaging

The presence of noise in the communication channel makes it difficult to use coherent chaotic communication systems (Rybin *et al.* 2023). Therefore, it is of interest to determine the most efficient way to analyze the synchronization error. In this study, we evaluate the effectiveness of variance, root mean square, median mean, and standard deviation values.

Variance The variance is a measure of the spread of numbers in a data set relative to the mean. Using variance, we can evaluate how stretched or squeezed a distribution is. If the variance value is small then the values are close to each other, if the values are large then it means the values are far away. The variance (σ^2) is quantified as:

$$\sigma^2 = \frac{\sum_{i=1}^{N}(x_i - \overline{x})^2}{N}, \tag{8}$$

where $\overline{x}$ stands for mean and x_i is the i^{th} data point.

Root mean square (RMS) the RMS (σ) is a measure of the dispersion of numbers in a data set relative to the mean value. It usually means the square root of the variance. It is calculates as follows:

$$\sigma = \sqrt{\frac{x_1^2 + x_2^2 + x_3^2 + \cdots + x_n^2}{N}}, \tag{9}$$

where N represents the number of data points.

Median value The median ($\tilde{x}$) of a finite list of numbers is the "middle" number when those numbers are listed in order from smallest to greatest. In general, with this convention, the median can be defined as follows: for a data set x of n elements, ordered from smallest to greatest, if n is odd:

$$\tilde{x} = x_{(n+1)/2}, \tag{10}$$

if n is even:

$$\tilde{x} = \frac{x_{(n/2)} + x_{((n/2)+1)}}{2}. \tag{11}$$

Arithmetic mean The arithmetic mean ($\overline{x}$) is the simplest and most widely used measure of a mean or average. It simply involves taking the sum of a group of numbers, then dividing that sum by the count of the numbers used in the series. The equation for a data set x of n elements is

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i = \frac{x_1 + x_2 + \cdots + x_n}{n}. \tag{12}$$

Standard deviation Standard deviation (S) is a statistic that measures the dispersion of a data set relative to its mean and is calculated as the square root of the variance by determining each data point's deviation relative to the mean. The equation for a data set x of n elements is

$$S = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \overline{x})^2}{n-1}}. \tag{13}$$

Experimental results for parameter b and c for Lorenz and Rössler system, respectively;

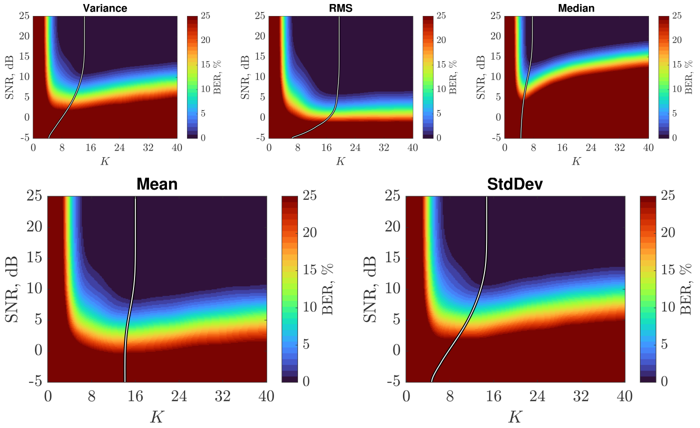


Figure 11 The dependence between BER, synchronization coefficient K, and SNR for Lorenz system with parameter b ($b_1 = 2.3$ and $b_2 = 2.7$). The black-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNRs.

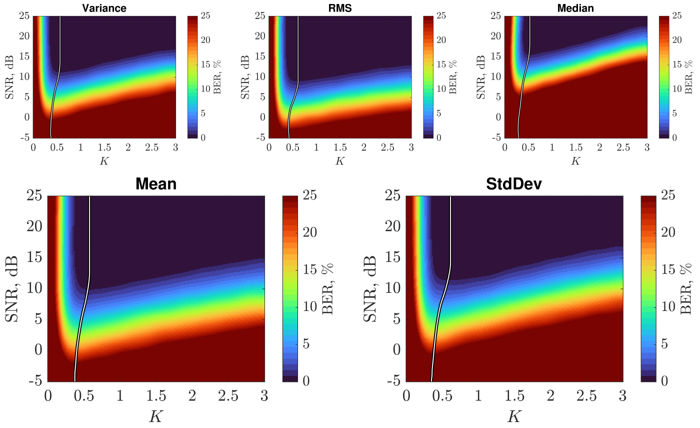


Figure 12 The dependence between BER, synchronization coefficient K, and SNR for Rössler system with parameter c ($c_1 = 5.7$ and $c_2 = 6.2$). The black-white line corresponds to the synchronization coefficient value where BER is minimal for certain SNRs.

LITERATURE CITED

Abib, G. A. and M. Eisencraft, 2015 On the performance of a digital chaos-based communication system in noisy channels. IFAC-PapersOnLine **48**: 976–981.

Afraimovich, V., N. Verichev, and M. I. Rabinovich, 1986 Stochastic synchronization of oscillation in dissipative systems. Radiophysics and Quantum Electronics **29**: 795–803.

Alexander, P., S. Emiroğlu, S. Kanagaraj, A. Akgul, and K. Rajagopal, 2023 Infinite coexisting attractors in an autonomous hyperchaotic megastable oscillator and linear quadratic regulator-based control and synchronization. The European Physical Journal B **96**: 12.

Arslan, H. and S. Reddy, 2003 Noise power and snr estimation for ofdm based wireless communication systems. In *Proc. of 3rd IASTED International Conference on Wireless and Optical Communications (WOC), Banff, Alberta, Canada*, pp. 1–6.

Babajans, R., D. Cirjulina, F. Capligins, D. Kolosovs, J. Grizans, *et al.*, 2023 Performance analysis of vilnius chaos oscillator-based digital data transmission systems for iot. Electronics **12**: 709.

Babajans, R., D. Cirjulina, D. Kolosovs, and A. Litvinenko, 2022 Quadrature chaos phase shift keying communication system based on vilnius chaos oscillator. In *2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW)*, pp. 5–8, IEEE.

Bai, C., H.-P. Ren, M. S. Baptista, and C. Grebogi, 2019 Digital underwater communication with chaos. Communications in Nonlinear Science and Numerical Simulation **73**: 14–24.

Bai, C., H.-P. Ren, C. Grebogi, and M. S. Baptista, 2018 Chaos-based underwater communication with arbitrary transducers and bandwidth. Applied Sciences **8**: 162.

Carroll, T. L. and L. M. Pecora, 1995 Synchronizing chaotic circuits. In *Nonlinear Dynamics in Circuits*, pp. 215–248, World Scientific.

Cirjulina, D., R. Babajans, D. Kolosovs, and A. Litvinenko, 2022 Experimental study on frequency modulated chaos shift keying communication system. In *2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW)*, pp. 1–4, IEEE.

Cordesses, L., 2004a Direct digital synthesis: A tool for periodic wave generation (part 1). IEEE Signal processing magazine **21**: 50–54.

Cordesses, L., 2004b Direct digital synthesis: a tool for periodic wave generation (part 2). IEEE Signal Processing Magazine **21**: 110–112.

Dedieu, H., M. P. Kennedy, and M. Hasler, 1993 Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **40**: 634–642.

Dmitriev, A. and A. Panas, 2002 Dynamic chaos: novel type of information carrier for communication systems. Izdatel'stvo Fiziko–matematicheskoj literatury **252**.

Emiroglu, S., A. Akgül, Y. Adıyaman, T. E. Gümüş, Y. Uyaroglu, *et al.*, 2022 A new hyperchaotic system from t chaotic system: dynamical analysis, circuit implementation, control and synchronization. Circuit World **48**: 265–277.

Fujisaka, H. and T. Yamada, 1983 Stability theory of synchronized motion in coupled-oscillator systems. Progress of theoretical physics **69**: 32–47.

Gaspard, P., 2005 Rössler systems. Encyclopedia of nonlinear science **231**: 808–811.

Hasan, A. N. and T. Shongwe, 2017 Impulse noise detection in ofdm communication system using machine learning ensemble algorithms. In *International Joint Conference SOCO'16-CISIS'16-ICEUTE'16: San Sebastián, Spain, October 19th-21st, 2016 Proceedings 11*, pp. 85–91, Springer.

Hedayatipour, A., R. Monani, A. Rezaei, M. Aliasgari, and H. Sayadi, 2022 A comprehensive analysis of chaos-based secure systems. In *Silicon Valley Cybersecurity Conference: Second Conference, SVCC 2021, San Jose, CA, USA, December 2–3, 2021, Revised Selected Papers*, pp. 90–105, Springer.

Kaddoum, G., 2016 Wireless chaos-based communication systems: A comprehensive survey. IEEE Access **4**: 2621–2648.

Kaddoum, G., M. Coulon, D. Roviras, and P. Chargé, 2010 Theoretical performance for asynchronous multi-user chaos-based communication systems on fading channels. Signal Processing **90**: 2923–2933.

Karimov, A., V. Rybin, E. Kopets, T. Karimov, E. Nepomuceno, *et al.*, 2023 Identifying empirical equations of chaotic circuit from data. Nonlinear Dynamics **111**: 871–886.

Karimov, T., O. Druzhina, A. Karimov, A. Tutueva, V. Ostrovskii, *et al.*, 2021a Single-coil metal detector based on spiking chaotic oscillator. Nonlinear Dynamics pp. 1–18.

Karimov, T., V. Rybin, G. Kolev, E. Rodionova, and D. Butusov, 2021b Chaotic communication system with symmetry-based modulation. Applied Sciences **11**: 3698.

Khan, A. M., V. Jeoti, M. Rehman, and M. Jilani, 2017 Noise power estimation for broadcasting ofdm systems. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–6.

Kharel, R., 2011 *Design and implementation of secure chaotic communication systems*. Ph.D. thesis, Northumbria University.

Koronovskii, A. A., O. I. Moskalenko, and A. E. Hramov, 2009 On the use of chaotic synchronization for secure communication. Physics-Uspekhi **52**: 1213.

Liao, T.-l., 1998 Adaptive synchronization of two lorenz systems. Chaos, Solitons & Fractals **9**: 1555–1561.

Liu, S.-H., D.-S. Wang, and L. Chen, 2007 Analysis of the ambiguity characteristic of digital synthesis signals with chaotic frequency modulation. ACTA ELECTONICA SINICA **35**: 1784.

Lukin, K. A. and O. V. Zemlyaniy, 2016 Digital generation of wide-band chaotic signal with the comb-shaped spectrum for communication systems based on spectral manipulation. Radioelectronics and Communications Systems **59**: 417–422.

Lyu, Y., L. Wang, G. Cai, and G. Chen, 2015 Iterative receiver for m-ary dcsk systems. IEEE Transactions on Communications **63**: 3929–3936.

Minati, L., M. Frasca, P. Oświecimka, L. Faes, and S. Drożdż, 2017 Atypical transistor-based chaotic oscillators: Design, realization, and diversity. Chaos: An Interdisciplinary Journal of Nonlinear Science **27**: 073113.

Moysis, L., C. Volos, I. Stouboulos, S. Goudos, S. Çiçek, *et al.*, 2020 A novel chaotic system with a line equilibrium: Analysis and its applications to secure communication and random bit generation. In *Telecom*, volume 1, pp. 283–296, MDPI.

Pecora, L. M. and T. L. Carroll, 1990 Synchronization in chaotic systems. Physical review letters **64**: 821.

Rajagopal, K., S. Çiçek, A. J. M. Khalaf, V.-T. Pham, S. Jafari, *et al.*, 2018 A novel class of chaotic flows with infinite equilibriums and their application in chaos-based communication design using dcsk. Zeitschrift Für Naturforschung A **73**: 609–617.

Rybin, V., D. Butusov, E. Rodionova, T. Karimov, V. Ostrovskii, *et al.*, 2022a Discovering chaos-based communications by recurrence quantification and quantified return map analyses. International Journal of Bifurcation and Chaos **32**: 2250136.

Rybin, V., T. Karimov, O. Bayazitov, D. Kvitko, I. Babkin, *et al.*, 2023 Prototyping the symmetry-based chaotic communication system using microcontroller unit. Applied Sciences **13**: 936.

Rybin, V., G. Kolev, E. Kopets, A. Dautov, A. Karimov, *et al.*, 2022b Optimal synchronization parameters for variable symmetry discrete models of chaotic systems. In *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–5, IEEE.

Rybin, V., A. Tutueva, T. Karimov, G. Kolev, D. Butusov, *et al.*, 2021 Optimizing the synchronization parameters in adaptive models of rössler system. In *2021 10th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, IEEE.

Shannon, C. E., 1984 Communication in the presence of noise. Proceedings of the IEEE **72**: 1192–1201.

Türkben, Ö. Ü. A. K. and V. S. A. Al-Akraa, 2022 Snr estimation in communication systems using cognitive radio. In *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, pp. 477–481, IEEE.

Tutueva, A., L. Moysis, V. Rybin, A. Zubarev, C. Volos, *et al.*, 2022 Adaptive symmetry control in secure communication systems. Chaos, Solitons & Fractals **159**: 112181.

Volos, C., I. Kyprianidis, and I. Stouboulos, 2013 Image encryption process based on chaotic synchronization phenomena. Signal Processing **93**: 1328–1340.

Voznesensky, A., D. Butusov, V. Rybin, D. Kaplun, T. Karimov, *et al.*, 2022 Denoising chaotic signals using ensemble intrinsic time-scale decomposition. IEEE Access **10**: 115767–115775.

Wang, L., X. Mao, A. Wang, Y. Wang, Z. Gao, *et al.*, 2020 Scheme of coherent optical chaos communication. Optics Letters **45**: 4762–4765.

Willsey, M. S., K. M. Cuomo, and A. V. Oppenheim, 2011 Quasi-orthogonal wideband radar waveforms based on chaotic systems. IEEE Transactions on Aerospace and Electronic Systems **47**: 1974–1984.

Yang, T. and L. O. Chua, 1996 Secure communication via chaotic parameter modulation. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **43**: 817–819.

Yang, Z., L. Yi, J. Ke, Q. Zhuge, Y. Yang, *et al.*, 2020 Chaotic optical communication over 1000 km transmission by coherent detection. Journal of Lightwave Technology **38**: 4648–4655.

How to cite this article: Rybin, V., Babkin, I., Kvitko, D., Karimov, T., Nardo, L., Nepomuceno, E., and Butusov, D. A Estimating Optimal Synchronization Parameters for Coherent Chaotic Communication Systems in Noisy Conditions. *Chaos Theory and Applications*, 5(3), 141-152, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.153-159
https://doi.org/10.51537/chaos.1246581

Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System

Berkay Emin[*,1] **and Zabit Musayev**[α,2]
[*]Department of Electronics and Automation, Osmancık Omer Derindere Vocational School, Hitit University, Corum, 19500, Turkiye, [α]Department of Electrical and Electronics Engineering,Faculty of Engineering and Architecture, Yozgat Bozok University, 66900 Yozgat, Turkiye.

ABSTRACT Digital data is increasing rapidly in the world day by day. Information security is important during data exchange over the Internet. The way to securely transmit images over the network is through the image encryption technique. In the proposed cryptography system, the hybridization of Lorenz-Rossler chaotic systems is used, and a random number sequence is generated. The security analyses such as histogram, correlation, differential attack, information entropy, and duration analysis of the study are performed. It is seen that the proposed system performs well, especially in terms of correlation. Additionally, the performance of the developed embedded system platforms is compared after testing on Nvidia Jetson Nano and Xilinx PYNQ Z1 boards. The Nvidia Jetson Nano board is more performant than the Xilinx PYNQ Z1 board. The safety and feasibility of the proposed system have been demonstrated.

KEYWORDS
Chaotic systems
Image encryption
Security analysis
Embedded systems

INTRODUCTION

With the development of technology and science, there has been an increase in the number of audio, video and other multimedia files in recent years. Data is mostly transferred to each other by people via the internet. This situation brings along information security (Ahmed *et al.* 2007). Especially military or health image data used in fields contain significant private information. The preservation of such images is very important in terms of information security. Therefore, the pixel values are changed to make the image incomprehensible before transferring the image. This is known as image encryption and is done with the help of a key.

Classical algorithms such as AES, RSA DES, and IDEA (Daemen and Rijmen 2020) have been recommended in the literature for image encryption. However, its use is often not considered appropriate due to its low speed. Many image encryption algorithms have been suggested as a way to solve the problem in the literature (Zhang and Karim 1999; Sinha and Singh 2003; Wang *et al.* 2020). Another method of image encryption is diffusion and confusion. During the confusion phase, the pixels are displaced.

During the diffusion process, the values of the pixels are changed. Usually, chaotic functions are used for this. Chaotic systems, on the other hand, are often used in image encryption operations due to their advantages such as unpredictability, pseudo-randomness, parameter sensitivity and initial value sensitivity (Zhang *et al.* 2016). When the literature in this field is examined, Al-Khasawneh and colleagues presented a new Chaos-based encryption technique using Henon, Logistic and Gaussian iterative maps and an external secret key. They applied this technique to images detected remotely (Al-Khasawneh *et al.* 2021). Akgül et al. designed a random number generator using a microcomputer-based, nonlinear chaotic system and implemented an image encryption application (Akgul *et al.* 2021). In the study, Wang et al. used the chaotic cat map for image encryption (Wang *et al.* 2009).

In this study, Lorenz-Rossler chaotic system and encryption-decryption algorithm are examined. The study's main purpose is to perform chaotic system-based RGB image encryption and decryption operations on embedded board platforms. Histogram, correlation, differential attack, information entropy and time analysis results and the obtained data are presented in the literature. It is expected that the encryption application applied on an embedded board basis will provide portability and usability due to its cost-effectiveness.

Manuscript received: 2 February 2023,
Revised: 5 April 2023,
Accepted: 16 June 2023.

---

[1] berkayemin@hitit.edu.tr (**Corresponding author**)
[2] zabit.musayev@bozok.edu.tr

MATERIAL AND METHODS

Lorenz-Rossler Chaotic System

The Lorenz-Rossler chaotic system was obtained by hybridizing two chaotic systems, Lorenz and Rossler, by Alsafasfeh and Al-Arni (Alsafasfeh and Al-Arni 2011). In this case, the control parameter has increased to six. The formula for the Lorenz-Rossler chaotic system is given in Equation 1.

$$\begin{aligned} \dot{x} &= (\delta - 1)y - \delta x - z, \\ \dot{y} &= (r+1)x - (1-a)y - 20xz, \\ \dot{z} &= 5xy - \beta z + b + xz - cx, \end{aligned} \tag{1}$$

Where delta,r,a,b,beta and c are the fixed control arguments and x,y,z are the system state variables. The researchers found the value delta = 20, r = 20, a = 9, beta = 8.5, b = 0 and c = 8 for the system to show chaotic properties. Differential equations are solved in the Google Colaboratory environment using the Runge-Kutta method with initial conditions x = 0.001, y = 0.001, z = 0.1 Figure 1 shows the chaotic behaviors of the Lorenz Rossler system.

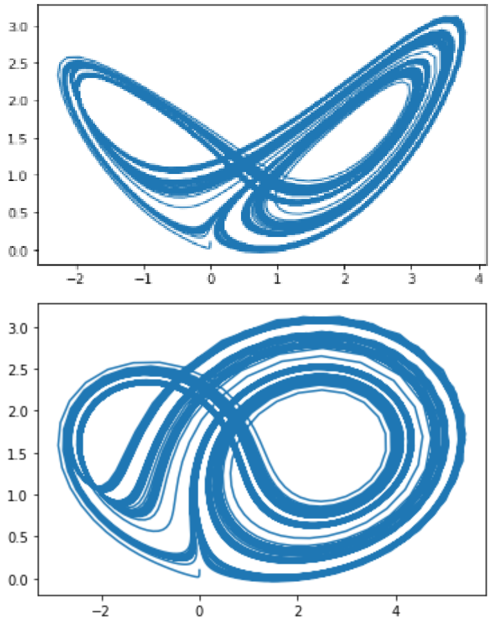


Figure 1 Attractors of Lorenz-Rossler System

Encryption and Decryption Algorithm

In the encryption process, the pixel positions of the image will be changed first. This process is called confusion. During the confusion phase, the positions of the pixels in the original image are mixed with controlled randomness. For this, a chaotic sequence is created using Equation 1. These arrays are used to encrypt the red, green and blue channels of the original view. The generated chaotic sequences are ordered from small to large and the sequences are obtained.

At the same time, the index of the values in the chaotic array is assigned to the array by sorting. Then, using these indexes, the picture is mixed. the confusion matrix is obtained separately for the three channels. The correlation coefficient between the blending process and adjacent pixels Decays, but the blended image continues to contain the statistical values of the original image. This indicates that the encryption process is not secure. In this case, the diffusion process is performed to increase encryption security.

At the propagation stage, the values of pixels are changed, the positions of which change in the process of confusion. Thus, the statistical values of the original image do not remain in the encrypted image. In the encrypted image, both pixel positions and pixel values are given in a different format from the original image. The pseudo-code for image encryption is given in Algorithm 1. The decryption algorithm, on the other hand, is the opposite of the image encryption algorithm.

Algorithm 1 Pseudo code of Image Encryption Algorithm

```
Input : Chaotic sequence and Image
Output : Encrypted Image
1: START
2: x,y,z chaotic sequence and image data
3: Split the image into R,G,B channels (imageR,imageG,imageB)
4: Get the dimensions of the image (m,n)
5: Normalize x,y,z chaotic arrays (x',y',z')
6: Sort the sequences x', y' and z' and mix the image R,G,B channels using the obtained index values. (shfR,shfG,shfB)
7:
    for $i = 0; m \times n$ do
        $encimgR[i] = x'[i]$ XOR $shfR[i]$
        $encimgG[i] = y'[i]$ XOR $shfG[i]$
        $encimgB[i] = z'[i]$ XOR$shfB[i]$
8: Merge encrypted R,G,B channels
9: EXIT
```

Image Encryption on NVIDIA Jetson Nano and Xilinx Pynq Z1 Embedded Boards

The proposed encryption and decryption algorithm was implemented on Nvidia Jetson Nano and Xilinx PYNQ Z1 platforms. General specifications of embedded boards are given in Table 1. Linux is installed as the operating system on both embedded system boards and the code written in Python on the Linux operating system is run on the system.The structure of the application of the proposed method to embedded boards is given in Figure 2. 256×256×3 peppers and 512×512×3 baboon images were used for encryption in both embedded boards.

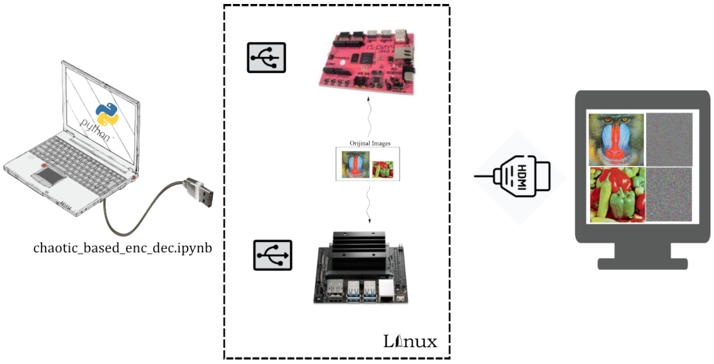


Figure 2 Application of the Proposed Method in Hardware

Table 1 The General Features of Embedded Boards

	 Xilinx Pynq Z1	 **Nvidia Jetson Nano**
GPU	ZYNQ XC7Z020-1CLG400C	NVIDIA Maxwell, 128 CUDA cores
CPU	650MHz dual-core Cortex-A9	Quad-core ARM Cortex-A57 MP-Core
Memory	512MB DDR3	4 GB 64-bit LPDDR4
Data storage	MicroSD card	MicroSD card
Power	7W-15W	5W-10W
Network	Gigabit Ethernet	Gigabit Ethernet
Other	16-pin GPIO	40-pin GPIO
Programmable logic	Artix-7 FPGA 13,300 logic segments, each with four 6-input LUTs and 8 flip-flops	-

RESULTS AND DISCUSSION

Histogram Analysis

The dispersion of pixel values in an image is revealed by histogram analysis. Color distribution in the original image According to the colors contained in the image, the histogram graph concentrates on a particular region and shows an uneven distribution. In the encryption process, the color distributions of the channels are equalized. Therefore, the histogram distributions of the original and encoded images must be different. All pixels of the encrypted image must be equally distributed in space. Therefore, the histogram distribution of the encrypted image should be uniform. In this direction, histogram analysis of the encrypted treat was performed.

Histogram graphics of the RGB channels of the original baboon image in Figure 3 (a-d) and the original peppers image in Figure 3 (i-l) are shown. When Figure 3 (a-d) and Figure 3 (i-j) are examined, it is seen that the color distributions in the original painting are uneven. The histogram graph of the RGB channels of the encrypted baboon image in Figure 3 (e-h) and the encrypted peppers image in Figure 3 (m-p) are shown. When Figure 3 (e-h) and Figure 3 (m-p) are examined, it is seen that the color distributions of the RGB channels are evenly distributed. This shows that the histogram of the encrypted image cannot be inferred and that the proposed encryption is secure.

Correlation Analysis

Correlation analysis (Cohen 1988) Decodes the linear relationship between two random variables. As a result of this analysis, the correlation coefficient was determined. Equation 2 using it, the correlation coefficient of a sequence with “n” elements is calculated, where x and y are two random variables.

$$\mathrm{r}_{\mathrm{xy}} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{2}$$

Hence;

$$\mathrm{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - \mathrm{E}(x)][y_i - \mathrm{E}(y)]$$

$$\mathrm{D}(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - \mathrm{E}(x)]^2$$

$$\mathrm{E}(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$$

The x and y values in the equation symbolize the two contiguous pixels in the image, and N indicates the number of pairs of pixels chosen. In our study, horizontal, vertical and diagonal pixel values were taken into account to calculate the pixel correlation in the original and encrypted images. Correlation analysis was performed for each R, G and B channel of peppers and baboon images. The horizontal correlation maps of the R, G, B channels of the peppers and baboon images are respectively shown

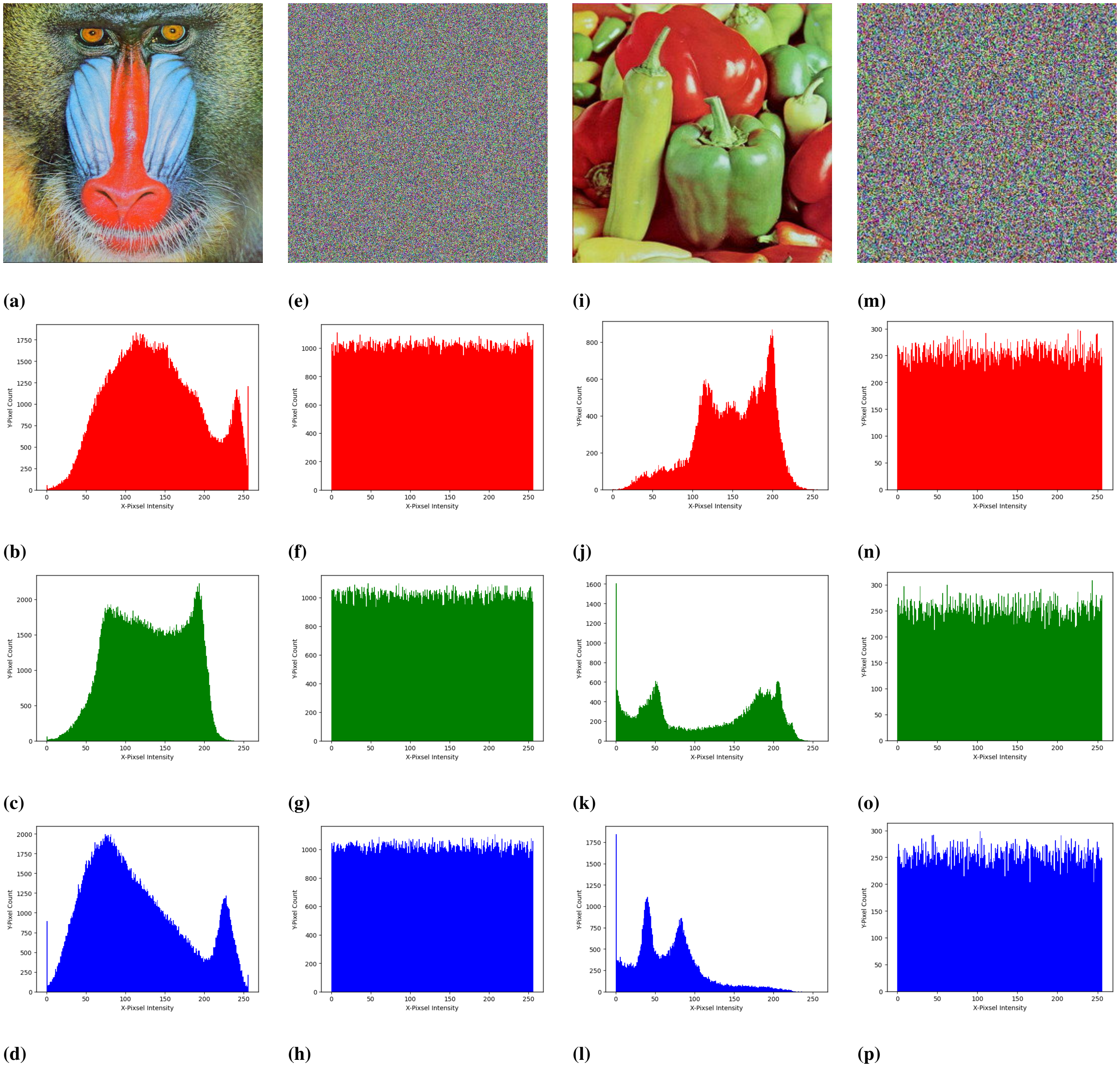


Figure 3 Histogram Graph of the Original and Encrypted Baboon-Peppers Image

in Figure 4 and Figure 5. The obtained correlation coefficient values and their comparison with the literature are given in Table 2.

The correlation cannot be less than -1 and greater than +1. The fact that the correlation coefficient is very close to -1 and +1 means that the relationship between pixel values is strong and that it is close to zero means the relationship between pixel values is weak. When Table 2 is examined, it is seen that the correlation coefficients to the original image are close to one. On the other hand, it is observed that the correlation coefficients of encrypted images for RGB channels are approximately zero. The results obtained are in harmony with recent studies in the literature. According to the results of correlation analysis, it can be said that the image encryption method performed successfully performs the encryption process.

Differential Attack Analysis (NPCR-UACI)

NPCR ("Number of Pixels Change Rate") and UACI ("Unified Average Changing Intensity") analyzes Differential cryptanalysis developed by Biham and Shamir (Biham and Shamir 1990) to examine how minor changes in the original image affect the encrypted images. NPCR is a metric that measures the rate of pixel change in an image. The NPCR value is calculated as given in Equation 3. The matrix D(i,j) in Equation 3 is calculated from Equation 4. Here, A and B represent the pixel value of the original and encrypted images, respectively. $M \times N$ represents the size of the encrypted image.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \qquad (3)$$

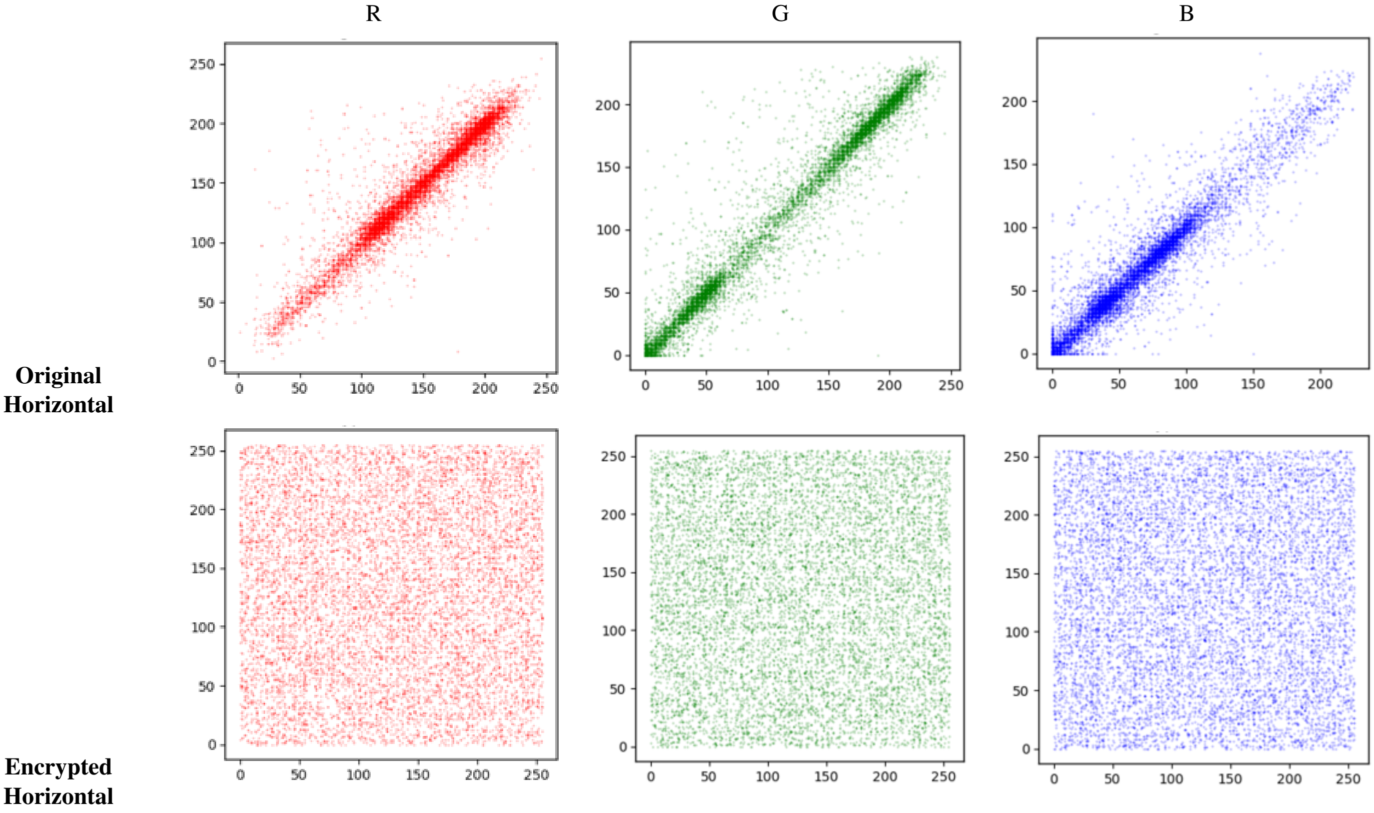


Figure 4 The horizontal correlation coefficient maps of the R, G, B channels of peppers

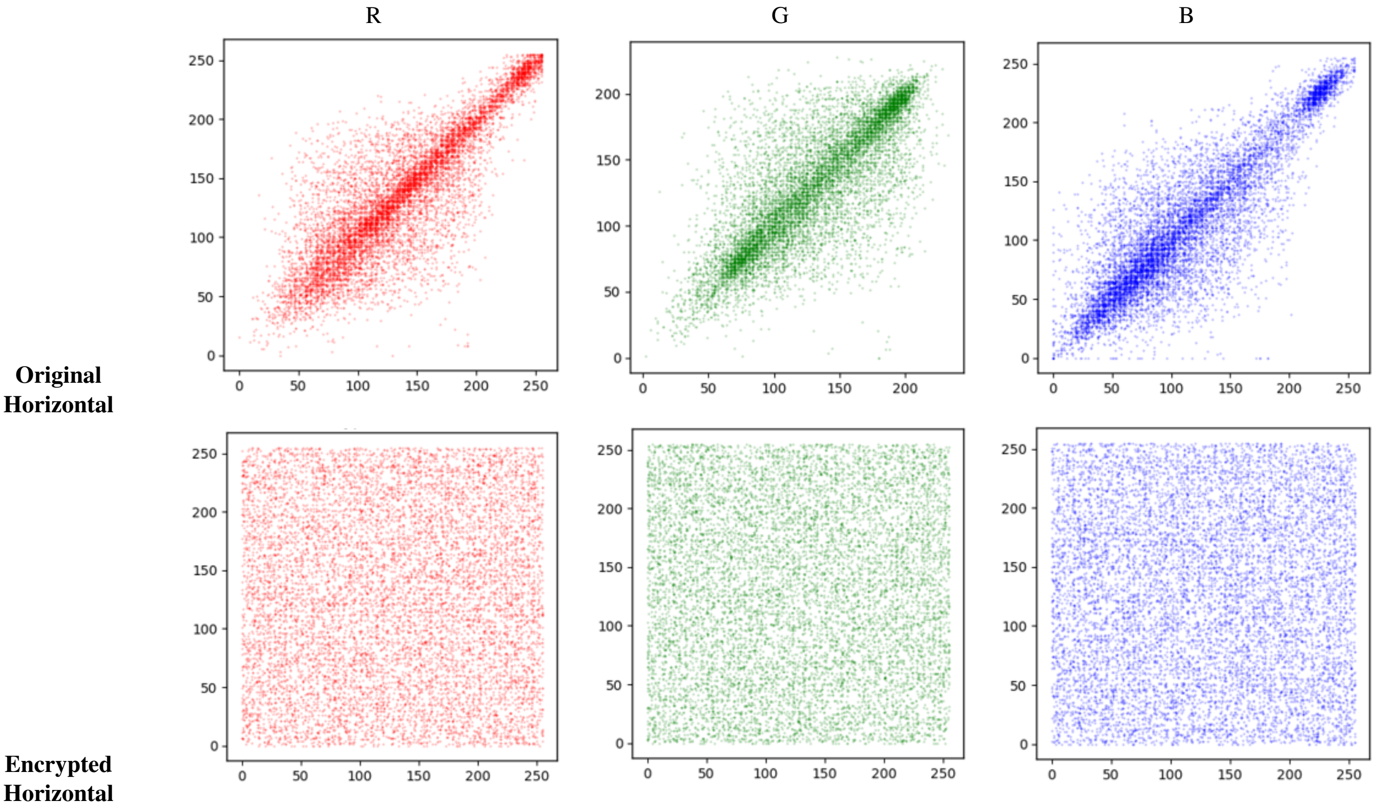


Figure 5 The horizontal correlation coefficient maps of the R, G, B channels of baboon

Table 2 Correlation Coefficients Values Comparison

		Original			Encrypted		
	Channel	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
proposed method (peppers)	**R**	0.9515	0.9463	0.9153	0.0181	-0.0007	-0.0011
	G	0.9759	0.9680	0.9487	0.0012	0.0157	-0.0079
	B	0.9472	0.9365	0.9050	-0.0019	0.0073	-0.0035
proposed method (baboon)	**R**	0.8512	0.9198	0.8449	0.0102	-0.0099	-0.0029
	G	0.7844	0.7599	0.9304	0.0025	0.0011	0.0026
	B	0.8736	0.9228	0.8529	0.0026	0.0024	-0.0153
(Xin *et al.* 2023) ***(512×512×3)***	**R**	0.9621	0.9646	0.9513	-0.0005	0.0004	0.0007
	G	0.9789	0.9774	0.9599	-0.0004	0.0002	0.0004
	B	0.9616	0.9628	0.9401	-0.0006	0.0003	0.0006
(Yan *et al.* 2023) ***(256×256×3)***	**R**	0.9904	0.9796	0.9701	0.0080	-0.0060	0.0026
	G	0.9820	0.9659	0.9547	-0.0092	-0.0090	0.00009
	B	0.9555	0.9324	0.9144	0.0060	-0.0069	0.0036
Demirtaş (2022) ***(512×512×3)***	**R**	0.9643	0.9635	0.9598	-0.0051	-0.0092	0.0012
	G	0.9808	0.9821	0.9695	0.0007	0.0068	-0.0034
	B	0.9645	0.9659	0.9455	0.0080	0.0014	-0.0052

$$\mathrm{D}(i,j) = \begin{cases} 1 & \text{if } A(i,j) \neq B(i,j) \\ 0 & \text{if } A(i,j) = B(i,j) \end{cases} \tag{4}$$

UACI is a metric that measures the average intensity of change in an image, calculated as given in Equation 5. The L value is the number of bits that express the pixel of the image.

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|A(i,j) - B(i,j)|}{2^L - 1}\right] \times 100 \tag{5}$$

In the literature, the most appropriate NPCR and UACI values are stated as NPCRopt = 99.61% and UACIopt =33.46% (Girdhar and Kumar 2018). In addition, NPCR, UACI values greater than 99.6% and close to or greater than 30%, respectively, is accepted as an indication of successful encryption (Praveenkumar *et al.* 2015).NPCR and UACI results are shown in Table 3. It is seen that the NPCR value is greater than 99.6% and the UACI value is close to 30% for both images used in the study. In addition, it was observed that the results were compatible with similar studies in the literature. Based on these results, it is clear that the developed encryption algorithm is strong against differential attacks.

Information Entropy Analysis

The encrypted data must be in such a way that no guesses can be made about the original data. Information entropy analysis measures the randomness in the encrypted image and demonstrates the average amount of information that the image carries. The entropy coefficient Equation 6 calculated by the given formula. Here, H (s) is the entropy value of the source, while N represents the bit value. In the literature, the ideal entropy value of the encrypted image is expected to be eight. The entropy test is applied to each of the RGB channels separately.

$$H(s) = \sum_{i=0}^{2^N-1} P(S_i) log_2 \frac{1}{P(S_i)} \tag{6}$$

Table 3 NPCR and UACI Results and Comparison

	NPCR	**UACI**
Proposed method (peppers)	99.6154	28.8371
Proposed method (baboon)	99.6067	29.9783
(Ali and Ali 2020)	99.6094	33.4635
(Yu *et al.* 2022)	99.6069	33.4422
(Sheela *et al.* 2018)	99.5865	28.6372

Table 4 Time Analysis of Embedded System (Unit: s)

	Embedded Board	**Encryption Time**	**Decryption Time**
proposed method (peppers)	Google Colaboratory Environment	0.6133	0.3978
	Xilinx PYNQ Z1	2.8670	6.6832
	Nvidia Jetson Nano	1.480	1.719
proposed method (baboon)	Google Colaboratory Environment	0.8842	1.3358
	Xilinx PYNQ Z1	11.4452	25.9610
	Nvidia Jetson Nano	5.8907	6.8535

The entropy values of the information obtained in the study and its comparison with the literature are given in Table ??. It is seen that the entropy values of the RGB channels of the encrypted images are close to 8. Therefore, it can be said that the proposed method is quite resistant to attacks.

Time Analysis

Operations performed on Google Colaboratory Environment were also performed on Xilinx PYNQ Z1 and Nvidia Jetson Nano embedded boards. Thus, the performances of different embedded boards in encryption and decryption processes were compared. In the table 4, the times obtained during the test phase are given in seconds. According to the results obtained, it is seen that the time in the software environment is more advantageous. In embedded platforms, it has been observed that the Nvidia Jetson Nano board is faster in encryption and decryption processes than the other boards.

CONCLUSION

In this study, an encryption algorithm is developed using Lorenz-Rossler chaotic systems. To measure the reliability of the designed system, histogram, correlation, differential attack, and information entropy analysis are performed. According to the results of the analysis, it has been determined that the developed encryption algorithm is resistant to attacks. Considering the experimental results, it has been observed that the proposed method allows the original image to be obtained again without any data loss. The application results obtained on embedded system boards are presented according to encryption and decryption duration comparatively. When the results are inspected, it is seen that the Nvidia Jetson Nano board is faster in encryption and decryption than the Xilinx PYNQ Z1. The authors are hopeful that a better, the mutually beneficial dialogue will gradually be established between the chaos and cryptography communities.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Ahmed, H. E. D. H., H. M. Kalash, and O. S. Farag Allah, 2007 An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for image encryption and decryption. Informatica (Ljubljana) .

Akgul, A., B. Gurevin, I. Pehlivan, M. Yildiz, M. C. Kutlu, *et al.*, 2021 Development of micro computer based mobile random number generator with an encryption application. Integration **81**: 1–16.

Al-Khasawneh, M. A., I. Uddin, S. A. A. Shah, A. M. Khasawneh, L. M. Abualigah, *et al.*, 2021 An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. Cluster Computing **25**: 999–1013.

Ali, T. S. and R. Ali, 2020 A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools and Applications **79**: 19853–19873.

Alsafasfeh, Q. H. and M. S. Al-Arni, 2011 A New Chaotic Behavior from Lorenz and Rossler Systems and Its Electronic Circuit Implementation. Circuits and Systems **02**: 101–105.

Biham, E. and A. Shamir, 1990 Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **4**: 3–72.

Cohen, J., 1988 *Statistical Power Analysis for the Behavioral Sciences*.

Daemen, J. and V. Rijmen, 2020 The Design of Rijndael: The Advanced Encryption Standard (AES). The Design of Rijndael .

Demirtaş, M., 2022 A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. Optik **265**: 0–2.

Girdhar, A. and V. Kumar, 2018 A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. Multimedia Tools and Applications .

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, 2015 Pixel scattering matrix formalism for image encryption-A key scheduled substitution and diffusion approach. AEU - International Journal of Electronics and Communications .

Sheela, S. J., K. V. Suresh, and D. Tandur, 2018 Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimedia Tools and Applications **77**: 25223–25251.

Sinha, A. and K. Singh, 2003 A technique for image encryption using digital signature. Optics Communications .

Wang, X., Y. Su, C. Luo, and C. Wang, 2020 A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling. PLoS ONE .

Wang, Y., K.-W. Wong, X. Liao, T. Xiang, and G. Chen, 2009 A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals **41**: 1773–1783.

Xin, J., H. Hu, and J. Zheng, 2023 3D variable-structure chaotic system and its application in color image encryption with new Rubik's Cube-like permutation. Nonlinear Dynamics .

Yan, S., L. Li, and B. Gu, 2023 *Design of a new four-dimensional chaotic system and its application to color image encryption*.

Yu, J., W. Xie, Z. Zhong, and H. Wang, 2022 Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. Chaos, Solitons and Fractals **162**: 112456.

Zhang, S. and M. A. Karim, 1999 Color image encryption using double random phase encoding. Microwave and Optical Technology Letters .

Zhang, Y. Q., X. Y. Wang, J. Liu, and Z. L. Chi, 2016 An image encryption scheme based on the MLNCML system using DNA sequences. Optics and Lasers in Engineering **82**: 95–103.

How to cite this article: Emin, B., and Musayev, Z. Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System. *Chaos Theory and Applications*, 5(3), 153-159, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.160-166
https://doi.org/10.51537/chaos.1276714

A New Secure Communications Scheme Based on a Chaotic Hybrid Optical Bistable System

Manal Messadi*,1, **Karim Kemih***,1 and **Hamid Hamiche**β,2
*L2EI Laboratory, Jijel University, Algeria, βL2CSP Laboratory, Mouloud Mammeri University, Tizi-Ouzou, Algeria.

ABSTRACT This paper presents a novel approach for secure communication utilizing a chaotic hybrid optical bistable system and chaotic modulation. The proposed crypto system encrypts the message at the transmitter using the chaotic hybrid optical bistable system with decorrelation operation to improve the chaotic sequence's performance. The encoded message is then injected into the dynamics of the chaotic memristor system. At the receiver, the synchronization of the two chaotic systems with passive control and predictive control allows for the recovery of the message through chaotic demodulation. The effectiveness of this approach is demonstrated through numerical simulation using medical images.

KEYWORDS
Chaotic synchronization
Passive control
Predictive control
Chaos-based cryptography
Chaotic demodulation

INTRODUCTION

The idea of using chaos in communication systems was inspired by the discovery of Pecora-Carroll (Pecora and Carroll 1990) in 1990. They showed that two identical chaotic systems with different initial conditions can possibly synchronize if they are suitably coupled, that is, under certain conditions.

In communication systems, synchronization is a very important key for successful transmission Halimi *et al.* (2014); Takhi *et al.* (2021); Zouad *et al.* (2019). The role of synchronization is to try to estimate some of the states of the dynamic system or sometimes unknown inputs. This means that two chaotic signals will be said to be synchronized if they are asymptotically identical when time tends to infinity. Sensitivity to initial conditions is a fundamental characteristic of chaotic systems, which makes chaotic synchronization seem difficult to achieve and presents more constraints. In the literature, there are several synchronization methods, synchronization by impulsive control Hamiche *et al.* (2011), observer-based synchronization Bouraoui and Kemih (2013); Kemih *et al.* (2011); Hamiche *et al.* (2021) and many other approaches Nestor *et al.* (2022); Tutueva *et al.* (2022); Kemih *et al.* (2014b); Roldán-Caballero *et al.* (2023).

One of the most important engineering applications of chaos synchronization is secure communication because of the properties of random behaviors and their sensitivity to initial conditions. For the purpose of establishing secure communication, the first step is to encrypt the signal that is intended to be transmitted. Encryption refers to the process of transforming the plain text signal into an unintelligible form so that unauthorized individuals cannot decipher the message content. Once the signal has been encrypted, it is sent to the receiver through a public channel. However, due to the open nature of the channel, it is possible for hackers to intercept and steal some information. This is where various encryption and decryption mechanisms come into play.

The receiver will utilize specific decryption mechanisms to reverse the encryption process and recover the original signal Chang *et al.* (2015). In the medical field, digital images consist of multimedia data that may contain confidential information. However, the development of a secure crypto system to safeguard the medical image content is a challenging task. In reference Bouhous and Kemih (2018), a new encryption approach is suggested utilizing optical time-delay chaotic systems and wavelets for data transmission. In Mohadeszadeh and Pariz (2022), to enhance the unpredictability of the information signal, the transmitted signals to the channel are deemed to be the fractional-order derivative of the product of the information signal and the chaotic system states.

To synchronize the master and slave systems, a proper adaptive fractional-order control law is derived on the receiver side using the Lyapunov stability theorem. Similarly, in Hashemi *et al.* (2020), the authors proposed a chaotic secure communication system between the base transmitter station and mobile equipment. By applying the Lyapunov stability theory and the finite-time synchronization concept, they designed a robust terminal sliding

---

Manuscript received: 4 April 2023,
Revised: 29 July 2023,
Accepted: 2 August 2023.

[1] messadi.manel@gmail.com (**Corresponding Author**)
[2] k.kemih@gmail.com
[3] hamid.hamiche@ummto.dz

mode controller. Furthermore, in Liao *et al.* (2021), the application of the Lu system to generate chaotic signals is proposed, which are then used to encrypt the biomedical information. Finally, using one of the states of the chaotic system, a simple proportional-derivative (PD) controller is designed to synchronize the master-slave chaotic systems for decrypting the biomedical information.

Motivated by the extent of previous work and on the other hand, adopting a combination-based transmission method can strengthen the security and complexity of the information transmission. In this work, we propose a novel encryption method based on a chaotic hybrid optical bistable system and chaotic modulation. In the existing results of chaos-based secure communication in literature, the transmitters are constructed with only one single chaotic system. In this paper, in order to enhance the security of the communication, we use two chaotic systems to construct the transmitter.

Our algorithm is composed of three steps: (1) encryption, (2) synchronization, and (3) extraction-decryption. The message is recovered by chaotic demodulation after synchronization of the two chaotic systems with passive control and predictive control. A numerical simulation with a medical image is provided to show the performance of the proposed approach.

The present work is structured as follows: Section 2 presents the proposed secure communications scheme, providing a brief description of the passive and predictive controllers. Section 3 details the design of the transmitter and receiver. Section 4 presents numerical simulations aimed at demonstrating the effectiveness of the proposed approach. Finally, Section 5 provides some concluding remarks.

THE PROPOSED SECURE COMMUNICATIONS SCHEME

Figure 1 summarizes the proposed secure communication scheme.

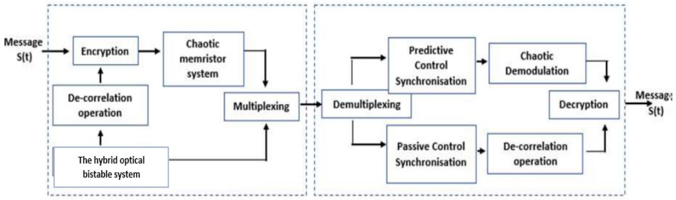


Figure 1 Proposed secure communication block diagram

Design of the Transmitter

The encryption sequence is generated using the hybrid optical bistable system Abdelouahab and Hamri (2012) at the transmitter:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= x_3 \\ \dot{x}_3 &= -ax_3 - x_2 + bx_1(1 - x_1^2) \end{aligned} \tag{1}$$

Where :x_1, x_2 and x_3 are the three states of the system and a and b the real constants. When system parameters $a = 0.5$ and $b = 0.65$,then, the system (1) exhibits a chaotic attractor as shown in Fig.2(a)-(b).

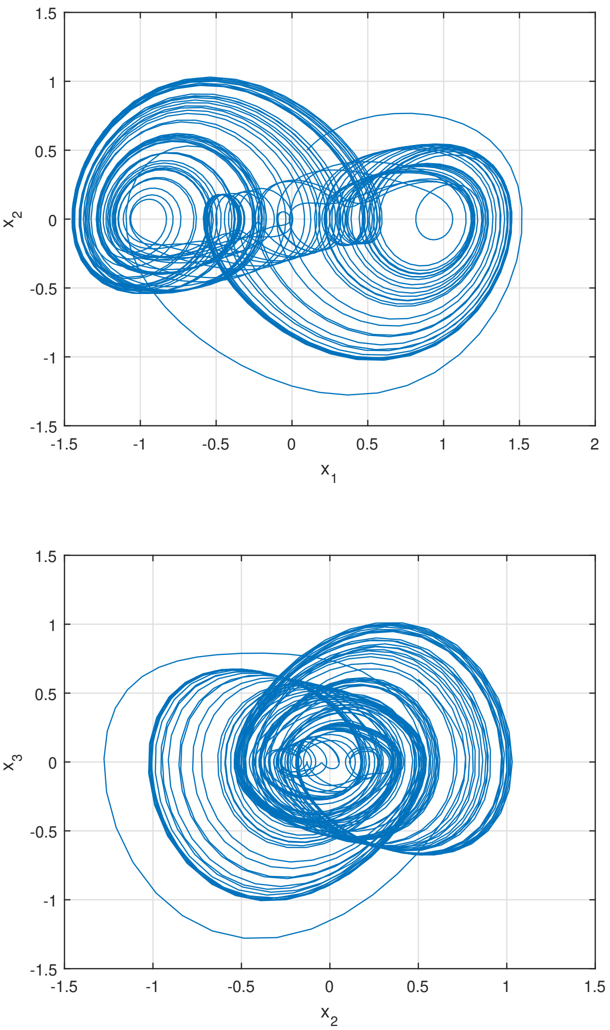


Figure 2 The phase portraits of system (1)

To optimize the performance of the chaotic sequence and its random statistical properties, the decorrelation operation was implemented using the following equations Liu *et al.* (2018):

$$S_1 = x_1 * 10^4 - floor\left(x_1{}^{*}10^4\right), \tag{2}$$

S_1 is the output sequence.

Fig. 3 represents an understanding between a chaotic sequence and the decorrelation result of a chaotic sequence. As we can see, this operation allows use to enhance the performance of the chaotic sequence and the random statistical properties.

The nonlinear encryption function is as follows:

$$G = 0.1 * (S_1^2 + S_1 m_t(t)) \tag{3}$$

Subsequently, the coded message is incorporated into the behavior of the chaotic memristor system for transmission and is governed by the subsequent equation Bao *et al.* (2011):

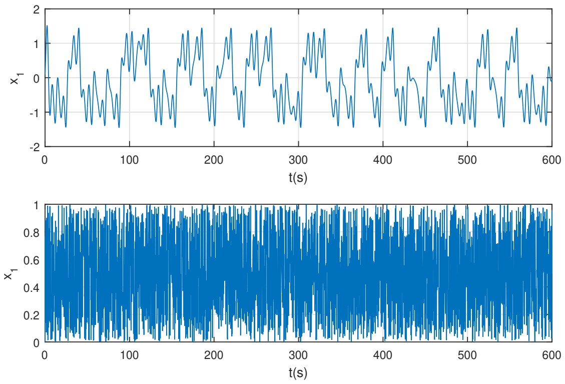


Figure 3 The chaotic sequence and the decorrelation result of chaotic sequence

$$
\begin{aligned}
\dot{x}x_1 &= xx_2 + G \\
\dot{x}x_2 &= \alpha(xx_3 - (3bxx_1{}^2 - a)xx_2) \\
\dot{x}x_3 &= x_2 - \gamma xx_3 + xx_4 \\
\dot{x}x_4 &= \beta xx_3
\end{aligned} \tag{4}
$$

where α, β, γ, a and b the real constants. When system parameters $\alpha = 21$, $\beta = 48$, $\gamma = 0.6$, $a = 1/7$, and $b = 2/7$, system (4) Manifests a chaotic attractor, as demonstrated in Fig.3(a)-(b).

Design of the receiver

The receiver is comprised of two chaotic systems that are exactly the same as the ones used in the transmitter. The primary purpose of these systems is to synchronize the signals between the transmitter and the receiver. This synchronization is crucial in order to demodulate and decrypt the received signal.

Synchronization of the chaotic The hybrid optical bistable system with passive control

Passivity based control : Considering the nonlinear system presented in the following:

$$
\begin{aligned}
\dot{x}\,(t) &= f\,(x\,(t)\,, u\,(t)) \\
y\,(t) &= h\,(x\,(t))
\end{aligned} \tag{5}
$$

$u(t)$ is the input vector and $y(t)$ is the output vector.

Definition 1 (Kemih *et al.* (2007); Yu (1999)). System (5) is said to be at " phase minimum" if the dynamic zero is asymptotically stable.

Definition 2 (Kemih *et al.* (2007); Yu (1999)). System (5) is considered passive if there exists a real constant β such that the following inequality is satisfied for all $\forall t \geq 0$:

$\int_0^t u^T(\tau)\ y(\tau) \geq \beta$ and

$$
\int_0^t u^T(\tau)\ y(\tau)\ dt + \beta \geq \int_0^t \rho y^T(\tau)\ y(\tau)\ d\tau \tag{6}
$$

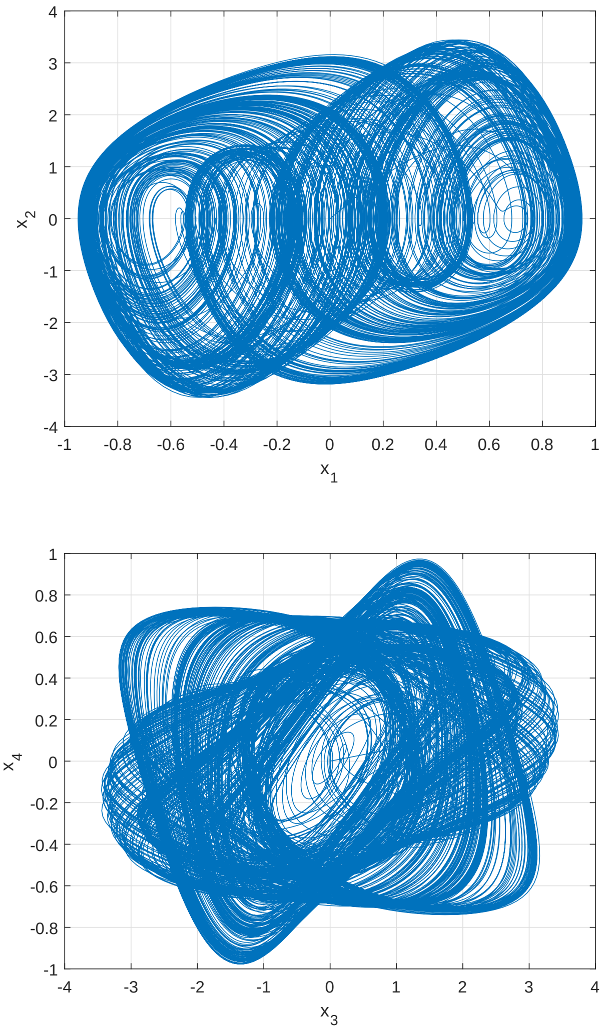


Figure 4 The phase portraits of system (4)

The definition implies that in a passive nonlinear system, the rise in stored energy is solely attributable to an external source.

System (5) in the ordinary form Yu (1999) :

$$
\begin{aligned}
\dot{z} &= f\,(z) + g\,(z, y)\,y \\
\dot{y} &= l\,(z, y) + k\,(z, y)\,u
\end{aligned} \tag{7}
$$

If System (5) is in the minimum phase, then the nonlinear system (7) could be treated as a passive system and stabilized asymptotically at equilibrium points through the use of closed-loop control in the form presented in references [23-24]:

$$
u = k(z, y)^{-1}\left[-l\,(z, y) - \frac{\partial W\,(z)}{\partial z} g\,(z) - \gamma y + \eta\right] \tag{8}
$$

Where $W(z)$ is Lyapunov's function of $f_0\,(z)$, γ is a positive value and η is an external signal connected to the reference input.

Synchronization of the chaotic hybrid optical bistable system by passive control: In this section, we will utilize the passive command to synchronize the chaotic hybrid optical bistable system. The equation (1) represents the master system, and the slave system is described as:

$$\begin{aligned} \dot{p}_1 &= p_2 + u_1 \\ \dot{p}_2 &= p_3 + u_2 \\ \dot{p}_3 &= -ap_3 - p_2 + bp_1(1 - p_1^2) \end{aligned} \tag{9}$$

we assume that the error is:

$$e = (e_1, e_2, e_3)^T = (p_1 - x_1, p_2 - x_2, p_3 - x_3)^T \tag{10}$$

We get the equations for the synchronization error, as follows:

$$\begin{aligned} \dot{e}_1 &= e_2 + u_1 \\ \dot{e}_2 &= e_3 + u_2 \\ \dot{e}_3 &= -ae_3 - e_2 + bp_1(1 - p_1^2) - bx_1(1 - x_1^2) \end{aligned} \tag{11}$$

after simplification, we get:

$$\begin{aligned} \dot{e}_1 &= e_2 + u_1 \\ \dot{e}_2 &= e_3 + u_2 \\ \dot{e}_3 &= -ae_3 - e_2 + be_1 - be_1^3 - 3be_1^2 x_1 - 3be_1 x_1^2 \end{aligned} \tag{12}$$

We start by rewriting the system in the form of a passive system (7), for that, we choose: $z_1 = e_3, y_1 = e_1, y_2 = e_2$.

Which allows us to get: $[f(z) = [-az_1], g(z,y) = [b - by_1^2 - 3by_1 x_1 - 3by_1^2, -1], l(z,y) = [y_2, z_1]^T, k(z,y) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

We take:

$$V(z,y) = W(z) + \tfrac{1}{2}y_1^2 + \tfrac{1}{2}y_2^2 \tag{13}$$

Where $W(z)$ is a Lyapunov function, with $W(0) = 0$:

$$W(z) = \tfrac{1}{2}z_1^2 \tag{14}$$

The calculation of the derivative of the Lyapunov function as a function of time is as follows:

$$\frac{dW(z)}{dt} = -az_1^2 \leq 0.$$

The dynamic zero of the synchronization error is stable in the sense of Lyapunov. The derivative $\frac{dW(z)}{dt}$ along the dynamics of the error system (12) is given as follows :

$$\frac{dV(z,y)}{dt} = \frac{\partial W(z)}{\partial z} \times \dot{z} + y \times \dot{y}$$

$$= \tfrac{\partial W(z)}{\partial z} f(z) + \tfrac{\partial W(z)}{\partial z} g(z,y)y + l(z,y)y + k(z,y)uy \tag{15}$$

Since :

$$\tfrac{dW(z)}{dz} f(z) \leq 0 \tag{16}$$

Then equation (15) becomes:

$$\tfrac{dV(z,y)}{dt} \leq \tfrac{\partial W(z)}{\partial z} g(z,g)y + (l(z,y) + k(z,y)u)y \tag{17}$$

Closed-loop control is selected in the form :

$$u = k^{-1}(z,y)\left[-l(z,y) - \frac{\partial W(z)}{\partial z} g(z,y) - \gamma y + v\right] \tag{18}$$

If we consider (18), we find :

$$u = \begin{bmatrix} -e_2 - be_3 + by_1^2 e_3 + 3by_1 x_1 e_3 + 3by_1^2 e_3 - \gamma e_1 \\ -\gamma e_2 \end{bmatrix} \tag{19}$$

Where γ is a positive constant. When substituting (18) into (17), we get:

$$\frac{\partial V(z,y)}{\partial t} \leq -\gamma y^2 + vy \tag{20}$$

Integrating (20) gives us:

$$V(z,y) - V(z_0,y_0) \leq \int_0^t -\gamma y^2(\tau)d\tau + \int_0^t v(\tau)y(\tau)d\tau \tag{21}$$

$V(z,y) \geq 0$ and $\rho = V(z_0,y_0)$

$$\int_0^t v(\tau)y(\tau)d\tau + \rho \geq V(z,y) + \int_0^t \gamma y^2(\tau)d\tau \geq V(z,y) \tag{22}$$

The relation (22) satisfies the definition of passivity given by the equation (6), so the synchronization error system (12) is strictly passive.

The error synchronization for all states is plotted in Fig. 5. We see that the state estimation effect is satisfactory.

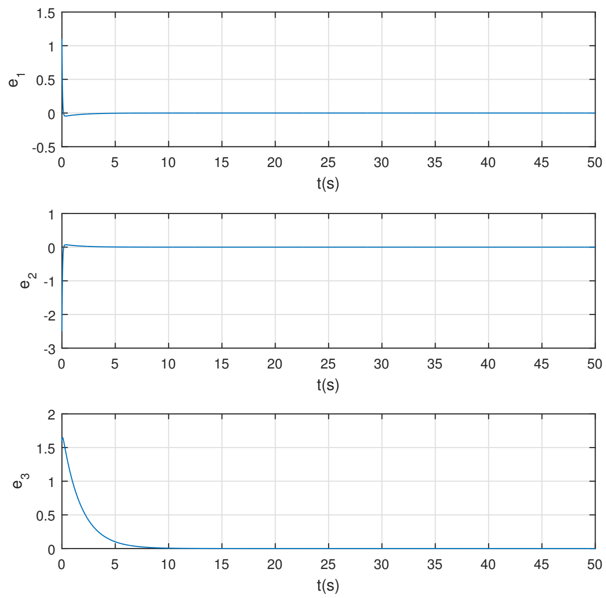


Figure 5 The synchronization error results between the chaotic hybrid optical bistable system transmitter/receiver

Predictive control: The controlled nonlinear system, in which chaos is to be suppressed, is represented as:

$$\dot{x}(t) = f_1(x(t)) + u_1(t) \tag{23}$$

The aim of predictive feedback control is to achieve asymptotic convergence of the system to either a stable fixed point or an unstable periodic orbit x_f

The fixed point or equilibrium point of the system (23) is the point x_f such as:

$$\frac{dx}{dt} = \dot{x} = f_1\left(x_f\right) = 0 \tag{24}$$

As part of predictive control, the command form $u_1(t)$ is chosen as the following form Messadi *et al.* (2015); Boukabou *et al.* (2008); Messadi and Mellit (2017); Wang and Wang (2003) :

$$u_1(t) = K(x_p(t) - x(t)) \tag{25}$$

Where : K represents the gain and $x_p(t)$ Represents the predicted state.

By making a one-step prediction ahead, we get:

$$u_1(t) = K(\dot{x}(t) - x(t)) \tag{26}$$

Synchronization of the chaotic memristor system by the predictive control We will apply predictive control to synchronize the chaotic memristor system. The master system is described by equation (4) and the slave system is:

$$\begin{aligned}
\dot{yy}_1 &= yy_2 + u_1 \\
\dot{yy}_2 &= \alpha(yy_3 - [yy_3 - (3byy_1{}^2 - a)yy_2] + u_2 \\
\dot{yy}_3 &= yy_2 - \gamma yy_3 + yy_4 + u_3 \\
\dot{yy}_4 &= -\beta yy_3 + u_4
\end{aligned} \tag{27}$$

The system is asymptotically synchronized in the sense that: $\lim_{t\to\infty} e(t) \to 0$

First of all, we start by calculating the error between the transmitter / receiver systems :

$[ee_1\ ee_2\ ee_3\ ee_4]^T = [yy_1 - xx_1\ yy_2 - xx_2\ yy_3 - xx_3\ yy_4 - xx_4]^T$

$$\begin{aligned}
\dot{ee}_1 &= ee_2 + u_1 \\
\dot{ee}_2 &= \alpha[ee_3 - \ (3byy_1{}^2 - a)yy_2 + (3bxx_1{}^2 - a)xx_2] + u_2 \\
\dot{ee}_3 &= ee_2 - \gamma ee_3 + ee_4 + u_3 \\
\dot{ee}_4 &= -\beta ee_3 + u_4
\end{aligned} \tag{28}$$

Based on equations (26), (28) and applying the LMIs we obtain the value of the matrix K as follows:

$$K = \begin{bmatrix} 4.7238 & -1 & -1 & -2.3619 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 \end{bmatrix} \tag{29}$$

And the command will have the following formula:

$$u_1\,(t) = K\,(\dot{ee}\,(t) - ee\,(t))$$

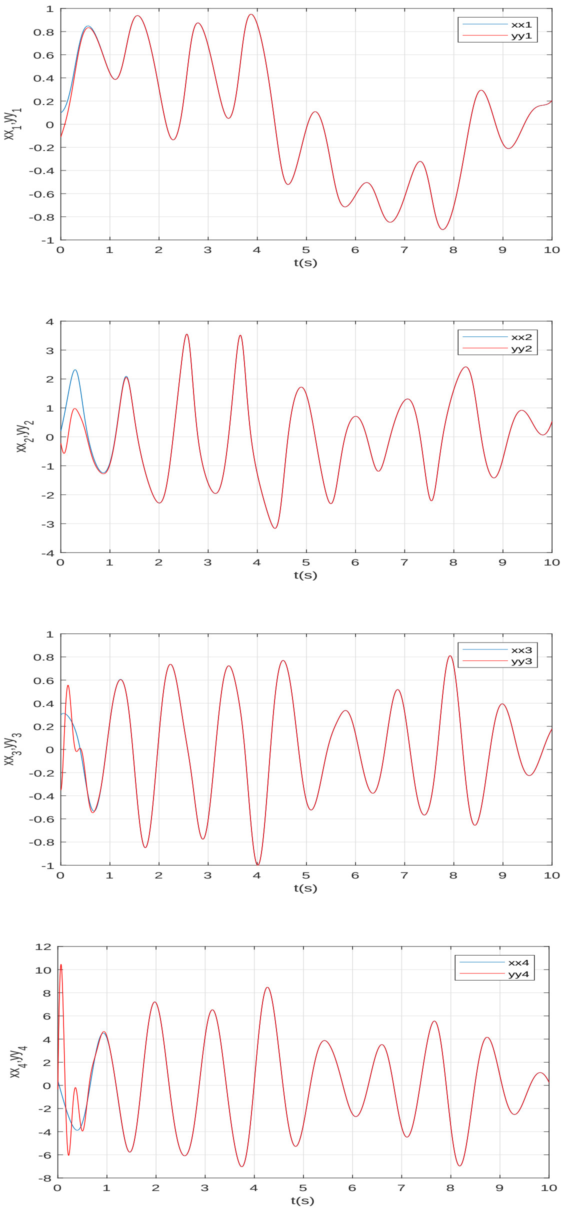


Figure 6 The synchronization results between the chaotic memristor transmitter/receiver

The chaotic 4D Memristor synchronization for all states is plotted in Fig. 5. We see that the state estimation effect is satisfactory.

To restore the message transmitted by inclusion at the receiver, we will use chaotic demodulation Wang and Wang (2003).

$$\begin{cases} \frac{dQ}{dt} = -\xi K\left(yy_1 + \xi \hat{G}(t)\right) \\ \hat{G}(t) = \xi K xx_1(t) + Q \end{cases} \tag{30}$$

$\widehat{\mathrm{G}}$ (t) the reconstructed signal

to decrypt the reconstructed signal, we use the following nonlinear function : $\widehat{m_r}(t) = (\widehat{G}(t) - \widehat{SS}^2(t))/\widehat{SS}(t)$ where $SS(t) = y_1(t) * 10^4 - floor\left(y_1(t)^* 10^4\right)$

To show the effectiveness of the proposed encryption system. we will first transmit a square signal of frequency f = 30 Hz. The

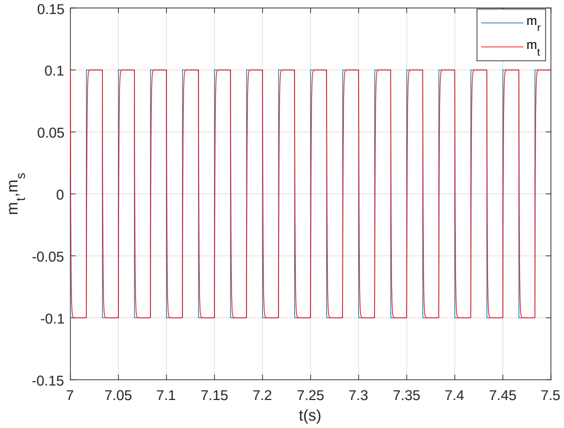


Figure 7 The transmitted message and the reconstructed message

performance of the proposed approach is shown in Fig. 6. As it can be seen in Fig 7, the original and recovered messages are nearly the same.

In the field of medicine, digital images are considered multimedia data that often contains confidential and sensitive information. Due to the highly sensitive nature of such information, it is imperative to protect digital medical images with a robust crypto system that can prevent unauthorized access or misuse. However, designing an effective crypto system that can safeguard medical image content poses a significant challenge due to the complexity and variety of medical imaging modalities. One of the alternatives to solving this problem is the approach proposed in this article. Fig. 8.a shows the original version of the medical image. Fig. 8.b shows the encrypted image, and Fig. 8.c shows the received and decrypted images. These simulation results demonstrate the feasibility of a secure communication strategy for the transmission of medical images.

CONCLUSION

In this study, we have put forward a new method for secure communication that relies on hybrid chaotic synchronization and chaotic modulation. The fundamental principle of the suggested method is straightforward: at the transmitter end, two chaotic systems are utilized to boost the security of communication. Specifically, the message is encrypted using the chaotic hybrid optical bistable system, and then the encoded message is incorporated into the dynamics of the chaotic memristor system. At the receiver end, the message is retrieved by means of chaotic demodulation after synchronization of the two chaotic systems with passive control and predictive control. To illustrate the efficacy of this approach, two examples have been presented, one based on a square signal and the other on medical imagery.

Availability of data and material

Not applicable.

Conflicts of interest

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

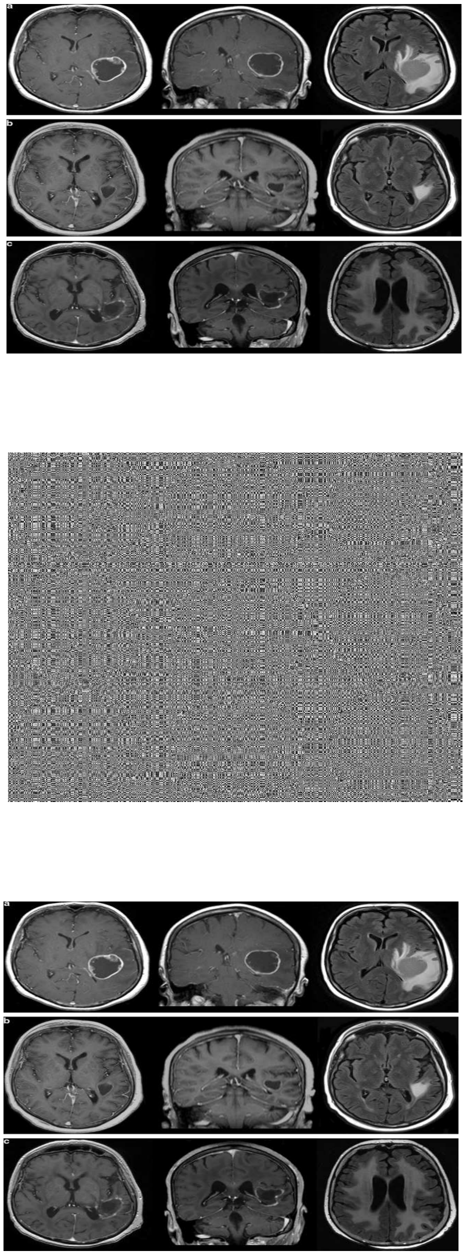


Figure 8 The original, transmitted and decrypted images (respectively)

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Abdelouahab, M.-S. and N.-E. Hamri, 2012 A new chaotic attractor from hybrid optical bistable system. Nonlinear Dynamics **67**: 457 – 463.

Bao, B., Z. Ma, J. Xu, Z. Liu, and Q. Xu, 2011 A simple memristor chaotic circuit with complex dynamics. International Journal of Bifurcation and Chaos **21**: 2629 – 2645.

Bouhous, A. and K. Kemih, 2018 Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission. Optics and Laser Technology **108**: 162 – 169.

Boukabou, A., A. Chebbah, and N. Mansouri, 2008 Predictive control of continuous chaotic systems. International Journal of Bifurcation and Chaos **18**: 587 – 592.

Bouraoui, H. and K. Kemih, 2013 Observer-based synchronization of a new hybrid chaotic system and its application to secure communications. Acta Physica Polonica A **123**: 259 – 262.

Chang, W.-D., S.-P. Shih, and C.-Y. Chen, 2015 Chaotic secure communication systems with an adaptive state observer. Journal of Control Science and Engineering **2015**.

Halimi, M., K. Kemih, and M. Ghanes, 2014 Circuit simulation of an analog secure communication based on synchronized chaotic chua's system. Applied Mathematics and Information Sciences **8**: 1509 – 1516.

Hamiche, H., K. Kemih, M. Ghanes, G. Zhang, and S. Djennoune, 2011 Passive and impulsive synchronization of a new four-dimensional chaotic system. Nonlinear Analysis, Theory, Methods and Applications **74**: 1146 – 1154.

Hamiche, H., H. Takhi, M. Messadi, K. Kemih, O. Megherbi, *et al.*, 2021 New synchronization results for a class of nonlinear discrete-time chaotic systems based on synergetic observer and their implementation. Mathematics and Computers in Simulation **185**: 194 – 217.

Hashemi, S., M. A. Pourmina, S. Mobayen, and M. R. Alagheband, 2020 Design of a secure communication system between base transmitter station and mobile equipment based on finite-time chaos synchronisation. International Journal of Systems Science **51**: 1969 – 1986.

Kemih, K., Y. Bennane, H. Bouraoui, and M. Ghanes, 2014a Synchronization of chaotic satellites systems. Nonlinear Phenomena in Complex Systems **17**: 203 – 206.

Kemih, K., M. Benslama, S. Filali, W.-Y. Liu, and H. Baudrand, 2007 Synchronization of chen system based on passivity technique for cdma underwater communication. International Journal of Innovative Computing, Information and Control **3**: 1301 – 1308.

Kemih, K., M. Halimi, M. Ghanes, H. Fanit, and H. Salit, 2014b Control and synchronization of chaotic attitude control of satellite with backstepping controller. European Physical Journal: Special Topics **223**: 1579 – 1589.

Kemih, K., M. Halimi, M. Ghanes, and G. Zhang, 2011 An application of chaotic chua's system for secure chaotic communication based on sliding mode observer. AIP Conference Proceedings **1400**: 344 – 349.

Liao, T.-L., H.-C. Chen, C.-Y. Peng, and Y.-Y. Hou, 2021 Chaos-based secure communications in biomedical information application. Electronics (Switzerland) **10**: 1 – 19.

Liu, J., Y. Ma, S. Li, J. Lian, and X. Zhang, 2018 A new simple chaotic system and its application in medical image encryption. Multimedia Tools and Applications **77**: 22787 – 22808.

Messadi, M. and A. Mellit, 2017 Control of chaos in an induction motor system with lmi predictive control and experimental circuit validation. Chaos, Solitons and Fractals **97**: 51 – 58.

Messadi, M., A. Mellit, K. Kemih, and M. Ghanes, 2015 Predictive control of a chaotic permanent magnet synchronous generator in a wind turbine system. Chinese Physics B **24**.

Mohadeszadeh, M. and N. Pariz, 2022 An application of adaptive synchronization of uncertain chaotic system in secure communication systems. International Journal of Modelling and Simulation **42**: 143 – 152.

Nestor, T., A. Belazi, B. Abd-El-atty, M. N. Aslam, C. Volos, *et al.*, 2022 A new 4d hyperchaotic system with dynamics analysis, synchronization, and application to image encryption. Symmetry **14**.

Pecora, L. M. and T. L. Carroll, 1990 Synchronization in chaotic systems. Physical Review Letters **64**: 821 – 824.

Ramakrishnan, B., V. K. Tamba, J. Metsebo, D. Tokoue Ngatcha, and K. Rajagopal, 2023 Control, synchronisation and antisynchronisation of chaos in two non-identical josephson junction models via sliding mode control and its fpga implementation. Pramana - Journal of Physics **97**.

Roldán-Caballero, A., J. H. Pérez-Cruz, E. Hernández-Márquez, J. R. García-Sánchez, M. Ponce-Silva, *et al.*, 2023 Synchronization of a new chaotic system using adaptive control: Design and experimental implementation. Complexity **2023**.

Takhi, H., K. Kemih, L. Moysis, and C. Volos, 2021 Passivity based sliding mode control and synchronization of a perturbed uncertain unified chaotic system. Mathematics and Computers in Simulation **181**: 150 – 169.

Tutueva, A. V., L. Moysis, V. G. Rybin, E. E. Kopets, C. Volos, *et al.*, 2022 Fast synchronization of symmetric hénon maps using adaptive symmetry control. Chaos, Solitons and Fractals **155**.

Wang, X. F. and Z. Q. Wang, 2003 A robust demodulation approach to communications using chaotic signals. International Journal of Bifurcation and Chaos in Applied Sciences and Engineering **13**: 227 – 231.

Yu, W., 1999 Passive equivalence of chaos in lorenz system. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **46**: 876 – 878.

Zouad, F., K. Kemih, and H. Hamiche, 2019 A new secure communication scheme using fractional order delayed chaotic system: design and electronics circuit simulation. Analog Integrated Circuits and Signal Processing **99**: 619 – 632.

How to cite this article: Messadi, M., Kemih, K., and Hamiche, H. A New Secure Communications Scheme Based on a Chaotic Hybrid Optical Bistable System. *Chaos Theory and Applications*, 5(3), 160-166, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / **No.**3 / 2023 / **pp.**167-177
https://doi.org/10.51537/chaos.1316437

A Secure Communication System of Synchronized Chua's Circuits in LC Parallel Coupling

V Satya Prakash [*,β,1], **S Narender Reddy** [*,α,2] and **A Sadananda Chary** [*,α,3]
[*]Department of Physics, Osmania University,Hyderabad,500007, India, [β]Tara Govt College, Sangareddy, 502001, India, [α]JNTU College of Engineering, Hyderabad, 500085, India.

ABSTRACT Synchronization capability of two identical chaotic systems can be used for constructing the secure communication systems where the chaotic signal is used as the information carrier. In this paper, a secure communication system is designed by using the bi-directionally synchronized identical Chua's circuits in LC parallel coupling. LC parallel circuit is used as the new coupling element instead of using a single resistor or capacitor or inductor as the coupling element. This makes the complete synchronization of Chua's circuits possible for many different sets of coupling inductance and capacitance values so that the flexibility of constructing the secure communication systems is realized. Both the synchronized Chua's circuits in LC parallel coupling and the corresponding secure communication system are constructed by using the LTspice software. The simulation results show that the secure communication system proposed in the present paper is very efficient for the message transmission for different pairs of coupling inductance and coupling capacitance values where the complete synchronization of Chua's circuits is observed occur. The two essential properties of an ideal secure communication system - perfect message masking and recovery are observed when compared to other secure communication systems already proposed and constructed previously. So, the simulation results of the present study can be used for practically constructing the efficient communication systems in future.

KEYWORDS
Chua's circuit
Chaotic masking
Secure communication system
LC parallel coupling
Complete synchronization
LTspice.

INTRODUCTION

Chaotic systems in nature are very important because of their unusual properties. The Chua's circuit is an example of chaotic systems with rich chaotic properties (Zhong and Ayrom 1985; Chua 1992) .This circuit consists of three linear energy storage elements - one inductor, two capacitors, one linear resistor and one non-linear resistor. The nonlinear resistor can be constructed in several ways. However, for the practical implementation, this can be conveniently constructed in Kennedy's implementation by using the two identical op-amps like TL082 and six resistors. The synchronization of chaotic systems is an important property as it shows some cooperative nature within the chaotic realm of the system.Furthermore, the synchronized chaotic systems can be used for some important applications in the secure communication systems.

The synchronization of two Chua's circuits in linear coupling with a resistor, capacitor and inductor is already studied by the number of researchers (Leon O.Chua and Itoh 1992; V.V.Astakhov and V.S.Anishchenko 1997; Zhilong Liu and Zhang 2019; Yao *et al.* 2019; Zhang and Wang 2023) . So, there is the scope for using some combinations of such simple coupling devices as the coupling elements between the two Chua's circuits. This is very important not only to observe the nature of chaos in the synchronization transition but also to know the possibility of complete synchronization for the various sets of parameter values. Such flexibility of using various sets of parameter values for the complete synchronization is observed in the simulations when compared to the results of previous studies with any single coupling element.

There are several methods for design and construction of the chaos based communication systems. The important methods are chaotic masking, chaotic modulation and chaotic switching (H.Dedieu and M.Hasler 1993; Ogorzalek 1993; Koh and Ushio

---

Manuscript received: 20 June 2023,
Revised: 1 September 2023,
Accepted: 13 September 2023.

[1] satyaprakashvpet@yahoo.co.in (**Corresponding author**)
[2] snrouphy60@gmail.com
[3] aschary60@gmail.com

1997) . In the chaotic masking method,the analogue message signal is added to a strong chaotic signal (L. Kocarev and Parlitz 1992; Cuomo and Oppenheim 1993; K.M. Cuomo and Strogatz 1993; Wu and Chua 1993; I.P. Marino and Grebogi 1999; Adel Ouannas and Luong 2021; Bonny T. *et al.* 2023) .In chaotic modulation method, the analogue message signal is modulated by the chaotic signal whereas in chaotic switching method, the digital message signals are modulated by the chaotic attractors.

The main problem of the study is to construct a secure communication system based on the chaotic masking method where the two completely synchronized chaotic systems are necessary. The chaotic masking is the very fundamental method for building any secure communication system.The masking of the message signals can be realized by using the two completely synchronized chaotic systems -with one system acting as a transmitter while the other system acting as a receiver. The required complete synchronization can be realized by using either the uni-directionally or bi-directionally coupled chaotic systems. In bi-directional or mutual coupling, the two chaotic systems will influence each other whereas in uni-directional coupling only one system will influence the other. In this study, a bi-directional coupling of two identical Chua's circuits is used for achieving the complete synchronization.

Trejo-Guerra et al. experimentally implemented the secure chaotic communication system by using the uni-directionally coupled Chua's oscillators built with the commercially available positive-type second generation current conveyor CCII+ (Trejo-Guerra and Sanchez-Lopez 2009) .The uni-directionally synchronized Chua's circuits in secure communication systems is also studied by Mustafa Mamat et al. by using Matlab® and MultiSIM® softwares (Mustafa Mamat and Maulana 2013) .The difference between the two studies is that - the first one is the experimental study whereas the second one is a simulation study.

The secure communication systems with bi-directionally synchronized chaotic systems are also studied and constructed by many researchers over the time.Shuh-Chuan Tsay et al. are proposed and tested the feasibility of constructing the secure communication systems with the bi-directionally synchronized Lorentz and Chua's circuits (Shuh-Chuan Tsay and Chen 2004; Shuh-Chuan Tsay and Wu 2005) .A hardware demonstrator for chaotic cryptography and secure communications is also constructed by Emiliia Nazarenko et al. by using the synchronized Chua's circuits in a bi-directional line coupling (Emiliia Nazarenko and Katzenbeisser 2023)

So, now the two bi-directionally synchronized directly coupled identical Chua's circuits with a different coupling element called LC parallel circuit are proposed to construct a flexible and secure communication system.

In the present study, a secure communication system based on the chaotic masking method is proposed. The circuit construction, masking and recovery of the message signals are performed by using the LTspice software(LinearTechnology 2020, 2011) . A communication system is designed with the two bi-directionally synchronized identical Chua's circuits in direct LC parallel coupling. The values of the parameters L and C are chosen such that the complete synchronization is possible. Then, the message signal masking and recovery- the two key parameters of the efficient secure communication system are studied. The proposed system is proved to be flexible in construction and efficient in both signal masking and recovery when compared to the previously constructed secure communication systems.

METHODOLOGY

Mathematical Model of Coupled Chua's Circuits

Consider two Chua's circuits each one as shown in Fig.1. Let C_1, C_2 are the two capacitors, R is the linear resistor and L_1 is the inductor of the first Chua's circuit. Similarly, let C_3, C_4 are the two capacitors, R' is the linear resistor and L_2 is the inductor of second Chua's circuit. Suppose that these two Chua's circuits are coupled with a parallel combination of inductor L_3 and capacitor C_5 between the two positive ends of the capacitor C_1 of the first Chua's circuit and capacitor C_3 of the second Chua's circuit respectively. Non-linear resistor N_R of each Chua's circuit consists of two op-amps TL082 and six resistors in Kennedy's implementation.

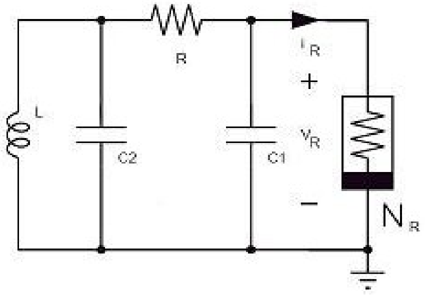


Figure 1 Basic schematic diagram of Chua's Circuit

The theory of coupled Chua's circuits can be obtained by applying the Kirchhoff's laws at the two ends of the resistance R and R' of the two Chua's circuits in the coupling:

Applying Kirchhoff's current laws at the two ends of the resistor R:

$$C_2\left(\frac{dV_{C_2}}{dt}\right) = I_{L_1} + \left(\frac{V_{C_1} - V_{C_2}}{R}\right) \tag{1}$$

where V_{C_1} is the voltage across the capacitor C_1
V_{C_2} is the voltage across the capacitor C_2
and I_{L_1} is the current passing through the inductor L_1
Similarly:

$$\left(\frac{V_{C_2} - V_{C_1}}{R}\right) = C_1\left(\frac{dV_{C_1}}{dt}\right) + f(V_{C_1}) - (I_{L_3} - I_{C_5}) \tag{2}$$

where f (V_{C_1}) is a function giving the characteristics of Chua's diode
$I_{L_3}$is the current passing through the coupling inductor L_3
and $I_{C_5}$is the current passing through the coupling capacitor C_5
Here the piecewise-linear function f (V_{C_1}) of the Chua's diode is given by:

$$f(V_{C_1}) = G_b V_{C_1} + 0.5(G_a - G_b)(|V_{C_1} + E| - |V_{C_1} - E|) \tag{3}$$

where G_a and G_b are the conductance values and E is the breaking point of the voltage

Since the voltage developed between the two ends of the capacitor with capacitance C_2 is equal to the voltage across the inductor L_1 :

$$-L_1\frac{dI_{L_1}}{dt} = V_{C_2} \tag{4}$$

where $I_{L_1}$is the current passing through the inductor L_1

Similarly:

$$-L_3\frac{dI_{L_3}}{dt} = V_{C_3} - V_{C_1} \tag{5}$$

where $I_{L_3}$is the current passing through the inductor L_3 and V_{C_3} is the voltage across the capacitor C_3

Applying the scale transformation of the variables, the dynamical equations in the dimensionless form are given by:

$$\dot{x} = \alpha[y - x - f(x) + \rho - \epsilon] \tag{6}$$

(or) using Eq.(5):

$$\dot{x} = \alpha[y - x - f(x) + \gamma(1-\delta)\int (x^{'} - x)d\tau] \tag{7}$$

$$\dot{y} = x - y + z \tag{8}$$

$$\dot{z} = -\beta y \tag{9}$$

where

$$\alpha = \frac{C_2}{C_1}, \beta = \frac{C_2R^2}{L_1}, \gamma = \frac{C_2R^2}{L_3} and \delta = \frac{I_{C_5}}{I_{L_3}} \tag{10}$$

$x = V_{C_1}/E$, $y = V_{C_2}/E$, $z = I_{L_1}R$ /E
τ = t/R C_2 , $\rho = (I_{L_3}R$ /E), $\epsilon = (I_{C_5}R$ /E)
and $\dot{x} = \left(\frac{dx}{d\tau}\right)$ etc.

Similarly, another set of equations are given by:

$$\dot{x^{'}} = \alpha^{'}[y^{'} - x^{'} - f(x^{'}) - \rho^{'} + \epsilon^{'}] \tag{11}$$

(or)

$$\dot{x^{'}} = \alpha^{'}[y^{'} - x^{'} - f(x^{'}) - \gamma^{'}(1-\delta^{'})\int (x^{'} - x)d\tau^{'}] \tag{12}$$

$$\dot{y^{'}} = x^{'} - y^{'} + z^{'} \tag{13}$$

$$\dot{z^{'}} = -\beta^{'} y^{'} \tag{14}$$

where

$$\alpha^{'} = \frac{C_4}{C_3}, \beta^{'} = \frac{C_4R^{'2}}{L_2}, \gamma^{'} = \frac{C_4R^{'2}}{L_3} and \delta^{'} = \frac{I_{C_5}}{I_{L_3}} \tag{15}$$

$x^{'} = \frac{V_{C_3}}{E}$, $y^{'} = \frac{V_{C_4}}{E}$ and $z^{'} = \frac{R^{'}I_{L_2}}{E}$
$\tau^{'}$ = t/$R^{'}C_4$, $\rho^{'} = (R^{'}I_{L_3}/E)$ and $\epsilon^{'} = (R^{'}I_{c_5}$/E)
and $\dot{x}^{'} = \left(dx^{'}/d\tau^{'}\right)$ etc.

For two identical Chua's circuits:

$\alpha = \alpha^{'}$, $\beta = \beta^{'}$ and $\gamma = \gamma^{'}$.

The difference equations are given by the differences p (τ), q (τ) and r (τ) defined by:

p (τ) = x (τ) - $x^{'}$ (τ)
q (τ) = y (τ) - $y^{'}$ (τ)
r (τ) = z (τ) - $z^{'}$ (τ)

From Eqs.(7), (8), (9) and Eqs.(12), (13), (14), the difference equations are given by:

$$\dot{p} = \alpha q - \alpha p - \alpha[f(x) - f(x^{'})] - 2[\gamma(1-\delta)]\int p d\tau \tag{16}$$

$$\dot{q} = p - q + r \tag{17}$$

$$\dot{r} = -\beta q \tag{18}$$

From the Eq. (16), it is clear that for $\delta = 1$, the difference equations decouple from each other.

Since, the non-linear part is given by: f(x) - f($x^{'}$) = $f^{'}(\eta)$(x-$x^{'}$) ; a<$f^{'}(\eta)$< 0, the equations assume the linear form:

$\dot{\xi}$ = A ξ

$$\text{where}\dot{\xi} = \begin{pmatrix} \dot{p} \\ \dot{q} \\ \dot{r} \end{pmatrix}, \xi = \begin{pmatrix} p \\ q \\ r \end{pmatrix} \text{ and}$$

$$A = \begin{pmatrix} -\alpha - f^{'}(\eta)\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & 0 \end{pmatrix} \tag{19}$$

When real parts of eigen values of the matrix A given by Eq.(19) are all negative, then the solutions of the system are stable. This is possible only when $f^{'}(\eta)\alpha > 0$. This makes the synchronization globally stable(Liao Xiao-Xin LUE Hai-Geng and XUBing-Ji 2005).

Scheme of Secure Communication System

There are four essential components in the secure communication system based on the two LC parallel coupled identical Chua's circuits, as shown in Fig.2.In this system, the masked signal s(t) which is transmitted from the transmitter is the sum of chaotic signal x(t) and the message signal m(t).When the two identical Chua's circuits are completely synchronized through LC parallel circuit, the chaotic signal produced at the receiver is identical to the chaotic signal produced at the transmitter. Then, this chaotic signal x(t) is subtracted from the masked signal s(t) by the using the difference amplifier at the receiver and the message signal m(t) is extracted.

Transmitter: Transmitter is mainly a Chua's circuit. It is used for producing the chaotic signal.

Summing amplifier: Summing amplifier is an integral part of the transmitter. It is used to mix the message signal with the chaotic signal produced by the transmitter.

Receiver: Receiver is mainly another Chua's circuit and it is used to produce an identical chaotic signal through the process of synchronization.

Difference amplifier: This circuit is an integral part of the receiver and it is used to subtract chaotic signal from the masked signal.

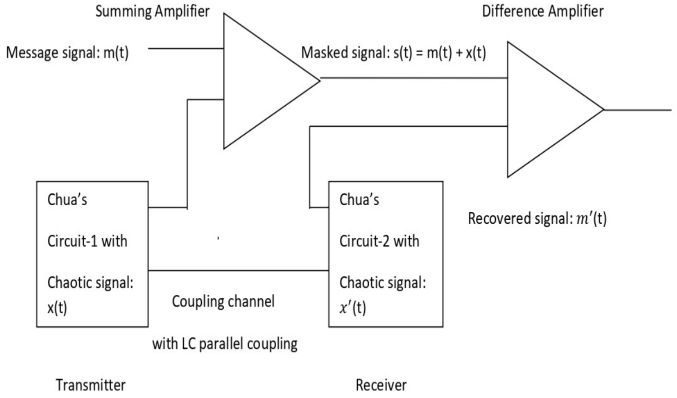


Figure 2 Schematic diagram of the secure communication system with two identical Chua's circuits in LC parallel coupling(at complete synchronization: $x^{'}$(t) = x(t) and $m^{'}$(t) = m(t))

Implementation in LTspice

LTspice is the Linear Technology's Simulation Programme with Integrated Circuit Emphasis. The basic version of this software was first developed at California University in the year 1972. The important feature of this software is that it is inexpensive and also consists of very extensive set of electronic component models. Apart from this, it facilitates the incorporation of some third party electronic device models like TL082 op-amp etc.

The two identical Chua's circuits in LC parallel coupling are constructed by using LTspice software, as shown in Fig.3. The components suggested in the Kennedy's paper are used, as shown in Table1(Kennedy 1992) . The synchronization is achieved by running the simulations for different values of the coupling inductance and coupling capacitance. The particular values for which the complete synchronization is observed to occur are used to construct the LC parallel coupled identical Chua's circuits to be used in constructing the secure communication systems.

The other supplementary sections of the communication system called summing amplifier and difference amplifier are also constructed by using the same LTspice software. Then, the secure communication system based on the two Chua's circuits in synchronization through LC parallel coupling is constructed, as shown Fig.4. The coupling used between two identical Chua's circuits is bi-directional as one Chua's circuit influences the other circuit and vice versa.

RESULTS AND DISCUSSION

Synchronization in LC parallel Coupling

Two Chua's circuits in LC parallel coupling are constructed with the components shown in Table1. Varying the inductance value L_3 for a fixed value of coupling capacitance of C_5=10 nF, the complete synchronization of the outputs of uncoupled capacitors in each Chua circuit is observed at the inductance values of L_3= 62 mH and 310 mH. This appears in Fig.5 and Fig.8 for the first and second cases respectively.

The synchronization errors up to 150 mV and 9 mV are observed in the first and second cases as shown in Fig.6 and Fig.9 respectively. The Lissajous figures confirming the complete synchronization in the first and second cases are given by the straight lines as shown in Fig.7 and Fig.10 respectively. Similarly, the complete synchronization of Chua's circuits is also observed at the coupling capacitance values of C_5= 2nF and 28nF at a fixed coupling inductance of L_3= 100mH. This can be seen in the first and second cases as shown in Fig.11 and Fig.14 respectively.

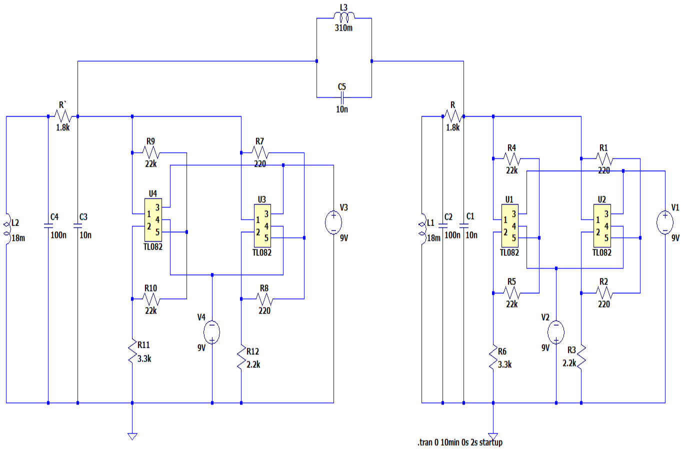


Figure 3 Chua's circuits in LC parallel coupling implemented with LT spice software for coupling parameters L_3 = 310 mH and C_5=10 nF.

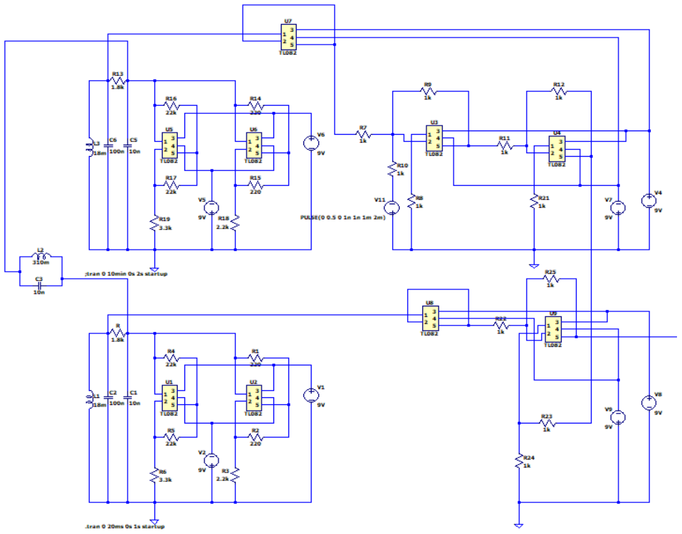


Figure 4 Chua's circuit based secure communication system implemented with LTspice software for coupling parameters L_2 = 310 mH and C_3= 10 nF

The synchronization errors up to 2 mV and 6 mV are observed in the first and second cases as shown in Fig.12 and Fig.15 respectively. The complete synchronization in the first and second cases is confirmed by the straight lines shown in Lissajous figures of Fig.13 and Fig.16 respectively. So, with these four sets of coupling inductance L_3 and coupling capacitance C_5values, the synchronized Chua's circuits in LC parallel coupling can be constructed for the use in the secure communication systems.

Table 1 Components in Chua's circuit in Kennedy's implementation

Sl. No	Component	Symbol	Value	Tolerance
1	Capacitor	C_1	10 nF	5%
2	Capacitor	C_2	100 nF	5%
3	Inductor	L_1	18 mH	5%
4	Resistance	R_1	220 Ω	5%
5	Resistance	R_2	220 Ω	5%
6	Resistance	R_3	2.2 kΩ	5%
7	Resistance	R_4	22 kΩ	5%
8	Resistance	R_5	22 kΩ	5%
9	Resistance	R_6	3.3 kΩ	5%
10	Battery	V_1	9 V	-
11	Battery	V_2	9 V	-
12	Op-amp(TL082)	A1	-	-
13	Op-amp(TL082)	A2	-	-
14	Potentiometer	R	2.0 kΩ	-

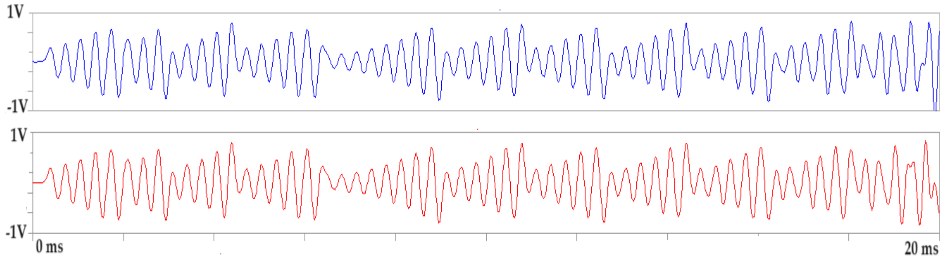


Figure 5 Time series graph of voltages across the capacitors C_2 and C_4 showing the synchronization at L_3 = 62 mH

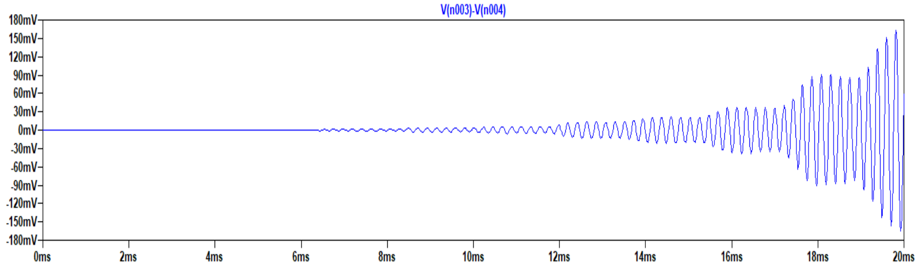


Figure 6 Error - time graph showing the synchronization error at L_3 = 62 mH

Secure Communication System with LC Parallel Coupling

A secure communication system is constructed with the synchronized Chua's circuits in LC parallel coupling with L_2= 62 mH and 310 mH with a fixed value capacitance C_3= 10 nF. A rectangular wave with amplitude of 0.5 V is used as the message signal. This message signal is recovered at the receiver in these two cases. The input and recovered message signals in the first and second cases are shown in Fig.17 and Fig.20 respectively.

The recovery of the message signal in the first and second cases is confirmed by the Lissajous figures shown in Fig.18 and Fig.21 respectively. This is because of the synchronization of chaotic signals at transmitter and receiver circuits due to LC parallel coupling. The

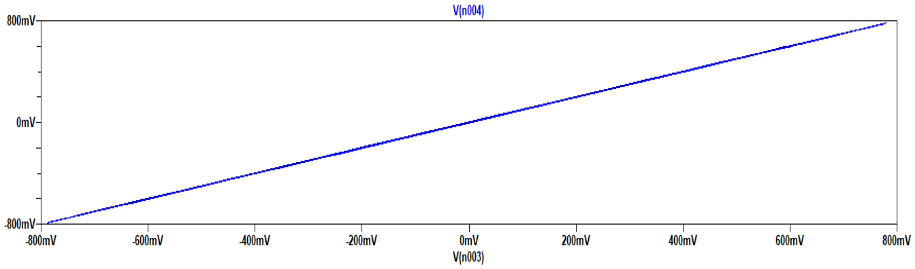


Figure 7 Lissajous figure of two chaotic signals **at** L_3 = 62 mH (X-axis: V_{c_4} and Y-axis: V_{C_2})

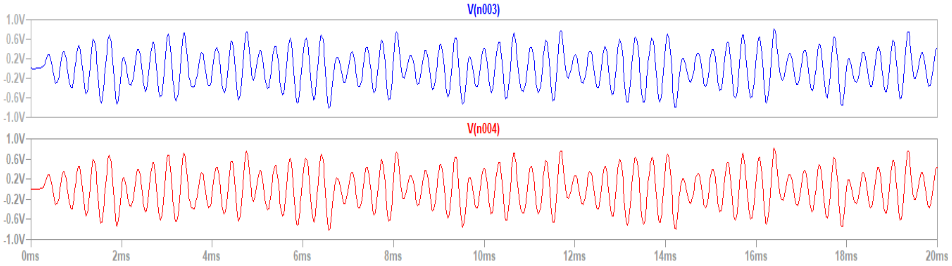


Figure 8 Time series graph of voltages across the capacitors C_2 and C_4 showing the synchronization at L_3 = 310 mH

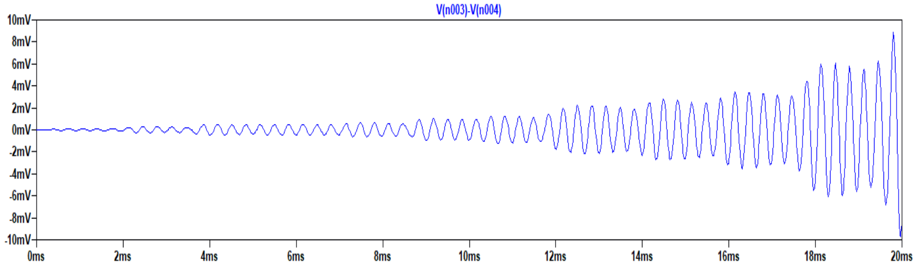


Figure 9 Error - time graph showing the synchronization error atL_3 = 310 mH (Error on Y- axis and time on X-axis)

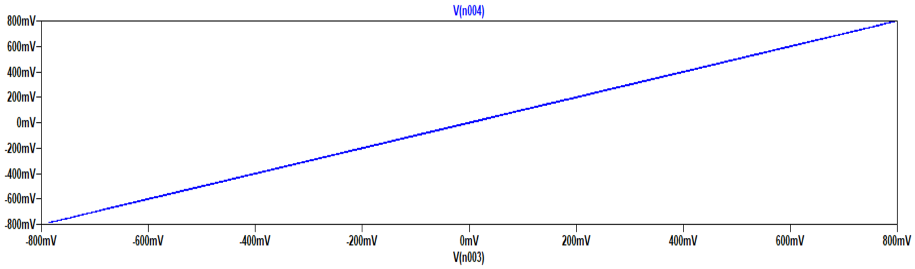


Figure 10 Lissajous figure of two chaotic signals at L_3 = 310 mH (X-axis: V_{c_4} and Y-axis: V_{C_2})

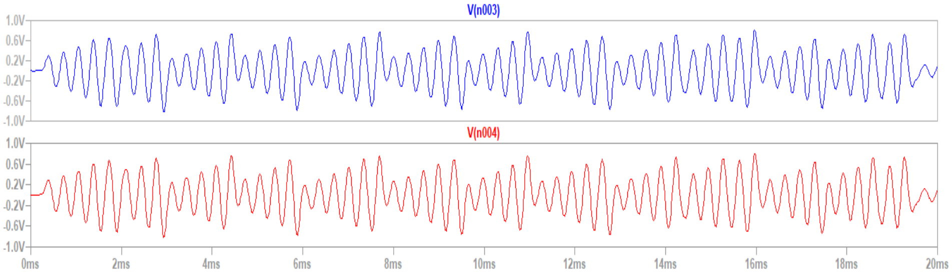


Figure 11 Time series graph of voltages across the capacitors C_2 and C_4 showing the synchronization at C_5 = 2 nF

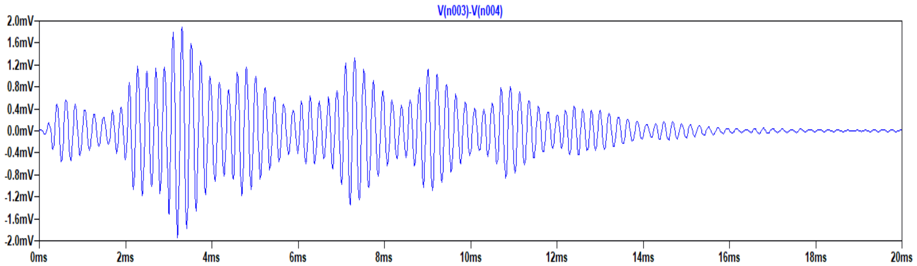


Figure 12 Error - time graph showing the synchronization error at C_5 = 2 nF (Error on Y- axis and time on X-axis)

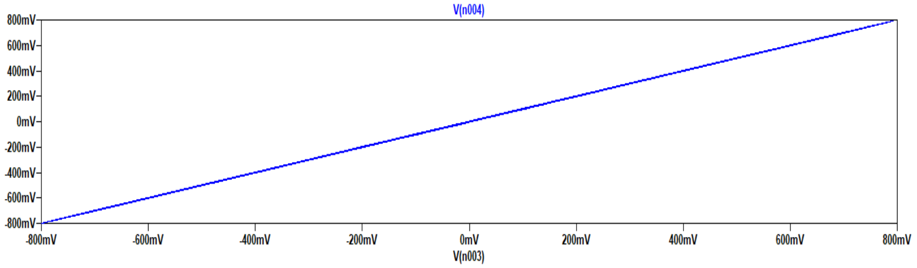


Figure 13 Lissajous figure of two chaotic signals **at**C_5 = 2 nF (X-axis: V_{c_4} and Y-axis: V_{C_2})

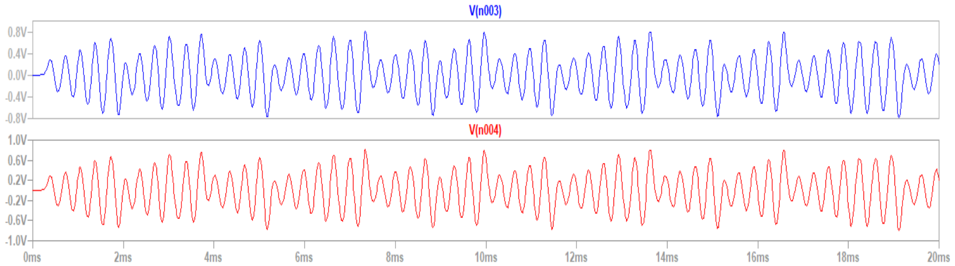


Figure 14 Time series graph of voltages across the capacitors C_2 and C_4 showing the synchronization at C_5 = 28 nF

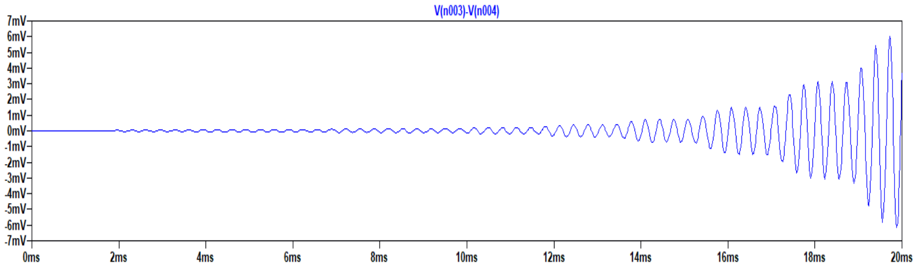


Figure 15 Error - time graph showing the synchronization error atC_5 = 28 nF (Error on Y- axis and time on X-axis)

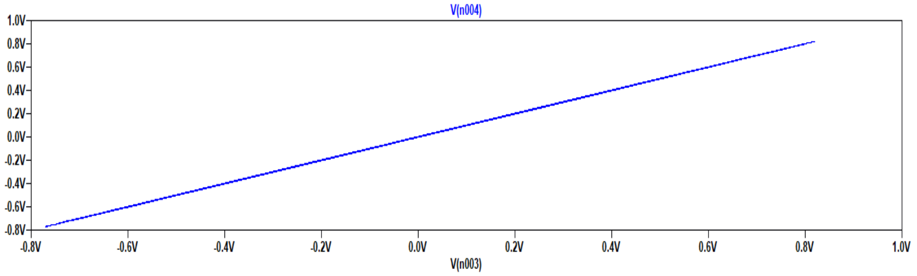


Figure 16 Lissajous figure of two chaotic signals at C_5 = 28 nF (X-axis: V_{c_4} and Y-axis: V_{C_2})

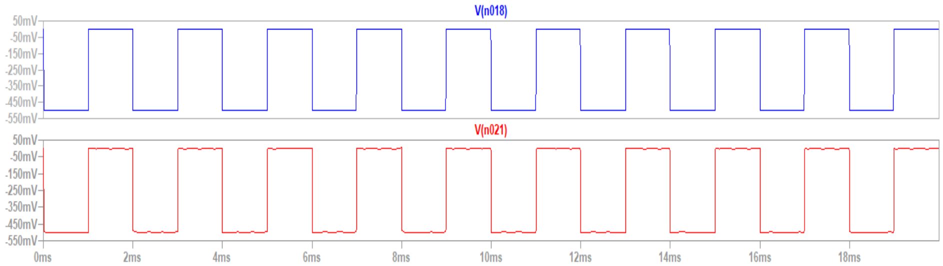


Figure 17 Time series graph of the input message and recovered signal at $L_2 = 62\ mH$ and C_3= 10 nF

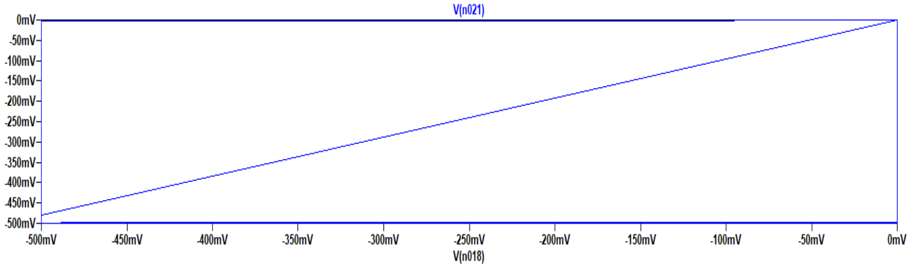


Figure 18 Lissajous figure of input and recovered message signals for $L_2 = 62\ mH$ and C_3= 10 nF.

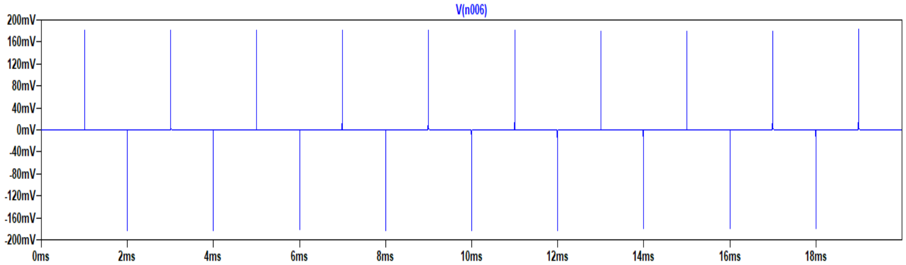


Figure 19 Masked signal at the transmitter for $L_2 = 62\ mH$ and C_3= 10 nF

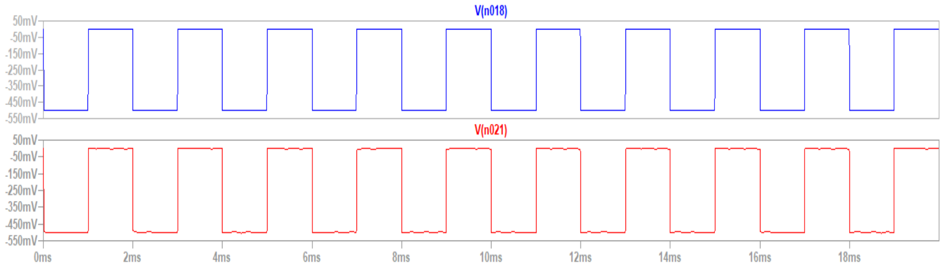


Figure 20 Time series graph of input and recovered message signals for $L_2 = 310\ mH$ and C_3= 10 nF.

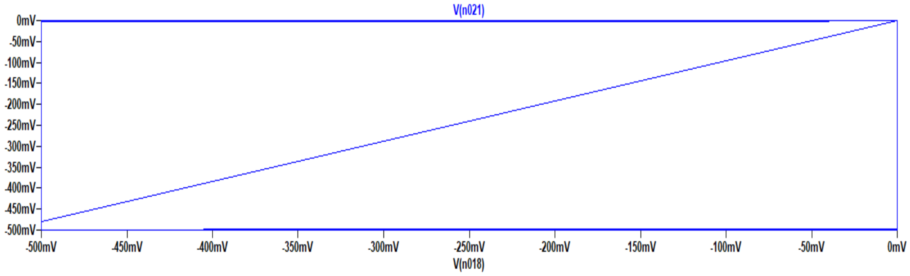


Figure 21 Lissajous figure of input and recovered message signals for $L_2 = 310\ mH$ and C_3= 10 nF.

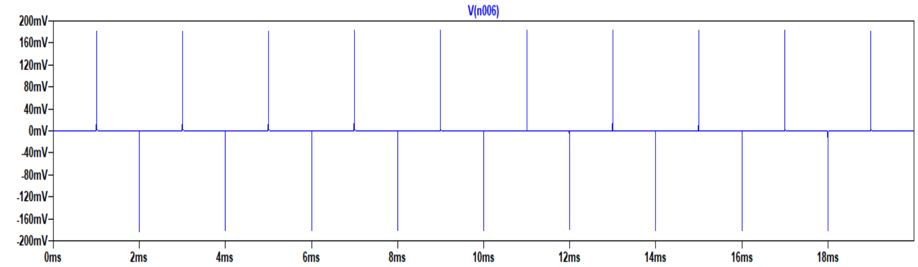


Figure 22 Masked message signal at the transmitter for $L_2 = 310\ mH$ and C_3= 10 nF

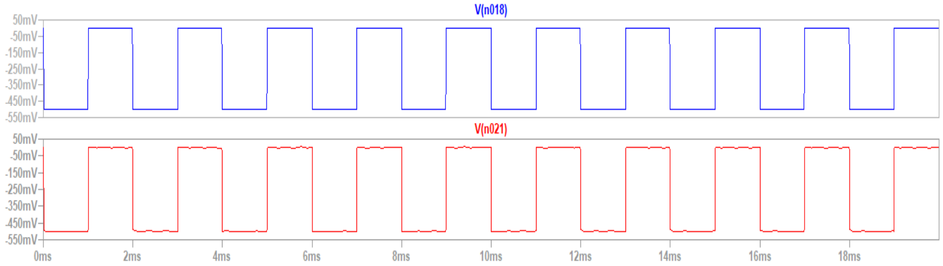


Figure 23 Time series graph of input and recovered message signals for $L_2 = 100\ mH$ and C_3= 2 nF

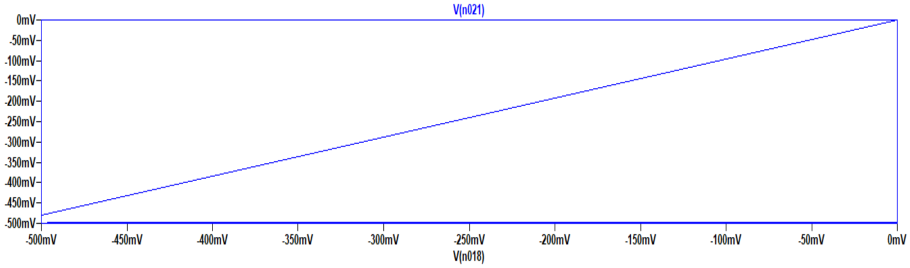


Figure 24 Lissajous figure of input and recovered message signals for $L_2 = 100\ mH$ and C_3= 2 nF.

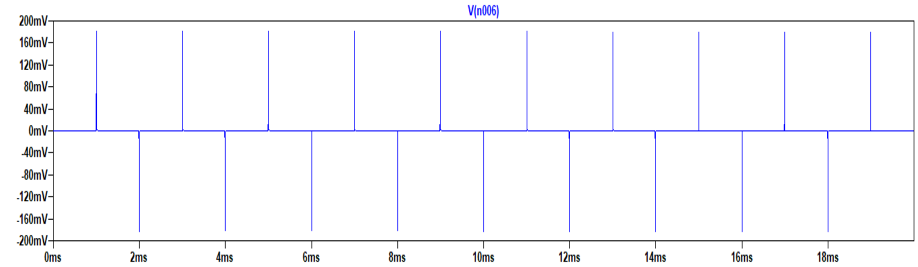


Figure 25 Masked message signal at the transmitter for $L_2 = 100\ mH$ and C_3= 2 nF.

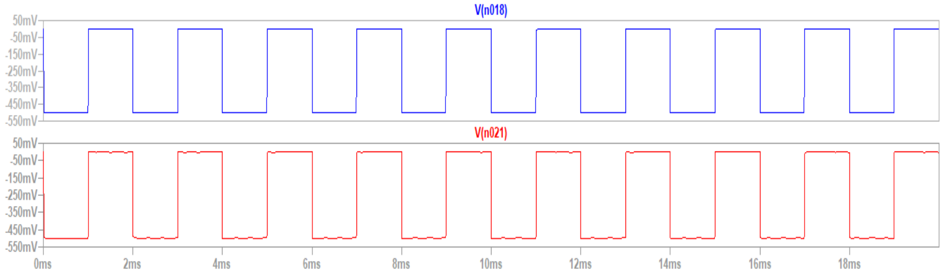


Figure 26 Time series graph of input and recovered message signals for $L_2 = 100\ mH$ and C_3= 28 nF.

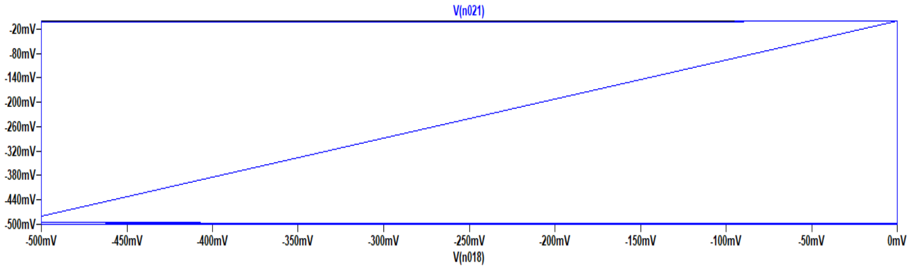


Figure 27 Lissajous figure of input and recovered message signals for $L_2 = 100\ mH$ and C_3= 28 nF.

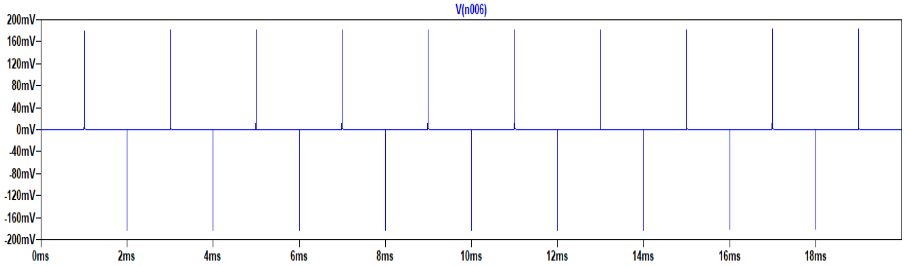


Figure 28 Masked message signal at transmitter for $L_2 = 100\ mH$ and C_3= 28 nF.

recovered signals are identical to those of input rectangular waves except small fluctuations about the horizontal portions. This is the result of small synchronization error in the respective cases. The masked signals in the first and second cases are shown in Fig.19 and Fig.22 respectively. The masked signals are concealing the identity of the original message signal, so that the actual message signal cannot be identified, except after the recovery at the receiver.

Similarly, a secure communication systems is constructed with the coupling capacitance values of C_3= 2 nF and 28 nF for a fixed coupling inductance value of L_2 = 100 mH. The message signals are recovered in this case also for the same input signal as before as the complete synchronization is achieved in this case as well. The input and recovered signals in first and second cases are shown in Fig.23 and Fig.26 respectively. The complete synchronization is confirmed in first and second cases by the Lissajous figures shown in Fig.24 and Fig.27 respectively. The input rectangular waves are completely recovered here except for very few small deviations just below and above the horizontal portions. The reason for this is again a small synchronization error in the respective cases. The masked signals in the first and second cases are shown in Fig.25 and Fig.28 respectively.

The message delivery is secure in this case also as the message signals are completely masked by the input chaotic signals.So, the proposed secure communication system constructed with synchronized Chua's circuits in LC parallel coupling can be used for efficient signal masking and delivery at all the four sets of coupling inductance and capacitance values. So, there is the greater flexibility in the construction and the efficiency in the working of the proposed communication system compared to the previous studies (Mustafa Mamat and Maulana 2013; Emiliia Nazarenko and Katzenbeisser 2023).

CONCLUSION

A new secure communication system is constructed by using the chaotic masking method. For this purpose, two identical synchronized Chua's circuits in a new LC parallel coupling are used. The advantage of this LC parallel coupling is that the complete synchronization can be achieved for various sets of coupling inductance and capacitance values.This provides some flexibility in constructing the secure communication systems with perfect masking and recovery of the message signals as observed through the time series graphs and Lissajous figures generated in LTspice simulations. These results are also good compared to the previous studies of using the same bi-directional coupling of two Chua's circuits but with some different coupling elements. So, the efficient secure communication systems can be practically constructed by using the synchronized Chua's circuits in the direct LC parallel coupling.

Furthermore, the bi-directional nature of coupling used here also provides some additional security in the message transmission, even if the coupling elements of the system are known to the intruder. A few limitations of such LC coupled based communication systems are mainly - the complexity in the construction due to the complexity in constructing the coupling element and the mathematical analysis of the problem.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Adel Ouannas, G. G. V.-T. P., Abdulrahman Karouma and V. S. Luong, 2021 A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. Alexandria Engineering Journal **60**: 1873–1884.

Bonny T., N. W., V. S., and S. A., 2023 Highly secured chaos-based communication system using cascaded masking technique and adaptive synchronization. Multimedia Tools and Applications **82**: 1–30.

Chua, L. O., 1992 The genesis of Chua's circuit. Archiv fur Elektronik und Ubertragungstechnik **46**: 250–257.

Cuomo, K. and A. Oppenheim, 1993 Circuit implementation of synchronized chaos with applications to communications. Phys. Rev. Lett. **71**: 65–68.

Emiliia Nazarenko, S. G. S. N. M. F. F. T. A., Nikolaos Athanasios Anagnostopoulos and S. Katzenbeisser, 2023 Real-world chaos based cryptography using synchronized chua chaotic circuits. https://arxiv.org/pdf/2210.11299.pdf.

H.Dedieu, M. and M.Hasler, 1993 Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing **40**: 634–642.

I.P. Marino, E. R. J. and C. Grebogi, 1999 Signal dropout reconstruction in communication with chaos. Int. J. Bifurc.,Chaos **9**: 2291–2293.

Kennedy, M. P., 1992 Robust op-amp realization of chua's circuit. Frequenz **46**.

K.M. Cuomo, A. O. and S. Strogatz, 1993 Synchronization of lorenz-based chaotic circuits with applications to communications. IEEE Trans. Circuits Syst. **40**: 626–633.

Koh, C. L. and T. Ushio, 1997 Digital communication method based on m-synchronized chaotic systems. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **44**: 383–390.

L. Kocarev, K. E. L. C., K.S. Halle and U. Parlitz, 1992 Experimental demonstration of secure communications via chaotic synchronization. Int. J.Bifurc. Chaos **2**: 709–713.

Leon O.Chua, K. E., Ljupco Kocarev and M. Itoh, 1992 Experimental synchronization in chua's circuit. International Journal of Bifurcation and Chaos **2**: 705–708.

Liao Xiao-Xin LUE Hai-Geng, Z. X.-J., JIAN Ji-Gui and XUBing-Ji, 2005 New results on global synchronization of chua's circuit. Acta Automatica Sinica. **31**.

LinearTechnology, 2011 Ltspice iv getting started guide,linear technology,2011. https://www.analog.com/media/en/simulation-models/spice-models/ltspicegettingstartedguide.pdf?modelType=spice-models.

LinearTechnology, 2020 Ltspice xvii software,2020. https://www.analog.com/en/design-center/design-tools-and-calculators/ltspice-simulator.html.

Mustafa Mamat, M. S. W. and D. S. Maulana, 2013 Numerical simulation chaotic synchronization of chua circuit and its application for secure communication. Applied Mathematical Sciences **7**: 1–10.

Ogorzalek, M. J., 1993 Taming chaos. i. synchronization. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **40**: 693–699.

Shuh-Chuan Tsay, D.-L. Q., Chuan-Kuei Huang and W.-T. Chen, 2004 Implementation of bidirectional chaotic communication systems based on lorenz circuits. Chaos, Solitons and Fractals **20**: 567–579.

Shuh-Chuan Tsay, W.-T. C., Chuan–Kuei Huang and Y.-R. Wu, 2005 Synchronization of chua chaotic circuits with application to the bidirectional secure communication systems. International Journal of Bifurcation and Chaos **15**: 605–616.

Trejo-Guerra, T.-C. E. C.-H. C., R. and C. Sanchez-Lopez, 2009 Highly secured chaos-based communication system using cascaded masking technique and adaptive synchronization. International Journal of Bifurcation and Chaos **19**: 4217–4226.

V.V.Astakhov, A. G., A.V.Shabunin and V.S.Anishchenko, 1997 Nonlinear dynamics of two chua's circuits coupled through a capacitance. Journal of Communications Technology and Electronics **42**: 294–301.

Wu, C. and L. Chua, 1993 A simple way to synchronize chaotic systems with applications to secure communication systems. Int. J. Bifurc.,Chaos **3**: 1619–1627.

Yao, Z., Y. Y. Jun Ma, and C. Wang, 2019 Synchronization realization between two non-linear circuits via an induction coil coupling. Nonlinear Dyn. **96**: 205–217.

Zhang, J. and X.-Y. Wang, 2023 Synchronous control study of chua circuit system via capacitor closed loop coupling. https://arxiv.org/pdf/2304.04568.pdf.

Zhilong Liu, G. Z., Jun Ma and Y. Zhang, 2019 Synchronization control between two chua's circuits via capacitive coupling. Applied Mathematics and Computation **360**: 94–106.

Zhong, G.-Q. and F. Ayrom, 1985 Periodicity and Chaos in Chua's Circuit . IEEE Transations on Circuits and Systems **32**: 501–503.

How to cite this article: Prakash, V. S., Reddy, S. N., and Chary, A. S. A Secure Communication System of Synchronized Chua's Circuits in LC Parallel Coupling. *Chaos Theory and Applications*, 5(3), 167-177, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS Theory and Applications in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / **No.**3 / 2023 / **pp.**178-187
https://doi.org/10.51537/chaos.1250317

Lossless Image Encryption using Robust Chaos-based Dynamic DNA Coding, XORing and Complementing

Vinod Patidar *,1 **and Gurpreet Kaur** α,2
*School of Computer Science, University of Petroleum and Energy Studies (UPES), Bidholi, Dehradun-284007, India, αAmity Institute of Information Technology, Amity University, Noida-201303, UP, India.

ABSTRACT In this paper, we present a lossless image encryption algorithm utilizing robust chaos-based dynamic DNA coding and DNA operations (DNA XOR and DNA Complement). The entire process of encryption is controlled by the pseudo-random number sequences generated through a 1D robust chaos map that exhibits chaotic behaviour in a very large region of parameter space with no apparent periodic window and therefore possesses a fairly large key space. Due to peculiar feed-forward and feedback mechanisms, which modify the synthetic image (created to initiate the encryption process) at the encryption of each pixel, the proposed algorithm possesses extreme sensitivity to the plain image, cipher image and secret key. The performance analysis proves that the proposed algorithm exhibits excellent features (as expected from ideal image encryption algorithms) and is robust against various statistical and cryptanalytic attacks.

KEYWORDS
Image encryption
DNA encryption
DNA complementing
DNA XORing
Robust chaos

INTRODUCTION

The transmission of images/videos over the networks, and storage of such visual media in the cloud has become increasingly popular due to the proliferation of fast and efficient network technologies as well as the advancement, and miniaturization of computing devices and storage media. It has inevitably posed security threats/concerns for the image/visual media. Images can be securely transmitted and stored in encrypted form to safeguard them from unauthorized access. Since images have different characteristics (bulk data, high spatial correlation, redundancies) than text data, therefore, require special attention and algorithms to encrypt them or hide them from unauthorized uses.

In recent years a variety of image encryption technologies like image encryption based on optical transforms (Hennelly and Sheridan 2003; Kaur *et al.* 2022a,b), based on chaos theory(Patidar *et al.* 2011), DNA-based image encryption (Adleman 1994; Xiao *et al.* 2006; Gehani *et al.* 2004) and algorithms based on the amalgamation of these technologies have been developed. Amongst them, the chaos-based image encryption algorithms have been most successful due to effective confusion and diffusion as recommended by Shannon(Shannon 1949). However, chaos-based image encryptions do suffer from some limitations like floating number-based operations, the existence of periodic windows in parameter space and smaller key space etc. (Teh *et al.* 2020). In recent years DNA computing has also gained popularity due to its huge information-carrying capacity, parallelism and ultra-low energy consumption. Rather than implementing DNA computing at the molecular level (Adleman 1994) which requires highly restricted laboratory conditions, it has been frequently used to carry the digital information (through representing it in DNA sequences) and manipulate it using feasible DNA operations like addition, subtraction, DNA XOR, DNA XNOR, DNA Complement etc.(Xiao *et al.* 2006; Gehani *et al.* 2004).

The sole use of DNA coding and operations does not introduce nonlinearity in the process of information manipulation (scrambling and altering) since these operations are primarily linear therefore have not been very successful in fulfilling Shannon's (Shannon 1949) criteria for developing perfect secrecy in image encryption or steganography algorithms. However, the DNA encoding and corresponding operations are found to be successful when used in combination with the dynamical chaos, which is bounded, aperiodic behaviour having sensitivity to initial conditions/parameters and exhibited by deterministic nonlinear dynamical systems. Such techniques have been termed hybrid DNA-chaos-based image encryption.

Manuscript received: 12 February 2023,
Revised: 6 April 2023,
Accepted: 17 April 2023.

[1] vinod.patidar@ddn.upes.ac.in (**Corresponding author**).
[2] gurpreet.preeti82@gmail.com

In DNA-chaos-based image encryption, the images to be encrypted are transformed into DNA sequences and then the scrambling of DNA bases is executed with the help of dynamical chaos. These scrambled sequences are then encoded with the help of DNA operations under the influence of the chaotic dynamical system(s). Broadly classifying, there are two ways to design a hybrid DNA-Chaos-based encryption algorithm: fixed DNA and dynamic DNA coding (Xue *et al.* 2020). A fixed rule is used for encoding, decoding and DNA operations in a fixed DNA scheme (Zhang *et al.* 2014; Wang *et al.* 2015) whereas rules are dynamically selected for encoding, decoding and DNA operations in dynamic DNA coding (Chai *et al.* 2019; Dagadu *et al.* 2019; Wang *et al.* 2020). For a detailed review and comparison of various existing hybrid DNA-Chaos-based encryption algorithms, we refer the readers to a recent work by Patidar and Kaur (Patidar and Kaur 2023).

In this paper, we propose a novel dynamic DNA coding algorithm for image encryption. All the operations (DNA encoding, DNA-based-XOR, DNA-based-complement and DNA decoding) are used under the control of a robust chaos map whose dynamical behaviour is chaotic in very large parameter space (2 parameter space) with no apparent periodic window. All of the above factors contribute towards a larger key space, thereby eliminating the possibility of brute force attack. The robust chaos map is mainly used in the algorithm to generate some pseudo-random number sequences and the various DNA-based operations in encryption (encoding, XORing, Complementing and decoding) are dynamically selected with the help of these pseudo-random number sequences for each pixel.

All the pseudorandom number sequences are interdependent (as generated sequentially) as well as dependent on the secret keys therefore the algorithm possesses extreme key sensitivity. To start the encryption process, we create a synthetic image (of the same size as the plain image) with the help of the same robust chaos map and the pixels of the synthetic image are modified and used in the encryption of the corresponding pixel of the plain image. The process of modification of each pixel of the synthetic image involves the information from the plain image as well as the cipher image pixels generated till now and hence, is different for each pixel. This interdependency leads to extreme sensitivity concerning plain and cipher images and makes the entire process of encryption super complex.

The subsequent sections of this paper are structured as: In Section 2, we briefly introduce the robust chaos map, in Section 3, the DNA coding, XORing and Complementing. In Section 4 all the steps of the proposed image encryption algorithm are described, in Section 5, the results of the performance analysis of the proposed algorithm are presented and finally, in Section 6 the conclusions are drawn.

THE ROBUST CHAOS MAP

The robust chaos is defined as the absence of periodic windows and co-existing attractors in some neighbourhoods within the parameter space (Zeraoulia 2012). We use the following form of an iterative one-dimensional map in the proposed image encryption algorithm as the source of robust chaos (Andrecut and Ali 2001; Patidar 2022).

$$x_{n+1} = F(x_n, a, v), (F(x, a, v) = \frac{1 - v^{-ax(1-x)}}{1 - v^{-(\frac{a}{4})}} \forall v \neq 1, v > 0, a > 0) \quad (1)$$

Here x is the state variable, a and v are the parameters. This iterative map is an S-unimodal map and has a negative Schwarzian derivative. The function has a unique maximum at $x = 0.5$ (Figure 1), hence there can be at most one attracting periodic orbit with the critical point in its basin of attraction. The orbit with initial condition $x = 0.5$ will approach to x = 0 in two iterates. Since the point $x = 0$ will be unstable if

$$(F'(0, a, v) = |\frac{ln(v)a}{1 - v^{-(\frac{a}{4})}}| > 1 \forall v \neq 1, v > 0, a > 0) \quad (2)$$

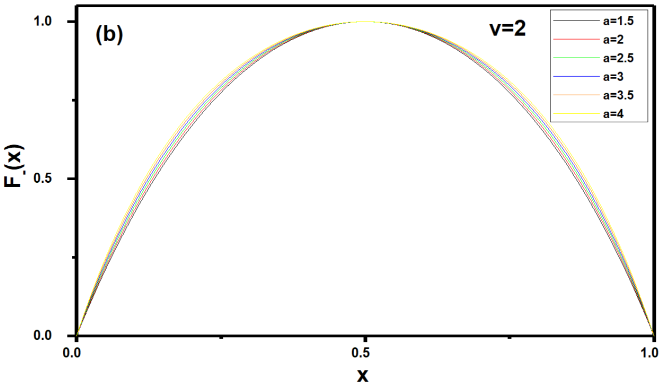


Figure 1 Function plots of robust chaos map maps (Eq.(1))

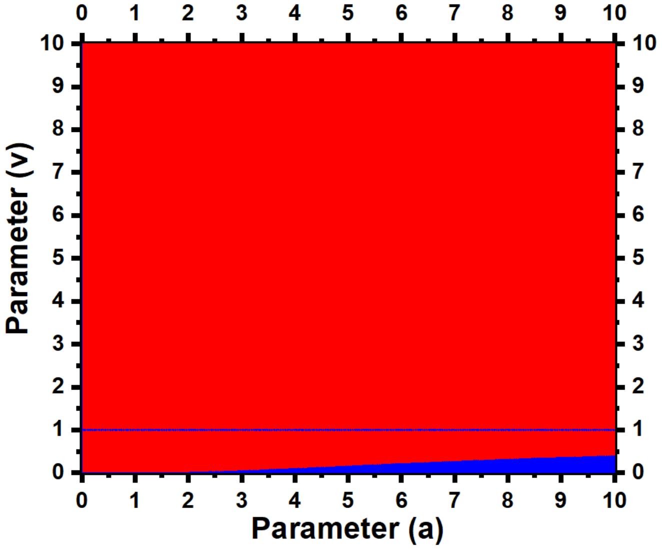


Figure 2 Derivative of the function F'(0,a,v), (Eq.2) red correspond to the positive value and blue corresponds to the negative value

In such a case, the map does not possess any stable periodic orbit hence a chaotic attractor/orbit prevails. In Figure 2, we have depicted the regions of the parameter space (a, v) where the derivative $F'(0, a, v)$ is positive and negative respectively through the red and blue colours. In the red region, the point x = 0 is unstable therefore the chaotic orbit may exist here. We have also plotted the bifurcation diagram for the robust chaotic map (Eq.1) by iterating the map for 5000 iterations and skipping the initial 500 iterations for (i) a fixed value of parameter $a = 7.1$ and varying v from 0 *to* 10 in the step of 0.01 and (ii) a fixed value of parameter $v = 4.3$ and varying a from 0 *to* 10 in the step of 0.01. The results have been depicted in Figure 3. We observe from the top frame (for $a = 7.1$) that point $x = 0$ is stable up to $v = 0.25$ and then it becomes unstable and a chaotic orbit prevails. This fact may be verified with the quantitative results of the stability condition (Eq.2) depicted in Figure 2 and the Lyapunov exponent results depicted in Figure 4. In the bottom frame (for $v = 4.3$) of Figure 3, we observe that chaos is present for the entire range of parameter a which is also confirmed from the quantitative results of stability condition (Eq.2) depicted in Figure 2 and the Lyapunov exponent results depicted in Figure 4.

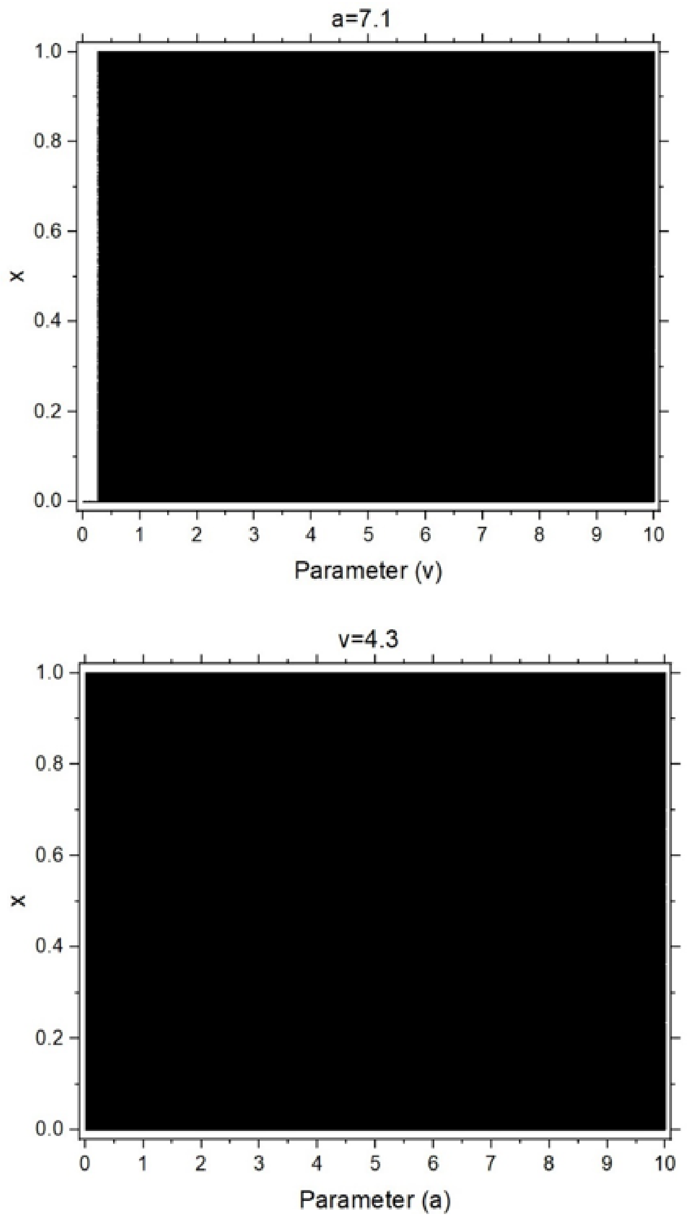


Figure 3 Bifurcation plot for the robust chaos map (Eq.(1)): Top frame for a=7.1 and bottom frame for v=4.3.

To confirm the existence of chaotic orbit and robust chaos, we have numerically computed the Lyapunov exponent for the above iterative map and the results are shown in Figure 4. It is clear that the Lyapunov exponent is positive in the entire parameter space (without any periodic window) defined by $v > 0, a > 0$ except for $v = 1$ and a very small region near $v = 0$. In the proposed image encryption algorithm, we use the above-mentioned iterated function in the parameter space defined by $v > 1, a > 1$ for generating the pseudorandom sequences.

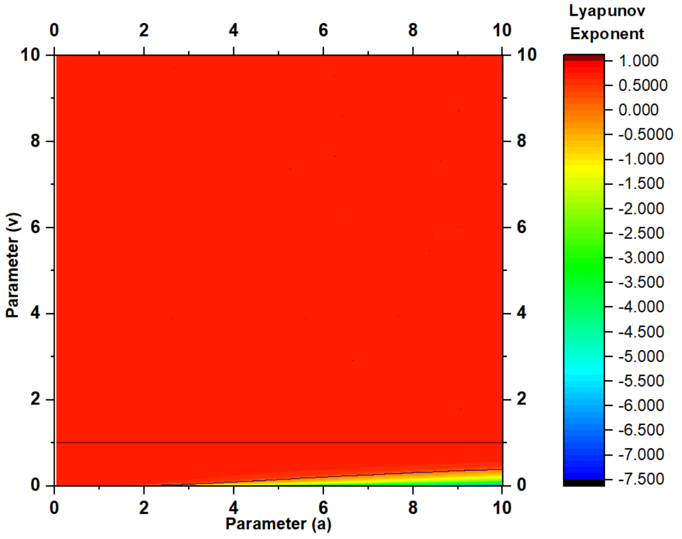


Figure 4 Lyapunov Exponent for the robust chaos map (1)

DNA CODING, XORING AND COMPLEMENTING

In DNA computing 4 nucleic acid bases: Adenine, Thymine, Cytosine and Guanine (A, T, C and G) are encoded as 00, 01, 10 and 11. There can be a total of 24 different possibilities for such coding out of them only eight comply with both the binary and DNA complement rules. In Table 1, we have summarized these eight rules (Wang *et al.* 2020). For each DNA rule, addition, subtraction and XOR operations can be formulated by following the conventional binary operations. Since in the present algorithm we are using XOR operation on DNA sequences therefore we are giving one such operation table (Table 2) for the XOR operation on DNA bases corresponding to the DNA encoding rule 3 (Wang *et al.* 2020).

The complement rules for the DNA sequences are defined based on the double helix structure of the DNA strand. If the complement operation is defined by the function $f_c(b_i)$ where b_i is one of the nucleic bases of DNA, then the following relation is satisfied:

$$b_i \neq f_c(b_i) \neq f_c\left(f_c\left(b_i\right)\right) \neq f_c\left(f_c\left(f_c\left(b_i\right)\right)\right)$$

$$b_i = f_c\left(f_c\left(f_c\left(f_c\left(b_i\right)\right)\right)\right)$$

According to the above-mentioned relation, there are six different complement base-pair relations (rules) possible. These are listed in Table 3 (Wang *et al.* 2020).

Rule 1, in Table 3, may be interpreted as follows:

$$f_c(A) = T;$$

$$f_c(f_c(A)) = f_c(T) = C$$

$$f_c\left(f_c\left(f_c(A)\right)\right) = f_c\left(f_c(T)\right) = f_c(C) = G$$

The $f_C(f_c(A))$ is the Level 2 complement of A that is equal to C as per the complement rule 1.

The recovery of the complement, for Rule 1, in Table 3, may be done in the following way:

Table 1 The Eight DNA Encoding Rules

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	C	C	G	G
01	G	C	G	C	A	T	A	T
10	C	G	C	G	T	A	T	A
11	T	T	A	A	G	G	C	C

Table 2 The XOR Operation (for DNA Encoding Rule 3)

$\oplus_{DNA}$	A	T	C	G
A	T	A	G	C
T	A	T	C	G
C	G	C	T	A
G	C	G	A	T

Table 3 Six DNA Complement Rules

Rule		Complement base pairs		
1	AT	TC	CG	GA
2	AT	TG	GC	CA
3	AC	CG	GT	TA
4	AC	CT	TG	GA
5	AG	GC	CT	TA
6	AG	GT	TC	CA

$$f_{cr}(A) = G;$$

$$f_{cr}(f_{cr}(A)) = f_{cr}(G) = C$$

$$f_{cr}\left(f_{cr}\left(f_{cr}(A)\right)\right) = f_{cr}\left(f_{cr}(G)\right) = f_{cr}(C) = T$$

The$f_{cr}\left(f_{cr}\left(f_{cr}(A)\right)\right)$ is the Level 3 complement recovery of A that is equal to T as per the complement rule 1.

THE PROPOSED ALGORITHM

Encryption Algorithm

In the proposed image encryption algorithm, the plain image is a grey image of dimension H × W and the secret key is a set of 15 floating-point numbers and one integer $(x_0, a_1, v_1, N, a_2, v_2, a_3, v_3, a_4, v_4, a_5, v_5, a_6, v_6, a_7, v_7)$. Here $0 < x_0 < 1$ and all $a > 1$, $v > 1$ and N is an integer preferably between 100 to 999.

1. Iterate the robust chaos map N times with the initial condition x_0 and parameters a_1, v_1 and throw the iterates and record the last value x_N for further use.
2. Iterate the robust chaos map HW times with the initial condition x_N and parameters a_1, v_1. These iterates are used to create a synthetic image (SI) of dimension H × W

   $SI(k) = \lfloor x_k \times 256 \rfloor$, k=1 to HW
3. A pseudo-random number sequence (PRS1) is generated having numbers 1 to 8 by iterating the robust chaos map with the initial condition x_{N+HW} and parameters a_2, v_2

   $$PRS1_i = \lfloor x_i \times 8 \rfloor + 1; i = 1 \ to \ HW$$
4. Step 3 is repeated with x_{N+2HW} and parameters a_3, v_3 to generate $PRS2_i$
5. Step 3 is repeated with x_{N+3HW} and parameters a_4, v_4 to generate $PRS3_i$

6. A pseudo-random number sequence (PRS4) is generated having numbers 1 to 6 by iterating the robust chaos map 4HW times with the initial condition x_{N+4HW} and parameters $a_5,\ v_5$

$$PRS4_i = \lfloor x_i \times 6 \rfloor + 1; i = 1 \ to \ 4HW$$

7. A pseudo-random number sequence (PRS5) is generated having numbers 0 to 3 by iterating the robust chaos map 4HW times with the initial condition x_{N+8HW} and parameters $a_6,\ v_6$

$$PRS5_i = \lfloor x_i \times 4 \rfloor ; i = 1 \ to \ 4HW$$

8. Step 3 is repeated with x_{N+12HW} and parameters $a_7,\ v_7$ to generate $PRS6_i$

   Now the process of encryption of i$^{\text{th}}$ pixel of the plain image is done in the following way:

9. Calculate the two terms PIS and CIS dependent on the plain and cipher images

$$PIS(i) = mod(sum\,(PI(i+1:HW))\,,\,256)$$

$CIS(i) = mod(sum(CI(1:i-1)), 256)$

For $i = 1$ the value of the previous cipher image pixel $CI(i-1)$ is 0.

10. Using PIS and CIS calculated above, the i$^{\text{th}}$ pixel of the synthetic image is modified

$$SI(i) = (SI(i) \oplus PIS(i)) \oplus CIS(i)$$

11. Convert the $SI(i)$ into the DNA sequence ($SIDNA(i)$) using the $PRS1_i^{th}$ DNA encoding rule

12. Convert the $PI(i)$ into the DNA sequence ($PIDNA(i)$) using the $PRS2_i^{th}$ DNA encoding rule

13. (i)DNA XORing using the $PRS3_i^{th}$XORing

$CIDNA1(i) = (PIDNA(i) \oplus_{DNA} SIDNA(i)) \oplus_{DNA} CIDNA1(i-1)$.

For $i = 1$ the DNA sequence for the previous cipher image pixel $CIDNA1(i-1)$ is 'ATCG'.

(ii) DNA Complement using $PRS4_i^{th}$ DNA Complement rule at the $PRS5_i^{th}$ level

$$CIDNA(i) = f_c(CIDNA1(i))$$

14. Convert the $CIDNA(i)$ into the binary form using the $PRS6_i^{th}$ DNA decoding rule.

    The process from Steps 9 to 14 is repeated for all the pixels of the plain image.

For a complete reference of the proposed image encryption algorithm and flow of operations, please refer to the block diagram given in Figure 5.

Decryption Algorithm

In the proposed image encryption method, the decryption process is identical to the encryption algorithm discussed earlier, except for the fact that it is executed in reverse order. This means that the last pixel of the cipher image is decrypted first, followed by the decryption of each pixel in reverse order until the first pixel is reached. If the same secret key is used, the original plain image can be fully recovered.

The decryption starts with the same secret key ($x_0,\ a_1,\ v_1,\ N,\ a_2,\ v_2,\ a_3,\ v_3,\ a_4,\ v_4,\ a_5,\ v_5,\ a_6,\ v_6,\ a_7,\ v_7$) followed by execution of Steps 1 to 8 of the encryption algorithm (as explained in subsection 4.1) to generate the synthetic image SI and pseudo-random sequences PRS1 to PRS6.

Now the process of decryption of i$^{\text{th}}$ pixel (starting from the last pixel) of the cipher image is done in the following way:

9. Calculate the two terms CIS and PIS dependent on the cipher and plain images

   $CIS(i) = mod(sum(CI(1:i-1)), 256)$

$$PIS(i) = mod(sum\,(PI(i+1:HW))\,,\,256)$$

For $i = 1$ (i.e., the last pixel to decrypt) the value of the previous cipher image pixel $CI(i-1)$ is 0.

10. Using PIS and CIS calculated above, the i$^{\text{th}}$ pixel of the synthetic image is modified

$$SI(i) = (SI(i) \oplus PIS(i)) \oplus CIS(i)$$

11. Convert the $SI(i)$ into the DNA sequence ($SIDNA(i)$) using the $PRS1_i^{th}$ DNA encoding rule

12. Convert the $CI(i)$ into the DNA sequence ($CIDNA(i)$) using the $PRS6_i^{th}$ DNA encoding rule

13. (i) DNA Complement recovery using $PRS4_i^{th}$ DNA Complement rule at the $PRS5_i^{th}$ level

$$CIDNA1(i) = f_{cr}(CIDNA(i))$$

(ii)DNA XORing using the $PRS3_i^{th}$XORing

$PIDNA(i) = (CIDNA1(i) \oplus_{DNA} CIDNA1(i-1)) \oplus_{DNA} SIDNA1(i)$.

For $i = 1$ (i.e., the last pixel to decrypt) the DNA sequence for the previous cipher image pixel $CIDNA1(i-1)$ is 'ATCG'.

14. Convert the $PIDNA(i)$ into the binary form using the $PRS2_i^{th}$ DNA decoding rule.

    The process from Steps 9 to 14 is repeated for all the pixels of the cipher image in reverse order i.e. from the last pixel to the first pixel.

NIST testing of pseudorandom sequences

To verify the pseudorandomness of the sequences generated through the robust chaotic map and used in the proposed image encryption scheme, we have used the NIST test suite. For testing purpose we have generated 100 sequences of 10^6 bits each starting with the randomly chosen initial conditions and parameters within the allowed robust chaos range as specified above (i.e. $0 < x_0 < 1$ and all $a > 1, v > 1$).

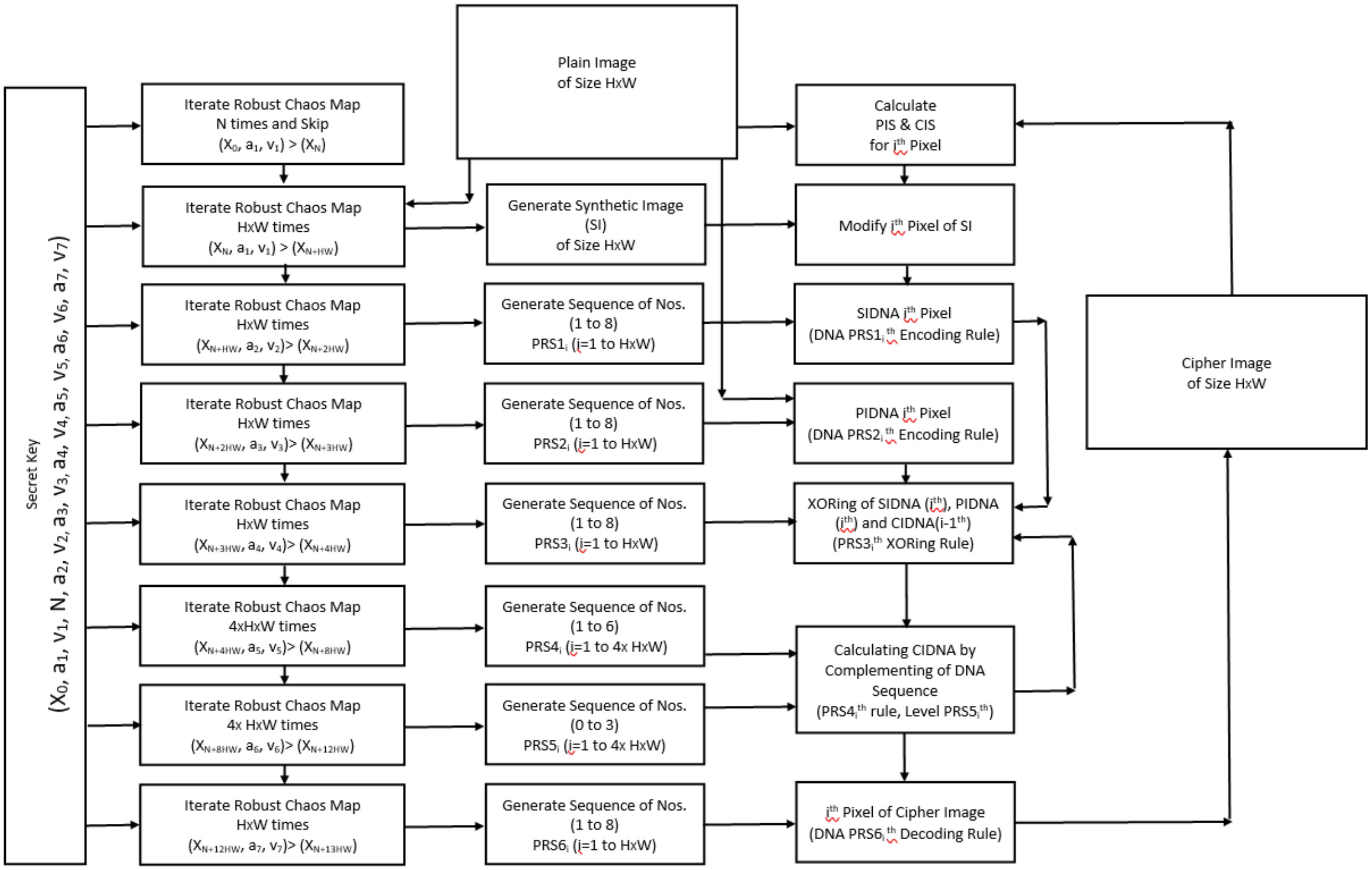

Secret Key
(X0, a1, V1, N, a2, V2, a3, V3, a4, V4, a5, V5, a6, V6, a7, V7)
Plain Image of Size HxW
Iterate Robust Chaos Map N times and Skip (X0, a1, v1) > (XN)
Iterate Robust Chaos Map HxW times (XN, a1, v1) > (XN+HW)
Iterate Robust Chaos Map HxW times (XN+HW, a2, v2)> (XN+2HW)
Iterate Robust Chaos Map HxW times (XN+2HW, a3, v3)> (XN+3HW)
Iterate Robust Chaos Map HxW times (XN+3HW, a4, v4)> (XN+4HW)
Iterate Robust Chaos Map 4xHxW times (XN+4HW, a5, v5)> (XN+8HW)
Iterate Robust Chaos Map 4x HxW times (XN+8HW, a6, v6)> (XN+12HW)
Iterate Robust Chaos Map HxW times (XN+12HW, a7, v7)> (XN+13HW)
Generate Synthetic Image (SI) of Size HxW
Generate Sequence of Nos. (1 to 8) PRS1i (i=1 to HxW)
Generate Sequence of Nos. (1 to 8) PRS2i (i=1 to HxW)
Generate Sequence of Nos. (1 to 8) PRS3i (i=1 to HxW)
Generate Sequence of Nos. (1 to 6) PRS4i (i=1 to 4x HxW)
Generate Sequence of Nos. (0 to 3) PRS5i (i=1 to 4x HxW)
Generate Sequence of Nos. (1 to 8) PRS6i (i=1 to HxW)
Calculate PIS & CIS for ith Pixel
Modify ith Pixel of SI
SIDNA ith Pixel (DNA PRS1ith Encoding Rule)
PIDNA ith Pixel (DNA PRS2ith Encoding Rule)
XORing of SIDNA (ith), PIDNA (ith) and CIDNA(i-1th) (PRS3ith XORing Rule)
Calculating CIDNA by Complementing of DNA Sequence (PRS4ith rule, Level PRS5ith)
ith Pixel of Cipher Image (DNA PRS6ith Decoding Rule)
Cipher Image of Size HxW

Figure 5 The image encryption algorithm

We have then run the entire NIST test suite comprising 15 parametric and nonparametric tests that generate a total of 188 p-values for each test statistic (there are multiple numbers of variants corresponding to some of the tests). Considering the significance level of 0.01, a p-value greater than 0.01 indicates that a particular test is passed by the sequence. We also find the total number of sequences passing the test out of the total sequences i.e. proportion for each test statistics and as per the chosen significance level 0.01, if it falls within the range (0.9833245, 0.9966745), the pseudorandom sequence generator qualifies for the cryptographic applications. For each test statistic, we may also observe the uniformity of all 100 p-values in the entire range [0,1] through the Chi-square test on the 100 p-values for each test statistic and generating the p-value of p-values i.e $p - value_T$. If $p - value_T > 0.0001$ then the distribution of the p-values for that particular test is declared uniform.

We have depicted the results of proportions and the p-value$_T$ obtained through the NIST test suite for each test statistic in Figure 6 that shows the pseudorandom sequence generator qualifies the NIST test suite criteria for the cryptographic applications.

PERFORMANCE AND ANALYSIS RESULTS

The performance of the proposed image encryption method is analyzed through various perceptual quality metrics, statistical measures, information entropy, plaintext sensitivity measures (NPCR, UACI), and measures based on DNA sequences (Hamming distance, base ratio) etc. The details and results of the analysis are presented below.

We have used two images *'Peppers'* and *'Lena'* and encrypted them with the secret key (x0=0.787; a1=1.65; v1=4.57; N=123; a2=6.73; v2=5.46; a3=2.57; v3=7.35; a4=6.54; v4=9.83; a5=6.27; v5=4.76; a6=3.52; v6=2.43; a7=8.53; v7=5.32).

In Figure 7, we have shown the plain images and corresponding cipher images generated with the help of the proposed image encryption algorithm. The cipher images look random. In Figure 8, we have depicted the histograms of the plain and cipher images shown in Figure 7. Visually, the histograms of the cipher images appear uniform. To confirm the uniformity of the histograms of cipher images quantitatively, we have calculated two statistical measures: Chi-square and variance of the histograms for the plain and cipher images. The results are given in Table 4. It can be observed that Chi-square and histogram variance are very small for the cipher images (almost 1% of plain images) which confirms the uniformity of the cipher image histograms.

The deviations of the cipher image histogram from the ideal (perfect uniform distribution) histogram are computed using the metric 'Deviation from Ideality'. The results are shown in Table 5. As is evident from the values thus obtained, the deviation from the ideality is negligible. This substantiates that the cipher image pixel distributions are nearly ideal/uniform.

Also, the deviations between the plain and cipher image histograms are computed using two metrics 'Maximum Deviation' and 'Irregular Deviation'. Observations are listed in Table 5. As is evident from the values, the deviations are quite large. This substantiates the fact that the proposed image encryption algorithm generates the cipher images with histograms significantly different

Table 4 Chi-Square and Histogram Variance

		Peppers	Lena
Chi-Square	Plain Image	1.9280e+04	2.5400e+04
	Cipher Image	218.3680	245.5680
Histogram Variance	Plain Image	1.1768e+04	1.5503e+04
	Cipher Image	133.2813	149.8828

Table 5 Deviation from Ideality, Maximum Deviation and Irregular Deviation

	Peppers	Lena
Deviation from ideality	0.0587	0.0618
Maximum Deviation	0.5676	0.6620
Irregular Deviation	0.6446	0.6908

Table 6 Correlation Coefficients

		Peppers	Lena
Horizontal Adjacent Pixels	Plain Image	0.9544	0.9322
Horizontal Adjacent Pixels	Cipher Image	0.0020	7.5469e-04
Vertical Adjacent Pixels	Plain Image	0.9646	0.9684
Vertical Adjacent Pixels	Cipher Image	0.0038	-8.3144e-04
2D Correlation Coefficients between plain image and cipher image		-0.0045	-0.0077

Table 7 Perceptual Quality Metrics

	Peppers	Lena
MAE	75.3073	72.9944
MSE	8.3264e+03	7.7428e+03
PSNR	8.9262	9.2418
SD	1.4226e+04	1.4087e+04
SSIM	0.0093	0.0066
FSIM	0.3689	0.3614

than the histograms of corresponding plain images.

2D correlation coefficients for various pairs of plain and cipher images as well as the correlation between the adjacent pixels (horizontally as well as vertically) in the plain and cipher images are evaluated. The results for correlation coefficients are summarized in Table 6. The correlation of two similar images in an ideal case is unity. As the values obtained for the proposed scheme are negligible as compared to the ideal value which clearly shows that the proposed image encryption algorithm is capable of removing the high correlation that exist in the plain image pixels.

Table 8 Hamming Distance (DNA)

	Peppers	Lena
Hamming Distance	119900	119682

Table 9 DNA Base Ratio (%)

	DNA Base	Peppers	Lena
Plain Image	A	25.6631	25.7550
	T	25.7494	25.0525
	C	24.1581	24.4994
	G	24.4294	24.6931
Cipher Image	A	25.1038	25.0575
	T	25.1713	25.1025
	C	24.8988	25.1438
	G	24.8263	24.6962

Table 10 Global and Local Information Entropy

		Block Size	Peppers	Lena
Global Information Entropy	Plain Image	200 X 200	7.5820	7.4351
	Cipher Image		7.9960	7.9956
Local Information Entropy	Plain Image	50 X 50	6.9406	6.6886
	Cipher Image		7.9230	7.9260
	Plain Image	40X 40	6.7164	6.5113
	Cipher Image		7.8806	7.8800
	Plain Image	25 X 25	6.2370	6.0016
	Cipher Image		7.6697	7.6724

Table 11 Plaintext Sensitivity

	Peppers	Lena	Theoretical Value/Range (Wu *et al.* 2011) (Significance Level 0.01)
NPCR	99.6450	99.7000	99.5527
UACI	33.4561	33.4321	[33.2255, 33.7016]

The perceptual quality analysis results for the cipher images produced by the proposed image encryption algorithm are summarized in Table 7. Ideally, the image encryption algorithm should be able to have significant quality degradation in the images so that no pattern/feature remains present in the cipher images leading to a clue for analysing and decoding the information about plaintext

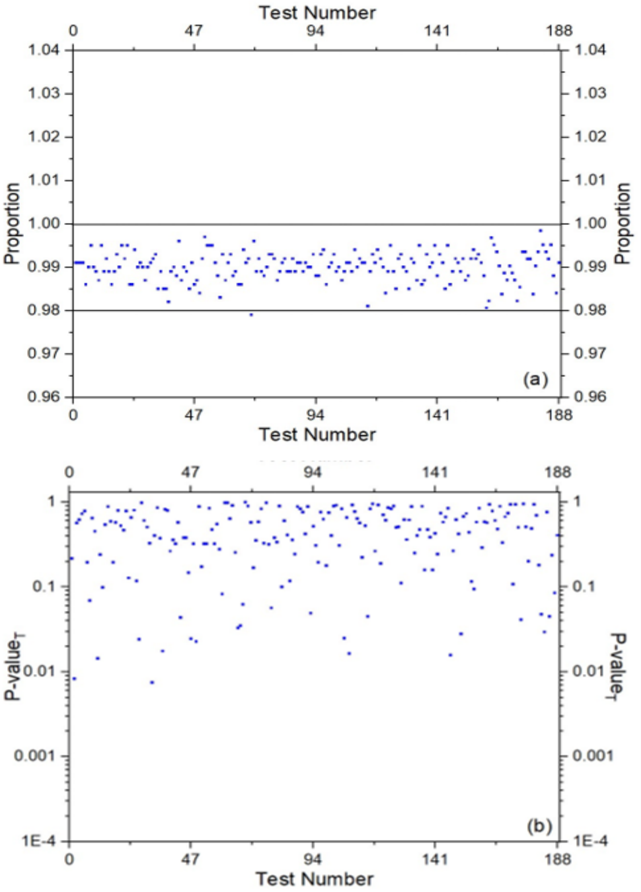


Figure 6 NIST Testing of pseudorandom sequences

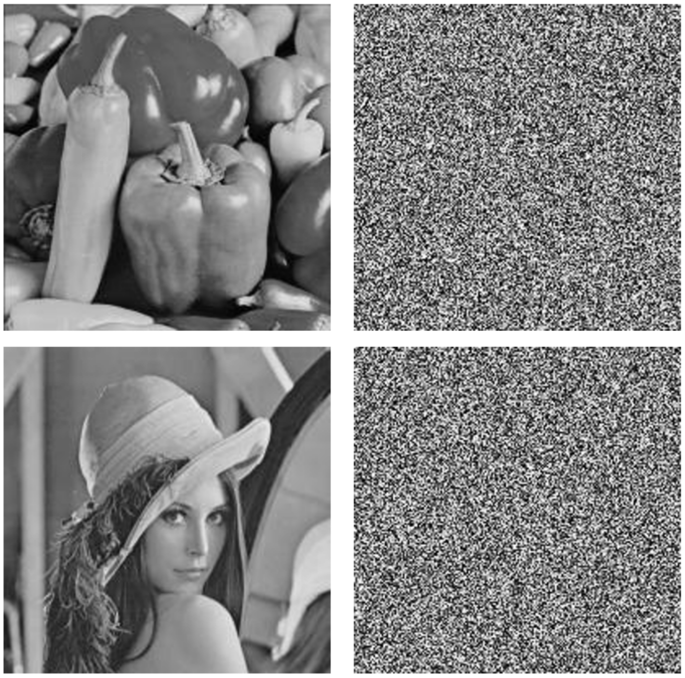


Figure 7 Plain images ‘Peppers’ and ‘Lena’ (first column) along with corresponding cipher images (second column) obtained with the proposed image encryption algorithm.

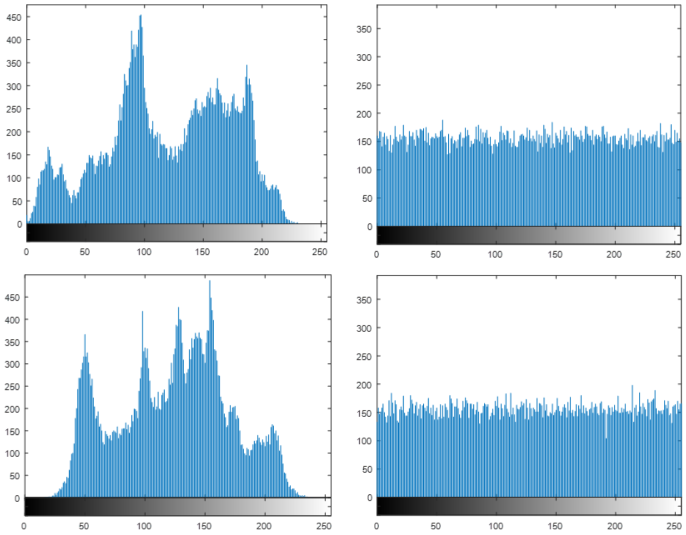


Figure 8 Histograms of ‘Peppers’ and ‘Lena’ (first column) and corresponding encrypted images (the second column).

images. The results of our computation of various perceptual quality metrics are given in Table 7. We may observe that the encrypted images possess very low perceptual quality.

As the proposed image encryption is based on the conversion of image pixels into DNA sequences followed by operations like XORing and complementing of the DNA bases in the DNA sequences of the image pixels, we have also done some analysis on the DNA sequences of the plain images and the cipher images generated through the proposed image encryption technique. We have computed the ‘Hamming distance’ between the DNA sequences of plain and cipher images, it measures the dissimilarity between the sequences in terms of DNA bases. The results have been shown in Table 8 which shows that the hamming distance is very large (almost 120K) which indicates the 75% dissimilarity in the DNA sequences of cipher and plain images. We have also computed the ‘Base Ratio’ for all the four DNA bases (A, T, C and G) in the DNA sequences of plain and cipher images. The base ratio is the percentage of occurrence of a particular base in the given sequence. The results have been summarized in Table 9. It is clear that all the bases have almost 25% occurrence in the plain as well as cipher images. It also conveys that while encoding the plain image into the DNA sequence in the proposed image encryption algorithm, sufficient randomness has been introduced so that the base distribution is almost uniform even in the DNA sequence of the plain image.

The information entropy is the measure of disorder. We have computed the information entropy for the whole of plain and cipher images (i.e., global information entropy) as well as the average of information entropy by dividing it into a finite number of non-overlapping blocks (i.e., local information entropy). The results have been shown in Table 10 which confirms that for the encrypted images, the global information entropy is very near to 8-bits and the local information entropy is also close to the global entropy and well above the desired thresholds.

To check the robustness of the proposed image encryption algorithm against the known-plaintext attack, we have also done a differential analysis of the proposed image encryption. For this purpose, we make a small change in the plain image (usually only one pixel) and compare the cipher images corresponding to two plain images with only a one-pixel difference and encrypted with the same secret key. We compute two metrics Net Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) and the results are shown in Table 11. It shows that these computed values of NPCR are higher than the theoretical/ideal critical value and computed values of UACI lie within the theoretical/ideal range obtained for a pair of random images, therefore, the two encrypted images, produced for the two plain images differing by only one-pixel value, are random like. Hence, the proposed image encryption algorithm is sensitive to the plaintext and robust against any differential attack.

For brevity, we have not provided the mathematical details/statistics of all the metrics used in the performance analysis. We refer the readers to (Kaur *et al.* 2022a; Patidar *et al.* 2011; Xue *et al.* 2020; Patidar and Kaur 2023; Wu *et al.* 2011) for complete details.

CONCLUSION

A novel image encryption algorithm utilizing the robust chaos-based dynamic DNA coding, DNA XORing and DNA Complementing is proposed. Though there are other DNA-Chaos-based schemes already available in literature but to the best of our knowledge, the proposed scheme is novel in its approach towards utilizing the dynamical behaviour of chaos for random selection of one of the DNA rules. Secondly, the chaotic map is carefully selected for its robustness due to the absence of periodic windows over the entire key space. The proposed algorithm possesses all the essential features of a practical image encryption algorithm. Various statistical measures, perceptual quality metrics, information entropy, plaintext sensitivity measures (NPCR, UACI), measures based on DNA sequences (Hamming distance, base ratio) etc. have been used to analyze the performance of the proposed image encryption algorithm and the results show the robustness of the proposed image encryption algorithm against any statistical or cryptanalytic attacks. In future, we will present different combinations of chaos/hyperchaos and DNA rules for a comparative analysis of our proposed work with the existing schemes in terms of speed and complexity as well.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Adleman, L. M., 1994 Molecular computation of solutions to combinatorial problems. science **266**: 1021–1024.

Andrecut, M. and M. Ali, 2001 Robust chaos in smooth unimodal maps. Physical Review E **64**: 025203.

Chai, X., X. Fu, Z. Gan, Y. Lu, and Y. Chen, 2019 A color image cryptosystem based on dynamic dna encryption and chaos. Signal Processing **155**: 44–62.

Dagadu, J. C., J. Li, E. O. Aboagye, and F. K. Deynu, 2019 Medical image encryption scheme based on multiple chaos and dna coding. Int. J. Netw. Secur. **21**: 83–90.

Gehani, A., T. LaBean, and J. Reif, 2004 Dna-based cryptography. Aspects of molecular computing: essays dedicated to tom head, on the occasion of his 70th birthday pp. 167–188.

Hennelly, B. M. and J. T. Sheridan, 2003 Image encryption and the fractional fourier transform. Optik **114**: 251–265.

Kaur, G., R. Agarwal, and V. Patidar, 2022a Color image encryption scheme based on fractional hartley transform and chaotic substitution–permutation. The Visual Computer **38**: 1027–1050.

Kaur, G., R. Agarwal, and V. Patidar, 2022b Image encryption using fractional integral transforms: Vulnerabilities, threats, and future scope. Frontiers in Applied Mathematics and Statistics **8**: 1039758.

Patidar, V., 2022 Development of new designs of secure image encryption schemes utilizing robust chaos & discrete fractional transforms. SERB India MATRICS Project Completion Report, SERB/MTR/2018/000203 .

Patidar, V. and G. Kaur, 2023 A novel conservative chaos driven dynamic dna coding for image encryption. Frontiers in Applied Mathematics and Statistics **8**: 1100839.

Patidar, V., N. Pareek, G. Purohit, and K. Sud, 2011 A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Optics communications **284**: 4331–4339.

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

Teh, J. S., M. Alawida, and Y. C. Sii, 2020 Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications **50**: 102421.

Wang, X., Y. Wang, X. Zhu, and C. Luo, 2020 A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level. Optics and Lasers in Engineering **125**: 105851.

Wang, X.-Y., Y.-Q. Zhang, and X.-M. Bao, 2015 A novel chaotic image encryption scheme using dna sequence operations. Optics and Lasers in Engineering **73**: 53–61.

Wu, Y., J. P. Noonan, S. Agaian, *et al.*, 2011 Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) **1**: 31–38.

Xiao, G., M. Lu, L. Qin, and X. Lai, 2006 New field of cryptography: Dna cryptography. Chinese Science Bulletin **51**: 1413–1420.

Xue, X., D. Zhou, and C. Zhou, 2020 New insights into the existing image encryption algorithms based on dna coding. Plos one **15**: e0241184.

Zeraoulia, E., 2012 *Robust chaos and its applications*, volume 79. World Scientific.

Zhang, J., D. Fang, and H. Ren, 2014 Image encryption algorithm based on dna encoding and chaotic maps. Mathematical Problems in Engineering **2014**: 1–10.

How to cite this article: Patidar, V., and Kaur, G. Lossless Image Encryption using Robust Chaos-based Dynamic DNA Coding, XORing and Complementing. *Chaos Theory and Applications*, 5(3), 178-187, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp. 188-197
https://doi.org/10.51537/chaos.1348302

Anomaly Detection in Cyber Security with Graph-Based LSTM in Log Analysis

Yusuf Alaca [*,1], **Yüksel Çelik** [α,2] **and Sanjay Goel** [β,3]
[*]Osmancık Omer Derindere Vocational School, Hitit University, Corum, Turkiye, [α]Department of Computer Engineering, Karabuk University, Karabuk,Turkiye, [β]University at Albany, State University of New York BA 310b, 1400 Washington Ave. Albany, NY 12222, USA.

ABSTRACT Intrusion detection systems utilize the analysis of log data to effectively detect anomalies. However, detecting anomalies quickly and effectively in large and heterogeneous log data can be challenging. To address this difficulty, this study proposes the GLSTM (Graph-based Long Short-Term Memory) framework, a graph-based deep learning model that analyzes log data to detect cyber-attacks rapidly and effectively. The framework involves standardizing the complex and diverse log data, training this data on an artificial intelligence model, and detecting anomalies. Initially, the complex and diverse log data is transformed into graph data using Node2Vec, enabling efficient and rapid analysis on the artificial intelligence model. Subsequently, these graph data are trained using LSTM (Long Short-Term Memory), Bi-LSTM, and GRU(Gated Recurrent Unit) deep learning algorithms. The proposed framework is tested using Hadoop's HDFS dataset, collected from different systems and heterogeneous sources, as well as the BGL and IMDB datasets. Experimental results on the selected datasets demonstrate high levels of success.

KEYWORDS
Anomaly detection
Graph
Node2Vec
Deep learning
Cyber security
HDFS

INTRODUCTION

Logging is the process of collecting numerical and textual data that captures the behavior of software, including events like low memory conditions or attempts to access files. The current focus of logging practices primarily revolves around the storage and organization of logs (Wang *et al.* 2019). Logging mechanisms consist of extensive datasets of log statements and their corresponding activation codes, which are implemented either by developers or specific software platforms.

In large internet networks, analyzing event and system-based logs using a combination of multiple systems, software, and hardware is crucial. Since log records are collected from devices and software responsible for system security, they often contain traces of attacks carried out by malicious actors during or after an attack. Therefore, it is essential to analyze log records and detect anomalies resulting from these traces in order to identify cyber-attacks (Elbasani and Kim 2021).

Numerous techniques have been developed to address the challenges associated with log analysis and anomaly detection. These techniques include frequent pattern mining, heuristics, clustering, evolutionary algorithms, and deep learning (He *et al.* 2020). However, it has been observed that these techniques are not as effective and efficient in detecting log anomalies as our proposed method.

To overcome these challenges, comprehensive log data collected from various devices and software in different structures needs to be converted into a standardized format for analysis. Additionally, it is necessary to analyze standardized data effectively and efficiently in order to detect attacks (Li and Li 2020).

In this study, we propose a framework that converts diverse log data into graphs and detects anomalies using deep learning methods. Our framework utilizes the node2vec algorithm, which is a semi-supervised and heuristic approach, to convert different log data into graphs. By leveraging node2vec, we can scale feature learning and select adjacent nodes through a random walk approach between nodes. This algorithm offers flexibility due to its adjustable parameters (Grover and Leskovec 2016).

For the deep learning component of our framework, we employ the LSTM algorithm, which is a type of recurrent neural network (RNN). Unlike traditional RNNs, LSTM networks address issues such as gradient weakening or gradient bursting that can occur in redundant neural networks (Hochreiter and Schmidhuber 1997).

Manuscript received: 23 August 2023,
Revised: 5 October 2023,
Accepted: 18 October 2023.

[1] yusufalaca@hitit.edu.tr (**Corresponding author**).
[2] yuksel.celik@karabuk.edu.tr
[3] goel@albany.edu

LSTM networks also utilize feedback connections instead of solely relying on feed-forward connections. In this study, the data is first transformed using the node2vec algorithm and then inputted into the LSTM algorithm. Our experiments have demonstrated that this approach achieves high accuracy in detecting anomalies.

When examining the literature, four different methods have been employed in studies on log anomaly detection. These methods are as follows: 1. Stencil removal, 2. Document management, 3. System monitoring, and 4. Learning-based anomaly detection. Several studies have focused on template extraction within these methods.

The template extraction method aims to extract word frequencies from log files, identify abnormal words, and detect anomalies. To be considered a template, terms must surpass a certain threshold. IPLoM, for instance, is a study that employs this method, recursively splitting log records assuming equal line lengths (Makanju *et al.* 2009).

Another study utilizing the template extraction technique applies deep learning to sequentially stored log records, using natural language processing to detect anomalies. Anomalies are detected when the sequential order is disrupted or when log records deviate from the expected flow. Meaningful words are extracted from log records and organized into templates. These templates are then converted into vectors, a method referred to as template2vector (Meng *et al.* 2019a). LSTM, a deep learning algorithm, is utilized in this study, with HDFS and BGL datasets employed for testing purposes(Alaca and Çelik 2023).

Document management, particularly using the Word2Vec method, is also prominent in log anomaly detection. Word groups are created, dividing words into different categories such as sentences and paragraphs based on the dataset size (Church 2017). In another study employing this method, natural language processing techniques are applied to detect anomalies in Thunderbird logs and system log records. Word2Vec and TF-IDF feature extraction algorithms are used, and the LSTM deep learning algorithm is employed for classification analysis (Wang *et al.* 2018).

System monitoring is another method used for anomaly detection. Log records from various systems can be monitored, and an exemplary tool in this context is Google's Dapper tool. This tool has demonstrated high success in complex, large-scale distributed systems (Sigelman *et al.* 2010).

In the literature, numerous studies are based on learning approaches, utilizing various machine learning techniques. DeepLog is a prominent study for log anomaly detection. The proposed approach consists of two main parts: defining the log key and establishing a workflow that includes anomaly parameters. The anomaly parameters are converted into vectors based on the log key, and the LSTM algorithm from artificial neural networks is employed to detect anomalies corresponding to the log key. The algorithm also incorporates manual feedback to improve accuracy (Du *et al.* 2017).

In another study, the CNN algorithm, a deep learning technique, is employed for anomaly detection from log records (Lu *et al.* 2018). This study identifies keywords in log records and detects anomalies based on these keywords. The identified keywords are digitized, normalized, and transformed into a 29x128 vector. This method is referred to as logkey2vector.

Deep learning is further explored in a study where different models are developed using datasets such as BGL (BlueGene/L), Thunderbird, Openstack, and IMDB (Internet Movie Database). The IMDB dataset is used to demonstrate the generalizability of the proposed model for other text classification problems. Positive and negative labeled data are fed into two distinct Autoencoders to enhance understanding of the original data, and the output is used as input for deep learning algorithms such as LSTM, BLSTM, and GRU (Farzad and Gulliver 2019).

An alternative approach to log anomaly detection aims to detect subsets of the original data space by making multiple passes over the entire dataset using frequent pattern mining. This approach involves three steps: summarizing the data by traversing the dataset, generating cluster candidates through another pass, and selecting suitable clusters from the candidates (Vaarandi 2003).

Graph structures have been employed in multiple studies for anomaly detection from log records. In one study, authentication logs are analyzed using graph structures to prevent unauthorized access to the operating system. A graph clustering method is developed specifically for forensic computing (Studiawan *et al.* 2017).

Another study utilizing graph structures detects anomalies from log data using time series and kill chain mechanisms. This advanced method creates attack profiles and simulates daily attacks on computer networks (Schindler 2017).

Graph structures have also been utilized in a study aiming to detect software errors in cloud computing (Yan *et al.* 2015). This method converts the complex relationships between log records into a graph and assigns importance scores to each log. The log anomaly detection method developed through this approach effectively identifies software errors.

In conclusion, various methods have been explored in the literature for log anomaly detection. These methods include stencil removal, document management, system monitoring, and learning-based approaches. Template extraction, deep learning algorithms like LSTM and CNN, as well as graph structures, have been utilized to detect anomalies in log records. Each method has its strengths and limitations, and further research is needed to enhance the accuracy and efficiency of log anomaly detection techniques.

It is crucial to continue advancing the field of log anomaly detection as it plays a vital role in ensuring the security and reliability of systems and networks. By detecting anomalies and potential cyberattacks, these techniques contribute to early threat identification and mitigation. Future research should focus on refining existing methods, exploring new algorithms, and leveraging emerging technologies to improve the effectiveness and scalability of log anomaly detection systems.

The aim of this study is to transform raw log data into meaningful and analyzable information that can effectively identify log anomalies. We achieve this by combining the node2vec and LSTM algorithms and applying them to the Hadoop HDFS dataset collected from multiple sources.

MATERIALS AND METHODS

The architecture of this study is based on the use of two algorithms together. First, the data converted to templates was vectorized using the Node2Vec algorithm to analyze it in deep learning algorithms. Then, this vectorial data was given as input to the LSTM algorithm, and models were created for anomaly detection; thus, anomaly detection was performed.

There are three types of anomalies in anomaly detection from log data. The first of these anomalies is the point anomaly. A point anomaly is data that deviates significantly from the mean or normal distribution of the remaining data (Gogoi *et al.* 2011). The second is the contextual anomaly. Contextual abnormality is an abnormal behavior confined to a specific context and standard in other contexts (Ahmed *et al.* 2016). The third is the collective anomaly. Unlike contextual and point anomalies, aggregate anomalies appear in the data as abnormal values. Aggregate anomalies are the abnormal behavior of a collection of data samples relative to the entire dataset (Li *et al.* 2015).

Log anomaly detection identifies abnormal system patterns in log data that do not conform to expected behavior. This section discusses our work based on the algorithms adopted here. The outline of our study is shown in Fig. 1. First, raw log data were taken from different log groups and made meaningful by removing unnecessary and noisy data. Templates were created from this log data and given input to the Node2Vec algorithm to generate the feature vector. Model training was done with the LSTM algorithm, and anomaly detection was made with these trained models.

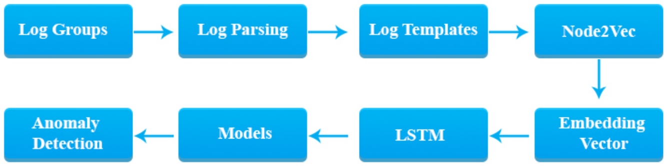


Figure 1 Flow chart of the proposed model algorithm.

Log parsing

Analysis of log data takes numerical and categorical data as input. This requires cleaning, sorting, and normalizing the raw log data. Log records consist of two main parts. Head part and text part. The head part usually consists of several features such as timestamps, hostnames, and severity of events. The developers manually predefine text message input. This can vary significantly between systems, even within one. These messages also consist of two parts: fixed messages and variable messages.

Each raw log data consists of two parts. One of them is the timestamp, and the other is the log complement part. The timestamp records the time of each log occurrence. Timestamps in different formats can be easily extracted from raw log data during log parsing, as they are regular expressions. A log identifier is a token that identifies multiple processes or message exchanges of the system(Du *et al.* 2017).

Log data $X_1,X_2,X_3,X_4 \ldots X_n$ let be created. These log data are $T_1,T_2,T_3,T_4 \ldots T_n$ corresponds to log templates. T_K is log parsing method, date(t), time(z), pid(p), type(r), component(b), content(i), templateid(j), template(l), and anomaly(k) performs the separation process.

$$t,z,p,r,b,i,j,l,k = T_K(\mathrm{X}) \tag{1}$$

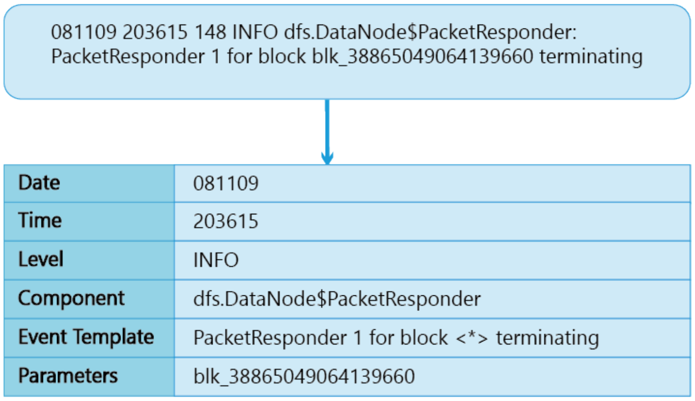
As a result of the log parsing method;

$$k = \left\{ \begin{matrix} 0 & Normal \\ 1 & Abnormal \end{matrix} \right\} \tag{2}$$

After creating the log templates in Eq.(1), they are transferred to the Node2Vec algorithm. With the embedding vector resulting from this algorithm, training and test data are created from the labeled abnormal data in Eq.(2).

As seen in Table 1, the first part is seen as a timestamp, the other part as a log complement. Thus, some of the log data contains numerical data, and the other part contains verbal data. Each word in the log data can be used as a log keyword or parameter. Log parameters usually consist of IP addresses, MAC information, or user information. Log anomaly detection is generally detecting that the log data is not abnormal. The presence of "INFO" in the log data does not mean that the log data is normal. It is unknown if parsing log data for this is abnormal or not. The purpose of log parsing is to extract meaningful data from raw log data. Thus, using these data, analyzes are made, and models are created.

To automatically analyze the logs, it is necessary to convert them into appropriate formats that can fit textual and machine learning algorithms. To analyze the log data, its unique parts must be determined. As shown in Fig. 2, unique templates were produced by labeling the parts with different similarity ratios in the log records.



```
081109 203615 148 INFO dfs.DataNode$PacketResponder:
PacketResponder 1 for block blk_38865049064139660 terminating
```

Date	081109
Time	203615
Level	INFO
Component	dfs.DataNode$PacketResponder
Event Template	PacketResponder 1 for block <*> terminating
Parameters	blk_38865049064139660

Figure 2 Log parsing steps for each log row.

Logs are preprocessed during log parsing. The values in the timestamp in Table 2 are also separated as date, time, and PID. Since each log template is different from the other, each template is labeled as TemplateID. Component and content parts were also subjected to separation under a different column.

Architecture of the Proposed Model Algorithm

It is challenging to detect anomalies in log analysis. Because log data consists of both numerical and categorical data. To be able to analyze these data, certain preprocesses are required. Different preprocessing techniques are applied to each study dataset mentioned in Section 2. Thus, the feature is extracted from the data set and made into a vector. Later, this vectorial data set was analyzed with deep learning algorithms, and anomaly detection was made.

In this study, the GLSTM algorithm is proposed. This algorithm consists of two stages. In the first stage, the data was transferred to a graph after converting the data into templates without making attributes from the data set. For this study, the Node2Vec algorithm, one of the graph algorithms, was used. Because it is the most effective algorithm for obtaining a vectorial data set for analyzing data. Experimental tests have proven that this algorithm is suitable and adequate for this study. The second stage is the analysis and classification process. At this stage, LSTM, one of the deep learning algorithms, was used. This algorithm is an iterative deep learning algorithm. It is one of the most preferred algorithms for detecting anomalies in log analysis. As a result of the experimental tests, a high success rate was obtained using Node2Vec and LSTM in anomaly detection.

The structure of the GLSTM architecture is shown in Fig. 3. When the structure is examined, log data from multiple heterogeneous sources is taken, and templates are created. Since the graph

Table 1 Raw log data structure.

Raw Log Data
081109 203615 148 INFO dfs.DataNode$PacketResponder: PacketResponder 1 for block blk_38865049064139660 terminating
081109 204005 35 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.73.220:50010 is added to blk_7128370237687728475 size 67108864
081109 214529 2747 WARN dfs.DataNode$DataXceiver: 10.251.123.132:50010: Got exception while serving blk_3763728533434719668 to /10.251.38.214:
081109 220032 3137 WARN dfs.DataNode$DataXceiver: 10.250.14.196:50010: Got exception while serving blk_-305633040016166849 to /10.251.38.53:

Table 2 Assigning log preprocessing parameters.

NoID	1,2,3,. . . ..
Date	081109 , 081110, ...
Time	203615, 203807, 204005
PID	148, 222, 35, 308, 329, ...
Level	INFO, WARN
Component	dfs.DataNode*PacketResponder, dfs.FSNamesystem, dfs.DataNode*DataXceiver

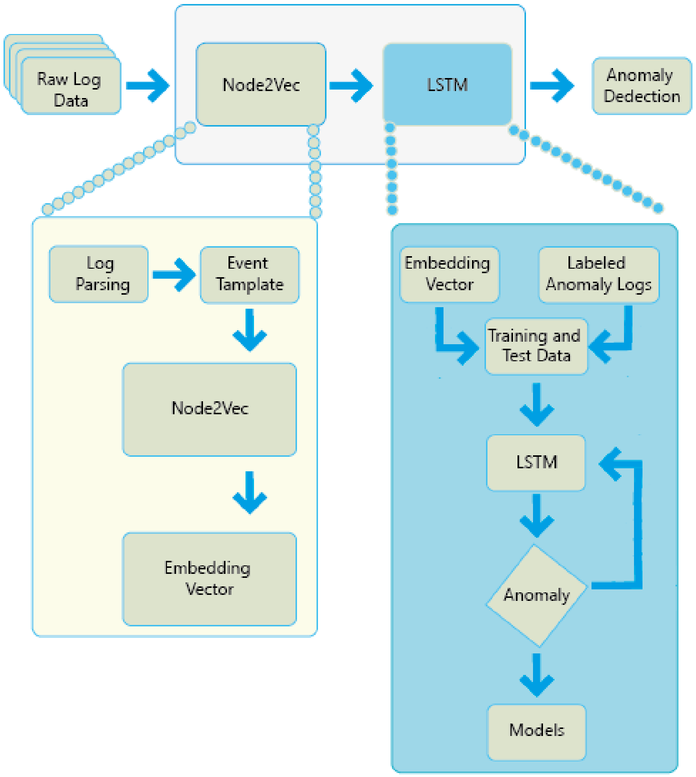


Figure 3 Proposed Model Architecture structure.

algorithm accepts the data set as numerical, the categorical part of the data set of these templates was digitized. Digitization was done by two methods used in the literature. One of them is Label Encoding, and the other is One Hot Encoding. The graph structure was created by giving the digitized data set to the Node2Vec algorithm as an edge and a node. A vectorial result was obtained from this graph structure. By providing this result as an input to the LSTM algorithm, log anomaly detection was made.

Exporting data to graph

The Node2Vec algorithm, one of the graph algorithms, has been developed as an alternative to the word2vec algorithm, a natural language processing algorithm. Although it was designed with natural language processing in mind, this algorithm has been used in more than one area. The approach of this algorithm uses probability to maximize the neighborhood of each node in the network in a d-dimensional feature space. A random walk approach is used to obtain the network neighborhood of the nodes.

The classical search algorithms in the graph are shown in Fig. 4. One of these algorithms is Breadth Priority Sampling (BFS), and the other is Depth Priority Sampling (DFS). It seems that BFS can detect close quarters, whereas DFS can detect distant neighborhoods. With its flexible structure, Node2Vec uses these two approaches together. Probability was used to find neighborhoods by taking a random walk. Semi-supervised operation in unweighted and undirected networks achieved better results than classical search approaches BFS and DFS(Grover and Leskovec 2016).

The structure of the Node2Vec algorithm differs from other algorithms. This algorithm takes four parameters. These are p, q, random walk, and walk length parameters. It is an algorithm that works as a semi-control as optimum results are obtained by

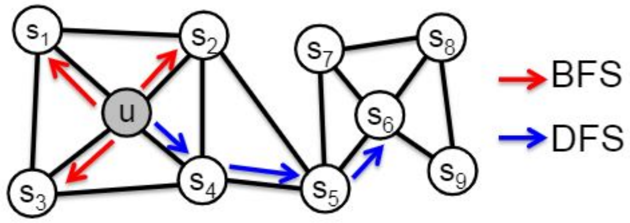


Figure 4 Classical search graph algorithms(Grover and Leskovec 2016)

changing these parameters. Of these parameters, p is the return parameter. It reduces the probability of sampling the previously visited node. The other parameter q is the input-output parameter. With this parameter, previously unvisited nodes are visited. If $q > 1$, the random walk is performed around the more visited node. In this respect, it is similar to the BFS algorithm. If $q < 1$, the random walk visits previously unvisited nodes. In this respect, it is similar to the DFS algorithm.

To get vector data from the Node2Vec algorithm, it needs to be exported to a Graf. In this study, StellarGraph was used because machine learning and deep learning structures are easy to use (CSIRO's Data61 2018). The main reasons for using this graphic structure are; 1. It can be used for visualization and various machine learning, 2. Ability to extract features from nodes and edges, 3. Applicable in big data, 4. Classification of nodes, It can perform many operations, such as easy and applicable. Multiple studies have been conducted on deep learning and machine learning using this graph structure(Rong 2014; Demeester *et al.* 2016; Kipf and Welling 2016).

The following procedure was followed for transferring the data to Graph. Graphs are made up of edges and nodes. Nodes, on the other hand, need to go from a specific source to the destination. TemplateID, which is different for each template, was chosen as the source, and anomaly or normal column was chosen for the target. The remaining columns are used for nodes. In Fig. 5, the edges and nodes of the data transferred to the Graph are shown.

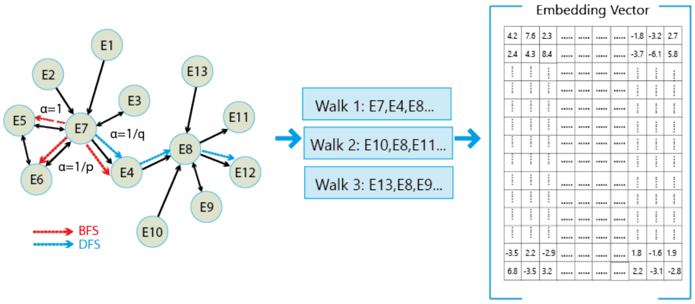


Figure 5 Data exported to graph.

Anomaly Detection

LSTMs are members of repetitive RNNs. RNNs are self-repetitive models, taking sequential data one item at a time. Compared to Markov models, although state-space sets increase, they give better results in the long run due to dependency(Specht 1990; Werbos 1988). LSTMs were developed to eliminate the disadvantages of RNNs. LSTMs work recursively like RNNs, the difference being that they run on different cells with their hidden display.

Fig. 6 shows the use of the LSTM algorithm in this study. Input data is used HDFS verse which Hadoop collects from multiple sources. These data were digitized with 1-hot encoding and label encoding methods. Then, these data are given to the Node2Vec algorithm as an input parameter, and an embedding vector is created as an output. Anomalous log data labeled with this embedding vector is provided as input parameters to the LSTM algorithm. Thus, models that detect abnormal values are created.

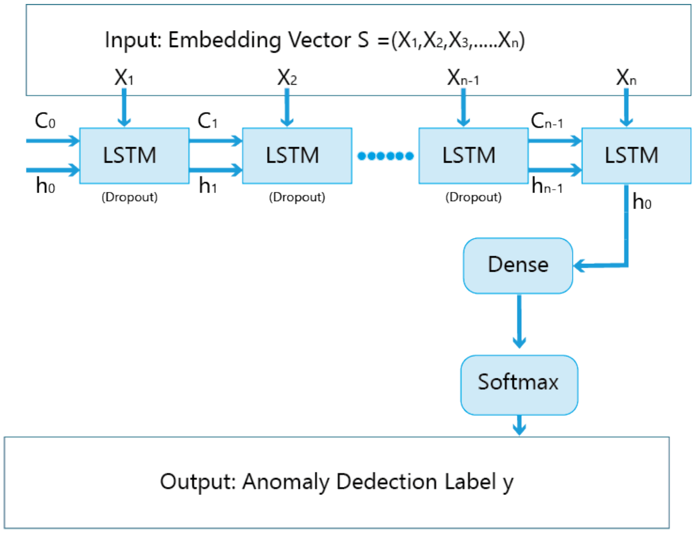


Figure 6 Anomaly detection in the proposed model.

RESULTS AND DISCUSSION

This study proposes a model to analyze log records to detect cyberattacks and to detect the anomalies created by the traces left by the attackers in the log records. HDFS dataset was used to test this model. The HDFS log dataset consists of 11,175,629 logs collected from more than 200 Amazon heterogeneous sources. HDFS log data records operations such as allocation, duplication, and deletion in a specific block using block_id. This dataset comprises 575,061 log blocks and has been labeled 16,838 abnormal by Hadoop's experts. Table 3 gives information about the HDFS data set.

The BGL dataset consists of a comprehensive collection of 4,747,963 logs, meticulously labeled as either anomalous or normal. Among these logs, 348,460 instances have been classified as anomalous. The BGL dataset was obtained from the Blue Gene/L supercomputer, a highly sophisticated computing system employed at Lawrence Livermore National Laboratory (LLNL). With its extensive infrastructure consisting of 128K processors, the Blue Gene/L supercomputer has played a crucial role in generating the BGL dataset for research and academic endeavors (Guo *et al.* 2021).

The IMDb dataset is a collection of film reviews. It comprises 50,000 reviews written by users on the IMDb website for various movies. The dataset includes reviews that have been labeled as positive or negative. The reviews are rated using a rating scale ranging from 1 to 10. Ratings between 1 and 4 are labeled as negative, while ratings between 7 and 10 are labeled as positive. Ratings of 5 and 6 are not included in the dataset. Each film has a maximum of 30 reviews. The IMDb dataset consists of 25,000 positive and 25,000 negative reviews (Tripathi *et al.* 2020).

Table 3 Detail of the datasets.

Dataset	Time	Log Line	Anomaly
HDFS	38,7 hours	11,175,629	16,838(block)
BGL	7 months	4,447,963	348,460(logs)
IMDB	-	50,000	25,000(negative)

Research Questions

Logging collects numerical and textual data of software behavior, such as low memory conditions or attempts to access a file. Log anomaly in modern software engineering is still challenging for three main reasons.

The main reasons for this are;

- Great effort is required for large volumes of logs and thus manual regular expression generation,
- The complexity of the software and, therefore, the variety of event templates,
- Frequency of software updates and hence frequent updating of logging statements.

In this study, templates were created for each row of log records, and these large-volume logs were made regularly by reducing their size using templates. Then, the embedding vector was created by establishing a relationship between these templates with the Node2Vec algorithm. The model was trained with LSTM, and anomaly detection was performed in the newly created log template.

Evaluation Metrics

A confusion matrix was used for the performance evaluation of experimental studies conducted to classify HDFS, BGL and IMDB datasets. In these experimental studies, the data was randomly partitioned into training, validation, and test sets, with 70% of the dataset allocated for training and 15% each for testing and validation. This data splitting strategy was employed to ensure reliable outcomes in the experiments. Performance metrics such as accuracy, sensitivity, specificity, precision, and F-score of the model were calculated using the confusion matrix. The calculation of these metrics is given in Eq. 3, 4, 5 and 6 mathematically.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

$$F1 = \frac{2 * TP}{2 * TP + FP + FN} \tag{6}$$

In the experimental studies, in the first stage, large volumes of log data were transformed into templates to reduce their size and make them regular. The Node2Vec algorithm was used to establish a relationship between these templates and to train the model with the deep learning algorithm. Then, model training was performed with the LSTM algorithm for anomaly detection. In the model created with this dataset, the LSTM input layer consists of 128, the hidden layer 64, and the output layer consists of 1 neuron to obtain the normal or abnormal result. As a result of the experimental study, an accuracy rate of 97.01% was obtained with the proposed model.

The performance results obtained with the proposed model are given in Table 4. The results vary depending on the datasets. In the tests conducted on the HDFS dataset, the LSTM method achieved an accuracy rate of 97.01%. The Bi-LSTM method followed closely with an accuracy rate of 96.98%. The GRU method demonstrated the highest performance with an accuracy rate of 98.15%. In the tests conducted on the BGL dataset, the LSTM method had an accuracy rate of 81.56%. The Bi-LSTM method performed slightly better with an accuracy rate of 84.21%. The GRU method exhibited the best performance with an accuracy rate of 86.44%. In the tests conducted on the IMDB dataset, the LSTM method achieved an accuracy rate of 97.40%, while the Bi-LSTM method outperformed with an accuracy rate of 98.54%. The GRU method showed the highest performance with an accuracy rate of 98.89%. Based on these experimental results, it can be observed that the GRU, Bi-LSTM, and LSTM methods perform differently on different datasets.

The Fig. 7 illustrates the progression of accuracy rates during the training and validation processes. The training accuracy curve represents the accuracy rate achieved on the training dataset, while the validation accuracy curve reflects the accuracy rate on the validation dataset. At the beginning of the graph, both the training and validation accuracy rates are low. However, as the training process progresses, the accuracy rates increase and eventually converge. This indicates that the model performs well on the training dataset and also provides good results on the validation dataset. Analyzing this graph is important to evaluate the model's performance during the training process and demonstrate the absence of issues such as overfitting or underfitting.

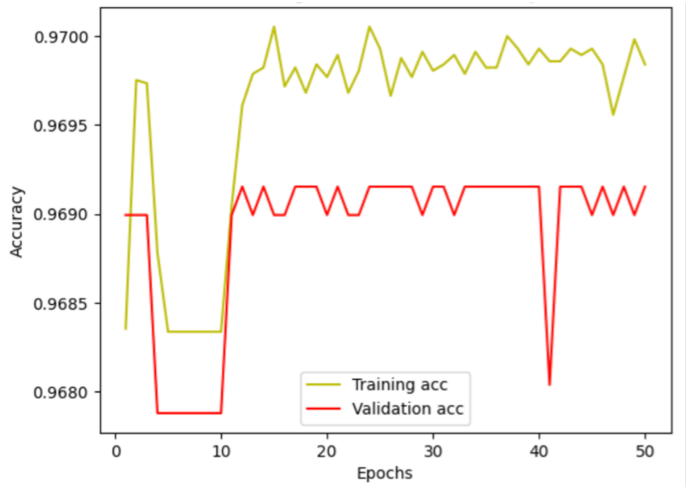


Figure 7 Training and Validation Accuracy Performance Curves.

Table 4 **Performance results of the proposed model.**

Datasets	Algorithm	Accuracy	Precision	Recall	F1_score	Average train time (second)
HDFS	LSTM	97.01	97.23	96.06	84.25	6.60
	Bi-LSTM	96.98	97.40	97.18	86.89	
	GRU	98.15	98.10	98.55	88.42	
BGL	LSTM	81.56	81.76	88.31	81.54	5.46
	Bi-LSTM	84.21	86.89	85.18	85.79	
	GRU	86.44	87.34	88.29	91.52	
IMDB	LSTM	97.40	95.99	98.18	95.89	7.21
	Bi-LSTM	98.54	97.44	97.39	96.22	
	GRU	98.89	97.49	98.28	97.36	

Fig. 8 illustrates the changes in training loss and validation loss during the training process. The training loss curve represents the loss on the training dataset, while the validation loss curve reflects the loss on the validation dataset. The graph shows that the training loss decreases over time, indicating that the model is learning and improving its performance. Initially, the validation loss also decreases, but at a certain point, it starts to increase again. This situation indicates that the model is not overfitting to the training data.

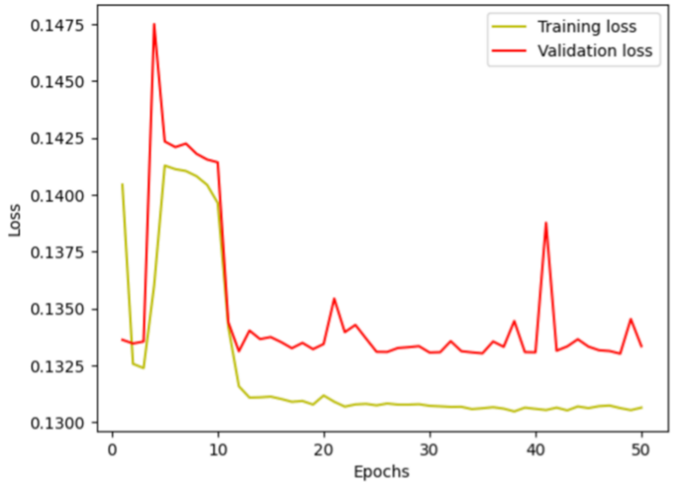


Figure 8 Training and Validation Loss Performance Curves.

The Confusion Matrix is given in Fig. 9, which shows the success status due to the tests performed in this study. This graph calculates the efficiency of the actual and predicted values. The important thing is that the estimated values obtained after training our model were compared with the actual values, and their accuracy was determined. This graph shows how many anomalies the actual anomaly detected after the model was trained. Thus, this graph shows that our model has achieved high success.

Two useful tools, AUC curves, are used to measure the outcome of experiments performed accurately. These curves are used to

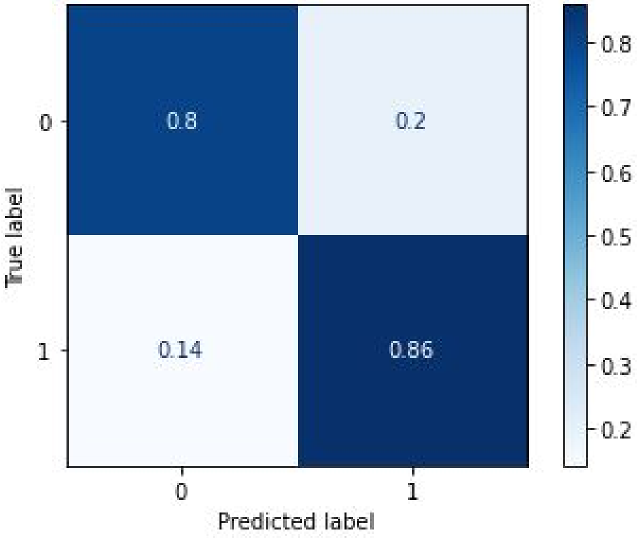


Figure 9 The confusion matrix of the experimental results of the proposed model.

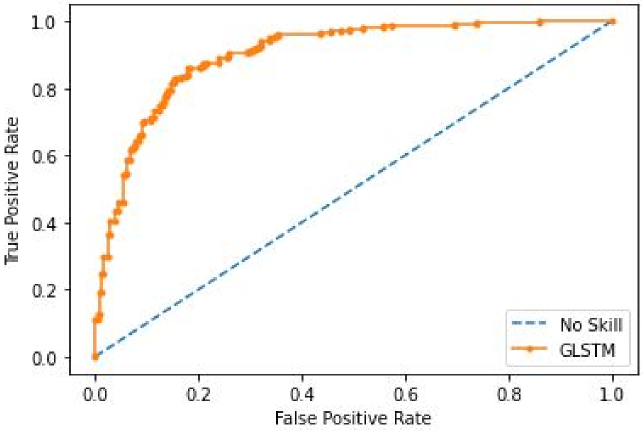


Figure 10 The graph of the AUC Curve.

eliminate two different errors. One of them is HPs. This error gives results as if there is an event when there is no event. The other is FN. This error also produces erroneous results because it does not detect the event when there is an event. Due to these two errors, the results of the experiments are not clearly understood. To avoid this, AUC curves are used.

$$TruePositiveRate = \frac{TP}{TP + FN} \tag{7}$$

$$TrueNegativeRate = \frac{TN}{FN + TN} \tag{8}$$

Two important ratios are calculated in the AUC curve. One of them is the True Positive Ratio shown in Eq. 7. The other is the True Negative Ratio shown in Eq. 8. Fig. 10 shows the graph of the AUC Curve. Smaller values on the graph's x-axis indicate lower false positives and higher true negatives. The graph's y-axis also shows larger values, i.e., higher true positives and lower false negatives. This shows that a good model shows a value higher than 0.5; the part is shown with dashed lines in the graph, that is, the threshold value. This shows that the model gives good results.

Another graph that measures the model accurately is the Precision – Accuracy graph. These curves are also called Sensitive Recall Curves. The precision shows how well the positive part of the model predicts, as shown in Eq. 8. The accuracy is shown in Eq. 3. This allows for a more accurate estimation of true positives. Fig. 11 shows the Precision vs. Accuracy graph. The integral of the area under the curve shows how accurately and accurately the model works.

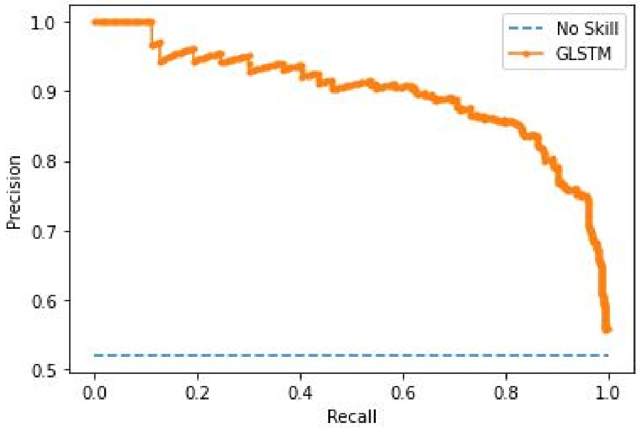


Figure 11 Precision-Accuracy Plot of the proposed model.

Competing Models

This study was carried out according to the method used, the dataset used, and the comparisons' accuracy with the previous run. Considering these criteria, comparisons for this use with other businesses are given in Table 5. LogAnomaly (Rodriguez *et al.* 1999) uses the same dataset as our proposed study and the same deep learning methods in the developed method. With LogAnomaly, primarily synonyms and antonyms were detected in the log data with Word2Vec. One sample for each log information is incorrect. These templates were then transferred to a vector and analyzed with LSTM. LogAnomaly faces significant challenges as log records consist of numeric and textual structures. Since the method we propose converts both numeric and textual data into graphs, it turned out to be in the size of such dimensions, and in fact, a better result was obtained than LogAnomay. DeepLog (Du *et al.* 2017) generates a key for each log information with a natural language processing method, and a vector result is obtained with the corresponding key. Anomaly data were made using this vectored LSTM. This method has difficulties analyzing numerical parts of log data at a certain level. Since the method we proposed analyzes using each feature of the whole data set, it achieved a more successful result despite using the same dataset and using this method. To reduce log anomaly, Bi-LSTM and PCA retentions (Meng *et al.* 2019b) were used with a dataset similar to our proposed work. With this work, the dataset was first separated and then made into templates. Then, it was converted into vectorial form with digitization and normalization processes. Although the examples we suggested used the same dataset, the model we did not particularly recommend was more successful than the results obtained with PCA. As a result, our proposed method has obtained more successful results than many previously applied models and evaluates that it can be used more effectively in daily anomalies.

In this study, graph structure was used instead of the NLP technique used in many studies. Node2vec from the graph algorithm is used. This algorithm was developed as an alternative to word2vec algorithms. In this study, it has been shown by tests that it achieves a better result than other algorithms in terms of decomposing logs and feature extraction.

To train deep learning network models and achieve high success in log anomaly detection, it should be brought to the level to be given as input to the model, especially after the log parsing process. In this study, the node2vec output vector was given to LSTM as input data, and 97.01% success was achieved. A better result was obtained than the methods using the NLP technique.

CONCLUSION

This study aims to make a large number of logs obtained from different sources in complex networks and uniformly contain different features and detect anomalies from them. The fact that the logs consist of huge and different data makes detecting fast and effective anomalies very difficult. For this reason, to process these different log data effectively and quickly, in this study, logs in different structures were turned into a template and then converted into a graph structure to obtain the relationships between these templates. Node2Vec, a graph algorithm, was used for graph transformation. The embedding vector of the log templates is obtained from this transformation. The obtained data containing these vector anomaly tags are divided into 70% training and 30% test data for the deep learning algorithm. These data were trained and tested using the LSTM algorithm, one of the deep learning methods. As a result of the tests, our Graf-based LSTM model, which we recommend, has achieved successful results with an accuracy of 97.01%.

Intrusion detection systems utilize the analysis of log data to effectively detect anomalies. However, detecting anomalies quickly and effectively in large and heterogeneous log data can be challenging. To address this difficulty, this study proposes the GLSTM (Graph-based Long Short-Term Memory) framework, a graph-based deep learning model that analyzes log data to detect cyber-attacks rapidly and effectively. The framework involves standardizing the complex and diverse log data, training this data on an artificial intelligence model, and detecting anomalies. Initially, the complex and diverse log data is transformed into graph data using Node2Vec, enabling efficient and rapid analysis on the artificial intelligence model. Subsequently, these graph data are

Table 5 Comparison of the proposed model with other payments.

Authors	Method	Datasets	Acc(%)
2019, Weibin Meng et al.(Rodriguez *et al.* 1999)	LSTM,Word2Vec	BGL,HDFS	96.00
2017,Min Du et al. (Du *et al.* 2017)	LSTM,tamplate2Vec	BGL,HDFS	92.00
2022, Zhang Yue et al.(Meng *et al.* 2019b)	Bi-LSTM,PCA	HDFS	95.60
2023, Proposed Method	LSTM,BGL,IMDB,Node2Vec	HDFS	97.01

trained using LSTM (Long Short-Term Memory), Bi-LSTM, and GRU (Gated Recurrent Unit) deep learning algorithms. The proposed framework is tested using Hadoop's HDFS dataset, collected from different systems and heterogeneous sources, as well as the BGL and IMDB datasets. Experimental results on the selected datasets demonstrate high levels of success.

Limitations of this study should be considered:

Data Diversity: Although this study was tested with Hadoop's HDFS dataset, its ability to generalize to datasets with greater diversity from various networks and systems may be limited. Specific anomalies based on different data types or sources could pose challenges. Data Size: Working with large datasets can be limited by computational resources and memory requirements. This study may provide limited insights into handling larger datasets. Feature Engineering: Data transformations and representation may pose challenges in feature engineering. Ensuring that data is accurately and meaningfully represented may not always be guaranteed. Training Data: The success of this study may be dependent on the specific datasets used and the training data. Results may vary with different datasets or data splitting strategies. Model Selection: This study employed specific deep learning algorithms like LSTM, Bi-LSTM, and GRU. The impact of these algorithms on model performance should be taken into account. Exploration of other deep learning methods may be warranted. Real-World Applications: The extent to which the study's results can be applied to real-world applications, generalize to specific network structures or systems, may require further investigation. These limitations should be considered for a better understanding of the study's findings and the real-world applicability of the model.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Ahmed, M., A. N. Mahmood, and M. R. Islam, 2016 A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems **55**: 278–288.

Alaca, Y. and Y. Çelik, 2023 Cyber attack detection with qr code images using lightweight deep learning models. Computers & Security **126**: 103065.

Church, K. W., 2017 Word2Vec. Natural Language Engineering **23**: 155–162.

CSIRO's Data61, 2018 StellarGraph Machine Learning Library.

Demeester, T., T. Rocktäschel, and S. Riedel, 2016 Lifted rule injection for relation embeddings. EMNLP 2016 - Conference on Empirical Methods in Natural Language Processing, Proceedings pp. 1389–1399.

Du, M., F. Li, G. Zheng, and V. Srikumar, 2017 DeepLog: Anomaly detection and diagnosis from system logs through deep learning. Proceedings of the ACM Conference on Computer and Communications Security pp. 1285–1298.

Elbasani, E. and J. D. Kim, 2021 LLAD: Life-Log Anomaly Detection Based on Recurrent Neural Network LSTM. Journal of Healthcare Engineering **2021**.

Farzad, A. and T. A. Gulliver, 2019 Log Message Anomaly Detection and Classification Using Auto-B/LSTM and Auto-GRU pp. 1–28.

Gogoi, P., D. K. Bhattacharyya, B. Borah, and J. K. Kalita, 2011 A survey of outlier detection methods in network anomaly identification. The Computer Journal **54**: 570–588.

Grover, A. and J. Leskovec, 2016 node2vec: Scalable Feature Learning for Networks .

Guo, H., S. Yuan, and X. Wu, 2021 Logbert: Log anomaly detection via bert. In *2021 international joint conference on neural networks (IJCNN)*, pp. 1–8, IEEE.

He, S., P. He, Z. Chen, T. Yang, Y. Su, *et al.*, 2020 A Survey on Automated Log Analysis for Reliability Engineering. arXiv preprint arXiv:2009.07237 .

Hochreiter, S. and J. Schmidhuber, 1997 Long Short-Term Memory. Neural Computation **9**: 1735–1780.

Kipf, T. N. and M. Welling, 2016 SEMI-SUPERVISED CLASSIFICATION WITH GRAPH CONVOLUTIONAL NETWORKS. Technical report.

Li, H. and Y. Li, 2020 LogSpy: System Log Anomaly Detection for Distributed Systems. Proceedings - 2020 International Conference on Artificial Intelligence and Computer Engineering, ICAICE 2020 pp. 347–352.

Li, Y., Y. Zheng, H. Zhang, and L. Chen, 2015 Traffic prediction in a bike-sharing system. In *Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 1–10.

Lu, S., X. Wei, Y. Li, and L. Wang, 2018 Detecting anomaly in big data system logs using convolutional neural network. Proceedings - IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, IEEE 16th International Conference on Pervasive Intelligence and Computing, IEEE 4th International Conference on Big Data Intelligence and Computing and IEEE 3 pp. 159–165.

Makanju, A. A. O., A. N. Zincir-Heywood, and E. E. Milios, 2009

Clustering event logs using iterative partitioning. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1255–1264.

Meng, W., Y. Liu, Y. Zhu, S. Zhang, D. Pei, *et al.*, 2019a Loganomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs. IJCAI International Joint Conference on Artificial Intelligence **2019-Augus**: 4739–4745.

Meng, W., Y. Liu, Y. Zhu, S. Zhang, D. Pei, *et al.*, 2019b Loganomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs. IJCAI International Joint Conference on Artificial Intelligence **2019-Augus**: 4739–4745.

Rodriguez, P., J. Wiles, and J. L. Elman, 1999 A recurrent neural network that learns to count. Connection Science **11**: 5–40.

Rong, X., 2014 word2vec Parameter Learning Explained pp. 1–21.

Schindler, T., 2017 Anomaly Detection in Log Data using Graph Databases and Machine Learning to Defend Advanced Persistent Threats. Technical report.

Sigelman, B. H., L. Andr, M. Burrows, P. Stephenson, M. Plakal, *et al.*, 2010 Dapper , a Large-Scale Distributed Systems Tracing Infrastructure. Google Research p. 14.

Specht, D. F., 1990 Probabilistic neural networks. Neural networks **3**: 109–118.

Studiawan, H., C. Payne, and F. Sohel, 2017 Graph clustering and anomaly detection of access control log for forensic purposes. Digital Investigation **21**: 76–87.

Tripathi, S., R. Mehrotra, V. Bansal, and S. Upadhyay, 2020 Analyzing sentiment using imdb dataset. In *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 30–33, IEEE.

Vaarandi, R., 2003 A data clustering algorithm for mining patterns from event logs. In *Proceedings of the 3rd IEEE Workshop on IP Operations Management (IPOM 2003)(IEEE Cat. No. 03EX764)*, pp. 119–126, Ieee.

Wang, M., L. Xu, and L. Guo, 2018 Anomaly detection of system logs based on natural language processing and deep learning. 2018 4th International Conference on Frontiers of Signal Processing, ICFSP 2018 pp. 140–144.

Wang, X., D. Wang, Y. Zhang, L. Jin, and M. Song, 2019 Unsupervised learning for log data analysis based on behavior and attribute features. In *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science*, pp. 510–518.

Werbos, P. J., 1988 Generalization of backpropagation with application to a recurrent gas market model. Neural networks **1**: 339–356.

Yan, X., W. Zhou, Y. Gao, Z. Zhang, J. Han, *et al.*, 2015 PADM: Page rank-based anomaly detection method of log sequences by graph computing. Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom **2015-Febru**: 700–703.

How to cite this article: Alaca, Y., Celik, Y., and Goel, S. Anomaly Detection in Cyber Security with Graph-Based LSTM in Log Analysis. *Chaos Theory and Applications*, 5(3), 188-197, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / **No.**3 / 2023 / **pp.**198-206
https://doi.org/10.51537/chaos.1321533

A New Fractional-order Derivative-based Nonlinear Anisotropic Diffusion Model for Biomedical Imaging

Alka Chauhan[*,1], **Santosh Kumar**[*,2] **and Yeliz Karaca**[α,3]
[*]Department of Mathematics, Sharda School of Basic Sciences and Research, Sharda University Greater Noida-201310 UP, India, [α]University of Massachusetts (*UMass*) Chan Medical School, Worcester, MA 01655, USA.

ABSTRACT Medical imaging, the process of visual representation of different organs and tissues of the human body, is employed for monitoring the normal as well as abnormal anatomy and physiology of the body. Imaging which can provide healthcare solutions ensuring a regular measurement of various complex diseases plays a critical role in the diagnosis and management of many complex diseases and medical conditions, and the quality of a medical image, which is not a single factor but a composite of contrast, artifacts, distortion, noise, blur, and so forth, depends on several factors such as the characteristics of the equipment, the imaging method in question as well as the imaging variables chosen by the operator. The medical images (ultrasound image, X-rays, CT scans, MRIs, etc.) may lose significant features and become degraded due to the emergence of noise as a result of which the process of improvement pertaining to medical images has become a thought-provoking area of inquiry with challenges related to detecting the speckle noise in the images and finding the applicable solution in a timely manner. The partial differential equations (PDEs), in this sense, can be used extensively in different aspects with regard to image processing ranging from filtering to restoration, segmentation to edge enhancement and detection, denoising in particular, among the other ones. In this research paper, we present a conformable fractional derivative-based anisotropic diffusion model for removing speckle noise in ultrasound images. The proposed model providing to be efficient in reducing noise by preserving the essential image features like edges, corners and other sharp structures for ultrasound images in comparison to the classical anisotropic diffusion model. Furthermore, we aim at proving the viscosity solution of the fractional diffusion model. The finite difference method is used to discretize the fractional diffusion model and classical diffusion models. The peak signal-to-noise ratio (PSNR) is used for the quality of the smooth images. The comparative experimental results corroborate that the proposed, developed and extended mathematical model is capable of denoising and preserving the significant features in ultrasound towards better accuracy, precision and examination within the framework of biomedical imaging and other related medical, clinical, and image-signal related applied as well as computational processes.

KEYWORDS
Anisotropic diffusion model
Nonlinear mathematical diffusion model
Fractional diffusion model
Fractional order derivatives
Biomedical imaging
Image processing
Denoising
Chaotic signals and noise
Image smoothing
Viscosity solution
Explicit scheme
Multiplicative noise
Conformable fractional derivative
Partial differential equations (PDEs)

INTRODUCTION

Nonlinear anisotropic diffusion equations ensure the enhancement of the image quality through the removal of noise while retaining the subtle details and edges (Gilboa *et al.* 2006). Image denoising is observed to be of utmost importance in image processing as well as in computer vision in order that images can be prepared with better resolutions. Given this, partial differential equations (PDEs) can extensively be employed in different aspects related to image processing rangining from filtering to restoration, segmentation to edge enhancement and detection, denoising in particular, amongst the other ones (Mazloum and Siahkal-Mahalle 2022). Chaos, as a ubiquitous phenomenon in nature, reveals that the observed chaotic and noisy signals are often disrupted by external interferences. Edge, as one of the most remarkable features for images, requires denoising via nonlinear means and wavelet transform to

Manuscript received: 1 July 2023,
Revised: 27 September 2023,
Accepted: 10 October 2023.

[1] alkachauhan5490@gmail.com
[2] skykumar87@gmail.com
[3] yeliz.karaca@ieee.org (**Corresponding author**).

attain optimal outcomes. When it comes to the image quality, if the additive degrades the quality of the images, it could be possible to end up with diagnostic failures. Ultrasonography, as a biomedical technique, produces the internal structure of the body and gives a great amount of information for clinical diagnosis and treatment. Considering these, detecting the additive noise in the images and finding the solution to such matters becomes a formidable challenge for researchers, clinicians, pharmaceutical authorities and related practitioners.

Speckle noise is the multiplicative noise, and the distorted image is the product of the original image and speckle noise. The Speckle noise can be expressed as:

$$u_0(i,j) = u(i,j) \times S_n(i,j),$$

where $u_0(i,j)$ denotes the noisy image, and let $u(i,j)$ denote the corresponding noiseless image and $S_n(i,j)$ represent the speckle noise.

Manifesting itself in the digital image in a randomly uncorrelated way, noise makes it unavoidable to degrade the visual quality of the images which restricts the accuracy and precision related to interpretation and examination processes. Imaging techniques ensure the generation of novel accurate imaging tools which have sensitivity, specificity and resolution at improving levels. Accordingly, image denoising employs advanced algorithms to remove noise from graphics, which makes an impact on the quality of the images. The impact of the environment, channels related to transmission as well as related factors cause contamination by noise, which brings about loss of image information and distortion. The recovery of the meaningful information from noisy images to obtain high quality in images is challenging, as noted above. In view of a perspective based on mathematical foundation, image denoising is stated to be an inverse problem whose solution is not unique (Fan *et al.* 2019). Image noise reduction and feature preserving stand to be other challenges as image noise removal shows a relevant matter in different image analyses and computer vision-related matters where retaining the essential image features like the edges, corners and other sharp structures during smoothing and other related processes (Barbu 2014).

Fractional calculus is capable of attaining a satisfactory denoising effect, and the application of its theory provides important inputs in image denoising. Thus, fractional calculus can weaken high-frequency signal and preserving low-frequency signal in a nonlinear way, which means high-frequency noise can be removed while the information of low-frequency image itself can be retained (Wang *et al.* 2020). Concerning fractional calculus, in image denoising and image restoration, fractional derivatives have been employed in different studies (Bai and Feng 2007; Chen *et al.* 2013; Hilfer 2000; Herrmann 2011). (Abirami *et al.* 2021) considered the classical anisotropic diffusion model under the Caputo fractional derivative with a variable order of derivative function and achieved better performance for biomedical images like ultrasound, CT scans, x-rays and so forth. (Fang *et al.* 2020) presented a time-fractional model under the Caputo fractional derivative to remove additive noise and applied binary block partition to discretize their model. Another work (Janev *et al.* 2011) introduced a new fractional anisotropic diffusion equation for the aim of noise removal which contained spatial and time fractional derivatives. To construct a numerical scheme, the proposed partial differential equation (PDE) was used to preserve the edges (Janev *et al.* 2011).

One other paper introduces a new class of fractional-order anisotropic diffusion equations to remove noise. The authors employ the discrete Fourier transform for the implementation of the numerical algorithm. Besides outlining the various numerical results regarding the denoising of real images, the experiments of the study demonstrate the proposed fractional-order anisotropic diffusion equations capacity to yield good visual effects and better signal-to-noise ratio (Bai and Feng 2007). A novel class of fractional-order nonlinear anisotropic diffusion equations based image restoration model is established employing the p-Laplace norm of fractional-order gradient of an image intensity function is introduced in another paper where fractional-order gradient helps to better accommodate the images texture details. Thus, the proposed method removed noise and kept high-frequency edge of images in an efficient way nonlinearly (Yin *et al.* 2015). Another research provides a novel fast fractional order anisotropic diffusion algorithm to remove noise removal. The authors improve the algorithms efficiency by implementing the fast explicit format iteration algorithm with periodic change of time step size. Showing numerical results on denoising tasks and presenting of the experimental results corroborate that the algorithm can obtain satisfactory denoising results more quickly (Zhang *et al.* 2021).

Regarding multiplicative noise removal, a paper uses a maximum a posteriori (MAP) estimator and the authors derive a functional with a minimizer corresponding to the denoised image desired to be recovered (Aubert and Aujol 2008). Concerning image segmentation, hybrid methods are said to provide benefits compared to conventional means in inhomogeneous image segmentation. Accordingly, (Chen *et al.* 2019) presents a new hybrid method to integrate image gradient, local environment and global information into a specific framework. Image segmentation method based on PDE reveals strong vitality terms of image processing and computer vision. A new simple well-behaved definition of the fractional derivative which is named conformable fractional derivative is handled in (Othman and Shaw 2021), where a geometrical approach of fractional derivatives was introduced. For the purpose of obtaining the solution of fractional order differential equation (FDE) with the integer-order initial condition, certain new criteria regarding fractional derivatives are proposed in the study. Finally, reducing denoise in images multiplicatively (DIM) is modified in (Ibrahim 2020) with the aim of presenting a new technique based on a new fractional calculus to solve the problem termed as conformable fractional calculus (CFC) which provides benefits due it its formula involving a controller to be implemented for complex problems like DIM. Another study (Karaca and Baleanu 2022) aims to construct a robust and accurate model, which is based on fractional-order calculus (FOC) and Artificial Neural Network (ANN) integration, concerned with differentiability prediction and diagnosis of stroke and breast cancer, which pose complex problems considering the diseases highly complex neurological and biological properties.

Furthermore, (Khalil *et al.* 2014) propose a definition of a conformable fractional derivative and provide some properties of a fractional derivative. The conformable fractional- order derivative is an extended version of the classical fractional derivative, and it is very efficient in terms of obtaining the solution of the fractional-order PDEs. Consequently, the conformable fractional derivative encompasses diverse applications in science, engineering, and so forth. (Zhao and kang Luo 2017) proposed the physical interpretation and application of the general conformable fractional derivative. Many applications of fractional derivatives and fractional integrals are discussed by (Butera and Paola 2014; Contreras *et al.* 2018; Cresson 2010; Zhao and kang Luo 2017; Zhou *et al.* 2018), and the analytic solution of the time-fractional heat equation is also pointed out, which may be further resorted to in (Hammad and Khalil 2014a,b).

Considering these ends, the model presented by (Catté *et al.* 1992), concerned with edge detection and image selective smoothing by nonliear diffusion, has been extended and developed to remove the additive noise for the ultrasound image. The improved model in the scheme of our study as proposed includes the time-fractional derivative with smoothness diffusivity, and subsequently, the viscosity solution of the fractional diffusion model is proven through the scheme in question as compared to other relevant and parallel stuies existing in the literature, the first approach to remove noise and preserve edges by partial differential equations based anisotropic diffusion model is proposed by (Perona and Malik 1990). The improved (Perona and Malik 1990) model for image restoration and edge detection is introduced by (Catté *et al.* 1992). They have used the smoothing diffusivity i.e. $G_\sigma * u$, G_σ is the Gaussian smoothing kernel. The diffusion tensor based anisotropic diffusion model is proposed by (Weickert 1997). The additive Gaussian white noise based anisotropic diffusion model for image denoising and deblurring is given by (Welk *et al.* 2005) They have proposed the forward-backward diffusivity to discretize diffusion model.

The weighted and well balanced based anisotropic diffusion model is given by (Prasath and Vorotnikov 2014). The smooth Gaussian kernel based diffusion model for image restoration is proposed by (Kumar and Ahmad 2014; Kumar *et al.* 2016). Accordingly, a fractional derivative-based nonlinear anisotropic diffusion model for biomedical imaging has been presented to reduce additive Gaussian white noise in this study. The fractional order a appears in the time derivative and finds the results with different fractional order α. The performance of the ultrasound images is measured by the PSNR values. The experimental results of the fractional and classical diffusion models are computed by the finite-difference explicit scheme. The results demonstrate that the proposed model (5) has larger PSNR values corresponding to (3) at the different iteration numbers. This study has been conducted to attain better results for ultrasound images based on the novel and extended scheme based on the motivational aspect that reducing noise in images is an essential task in image processing.

The rest of the paper is structured in the following manner: Section 2 introduces the definition of Conformable Fractional Derivatives. Denoising Based Time Fractional Diffusion Algorithm is given in Section 3 and Theoretical Considerations for the Diffusion Model are introduced in Section 4. In Section 5, Discretized Scheme for the Anisotropic Diffusion and Fractional Anisotropic Diffusion Model is provided and depicted. Section 6 addresses Experimental Results of the Diffusion Model and Fractional Diffusion Model. Finally, Section 6 provides Conclusion, Discussions and Future Directions.

CONFORMABLE FRACTIONAL DERIVATIVES

The conformable fractional derivative which contains many applications and the conformable fractional derivative is implemented to anomalous diffusion by (Zhao and kang Luo 2017; Zhou *et al.* 2018). The fractional derivative function with the order α is as $h : (0, \infty) \to R$ and it is defined in the following way:

$$F_\alpha(h)(t) = F_\alpha h(t) = \lim_{\epsilon \to 0} \frac{h(t + \epsilon\, t^{1-\alpha}) - h(t)}{\epsilon},$$

provided the limit exists for all values $t > 0$ and $\alpha \in (0, 1)$.

The function h represented α- differentiable in $(0, a)$ for some $a > 0$ and also can be written as:

$$h^\alpha(0) = \lim_{t \to 0^+} h^\alpha(t). \tag{1}$$

If h is α- differentiable in the conformable sense at $t > 0$, then it must be differentiable in the classical sense at t and

$$F_\alpha h(t) = t^{1-\alpha} h'(t). \tag{2}$$

DENOISING BASED TIME FRACTIONAL DIFFUSION ALGORITHM

The nonlinear anisotropic diffusion models obtained remarkable success in the reduction of Gaussian noise, multiplicative noise etc., and this scheme depends on the parabolic partial differential equation introduced by (Perona and Malik 1990). By this scheme, edges can be preserved during the noise reduction and diffusion acts in an inhomogeneous way; it is maximum over the flat areas and has the lowest value over the edges. (Catté *et al.* 1992) introduced the Perona and Malik model improved for image restoration model and it can be denoted as below:

$$\frac{\partial u}{\partial t} = \nabla \cdot (\zeta(|\nabla G_\sigma * u|)\nabla u), \tag{3}$$

with homogeneous Neumann boundary conditions $\frac{\partial u}{\partial \vec{n}} = 0$ on the boundary of $\partial\Omega$ and Ω is a bounded domain of R^n, $\vec{n}$ the unit outer normal to Ω.

where G_σ is the Gaussian kernel and it is depends on scale parameter (Bai and Feng 2007), $*$ represents the notation for convolution i.e. $G_\sigma * u$. The solution of heat equation is equivalent to the convolution of the signal with Gaussian discussed by (Witkin 1983). Therefore, G_σ can be consider to be any smoothing kernel or low pass filter (Álvarez *et al.* 1992; Catté *et al.* 1992).

As indicated, the classical diffusion model is intended to be converted into (3) to the time-fractional diffusion model for biomedical imaging, which can be denoted as:

$$\frac{\partial^\alpha u}{\partial t^\alpha} = \nabla \cdot (\zeta(|\nabla G_\sigma * u|)\nabla u). \tag{4}$$

After applying the definition of the conformable fractional derivative as provided in section 2., equation (4) can be written as:

$$t^{1-\alpha}\frac{\partial u}{\partial t} = \nabla \cdot (\zeta(|\nabla G_\sigma * u|)\nabla u). \tag{5}$$

This is a PDE-based time-fractional diffusion model and α is the fractional order derivative and the diffusivity ζ, the diffusion threshold parameter K, s is the gradient of the image, and $\zeta(s)$ is a nonnegative function. The parameter K is used to the controlling the even enhancement of edges preserved. The Charbonnier diffusivity $\zeta(s) = \frac{1}{\sqrt{1+(|s|^2/K^2)}}$, related to the convex regularizer $\psi(s^2) = \sqrt{K^4 + K^2 s^2} - K^2$, can be resorted to in (Charbonnier *et al.* 1994; Weickert 1997) as used in the numerical experiments conducted in this study.

(Barbu *et al.* 2009) and (Strong 1997) have introduced the class of functions for the diffusion model and which can be defined as:

$$\zeta(x, |\nabla u|) = \delta \zeta_g(|\nabla u|). \tag{6}$$

The function ζ_g relies upon the magnitude of the gradient u and it can be similar to $\zeta(s)$ and δ is the adaptive parameter. We choose the values of $\delta(x) = 1$, $\zeta_g = \zeta(s)$, $G_\sigma * u$ as u. Then the fractional diffusion model (4) it can be presented in another form as follows:

$$\frac{\partial^\alpha u}{\partial t^\alpha} = \nabla \cdot (\zeta(x, |\nabla u|)\nabla u). \tag{7}$$

Motivated by (Álvarez *et al.* 1992; Prasath and Vorotnikov 2014) and (Giga *et al.* 2022), we want to show the theoretical considerations and viscosity solution of the fractional diffusion model in the next section.

THEORETICAL CONSIDERATIONS FOR THE FRACTIONAL DIFFUSION MODEL

This section provides the viscosity solution and some theoretical considerations for the diffusion model (7):

$$\frac{\partial^\alpha u}{\partial t^\alpha} = \nabla \cdot (\zeta(x, |\nabla u|)\nabla u), \tag{8}$$

Let x and q be two auxiliary functions that are defined from $\mathbb{R}^n$. A vector χ, symmetric matrix c then, the following equations are to be noted

$$c_{ij}(x, q) = \zeta(x, |q|)\delta_{ij} + \zeta_y(x, |q|)\frac{q_i q_j}{|q|}, \tag{9}$$

$$\chi_i(x, q) = \frac{\partial \zeta(x, |q|)}{\partial x_i}. \tag{10}$$

In this part, δ_{ij} is the Kronecker's delta and ζ_y is the partial derivative w.r.to y of the function $\zeta(x, y)$. (Alvarez and Esclarin 1997) have proposed the spatially periodic boundary conditions; thus may we assume that the orthogonal basis b_i in $\mathbb{R}^n$ is defined as

$$u(., x + b_i) = u(., x), \quad x \in \mathbb{R}^n, \quad i = 1, 2, \ldots.n. \tag{11}$$

The functions c and χ are bounded continuously differentiable in x, periodic and x-derivatives are uniformly bounded w.r.t. q. The function u_0 Lipschitz and satisfy equation (11). ζ and (c and χ) satisfy periodicity restriction w.r.to x but not to y or q.

$$c_{ij}(x, q)\xi_i\xi_j \geq K\left[\text{mod}\left(\frac{\partial c(x, q)}{\partial x_k}\right)\right]_{ij}\xi_i\xi_j, \quad k = 1, \ldots\ldots.n, \ \xi, x, q \in \mathbb{R}^n. \tag{12}$$

The generic positive constant number K for different values in different lines.

The viscosity subsolution and super solution is known as the viscosity solution for equation (8), if $\Psi \in K^2([0, T] \times \mathbb{R}^n)$ is any function and $(x_0, t_0) \in (0, T] \times \mathbb{R}^n$ is any point then $u - \phi$ attains local maximum/minimum (Evans and Spruck 1991) and the equivalence of the viscosity solution (Giga *et al.* 2022) as follows:

$$\frac{\partial \Psi^\alpha(x_0, t_0)}{\partial t^\alpha} - \nabla \cdot (\zeta(x_0, |\nabla\Psi(x_0, t_0)|)\nabla\Psi(x_0, t_0)) \leq 0/\geq 0 \tag{13}$$

Lemma. The quadratic matrices of order $n \times n$ are P and Q. Let Q is symmetric matrix then a constant number $N \geq 0$ can be defined as

$$NP_{ij}\xi_i\xi_j \geq \text{mod }(Q)_{ij}\xi_i\xi_j, \quad \forall\, \xi \in \mathbb{R}^n. \tag{14}$$

For every matrix U is not necessarily symmetric of order $n \times n$ has

$$Tr^2(QU^\top) \leq N||Q||Tr(UPU^\top). \tag{15}$$

Here the norm operator of a matrix is denoted by $||.||$ and Q is the matrix whose pixel values are positive.

Proof. From equations (14) and (15) are invariant w.r.to to orthogonal changes of bases. We can therefore assume that Q has already been diagonalized by an axial transform without losing generality. Then

$$Tr^2(QU^\top) = (Q_{ii}U_{ii})^2 \leq ||Q|||Q_{ii}U_{ii}^2$$
$$= ||Q||(\text{mod}(Q)_{ii}U_{ii}^2 \leq ||Q||(\text{mod}(Q)_{ii}U_{ki}U_{kj}$$
$$= ||Q||(\text{mod}(Q)_{ij}U_{ki}U_{kj} \leq N||Q||P_{ij}U_{ki}U_{kj} = N||Q||Tr(UPU^\top).$$

Theorem. A function $u \in K([0, T] \times \mathbb{R}^n) \cap L^\infty(0, T, W^{1,\infty}(\mathbb{R}^n))$ is a viscosity solution (8) for any $T \in [0, \infty)$, if $v \in K(\mathbb{R}^n \times [0, T))$ is a viscosity solution of (8) then a periodic function u_0 is Lipschitz continuous on $\mathbb{R}^n$ is replaced by Lipschitz continuous function v_0 for any $T \in [0, \infty)$, then there exist a positive number K, which depends on T, u_0 and v_0 as below:

$$\sup_{0 \leq t \leq T} ||u(x, t) - v(x, t)||_{L^\infty(\mathbb{R}^n)} \leq K||u_0 - v_0||_{L^\infty(\mathbb{R}^n)}. \tag{16}$$

Furthermore, $\inf_{\mathbb{R}^n} u_0 \leq u(x, t) \leq \sup_{\mathbb{R}^n} u_0$.

The diffusion model (8) which contains the viscosity sub/super solution. i.e. a unique viscosity solution u.

Proof. The viscosity solution u of (8) on $\mathbb{R}^n \times \mathbb{R}^+$ satisfy the inequality:

$$\inf_{\mathbb{R}^n} u_0 \leq u(x, t) \leq \sup_{\mathbb{R}^n} u_0, \ \text{ on } \ \mathbb{R}^n \times \mathbb{R}_+. \tag{17}$$

Let $\Psi(x, t) = \delta t$ at the point (x_0, t_0), $t_0 > 0$, of the global maximum of $u(x, t) - \delta t$, the equation (13) gives $\delta + \lambda(u(t_0, x_0) - u_0(x_0)) \leq 0$, when $u(x_0, t_0) < u_0(x_0)$, it is contradiction because $u(x_0, t_0) - \delta t_0 \geq u_0(x_0)$, then $u(x, t) - \delta t$ achieves a global maximum at $t = 0$, and let $\delta \to 0^+$ and (x_0, t_0) is the global maximum point thus we get (17).

The formal a priori estimate for $\sup_{\mathbb{R}^n}|\nabla u|$ is established. It should be noted that (8) is identical to such that:

$$\frac{\partial^\alpha u}{\partial t^\alpha} = [c_{ij}(x, \nabla u)u_{x_i x_j} + \chi_i(x, \nabla u)u_{x_i}]. \tag{18}$$

The equation (18) differentiate in relation to each x_k, $k = 1, \ldots, n$, and through the multiplication by $2u_{x_k}$ and taking a summation with respect to k, we obtain

$$\beta(|\nabla u|^2) := \frac{\partial^\alpha |\nabla u|^2}{\partial t^\alpha} - c_{ij}(x, \nabla u)\frac{\partial^2}{\partial x_i \partial x_j}|\nabla u|^2 -$$
$$\frac{\partial c_{ij}(x, \nabla u)}{\partial p_l}u_{x_i x_j}\frac{\partial}{\partial x_l}|\nabla u|^2 - \chi_i(x, \nabla u)\frac{\partial}{\partial_i}|\nabla u|^2 -$$
$$\frac{\partial \chi_i(x, \nabla u)}{\partial p_l}u_{x_i}\frac{\partial}{\partial x_l}|\nabla u|^2$$
$$= -2c_{ij}(x, \nabla u)u_{x_k x_i}u_{x_k x_j} + 2\frac{\partial c_{ij}(x, \nabla u)}{\partial x_k}u_{x_i x_j}u_{x_k}$$
$$+ 2\frac{\partial \chi_{ij}(x, \nabla u)}{\partial x_k}u_{x_i}u_{x_k}. \tag{19}$$

The option to eliminate the second term's undesirable influence from the right side of (19) and using Cauchy's inequality for the second term and Lemma 3.1, we obtain

$$\left|2\frac{\partial c_{ij}(x, \nabla u)}{\partial x_k}u_{x_i x_j}u_{x_k}\right| \leq K|u_{x_k}|\sqrt{c_{ij}(x, \nabla u)u_{x_k x_i}u_{x_k x_j}}$$
$$\leq c_{ij}(x, \nabla)u_{x_k x_i}u_{x_k x_j} + K|\nabla u|^2. \tag{20}$$

From the equation (19), the sum of the terms does not exceed $K(1+|\nabla u|^2)$. Hence,

$$\beta(|\nabla u|^2) \leq K(1+|\nabla u|^2), \tag{21}$$

$$\beta(e^{-Kt}(1+|\nabla u|^2)) \leq 0. \tag{22}$$

Using the definition of the weak maximum principle, the operator β can be yield

$$|\nabla u|^2 \leq K. \tag{23}$$

The uniform Hölder estimate by equation (17) and (23) (Alvarez and Esclarin 1997). we can denote the following:

$$|u(x,t) - u(x,r)|^2 \leq K|t-r|. \tag{24}$$

The solution of these equations (17), (23) and (24) are uniformly bounded and equicontinuous on $\mathbb{R}^n \times [0,T]$ and also satisfy the stability results (Crandall *et al.* 1992). The uniqueness solutions exist by the stability estimate of the equation (16) and proof of a similar bound and the matrix τ, the following work can be referred to (Shi and Chang 2006) by replaced by

$$\tau = \begin{pmatrix} M_1 & \sqrt{M_1}\sqrt{M_2} \\ \sqrt{M_1}\sqrt{M_2} & M_2 \end{pmatrix}, \tag{25}$$

where

$$M_1 = d\left(x_0, \frac{|x_0-y_0|^2(x_0-y_0)}{\delta}\right), \; M_2 = d\left(y_0, \frac{|x_0-y_0|^2(x_0-y_0)}{\delta}\right).$$

DISCRETIZED SCHEME FOR THE ANISOTROPIC DIFFUSION AND FRACTIONAL ANISOTROPIC DIFFUSION MODEL

The discretized scheme for both anisotropic diffusion and fractional anisotropic diffusion model is discussed herein. Let $x_i = i\Delta x$, $y_j = j\Delta x$, i, j=1,2,3.......N, $N\Delta x = 1$, (Δx is spatial step size) and $t_n = n\Delta t$, $\;n \geq 1$ (Δt is the time step size).

It is possible to denote the explicit scheme of (5) as follows:

$$u^t_{ij} = t^{\alpha-1}\frac{1}{2\Delta x}\left[(\zeta^n_{i+1,j}+\zeta^n_{i,j})(u^n_{i+1,j}-u_{i,j}) - (\zeta^n_{i,j}+\zeta^n_{i-1,j})(u^n_{i,j}-u^n_{i-1,j})\right]$$

$$+t^{\alpha-1}\frac{1}{2\Delta x}\left[(\zeta^n_{i,j+1}+\zeta^n_{i,j})(u^n_{i,j+1}-u_{i,j}) - (\zeta^n_{i,j}+\zeta^n_{i,j-1})(u^n_{i,j}-u^n_{i,j-1})\right]).$$

It is similar to the discrete scheme for the diffusion model (3) if $\alpha = 1$.

The diffusivity $\zeta(|\nabla u|^2)$ is discretized by,

$$\zeta^n_{ij} = \psi'\left(\left(\frac{u^n_{i+1,j}-u^n_{i-1,j}}{\Delta x}\right)^2 + \left(\frac{u^n_{i,j+1}-u^n_{i,j-1}}{\Delta x}\right)^2\right),$$

The explicit method is stable and convergent for $\Delta t/\Delta x^2 < 0.5$, see (Lapidus and Pinder 1983). The numerical explicit scheme (5) is stable and consistent with the diffusion based fractional model. It is then used in our numerical experiments which are given in the next section.

EXPERIMENTAL RESULTS OF THE DIFFUSION MODEL AND FRACTIONAL DIFFUSION MODEL

In this section, we want to give experimental results of the diffusion model and proposed fractional diffusion model for original ultrasound images are taken (Al-Dhabyani *et al.* 2020). The original images size 256 × 256 contain the pixel value [0, 255]. To perform the experiments, we reduce the pixel value of all images in between [0, 1]. Speckle noise can be added by the function imnoise(u, 'speckle', σ) in Matlab [MATLAB, 2022 version 9.12.0 (R2022a). The Math-Works Inc., Natick, Massachusetts]. In our all experiment, we have taken the parameters $\Delta t/\Delta x^2 = 0.45$, diffusivity parameter $K = 5$, time parameter $t = 0.02$ and $\lambda = 0.85$, see reference (Hammad and Khalil 2014b; Chan *et al.* 1999; Chang and Chern 2003).

The experimental results for different fractional orders significantly reduce the iteration step and better PSNR value provided herein. The fractional-order α proves to be very important in the experiment. This is because a small fractional-order α will get more clarity denoising the image at a smaller number of iterations. We check the clarity of the denoising image by the PSNR value. The larger PSNR value of the images has a satisfactory level of result, while the fractional model provides fast process images when image denoising and edge-preserving are conducted together. To check the quality of the denoised image, the following denotation is to be referred to:

$$\text{PSNR} = 10\log_{10}\left(\frac{S^2}{\frac{1}{MN}\sum^n_{i,j}(u_1(i,j)-u(i,j))^2}\right). \tag{26}$$

Here $u_1(i,j)$ and $u_{(}i,j)$ are the restored and original image respectively, S is the maximum pixel value of the image and MN is the order of the matrix.

Ultrasound image and breast cancer benign ultrasound images are provided in Figure 1 (a) and (b). In addition, Figure 2 provides the speckle noisy image (σ = 0.1) and related denoised images, whereas Figure 3 presents the speckle noisy image (σ = 0.3) and related denoised images. Figure 4 shows the speckle noisy image (σ = 0.5) and related denoised images, while Figure 5 depicts the speckle noisy image (σ= 0.06) and related denoised images. Figure 6 provides the speckle noisy image (σ = 0.08) and related denoised images, whereas Figure 7 presents the speckle noisy image (σ= 0.10) and related denoised images.

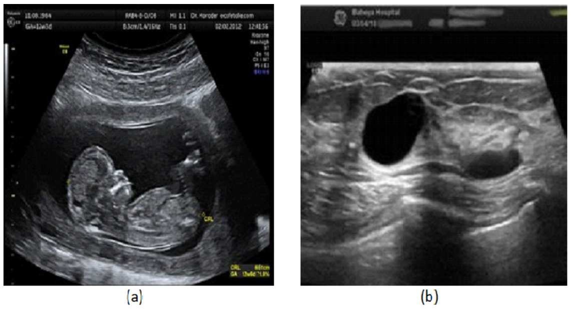

(a)
(b)

Figure 1 (a) Ultrasound image and (b) breast cancer benign ultrasound image.

The experimental results provided in terms of PSNR values with different levels of speckle noise ($\sigma = 0.1, 0.3, 0.5$) by using models (3) and (5) can be seen in Table 1.

The experimental results provided in terms of PSNR values with different levels of speckle noise ($\sigma = 0.06, 0.08, 0.10$) by using models (3) and (5) can be seen in Table 2.

Table 1 The experimental results in terms of PSNR values with different levels of speckle noise (σ = 0.1, 0.3, 0.5) by using models (3) and (5).

Images	PSNR for the noisy images	PSNR for the denoised images by model (3)	PSNR for the denoised images by model (5)			
			$\alpha = 0.7$	$\alpha = 0.5$	$\alpha = 0.3$	$\alpha = 0.1$
Figure 2(a-f)	22.19	22.76	23.12	24.22	25.25	25.66
Figure 3(a-f)	17.69	18.20	18.57	19.36	21.03	22.94
Figure 4(a-f)	15.87	16.33	16.64	17.47	19.02	21.17
No. of iterations		100	50	50	50	50

Table 2 The experimental results in terms of PSNR values with different levels of speckle noise (σ = 0.06, 0.08, 0.10) by using models (3) and (5).

Images	PSNR for the noisy images	PSNR for the denoised images by model (3)	PSNR for the denoised images by model (5)			
			$\alpha = 0.7$	$\alpha = 0.5$	$\alpha = 0.3$	$\alpha = 0.1$
Figure 5(a-f)	21.80	22.07	22.26	22.43	23.32	24.10
Figure 6(a-f)	20.62	21.18	21.35	21.50	22.75	23.88
Figure 7(a-f)	19.66	20.29	20.66	20.85	22.24	23.52
No. of iterations		300	100	50	50	50

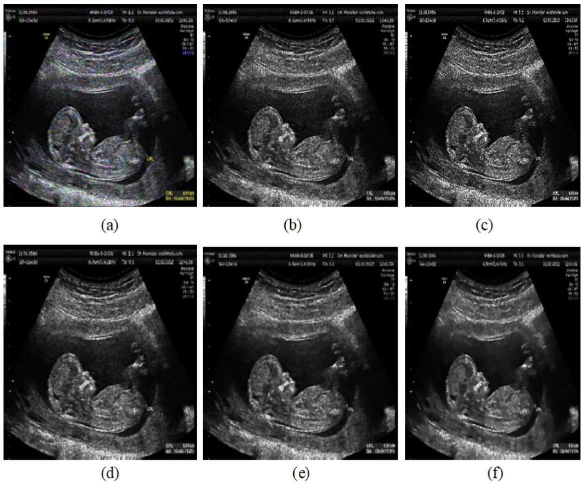


Figure 2 (a) Speckle noisy image with ($\sigma = 0.1$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1, respectively.

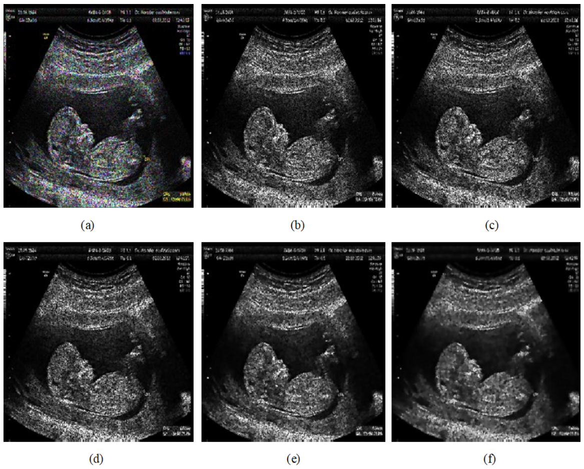


Figure 3 (a) Speckle noisy image with ($\sigma = 0.3$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1, respectively.

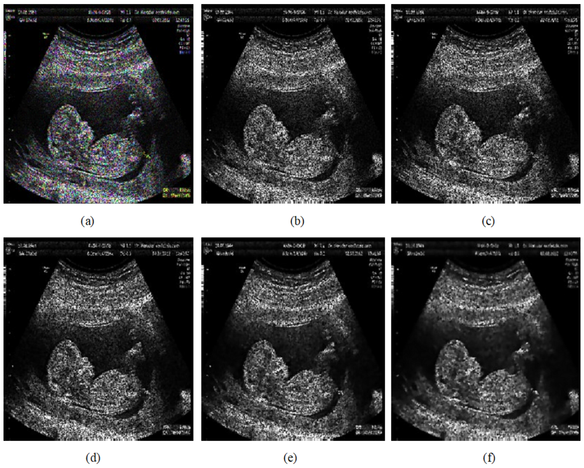


Figure 4 (a) Speckle noisy image with ($\sigma = 0.5$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1 in the related order.

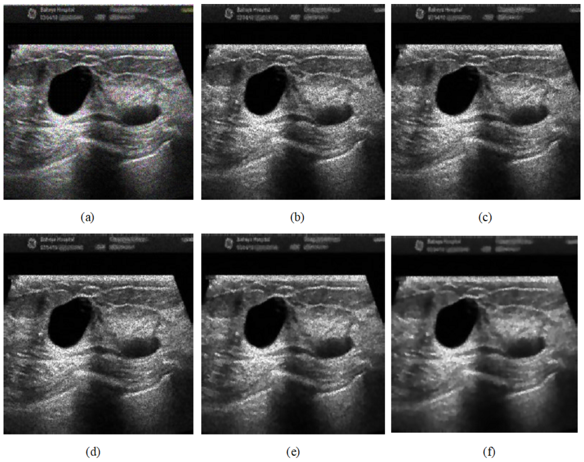


Figure 5 (a) Speckle noisy image with ($\sigma = 0.06$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1, respectively.

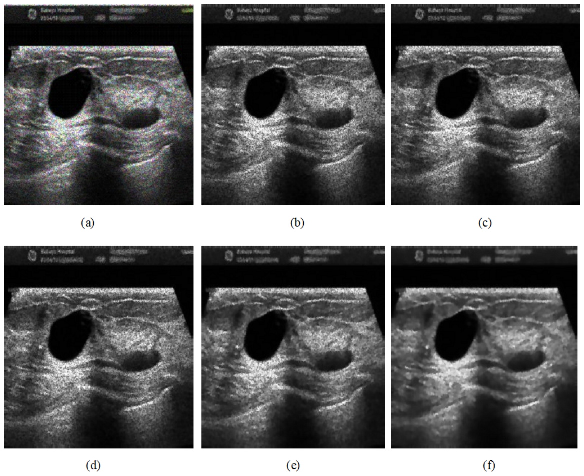


Figure 6 (a) Speckle noisy image with ($\sigma = 0.08$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1, respectively.

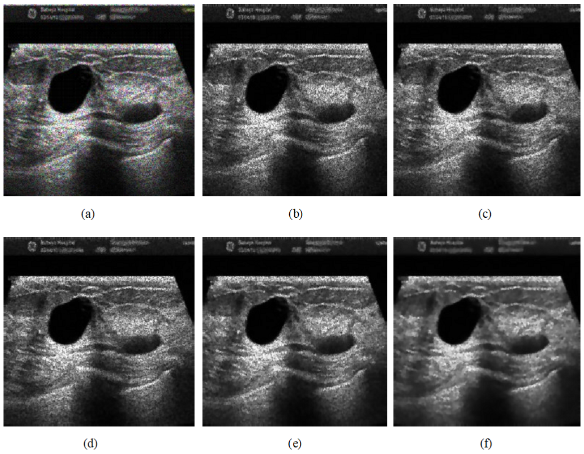


Figure 7 (a) Speckle noisy image with ($\sigma = 0.10$); (b) Denoised image by (3); (c-f) Denoised images by (5) at $\alpha = 0.7, 0.5, 0.3$ and 0.1, respectively.

CONCLUSION, DISCUSSIONS AND FUTURE DIRECTIONS

Reducing noise in images is a critical task for accuracy and precision in image processing, and it is possible that noises can emerge with images through achievement pertaining to diffusion. Accordingly, a fractional order derivative-based diffusion model for biomedical imaging has been presented to reduce additive speckle noise. The medical images (ultrasound image, X-rays, CT scans, MRIs, etc.) may lose significant features and become degraded due to the emergence of noise. Detecting the additive noise in the images and finding the applicable solution in a timely manner becomes particularly essential, which is a detecting the additive noise in the images and finding the solution to such matters becomes a challenge to be tacked effectively for researchers, clinicians, pharmaceutical authorities and related practitioners.

The aim of this study has been to prove the viscosity solution of the diffusion model with the proposed model providing to be efficient in reducing noise by preserving the essential image features like edges, corners and other sharp structures for ultrasound images in comparison to the classical anisotropic diffusion model. Consequently, this paper has presented a conformable fractional derivative-based anisotropic diffusion model for removing speckle noise in ultrasound images to attain the optimal outcomes. The finite difference method has been used to discretize the fractional diffusion model and classical diffusion models. The peak signal-to-noise ratio (PSNR) has also been used for the quality of the smooth images. The proposed mathematical model in this study is a generalization of the classical diffusion model. The fractional order α appears in the time derivative and finds the results with different fractional order a. The performance of the ultrasound images is measured by the PSNR values.

The comparative experimental results of the fractional and classical diffusion models as presented herein are computed by the finite difference explicit scheme. Thus, the results demonstrate that the proposed mathematical model (5) has larger PSNR values corresponding to (3) at the different iteration number. We may, therefore, draw the conclusion that the proposed model obtained yield better results for ultrasound images based on the novel and extended scheme. Another relevant novel contribution has been that the improved mathematical model in the scheme of our study based on the experimental results, as has been proposed, includes the time-fractional derivative with smoothness diffusivity, and subsequently, the viscosity solution of the fractional diffusion model has been proven through the scheme under consideration. In future endeavors, the applicability of various fractional derivatives on these mathematical diffusion-related and other equivalent schemes can be compared and put forth to serve biomedical imaging like X-rays, CT scans, MRIs, etc., bioengineering and other related medical, clinical and image-signal related applied as well as computational processes.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Abirami, A., P. Prakash, and Y.-K. Ma, 2021 Variable-Order Fractional Diffusion Model-Based Medical Image Denoising. Mathematical Problems in Engineering **2021**: 1–10.

Al-Dhabyani, W., M. Gomaa, H. Khaled, and A. Fahmy, 2020 Dataset of breast ultrasound images. Data in Brief **28**: 104863.

Alvarez, L. and J. Esclarin, 1997 Image quantization using reaction-diffusion equations. SIAM Journal on Applied Mathematics **57**: 153–175.

Álvarez, L., P.-L. Lions, and J.-M. Morel, 1992 Image selective smoothing and edge detection by nonlinear diffusion. ii. SIAM Journal on Numerical Analysis **29**: 845–866.

Aubert, G. and J.-F. Aujol, 2008 A variational approach to removing multiplicative noise. SIAM Journal on Applied Mathematics **68**: 925–946.

Bai, J. and X.-C. Feng, 2007 Fractional-order anisotropic diffusion for image denoising. IEEE Transactions on Image Processing **16**: 2492–2502.

Barbu, T., 2014 Robust anisotropic diffusion scheme for image noise removal. Procedia Computer Science **35**: 522–530, Knowledge-Based and Intelligent Information and Engineering Systems 18th Annual Conference, KES-2014 Gdynia, Poland, September 2014 Proceedings.

Barbu, T., V. Barbu, V. Biga, and D. Coca, 2009 A pde variational approach to image denoising and restoration. Nonlinear Analysis: Real World Applications **10**: 1351–1361.

Butera, S. and M. D. Paola, 2014 A physically based connection between fractional calculus and fractal geometry. Annals of Physics **350**: 146–158.

Catté, F., P. Lions, J. Morel, and T. Coll, 1992 Image selective smoothing and edge detection by nonlinear diffusion*. SIAM J. Numer. Anal. **29**: 182–193.

Chan, T. F., G. H. Golub, and P. Mulet, 1999 A nonlinear primal-dual method for total variation-based image restoration. SIAM J. Sci. Comput. **20**: 1964–1977.

Chang, Q. and I.-L. Chern, 2003 Acceleration methods for total variation-based image denoising. SIAM Journal on Scientific Computing **25**: 982–994.

Charbonnier, P., L. Blanc-Féraud, G. Aubert, and M. Barlaud, 1994 Two deterministic half-quadratic regularization algorithms for computed imaging. Proceedings of 1st International Conference on Image Processing **2**: 168–172 vol.2.

Chen, B., S. Huang, Z. Liang, W. Chen, and B. Pan, 2019 A fractional order derivative based active contour model for inhomogeneous image segmentation. Applied Mathematical Modelling **65**: 120–136.

Chen, D., S. Sun, C. Zhang, Y. Chen, and D. Xue, 2013 Fractional-order TV-L^2 model for image denoising. Central European Journal of Physics **11**: 1414–1422.

Contreras, A. O., J. Rosales, L. M. Jimenez, and J. M. Cruz-Duarte, 2018 Analysis of projectile motion in view of conformable derivative. Open Physics **16**: 581–587.

Crandall, M. G., H. Ishii, and P.-L. Lions, 1992 Users guide to viscosity solutions of second order partial differential equations. Bulletin of the American Mathematical Society **27**: 1–67.

Cresson, J., 2010 Inverse problem of fractional calculus of variations for partial differential equations. Communications in Nonlinear Science and Numerical Simulation **15**: 987–996.

Evans, L. C. and J. Spruck, 1991 Motion of level sets by mean curvature. I. Journal of Differential Geometry **33**: 635–681.

Fan, L., F. Zhang, H. Fan, and C. Zhang, 2019 Brief review of image denoising techniques. Vis. Comput. Ind. Biomed. Art **2**.

Fang, Z.-W., H.-W. Sun, and H. Wang, 2020 A fast method for variable-order caputo fractional derivative with applications to time-fractional diffusion equations. Computers and Mathematics with Applications **80**: 1443–1458.

Giga, Y., H. Mitake, and S. Sato, 2022 On the equivalence of viscosity solutions and distributional solutions for the time-fractional diffusion equation. Journal of Differential Equations **316**: 364–386.

Gilboa, G., N. Sochen, and Y. Zeevi, 2006 Variational denoising of partly textured images by spatially varying constraints. IEEE Transactions on Image Processing **15**: 2281–2289.

Hammad, I. A. and R. Khalil, 2014a Fractional fourier series with applications. American Journal of Computational and Applied Mathematics **4**: 187–191.

Hammad, M. A. and R. Khalil, 2014b Conformable fractional heat differential equation. International journal of pure and applied mathematics **94**: 215–221.

Herrmann, R., 2011 *Fractional Calculus: An Introduction for Physicists*. World Scientific.

Hilfer, R., 2000 *Applications of Fractional Calculus in Physics*. World Scientific.

Ibrahim, W. R., 2020 A new image denoising model utilizing the conformable fractional calculus for multiplicative noise. SN Applied Sciences **2**: 120–136.

Janev, M., S. Pilipoviaea, T. Atanackoviaea, R. Obradoviaea, and N. Raleviaea, 2011 Fully fractional anisotropic diffusion for image denoising. Mathematical and Computer Modelling **54**: 729–741.

Karaca, Y. and D. Baleanu, 2022 Chapter 9 - computational fractional-order calculus and classical calculus ai for comparative differentiability prediction analyses of complex-systems-grounded paradigm. In *Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems*, edited by Y. Karaca, D. Baleanu, Y.-D. Zhang, O. Gervasi, and M. Moonis, pp. 149–168, Academic Press.

Khalil, R., M. Al Horani, A. Yousef, and M. Sababheh, 2014 A new definition of fractional derivative. Journal of Computational and Applied Mathematics **264**: 65–70.

Kumar, S. and M. Ahmad, 2014 A time dependent model for image denoising. Journal of Signal and Information Processing **6**: 28–

38.
Kumar, S., M. Sarfaraz, and M. Ahmad, 2016 An efficient pde-based nonlinear anisotropic diffusion model for image denoising. Neural, Parallel and Scientific Computations **24**: 305–315.
Lapidus, L. and G. F. Pinder, 1983 Numerical solution of partial differential equations in science and engineering. SIAM Review **25**: 581–582.
Mazloum, B. and H. Siahkal-Mahalle, 2022 A time-splitting local meshfree approach for time-fractional anisotropic diffusion equation: application in image denoising. Adv Cont Discr Mod **56**.
Othman, M. I. A. and S. Shaw, 2021 On the concept of a conformable fractional differential equation. Journal of Engineering and Thermal Sciences **1**: 17–29.
Perona, P. and J. Malik, 1990 Scale-space and edge detection using anisotropic diffusion. IEEE Trans. Pattern Anal. Mach. Intell. **12**: 629–639.
Prasath, V. B. S. and D. Vorotnikov, 2014 Weighted and well-balanced anisotropic diffusion scheme for image denoising and restoration. Nonlinear Analysis-real World Applications **17**: 33–46.
Shi, Y. and Q. Chang, 2006 New time dependent model for image restoration. Applied Mathematics and Computation **179**: 121–134.
Strong, D., 1997 *Adaptive total variation minimizing image restoration*.
Wang, Q., J. Ma, S. Yu, and L. Tan, 2020 Noise detection and image denoising based on fractional calculus. Chaos, Solitons and Fractals **131**: 109463.
Weickert, J., 1997 A review of nonlinear diffusion filtering. In *Scale-Space Theory in Computer Vision*, edited by B. ter Haar Romeny, L. Florack, J. Koenderink, and M. Viergever, pp. 1–28, Berlin, Heidelberg, Springer Berlin Heidelberg.
Welk, M., D. Theis, T. Brox, and J. Weickert, 2005 Pde-based deconvolution with forward-backward diffusivities and diffusion tensors. In *Scale Space and PDE Methods in Computer Vision*, edited by R. Kimmel, N. A. Sochen, and J. Weickert, pp. 585–597, Berlin, Heidelberg, Springer Berlin Heidelberg.
Witkin, A. P., 1983 Scale-space filtering. In *International Joint Conference on Artificial Intelligence*.
Yin, X., S. Zhou, and M. A. Siddique, 2015 Fractional nonlinear anisotropic diffusion with p-laplace variation method for image restoration. Multimedia Tools and Applications **75**: 4505 – 4526.
Zhang, Z., Q. Liu, and T. Gao, 2021 A fast explicit diffusion algorithm of fractional order anisotropic diffusion for image denoising.
Zhao, D. and M. kang Luo, 2017 General conformable fractional derivative and its physical interpretation. Calcolo **54**: 903–917.
Zhou, H., S. Yang, and S. Zhang, 2018 Conformable derivative approach to anomalous diffusion. Physica A: Statistical Mechanics and its Applications **491**: 1001–1013.

How to cite this article: Chauhan, A., Kumar, S., and Karaca, Y. A New Fractional-order Derivative-based Nonlinear Anisotropic Diffusion Model for Biomedical Imaging. *Chaos Theory and Applications*, 5(3), 198-206, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.207-218
https://doi.org/10.51537/chaos.1357543

Analyzing Predator-Prey Interaction in Chaotic and Bifurcating Environments

Ansar Abbas *,1 **and Abdul Khaliq** *,2
*Department of Mathematics, Riphah International University, Lahore, Pakistan.

ABSTRACT An analysis of discrete-time predator-prey systems is presented in this paper by determining the minimum amount of prey consumed before predators reproduce, as well as by analyzing the system's stability and bifurcation. In order to investigate the local stability of the interior equilibrium point of the proposed model, discrete dynamics system theory is employed first. Moreover, the characteristic equation is analyzed to determine the Neimark-Sacker (NS) bifurcation of the system. The normal form and bifurcation theory are used to investigate the NS bifurcation around the interior equilibrium point. Based on its analysis, the system exhibits Neimark-Sacker bifurcation when positive parameters are present and non-negative conditions are met. The region of stability of chaotic behavior can be discovered by developing a feedback control strategy. By utilizing the maximum Lyapunov exponent, the effect of initial conditions on developed systems is further explored. Finally, a computer simulation illustrates the results of the analysis.

KEYWORDS
Lotka-volterra
stability
Predator-Prey model
fixed points
Neimark-sacker bifurcation
Maximum lyapunov exponent
Chaos control

INTRODUCTION

It is widely known that predators and prey interact dynamically in nature, which helps to link complex food chains and food networks. The biological functions of predator-prey system dynamics have been explained by several predator-prey models. Predator-prey models are widely regarded as being one of the best, Lotka-Volterra is receiving increasing attention in recent years (R. M. Eide 2018; Pan 2013). Many studies have sought to understand the dynamical properties of the Lotka-Volterra model, since it plays an important role in ecosystem studies. These properties include dynamical behavior, stability, persistence, and antiperiodic, periodic, and near periodic solutions (Z. L. Luo 2016; X. W. Jiang 2021).

Natural interactions between predators and prey are fascinating puzzles. Ecology's fascination with ecosystems comes from the intimate interconnections between species. When chaos and bifurcation are introduced into this intricate dance, figuring out the dynamics becomes even more difficult. A chaotic environment characterized by sudden shifts and unpredictability complicates predator-prey relationships. An environment such as this is conducive to the development of novel patterns, unexpected results, as well as a better understanding of the nature of life. The purpose of this study is to shed light on predator-prey interactions within chaotic and bifurcating environments, as well as their mechanisms, effects, and ecological implications. To understand these systems and reveal hidden connections, we will utilize chaos theory, mathematical modeling, and ecological studies (Zu *et al.* 2018; Q. 2015; Hu Z. 2011; Ibrahim and Touafek 2014; L. Men 2015).

In this exploration, we will draw on innovative research and seminal studies on predator-prey interactions. By examining the works of ecological pioneers like Lotka and Volterra, our scientific investigation will weave a rich tapestry. It is our goal to examine predator-prey relationships in environments that challenge conventional wisdom and our understanding of the natural world. This investigation will help us unravel the enigmatic language of life, which is enigmatic.

When it comes to population dynamical models, difference equation-based models and differential equation-based models can be distinguished from each other. Recent years have seen an increase in the popularity of discrete-time population models (Q. 2015; L. Men 2015). For the following reasons, discrete-time models are more appropriate than continuous-time models when populations have non-overlapping generations and small numbers of populations. The second reason is that discrete-time simulation results are more accurate. Moreover, continuous-time models can be numerically simulated by discretising and transforming them

---

Manuscript received: 8 September 2023,
Revised: 22 October 2023,
Accepted: 23 October 2023.

[1] kute_ansar@yahoo.com (**Corresponding Author**)
[2] khaliqsyed@gmail.com

into its discrete counterpart . As a result, discrete-time models exhibit rich dynamical behaviors. In a study entitled Periodic Solution of Predator-Prey Models, (Fazly and Hesaaraki 2007; X. Zhang 2016), (Zhang C.H 2010) performed studies on periodic solutions to determine their stability, permanence, and existence. In discrete dynamical systems, properties such as periodicity, local and global stability, persistence, uniqueness of equilibrium, and boundedness of solutions are taken into account (Garic Demirovic M. 2009; Q. 2015; Kalabusic S. 2011; Ibrahim and Touafek 2014). Numerous articles also investigated the possibility of bifurcation and chaos when using discrete-time models (Hu Z. 2011; Sen M 2012; Chen and Changming 2008; Gakkhar and Singh 2012; Joydip Dhar 2015).

Smith et. al. (Smith 1968) introduced the following predator-prey model where U_n and V_n represent the prey and predator population sizes, respectively.

$$\left.\begin{aligned} U_{n+1} &= \left(R - \frac{U_n(R-1)}{U_E} - CV_n\right) U_n \\ V_{n+1} &= \frac{r}{U_E} U_n V_n \end{aligned}\right\} \qquad (1)$$

Where, U_E represents the equilibrium density of preys in the absence of predator. R and r denote the maximum reproductive rates of the prey and predator respectively, C is a constant. Unfortunately, (Smith 1968) was unable to find the bifurcation parameter of the system (1) as well as the equilibrium point where the bifurcation exists. A modification to the predator-prey model is made by (Khan 2016) and is presented as follows:

$$\left.\begin{aligned} s_{n+1} &= \rho\,(1-s_n)s_n - s_n t_n, \\ t_{n+1} &= \frac{1}{\Upsilon} s_n t_n \end{aligned}\right\} \qquad (2)$$

where s_n and t_n represent the number of preys and predators, respectively. The initial values s_0, t_0 are positive real numbers while ρ, Υ are parameters. In contrast to (Smith 1968), (Khan 2016) did not find out numerically the results of the Neimark-Sacker bifurcation for model (2) but discussed in an understandable manner all the theoretical aspects of the Neimark-Sacker bifurcation that has become an important topic.

In dynamical systems theory, Neimark-Sacker bifurcations are named after Russian mathematician L. A. Neimark and American mathematician A.F Shilnikov. Dynamic systems are characterized by the point at which a stable periodic orbit turns into chaos. As a result of this bifurcation, the system exhibits a complex, non-repeating behavior. Natural and engineered systems, such as weather patterns and electricity circuits, exhibit Neimark-Sacker bifurcations, which are fundamental to understanding chaos.

Based on (Smith 1968), we have developed a modified discrete predator-prey model that follows:

$$\left.\begin{aligned} x_{n+1} &= (1-A)x_n^2 + x_n(A-y_n) \\ y_{n+1} &= \frac{1}{B} x_n y_n \end{aligned}\right\} \qquad (3)$$

Biological description of parameters are mentioned in Table 1

Considering its structure, this paper can be separated into the following sections. In Section-2, we discuss how equilibria exists and how they are stable locally in R_2^+ for the system (3). Furthermore, our discussion focuses on the specific parametric conditions required for the existance of a Neimark-Sacker bifurcation. As a bifurcation parameter A is used in Section-3 to study bifurcation (NS). By using feedback control methods, a stable region is achieved in section-4. The numerical simulations presented in Section-5 support the theoretical discussion. By showing the Maximum Laypnuov exponent in section-6, the fluctuation of the system is discussed according to its initial condition. Finally, we present a brief conclusion in Section-7.

EQUILIBRIUM POINTS AND THEIR STABILITY

The purpose of this section is to examine the existence of fixed points in discrete systems and analyses their stability. By using the formula given below, we can determine the fixed points of system (3) which satisfy

$$\left.\begin{aligned} x_n &= x_{n+1} = x^*, \\ y_n &= y_{n+1} = y^* \end{aligned}\right\}$$

When we use it in the model (3), we get the following result:

$$\left.\begin{aligned} x^* &= (1-A)(x^*)^2 + x^*(A-y^*), \\ y^* &= \frac{1}{B} x^* y^* \end{aligned}\right\} \qquad (a^*)$$

Framework (a^*) clearly describes the fixed points of model (1).

(i) The system (3) has always a Extinction equilibrium point $E_1 = (0,0)$.

(ii) The system (3) has Extinction and Exclusion equilibrium points
$E_1 = (0,0)$ and $E_2 = (1,0)$ for $B < 1$.

(iii) There is a unique equilibrium point for the system (3) that is $E_3 = (B, A + (1-A)B - 1)$ for $A < 1, B > 1$.

Our discussion now turns to the dynamics of model (1) about these equilibrium points. Linearized system (1) about fixed points (x, y) can be described by the Jacobian matrix

$$J(E_i) = \begin{pmatrix} A + 2(1-A)x - y & -x \\ \frac{y}{B} & \frac{x}{B} \end{pmatrix}$$

as a result, the Jacobian matrix J of the linearized system (3) over the unique positive equilibrium $(B,\ A + (1-A)B - 1)$ is defined by

$$\lambda^2 + r\lambda + s = 0 \qquad (a^{**})$$

where, $r = AB - B - 2\,,\quad s = A - 2AB + 2B$

Additionally, As can be seen from the equation above, all eigenvalues of the Jacobian of (3) evaluated at the unique positive equilibrium $(B, /A + (1-A)B - 1)$ are calculated as follows:

$$\lambda_{1,2} = \frac{1}{2}(2 + B - AB \pm \sqrt{\Delta})$$

where,

$$\Delta = r^2 - 4rs$$

Table 1 Description of the parameters

Parameter	Role in the Model
x_n	Prey population size at a particular time step.
y_n	Predator population size at a particular time.
A	Represents prey population intrinsic growth rate, which determines the reproduction rate of preys.
B	Measuring predator productivity in converting prey. When predators successfully consume their prey.

$$\Delta = -4(A + 2B - 2AB) + (-2 - B + AB)^2$$

As a means of analyzing how stable the fixed points of the model (3) are, here is the following definition:

Definition 1:

A fixed point (P, Q) is called

(i) a sink if $|\lambda_1| < 1$ and $|\lambda_2| < 1$, it is locally asymptotically stable.

(ii) when $|\lambda_1| > 1$ and $|\lambda_2| > 1$, the source is unstable.

(iii) if $|\lambda_1| < 1$ and $|\lambda_2| > 1$ or ($|\lambda_1| > 1$ and $|\lambda_2| < 1$), it is saddle.

(iv) if either $|\lambda_1| = 1$ or $|\lambda_2| = 1$, it is not hyperbolic. Using the definition above, we will derive the lemma (2.1) from the topological classification of the fixed points within the model (3). If we evaluate the dynamical map in (3) at any point (x, y), Jacobian matrix is calculated as follows:

$$J(E_1) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

$$J(E_2) = \begin{pmatrix} 2 - A & -1 \\ 0 & \frac{1}{B} \end{pmatrix}$$

$$J(E_3) = \begin{pmatrix} 1 + B - AB & -B \\ \frac{-1+A+B-AB}{B} & 1 \end{pmatrix}$$

Having discussed the models' fixed points (3), we will now discuss their topological classification. From $(a**)$ we have:

Lemma 1: The following topological classification holds for the fixed point $E_1(0, 0)$

(i) When $A < 1$ the point E_1 becomes sink .

(ii) When $A > 1$ the point E_1 is saddle .

(iii) When $A = 1$ the point E_1 is non-hyperbolic.

Lemma 2:

The following topological classification holds for the fixed point $E_2(1, 0)$

(i) If $A > 1$ and $B > 1$ then $E_2(1, 0)$ is a sink .

(ii) If $A < 1$ and $B > 1$ then $E_2(1, 0)$ is a saddle .

(iii) If $A = 1$ or $B = 1$ then $E_2(1, 0)$ will be non-hyperbolic .

Lemma 3:

The following topological classification holds for the fixed point

$$E_3 = (B, A + (1 - A)B - 1) \; for \; A < 1, \; B > 1$$

(i) Among the following parametric conditions, E_3 is a sink if one of the following parametric conditions holds:

$(i.a)$ $r \geq 4s$ and $0 < A < 1$

$(i.b)$ $r < 4s$ and $A < (\frac{B-2}{B})^2$

(ii) It is possible for E_3 to be a source if one of the following parametric conditions holds:

$(ii.a)$ $r \geq 4s$ and $A > 1$

$(ii.b)$ $r < 4s$ and $A > (\frac{B-2}{B})^2$

(iii) When one parametric condition is satisfied, E_3 will not be hyperbolic if one of the following parametric conditions holds:

$(iii.a)$ $r \geq 4s$ and $A = 1$

$(iii.b)$ $r < 4s$ and $A = (\frac{B-2}{B})^2$

NEIMARK-SACKER BIFURCATION AT E_3

Using Lemma(2.3), E_3 cannot be hyperbolic when $A = 1$. The Neimark-Sacker bifurcation in the system (3) can therefore be studied by choosing A as the bifurcation parameter near the point E_3. In this context, non-hyperbolic parameters are denoted as

$$H_k = \{ \; (A, B); \; \Delta < 0, \; A = (\frac{B-2}{B})^2, \; B > 1, \; A, B > 0 \; \}$$

Here's a description of the system (3) with arbitrary parameters $(\alpha, \beta) \in H_k$

$$\left.\begin{array}{rcl} x_{n+1} & = & (1-\alpha)x_n^2 + x_n(\alpha - y_n), \\ y_{n+1} & = & \frac{1}{\beta} x_n y_n \end{array}\right\} \quad (4)$$

One can easily found that the point $(\beta, \alpha + (1 - \alpha)\beta - 1)$ is the unique positive equilibrium point for the system (4) when $\beta > 1$, $\alpha < 1$. The following perturbations would be made to model (4)

$$\left.\begin{array}{rcl} x_{n+1} & = & (1-(\alpha+\alpha_1))x_n^2 + x_n((\alpha+\alpha_1) - y_n), \\ y_{n+1} & = & \frac{1}{\beta} x_n y_n \end{array}\right\} \quad (5)$$

where $|\alpha_1| << 1$, which is small parameter. Using (5) as a linearized system and $P_1(\beta, \alpha + (1 - \alpha)\beta - 1)$, as a unique point of positive equilibrium, the Jacobian matrix has the following characteristic equation:

$$\varsigma^2 + r(\alpha_1)\varsigma + s(\alpha_1) = 0$$

where,

$$r(\alpha_1) = (\alpha + \alpha_1)\beta - \beta - 2\,, \quad s(\alpha_1) = (\alpha + \alpha_1) - 2\alpha\beta + 2\beta$$

The characteristic equation, as well as the roots of the characteristic equation, change when α varies in a small radius around 0,

$$\varsigma_{1,2} = \frac{-r(\alpha_1) \pm \sqrt{r^2(\alpha_1) - 4s(\alpha_1)}}{2}$$

$$\varsigma_{1,2} = \frac{(\alpha+\alpha_1)\beta - \beta - 2 \pm \sqrt{((\alpha+\alpha_1)\beta-\beta-2)^2 - 4((\alpha+\alpha_1)-2\alpha\beta+2\beta)}}{2}$$

$$\varsigma_{1,2} = \frac{(\alpha+\alpha_1)\beta - \beta - 2 \pm \iota\sqrt{-((\alpha+\alpha_1)\beta-\beta-2)^2 + 4((\alpha+\alpha_1)-2\alpha\beta+2\beta)}}{2}$$

For $\alpha_1 < \frac{2((s(\alpha_1))^{\frac{1}{2}}+1)+\beta(1-\alpha)}{\beta}$ there are two complex conjugate roots.

Also, we have

$$trJ(P_1) \neq 0, -1$$

,

$$\frac{d \mid \varsigma_{1,2} \mid}{d\alpha_1}_{|\alpha_1} = 4(\alpha\beta^2 - (\beta+1)^2) > 0$$

After simplification we get $\varsigma_{1,2}^i \neq 1$ for $i = 1, ..., 4$, is satisfied.

A method for transforming the equilibrium point $P_1(\beta, \alpha + (1-\alpha)\beta - 1)$ of the system (5) into its origin, we take $u_n = x_n - \beta,\ v_n = y_n - \alpha - (1-\alpha)\beta + 1$. After calculation we get,

$$\left.\begin{aligned} u_{n+1} &= (1-(\alpha+\alpha_1))(u_n+\beta)^2 + (u_n+\beta)((\alpha+\alpha_1) - \\ &\qquad (v_n + \alpha + (1-\alpha)\beta - 1)) \\ v_{n+1} &= \frac{1}{\beta}(u_n+\beta)(v_n + \alpha + (1-\alpha)\beta - 1) \end{aligned}\right\} \quad (6)$$

We examine system (5) in its normal form when $\alpha_1 = 0$ in the following way. The Taylor series at $(u_n, v_n) = (0, 0)$ is as follows:

$$\left.\begin{aligned} u_{n+1} &= b_{11}u_n + b_{12}v_n + b_{13}u_n^2 + b_{14}u_nv_n + b_{15}, \\ v_{n+1} &= b_{21}u_n + b_{22}v_n + b_{23}u_nv_n + b_{24} \end{aligned}\right\} \quad (7)$$

Where,

$$b_{11} = 1 - \beta - \alpha\beta, b_{12} = -\beta, b_{13} = -\alpha, b_{14} = -1, b_{15} = 1 + \beta - \beta^2$$

$$b_{21} = \frac{(1-\alpha)(\beta-1)}{\beta}, b_{22} = 1, b_{23} = \frac{1}{\beta}, b_{24} = (1-\alpha)(\beta-1)$$

The linear part of (7) is transformed into a canonical form by the matrix T

$$T = \begin{pmatrix} b_{12} & 0 \\ \mu - b_{11} & -\eta \end{pmatrix} \begin{pmatrix} X_n \\ Y_n \end{pmatrix}$$

where,

$$\mu = \frac{(\alpha+\alpha_1)\beta - \beta - 2}{2},$$

and

$$\eta = \frac{\sqrt{((\alpha+\alpha_1)\beta - \beta - 2)^2 - 4((\alpha+\alpha_1) - 2\alpha\beta + 2\beta)}}{2}.$$

In this way, the system (7) can be expressed as follows:

$$\left.\begin{aligned} X_{n+1} &= \mu X_n - \eta Y_n + \widetilde{H}(X_n, Y_n) \\ Y_{n+1} &= \eta X_n + \mu Y_n + \widetilde{K}(X_n, Y_n) \end{aligned}\right\} \quad (8)$$

where

$$\left.\begin{aligned} \widetilde{H}(X_n, Y_n) &= m_{11}X_n^2 + m_{12}X_nY_n + m_{13} \\ \widetilde{K}(X_n, Y_n) &= m_{21}X_n^2 + m_{22}X_nY_n + m_{23} \end{aligned}\right\} \quad (9)$$

and

$$m_{11} = b_{12}b_{13} + (\mu - b_{11})b_{14}, \quad m_{12} = -b_{14}\eta, m_{13} = b_{15}$$

$$m_{21} = b_{12}b_{23}(\mu - \eta), \quad m_{22} = -b_{12}b_{23}\eta, m_{23} = b_{24}$$

Furthermore,

$$\widetilde{H}_{X_nX_n} \mid_{(0,0)} = 2m_{11}, \widetilde{H}_{X_nY_n} \mid_{(0,0)} = m_{12}, \widetilde{H}_{Y_nY_n} \mid_{(0,0)} = 0$$

$$\widetilde{H}_{X_nX_nX_n} \mid_{(0,0)} = \widetilde{H}_{X_nX_nY_n} \mid_{(0,0)} = \widetilde{H}_{X_nY_nY_n} \mid_{(0,0)} = \widetilde{H}_{Y_nY_nY_n} \mid_{(0,0)} = 0$$

and

$$\widetilde{K}_{X_nX_n} \mid_{(0,0)} = 2m_{21}, \widetilde{K}_{X_nY_n} \mid_{(0,0)} = m_{22}, \widetilde{K}_{Y_nY_n} \mid_{(0,0)} = 0$$

$$\widetilde{K}_{X_nX_nX_n} \mid_{(0,0)} = \widetilde{K}_{X_nX_nY_n} \mid_{(0,0)} = \widetilde{K}_{X_nY_nY_n} \mid_{(0,0)} = \widetilde{K}_{Y_nY_nY_n} \mid_{(0,0)} = 0$$

For (8) to experience the Neimark-Sacker bifurcation, the following relation must be nonzero (Singh and Deolia 2020)

$$\Omega = -Re\left[\frac{(1-2\bar{\lambda})\bar{\lambda}^2}{1-\lambda}\zeta_{11}\zeta_{20}\right] - \frac{1}{2} \parallel \zeta_{11} \parallel^2 - \parallel \zeta_{02} \parallel^2 + Re(\bar{\lambda}\,\zeta_{21})$$

Where,

$$\zeta_{02} = \frac{1}{8}[\widetilde{H}_{X_nX_n} - \widetilde{H}_{Y_nY_n} + 2\widetilde{K}_{X_nY_n} + \iota(\widetilde{K}_{X_nX_n} - \widetilde{K}_{Y_nY_n} + 2\widetilde{H}_{X_nY_n})] \mid_{(0,0)},$$

$$\zeta_{11} = \frac{1}{4}[\widetilde{H}_{X_nX_n} - \widetilde{H}_{Y_nY_n} + \iota(\widetilde{K}_{X_nX_n} + \widetilde{K}_{Y_nY_{n)}}] \mid_{(0,0)},$$

$$\zeta_{20} = \frac{1}{8}[\widetilde{H}_{X_nX_n} - \widetilde{H}_{Y_nY_n} + 2\widetilde{K}_{Y_nY_n} + 2\widetilde{K}_{X_nY_n} + \iota(\widetilde{K}_{X_nX_n} - \widetilde{K}_{Y_nY_n} - 2\widetilde{H}_{X_nY_n})]\,|_{(0,0)}$$

$$\zeta_{21} = \tfrac{1}{16}[\widetilde{H}_{X_nX_nX_n} + \widetilde{H}_{X_nY_nY_n} + \widetilde{K}_{X_nX_nY_n} + \widetilde{K}_{Y_nY_nY_n} + \iota(\widetilde{K}_{X_nX_nX_n} + \widetilde{K}_{X_nY_nY_n} - \widetilde{H}_{X_nX_nY_n} - \widetilde{H}_{X_nX_nY_n})]\,|_{(0,0)}$$

.

After calculation , we get

$$\zeta_{02} = \frac{1}{4}[m_{11} + m_{22} + \iota(m_{21} + m_{12})],$$

$$\zeta_{11} = \frac{1}{2}[m_{11} + \iota m_{21}],$$

$$\zeta_{20} = \frac{1}{4}[m_{11} + m_{22} + \iota(m_{21} - m_{12})],$$

$$\zeta_{21} = 0,$$

CHAOS CONTROL

The whole point of this section is to explore chaos control via state feedback control (Singh and Deolia 2020; Salman SM 2016; Alaydi 1996; Rana *et al.* 2017; Abarbanel 1996). To ensure that this section is comprehensive, we will first give an explanation of marginal stability.

Definition 2: Marginally stable refers to systems or processes that are neither stable nor unstable, but exist at the boundary between stability and instability. This indicates the possibility of an unstable system occurring when a small perturbation occurs.

In this case, we have a discrete biological model (3) that is as follows:

$$\left.\begin{aligned} x_{n+1} &= (1-A)x_n^2 + x_n(A - y_n) + w_n \\ y_{n+1} &= \tfrac{1}{B}x_n y_n \end{aligned}\right\} \tag{10}$$

Control is added by the addition of $w_n = -p\,(x_n - B) - q\,(y_n - (A + (1-A)B - 1))$, with p, q indicating feedback gains. At the interior fixed point P of the controlled system (10), the variational matrix V_P is evaluated according to the map below:

$$(F, G) \longmapsto (x_{n+1}, y_{n+1}) \tag{11}$$

Where

$$\left.\begin{aligned} F :&= (1-A)x_n^2 + x_n(A - y_n) - p\,(x_n - B) - \\ &\quad q\,(y_n - (A + (1-A)B - 1)) \\ G :&= \frac{1}{B}x_n y_n \end{aligned}\right\} \tag{12}$$

$$V_P = \begin{pmatrix} A - p + 2(1-A)x - y & -q - x \\ \frac{y}{B} & \frac{x}{B} \end{pmatrix}$$

If characteristic root corresponding to V_P is represented by Λ_1, Λ_2 at P, then

$$\Lambda_1 + \Lambda_2 = 2 + B - AB - p \tag{13}$$

$$\Lambda_1\Lambda_2 = A + 2B - 2AB - p - \frac{(-1+A)(-1+B)\,q}{B} \tag{14}$$

Solving equations (13) and (14) brings out the lines of marginal stability under the following conditions ($\Lambda_1 = \pm 1$ and $\Lambda_1\Lambda_2 = 1$). The presence of these conditions guarantees that the moduli of the eigenvalues are less than 1.

When $\Lambda_1\Lambda_2 = 1$, then from (14), we can get

$$M_1 : A + 2B - 2AB - p - \frac{(-1+A)(-1+B)\,q}{B} - 1 = 0 \tag{15}$$

When $\Lambda_1 = 1$, then from (13) and (14), we can get

$$M_2 : \frac{(-1+A)\,(-1+B)\,(B+q)}{B} = 0 \tag{16}$$

When $\Lambda_1 = -1$, then from (13) and (14), we can get

$$M_3 : 3AB + 2p + \frac{(-1+A)\,(-1+B)q}{B} - 3 - A - 3B = 0 \tag{17}$$

By taking (15), (16) and (17) in conjunction, we obtain the triangular region, which further reveals the fact that $|\Lambda_{1,2}| < 1$.

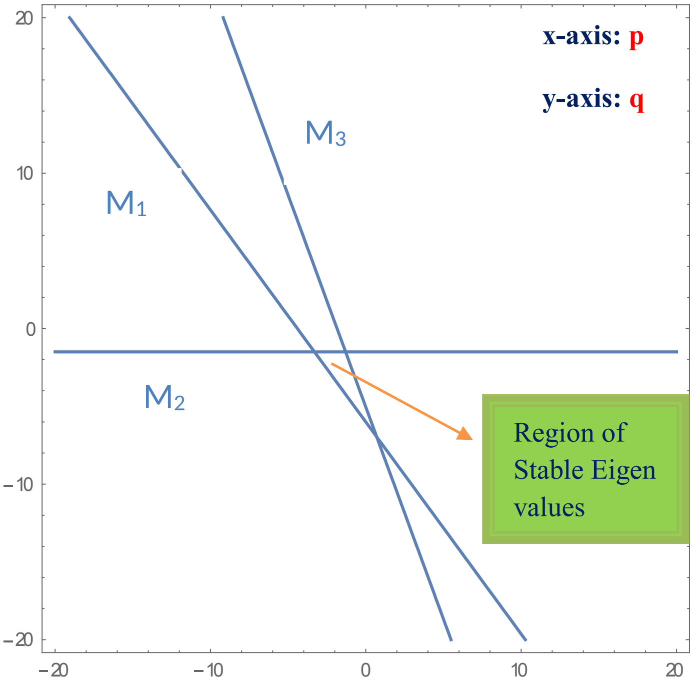


Figure 1 Region of stability where $|\Lambda_{1,2}| < 1$

NUMERICAL SIMULATION

As a follow-up to our theoretical results, here we will provide some numerical simulations to support the dynamical behavior of the system (3). Our results would not be hyperbolic if $B = 0.5$. According to Lemma 2.3, if $A = 2.5$, the bifurcation parameter will be stable. It is however not possible to have a stable bifurcation parameter if $A < 2.5$, as then attracting close curves will emerge from a positive equilibrium. Based on Figures 14 and 25, the local stability of the unique positive equilibrium is ensured. Based on

Figures 15 and 17, one can immediately see from Figure 16 and Figure 18 an attractor of the system (3). As a result, Figure 2 to Figure 13 represent the local stability of the system (3), whereas Figure 14 to Figure 25 illustrate the global asymptotic stability of the unique positive equilibrium. As shown in Figure 20 to Figure 24, the unique positive equilibrium is unstable for different parameter choices when $B < 0.5$, whereas an attracting invariant closed curve bifurcates from the positive equilibrium. Figure 26 and Figure 27 show the Neimark-Sackar bifurcation of the system (3). The state feedback control method is then used to stabilize the chaos in the discrete biological model (3). We now proceed to Section (4) to verify the validity of the results obtained. Suppose $A = 3.2$ and $B = 1.5$, then (15), (16) and (17) can be obtained based on these values

$$M_1 : -4.4 - p - 0.733333q = 0 \tag{18}$$

$$M_2 : 0.733333(1.5 + q) = 0 \tag{19}$$

$$M_3 : 3.7 + 2p + 0.733333q = 0 \tag{20}$$

The lines found in (18), (19) and (20) form a triangle that represents the region encompassing $|\Lambda_{1,2}| < 1$ (see Figure 1). Figure 28 and Figure 29 show that the system (3) is sensitive to their initial conditions, which is a useful indicator of the system's sensitivity. Last but not least, numerical verification was performed to confirm the theoretical results. In different aspects of biology, especially in the field of ecology, this research can provide a theoretical basis for research.

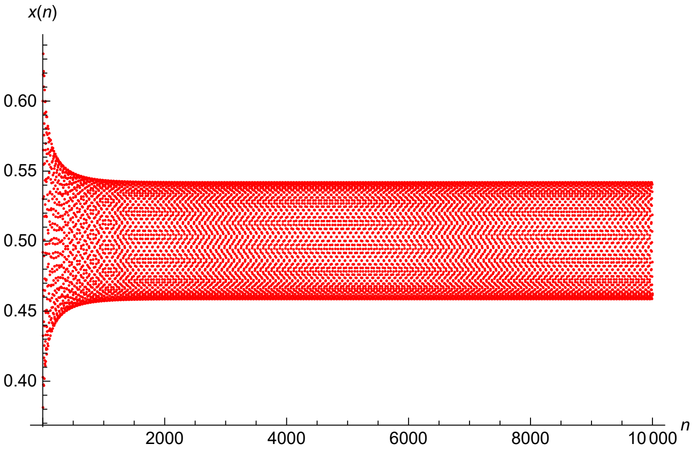


Figure 2 Shows behavior of solution of x_n, when $A = 2.3, B = 0.499, x_0 = 0.6, y_0 = 0.7$

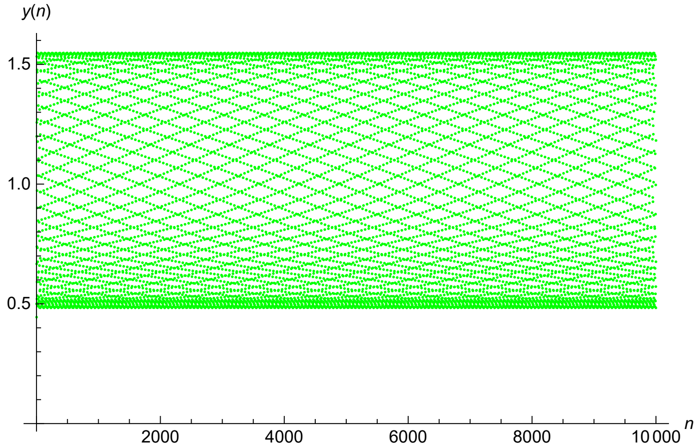


Figure 3 Shows behavior of solution of y_n, when $A = 2.98, B = 0.45, x_0 = 0.4, y_0 = 0.5$

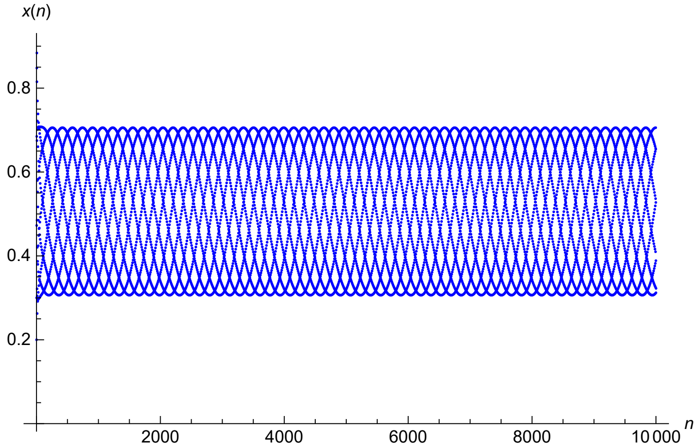


Figure 4 Shows behavior of solution of x_n, when $A = 2, B = 0.48, x_0 = 0.2, y_0 = 0.3$

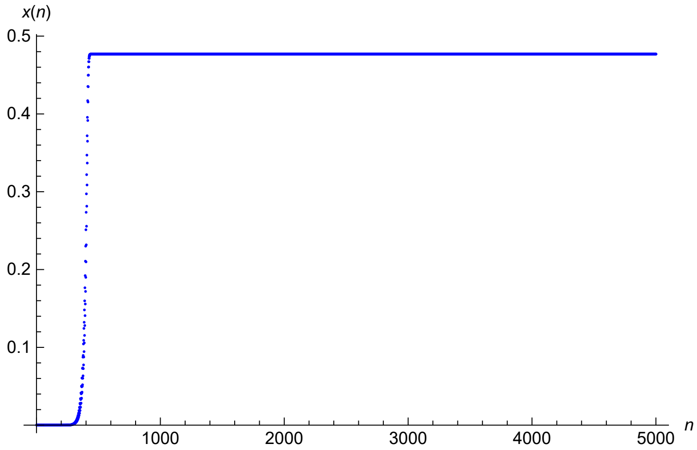


Figure 5 Shows behavior of solution of x_n, when $A = 3.51, B = 0.81, x_0 = 0.003, y_0 = 0.004$

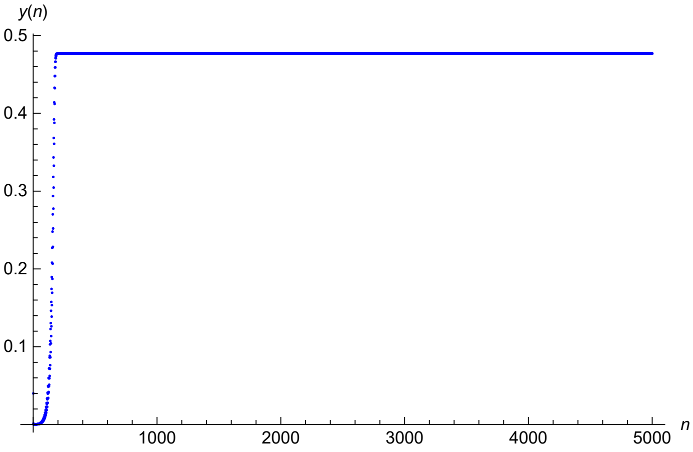


Figure 6 Shows behavior of solution of y_n, when $A = 3.51, B = 0.81, x_0 = 0.03, y_0 = 0.04$

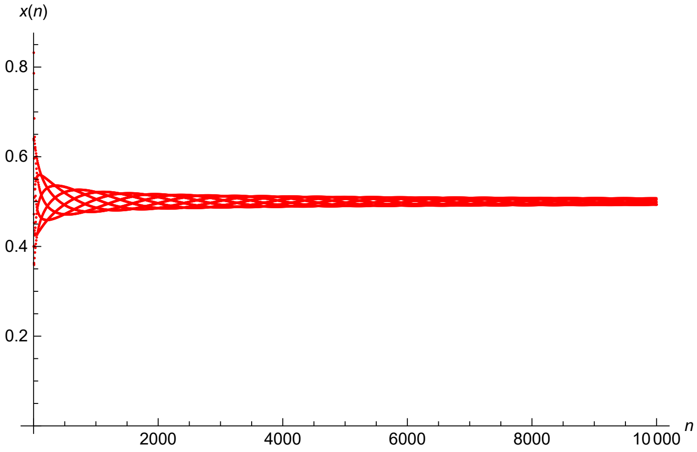


Figure 9 Shows behavior of solution of x_n, when $A = 2.5, B = 0.5, x(0) = 0.4, y_0 = 0.3$

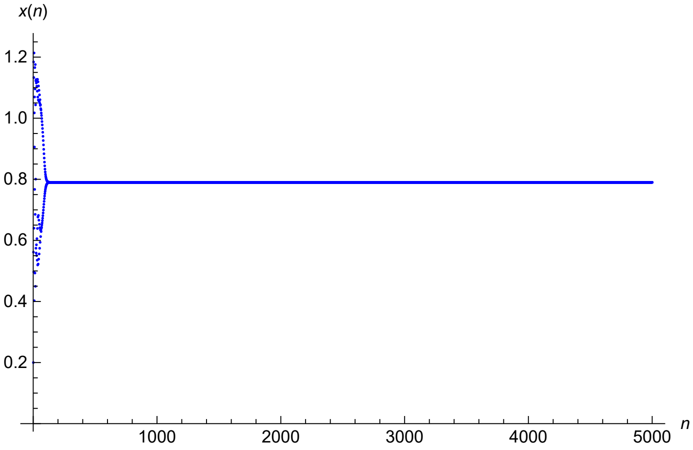


Figure 7 Shows behavior of solution of x_n, when $A = 3.76, B = 0.79, x_0 = 0.2, y_0 = 0.4$

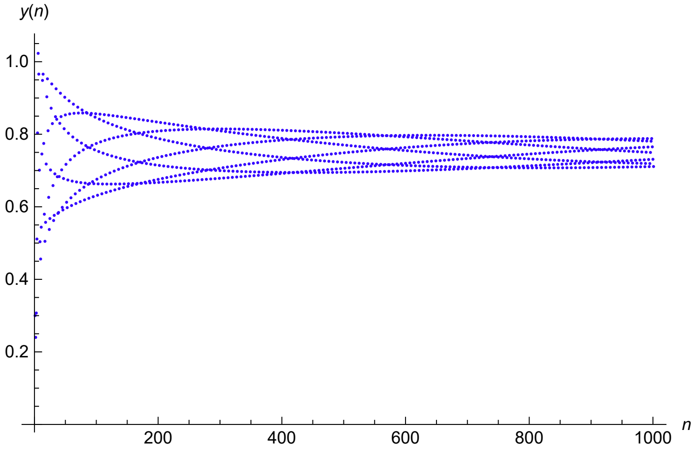


Figure 10 Shows behavior of solution of y_n, when $A = 2.5, B = 0.5, x_0 = 0.4, y_0 = 0.3$

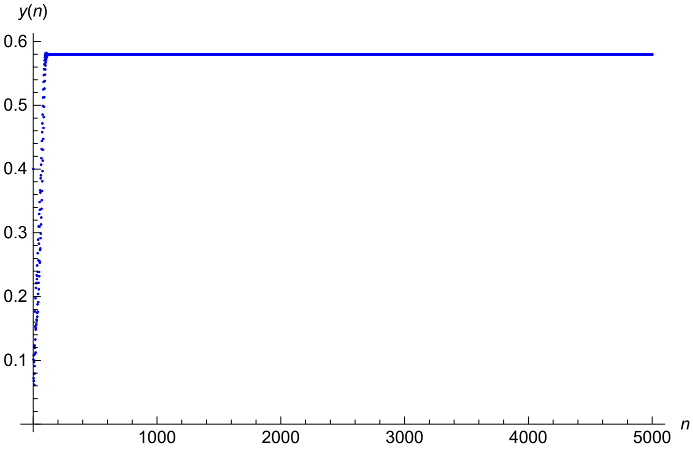


Figure 8 Shows behavior of solution of y_n, when $A = 3.76, B = 0.79, x_0 = 0.2, y_0 = 0.4$

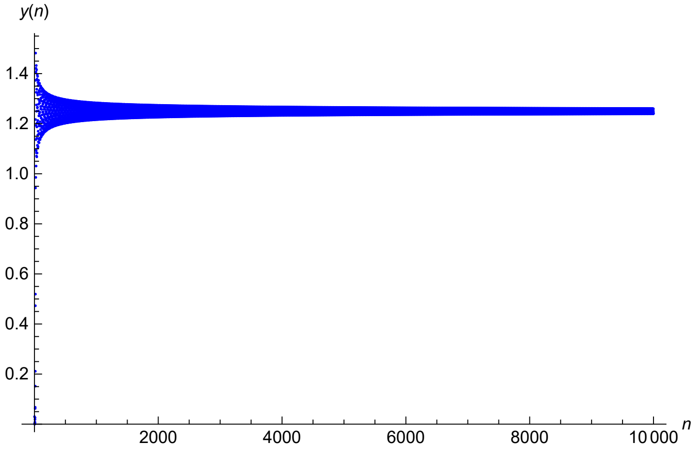


Figure 11 Shows behavior of solution of y_n, when $A = 3.5, B = 0.5, x_0 = 0.04, y_0 = 0.03$

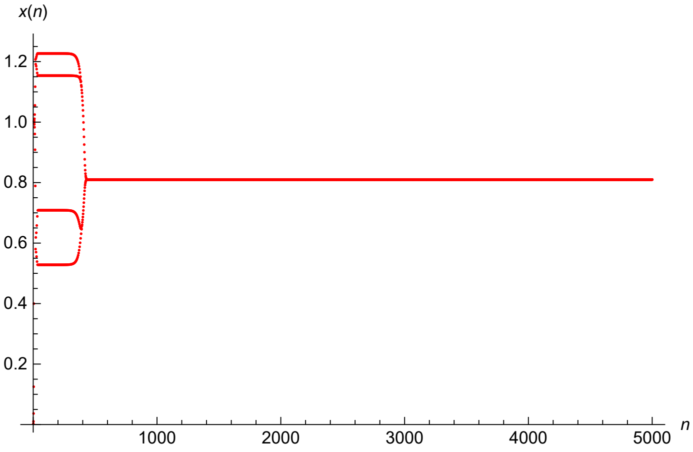


Figure 12 Shows behavior of solution of x_n, when $A = 3.51, B = 0.81, x_0 = 0.003, y_0 = 0.004$

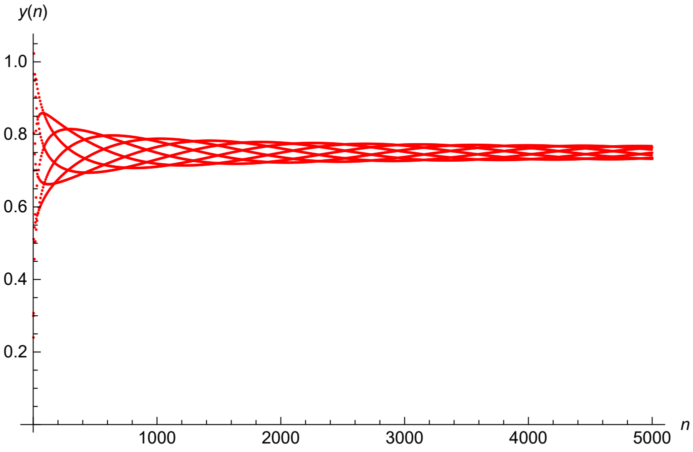


Figure 13 Shows behavior of solution of y_n, when $A = 2.5, B = 0.5, x_0 = 0.4, y_0 = 0.3$

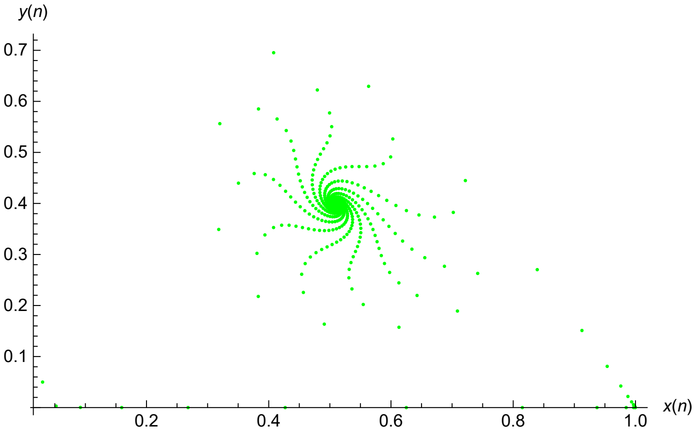


Figure 14 Shows phase portrait in (x, y) plane, when $A = 1.81, B = 0.51, x_0 = 0.03, y_0 = 0.05$, of system (3)

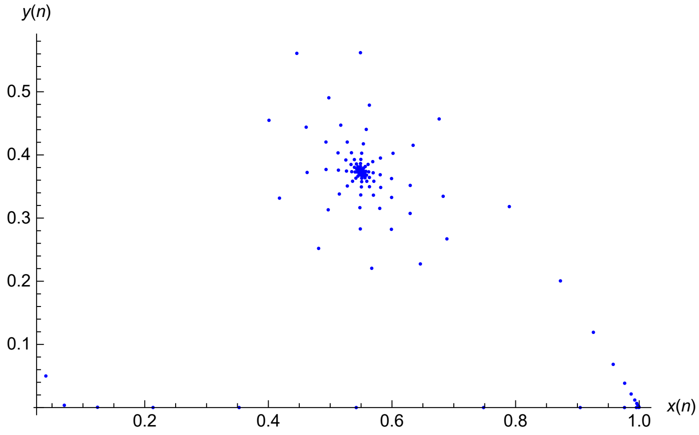


Figure 15 Shows phase portrait in (x, y) plane, when $A = 2.33, B = 0.5, x_0 = 0.003, y_0 = 0.005$, of system (3)

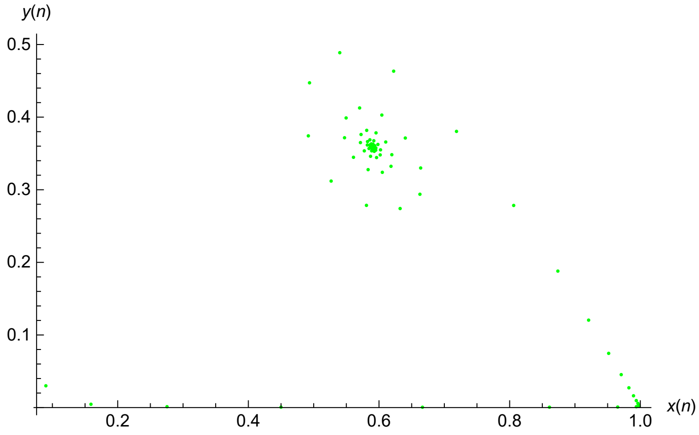


Figure 16 Shows phase portrait in (x, y) plane, when $A = 1.83, B = 0.55, x_0 = 0.04, y_0 = 0.05$, of system (3)

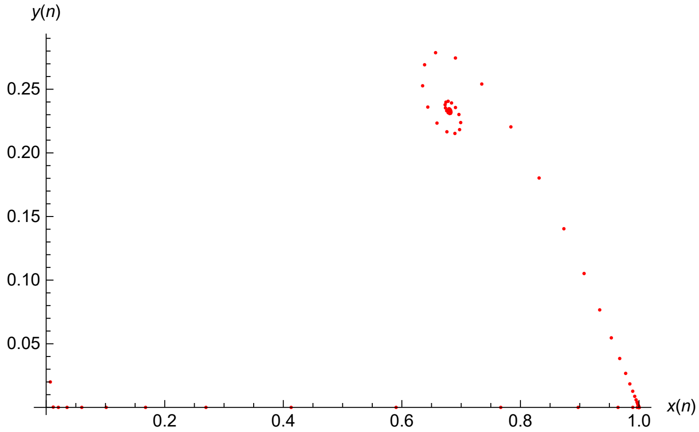


Figure 17 Shows phase portrait in (x, y) plane, when $A = 1.876, B = 0.59, x_0 = 0.09, y_0 = 0.03$, of system (3)

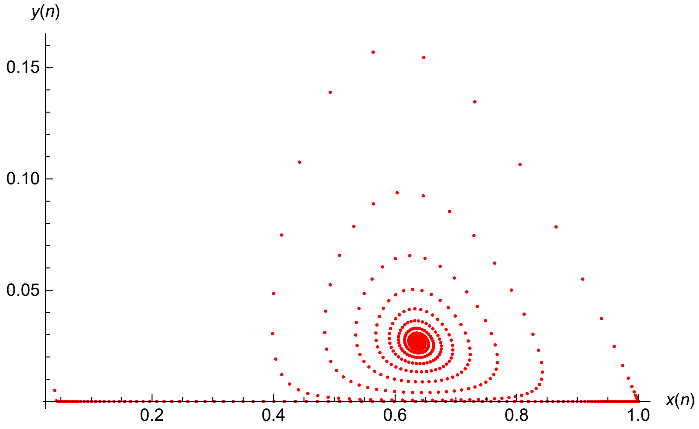


Figure 18 Shows phase portrait in (x,y) plane, when $A = 1.073, B = 0.637, x_0 = 0.04, y_0 = 0.005$, of system (3)

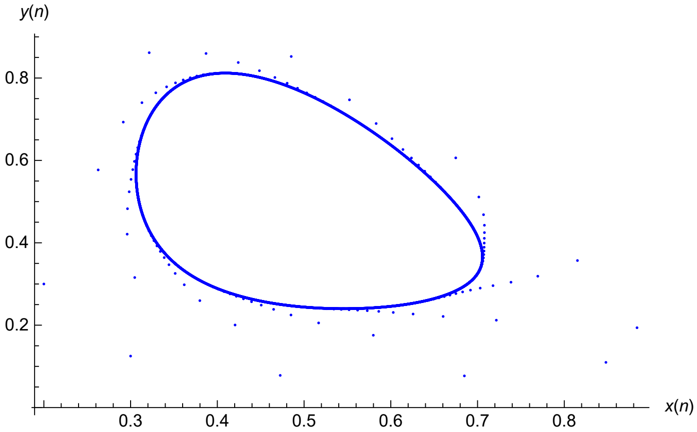


Figure 21 Shows phase portrait in (x,y) plane, when $A = 2, B = 0.48, x_0 = 0.2, y_0 = 0.3$, of system (3)

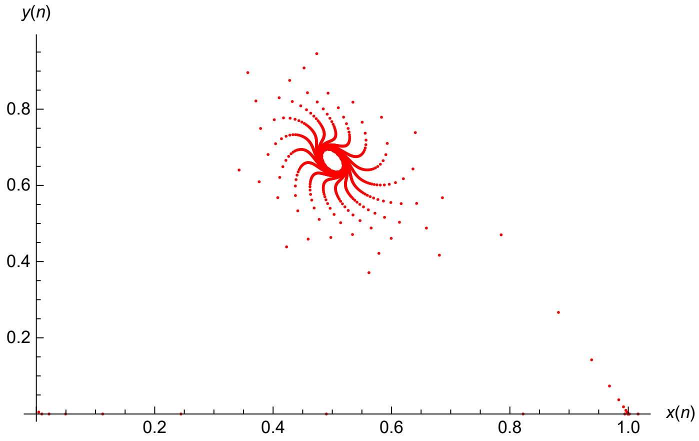


Figure 19 Shows phase portrait in (x,y) plane, when $A = 2.43, B = 0.44, x_0 = 0.0035, y_0 = 0.041$, of system (3)

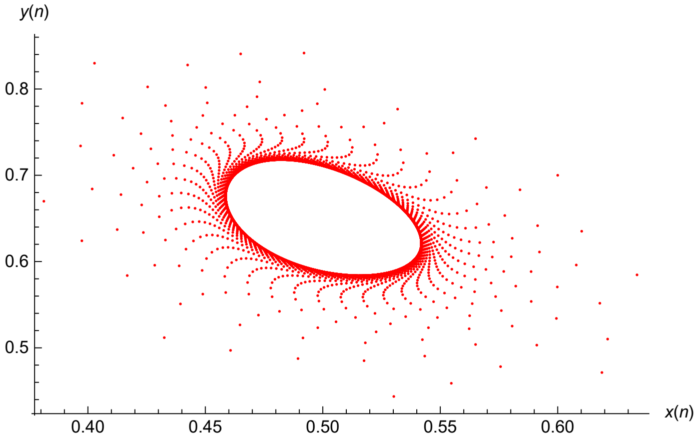


Figure 22 Shows phase portrait in (x,y) plane, when $A = 2.3, B = 0.499, x_0 = 0.6, y_0 = 0.7$, of system (3)

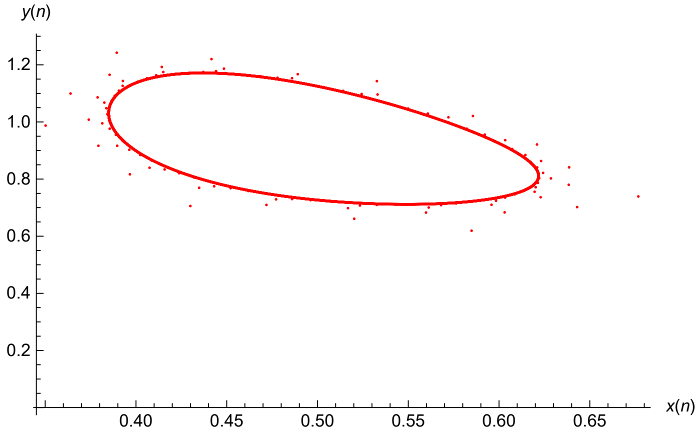


Figure 20 Shows phase portrait in (x,y) plane, when $A = 2.87, B = 0.49, x_0 = 0.7, y_0 = 0.8$, of system (3)

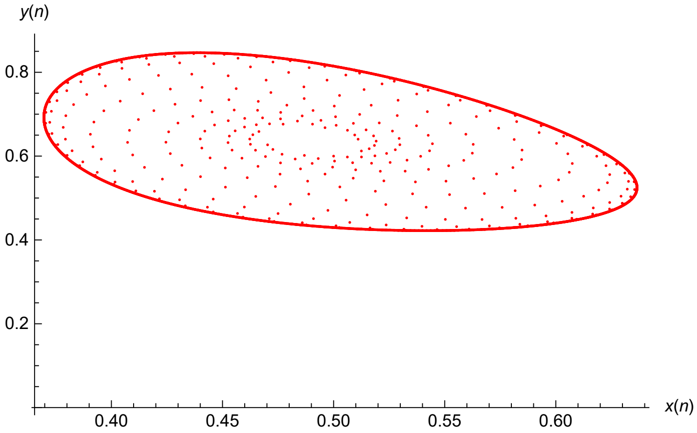


Figure 23 Shows phase portrait in (x,y) plane, when $A = 2.25, B = 0.49, x_0 = 0.5, y_0 = 0.6$, of system (3)

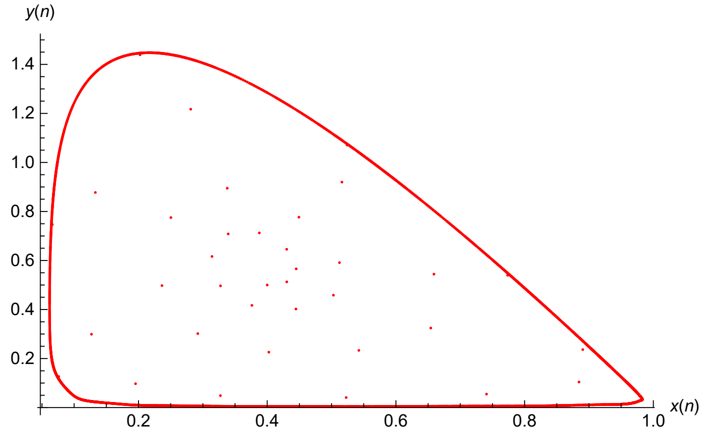


Figure 24 Shows phase portrait in (x, y) plane, when $A = 1.96, B = 0.39, x_0 = 0.4, y_0 = 0.5$, of system (3)

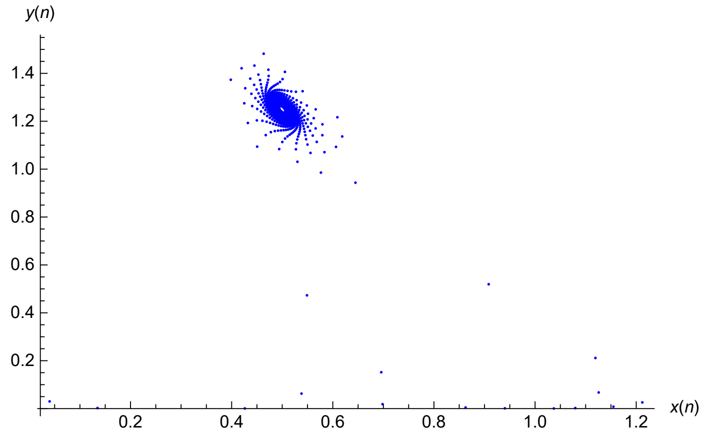


Figure 25 Shows phase portrait in (x, y) plane, when $A = 1.96, B = 0.39, x_0 = 0.4, y_0 = 0.5$, of system (3)

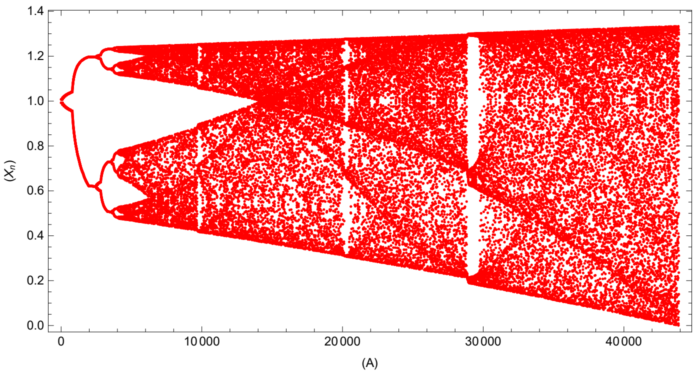


Figure 26 Neimark-Sacker bifurcation diagram of system (3) in (A, x_n) plane

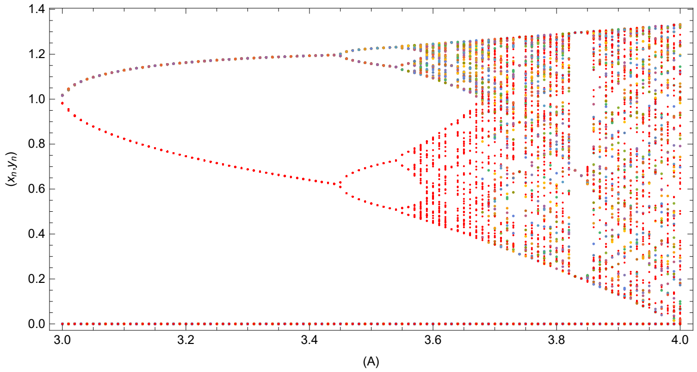


Figure 27 Neimark-Sacker bifurcation diagram of system (3) in (A, y_n) plane

MAXIMUM LYAPUNOV EXPONENT

The Lyapunov exponent is a concept derived from chaos theory and dynamical systems. The aim of this measurement is to determine how sensitive chaotic systems are to their initial conditions. When calculating adjacent trajectory divergences in phase space, one can use the Lyapunov exponent (Abarbanel 1996).

Positive Lyapunov exponents cause the trajectory of a system to diverge exponentially, leading to it being classified as chaotic. When Lyapunov exponents are above zero, the system outcomes are highly sensitive to conditions at the start, indicating even small changes could have major impacts. Alternatively, a negative Lyapunov exponent indicates that nearby trajectories are convergent, which indicates a predictable and stable system. From a mathematical perspective, it is defined as:

Definition 3: For the map

$$\Theta : \mathbb{R} \mapsto \mathbb{R}$$

The Lyapunov exponent is defined as:

$$\tilde{L} = \lim_{n \to \infty} ln \mid \frac{d}{dx} \Theta^n (x = x_0) \mid^{\frac{1}{n}} \tag{21}$$

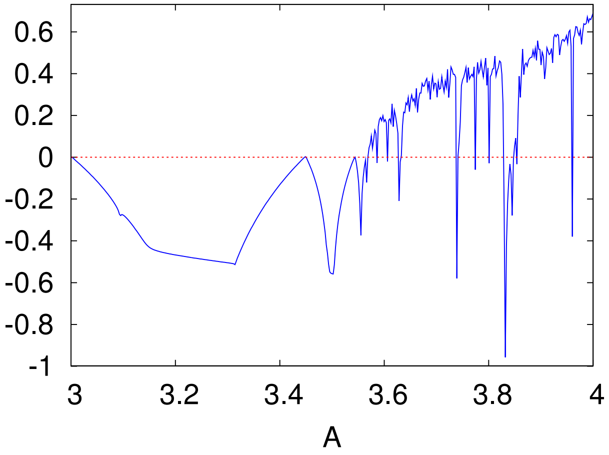


Figure 28 Maximum Lyapunov Exponent of the model (3)

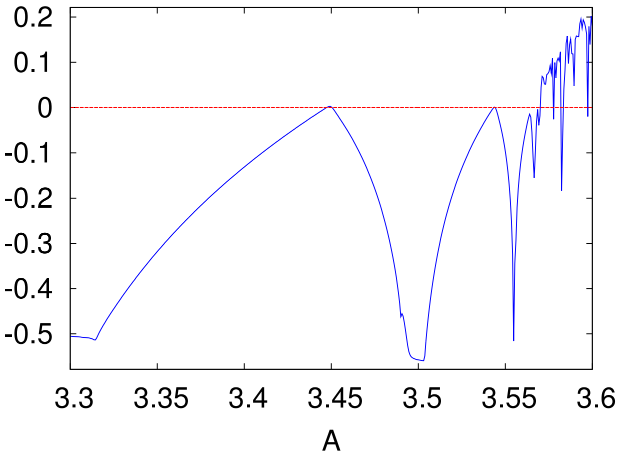


Figure 29 Maximum Lyapunov Exponent of the model (3)

CONCLUSION AND DISCUSSION

Previous research has demonstrated that population models described by difference equations have a crucial role in population dynamics and mathematical ecology. In this study, we examine the qualitative and dynamic properties of discrete predator-prey models. Based on bifurcation theory, we determined the stability conditions for a unique steady state. In this paper, we demonstrate that the model (3) undergoes NS bifurcation. Moreover, we present some numerical simulations including the behavior of solution of prey x_n and predator y_n over time (n), phase portraits of system by taking different initial conditions and the values of parameters and the bifurcation diagram determining the range of the bifurcation parameter $(3 < A < 4)$. All this numerical study has been conducted by using "Mathematica" program which verify our theoretical results.

In this paper, we demonstrate that the stability of the unique fixed point (3) occurs at a critical bifurcation value when the bifurcation parameter (A) reaches this critical value. Neimark-Sacker bifurcation follows. A more complex dynamics is also visible in certain regions in the model (3) when the parameter values are changed. We can conclude that parameter (A) is highly important for the stability of model (3). Additionally, under the influence of the Neimark-Sacker bifurcation, invariant closed curves are dynamically unstable. Model (3) is an interaction between predators and prey that can be viewed from the perspective of biology. As a result, both prey and predator populations are capable of oscillating around some mean values under suitable conditions since NS bifurcation exists in the model (3). In addition, the chaotic behavior of the model (3) can be controlled by using feedback control techniques. Besides showing the MLE, the article concludes that the system fluctuates within the chaotic region.

Availability of data and material

Not applicable.

Conflicts of interest

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

LITERATURE CITED

Abarbanel, H. D. I., 1996 *Analysis of Observed Chaotic Data*. Number 34, Springer New York, NY.

Alaydi, S., 1996 *An introduction to difference equations*. Number 32, Springer New York, NY.

Chen, Y. and S. Changming, 2008 Stability and hopf bifurcation analysis in a prey–predator system with stage-structure for prey and time delay. Chaos, Solitons & Fractals **38**: 1104–1114.

Fazly, M. and M. Hesaaraki, 2007 Periodic solutions for a discrete time predator–prey system with monotone functional responses. Comptes Rendus. Mathématique **345**: 199–202.

Gakkhar, S. and A. Singh, 2012 Complex dynamics in a prey predator system with multiple delays. Communications in Nonlinear Science and Numerical Simulation **17**: 914–929.

Garic Demirovic M., K. M. . N. M., 2009 Global behavior of four competitive rational systems of difference equations in the plane. Discrete Dynamics in Nature and Society **2009**: 153058–153092.

Hu Z., T. Z. . Z., 2011 Stability and bifurcation analysis of a discrete predator-prey model with nonmonotonic functional response. Nonlinear Analysis: Real World Applications **12(4)**: 2356–2377.

Ibrahim, T. F. and N. Touafek, 2014 Max-type system of difference equations with positive two-periodic sequences. Math. methods Appl. sci **37**: 2562–2569.

Joydip Dhar, H. S. . H. S. B., 2015 Discrete-time dynamics of a system with crowding effect and predator partially dependent on prey. Applied Mathematics and Computation **252**: 1104–1114.

Kalabusic S., K. M. . P. E., 2011 Multiple attractors for a competitive system of rational difference equations in the plane. Abstract and Applied Analysis **37(16)**: 1–17.

Khan, A., 2016 Neimark-Sacker bifurcation of a two-dimensional discrete-time predator-prey model. SpringerPlus **5**: 121–126.

L. Men, G. W. Z. W. L. . W. L., B. S. Chen, 2015 Hopf bifurcation and nonlinear state feedback control for a modified Lotka-Volterra differential algebraic predator-prey system. Fifth International Conference on Intelligent Control and Information Processing **2015**: 233–238.

Pan, S. X., 2013 Asymptotic spreading in a Lotka-Volterra predator-prey system. The Journal of Mathematical Analysis and Applications **407**: 230–236.

Q., Q. M. . K. A., 2015 Periodic solutions for discrete time predator-prey system with monotone functional responses. International Academy of Ecology and Environmental Sciences **5(1)**: 48–62.

R. M. Eide, N. T. F. . R. A. V. G., A. L. Krause, 2018 The origins and evolutions of predator-prey theory. Journal of Theoretical Biology **451**: 19–34.

Rana, S., U. Kulsum, *et al.*, 2017 Bifurcation analysis and chaos control in a discrete-time predator-prey system of leslie type with simplified holling type iv functional response. Discrete Dynamics in Nature and Society **2017**.

Salman SM, Y. A. . E. A., 2016 Stability, bifurcation analysis and chaos control of a discrete predator-prey system with square root functional response. Chaos Solitons Fractals **93**: 20–31.

Sen M, B. M. . M. A., 2012 Bifurcation analysis of a ratio-dependent prey-predator model with the Allee effect. Ecological Complexity **11**: 12–27.

Singh, A. and P. Deolia, 2020 Dynamical analysis and chaos control in discrete-time prey-predator model. Communications in Nonlinear Science and Numerical Simulation **90**: 105313.

Smith, J. M., 1968 *Mathematical Ideas in Biology*, volume 1. Cambridge University Press.

X. W. Jiang, T. W. H. . H. C. Y., X. Y. Chen, 2021 Bifurcation and control for a predator-prey system with two delays. IEEE Transactions on Circuits and Systems II: Express Briefs **68**: 376–380.

X. Zhang, Z. W. . T. Z., 2016 Periodic solutions for discrete time predator-prey system with monotone functional responses. Journal of Biological Dynamics **10**: 1–17.

Z. L. Luo, Y. P. L. . Y. X. D., 2016 Rank one chaos in periodically kicked Lotka-Volterra predator-prey system with time delay. Nonlinear Dynamics **85**: 797–811.

Zhang C.H, Y. X. . C. G., 2010 Hopf bifurcations in a predator-prey system with a discrete delay and a distributed delay. Nonlinear Anal Real World Application **10**: 4141–4153.

Zu, L., D. Jiang, D. O'Regan, T. Hayat, and B. Ahmad, 2018 Ergodic property of a lotka–volterra predator–prey model with white noise higher order perturbation under regime switching. Applied Mathematics and Computation **330**: 93–102.

How to cite this article: Abbas, A., and Khaliq, A. Analyzing Predator-Prey Interaction in Chaotic and Bifurcating Environments. *Chaos Theory and Applications*, 5(3), 207-218, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / **No.**3 / 2023 / **pp.**219-232
https://doi.org/10.51537/chaos.1285094

Analyses of Reconfigurable Chaotic Systems and their Cryptographic S-box Design Applications

Mangal Deep Gupta[*,1], **Rajeev Kumar Chauhan**[α,2] **and Vipin Kumar Upaddhyay**[β,3]
[*]Department of Electronics and Communication Engineering, University Institute of Engineering & Technology, Babasaheb Bhimrao Ambedkar Central University, Lucknow, Uttar Pradesh, India, [α]Department of Electronics and Communication Engineering, MMMUT, Gorakhpur, Uttar Pradesh, India, [β]Electronics Engineering, Harcourt Butler Technical University, Kanpur, Uttar Pradesh, India.

ABSTRACT This manuscript includes the design and evaluation of the new four 16×16 S-boxes for subbyte operation in image encryption applications and estimates their strength using the following parameters: Dynamic Distance, BIC non-linearity, Bijective, Non-linearity, Strict Avalanche Criterion (SAC), and Balanced criterion. The S-box matrix is designed by a new reconfigurable 3D-Chaotic PRNG. This PRNG is designed using four different 3D chaotic systems i.e. Lorenz, Chen, Lu, and Pehlivan's chaotic systems. This reconfigurable architecture of PRNG exploits the ODEs of these four attractors that fit all four chaotic systems in a single circuit. The first part of this manuscript is focused to develop hardware-efficient VLSI architecture. To demonstrate the hardware performance, the PRNG circuit is implemented in Virtex-5 (XC5VLX50T) FPGA. A performance comparison of proposed and existing PRNGs (in terms of timing performance, area constraint, power dissipation and statistical testing) has been presented in this work. The PRNG generates the 24-bit random number at 96.438-MHz. The area of FPGA is occupied by only 16.66 %, 1.08%, 0.33 %, and 1.15% of the available DSP blocks, slice LUTs, slice registers and slices respectively. The designed S-boxes using reconfigurable PRNG fulfill the following criteria: Dynamic Distance, BIC non-linearity, Bijective, Non-linearity, Strict Avalanche Criterion (SAC), and Balanced criterion.

KEYWORDS
Cryptography
Chaotic systems
PRNG
Operating frequency
NIST Tests
S-Boxes
FPGA

INTRODUCTION

Random number generators are one of the essential components in cryptography, testing of VLSI circuits, bank transactions, financial market, avionics communications, etc. Random keys are required in various steps of cryptography like subbyte operation using S-box, encryption, decryption, etc. (Lambić and Nikolic 2019; ElSafty *et al.* 2021; Garcia-Bosque *et al.* 2018; Garipcan and Erdem 2020). Nowadays, smart systems that are used in the automation of houses and buildings, industry, energy, medical, transportation, communication system, etc. require the security of data transfer and Internet of Things (IoT) applications (G. Di Patrizio Stanchieri and Faccio 2019). Multimedia data such as video, image, audio and text can be communicated over the network very hugely but these shared data have a serious security concern. The general way to achieve this request is to design complex software or/and hardware-based systems, which can generate random sequences that provide the private and public keys to get the effective data encryption and decryption process.

In general, there are two types of PRNG: (1) Linear and (2) Nonlinear PRNG. Nonlinear PRNG is designed using nonlinear dynamical systems that exhibit chaos behaviour (L'Ecuyer 2012). In these types of systems, extreme sensitivity with the initial conditions causes chaotic behaviors over long-term randomness or unpredictability (H. S. Alhadawi and Lambi 2019). So, the chaotic system determines the nonlinear system with high randomness characteristics and low design cost. This makes it suitable for the designing of nonlinear PRNG. For designing a chaos-based cipher, a plain message is masked or encrypted using random keys (which is generated from chaotic maps) (Ü. Çavuşoğlu and Kaçar 2019; Wang *et al.* 2016). Chaotic systems generate a pseudorandom sequence, which can be applied in designing cryptographic

---

Manuscript received: 18 April 2023,
Revised: 6 August 2023,
Accepted: 28 October 2023.

[1]mangaldeepgcet@gmail.com (**Corresponding author**).
[2]rkchauhan27@gmail.com
[3]vipin08120@gmail.com

keys to get their valuable characteristics like random behavior, sensitivity to the initial conditions, and ergodicity (Li *et al.* 2001). So, the cryptographic properties of chaotic-map-based random sequences are very crucial from a security point of view for encryption algorithms. The idea of utilizing a 3D chaotic attractor for the designing of the PRNG is based on its ability that can generate a sequence of random numbers (X. Y. Wang and Kadir 2010; Artuğer and Özkaynak 2022b).

For the last 40 years, various simple chaotic systems have been found and continue the studied within the 3D quadratic autonomous framework. There are four criteria for the existence of chaotic behavior in the study of dynamic nonlinear systems (Pehlivan and Uyaroğlu 2012). The first well-known criterion is Lyapunov exponents (Wolf *et al.* 1985). It decides the chaotic behavior of dynamic systems. If at least one positive Lyapunov exponent presents in the dynamic system, the dynamic of this system is chaotic. The second criterion is Melnikov's. It is used to investigate the occurrence of chaotic behavior in Hamiltonian systems and it analyzes by estimating the distance between unstable and stable manifolds (Xu *et al.* 2009). The third one is Sil'nikov's criterion (T. Zhou and Čelikovský 2005). The last criterion is the topological horseshoes theory; it is based on some subsets of interest in the state space of continuous maps (Li and Yang 2010). These four criteria have been fulfilled by Lorenz (Lorenz 1963), Chen & Gupta (Gupta and Chauhan 2022, 2020), Lu (Lu and Chen 2002), and Pehlivan (Pehlivan and Uyaroğlu 2010) chaotic attractors.

The first 3D chaotic system was founded by Lorenz in 1963, it is a third-order autonomous system that displays very complex dynamic behaviors (Lorenz 1963). Another similar chaotic attractor was found by Chen in 1999. It is dual to the Lorenz system and topologically non-equivalent 3D chaotic system that shows interesting characteristics (Gupta and Chauhan 2022). Lu *and Chen* found another chaotic attractor known as Lu 3D chaotic system (Lu and Chen 2002). It represents the transition between Chen and Lorenz 3D attractors. It is important to note that the 3D chaotic attractors i.e. Lorenz (Lorenz 1963; Artuğer and Özkaynak 2022a), Chen (Gupta and Chauhan 2022), and Lu chaotic system (Lu and Chen 2002), have three particular fixed points: one saddle-foci and two unstable saddle-foci. Recently, Pehlivan *et al.* introduced a new 3D chaotic attractor (Pehlivan and Uyaroğlu 2010). It is similar to the Lorenz and Chen systems, but it includes six terms with two quadratics in a form and they have two very different fixed points (*i.e.* two stable node-foci).

The Lorenz, Chen, Lu, and Pehlivan chaotic attractors have been utilized in cryptography as PRNGs (Akgul *et al.* 2019; Alçın *et al.* 2016) due to their advantageous properties as discussed. To model the mathematical formation of a chaotic system, an ordinary differential equation (ODE) is used. It represents the rate-of-change of variables of a chaotic system. The ODEs can be solved using three different techniques i.e. Runge-Kutta, mid-point, or Euler's method (Zidan *et al.* 2011). Each chaotic system has a certain parameter value, which leads to the desired behavior of a chaotic system. One method to see the chaotic behavior of dynamic systems is to draw a three-dimensional (3D) plot, which is also known as an attractor. It demonstrates how the solutions of system variables evolve. Various analog and digital encryption circuits/systems have been designed using different chaotic attractors (Alawida *et al.* 2020; Zamli *et al.* 2023; Zhao *et al.* 2019; Rezk *et al.* 2020; Garcia-Bosque *et al.* 2019).

The subbyte operation in image encryption algorithms is the first step and primarily it decides the security strength of encrypted images. This operation is performed by the S-Box matrix (Zahid *et al.* 2021; Ahmad and Alsolami 2020; Alhadawi *et al.* 2020). It includes the 8-bit integers in random order in the form of a matrix. Therefore, the S-box plays the important role in image encryption algorithms. There is various image encryption algorithms available in the literature which shows the importance of S-boxes. The image encryption method using a chaotic attractors-based S-box matrix was proposed by Tang et. al. in (Tang *et al.* 2005). The S-box-based encryption using tent maps chaotic system was proposed by Y. Wong et. al. in (Wang *et al.* 2009). *M. Khan et. al.* proposed the new S-boxes using a Boolean function of a chaotic system (Khan *et al.* 2016, 2022). *Unal Çavusoglu et. al.* developed the chaotic S-box-based new image encryption algorithm which offers high-security strength and fast operation (Çavusoglu *et al.* 2017). The image encryption algorithm that uses different S-boxes in each cycle was proposed by Xiong Wang et. al. in (Wang *et al.* 2019; Artuğer 2023). The selection of S-boxes in this method is random which performs the image encryption.

This manuscript has introduced the four new S-boxes using reconfigurable PRNG. This reconfigurable PRNG is designed using four different 3D chaotic systems i.e. Lorenz, Chen, Lu, and Pehlivan attractors. All four chaotic systems reconfigure in a single architecture due to exploiting the similarities between the differential equations. The VLSI architecture of the proposed reconfigurable PRNG replaces the complex multiplication by hardwired shifting operation. The first part of this manuscript aims to develop hardware-efficient VLSI architecture that enhances the timing performances (in terms of latency, bit rate, and maximum operating frequency), length of the sequence, and randomness. The random sequences from all four chaotic systems are tested for randomness using the NIST test suite.

To evaluate the hardware performance, the proposed architecture has been implemented on prototype Virtex-5 (XC5VLX50T) FPGA. The next part of this manuscript includes the design of four new 16×16 S-boxes using the proposed reconfigurable PRNG. To check the suitability of proposed S-boxes in encryption applications, the following parameters: Dynamic Distance, Bijective, Balanced, Non-linearity, BIC non-linearity criterion and SAC have been evaluated in this manuscript. The remaining sections of this manuscript are arranged as follows: The dynamic behavior of Lorenz, Chen, Lu, and Pehlivan's chaotic systems are presented in Section-2. Section-3 includes the reconfigurable architecture of PRNG. The statistical description of generated bit Sequences using NIST is discussed in Section-4. A comprehensive description and comparison of PRNGs is presented in Section-5. Section-6 includes the design and evaluation of proposed S-boxes. The final conclusion of this manuscript is mentioned in Section-7.

DESCRIPTION OF LORENZ, CHEN, LU AND PEHLIVAN CHAOTIC SYSTEM

In this section, we construct parameter variables of Lorenz, Chen, Lu, and Pehlivan's three-dimensional (3D) chaotic attractors to design the hardware efficient and secure digital system of reconfigurable PRNG. The mathematical formation of chaotic attractors is done by ODEs. The numerical solution of ODEs can be done by three different methods: Runge-Kutta, Euler's method or mid-point. Hardware point of view, the most suitable approach is Euler's method. In this work, this method is adopted to solve the ODEs of a chaotic system. Eqs. (1) to (3) represent the Euler's equations corresponding variables: x_i, y_i and z_i.

$$x_{i+1} = x_i + h.\dot{x}_i \tag{1}$$

$$y_{i+1} = y_i + h.\dot{y}_i \tag{2}$$

$$z_{i+1} = z_i + h.\dot{z}_i \tag{3}$$

Table 1 to Table 4 includes the parameter values, range of variables and ODEs corresponding to Lorenz (Lorenz 1963), Chen (Gupta and Chauhan 2022), Lu (Lu and Chen 2002), and Pehlivan (Pehlivan and Uyaroğlu 2010) chaotic attractors. The selection of parameter values (as shown in Tables 1 to 4) offers hardware efficient reconfigurable architecture of PRNG. Table 1 shows the ODEs, range of variables, and parameter value for the Lorenz chaotic system.

Three variables of this chaotic system are represented by x_i, y_i and z_i, while a, b and c are the parameters. Similarly, Table 2 presents the ODEs, range of variables, parameter's value for Chen's chaotic system, where x_i, y_i and z_i, a, b and c show the same meaning. The third attractor is the Lu chaotic system. It has a wide range of parameter values in which the attractor displaces a different shape and represents the transition between Chen and Lorenz 3D attractors. The ODEs and range of variables are mentioned in Table 3, where a, b, c are the parameter variables. The last one is Pehlivan's chaotic system. It is similar to the Chen, and Lorenz systems, but it includes six terms with two quadratics in a form and they have two very different fixed points (i.e. two stable node-foci). Its ODEs are mentioned in Table 4, where a is the parameter variable, and x_i, y_i and z_i are system variables.

This section includes the simulation of the dynamic behavior of Lorenz, Chen, Lu, and Pehlivan's chaotic system using the Matlab Tool. To replace a large number of binary multiplication, parameter variables of chaotic systems are set to be specific values (as shown in Tables 1 to 4). The benefit of this approach is able to design multiplierless (except $x_i.y_i$ and $x_i.z_i$) reconfigurable digital chaotic PRNG. The plane and space plot of the proposed Lorenz, Chen, Lu, and Pehlivan's chaotic system are shown in Fig. 1. The Lorenz system has a 3D attractor as shown in Fig. 1(a), with parameters values: $a = 32, b = 4, c = 32$, initial condition $(x_0, y_0, z_0) = (1, 1, 1)$ and step size: $h = 2^{(-8)}$. Next, the 3D attractor of the Chen chaotic system is present in Fig. 1(b), with the parameters values: $a = 32, b = 4, c = 24$, initial condition $(x_0, y_0, z_0) = (5, -15, 40)$ and step size:$h = 2^{(-8)}$ Fig. 1(c) shows the chaotic attractor of Lu system with $a = 32, b = 4, c = 16$, initial condition $(x_0, y_0, z_0) = (1, 1, 1)$ and step size: $h = 2^{(-8)}$. Similarly, Fig. 1(d) represents the chaotic attractor of Pehlivan system with $a = 0.5, h = 2^(- 8)$ and initial condition $(x_0, y_0, z_0) = (0.001, 0.001, 0)$. The phase plane behavior of Lorenz, Chen, Lu, and Pehlivan's chaotic system are shown in Fig. 2 to Fig. 5, correspondingly.

The xy, xz, and yz phase portraits of the Lorenz system are shown in Fig. 2 with the same parameter values and initial condition. The two-dimensional (2D) attractor plots in the plane of Chen's chaotic system are displayed (with the following details: parameter values $a = 32, b = 4, c = 24, h = 2^{-8}$ and initial condition: $(x_0, y_0, z_0) = (5, -15, 40)$ in Fig. 3. Similarly, Fig. 4 represents the phase portraits of Lu system with $a = 32, b = 4, c = 16, h = 2^{-8}$ and initial condition $(x_0, y_0, z_0) = (1, 1, 1)$. Finally, the xy,xz and yz phase portraits of the Pehlivan system with the same parameter value and initial condition (as discussed in Table 4) are shown in Fig. 5.

Table 1 Variables range and Parameter's value for Lorenz chaotic system.

Lorenz chaotic system		
ODEs Lorenz (1963)	Parameters	Range
$\dot{x}_i = a(y_i - x_i)$	$a = 32, b = 4, c = 32,$	$-28.1805 \leq x \leq 29.2467$
$\dot{y}_i = -x_i z_i + c x_i - y_i$	$h = 2^{-8}, x_0 = 1,$	$-31.1805 \leq y \leq 33.1210$
$\dot{z}_i = x_i y_i - b z_i$	$y_0 = 1, z_0 = 1$	$0.9215 \leq z \leq 58.6626$

Table 2 Variables range and Parameter's value for Chen's chaotic system.

Chen Chaotic System		
ODEs Gupta and Chauhan (2022)	Parameters	Range
$\dot{x}_i$=a.$(y_i - x_i)$	$a = 32, b = 4, c = 14,$	-24.280$\leq x \leq$ 23.9385
$\dot{y}_i$=-x_i.z_i+(c-a).x_i+c.y_i	h=$2^{-8}, x_0 = 5,$	-27.4307$\leq$ y $\leq$27.0290
$\dot{z}_i$= x_i.y_i- b.z_i	$y_0 = -15, z_0 = 40$	1.7161$\leq$ z $\leq$ 47.230

Table 3 Variables range and Parameter's value for Lü chaotic system.

Lu Chaotic System		
ODEs Lu and Chen (2002)	Parameters	Range
$\dot{x}_i$=a.$(y_i - x_i)$	$a = 32, b = 4, c = 16,$	-20.8399$\leq$ x $\leq$ 21.2057
$\dot{y}_i$=-x_i.z_i+c.y_i	h=$2^{-8}, x_0 = 1,$	-22.8983$\leq$ y $\leq$23.3546
$\dot{z}_i$= x_i.y_i- b.z_i	$y_0 = 1, z_0 = 1$	0.8931$\leq$ z $\leq$ 34.5366

Table 4 Variables range and Parameter's value for Pehlivan's chaotic system.

Pehlivan Chaotic System		
ODEs Pehlivan and Uyaroğlu (2010)	Parameters	Range
$\dot{x}_i$=$y_i - x_i$	$a = 0.5, h = 2^{-8},$	-2.8411$\leq$ x $\leq$ 2.7743
$\dot{y}_i$=-x_i.z_i+a.y_i	$x_0 = 0.001, y_0 = 0.001,$	-4.7402$\leq$ y $\leq$4.8913
$\dot{z}_i$= x_i.y_i- a	$z_0 = 0$	-2.9902$\leq$ z $\leq$ 6.6909

PROPOSED DIGITAL ARCHITECTURE OF RECONFIGURABLE CHAOTIC PRNG

This section includes the VLSI circuit of reconfigurable chaotic PRNG using Lorenz, Chen, Lu, and Pehlivan 3D attractors. The general architecture has been constructed by the exploitation of similarity between all chaotic attractors which leads to fit into a single structure. The parameters of Lorenz system has been set to $(2^5, 2^2, 2^5, 2^{-8})$ corresponding (a, b, c, h). Moreover, Table 1 depicts the range of variables: $-28.1805 \leq x \leq 29.2467, -31.1805 \leq y \leq 33.1210$ and $0.9215 \leq z \leq 58.6626$. Similarly, Table 2 to Table 4 include the step size, parameters, and variable range of the system of Chen, Lu, and Pehlivan correspondingly. The benefits of this approach, all binary multiplication operations of ODEs and Euler's expressions (except $x_i.y_i$ and $x_i.z_i$) has been carried out by the operation of hardwire shifting rather than binary multiplication. In this modelling, 2's complement and the fixed-point scheme have been used in which 7 MSB represent the amount of integer including sign bit. On the other side, the rest 25 bits represent the fractional value of all parameters and variables. To retain the same fractional bits of 25, the truncation rounding scheme is performed in this operation.

This reconfigurable feature of PRNG is designed by hardwired shifting operations, additions, subtractions, and multiplexing schemes. Fig. 6 represents the VLSI architecture of proposed reconfigurable PRNG using Lorenz, Chen, Lu, and Pehlivan 3D attractors. This architecture offers the opportunity to configure the four different systems and it is controlled by a 2-bit signal which is denoted by *Confg*[1:0]. Pehlivan's chaotic system is configured by *Confg*[1:0]=2′b00, similarly, Lu chaotic system is configured by *Confg*[1:0]=2′b01. Similarly, when *Confg*[1:0] value is 2′b10, the multiplexer switches to the Lorenz system, while the value is 2′b11, architecture computes the Chen system for generating pseudorandom numbers. Three separate 32-bit register block of this figure is designed to evaluate the value of Euler's equations (as given in Eq. (1) to Eq. (3)). The initialization of registers corresponding to three variable is done by Reset signal which controls the 2×1-multiplexer, initially all registers hold the value of X_0, Y_0 and Z_0 correspondingly. The adder used in this block to add the present value of variables (X_i, Y_i, Z_i) with differential value $(h.X, h.Y, h.Z)$ as shown in blocks.

The computational process to evaluate differential value h.X is depicted in Block-1. It is required subtraction to subtract the value of X_i from Y_i. In this block, the logical OR value of *Confg*[1] and *Confg*[0] signal, act as a select line of 2×1-multiplexer. When the value of logic OR operation is '0', the multiplexer gives the differential value (h.X) of Pehlivan's chaotic system, which is the 8-bits hardwired left-shifted of subtracted value. While the value of logic OR operation is '0', the multiplexer gives the 3-bit left shifting of subtracted value as a differential value (h.X) corresponding to Lorenz, Chen, and Lu chaotic system.

The evaluation of h.Y according to the ODE of variable Y (corresponding Lorenz, Chen, Lu, and Pehlival chaotic systems) given in Block-2. In this block, 2-bit *Confg*[1:0] signal, act as a control signal of a 4×1-multiplexer. When the value of *Confg* signal is $2^{'b00}$, multiplexer passes the 9-bit hardwired left shifted value of Y_i according to Pehlivan's chaotic system. The multiplexer passes the 4-bit hardwired left shifted value of Y_i according to Lu, when the value of *Confg* signal is $2^{'b01}$. When the value of *Confg* signal is $2^{'b10}$, multiplexer passes the subtracted value (8-bit hardwired left shifted value of X_i from the 3-bit hardwired left shifted value of Y_i). When the value of *Confg* signal is $2^{'b11}$, multiplexer passes the computational value of $2^{-8}.(8.x_i + 24.y_i))$ according to Chen's chaotic system. One 32-bit binary multiplier is required in this block to multiply the value of Z_i with X_i. To subtract the multiplexer's output with an 8-bit left-shifted multiplier's output, one 32-bit subtractor is used as shown in the figure and their output gives the differential value (h.Y). Here, the shifting operation performs the multiplication operation which is not utilized any hardware resources.

Similarly, Block-3 presents the computational block to evaluate the differential value (h.Z). Here, the logical OR value of *Confg*[1] and *Confg*[0] act as a control signal of the multiplexer. It passes the

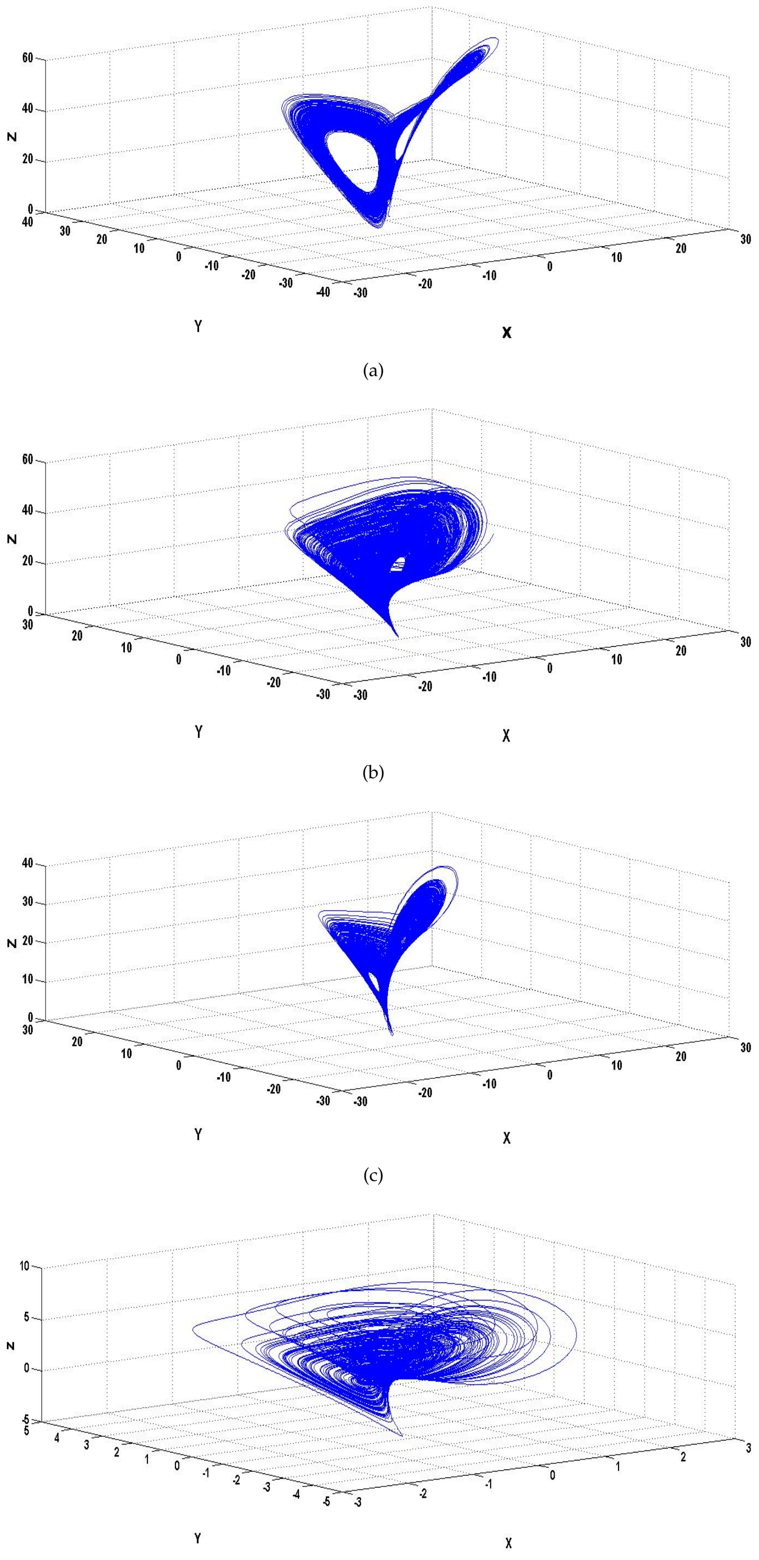
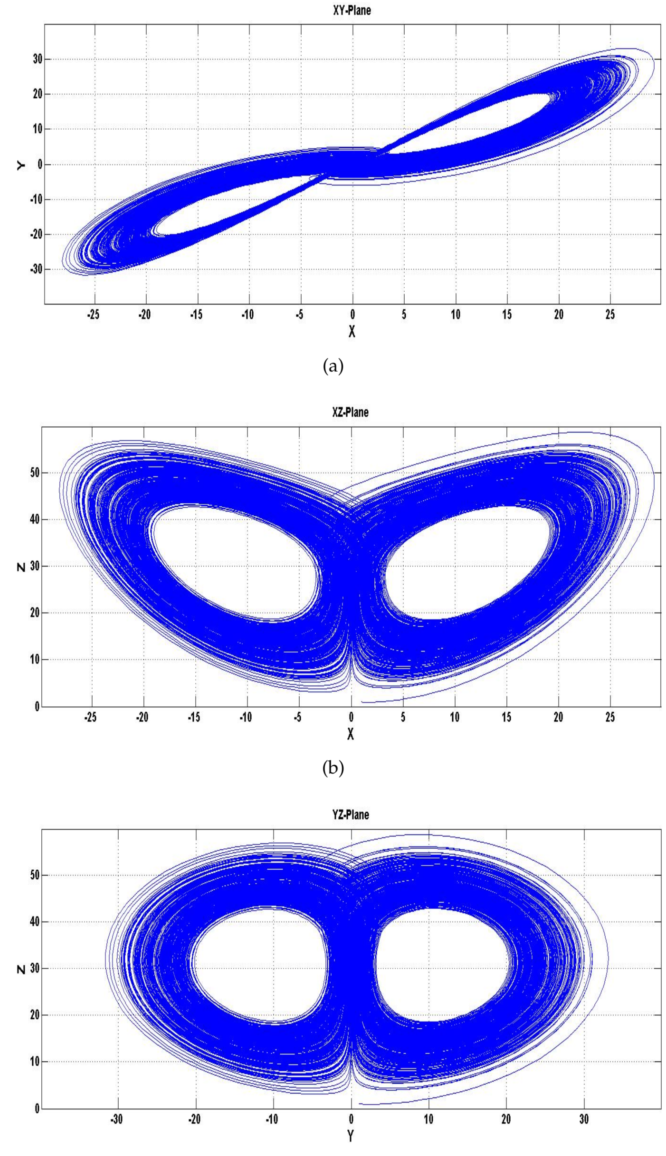


Figure 1 Chaotic attractor in the plane of: (a) Lorenz; (b) Chen; (c) Lu; and (d) Pehlivan systems.

value $2^{(-9)}$, when the control signal is equal to logic '0′. While, for control signal equal to logic "1", multiplexer pass the 6-bits left shifted value of Z_i. This block includes one 32-bit binary multiplier

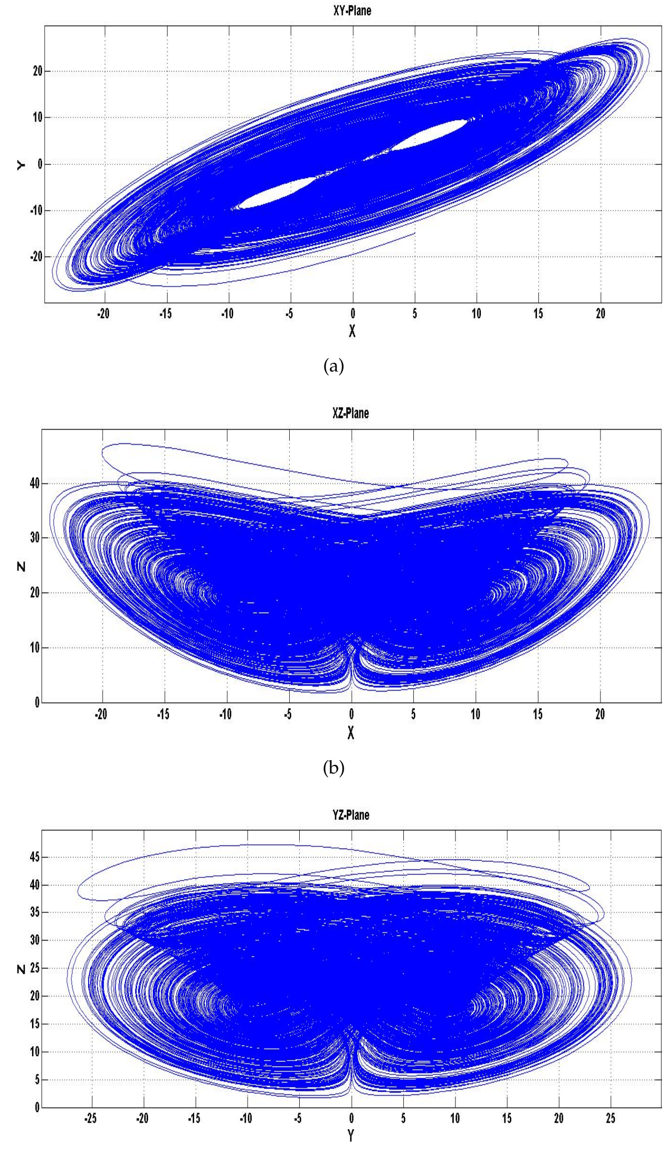


(a)

(b)

(c)

Figure 2 Chaotic attractor in plane of Lorenz system with , $h = 2^{-8}$, $a = 32$, $b = 4$, $c = 32$ and initial condition (x_0, y_0, z_0) = (1, 1, 1): (a) x-y plane; (b) x-z plane; (c) y-z plane.



(a)

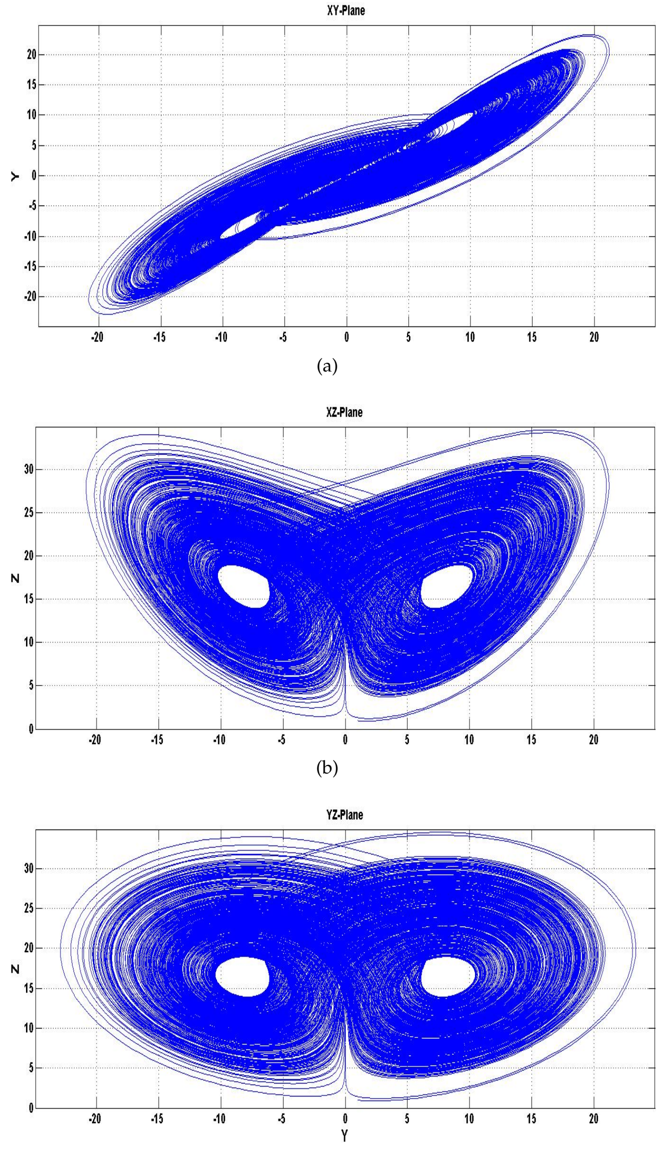
(b)

(c)

Figure 3 Chaotic attractor in plane of Chen's system with , $h = 2^{-8}$, $a = 32$, $b = 4$, $c = 24$ and initial condition (x_0, y_0, z_0) = (5, -15, 40): (a) x-y plane; (b) x-z plane; (c) y-z plane.

that multiplies the 32-bit value of Y_i with X_i. The subtraction circuit is also used in this block that subtracts the multiplexer's output with the 8-bit left-shifted of multiplier's output, which gives the differential value h.Z . The output of this block generates the 24-bit random numbers in each iteration. These 24-bit data is captured from 8 Least Significant Bits (LSBs) from each chaotic variable.

Example of the Proposed reconfigurable PRNG: Let $a = 32$, $b = 4$, $c = 24$, $h = 2^{(-8)}$, X_0=5 (00001010000000000000000000000000), Y_0=-15 (11100010000000000000000000000000), Z_0=40 (01010000000000000000000000000000) and *Confg*=3. When the *Confg* value is 2'b11, architecture computes the Chen system for generating pseudorandom numbers. Block-1 generates the differential value: $h.(X_0)$ =11111111011000000000000000000000, Block-2 generates the differential value: $h.(Y_0)$ =11111111110101111111110011100000, and Block-3 generates the differential value: $h.(Z_0)$=11111111111110101111111011010100. The value of X_1=00001001011000000000000000000000, Y_1=11100001110101111111110011100000, and Z_1=01001111111110101111111011010100 have been generated from three Euler's blocks separately. Finally, captured the 8 Least Significant Bits (LSBs) of each chaotic variable: X_1=00000000, Y_1=11100000 and Z_1=11010100, this architecture generates a 24-bits pseudo-random number in 1st iteration: OUT_1=000000001110000011010100. Similarly, OUT_2=000000001100000010101000, OUT_3= 111100111100111011011110 and so on, generate in the next iterations.

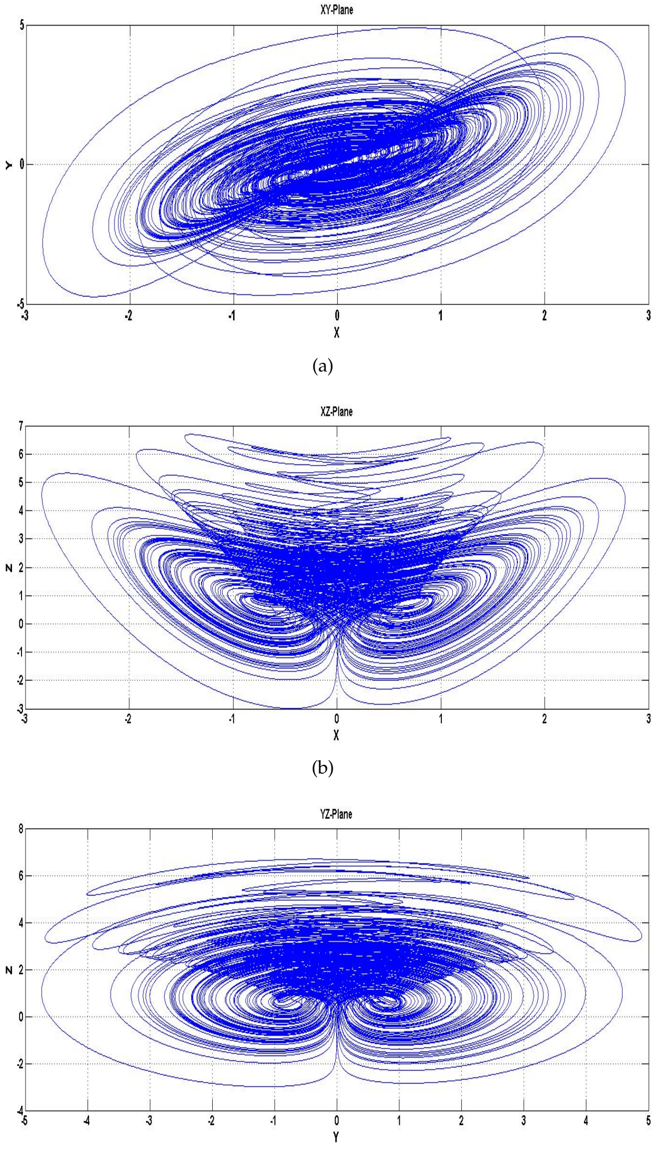


(a)

(b)

(c)

Figure 4 The chaotic attractor in the plane of Lu system with, $h = 2^{-8}$, $a = 32$, $b = 4$, $c = 16$ and initial condition $(x_0, y_0, z_0) =$ (1, 1, 1): (a) x-y plane; (b) x-z plane; (c) y-z plane.



(a)

(b)

(c)

Figure 5 Chaotic attractor of Pehlivan system with $a = 0.5$, initial condition $(x_0, y_0, z_0) = (0.001, 0.001, 0)$ and $h = 2^{-8}$: (a) x-y plane; (b) x-z plane; (c) y-z plane.

IMPLEMENTATION OF 32-BIT PRNG AND STATISTICAL TESTS

The implementation of 32-bit PRNG circuits is done on Virtex-5 FPGA (XC5VLX110T). Its synthesis has been done on the ISE design suite by Xilinx. Initially, its Register Transfer Level (RTL) design is done using Verilog HDL. Table 6 depicts the hardware performance including the parameters: area constraint (in terms of slice look-up-tables (LUTs), occupied slices and slice registers), Digital signal processing (DSP) blocks, timing performance (in terms of critical path delay and maximum operating frequency), and power dissipation per unit frequency. The post-layout simulation waveform of proposed PRNGs are shown in Fig. 7(a), 7(b), 7(c), and 7(d) corresponding to four different configurations i.e. Pehlivan, Lu, Lorenz, and, Chen's PRNG.

The post routing simulation waveform of 32-bit Pehlivan's chaotic system-based PRNG is shown in Fig. 7(a). The control signal *(Confg)* is used to configure the systems, when its value is equal to 00, it configures Pehlivan's chaotic system. This simulation takes the initial value: $(X_0, Y_0, Z_0) = (0.96248769, 1.20541650, 42.13836362)$. The signal "CLK" and "Reset" are the master clock signal and reset signal respectively. Initialization of the registers with X_0,Y_0, and Z_0 is done by "Reset" signal. The three variable X_i[32:0], Y_i[32:0] and Z_i[32:0] represent the iterative values. Its 8-bit LSBs segments combine to generate a 24-bit pseudo-random number, which is given by the variable *OUT[23:0]*.

Similarly, Fig. 7(b), 7(c), and 7(d) show the post routing simulation waveform of 32-bits reconfigurable PRNG for Lu, Lorenz, and Chen 3D attractors with *Confg[1:0]* equal to 2'b01, 2'b10 and 2'b11 correspondingly. This simulation takes the initial value:

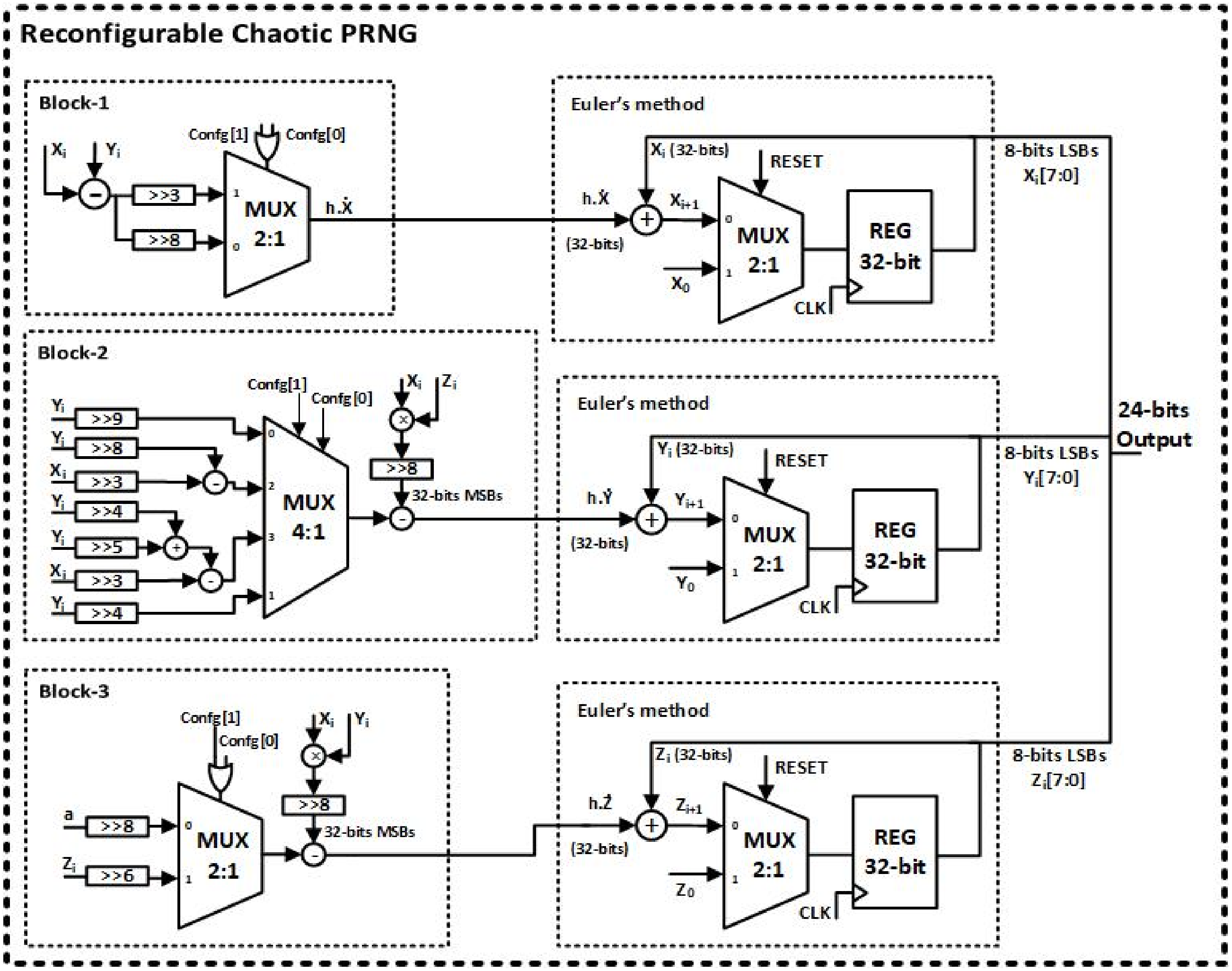


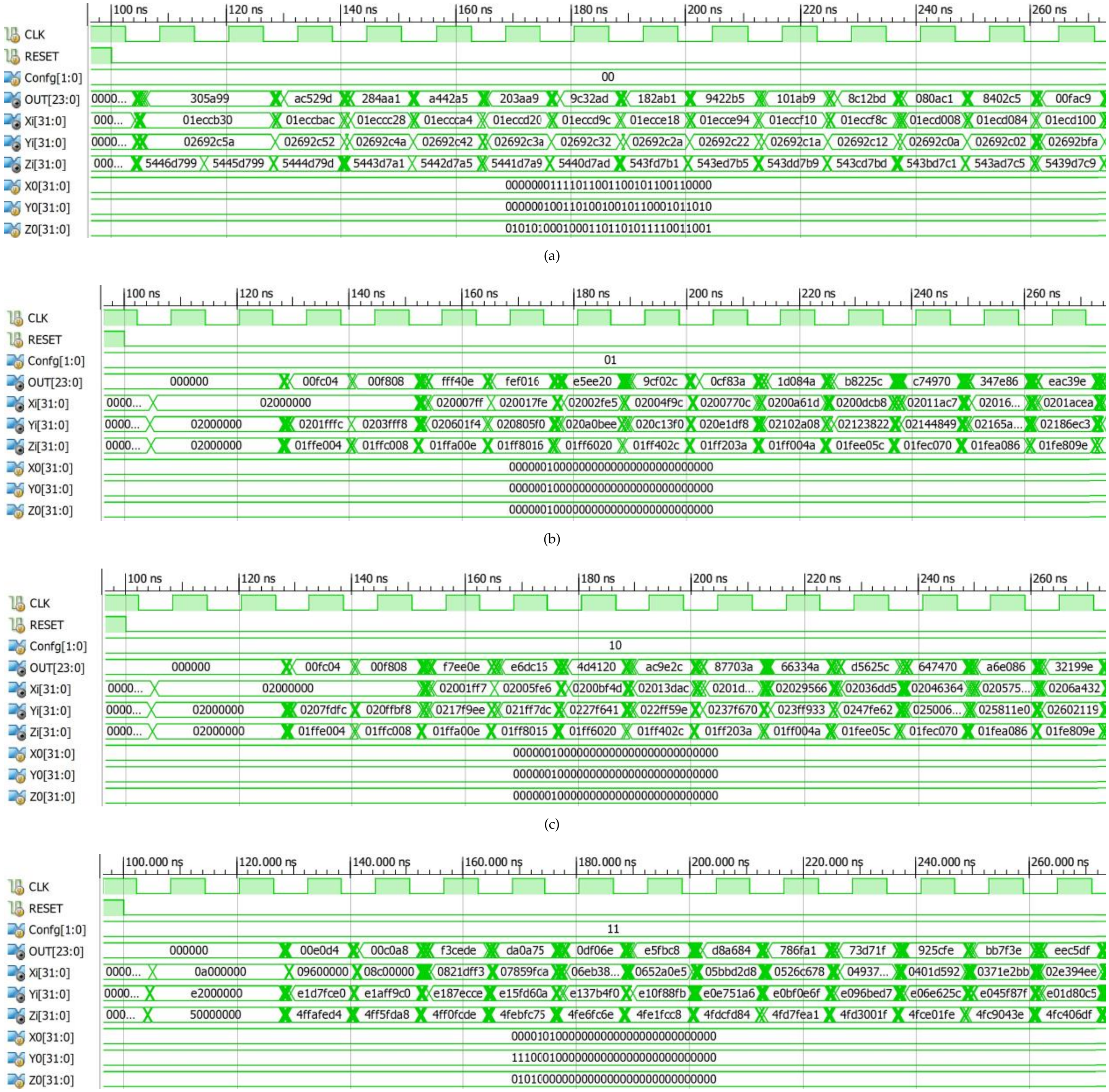
Figure 6 Proposed architecture of reconfigurable chaotic PRNG using Lorenz, Chen, Lu, and Pehlivan chaotic systems.

$(X_0, Y_0, Z_0) = (1,1,1), (1,1,1)$, and $(5, -15, 40)$ respectively. In this figure, the *"CLK"* and *"Reset"* signals represent the same meaning. Similarly, the three variable X_i[32:0], Y_i[32:0], and Z_i[32:0] represent the iterative values. Its 8-bit LSBs segments combine to generate 24-bits pseudo-random numbers, which are given by the variable *OUT[23:0]*.

The proposed reconfigurable PRNG demonstrates over the existing architectures of PRNGs. It provides the opportunity to switch between four different 3D-Chaotic systems. This architecture is a completely digital circuit, which is easily suitable for real-time digital applications where PRNG is required. The comparison table of the hardware performance and security strength is given in Table 6. This table summarizes the NIST results, timing performance, power consumption, and area resources.

The maximum operating frequency of proposed PRNG is increased by 23.40% as compared with PRNG (Rezk *et al.* 2019), while it increases by 3.69% as compared with PRNG based on logistics (Pande and Zambreno 2013). A resources of FPGA (in terms of occupied slices, slice registers, slice LUTs, and DSP blocks) is utilized by designed PRNG circuit is slight increases (as compared with existing literature) due to the involvement of four different chaotic systems in a single architecture. However, it is suitable for generating a high degree of randomness and large period pseudorandom numbers. The proposed architecture consumes 8.6125 mW/MHz total power on Virtex-5 for a 32-bit design. The statistical analysis of generated keys has been done by the NIST test suit. This result also depicts that the security strength of keys from four different configurations is highly secure and it can be used in S-box generation, image encryption, etc.

The statistical testing of a random number generator is federal information, which processes the standard issued by the NIST (Rukhin *et al.* 2000). This test includes the fifteen different statistical tests that perform to check the security strength of generated random sequences in all aspects of security. For this test, we take 100 samples of bit sequences (each sample has a 10^6 random bits sequence). The NIST benchmark test of these four sequences has been performed. This test suite set the level of significance equal to 0.01. This means that the resulting p-value of each sample should be greater than or equal to the level of significance for indicating the randomness strength of generated bit sequences. The sequences have been generated using parameters and initial seed values as mentioned in Table 1 to Table 4. The four different generated sequences from the proposed reconfigurable PRNG have been passed all the tests. Table 5 present the proportional value and maximum p-value corresponding to each test of NIST. This table depicts that test sequences pass all fifteen test of NIST, which indicate the high security strength of generated random sequences from the proposed PRNG circuit.



(a)

(b)

(c)

(d)

Figure 7 Post routing simulation waveform of proposed 32-bit reconfigurable chaotic PRNG: (a) Pehlivan; (b) LU; (c) Lorenz and (d) Chen system.

Table 5 FPGA synthesis result of proposed and existing architecture of Chaotic-based PRNG

	Proposed	(Zidan et al., 2011)	(de la Fraga et al., 2017)	(Rezk et al., 2019)	(Pande & Zambreno, 2013)
Chaotic System	**(Lorenz + Chen + Lu + Pehlivan)**	**Lorenz & Bernoulli**	**(Lu + Lorenz)**	**Logistic**	
Operand Size	32-bits	32-bits	32-bits	32-bits	32-bits
Number of 3D chaotic attractors	4	1	1	2	1
FPGA	Virtex 5 (XC5VLX50T)	Virtex 4 (XC4VSX35)	Spartan 3E (XC3S500E)	Virtex 5 (XC5VLX50T)	Virtex 6 (XC6VLX75T)
Occupied Slices/Total	83/7200	145/15360	342/7200	100/7200	181/11640
Slice registers/Total	96/28800	96 /30,720	108/28,800	96 /28800	160/93120
Slice LUTs/Total	313/28800	287 /30,720	575/28,800	276/28800	643/46560
DSP blocks/Total	8/48	8/192	9/48		16/288
Frequency (MHz)	96.438	53.53	36.90		93.00
NIST	Pass	–	–		–

Table 6 NIST Test Results

Test	Lorenz (10)		Chen (11)		Lu (01)		Pehlivan (00)	
	P-value within success sequence	Proportion successful out of 100	P-value within success sequence	Proportion successful out of 100	P-value within success sequence	Proportion successful out of 100	P-value within success sequence	Proportion successful out of 100
Frequency Test within a Block	0.961876	98	0.905225	99	0.998261	96	0.802587	99
Frequency (Monobit)	0.719747	99	0.657933	100	0.888660	96	0.841481	98
Runs Test	0.955825	99	0.474986	100	0.639464	98	0.996907	99
Longest-Run-of-Ones in a Block	0.844731	99	0.719747	97	0.951366	99	0.942871	96
Linear Complexity	0.657933	98	0.699313	98	0.798139	97	0.933026	98
Binary Matrix Rank	0.862457	99	0.949536	99	0.949536	98	0.862457	97
Approximate Entropy	0.534146	98	0.574903	99	0.153763	98	0.999952	100
Discrete Fourier Transform	0.657933	99	0.926884	96	0.771671	97	0.646355	99
Overlapping Template Matching	0.822183	100	0.883171	100	0.856837	100	0.924076	97
Non-overlapping Template Matching	0.971699	98	0.851383	97	0.779188	99	0.798139	97
Cumulative Sums	0.554420	100	0.867692	100	0.762693	96	0.990843	98
Universal Statistical Test	0.498264	98	0.697354	100	0.802673	96	0.864253	100
Serial Test	0.042808	100	0.304126	100	0.759756	99	0.989703	98
	0.474986	99	0.946308	99	0.262249	99	0.653842	99
Random Excursions	0.867523	98	0.643582	99	0.943559	96	0.983256	100
Random Excursions Variant	0.578556	96	0.732568	99	0.969182	99	0.827614	96

DESIGN AND EVALUATION OF S-BOXES

This section designs the four different new S-box matrixes using the proposed reconfigurable PRNG. The steps for designing S-boxes from PRNG are illustrated: The first step is to segment the 24-bit random numbers into three parts and each 8-bit binary value is converted into decimal form. This decimal value compares with the existing value of the matrix in Step two and it includes the element of the matrix if the value is not repeated. This process is repeated until the entire matrix element is filled. And finally generates the S-boxes, which contain the 256 different 8-bit elements in random order. Tables 6, 7, 8 and 9 present the S-box matrix corresponding to *Confg* equal to 2′b00, 2′b 01, 2′b 10, and 2′b 11.

Since the critical part of cryptography is S-boxes thus, important characteristics of a cryptographically strong S-box have been examined in this section. The evaluated characteristics exhibit features like Average non-linearity of all Boolean functions, non-linearity of Boolean functions, Balanced, Bijective, Non-linearity of S-Box, BIC non-linearity criterion, Strict Avalanche Criterion (SAC), and Dynamic Distance. Moreover, Outcomes have been compared with other techniques reported in the literature. The reference of the all-mathematical definitions of the above-mentioned parameters is (Cassal-Quiroga and Campos-Cantón 2020; Ishfaq 2018; Gupta and Chauhan 2021).

It is well known that the criterion of bijective property of S-boxes is equivalent to $2^{n-1} = 128$ where $n = 8$. Since it satisfies the bijective criterion for all proposed S-boxes thus it is considered as desired value for the bijective criterion. Simultaneously, the balanced, one-to-one and surjective properties are also satisfied for the proposed S-boxes.

The non-Linearity criterion is another parameter that holds the nonlinearity property between the vector of input and output of S-boxes. It holds a better explanation for the dissimilarity degree between Boolean and linear functions (Cassal-Quiroga & Campos-Cantón, 2020). The calculation of eight Boolean functions of non-linearity property has been performed for the S-boxes. The calculated value of eight non linearity function of non-linearity property for the S-box-1 are 104, 106, 104, 102, 100, 102, 108 and 104, and for the S-box-2 are 104, 104, 104, 106, 106, 102, 104 and 104. In same way the eight non linearity Boolean values for S-box-3 and S-Box-4 are (102, 104, 106, 104, 110, 106, 106, 102) and (102, 104, 106, 104, 110, 106, 106 and 102) respectively. It is well-identified that larger non-linear values ensure the highest ability to resist

Table 7 S-Box-1 using proposed chaotic PRNG with *Confg* equal to 00.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	89	112	123	134	4	146	179	152	169	224	44	192	13	215	58	65
2	232	121	88	21	15	111	66	165	59	157	156	210	180	87	30	119
3	240	53	164	137	76	209	34	99	254	187	122	43	84	217	55	251
4	6	18	52	109	41	98	8	64	144	190	193	216	36	239	238	194
5	28	96	29	74	195	158	100	181	5	204	168	167	227	214	73	250
6	235	22	186	94	2	166	211	32	199	110	49	113	160	171	97	207
7	253	145	45	39	57	86	155	81	133	71	105	243	129	159	153	12
8	106	31	200	206	161	241	175	79	19	126	197	173	202	188	42	90
9	138	218	125	10	162	154	234	26	27	212	141	170	70	3	0	247
10	182	117	147	196	140	78	108	16	148	255	69	77	118	17	213	9
11	93	131	68	231	11	25	75	101	233	47	103	249	128	127	142	178
12	177	102	51	229	205	23	230	120	24	237	191	50	85	1	136	33
13	80	150	221	67	132	37	62	248	245	223	225	95	198	48	244	219
14	201	130	116	220	246	222	72	115	151	61	54	40	236	35	242	14
15	252	228	92	46	83	60	163	82	139	63	203	189	107	104	114	174
16	38	20	185	143	208	135	7	176	183	124	172	184	149	91	226	56

Table 8 S-Box-2 using proposed chaotic PRNG with *Confg* equal to 01

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	229	238	32	156	240	44	12	248	58	29	8	74	184	34	92	199
2	211	201	103	52	76	235	151	202	252	56	33	99	140	216	204	196
3	41	39	217	23	90	145	210	97	75	87	62	7	161	244	220	153
4	223	116	236	254	162	251	59	233	6	31	182	86	30	158	85	122
5	113	123	207	147	70	187	175	27	28	141	212	25	142	143	146	243
6	178	71	128	114	173	81	253	55	169	197	73	127	10	93	215	181
7	171	2	5	18	189	249	230	206	84	195	200	37	82	4	109	150
8	225	36	14	72	17	69	110	131	239	208	194	247	125	163	13	26
9	186	226	219	106	38	214	57	213	117	152	191	133	64	50	0	9
10	137	126	168	107	45	172	179	190	205	118	192	79	95	120	155	83
11	177	22	136	167	231	174	180	157	119	121	42	88	105	100	124	224
12	68	63	222	134	98	166	20	53	96	246	149	242	66	43	154	237
13	159	48	89	255	160	1	67	40	232	21	241	15	144	3	250	170
14	148	193	94	60	218	78	61	102	185	221	111	129	130	11	108	203
15	228	135	164	47	234	176	46	112	188	139	198	183	65	51	80	209
16	104	245	77	54	24	132	35	138	115	49	101	227	165	91	19	16

Table 9 S-Box-3 using proposed chaotic PRNG with *Confg* equal to 10

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	247	238	14	230	220	22	77	65	32	172	158	44	135	112	58	102
2	81	177	12	119	19	99	210	92	179	221	233	107	69	30	9	17
3	20	199	222	229	54	235	73	126	13	248	209	129	98	138	190	36
4	48	181	228	226	16	156	18	237	197	78	187	110	123	27	203	43
5	127	184	80	55	219	87	70	183	120	174	46	71	171	60	23	131
6	96	200	25	45	62	168	109	133	84	94	31	164	143	33	21	213
7	47	7	49	215	163	37	117	147	83	29	79	41	169	212	40	191
8	53	8	93	34	68	195	104	3	236	188	4	194	241	245	125	162
9	5	89	185	225	88	227	218	128	42	250	202	207	189	66	132	63
10	118	51	75	141	160	111	243	137	204	86	155	205	206	232	176	82
11	139	255	186	167	6	246	165	136	39	103	114	211	214	244	192	208
12	28	239	253	0	61	242	100	251	57	101	157	161	152	148	52	216
13	145	249	170	154	113	142	178	124	90	105	151	15	224	56	182	72
14	64	134	140	97	91	35	159	231	198	146	150	2	234	193	153	252
15	175	130	115	122	201	74	50	173	254	223	121	95	1	38	217	166
16	24	149	76	26	116	240	67	85	10	180	196	144	11	59	108	106

Table 10 S-Box-4 using proposed chaotic PRNG with *Confg* equal to 11

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	243	206	222	218	10	117	13	240	110	229	251	200	216	166	132	120
2	85	101	18	194	68	209	143	50	138	188	32	221	73	53	106	82
3	123	30	213	89	214	184	15	69	104	25	159	56	8	40	178	145
4	142	205	37	226	108	136	203	233	34	163	135	174	212	20	118	137
5	27	168	156	207	246	1	141	211	95	189	71	91	193	154	116	177
6	190	124	97	128	172	61	3	19	234	139	35	245	247	153	114	63
7	228	78	122	75	70	76	38	94	33	115	62	45	152	16	80	66
8	165	160	7	161	90	83	175	67	130	148	86	219	220	167	225	144
9	28	198	249	239	158	237	98	88	49	87	113	65	147	2	252	131
10	9	253	197	238	12	201	11	140	192	185	111	248	173	39	187	41
11	241	105	224	22	250	126	103	217	74	164	44	29	36	0	150	60
12	54	223	119	210	244	121	176	64	215	169	208	59	133	17	43	46
13	93	57	236	171	195	199	191	196	14	72	180	24	52	146	254	235
14	42	232	21	227	47	99	96	181	26	186	77	129	179	92	157	109
15	125	48	230	242	55	84	204	5	102	134	81	162	183	255	127	202
16	31	149	100	79	4	58	182	23	112	6	51	151	155	231	170	107

powerful attacks.

The randomness of the S-box is measured by Strict Avalanche Criterion (SAC). If there is an input change then random behavior comes into the picture which is regarded as the avalanche effect in S-box. There is an alteration in each output bit with one-half of the probability if any change is made in the single bit of input. This phenomenon reflects the Strict Avalanche Criterion (SAC). It is well known that there is a 50% dependency of Boolean function on each input bit for a better explanation of this criterion. The generated SAC values of S-box-1, -2, -3 and -4 are tabulated in Table [16, 17,18] respectively. The corresponding minimum, maximum, and average SAC values of 0.3606, 0.5938, and 0.500016 for S-box-1 have been obtained. In the same way, the corresponding minimum, maximum, and average SAC values of 0.3906, 0.6406, and 0.504894 for S-box-2 have been evaluated and for S-box-3 the minimum, maximum and average values are 0.3906, 0.5781, and 0.503669. At last, the minimum, maximum, and average values for S-box-4 are 0.4063, 0.6094, and 0.5005 respectively. Its average value corresponding to S-boxes is very closer to 0.5. Thus, the property of SAC for proposed S-Boxes is satisfied.

To evaluates the security strength of S-Box, Bits Independence Criterion (BIC) is also important. For the S-boxes, the static pattern among output vectors and no dependency on each other is ensured by the BIC parameters. The corresponding BIC non-linearity for the S-box-1, -2, -3, and -4 has been tabulated in Table [19, 20, 21, 22]. Further, the BIC non-linearity value of 102.5714, 103.1429, 102.8571, and 103.2143 also has been calculated for the S-box-1, -2, -3, and -4 respectively. The SAC properties are also measured by the dynamic distance (DD) (Ishfaq 2018) and it is satisfied only when there is a small integral value for dynamic distance. The DD for S-Box-1, -2, -3, and -4 have been tabulated in Table [11, 12, 14, 15]. The calculated average values of DD for S-box-1, -2, -3 and -4 are 5.3125, 5.125, 4.34375 and 4.625 respectively which holds a better inclination for the fulfill the BIC criterion.

Table 10 illustrates the comparison of proposed S-boxes in terms of the property of Bijection, Nonlinearity, SAC, and BIC Non-Linearity with the existing literature. This table helps to conclude the important criterion such as Bijective, Balanced, Non-linearity, and Avalanche Criteria. It has been satisfied by these boxes. Further, the average value of non-linearity of S-box-1, -2, -3, and -4 are 103.75, 104.25, 104.00, and 105.00 correspondingly, which indicates the value of proposed S-boxes is much better than that reported in the literature (Cassal-Quiroga & Campos-Cantón, 2020). It has been observed that the expected bijection value of 128 has been fulfilled by the S-Boxes. Moreover, S-Box-1, -2, -3, and -4 have mean SAC value of 0.500016, 0.504894, 0.503669 and 0.5005 respectively that is much closer to 0.5. The BIC-nonlinearity average values are 102.5714, 103.1429, 102.8571, and 103.2143 for S-box-1, -2, -3, and -4 which reveal the betterment of S-boxes.

Table 11 Dynamic Distance (DD) of S-box-1

2	12	2	2	6	8	4	2
6	8	2	6	12	2	6	10
6	6	4	6	0	10	6	2
6	4	10	0	6	4	12	0
8	10	8	6	14	2	10	2
4	10	2	2	2	12	4	4
2	2	2	10	4	2	2	0
4	8	0	10	4	8	4	6

Table 12 Dynamic Distance Table of S-box-2

4	4	4	0	0	2	2	6
2	2	2	6	2	6	10	6
0	6	0	8	2	4	18	8
2	6	4	8	12	0	6	6
4	2	2	14	10	10	8	2
4	4	10	4	14	2	0	0
12	2	8	6	6	8	4	2
6	2	6	6	6	10	2	4

Table 13 Dynamic Distance Table of S-box-2

4	4	4	0	0	2	2	6
2	2	2	6	2	6	10	6
0	6	0	8	2	4	18	8
2	6	4	8	12	0	6	6
4	2	2	14	10	10	8	2
4	4	10	4	14	2	0	0
12	2	8	6	6	8	4	2
6	2	6	6	6	10	2	4

Table 14 Dynamic Distance Table of S-box-3

2	4	2	2	2	10	0	12
2	6	4	8	2	8	6	8
4	2	6	4	2	6	2	6
12	2	0	2	6	0	2	0
14	4	10	4	0	2	6	10
4	4	4	0	6	4	2	10
0	0	0	2	12	4	2	2
2	0	8	6	4	2	10	6

Table 15 Dynamic Distance Table of S-box-4

0	2	8	2	10	2	4	4
6	12	2	2	4	8	6	16
6	0	4	0	2	8	14	4
2	6	2	10	0	6	4	2
8	10	0	4	6	8	2	8
2	8	10	2	4	2	0	0
10	8	4	2	0	8	4	4
10	2	2	2	2	2	4	0

Table 16 SAC criterion result of the generated S-box-1

0.4844	0.5938	0.4844	0.4844	0.5469	0.5625	0.5313	0.4844
0.5469	0.4375	0.5156	0.4531	0.4063	0.5156	0.5469	0.4219
0.5469	0.5469	0.5313	0.5469	0.5	0.5781	0.5469	0.4844
0.5469	0.4688	0.4219	0.5	0.5469	0.5313	0.4063	0.5
0.5625	0.4219	0.5625	0.5469	0.3906	0.5156	0.5781	0.5156
0.4688	0.5781	0.4844	0.4844	0.5156	0.4063	0.4688	0.5313
0.5156	0.4844	0.5156	0.4219	0.4688	0.5156	0.4844	0.5
0.4688	0.5625	0.5	0.4219	0.4688	0.4375	0.5313	0.4531

Table 17 SAC criterion result of the generated S-box-3

0.5156	0.5313	0.4844	0.5156	0.5156	0.5781	0.5	0.4063
0.5156	0.5469	0.5313	0.5625	0.4844	0.5625	0.4531	0.4375
0.4688	0.5156	0.5469	0.4688	0.4844	0.4531	0.5156	0.5469
0.4063	0.5156	0.5	0.5156	0.4531	0.5	0.4844	0.5
0.3906	0.4688	0.5781	0.5313	0.5	0.5156	0.5469	0.5781
0.4688	0.5313	0.5313	0.5	0.4531	0.5313	0.5156	0.4219
0.5	0.5	0.5	0.5156	0.5938	0.5313	0.4844	0.5156
0.5156	0.5	0.5625	0.4531	0.4688	0.4844	0.5781	0.4531

Table 18 SAC criterion result of the generated S-box-4

0.5	0.5156	0.5625	0.4844	0.4219	0.5156	0.4688	0.4688
0.4531	0.4063	0.5156	0.4844	0.4688	0.5625	0.5469	0.625
0.5469	0.5	0.5313	0.5	0.4844	0.4375	0.6094	0.5313
0.5156	0.5469	0.4844	0.5781	0.5	0.5469	0.4688	0.5156
0.5625	0.4219	0.5	0.5313	0.4531	0.5625	0.4844	0.4375
0.4844	0.4375	0.5781	0.5156	0.5313	0.4844	0.5	0.5
0.4219	0.4375	0.5313	0.4844	0.5	0.4375	0.4688	0.5313
0.4219	0.5156	0.5156	0.5156	0.4844	0.5156	0.4688	0.5

Table 19 BIC Non-linearity criterion of S-box-1

0	98	100	104	102	106	108	106
98	0	100	102	104	98	100	104
100	100	0	102	104	96	100	98
104	102	102	0	106	102	106	100
102	104	104	106	0	104	104	108
106	98	96	102	104	0	102	106
108	100	100	106	104	102	0	102
106	104	98	100	108	106	102	0

Table 20 BIC Non-linearity criterion of S-box-2

0	104	104	104	102	100	102	106
104	0	104	104	98	106	102	104
104	104	0	102	106	104	104	106
104	104	102	0	100	102	108	104
102	98	106	100	0	102	98	104
100	106	104	102	102	0	100	102
102	102	104	108	98	100	0	106
106	104	106	104	104	102	106	0

Table 21 BIC Non-linearity criterion of S-box-3

0	106	100	102	106	104	102	102
106	0	100	102	106	106	100	104
100	100	0	106	100	104	96	106
102	102	106	0	98	102	104	104
106	106	100	98	0	106	104	102
104	106	104	102	106	0	98	106
102	100	96	104	104	98	0	104
102	104	106	104	102	106	104	0

Table 22 BIC Non-linearity criterion of S-box-4

0	106	100	106	104	100	102	104
106	0	106	104	104	104	100	102
100	106	0	104	106	104	108	98
106	104	104	0	100	104	96	104
104	104	106	100	0	106	102	102
100	104	104	104	106	0	108	102
102	100	108	96	102	108	0	104
104	102	98	104	102	102	104	0

Table 23 Comparison of our S-boxes and other S-boxes used in typical block ciphers.

		Bijection	Nonlinearity			SAC			BIC Non-Linearity
			Min.	Max.	Average	Min.	Max.	Average	
(Cassal-Quiroga & Campos-Cantón, 2020)	S-box-1	128	96	104	101.75	0.3906	0.5781	0.5012	103.42
	S-box-2	128	96	108	102.25	0.4219	0.6094	0.5059	103.50
(Gupta & Chauhan, 2021)	S-box-1	128	98	108	103.7500	0.4063	0.5938	0.507583	103.7857
	S-box-2	128	94	108	100.5000	0.3906	0.6094	0.498792	102.9286
Proposed	S-box-1	128	100	108	103.75	0.3906	0.5938	0.500016	102.5714
	S-box-2	128	102	106	104.25	0.3906	0.6406	0.504894	103.1429
	S-box-3	128	100	106	104.00	0.3906	0.5781	0.503669	102.8571
	S-box-4	128	102	110	105.00	0.4063	0.6094	0.5005	103.2143

CONCLUSION

This paper summarizes the design and evaluation of the new four S-boxes for subbyte operation in image encryption applications and estimates their strength using the following parameters: Dynamic Distance, BIC non-linearity, Bijective, Non-linearity, Strict Avalanche Criterion (SAC), and Balanced criterion. The S-box matrix is designed by a new reconfigurable 3D-Chaotic PRNG. This PRNG is designed using four different 3D chaotic systems i.e. Lorenz, Chen, Lu, and Pehlivan's chaotic systems. This reconfigurable architecture of PRNG exploits the ODEs of these four attractors that fit all four chaotic systems in a single circuit. The novelty of this PRNG is multiplierless VLSI architecture. That offers relatively better performance. To demonstrate the hardware performance, the PRNG circuit is implemented in Virtex-5 (XC5VLX50T) FPGA and finds the timing performance which generates the 24-bit random number at 96.438-MHz. The area of FPGA is occupied by only 16.66%, 1.08%, 0.33%, and 1.15% of the available DSP blocks, slice LUTs, slice registers and slices respectively. Finally, the proposed four different S-box matrixes fulfill the following criteria: Dynamic Distance, BIC non-linearity, Bijective, Non-linearity, Strict Avalanche Criterion (SAC), and Balanced criterion. Therefore, it can conclude that the proposed S-boxes are used for secure image encryption algorithms.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Ahmad, M. and E. A. Alsolami, 2020 Evolving dynamic s-boxes using fractional-order hopfield neural network based scheme. Entropy **22**.

Akgul, A., C. Arslan, and B. Arıcıoğlu, 2019 Design of an interface for random number generators based on integer and fractional order chaotic systems. volume 1, pp. 1–18.

Alawida, M., A. Samsudin, and J. S. Teh, 2020 Enhanced digital chaotic maps based on bit reversal with applications in random bit generators. Inf. Sci. **512**: 1155–1169.

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.

Alhadawi, H. S., D. Lambić, M. F. B. Zolkipli, and M. Ahmad, 2020 Globalized firefly algorithm and chaos for designing substitution box. J. Inf. Secur. Appl. **55**: 102671.

Artuğer, F., 2023 A new s-box generator algorithm based on 3d chaotic maps and whale optimization algorithm. Wireless Personal Communications **131**: 1–19.

Artuğer, F. and F. Özkaynak, 2022a A method for generation of substitution box based on random selection. Egyptian Informatics Journal **23**: 127–135.

Artuğer, F. and F. Özkaynak, 2022b Sbox-cga: substitution box generator based on chaos and genetic algorithm. Neural Computing and Applications **34**: 1–9.

Cassal-Quiroga, B. B. and E. Campos-Cantón, 2020 Generation of dynamical s-boxes for block ciphers via extended logistic map. Mathematical Problems in Engineering **2020**: 1–12.

ElSafty, A. H., M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, 2021 Analog integrated circuits and signal processing. Hardware realization of a secure and enhanced s-box based speech encryption engine **106**: 385–397.

G. Di Patrizio Stanchieri, E. P., A. De Marcellis and M. Faccio, 2019 A true random number generator architecture based on a reduced number of fpga primitives. AEU - Inte. J. Electron. Commun. **105**.

Garcia-Bosque, M., A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, 2019 Chaos-based bitwise dynamical pseudorandom number generator on fpga. IEEE Transactions on Instrumentation and Measurement **68**: 291–293.

Garcia-Bosque, M., A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, 2018 A new technique for improving the security of chaos based cryptosystems. In *2018 IEEE International*

Symposium on Circuits and Systems (ISCAS), pp. 1–5.

Garipcan, A. M. and E. Erdem, 2020 A trng using chaotic entropy pool as a post-processing technique: analysis, design and fpga implementation. Analog Integr. Circuits Signal Process. **103**: 391–410.

Gupta, M. and R. Chauhan, 2020 Efficient hardware implementation of pseudo-random bit generator using dual-clcg method. Journal of Circuits, Systems and Computers **30**.

Gupta, M. D. and R. K. Chauhan, 2021 Secure image encryption scheme using 4d-hyperchaotic systems based reconfigurable pseudo-random number generator and s-box. Integr. **81**: 137–159.

Gupta, M. D. and R. K. Chauhan, 2022 "hardware efficient pseudo-random number generator using chen chaotic system on fpga. J. Circuits, Syst. Comput. **31**: 2250043.

H. S. Alhadawi, S. M. I., M. F. Zolkipli and D. Lambi, 2019 Designing a pseudorandom bit generator based on lfsrs and a discrete chaotic map. Cryptologia **43**: 190–210.

Ishfaq, F., 2018 *A MATLAB Tool for the Analysis of Cryptographic Properties of S-boxes*. MATLAB Tool for the Analysis of Cryptographic Properties of S-boxes.

Khan, H., M. M. Hazzazi, S. S. Jamal, I. Hussain, and M. Khan, 2022 New color image encryption technique based on three-dimensional logistic map and grey wolf optimization based generated substitution boxes. Multimedia Tools and Applications **82**: 1–22.

Khan, M., T. Shah, and S. I. Batool, 2016 Construction of s-box based on chaotic boolean functions and its application in image encryption. Neural Computing and Applications **27**: 677–685.

Lambić, D. and M. Nikolic, 2019 New pseudo-random number generator based on improved discrete-space chaotic map. Filomat **33**: pp. 2257–2268.

Li, Q. and X. S. Yang, 2010 simple method for finding topological horseshoes. A simple method for finding topological horseshoes **20**: 467–478.

Li, S., X. Mou, and C. Yuanlong, 2001 Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In *International Conference on Cryptology in India*.

Lorenz, E. N., 1963 Deterministic nonperiodic flow. Journal of the Atmospheric Sciences **20**: 130–141.

Lu, J. and G. Chen, 2002 A new chaotic attractor coined. Int. J. Bifurc. Chaos **12**: 659–661.

L'Ecuyer, P., 2012 Random number generation. in Handbook of Computational Statistics .

Pande, A. and J. Zambreno, 2013 A chaotic encryption scheme for real-time embedded systems: design and implementation. Telecommunication Systems **52**: 551–561.

Pehlivan, I. and Y. Uyaroğlu, 2010 A new chaotic attractor from general lorenz system family and its electronic experimental implementation. Turkish Journal of Electrical Engineering and Computer Sciences **18**: 171–184.

Pehlivan, I. and Y. Uyaroğlu, 2012 A new 3d chaotic system with golden proportion equilibria: Analysis and electronic circuit realization. Comput. Electr. Eng **38**: 285–317.

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 .

Rezk, A. A., A. H. Madian, A. G. Radwan, and A. M. Soliman, 2020 Multiplierless chaotic pseudo random number generators. Aeu-international Journal of Electronics and Communications **113**: 152947.

Rukhin, A. L., J. Soto, J. Nechvatal, M. E. Smid, and E. B. Barker, 2000 A statistical test suite for random and pseudorandom number generators for cryptographic applications. volume 2, pp. 1–8.

T. Zhou, G. C. and S. Čelikovský, 2005 Lnikov chaos in the generalized lorenz canonical form of dynamical systems,. Nonlinear Dyn. **39**: 319–334.

Tang, G., X. Liao, and Y. Chen, 2005 A novel method for designing s-boxes based on chaotic maps. Chaos Solitons & Fractals **23**: 413–419.

Wang, X., Ü. Çavusoglu, S. Kaçar, A. Akgul, V.-T. Pham, *et al.*, 2019 S-box based image encryption application using a chaotic system without equilibrium. Applied Sciences **9**: 4.

Wang, Y., Z. Liu, J. Ma, and a. H. He, 2016 pseudorandom number generator based on piecewise logistic map. Nonlinear Dyn. **83**: 2373–2391.

Wang, Y., K. wo Wong, X. Liao, and T. Xiang, 2009 A block cipher with dynamic s-boxes based on tent map. Communications in Nonlinear Science and Numerical Simulation **14**: 3089–3099.

Wolf, A., J. B. Swift, H. L. Swinney, and J. A. Vastano, 1985 A new 3d chaotic system with golden proportion equilibria: Analysis and electronic circuit realization. Phys. D Nonlinear Phenom. **16**: 285–317.

X. Y. Wang, R. L., L. Yang and A. Kadir, 2010 A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**: 615–621.

Xu, W., J. Feng, and H. Rong, 2009 Melnikov's method for a general nonlinear vibro-impact oscillator. Nonlinear Anal. Theory, Methods Appl. **71**: 418–426.

Zahid, A. H., A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, *et al.*, 2021 A novel construction of dynamic s-box with high nonlinearity using heuristic evolution. IEEE Access **9**: 67797–67812.

Zamli, K. Z., F. Din, H. S. Alhadawi, S. Khalid, H. Alsolai, *et al.*, 2023 Exploiting an elitist barnacles mating optimizer implementation for substitution box optimization. ICT Express **9**: 619–627.

Zhao, Y., C. Gao, J. Liu, and S. Dong, 2019 A self-perturbed pseudo-random sequence generator based on hyperchaos. volume 4, p. 100023.

Zidan, M. A., A. G. Radwan, and K. N. Salama, 2011 The effect of numerical techniques on differential equation based chaotic generators. ICM 2011 Proceeding pp. 1–4.

Çavusoglu, Ü., S. Kaçar, I. Pehlivan, and A. Zengin, 2017 Secure image encryption algorithm design using a novel chaos based s-box. Chaos Solitons & Fractals **95**: 92–101.

Ü. Çavuşoğlu, A. A. S. J., S. Panahi and S. Kaçar, 2019 A new chaotic system with hidden attractor and its engineering applications: analog circuit realization and image encryption,.

How to cite this article: Gupta, M. D., Chauhan, R. K., and Upaddhyay, V. K. Analyses of Reconfigurable Chaotic Systems and their Cryptographic S-box Design Applications. *Chaos Theory and Applications*, 5(3), 219-232, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.233-241
https://doi.org/10.51537/chaos.1320492

Chaos and Control of COVID-19 Dynamical System

Vivek Mishra[*,α,1], **Sarit Maitra**[α,2], **Mihir Dash**[α,3], **Saurabh Kumar Agrawal**[§,4] **and Praveen Agarwal**[γ,θ,5]
[*]Alliance School of Applied Mathematics, Alliance University, Bengaluru, 560102, India, [α]Alliance school of Business, Alliance University, Bengaluru, 560102, India, [§]Department of Applied Science, Bharati Vidyapeeth College of Engineering, New Delhi-110063, India, [γ]Department of Mathematics, Anand International College of Engineering, Jaipur 303012, India, [θ]Nonlinear Dynamics Research Center (NDRC), Ajman University, Ajman, UAE.

ABSTRACT Chaos, which is found in many dynamical systems, due to the presence of chaos, systems behave erratically. Due to its erratic behaviour, the chaotic behaviour of the system needs to be controlled. Severe acute respiratory syndrome Coronavirus 2 (Covid-19), which has spread all over the world as a pandemic. Many dynamical systems have been proposed to understand the spreading behaviour of the disease. This paper investigates the chaos in the outbreak of COVID-19 via an epidemic model. Chaos is observed in the proposed SIR model. The controller is designed based on the fractional-order Routh Hurwitz criteria for fractional-order derivatives. The chaotic behaviour of the model is controlled by feedback control techniques, and the stability of the system is discussed.

KEYWORDS
Chaos
Feedback control
Fractional order
Routh Hurwitz criteria
Chaotic attractor
Stability

INTRODUCTION

Mathematical modelling is one of the best ways to understand the dynamics of physical phenomena. Some dynamical systems, whether they are linear or nonlinear, show unpredictable behaviour which is termed "chaos." Chaos is a very active area of research for researchers who are working particularly in the nonlinear dynamical system. Chaos does not have a unified definition, yet this phenomenon is observed and studied in different branches of science and technology, whether it is science, population dynamics, telecommunication engineering, etc.

The COVID-19 epidemic first broke out in December 2019, when its danger and impact were not known. The conditions under which this disease will propagate are also unknown to the world. It is necessary to control the spread of any disease. To control the spread of the disease, we must understand its behaviour particularly the virus's speed of infection and the duration of its symptoms. All the governments and world health organisations are trying to control and prevent the spread of COVID-19. One of the important steps to controlling the spread of COVID-19 is the mathematical modelling of this disease and its analysis. Various techniques have been developed to model infectious diseases. One of the popular methods is the compartmental method. In this method, the entire population is segregated into different compartments, and the interplay between these compartments is represented in the form of equations to represent the model. (Kermack and McKendrick 1927) have proposed for the first time the mathematical model of an epidemic where they have separated the entire population into three compartments: (i) people who are prone to the disease; (ii) people who are already infected and can spread the infection; (iii) people who are already recovered and have developed the immune system; or (iv) people who have left the study area. Many mathematical models (Alsadat *et al.* 2023; Debbouche *et al.* 2021; Giordano *et al.* 2020; Haq *et al.* 2022; Javeed *et al.* 2021; Babu *et al.* 2021; Mandal *et al.* 2020) are proposed for the study of COVID-19. (Xie 2020; Maltezos and Georgakopoulou 2021; Farshi 2020) have used Monte Carlo simulation models to determine the development of COVID spread.

Chaos in the dynamical system of COVID-19 was analysed by (Mangiarotti *et al.* 2020) in 2020, where he worked on the data of the national health commission of the People's Republic of China. In this work, (Mangiarotti *et al.* 2020) have proposed a model based on three variables: (i) the cumulated number of daily confirmed cases; (ii) the daily number of serious cases and those who are under intensive care at present; (iii) the daily cumulated number of deaths. From these parameters, the daily number of new cases, the daily number of additional severe cases, and the daily number of new deaths are derived. The chaos in this model has been observed with 11 parameters. (Debbouche *et al.* 2021)have conceived the dynamical system model proposed by (Mangiarotti *et al.* 2020) of COVID-19 with fractional order differentiation in the

Manuscript received: 28 June 2023,
Revised: 15 October 2023,
Accepted: 27 October 2023.

---

[1] vivmish2010@gmail.com (**Corresponding author**).
[2] sarit.maitra@alliance.edu.in
[3] mihirda@rediffmail.com
[4] saurabh.goel9944@gmail.com
[5] goyal.praveen2011@gmail.com

Caputo sense. The fractional order derivative with commensurate and incommensurate order has been analyzed, and the chaotic behaviour of it has been observed. (Postavaru *et al.* 2021) in 2021 studied the Covid-19 pandemic and chaos.

The fractional order derivative is considered for the consideration of memory concepts in the dynamical system. Although it is quite difficult to formulate a complete model of any novel epidemic, many parameters may still not be known. (Higazy 2020) has used the fractional-order SIDARTHE model and proposed the control strategy. (Ahmad *et al.* 2022) proposed the fractional order model considering five classes of the population. (Borah *et al.* 2022) have investigated the memory effect by introducing the fractional derivative and chaos. They used different methods for controlling the chaos. (Xu and Tang 2021) proposed an integrated epidemic modelling framework for the real time forecast of COVID-19.(Xu *et al.* 2020) proposed a generalised fractional order SEIR model for forecast analysis of the epidemic trends in the USA.(Chandra and Bajpai 2022) have proposed the fractional order model with the consideration of social distancing as one parameter to make the model mimic real-time data.

These proposed COVID-19 models do not address how to control the chaos present in the dynamical system. There are numerous methods to achieve chaos control. Due to their ease of design, the first two primary methods for managing chaos are feedback control and non-feedback control, which are particularly appealing and have been widely used in actual implementation. (Bai and Lonngren 2000) put forth the Active Control Method, which, due to its ease of use and simplicity in applications, has drawn the attention of many researchers working in the field of nonlinear dynamics. (Srivastava *et al.* 2014) have controlled the chaos of the fractional-order Rabinovich-Fabrikant system. (Borah *et al.* 2021) have controlled and anti-controlled fractional order models of diabetes, HIV, dengue, migraine, Parkinson's, and Ebola-virous diseases.

The present article is further divided in the following sections: (i) Section 2 explains the preliminary concepts of fractional differentiations and the stability of fractional order Routh-Hurwitz criterion, it has the basic information about the proposed model (ii). Section 3 contains the stability analysis of the system (iii). Section 4 contains the analysis of the chaos controls, and the parameters required for the control are presented in this section. (iv) Section 5 talks about the results (v). Section 6 is the conclusion. It is to the author's knowledge that no author has tried to control the chaos of a dynamical system of the kind proposed in the current article.

PRELIMINARIES

Definition: The Riemann-Liouville (Podlubnv 1999) type fractional derivative of order $\alpha \geq 0$ of function f(0,∞)$\mapsto$ R. is defined by

$$D^{\alpha} f\left(t\right) = \frac{d^n}{dt^n} \frac{1}{\Gamma\left(n-\alpha\right)} \int_0^t \left(t-\tau\right)^{n-\alpha-1} f\left(\tau\right) d\tau \tag{1}$$

where n=[α]+1 and [α] is the integer part of α.

Definition: The Caputo type (Podlubnv 1999) fractional derivative of order α>0 of the function f (0,∞)→ R is defined by

$$D^{\alpha} f\left(t\right) = \frac{1}{\Gamma\left(n-\alpha\right)} \int_0^t \left(t-\tau\right)^{\alpha-1} f^{(n)}\left(\tau\right) d\tau \tag{2}$$

where n= [α]+1 and [α] is the integer part of α.

Theorem: (Matignon 1996) an autonomous system of type (3)

$$\begin{aligned} D_t^{\alpha} x\left(t\right) &= f_1\left(x,y,z\right) \\ D_t^{\alpha} y\left(t\right) &= f_2\left(x,y,z\right) \\ D_t^{\alpha} z\left(t\right) &= f_3\left(x,y,z\right) \end{aligned} \tag{3}$$

is said to be asymptotically stable by if and only if all its eigenvalues of the Jacobian matrix.

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} & \frac{\partial f_1}{\partial z} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} & \frac{\partial f_2}{\partial z} \\ \frac{\partial f_3}{\partial x} & \frac{\partial f_3}{\partial y} & \frac{\partial f_3}{\partial z} \end{bmatrix} \tag{4}$$

at its equilibrium point meets specific requirements of.$|arg(\lambda)| > \frac{\alpha\pi}{2}$.This result is derived by (Matignon 1996) for a linear dynamical system. Since local linearization is a technique used to test the local stability of equilibrium points in nonlinear systems, the theorem can be used in this context (Srivastava *et al.* 2014).
The characteristic equation of the Jacobian matrix at the equilibrium is

$$TP\left(\lambda\right) = \lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 \tag{5}$$

The discriminant is
$D(P) = 18a_1a_2a_3 + (a_1a_2)^2 - 4a_3{a_1}^3 - 4a_2^3 - 27a_3^2$
The fractional order Routh-Hurwitz criterion (Ahmed *et al.* 2006; Srivastava *et al.* 2014) is as follows for the system to be stable.:
(i) The equilibrium point meets the necessary and sufficient conditions in order to be locally asymptotically stable, and if $D(P) > 0$, these conditions are $a_1 > 0, a_3 > 0, a_1a_2 - a_3 > 0$.
(ii)If $D(P) < 0, a_1 \geq 0, a_2 \geq 0, a_3 > 0$ then the equilibrium point is locally asymptotically stable for $\alpha < \frac{2}{3}$. However, if $D(P) < 0, a_1 < 0, a_2 < 0, \alpha > \frac{2}{3}$,then all the roots of the characteristic equation satisfy the condition
(iii)If $D(P) < 0, a_1 > 0, a_2 > 0,\ a_1a_2 - a_3 = 0$then all individuals $0 \leq \alpha < 1$ are locally asymptotically stable at the equilibrium point.
(iv) A need for equilibrium points to be locally stable asymptotically is $a_3 > 0$.

Proposed Model: The considered model in this article is. As proposed in (Mangiarotti *et al.* 2020) The three decision variable x (Number of daily cases) ,y (Number of daily serious cases reported) and Z(Number of daily deaths) along with 11 parameters $\alpha_1,\alpha_2,\ \alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8,\alpha_9,\alpha_{10},\alpha_{11}$.

$$\begin{aligned} \frac{d^{\alpha}x}{dt^{\alpha}} &= \alpha_1 z^2 + \alpha_2 x^2 + \alpha_3 y\left(z + \alpha_4 x\right) \\ \frac{d^{\alpha}y}{dt^{\alpha}} &= \alpha_5 x + \alpha_6 y + \alpha_7\, z^2 \\ \frac{d^{\alpha}z}{dt^{\alpha}} &= \alpha_8 xz + \alpha_9 xy + \alpha_{10} z + \alpha_{11} x^2 \end{aligned} \tag{6}$$

Values of the parameters are considered as The above model shows the chaotic behaviour with initial values x=180, y=30, z=8 for the time variation of t=100, for order of derivatives α=0.97.

Table 1 Values of the parameter in the model (6)

$\alpha_1 = -0.10530723$	$\alpha_2 = 2.343X10^{-5}$	α_3=0.15204	α_4=-0.01451520 .
α_5=-0.20517824	α_6=0.44040714	α_7=0.16060376	α_8=-0.00011493.
α_9=$-1.215X10^{-5}$	α_{10}=0.2844499	α_{11}=$2.38X10^{-6}$	.

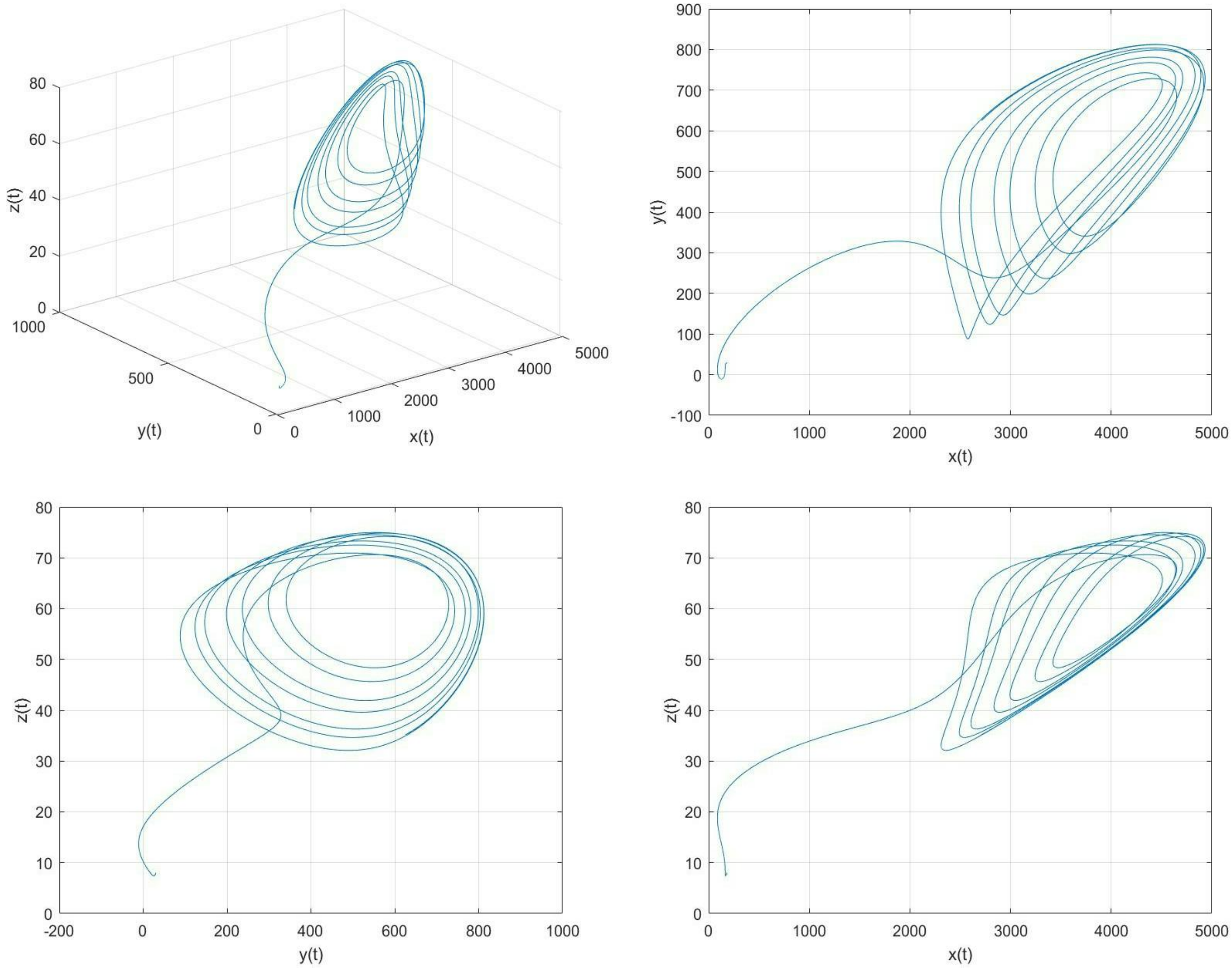


Figure 1 Chaotic behaviour of the system in (6) with initial values x=180, y=30, z=8 for the time variation of t=100, for order of derivatives $\alpha = 0.97$

STABILITY OF THE SYSTEM

To analyse the stability of the system we have

$$\begin{aligned} \alpha_1 z^2 + \alpha_2 x^2 + \alpha_3 y\,(z + \alpha_4 x) &= 0 \\ \alpha_5 x + \alpha_6 y + \alpha_7\, z^2 &= 0 \\ \alpha_8 xz + \alpha_9 xy + \alpha_{10} z + \alpha_{11} x^2 &= 0 \end{aligned} \tag{7}$$

On solving this nonlinear system of equations with the given parameters as in proposed model is given, we have. The Jacobian matrix (J) of the above system is

$$J = \begin{bmatrix} 2\alpha_2 x + \alpha_3\alpha_4 y & \alpha_3 z & 2\alpha_1 z + \alpha_3 y \\ \alpha_5 & \alpha_6 & 2\alpha_7 z \\ \alpha_8 z + \alpha_9 y + 2\alpha_{11} x & \alpha_9 x & \alpha_8 x + \alpha_{10} \end{bmatrix} \tag{8}$$

The equilibrium point is calculated on solving the equations in (7) and we get 4 equilibrium points which are $E_1(0,0,0)$,$E_2(-1149.44, -590.097, 12.2352)$,$E_3(-619.232, -6075.71, 125.975)$, $E_4(25638.5, 6103.77, -126.557)$.

The eigen values of the Jacobian matrix at these points are $0.2202+18.7956i, 0.2202-18.7956i, 0.2844+0.000i$, on E_1, on E_2 the eigen values are $0.0007+9.4981i, 0.0007-9.4981i, 0.0004+0.000i$ .The eigen vales of the Jacobian matric on E_3 is $0.0007+2.0519i, 0.0007-2.0519i, 0.001+0.000i$ on the last point E_4 the eigen values are $-3.9423, 3.9415, -0.0001$ which shows that all the equilibrium points are unstable.

CHAOS CONTROL

To control the chaos of the covid dynamical system as proposed in (6) let us construct the feedback controller such as

$$\begin{aligned} \frac{d^\alpha x}{dt^\alpha} &= \alpha_1 z^2+\alpha_2 x^2+\alpha_3 y\,(z+\alpha_4 x)-k_1\,(x-\bar{x}) \\ \frac{d^\alpha y}{dt^\alpha} &= \alpha_5 x+\alpha_6 y+\alpha_7\, z^2-k_2\,(y-\bar{y}) \\ \frac{d^\alpha z}{dt^\alpha} &= \alpha_8 xz+\alpha_9 xy+\alpha_{10} z+\alpha_{11} x^2-k_3\,(z-\bar{z}) \end{aligned} \tag{9}$$

Where k_1, k_2, k_3 are control parameters and $\bar{x}$, $\bar{y}$, $\bar{z}$ are Equilibrium points of the system. At equilibrium point the Jacobian of this system is

$$\begin{bmatrix} 2\alpha_2\bar{x}+\alpha_3\alpha_4\bar{y}-k_1 & \alpha_3\,(\bar{z}+\alpha_4\bar{x}) & 2\alpha_1\bar{z}+\alpha_3\bar{y} \\ \alpha_5 & \alpha_6-k_2 & 2\alpha_7\bar{z} \\ \alpha_8\bar{z}+\alpha_9\bar{y}+2\alpha_{11}\bar{x} & \alpha_9\bar{x} & \alpha_8\bar{x}+\alpha_{10}-k_3 \end{bmatrix} \tag{10}$$

characteristic polynomial of the above Jacobian matrix with the parameters as in Table 1 is

$$\begin{aligned} P(t) =& t^3+(k_1+k_2+k_3-0.72485704+0.00007\bar{x}+0.00221\bar{y})\ t^2 \\ &+(-0.44040714\,k_3+0.125273767-0.72485704k_1+ \\ &0.2844499k_2+k_1k_2+k_1k_3+k_2k_3-0.00047\,\bar{x}+0.00012\,k_1\,\bar{x} \\ &+0.000068069999999999999\,k_2\,\bar{x}-0.00004686\,k_3\,\bar{x}- \\ &5.3856198\times 10^{-9}\,\bar{x}^2-0.00158\,\bar{y}+0.00221\,k_2\,\bar{y}+0.00221 \\ &-4.700724164505601\times 10^{-7}\bar{x}\,\bar{y}+0.031171093689712204\,\bar{z}- \\ &0.000002558965689\,\bar{y}\,\bar{z}+0.0000049\,\bar{x}\,\bar{z}+0.00000185\,\bar{y}^2)\ t \\ &-0.2844499\,k_1\,k_2+0.12527376693228598\,k_1-0.44040714\,k_1k_3 \\ &+k_1k_2k_3+0.00012293029636844125\bar{x}-0.00005\,k_1\bar{x} \\ &+0.000013329322313999999\,k_2\bar{x}+0.00011493\,k_1\,k_2\,\bar{x}- \\ &0.00043216853431286569\,k_3\,\bar{x}-0.00004686\,k_2\,k_3\,\bar{x}+0.00027\bar{y} \\ &-0.0006102759693364992\,k_2\,\bar{y}-0.0009719305571249997\,k_3\,\bar{y}+ \\ &0.002206891008\,k_2\,k_3\,\bar{y}\ -1.719996417347599\times 10^{-7}\bar{x}\,\bar{y} \\ &-4.700724164505601\times 10^{-7}\,k_2\,\bar{x}\,\bar{y}-0.008862839394471904\,\bar{z} \\ &-0.0000242059198878\,k_2\bar{z}+0.03119529961\,k_3\,\bar{z}+ \\ &0.000003587\,\bar{x}\,\bar{z}-4.966912964857768\times 10^{-8}\,\bar{x}^2- \\ &5.3856198\times 10^{-9}\,k_2\,\bar{x}^2-8.13557944\times 10^{-7}\bar{y}^2+0.00000185\,k_2\,\bar{y}^2 \\ &+0.000003902671368\,k_1\,\bar{x}\,\bar{z}+0.0000010025248296\,k_2\,\bar{x}\,\bar{z}+ \\ &3.191341960623825\times 10^{-9}\,\bar{x}^2\,\bar{z}+0.00000112698676045061\,9\bar{y}\,\bar{z} \\ &-0.000002558965689\,k_2\,\bar{y}\,\bar{z}+0.0000056128\,\bar{z}^2- \\ &-0.00000255897\,k_2\,\bar{y}\,\bar{z}+0.000005618\,\bar{z}^2- \\ &2.32461222782208\times 10^{-7}\bar{x}\,\bar{z}^2+5.933621547907201\times 10^{-7}\bar{y}\bar{z}^2 \end{aligned} \tag{11}$$

For Routh Hurwitz criteria for fractional order, we have

$$a_1 = k_1+k_2+k_3-0.72485704+0.00006807\bar{x}+0.00220689101\bar{y} \tag{12}$$

$$\begin{aligned} a_2 =& -0.44040714\,k_3+0.1252737669-0.72485704\,k_1+0.2844499k_2 \\ &+k_1k_2+k_1k_3+k_2k_3-0.00046945520459906590\ \bar{x}+0.00011493\,k_1\,\bar{x} \\ &+0.000068069999999999999\,k_2\,\bar{x}-0.00004686\,k_3\,\bar{x}+0.00011493\,k_1\,\bar{x} \\ &+0.00006807\,k_2\,\bar{x}-0.00004686\,k_3\,\bar{x}-5.3856198\times 10^{-9}\,\bar{x}^2 \\ &-0.0015822065264615\,\bar{y}+0.002206891008\,k_2\,\bar{y}+0.0022069\,k_3\,\bar{y} \\ &-4.700724164505601\times 10^{-7}\bar{x}\,\bar{y}+0.031171094\,\bar{z}-0.00000256\,\bar{y}\,\bar{z} \\ &+0.0000049051962\,\bar{x}\,\bar{z}+0.0000018473\,\bar{y}^2, \end{aligned} \tag{13}$$

$$\begin{aligned} a_3 =& -0.2844499\,k_1\,k_2+0.12527376693228598\,k_1-0.44040714\,k_1k_3 \\ &+k_1k_2k_3+0.0001229303\bar{x}-0.000050615992600199994\,k_1\bar{x} \\ &+0.00001333\,k_2\bar{x}+0.000115\,k_1\,k_2\,\bar{x}-0.0004322\,k_3\,\bar{x} \\ &-0.0000479\,k_2\,k_3\,\bar{x}+0.00027\,\bar{y}-0.0006103\,k_2\,\bar{y}-0.00097\,k_3\,\bar{y} \\ &+0.0022069\,k_2\,k_3\,\bar{y}\ -1.71999642\times 10^{-7}\bar{x}\,\bar{y} \\ &-4.700724165\times 10^{-7}\,k_2\,\bar{x}\,\bar{y}-0.00886284\,\bar{z}-0.00002421\,k_2\bar{z} \\ &+0.0311953\,k_3\,\bar{z}+0.0000035873303397638 96\,\bar{x}\,\bar{z} \\ &-4.966912964857768\times 10^{-8}\,\bar{x}^2-5.3856198\times 10^{-9}\,k_2\,\bar{x}^2 \\ &-8.1355794402204\times 10^{-7}\bar{y}^2+0.00000185\,k_2\,\bar{y}^2 \\ &+0.00000390267\,k_1\,\bar{x}\,\bar{z}+0.0000010025248296\,k_2\,\bar{x}\,\bar{z} \\ &+3.191341960624\times 10^{-9}\,\bar{x}^2\,\bar{z}+0.000001126986760451\,\bar{y}\,\bar{z} \\ &-0.00000255897\,k_2\,\bar{y}\,\bar{z}+0.0000056127665\,\bar{z}^2 \\ &-2.32461222782208\times 10^{-7}\bar{x}\,\bar{z}^2+5.93362154791\times 10^{-7}\bar{y}\bar{z}^2 \end{aligned} \tag{14}$$

$$D(P) = 18a_1a_2a_3+(a_1a_2)^2-4a_3a_1^3-4a_2^3-27a_3^2 \tag{15}$$

RESULTS AND DISCUSSION

In the control analysis of the above problem, we observe that the system is getting controlled at every equilibrium point with the feedback controller. At first equilibrium point $E_1(0,0,0)$ the stability is achieved at $k_1=1, k_2=2, k_3=5$ for the values of $\alpha=0.97$. when we increase the values of k_3, the first eigenvalue of the Jacobian matrix increases in negative direction very fast so that system goes towards the equilibrium point with fast rate.

It shows that if we subtract from the first equation in the model (6) the daily cases one time, from the second equation twice the rate of change of the daily number of critical cases, and from the third equation five times the daily deaths, then the system is under control. The other case that is possible is that instead of controlling too many death cases, we could reduce the 6 times daily critical cases and control the chaos in the system. If we could control the 3 times daily critical cases, then the system would also be under control.

The second equilibrium point E_2 shoes the stability with $k_1=8$, which means that at this juncture the system will not be chaotic if 8 times we could reduce the daily cases or 5 times we reduce the daily critical cases, or if the daily cases are reduced by 10 times and daily deaths are reduced by 12 times or more, the system is under control.

Table 2 : Stability using Routh Hurwitz criteria at the first equilibrium point $E_1(0,0,0)$ after putting these points in the equation $12, 13, 14, 15$ is as follows.

Sr. No	k_1	k_2	k_3	a_1	a_3	$a_1a_2 - a_3$	D(P)	Eigen values of Jacobian Matrix of Controlled system	Stable / Unstable
1	1	2	5	7.2751	7.3543	100.08	94.97	-4.7156, -1.5596, -1.0000	Stable for $0 < \alpha < 1$.
2	1	2	10	12.2751	15.1523	323.2150	$4.6960x10^3$	-9.7156 -1.5596 -1.0000	Stable for $0 < \alpha < 1$
3	1	2	≥ 5	+ive	+ive	+ive	+ive	-ive	Stable for $0 < \alpha < 1.$
4	1	6	1	7.2751	3.9782	95.4491	240.2804	-0.7156, -5.5596, -1.0000	Stable for $0 < \alpha < 1..$
5	1	≥ 6	1	+ive	+ive	+ive	+ive	-ive	Stable for $0 < \alpha < 1.$
6	3	1	1	4.2751	1.2013	19.2970	8.0779	-0.7156, -0.5596, -3.0000	Stable for $0 < \alpha < 1.$
7	≥ 3	1	1	$+ive$	$+ive$	$+ive$	$+ive$	$-ive$	Stable for $0 < \alpha < 1$.

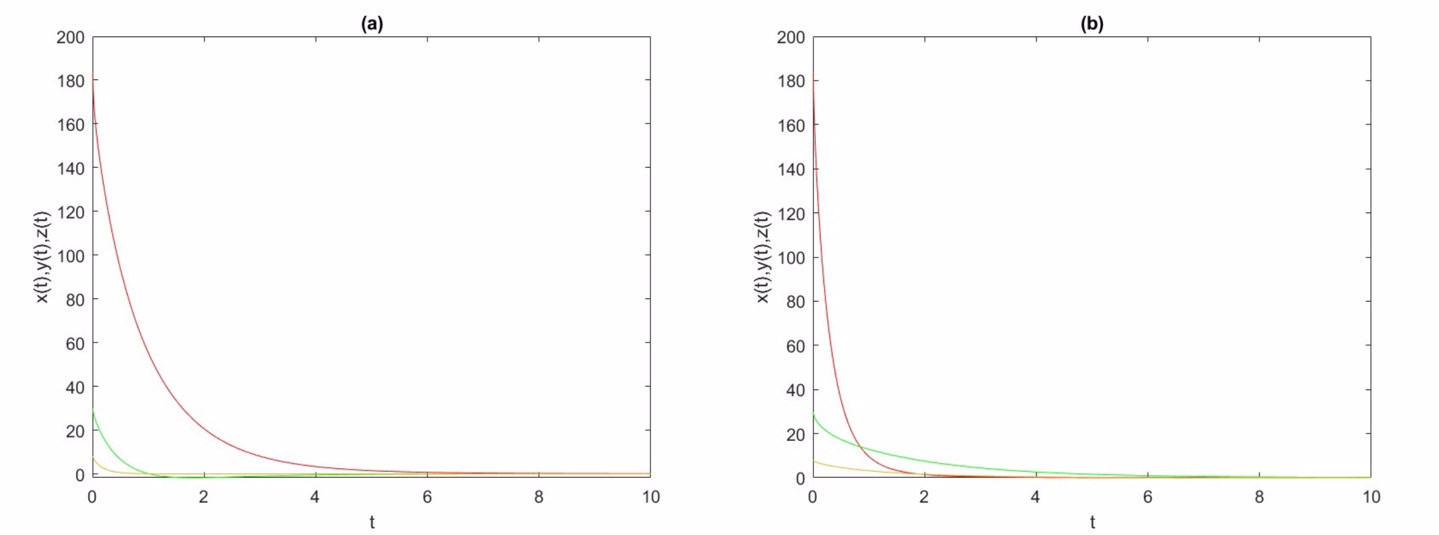


Figure 2 Plot x,y,z at (a) $k_1 = 1, k_2 = 2, k_3 = 5$ at α=0.97 at E_1 (b) Plot at $k_1 = 3, k_2 = 1, k_3 = 1$ at α=0.97 at E_1

The third equilibrium point, E_3 is such that we need to reduce the critical cases by $12 - 15$ times and the daily deaths by 21 times to control the system. we need to reduce the daily critical cases by 3 times, or more than system is under control. Similarly, at the fourth equilibrium point E_4 the system is under control if 9 times daily cases are reduced and 3 times daily critical cases are reduced,

Table 3 : Stability using Routh Hurwitz criteria at the second equilibrium point $E_2(1149.44, 590.097, 12.2352)$ after putting these points in the equation $12, 13, 14, 15$ is as follows.

Sr. No	k$_1$	k$_2$	k$_3$	a_1	a_3	$a_1a_2 - a_3$	D(P)	Eigen values of Jacobian Matrix of Controlled system	Stable / Unstable
1	8	1	1	7.8946	0.0762	75.7604	$2.1594x10^3$	-6.5686, -0.9980, -0.3280	Stable for $0 <\alpha< 1$.
2	≥ 8	1	1	+ive	+ive	+ive	+ive	-ive	Stable for $0 <\alpha< 1$
3	1	5	1	4.8946	0.4466	25.1061	74.3602	-4.3634 -0.1542 -0.3770	Stable for $0 < \alpha < 1$
4	1	≥ 5	1	+ive	+ive	+ive	+ive	-ive	Stable for $0 <\alpha< 1$
5	10	1	12	20.8946	54.6713	$2.3339x10^3$	$4.7597x10^3$	-0.6626, -8.7041, -11.5279	Stable for $0 <\alpha< 1$
6	10	1	≥ 12	$+ive$	$+ive$	+ive	+ive	-ive	Stable for $0 <\alpha< 1$

Table 4 : Stability using Routh Hurwitz criteria at the Third equilibrium point $E_3(-619.232, -6075.71, 125.975)$ after putting these points in the equation $12, 13, 14, 15$ is as follows.

Sr. No	k$_1$	k$_2$	k$_3$	a_1	a_3	$a_1a_2 - a_3$	D(P)	Eigen values of Jacobian Matrix of Controlled system	Stable / Unstable
1	12	3	21	21.8246	24.3566	$2.0203x10^3$	7.5909x105	-16.7962 + 0.0000i, -2.5142 + 1.0957i, -2.5142 - 1.0957i	Stable for 0<α<1
2	12	≥ 3	21	+ive	+ive	+ive	+ive	-ive	Stable for 0<α<1
3	12	3	21-27	+ive	+ive	+ive	+ive	-ive	Stable for 0<α<1
4	12-15	3	21	+ive	+ive	+ive	+ive	-ive	Stable for $0 <\alpha< 1$

whereas 13 times daily deaths are reduced. The system is under control, and it will not generate chaos.

On observing all the cases at the equilibrium points we observe that system is under control if we could reduce the daily cases by 12 times and daily critical cases by 3 times and daily deaths by 21 times then system is under control. These changes in the system

Table 5 : Stability Using Routh Hurwitz criteria at the first equilibrium point $E_4(25638.5, 6103.77, -126.557)$ after putting these points in the equation $12, 13, 14, 15$ is as follows.

Sr. No	k_1	k_2	k_3	a_1	a_3	$a_1a_2 - a_3$	D(P)	Eigen values of Jacobian Matrix of Controlled system	Stable / Unstable
1	9	3	13	39.4907	211.1828	$1.3829x10^4$	$1.7508x10^7$	-0.0417, -25.7969, -13.6521	Stable for $0<\alpha<1$
2	≥ 9	3	13	+ive	+ive	+ive	+ive	-ive	Stable for $0<\alpha<1$
3	9	≥ 3	13	+ive	+ive	+ive	+ive	-ive	Stable for $0<\alpha<1$
4	9	3	≥ 13	+ive	+ive	+ive	+ive	-ive	Stable for $0 <\alpha< 1$

Table 6 : Stability analysis with the control parameters values as $k_1 = 12, k_2 = 3, k_3 = 21$

Equilibrium Point	a_1	a_3	$a_1a_2 - a_3$	D(P)	Eigen values of Jacobian Matrix of Controlled system	Stable / Unstable
E1	35.2751	636.2805	$1.1147x10^4$	$2.0627x10^6$	-20.7156, -2.5596, -12.0000	stable
E2	33.8946	565.7037	$9.7454x10^3$	$1.9480x10^6$	-2.6660, -10.6586, -20.5700	stable
E3	21.8246	24.3566	$2.0203x10^3$	$7.5909x10^5$	-16.7962 + 0.0000i, -2.5142 + 1.0957i, -2.5142 - 1.0957i	stable
E4	50.4907	788.8388	$3.0759x10^4$	$4.4526x10^7$	-0.8051, -30.6777, -19.0079	stable

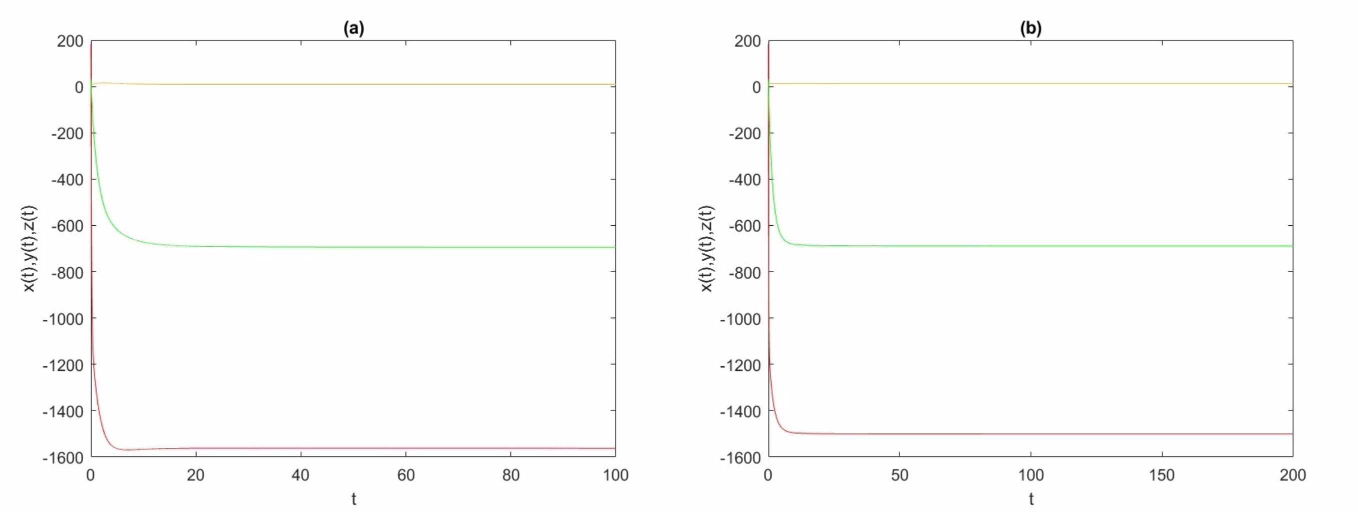


Figure 3 Plot x,y,z at (a) $k_1 = 8, k_2 = 1, k_3 = 1$ at α=0.97 at E_2 (b) $k_1 = 10, k_2 = 1, k_3 = 12$ at α= 0.97 at E_2

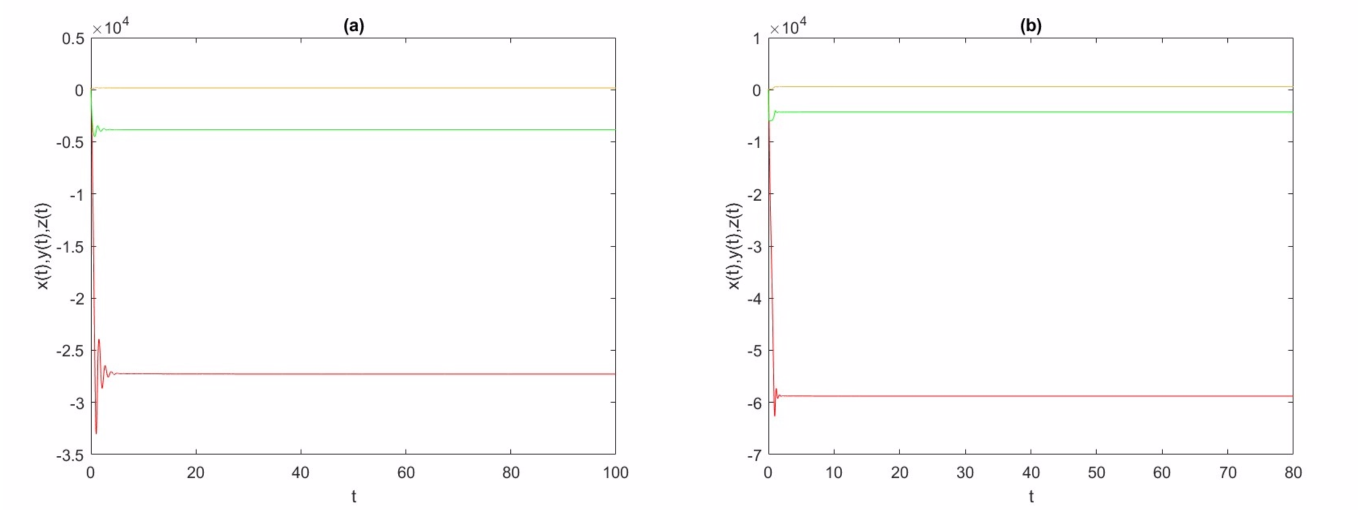


Figure 4 Plot x,y,z at (a) $k_1 = 12, k_2 = 3, k_3 = 21$ at α=0.97 at E_3 (b) $k_1 = 15, k_2 = 31, k_3 = 21$ at α= 0.97 at E_3

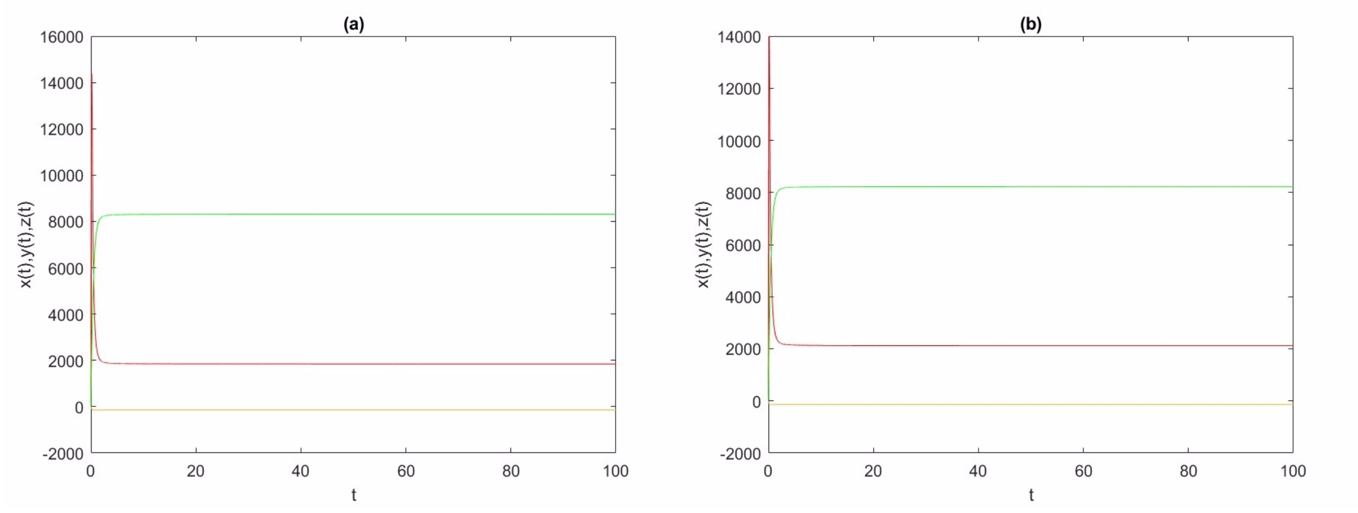


Figure 5 Plot x,y,z at (a) $k_1 = 9, k_2 = 3, k_3 = 13$ at α=0.97 at E_4 (b) $k_1 = 9, k_2 = 3, k_3 = 20$ at α= 0.97 at E_4

can be achieved by the social distancing which could reduce the daily cases and daily critical cases and preventing deaths by proper treatment on time.

CONCLUSION

In the present article, the feedback control method has been applied to control the chaos in the dynamical system of COVID-19, as proposed by (Mangiarotti *et al.* 2020) , which has been studied by (Debbouche *et al.* 2021). In the present article, the fractional order Routh- Hurwitz stability criteria have been utilized, and to solve the fractional-order system, Adams-Bashforth-Molton methods are used. The control of chaos is obtained under different equilibrium points and parameters. In this article, chaos is studied in the dynamical system that is proposed for representing the spread of COVID-19. In the present article, it is shown under what conditions the control parameters of daily infected cases, daily critical cases, and daily deaths should be controlled so that chaos can be controlled in the dynamical system.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Ahmad, S. W., M. Sarwar, G. Rahmat, K. Shah, H. Ahmad, *et al.*, 2022 Fractional order model for the coronavirus (covid-19) in wuhan, china. Fractals **30**: 2240007.

Ahmed, E., A. El-Sayed, and H. A. El-Saka, 2006 On some routh–hurwitz conditions for fractional order differential equations and their applications in lorenz, rössler, chua and chen systems. Physics Letters A **358**: 1–4.

Alsadat, N., M. Imran, M. H. Tahir, F. Jamal, H. Ahmad, *et al.*, 2023 Compounded bell-g class of statistical models with applications to covid-19 and actuarial data. Open Physics **21**: 20220242.

Babu, G. R., D. Ray, R. Bhaduri, A. Halder, R. Kundu, *et al.*, 2021 Covid-19 pandemic in india: Through the lens of modeling. Global Health: Science and Practice **9**: 220–228.

Bai, E.-W. and K. E. Lonngren, 2000 Sequential synchronization of two lorenz systems using active control. Chaos, Solitons & Fractals **11**: 1041–1044.

Borah, M., D. Das, A. Gayan, F. Fenton, and E. Cherry, 2021 Control and anticontrol of chaos in fractional-order models of diabetes, hiv, dengue, migraine, parkinson's and ebola virus diseases. Chaos, Solitons & Fractals **153**: 111419.

Borah, M., A. Gayan, J. S. Sharma, Y. Chen, Z. Wei, *et al.*, 2022 Is fractional-order chaos theory the new tool to model chaotic pandemics as covid-19? Nonlinear dynamics **109**: 1187–1215.

Chandra, S. K. and M. K. Bajpai, 2022 Fractional model with social distancing parameter for early estimation of covid-19 spread. Arabian Journal for Science and Engineering **47**: 209–218.

Debbouche, N., A. Ouannas, I. M. Batiha, and G. Grassi, 2021 Chaotic dynamics in a novel covid-19 pandemic model described by commensurate and incommensurate fractional-order derivatives. Nonlinear Dynamics pp. 1–13.

Farshi, E., 2020 Simulation of herd immunity in covid-19 using monte carlo method. Austin J Pulm Respir Med **7**: 1066.

Giordano, G., F. Blanchini, R. Bruno, P. Colaneri, A. Di Filippo, *et al.*, 2020 Modelling the covid-19 epidemic and implementation of population-wide interventions in italy. Nature medicine **26**: 855–860.

Haq, I. U., N. Ali, H. Ahmad, and T. A. Nofal, 2022 On the fractional-order mathematical model of covid-19 with the effects of multiple non-pharmaceutical interventions. AIMS Math **7**: 16017–16036.

Higazy, M., 2020 Novel fractional order sidarthe mathematical model of covid-19 pandemic. Chaos, Solitons & Fractals **138**: 110007.

Javeed, S., S. Anjum, K. S. Alimgeer, M. Atif, M. S. Khan, *et al.*, 2021 A novel mathematical model for covid-19 with remedial strategies. Results in Physics **27**: 104248.

Kermack, W. O. and A. G. McKendrick, 1927 A contribution to the mathematical theory of epidemics. Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character **115**: 700–721.

Maltezos, S. and A. Georgakopoulou, 2021 Novel approach for monte carlo simulation of the new covid-19 spread dynamics. Infection, Genetics and Evolution **92**: 104896.

Mandal, M., S. Jana, S. K. Nandi, A. Khatua, S. Adak, *et al.*, 2020 A model based study on the dynamics of covid-19: Prediction and control. Chaos, Solitons & Fractals **136**: 109889.

Mangiarotti, S., M. Peyre, Y. Zhang, M. Huc, F. Roger, *et al.*, 2020 Chaos theory applied to the outbreak of covid-19: an ancillary approach to decision making in pandemic context. Epidemiology & Infection **148**.

Matignon, D., 1996 Stability results for fractional differential equations with applications to control processing. In *Computational engineering in systems applications*, volume 2, pp. 963–968, Citeseer.

Podlubnv, I., 1999 Fractional differential equations academic press. San Diego, Boston **6**.

Postavaru, O., S. Anton, and A. Toma, 2021 Covid-19 pandemic and chaos theory. Mathematics and Computers in Simulation **181**: 138–149.

Srivastava, M., S. Agrawal, K. Vishal, and S. Das, 2014 Chaos control of fractional order rabinovich–fabrikant system and synchronization between chaotic and chaos controlled fractional order rabinovich–fabrikant system. Applied Mathematical Modelling **38**: 3361–3372.

Xie, G., 2020 A novel monte carlo simulation procedure for modelling covid-19 spread over time. Scientific reports **10**: 13120.

Xu, C., Y. Yu, Y. Chen, and Z. Lu, 2020 Forecast analysis of the epidemics trend of covid-19 in the usa by a generalized fractional-order seir model. Nonlinear dynamics **101**: 1621–1634.

Xu, J. and Y. Tang, 2021 An integrated epidemic modelling framework for the real-time forecast of covid-19 outbreaks in current epicentres. Statistical Theory and Related Fields **5**: 200–220.

How to cite this article: Mishra, V., Maitra, S., Dash, M., Agrawal, S. K., and Agarwal, P. Chaos and Control of COVID-19 Dynamical System. *Chaos Theory and Applications*, 5(3), 233-241, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

CHAOS Theory and Applications in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / **No.**3 / 2023 / **pp.** 242-255
https://doi.org/10.51537/chaos.1305009

Time-Varying Fractal Analysis of Exchange Rates

Baki Unal*,1
*Iskenderun Technical University, Faculty of Engineering and Natural Sciences, Industrial Engineering, 31200, Iskenderun, Hatay, Turkiye.

ABSTRACT The foreign exchange (forex) market is a dynamic and complex financial arena where the exchange rates of various currency pairs fluctuate continuously. Among these currency pairs, EUR/TRY and USD/TRY hold significant economic relevance due to their roles in international trade and finance. In this study, we analyze the multifractality of hourly EUR/TRY and USD/TRY exchange rate data for the whole period, as well as its time-varying individual and cross correlations, spanning from May 31, 2018, to March 21, 2022. We employ multifractal detrended cross-correlation analysis (MF-DCCA) and multifractal detrended fluctuation analysis (MF-DFA) methodologies. The aim of studying multifractality in exchange rates is to comprehend and model the complex and intricate nature of price movements and dynamics of the EUR/TRY and USD/TRY exchange rates. In the analysis of the whole period, multifractality is detected in individual exchange rates and cross correlations. In the rolling window analysis, we demonstrated how multifractality and cross correlation multifractality change over time. Additionally, contributions of the sources of the multifractality are investigated in a time-varying framework. Multifractal nature of these exchange rates indicate that they exhibit complex and scale-dependent behaviors, which go beyond the traditional linear models. The existence of multifractality in EUR/TRY and USD/TRY exchange rates has significant implications for financial modeling, risk management, and trading strategies. It implies that standard linear models may not capture the full complexity of these markets, necessitating the development of more sophisticated models that account for multifractal properties.

KEYWORDS
Exchange rates
Multifractality
MF-DFA
MF-DCCA
Fractal theory

INTRODUCTION

Fractal theory is originated from (Mandelbrot 1982) and used to provide an explanation for economic and financial data where traditional efficient market hypothesis (EMH) failed. Fractal geometry is applied in the analysis of systems which are irregular and self-similar at all scales. One of the key characteristics of these systems are non-integer dimensions. Fractal systems can be categorized as monofractal or multifractal. Monofractal systems can be defined by a single scaling exponent and different regions of these systems have same scaling properties. However, multifractal systems display varying scaling properties in different regions, requiring multiple scaling exponents to describe the system.

Firstly, in the field of hydrology (Hurst 1951, 1957) suggested rescaled range (R/S) methodology for studying systems exhibiting fractal properties. However, Lo (1991) demonstrated the shortcomings of Hurst methodology such as sensitivity to short-term autocorrelation. To address this deficiency (Peng *et al.* 1994) proposed a methodology called Detrended Fluctuation Analysis (DFA). DFA methodology is successfully applied to noisy and non-stationary time series which exhibiting long-range correlations and fractal scaling properties. Numerous data sets have been successfully analyzed using this method, including geological, economic, financial, weather and earthquake data (Liu *et al.* 1999; Buldyrev *et al.* 1998; Blesić *et al.* 1999; Bunde *et al.* 2000; Ashkenazy *et al.* 2001; Talkner and Weber 2000). However, studies in this field have revealed that some data from various fields such as medicine, geophysics, economy and finance do not exhibit monofractal scaling behavior. Consequently, a single scaling exponent cannot adequately represent these multifractal systems (Kantelhardt *et al.* 2001; Hu *et al.* 2001), and multiple scaling exponents are required.

To analyze multifractal systems (Kantelhardt *et al.* 2002) purposed Multifractal Detrended Fluctuation Analysis (MF-DFA) which is an extension of the DFA. MF-DFA methodology has been successfully applied to many nonstationary time series datasets in

Manuscript received: 28 May 2023,
Revised: 13 September 2023,
Accepted: 26 September 2023.

[1] bakiunal@gmail.com (**Corresponding author**).

the literature (Kantelhardt *et al.* 2003; Movahed *et al.* 2006; Telesca *et al.* 2004). The literature demonstrates that many time series from various fields exhibit multifractal properties, and a single scaling exponent is not sufficient to describe these datasets (Matia *et al.* 2003; Chen and He 2010; He and Chen 2010b,a; Zunino *et al.* 2009).

Afterwards, by developing DFA methodology Podobnik and Stanley (2008) introduced the detrended cross-correlation analysis (DCCA) methodology for studying cross correlations between two systems. Subsequently, Zhou (2008) combined MF-DFA and DCCA to propose the multifractal detrended cross-correlation analysis (MF-DCCA) methodology for investigating multifractal properties of two correlated nonstationary time series. MF-DCCA methodology has been successfully applied to numerous economic and financial datasets from foreign exchange market (Xie *et al.* 2017; Li *et al.* 2016), the stock market (Ma *et al.* 2013a; Yue *et al.* 2017), the crude oil market (Ma *et al.* 2013b, 2014; Wang *et al.* 2011b), carbon market (Zhuang *et al.* 2014, 2015) and the commodity market (Wang *et al.* 2011a; Lu *et al.* 2017).

Furthermore foreign exchange market is of great importance to global economy. This market connects economies around the world without geographic and temporal boundaries. Exchange rates are vital macroeconomic variables for policy makers, investors, researchers and economists. Instabilities of exchange rates can have devastating effects on the economies. Therefore, researchers and economists have attempted to model exchange rates using various methodologies. These studies have revealed that predicting and explaining fluctuations in exchange rates is challenging. Efficient market hypothesis suggested by (Fama 1965) indicated, share prices follow random walk and are unpredictable. However, this hypothesis challenged by different authors subsequently (Yen and Lee 2008; Lim and Brooks 2011). An alternative to EMH is fractal market hypothesis (FMH) which is suggested by (Lim and Brooks 2011; Peters 1994). This hypothesis suggests that markets exhibit the same structure on different scales (daily, weekly, monthly, etc.). The EMH has led to investigations into the fractal and multifractal properties of economic and financial time series.

To the best of our knowledge, there is only one study in the literature that investigates the multifractal properties of USD/TRY exchange rates (Gülbaş and Gazanfer 2013). This study detected multifractality in USD/TRY exchange rates but did not provide a time varying analysis to investigate how multifractality and sources of multifractality change over time. There are other studies in the literature that examine the multifractal properties of various exchange rates as well (Stošić *et al.* 2015; Schmitt *et al.* 1999; Caraiani and Haven 2015; Han *et al.* 2019). While these studies have detected multifractality in other exchange rates, they have not shed light on how multifractality and its sources change over time.

MF-DFA and MF-DCCA methods are important methods in the field of time series analysis, particularly for studying complex and non-linear behaviors in financial data and other complex systems. The importance of these methods is presented below:

a) Capturing Nonlinear Behavior: Financial and economic data often exhibit nonlinear behaviors that cannot be adequately captured by traditional linear methods. MF-DFA and MF-DCCA are designed to detect and quantify these nonlinear characteristics, providing a more accurate representation of the underlying dynamics.

b) Multiscale Analysis: MF-DFA and MF-DCCA allow for the analysis of data across multiple time scales. This is important because financial data often exhibit different patterns and behaviors at different scales. By analyzing multiple scales, these methods offer a more comprehensive view of the system's complexity.

c) Multifractality: These methods are specifically designed to identify and characterize multifractal behavior in time series data. Multifractality refers to the property where different scales of observation exhibit different levels of self-similarity and irregularity. This is a common feature in financial data and other complex systems.

d) Cross-Correlation Analysis: MF-DCCA goes beyond traditional correlation analysis by accounting for cross-correlations that exist at different time scales. This is crucial in understanding how different variables interact and influence each other over different horizons.

MF-DFA and MF-DCCA methods have some differences from other methods. These differences are summarized as below:

a) Fractal vs. Multifractal Analysis: Traditional fractal analysis focuses on self-similarity at a single fractal dimension. In contrast, multifractal analysis considers multiple fractal dimensions, which allows for a more nuanced understanding of complex systems.

b) Nonlinear vs. Linear Methods: While linear methods assume a linear relationship between variables, MF-DFA and MF-DCCA are designed to capture nonlinear and multifractal behaviors. This is particularly important in financial markets where linearity often fails to explain the full complexity.

c) Time Scale Consideration: MF-DFA and MF-DCCA analyze data across multiple time scales, which provides insights into the dynamics at different levels. Traditional methods might overlook these multiscale interactions.

d) Cross-Correlation Consideration: MF-DCCA specifically addresses cross-correlations between multiple variables at different time scales. This is a feature that many traditional methods lack.

e) Complexity: MF-DFA and MF-DCCA are more complex and sophisticated methods compared to traditional linear analysis. They require a deeper understanding of their underlying principles and assumptions.

In recent years Turkey has become integrated into international economic markets. According to the general trade system in Turkey, in the January-April period of 2022, exports increased by 21.6% compared to the previous year and reached 83.5 billion dollars, while imports increased by 40.2% and reached 116 billion 85 million dollars. Therefore USD/TRY and EUR/TRY exchange rates are of great importance to the Turkish economy and have significant effects on other macroeconomic variables such as GDP, current account deficit, inflation and unemployment. The selection of the preferred dataset, specifically the USD/TRY and EUR/TRY exchange rates, was based on careful consideration of several criteria that these currency pairs satisfy, making them ideal candidates for multifractality analysis. We chose to test the multifractality of USD/TRY and EUR/TRY exchange rates because of the several reasons. Firstly, USD/TRY and EUR/TRY are important currency pairs involving major global currencies (US Dollar and Euro) and the Turkish Lira.

These exchange rates reflect economic relationships between Turkey and the United States or the Eurozone. Studying their multifractality can provide insights into the dynamics of these economic relationships. Secondly, these currency pairs are among the most actively traded pairs in the foreign exchange market due to Turkey's significant economic activities and its geopolitical positioning. High trading activity often results in complex and multifractal price behaviors, making them interesting candidates for analysis. Thirdly, the Turkish Lira has historically exhibited notable volatility in comparison to major currencies. Such volatility often results in intricate, non-linear, and multifractal price movements. Studying these complex behaviors is vital for understanding the underlying dynamics and interactions in the market. Given the potential volatility of the Turkish Lira, individuals, businesses, and investors involved in transactions or investments with Turkey have a vested interest in understanding the multifractal nature of these exchange rates for effective risk management. Fourthly, exchange rates have policy implications for governments and central banks.

Understanding the multifractality of USD/TRY and EUR/TRY can aid in policy decisions related to trade, investment, and monetary policy. Finally, in the literature time-varying multifractality of USD/TRY and EUR/TRY exchange rates are not investigated in the literature. The selection of USD/TRY and EUR/TRY exchange rates is motivated by their substantial economic importance. The USD/TRY exchange rate is a key benchmark for Turkey's foreign exchange market, and the EUR/TRY exchange rate represents another critical currency pair in the region. Both are integral to international trade, investment, and financial stability within the Turkish economy.

In this study time-varying multifractal properties of exchange rates are analyzed using MFDFA and MF-DCCA methodologies. In this context, two different types of analysis were conducted. These are whole period analysis and rolling window analysis. In the whole period analysis MFDFA and MF-DCCA methodologies are applied to the entire dataset to investigate multifractality over the entire period. In the rolling window analysis MFDFA and MF-DCCA methodologies are applied to data windows and by sliding the window changes in multifractality are examined. Our study addresses seven research questions:

1. Whether USD/TRY and EUR/TRY exchange rates are multifractal?
2. How the multifractality levels of USD/TRY and EUR/TRY exchange rates change over time?
3. Whether cross-correlations between USD/TRY and EUR/TRY exchange rates are multifractal?
4. How the multifractality level of cross correlation between USD/TRY and EUR/TRY exchange rates changes over time?
5. How the fat-tailed distribution's contribution to the level of multifractality of USD/TRY and EUR/TRY exchange rates changes over time?
6. How the long-range correlation's contribution to the level of multifractality of USD/TRY and EUR/TRY exchange rates changes over time?
7. Which cause of multifractality of USD/TRY and EUR/TRY exchange rates is more prevalent over time: long-range autocorrelation or fat-tailed distribution?

Studying multifractality in exchange rates serves several purposes:

a) Better Understanding of Market Behavior: Multifractal analysis helps researchers and analysts delve deeper into the underlying structure of exchange rate movements. It allows them to identify complex patterns and irregularities that are not apparent through traditional methods.

b) Risk Management: Exchange rate movements can have significant implications for international trade, investment, and risk management. Understanding multifractality can aid in developing more accurate risk assessment models, which is crucial for businesses and financial institutions exposed to currency fluctuations.

c) Model Improvement: Traditional financial models often assume certain levels of linearity and Gaussian (normal) distribution of returns. However, exchange rates frequently exhibit fat tails, extreme events, and time-varying volatility. Studying multifractality can lead to the development of more accurate models that capture these characteristics.

d) Algorithmic Trading: Many financial institutions use algorithmic trading strategies to make investment decisions. Understanding multifractality can lead to the development of more sophisticated trading algorithms that adapt to the nonlinear and irregular behavior of exchange rates.

e) Policy Formulation: Central banks and governments make policy decisions based on economic conditions, including exchange rates. Multifractal analysis can provide insights into the underlying dynamics of exchange rates, which can inform more effective policy decisions.

f) Academic Research: Academics study multifractality in exchange rates to contribute to the theoretical understanding of financial markets and to advance the field of financial economics.

In conclusion our study makes several contributions to the literature. Firstly, as far as we know fractal properties of hourly exchange rates are not investigated in the literature. We used hourly data in our multifractal analysis because hourly data provides a higher frequency of observations compared to daily or weekly data. This increased frequency allows for a more detailed analysis of price movements and captures finer nuances in market behavior. Also, financial markets exhibit distinct intraday patterns and volatility changes and hourly data captures these patterns. Additionally, multifractal analysis involves studying patterns at various scales or time horizons. Hourly data allows for a broader range of scales to be analyzed, from short-term fluctuations to longer-term trends.

Usage of hourly data distinguish our study from other studies since hourly data offers a finer level of granularity, captures intraday price movements, reveals higher-frequency fluctuations and volatility changes, and enables researchers to study the immediate market reactions. Secondly, in the literature fractal analysis is usually applied to one or few time periods. However, we presented a time-varying analysis in a rolling window framework. Thirdly, we also presented how the contributions of multifractality sources have changed over time in a rolling window framework. The following is how our study is set up. Section 2 presents the MF-DFA and MF-DCCA techniques. Data is provided in Section 3. In Section 4, empirical findings are given. And Section 5 provides conclusions.

METHODOLOGY

Multifractal Detrended Fluctuation Analysis (MF-DFA)

Suppose x_t denotes a time series where $t = 1, 2, \ldots, N$ The MF-DFA method consist of five steps.

Step1: In the first step the profile is calculated as follows:

$$X_i = \sum_{t=1}^{i} (x_t - \bar{x}) \tag{1}$$

In the expression above $\bar{x}$ is calculated as below:

$$\bar{x} = \frac{1}{N} \sum_{t=1}^{N} x_t \tag{2}$$

Step 2: In the next step the profile X_i is divided into $N_s = int(N/s)$ equal-length parts that don't overlap. There might be a little residue at the end of the profile since the length of the series x_t might not be multiple of the time scale s. The identical process used at the end of the series was repeated in order to account for this residue. As a result of this procedure $2N_s$ total segments are obtained.

Step 3: The variance is calculated by following two formulas for segments $v = 1, 2, \ldots, N_s$ and for segments $v = N_s + 1, N_s + 2, \ldots, 2N_s$ respectively:

$$F_X^2(s, v) = \frac{1}{s} \sum_{j=1}^{s} \left(X_{(v-1)s+j} - \widehat{X}_j^v \right)^2 \tag{3}$$

$$F_X^2(s, v) = \frac{1}{s} \sum_{j=1}^{s} \left(X_{N-(v-N_s)s+j} - \widehat{X}_j^v \right)^2 \tag{4}$$

In the above formulas $\hat{X}_j^v$ denotes the fitting polynomial in segment v with order m. In this study fitting polynomial order m is selected as one.

Step 4: In the next step qth order fluctuation function $F_X^q(s)$ is computed by averaging all segments using following two formulas for $q \neq 0$ and $q = 0$ respectively:

$$F_X^q(s) = \left(\frac{1}{2N_s} \sum_{v=1}^{2N_s} \left[F_X^2(s, v) \right]^{\frac{q}{2}} \right)^{\frac{1}{q}} \tag{5}$$

$$F_X^q(s) = \exp \left(\frac{1}{4N_s} \sum_{v=1}^{2N_s} \left[F_X^2(s, v) \right] \right) \tag{6}$$

Step 5: By analyzing logarithm plots of $F_X^q\ (s)$ versus logarithms of s for each q value the scaling behavior of the fluctuation function is determined. If long-range power-law correlation exists between the series, there is a power-law relationship expressed as below:

$$F_X^q(s) \sim s^{h(q)} \tag{7}$$

The generalized Hurst exponent, or $h(q)$, in the expression above reflects the correlation with power-law. The expression $h(q)$ represents the scaling behavior of segments with large fluctuations for positive values of q, whereas for negative values of q, it represents the scaling behavior of segments with smaller variations. To describe a multifractal series the singularity spectrum $f(\alpha)$ can be used which is calculated as below:

$$\alpha(q) = h(q) + qh'(q) \tag{8}$$

$$f(\alpha) = q[\alpha(q) - h(q)] + 1 \tag{9}$$

The derivative of $h\ (q)$ with respect to q is denoted by $h\prime(q)$ in the expression above. The Hölder exponent, denoted by the symbol $\alpha\ (q)$, measures the singularity's power, while the singularity spectrum, denoted by the symbol $f\ (\alpha)$, measures the Hausdorff dimension of the subset of the series that is characterized by $\alpha\ (q)$. Multifractal mass function can be calculated as below:

$$\tau(q) = qh(q) - 1 \tag{10}$$

The width of the multifractal spectrum $(\Delta\alpha)$, which is calculated as follows, can be used to gauge the level of multifractality:

$$\Delta\alpha = \alpha_{\max} - \alpha_{\min} \tag{11}$$

Higher $\Delta\alpha$ values indicate higher levels of multifractality and lower $\Delta\alpha$ values indicate lower levels of multifractality. The singularity spectrum possesses an α_0 value which corresponds to maximum $f(\alpha)$, i.e. $f(\alpha_0) = 1$. Skewness of the spectrum indicates information on the dominant fluctuations. Right-skewed spectrum suggests that minor variations will predominate, while left-skewed spectrum suggests that huge fluctuations will.

Multifractal Detrended Cross-Correlation Analysis (MF-DCCA)

The MF-DCCA methodology combines two methods namely DCCA and MF-DFA. The MF-DCCA methodology can be utilized to demonstrate multifractal properties of two power-law correlated time series. Suppose x_t and y_t represent two time series with $t = 1, 2, \ldots, N$. The MF-DCCA method consist of following five steps:

Step1: In the first step the profiles are calculated as follows:

$$X_i = \sum_{t=1}^{i} (x_t - \bar{x}) \tag{12}$$

$$Y_i = \sum_{t=1}^{i} (y_t - \bar{y}) \tag{13}$$

In the expressions above $\bar{x}$ and $\bar{y}$ are the average values of the series.

Step 2: In the second step each profile is divided into $2N_s$ segments as in MF-DFA.

Step 3: Next covariance is calculated by following two formulas for segments $v = 1, 2, \ldots, N$ and for segments $v = N_s + 1, N_s + 2, \ldots, 2N_s$ respectively:

$$F_{XY}^2(s, v) = \frac{1}{s} \sum_{j=1}^{s} \left| X_{(v-1)s+j} - \widehat{X}_j^v \right| \cdot \left| Y_{(v-1)s+j} - \widehat{Y}_j^v \right| \tag{14}$$

$$F_{XY}^2(s, v) = \frac{1}{s} \sum_{j=1}^{s} \left| X_{N-(v-N_s)s+j} - \widehat{X}_j^v \right| \cdot \left| Y_{N-(v-N_s)s+j} - \widehat{Y}_j^v \right| \tag{15}$$

In the above formulas $\hat{X}_j^v$ and $\hat{Y}_j^v$ denote the fitting polynomials in segment v with order m. In this study fitting polynomial order m is selected as one.

Step 4: In the next step fluctuation function with order q, $F_{XY}^q(s)$, is computed by averaging all segments using following two formulas for $q \neq 0$ and $q = 0$ respectively:

$$F_{XY}^q(s) = \left(\frac{1}{2N_s} \sum_{v=1}^{2N_s} \left[F_{XY}^2(s, v) \right]^{q/2} \right)^{1/q} \tag{16}$$

$$F_{XY}^q(s) = \exp \left(\frac{1}{4N_s} \sum_{v=1}^{2N_s} \left[F_{XY}^2(s, v) \right] \right) \tag{17}$$

Step 5: By analyzing logarithm plots of $F_{XY}^q\ (s)$ versus logarithm s the scaling behavior of the fluctuation function is determined for each value of q. If the considered series are power-law cross-correlated, there is a power-law relationship expressed as below:

$$F_X Y^q \ (s) \ s^(h_X Y \ (q)) \tag{18}$$

In the expression above $h_{XY}(q)$ represents generalized correlation exponent which reflects the power-law relationship. If $h_{XY}(q)$ depends on q then correlation between the two time series is multifractal. However, if $h_{XY}(q)$ is independent of q then correlation is monofractal.

Similar to MF-DFA multifractal spectrum $f_{XY}(\alpha)$ can be obtained from following formulas:

$$\alpha_{XY}(q) = h_{XY}(q) + qh'_{XY}(q) \tag{19}$$

$$f_{XY}(\alpha) = q[\alpha_{XY}(q) - h_{XY}(q)] + 1 \tag{20}$$

The term $h'_{XY}(q)$ in the expression above refers to the derivative of $h_{XY}(q)$ with regard to q. The $\alpha_{XY}\,(q)$ is called Hölder exponent and reflects the power of the singularity. Also, width of the multifractal spectrum $(\Delta\alpha)$ indicates strength of multifractality.

DATA AND PRELIMINARY ANALYSIS

In this study hourly data for EUR/TRY and USD/TRY exchange rates are utilized. The dataset comprises 23600 observations and spans period between 2018-05-31 13:01 and 2022.03.21 08:01:00. The data is sourced from GCM Forex company. Two types of data analyses were conducted in this study: whole-period analysis and rolling window analysis. In the rolling window analysis, a window size of 4,000 observations was selected, with a sliding step of 400 observations. The changes in exchange rates in the whole period are depicted in Figure 1 and Figure 2. Summary statistics for exchange rates are also presented in Table 1. As shown in Table 1 both exchange rates exhibit right-skewed distributions. Additionally, both exchange rates are leptokurtic and possess fat tailed distributions. Since one source of multifractality is fat tailed distribution, we can anticipate multifractality in both exchange rates. In Figure 3 and Figure 4 autocorrelations for exchange rates are plotted.

As evident in these figures, significant autocorrelations are observed in EUR/TRY and USD/TRY exchange rates up to lags 8,653 and 8,804, respectively. Therefore, there are long-range autocorrelations in both exchange rates. Since another source of multifractality is long-range autocorrelation, we can expect multifractality in these exchange rates. Long-range autocorrelation can lead to multifractality because it can create a heterogeneous distribution of the values of the time series. This heterogeneous distribution can lead to different scaling behaviors over different time intervals. For example, if the values of a time series are clustered together above the mean, then the time series will be more volatile over short time intervals. This is because the values of the time series are more likely to change rapidly when they are clustered together.

On the other hand, if the values of a time series are clustered together below the mean, then the time series will be more volatile over long time intervals. This is because the values of the time series are more likely to change slowly when they are clustered together. Therefore, long-range autocorrelation can lead to multifractality by creating a heterogeneous distribution of the values of the time series. This heterogeneous distribution can lead to different scaling behaviors over different time intervals (Jafari *et al.* 2007; Dashtian *et al.* 2011; Tanna and Pathak 2014). In our preliminary analysis we calculated fractal dimensions for USD/TRY and EUR/TRY exchange rates using Box-count estimator, Hall-Wood estimator, Wavelet estimator and DCT-II estimator (Gneiting *et al.* 2012) and presented the results in Table 2. To illustrate how these fractal dimensions change over time, we applied a rolling window analysis and displayed the findings in Figure 5 and Figure 6. As evident from Table 2 and Figures 5-6, both USD/TRY and EUR/TRY exchange rates exhibit fractal (non-integer) dimensions.

EMPIRICAL RESULTS

In this study firstly MFDFA is applied to exchange rates individually. In individual analyzes firstly, multifractality is investigated for the whole dataset. Secondly, a rolling window methodology is used to investigate how multifractal properties change over time and to assess the contributions of long-range autocorrelation and fat-tailed distribution to multifractality. Afterwards, MF-DCCA is applied to both EUR/TRY and USD/TRY exchange rates. In this Section firstly MF-DCCA is applied to whole dataset to examine the multifractal properties of the complete dataset. Secondly, using a rolling window methodology, changes in the cross-correlation multifractality between the exchange rates over time are examined. Additionally, the study explores how contributions of long-range autocorrelation and fat-tailed distribution to cross-correlation multifractality change over time.

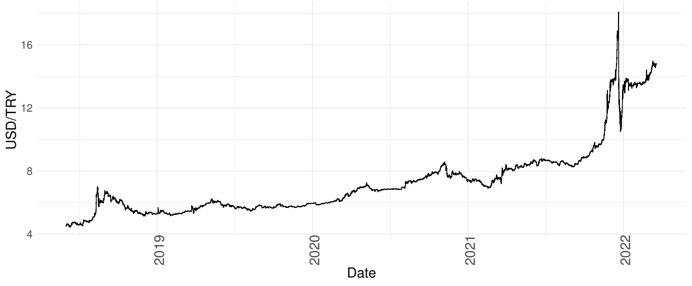


Figure 1 USD/TRY Exchange rate

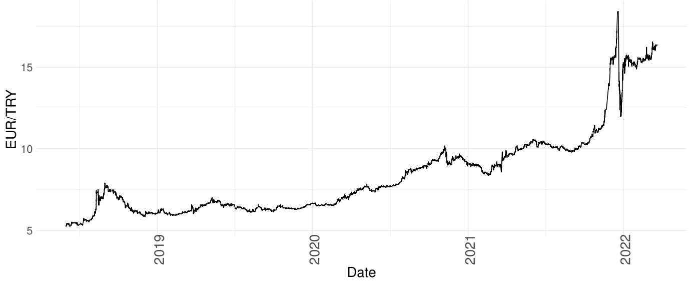


Figure 2 EUR/TRY Exchange rate

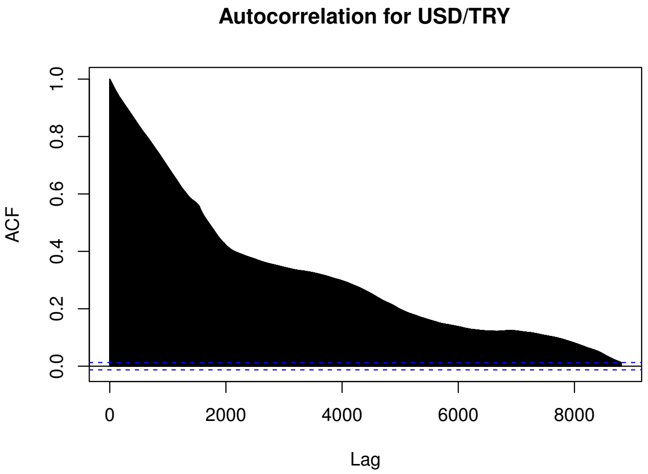


Figure 3 Autocorrelation for USD/TRY exchange rate

In order to apply MFDFA and MF-DCCA methods three parameter values must be determined: vector of scales, q-order of the moment (q) and polynomial order for the detrending (m). In both whole period analysis and rolling window analysis q-order of the moment values are selected from -10 to +10 in steps of 1 including zero and polynomial order for the detrending is set to 1. However, in whole period analysis scales values are selected from 100 to 5900 in steps of 10 and in rolling window analysis scales

Table 1 Descriptive Statistics

Exchange Rate	Min	1st Q.	Median	Mean	3st Q.	Max	Std. Dev.	Skewness	Kurtosis
USD/TRY	4.451	5.738	6.792	7.302	8.203	18.080	2.3026	1.72126	5.7037
EUR/TRY	5.253	6.387	7.532	8.392	9.747	18.413	2.6457	1.44015	4.6592

Table 2 Fractal Dimensions

Method	USD/TRY	EUR/TRY
Box-count estimator	1.328052	1.316235
Hall-Wood estimator	1.510337	1.480936
Wavelet estimator	1.518846	1.405108
DCT-II estimator	1.526528	1.435383

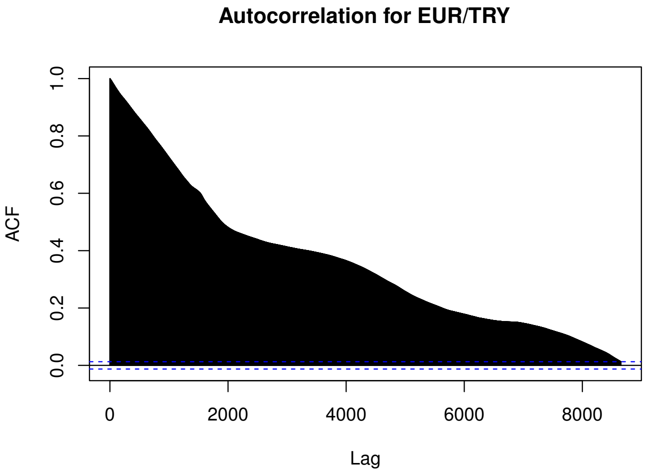


Figure 4 Autocorrelation for EUR/TRY exchange rate

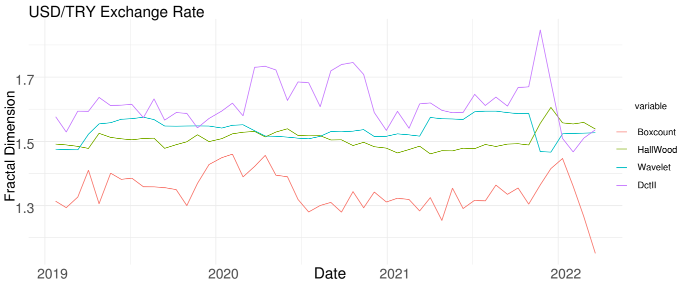


Figure 5 Change in fractal dimensions for USD/TRY exchange rate

values are selected from 10 to 400 in steps of 10. In our analysis to measure the level of multifractality $(\Delta\alpha)$ values are utilized. To illustrate how individual and cross correlated multifractality levels of the exchange rates change over time we presented the changes in $(\Delta\alpha)$ values within a rolling window framework.

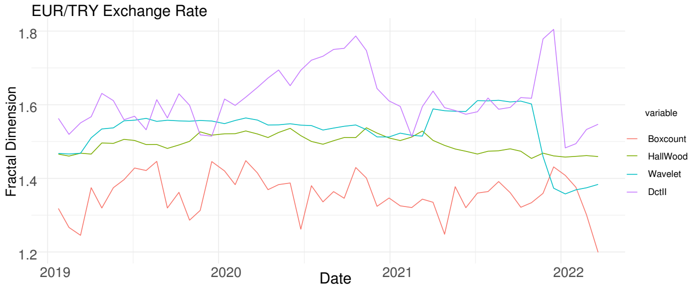


Figure 6 Change in fractal dimensions for EUR/TRY exchange rate

In the literature, not only the level of multifractality but also the factors contributing to multifractality has been investigated. Multifractality is primarily influenced by two factors. These are fat-tailed distribution and long-range autocorrelation. To measure the contribution of these two causes to the multifractality, surrogate and shuffled data are generated and utilized. In the generation of shuffled data autocorrelations are destroyed but the distribution is preserved. After generation of shuffled data, $(\Delta\alpha_{S}huffled)$ Shuffled value is calculated from this shuffled data. Eventually, when $(\Delta\alpha_{S}huffled)$ Shuffled is subtracted from original $(\Delta\alpha)$ value, long-range autocorrelations' contribution to the multifractality are obtained.

Another factor that contributes to multifractality is the presence of a fat-tailed distribution. To assess the multifractality's contribution from the fat-tailed distribution, surrogate data is employed. Surrogate data is generated by using a phase randomization procedure. In this procedure fat-tails in the distribution is eliminated but linear properties of the distribution are preserved. To evaluate contribution of fat tails to the multifractality, $(\Delta\alpha_{S}urrogate)$ surrogate value is calculated from surrogate data. Subsequently, $(\Delta\alpha_{S}urrogate)$ Surrogate value is subtracted from original $(\Delta\alpha)$ value to calculate contribution of fat tails to the multifractality.

In next sections to illustrate how the contributions of long-range autocorrelation factor and fat-tailed distribution factor to multifractality change over time fifty shuffled time series and fifty surrogate time series are generated for each time window and $(\Delta\alpha)$ values are calculated for each of the fifty series. Subsequently, mean and standard deviation values of fifty $(\Delta\alpha)$ parameters for shuffled and surrogate series are calculated in each time window. Since MF-DCCA method requires two time series we generated fifty pairs of surrogate and shuffled time series to explore the contributions of fat-tailed distribution and long-range autocorrelation to multifractality of the cross-correlations. By utilizing the means and standard deviations of $(\Delta\alpha)$ values calculated from surrogate and shuffled time series, contributions of two factors to the multifractality are examined. We generated multiple shuffled and surrogate series because in each realization different series are obtained. Therefore, multiple surrogate and shuffled series are required for robust results.

MF-DFA of USD/TRY Exchange Rate

Firstly, we analyzed multifractality of USD/TRY exchange rate by using whole period data. The results are presented in Figure 7. Upper left panel of Figure 7 indicates logarithm–logarithm plots of fluctuation function $F_q(s)$ versus time scale s for q values equal to 10, 0 and -10. The linearity of points in this graph reveals presence of power-law cross-correlations between time scale and fluctuation function. The upper right panel of Figure 7 illustrates how the Hurst exponent changes for various values of q. The Hurst exponents do not remain constant across a range of q values, leading us to the conclusion that the USD/TRY exchange rate exhibits multifractality.

Additionally, for q = 2 Hurst exponent is computed as 0.5268 which is slightly higher than 0.5, indicating a very weakly persistent time series. Lower left panel of Figure 7 shows how mass exponent change for different values of q. Since mass exponent nonlinearly depends on q, this provides further evidence of multifractality of USD/TRY exchange rate. Lower right panel of Figure 7 presents multifractal spectrum of USD/TRY exchange rate. Here width of the multifractal spectrum $(\Delta\alpha)$ reveals the level of multifractality and a positive $(\Delta\alpha)$ value indicates the existence of multifractality. Also, since α_0 value is higher than 0.5 there is persistent long-range correlations in the USD/TRY exchange rate series. Left-skewed spectrum implies that large fluctuations are dominant in the time series.

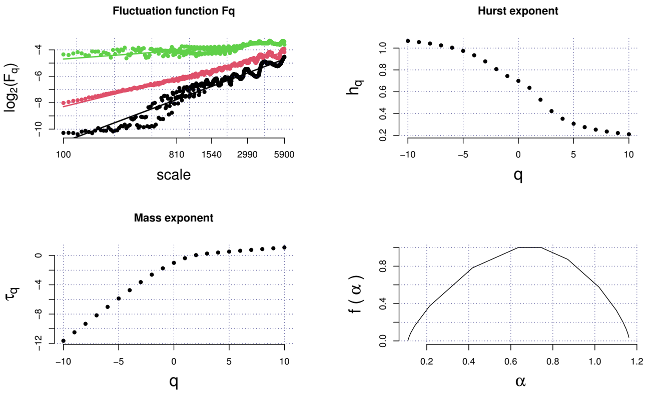


Figure 7 Change in fractal dimensions for USD/TRY exchange rate

To explore how the level of multifractality for USD/TRY exchange rate change over time we illustrated how multifractal spectrum $(\Delta\alpha)$ change over time in a rolling window framework. Results are depicted in Figure 8 and Figure 9 with black curves. In these figures with dots on black curve fifty original $(\Delta\alpha)$ values are presented and each of these corresponds to single time window. When the original $(\Delta\alpha)$ values are examined three different regimes in terms of multifractality are distinguished. In period between 2018-05-31 13:01 and 2020-06-24 13:01 and in period between 2020-07-17 06:01 and 2022-03-21 08:01 multifractality levels of USD/TRY exchange are higher than the period between 2019-11-22 19:01 and 2021-02-16 12:01. Also, there is a noticeable peak in the multifractality in the period between 2018-08-09 13:01 and 2019-04-04 00:01. Moreover, there is a collapse in the multifractality in the period between 2021-04-27 15:01 and 2021-12-16 10:01.

In our analysis we generated 50 shuffled and 50 surrogate series for each time window to illustrate how the contribution of long-range autocorrelation and fat-tailed distribution to multifractality change over time. Mean $(\Delta\alpha_{S}urrogate)$ values of surrogate series computed in each time window are shown with a blue curve in Figure 8 and mean $(\Delta\alpha_{S}huffled)$ values of shuffled series computed in each time window are shown with a blue curve in Figure 9. Red error bars represent ±1 standard deviations of generated surrogate and shuffled series in each time window.

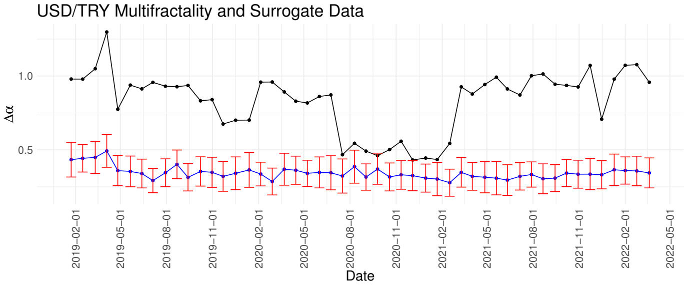


Figure 8 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from surrogate data

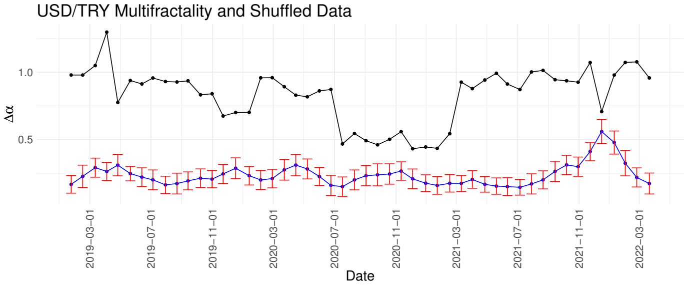


Figure 9 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from shuffled data

To assess the change in the contribution of fat-tailed distribution to multifractality we subtracted mean values of $(\Delta\alpha_{S}urrogate)$ obtained from surrogate data from original $(\Delta\alpha)$ values and presented this in Figure 10. In this figure, high values indicate a strong fat-tailed distribution's contribution to the multifractality, while low values indicate a low fat-tailed distribution's contribution to the multifractality. As seen from Figure 10 fat-tailed distribution's contribution to the multifractality is weakened in the period between 2019-11-22 19:01 and 2021-02-16 12:01.

Furthermore, to assess the change in long-range correlation's contribution to multifractality mean $(\Delta\alpha_{S}huffled)$ values obtained from shuffled data are subtracted from original $(\Delta\alpha)$ values. The results are illustrated in Figure 11. In this figure each value represents contribution level of long-range autocorrelation to multi-

Table 3 Multifractality regimes in USD/TRY exchange rate

$(\Delta\alpha)$	1. Regime	2. Regime	3. Regime
Mean	0.8966261	0.4876900	0.9534882
Variance	0.016327789	0.002052737	0.007530036

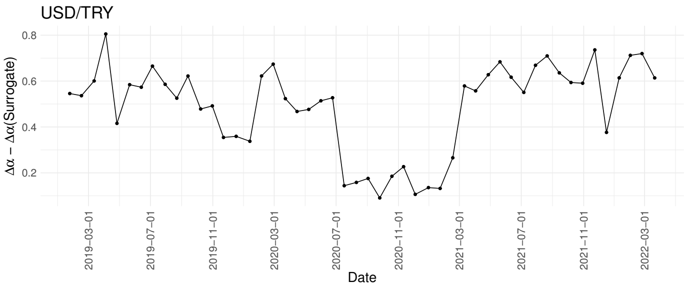


Figure 10 Change in the fat-tailed distribution's multifractality contribution

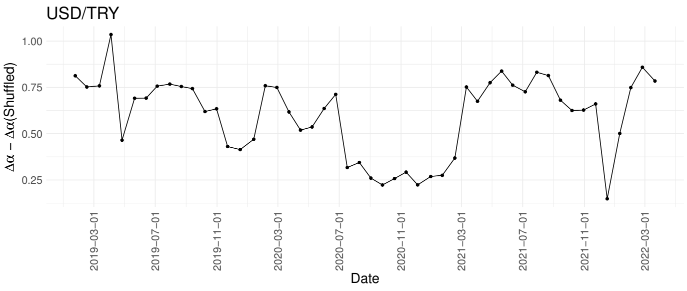


Figure 11 Change in the multifractality's long-range autocorrelation contribution

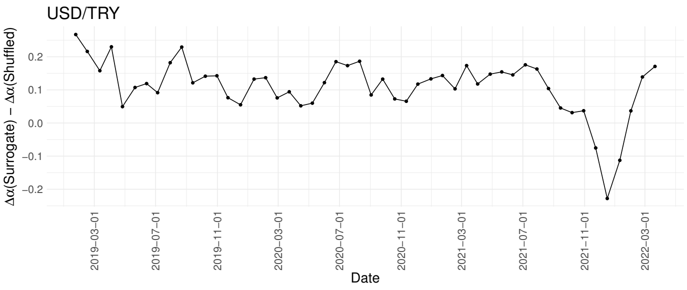


Figure 12 Examining the impacts of fat-tailed distribution and long-range autocorrelation on multifractality

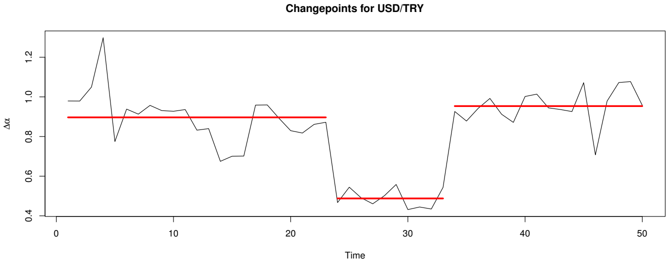


Figure 13 Change points in multifractality of USD/TRY exchange rate

fractality. This figure reveals that the long-range autocorrelation's contribution to multifractality is once again weakened between 2019-11-22 19:01 and 2021-02-16 12:01. Additionally, the contribution of long-range autocorrelation to multifractality shows a striking decline between 2021-04-27 15:01 and 2021-12-16 10:01.

Figure 12 is presented to compare the contributions of the fat-tailed distribution and long-range autocorrelation to the multifractality. This figure illustrates the difference between mean $(\Delta\alpha_{S}urrogate)$ value obtained from surrogate data and mean $(\Delta\alpha_{S}huffled)$ value obtained from shuffled data. Positive values in Figure 12 indicate that the long-range autocorrelation has a greater contribution to the multifractality than the fat-tailed distribution. Figure 12 reveals that, except for the time period from 2021-04-02 23:01 to 2022-01-10 06:01, long-range autocorrelation contributes more to multifractality than the fat-tailed distribution.

To detect change points and regimes in the level of multifractality in USD/TRY exchange rate binary segmentation algorithm is applied (Scott and Knott 1974; Sen and Srivastava 1975). We identified two change points in the 23rd and 33rd windows, resulting in three regimes. Results are presented in Table 3 and Figure 13.

MF-DFA of EUR/TRY Exchange Rate

Multifractal analysis results for EUR/TRY exchange rate covering whole period data are presented in Figure 14. Upper left panel of Figure 14 displays power-law cross-correlations between time scale s and fluctuation function $F_q(s)$ for q values equal to 10, 0 and -10. Upper right panel of Figure 14 reveals a varying Hurst exponent according to value of q, providing evidence for multifractality. Additionally, Hurst exponent for q = 2 is computed as 0.5637, slightly higher than 0.5, indicating a weakly persistent time series. Notably, this Hurst exponent value of 0.5637 is greater than the Hurst exponent value of 0.5268 for the USD/TRY exchange rate, indicating that the EUR/TRY exchange rate is more persistent than the USD/TRY exchange rate. As observed in the lower left panel of Figure 14 mass exponents are nonlinear, providing further evidence of multifractality. The lower right panel of Figure 14 displays the multifractal spectrum of the EUR/TRY exchange rate. Here positive value for $(\Delta\alpha)$ indicates evidence for multifractality.

Additionally, since α_0 value is higher than 0.5 there is persistent long-range correlations in the EUR/TRY exchange rate series. The left-skewed spectrum suggests that large fluctuations dominate the time series.

Similar to the USD/TRY exchange rate, to illustrate how multifractality level for the EUR/TRY exchange rate change over time Figure 15 and Figure 16 presented. In these figures black curves represents $(\Delta\alpha)$ values calculated from original data. As observed in these figures level of multifractality is maximum in the period between 2018-05-31 13:01 and 2019-01-23 22:01. After 2018-05-31 13:01 there is steady decline in multifractality until 2019-07-30 08:01. In the period between 2018-12-29 00:01 and 2019-10-31 01:01 slightly higher values and a horizontal trend are observed for multifractality. In the period between 2019-04-04 01:01 and 2020-09-02 13:01 multifractality remains relatively flat and low. After 2020-02-05 11:01 an upward trend is observed until 2021-10-30 01:00. However, in the period between 2021-04-27 15:01 and 2021-12-16 10:01 a collapse in the multifractality is observed.

To reveal contributions of long-range autocorrelation and fat-tailed distribution to multifractality 50 shuffled time series and 50 surrogate time series are generated in each time window. Mean values of $(\Delta\alpha_{S}urrogate)$ calculated from surrogate series in each time window is presented in Figure 15 with blue curve and mean values of $(\Delta\alpha_{S}huffled)$ calculated from shuffled series in each time window is also presented in Figure 16 with blue curve. In these figures error bars represent ±1 standard deviations of $(\Delta\alpha_{S}urrogate)$ and $(\Delta\alpha_{S}huffled)$ values obtained from surrogate and shuffled series.

To demonstrate how contribution of fat-tailed distribution to multifractality is change over time Figure 17 is plotted. To obtain this figure mean $(\Delta\alpha_{S}urrogate)$ values obtained from surrogate series are subtracted from original $(\Delta\alpha)$ values. As observed in Figure 17 contribution of fat-tailed distribution to multifractality is highest in period between 2018-05-31 13:01 and 2019-01-23 22:01. Following this period, the fat-tailed distribution's contribution to multifractality decreased. After 2020-02-05 11:01 a steady increase in the fat-tailed distribution's contribution to multifractality is observed. However, between 2021-04-27 15:01 and 2021-12-16 10:01, there appears to have been a decline in the fat-tailed distribution's contribution to multifractality.

The change in the contribution of long-range autocorrelation to multifractality over time is presented in Figure 18. In this figure, it can be observed that the long-range correlation's contribution to multifractality is highest in the early period and gradually decreases untill 2019-05-21 8:01. After this date two relatively horizontal trend periods are distinguished. First horizontal trend period is between 2019-04-04 01:01 and 2021-03-11 04:01. Second horizontal trend period is between 2020-08-10 22:01 and 2021-10-30 01:00. Additionally, between 2021-04-27 15:01 and 2021-12-16 10:01, there is a collapse in the long-range correlation's contribution to multifractality. This period also corresponds to a decline in the contribution of long-range autocorrelation to multifractality.

Comparison between contributions of long-range autocorrelation and fat-tailed distribution to multifractality is presented in Figure 19. Positive values in this figure indicate that the long-range autocorrelation has a greater contribution to the multifractality than the fat-tailed distribution. Figure 19 remains relatively flat and have positive values until the date 2021-11-23 18:01. This indicates that long-range autocorrelation has been the primary source of multifractality up to this point. However negative values are observed in this figure during the period between 2021-04-27 15:01 and 2022-01-10 06:01. These negative values indicate that the fat-tailed distribution now contributes more to multifractality than long-range autocorrelation does.

To detect change points and regimes in the level of multifractality in EUR/TRY exchange rate, a binary segmentation algorithm is applied (Scott and Knott 1974; Sen and Srivastava 1975). We detected three change points in 4th, 13th and 34th windows, resulting in four regimes. Results are presented in Table 4 and Figure 20.

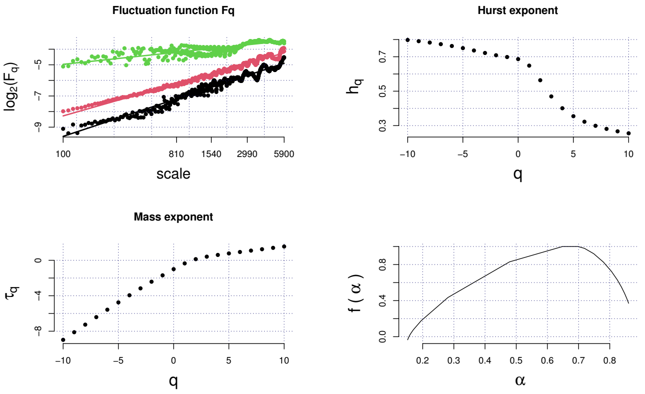


Figure 14 Whole period multifractality of EUR/TRY exchange rate

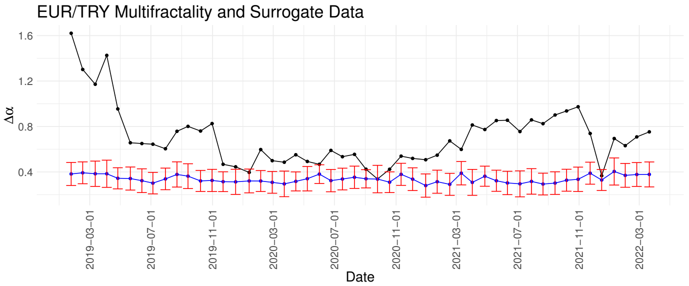


Figure 15 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from surrogate data

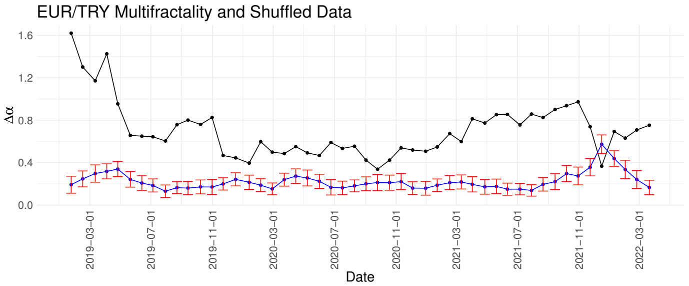


Figure 16 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from shuffled data

MF-DCCA of USD/TRY and EUR/TRY Exchange Rates

In this stage, the EUR/TRY and USD/TRY exchange rates are studied using multifractal detrended cross-correlation analysis. Firstly, results from whole dataset are presented.

Table 4 Multifractality regimes in EUR/TRY exchange rate

$(\Delta\alpha)$	1. Regime	2. Regime	3. Regime	4. Regime
Mean	1.3802250	0.7392889	0.5069429	0.7771875
Variance	0.027409312	0.011176401	0.005778175	0.019095466

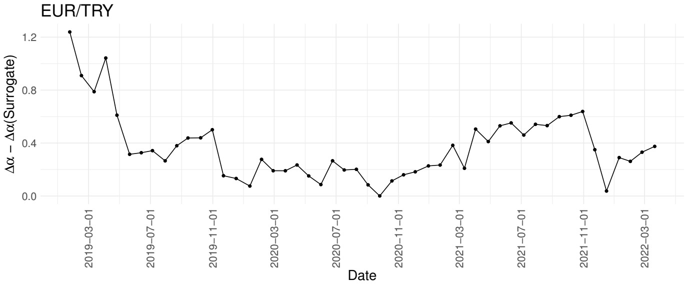


Figure 17 Change in the fat-tailed distribution's multifractality contribution

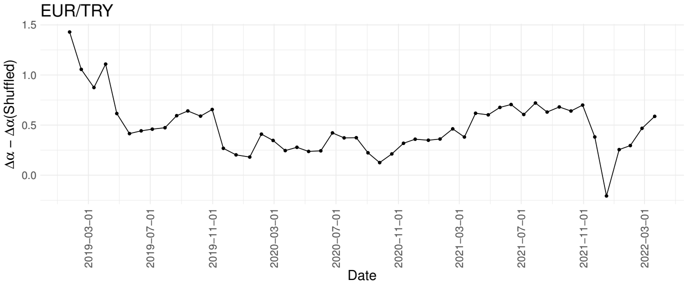


Figure 18 Change in the multifractality's long-range autocorrelation contribution

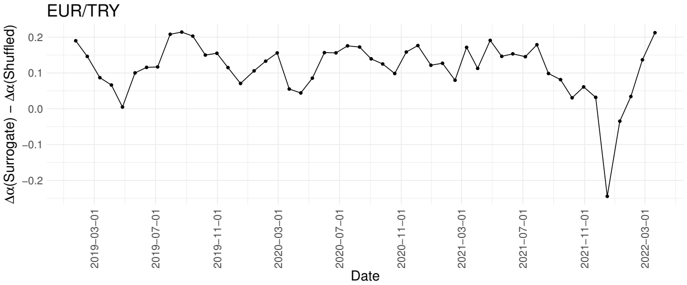


Figure 19 Examining the impacts of fat-tailed distribution and long-range autocorrelation on multifractality

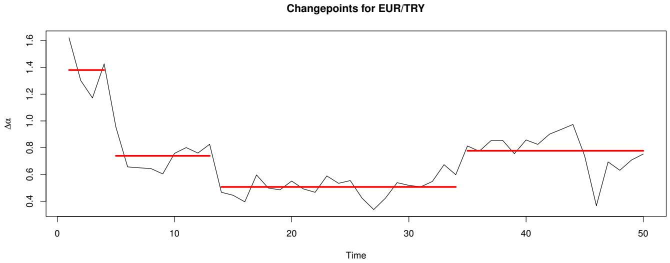


Figure 20 Change points in multifractality of EUR/TRY exchange rate

In Figure 21 relationships between time scale s and fluctuation function for q values equal to 10, 0 and -10 are plotted. The linearity of these points indicates that there is a power-law relationship between these two values. In Figure 22 generalized cross-correlation exponent between the two exchange rates are presented. In this figure, since generalized cross-correlation exponents are dependent on q values, it suggests that the cross-correlation between the exchange rates is multifractal. Additionally, for logarithm difference data, generalized cross-correlation exponent for q=2 is computed as 0.5393, slightly higher than 0.5, indicating that the cross-correlated series has a weak persistent structure. The multifractal spectrum for cross-correlation between USD/TRY and EUR/TRY exchange rates is shown in Figure 23. In this figure it can be observed that width of the multifractal spectrum $(\Delta\alpha)$ is positive, providing further evidence for multifractality in the cross-correlation. Moreover, since α_0 value is greater than 0.5, it indicates the presence of persistent long-range correlations.

In MF-DCCA level of correlation multifractality between two exchange rate series can be measured with the multifractal spectrum's width $(\Delta\alpha)$. In this part we demonstrated how multifractality level of cross correlation between the two exchange rates and source of multifractality change over time in a rolling window framework.

Long-range autocorrelation and fat-tailed distribution are the two sources of multifractality for cross correlation. To measure the contribution of these sources shuffled time series and surrogate time series are utilized. However, in MF-DCCA, since there must be two series, 50 pairs of surrogate series and 50 pairs of shuffled series are generated for each time window. The $(\Delta\alpha_Surrogate)$ values obtained from pairs of surrogate series are presented in Figure 24 and $(\Delta\alpha_Shuffled)$ values obtained from pairs of shuffled series are presented in Figure 25 with blue curves. In these figures red error bars represent ±1 standard deviation.

When Figure 24 and Figure 25 are examined, a downward trend in multifractality for original series is observed in the period between 2018-05-31 13:01 and 2021-01-22 20:01. In the period between 2020-06-01 22:01 and 2021-04-02 22:01 there is a rapid rise in multifractality. Also, in the period between 2020-08-10 22:01 and 2021-10-30 01:01 a gradual increase in multifractality is observed. However, there is a collapse in multifractality during the period between 2021-04-27 15:01 and 2021-12-16 10:01.

Figure 26 is presented to examine how the fat-tailed distribution's contribution to the multifractality changes over time. Additionally, Figure 27 is presented to reveal how the contribution of long-range correlation to multifractality changes over time. These two figures display similar pattern. In both Figure 26 and Figure 27 there are significant collapse in contributions to multifractality during the period between 2021-04-27 15:01 and 2021-12-16 10:01.

To compare fat-tailed distribution's and long-range autocorrelation's contributions to multifractality Figure 28 is presented. Positive values in this figure indicate that the long-range autocorrelation has a greater contribution to the multifractality than the fat-tailed distribution. When examining this figure, a negative value is observed for the period between 2021-04-27 15:01 and 2021-12-16 10:01. This negative value suggests that the fat-tailed distribution's contribution to multifractality has surpassed the long-range correlation's contribution. Apart from this period, dominant source of multifractality is long-range correlation.

To identify change points and regimes in the level of cross correlation multifractality between exchange rates a binary segmentation algorithm is applied (Scott and Knott 1974; Sen and Srivastava 1975). We detected seven change points in 5th, 13th, 16th, 23th, 34th, 42th, and 47th windows, resulting in eight regimes. Results are presented in Table 5 and Figure 29.

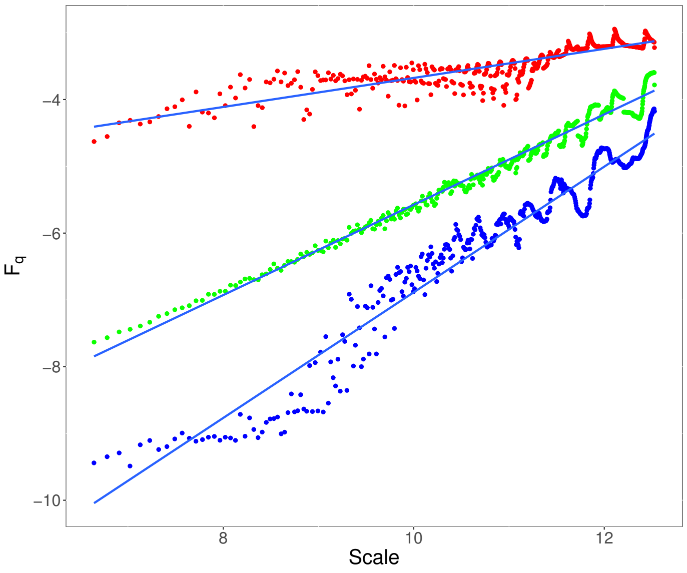


Figure 21 Fluctuation function for cross correlation

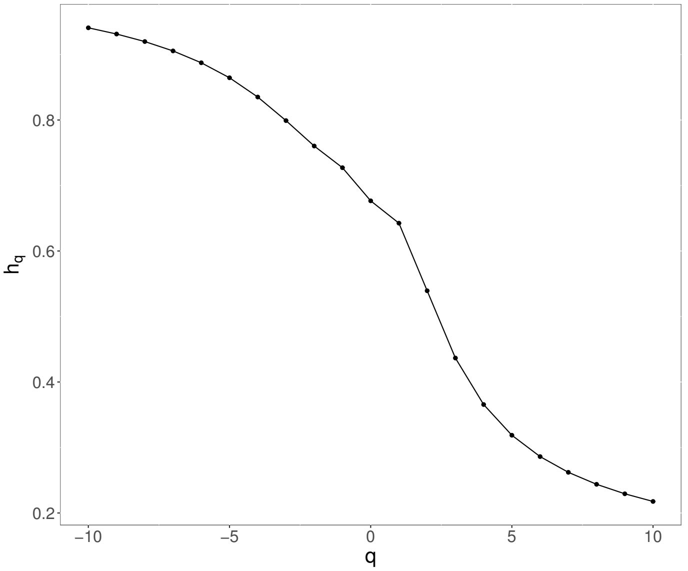


Figure 22 Generalized cross-correlation exponent between EUR/TRY and USD/TRY exchange rates

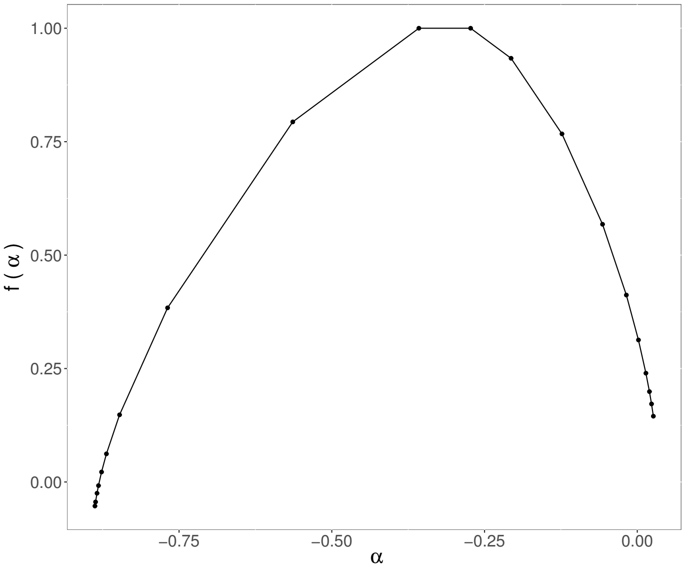


Figure 23 Multifractal spectrum for cross-correlation between EUR/TRY and USD/TRY exchange rates

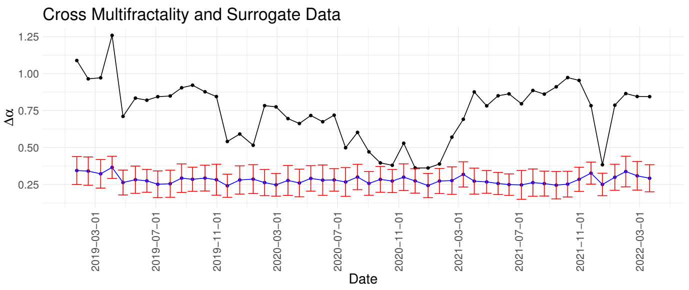


Figure 24 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from surrogate data

Table 5 Multifractality regimes in EUR/TRY exchange rate

$(\Delta\alpha)$	1. Regime	2. Regime	3. Regime	4. Regime	5. Regime	6. Regime	7. Regime	8. Regime
Mean	0.9991	0.8620	0.5493	0.7182	0.4773	0.8532	0.7763	0.8518
Variance	3.22e-02	1.11e-03	1.00e-03	1.86e-03	1.13e-02	1.68e-03	4.50e-02	9.31e-05

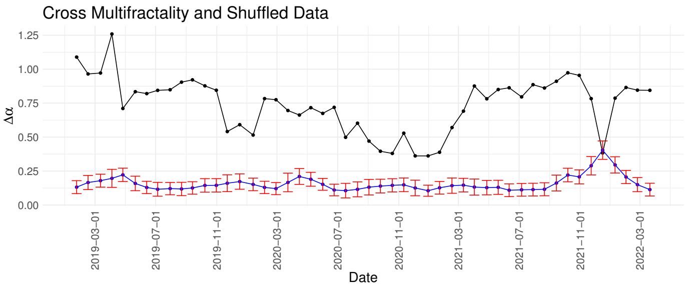


Figure 25 Change in $(\Delta\alpha)$ calculated from original data and change in $(\Delta\alpha)$ calculated from shuffled data

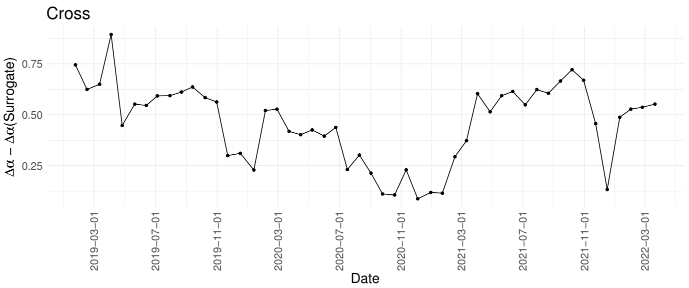


Figure 26 Change in the fat-tailed distribution's multifractality contribution

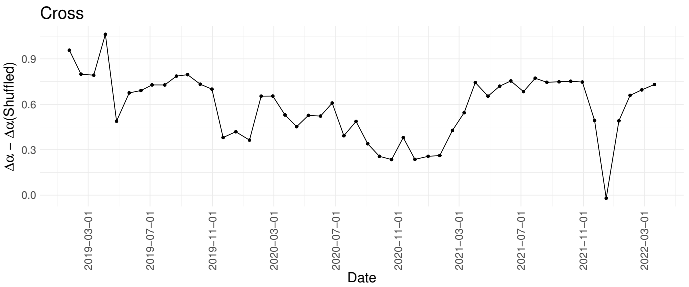


Figure 27 Change in the multifractality's long-range autocorrelation contribution

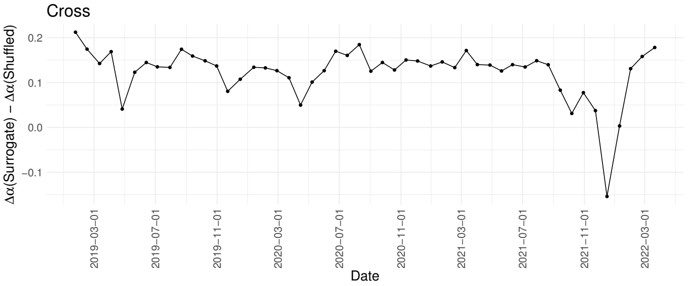


Figure 28 Examining the impacts of fat-tailed distribution and long-range autocorrelation on multifractality

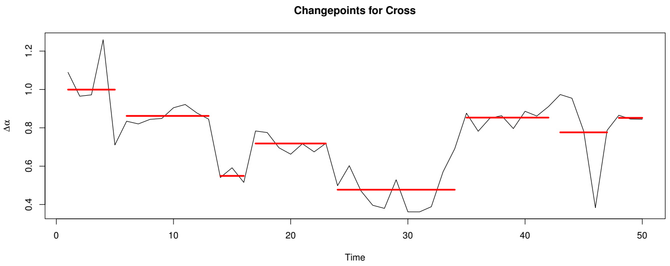


Figure 29 Change points in cross-correlation multifractality

CONCLUSION

A multifractal system is a general type of fractal system in which the system cannot be adequately described by a single exponent. In the literature, it has been demonstrated that many systems from different fields exhibit multifractality. In this study individual and cross correlation multifractality of EUR/TRY and USD/TRY exchange rates are explored with MF-DFA and MF-DCCA methodologies. In the analysis both whole period data and rolling window data are utilized. Whole period analyses reveal that the two exchange rates as well as correlation between the exchange rates are multifractal.

Multifractality in these exchange rates implies presence of inefficiencies which can be exploited by investors. These inefficiencies can be exploited by investors who are able to identify them and trade accordingly. For example, investors who believe that the volatility of a particular exchange rate is about to increase may choose to sell that currency, while investors who believe that the volatility is about to decrease may choose to buy that currency. Advanced trading algorithms can be designed to detect and act upon multifractal patterns in exchange rates. Multifractality can create arbitrage opportunities where an asset's price differs on different time scales or in different markets.

Arbitrageurs can profit from these price differentials by buying low and selling high. By using rolling window method, we illustrated how multifractal properties of the exchange rates change over time. As indicated by $(\Delta\alpha)$ values multifractality levels of the exchange rates change over time and higher multifractal levels implies higher complexity, higher risks and more violent fluctuations. Additionally, we examined how contributions of long-range autocorrelation and fat-tailed distribution to multifractality change over time. Shape of the singularity spectra for exchange rates suggests that large fluctuations are more dominant in EUR/TRY exchange rate than USD/TRY exchange rate.

Our results suggest that long-range autocorrelation's contribution to multifractality is higher than the fat-tailed distribution's contribution except during the period between 2021-04-27 15:01 and 2021-12-16 10:01. Therefore, dominant source of multifractality is the long-range autocorrelation. However, when the multifractality of the two exchange rates are examined a collapse in the multifractality is observed during in the period between 2021-04-27 15:01 and 2021-12-16 10:01. Moreover, in this period, contribution of fat-tailed distribution to multifractality become dominant. As evident from Figure 1 and Figure 2, during this period, both USD/TRY and EUR/TRY exchange rates exhibit significant instability, and there is substantial government intervention in the foreign exchange market. Since USD/TRY and EUR/TRY exchange rates are multifractal and characterized by autocorrelation, non-linearity, and long memory (persistence), traditional efficient markets hypothesis which assumes normal distribution and linearity is not appropriate for these exchange rates.

The implications of multifractality of USD/TRY and EUR/TRY exchange rates are significant and can impact various areas within finance, economics, and decision-making. Multifractal behavior suggests that exchange rate movements are not only random but also characterized by irregular patterns and fluctuations across different time scales. This complexity can lead to unexpected and extreme price movements, which are important considerations for risk assessment and management. Multifractality for these exchange rates implies that the volatility of these exchange rates can vary depending on the time scale being considered. This makes it difficult to predict the future volatility of these exchange rates, and it can also make it difficult to trade these exchange rates profitably. Also, the multifractality of these exchange rates suggests that they are not efficient markets. This means that there are opportunities to make profits by exploiting the inefficiencies in these markets.

However, these opportunities are often difficult to find and exploit, and they can also be risky. Multifractal analysis can provide insights for traders and algorithmic trading systems. By understanding the non-linear dynamics of exchange rates, traders can develop strategies that adapt to the multifractal nature of the market, potentially improving trading outcomes. Traditional linear models may not fully capture the complexities of multifractal behavior. The findings from multifractal analysis can lead to the development of more sophisticated models that better reflect the true nature of exchange rate movements. Multifractal behavior can affect portfolio diversification strategies. Investors need to consider how different assets, including USD/TRY and EUR/TRY exchange rates, interact and exhibit multifractal patterns to effectively manage risk and optimize returns. Multifractality in exchange rates can have policy implications for central banks and governments. Understanding the intricate and non-linear behaviors of currencies can inform decisions related to monetary policy, trade agreements, and economic interventions. The recognition of multifractal behavior can influence how financial markets are regulated. Regulators might need to consider the implications of non-linear and complex behaviors for market stability and investor protection.

In the future studies how multifractality and its sources evolve over longer time periods can be investigated. Comparative analysis with other currency pairs or financial assets can be conducted to identify commonalities and differences in multifractal behavior. The impact of external factors, such as geopolitical events, economic policies, or global financial crises, on the multifractality of exchange rates can be explored. Machine learning techniques to enhance the prediction and forecasting capabilities based on multifractal properties can be incorporated.

Availability of data and material

Not applicable.

Conflicts of interest

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

LITERATURE CITED

Ashkenazy, Y., P. C. Ivanov, S. Havlin, C.-K. Peng, A. L. Goldberger, *et al.*, 2001 Magnitude and sign correlations in heartbeat fluctuations. Physical Review Letters **86**: 1900.

Blesić, S., S. Milošević, D. Stratimirović, and M. Ljubisavljević, 1999 Detrended fluctuation analysis of time series of a firing fusimotor neuron. Physica A: Statistical Mechanics and its Applications **268**: 275–282.

Buldyrev, S., N. Dokholyan, A. Goldberger, S. Havlin, C.-K. Peng, *et al.*, 1998 Analysis of dna sequences using methods of statistical physics. Physica A: Statistical Mechanics and its Applications **249**: 430–438.

Bunde, A., S. Havlin, J. W. Kantelhardt, T. Penzel, J.-H. Peter, *et al.*, 2000 Correlated and uncorrelated regions in heart-rate fluctuations during sleep. Physical review letters **85**: 3736.

Caraiani, P. and E. Haven, 2015 Evidence of multifractality from cee exchange rates against euro. Physica A: Statistical Mechanics and its Applications **419**: 395–407.

Chen, S.-P. and L.-Y. He, 2010 Multifractal spectrum analysis of nonlinear dynamical mechanisms in china's agricultural futures markets. Physica A: Statistical Mechanics and its Applications **389**: 1434–1444.

Dashtian, H., G. R. Jafari, M. Sahimi, and M. Masihi, 2011 Scaling, multifractality, and long-range correlations in well log data of large-scale porous media. Physica A: Statistical Mechanics and its Applications **390**: 2096–2111.

Fama, E. F., 1965 The behavior of stock-market prices. The journal of Business **38**: 34–105.

Gneiting, T., H. Ševčíková, and D. B. Percival, 2012 Estimators of fractal dimension: Assessing the roughness of time series and spatial data. Statistical Science pp. 247–277.

Gülbaş, E. and Ü. Gazanfer, 2013 Multifractal analysis of the dynamics of turkish exchange rate. International Journal of Economics and Finance Studies **5**: 96–107.

Han, C., Y. Wang, and Y. Ning, 2019 Comparative analysis of the multifractality and efficiency of exchange markets: Evidence from exchange rates dynamics of major world currencies. Physica A: Statistical Mechanics and its Applications **535**: 122365.

He, L.-Y. and S.-P. Chen, 2010a Are crude oil markets multifractal? evidence from mf-dfa and mf-ssa perspectives. Physica A: Statistical Mechanics and its Applications **389**: 3218–3229.

He, L.-Y. and S.-P. Chen, 2010b Are developed and emerging agricultural futures markets multifractal? a comparative perspective.

Physica A: Statistical Mechanics and its Applications **389**: 3828–3836.

Hu, K., P. C. Ivanov, Z. Chen, P. Carpena, and H. E. Stanley, 2001 Effect of trends on detrended fluctuation analysis. Physical Review E **64**: 011114.

Hurst, H. E., 1951 Long-term storage capacity of reservoirs. Transactions of the American society of civil engineers **116**: 770–799.

Hurst, H. E., 1957 A suggested statistical model of some time series which occur in nature. Nature **180**: 494–494.

Jafari, G. R., P. Pedram, and L. Hedayatifar, 2007 Long-range correlation and multifractality in bach's inventions pitches. Journal of Statistical Mechanics: Theory and Experiment **2007**: P04012.

Kantelhardt, J. W., E. Koscielny-Bunde, H. H. Rego, S. Havlin, and A. Bunde, 2001 Detecting long-range correlations with detrended fluctuation analysis. Physica A: Statistical Mechanics and its Applications **295**: 441–454.

Kantelhardt, J. W., D. Rybski, S. A. Zschiegner, P. Braun, E. Koscielny-Bunde, *et al.*, 2003 Multifractality of river runoff and precipitation: comparison of fluctuation analysis and wavelet methods. Physica A: Statistical Mechanics and its Applications **330**: 240–245.

Kantelhardt, J. W., S. A. Zschiegner, E. Koscielny-Bunde, S. Havlin, A. Bunde, *et al.*, 2002 Multifractal detrended fluctuation analysis of nonstationary time series. Physica A: Statistical Mechanics and its Applications **316**: 87–114.

Li, J., X. Lu, and Y. Zhou, 2016 Cross-correlations between crude oil and exchange markets for selected oil rich economies. Physica A: Statistical Mechanics and its Applications **453**: 131–143.

Lim, K.-P. and R. Brooks, 2011 The evolution of stock market efficiency over time: A survey of the empirical literature. Journal of economic surveys **25**: 69–108.

Liu, Y., P. Gopikrishnan, H. E. Stanley, *et al.*, 1999 Statistical properties of the volatility of price fluctuations. Physical review e **60**: 1390.

Lu, X., J. Li, Y. Zhou, and Y. Qian, 2017 Cross-correlations between rmb exchange rate and international commodity markets. Physica A: Statistical Mechanics and its Applications **486**: 168–182.

Ma, F., Y. Wei, and D. Huang, 2013a Multifractal detrended cross-correlation analysis between the chinese stock market and surrounding stock markets. Physica A: Statistical Mechanics and its Applications **392**: 1659–1670.

Ma, F., Y. Wei, D. Huang, and L. Zhao, 2013b Cross-correlations between west texas intermediate crude oil and the stock markets of the bric. Physica A: Statistical Mechanics and its Applications **392**: 5356–5368.

Ma, F., Q. Zhang, C. Peng, and Y. Wei, 2014 Multifractal detrended cross-correlation analysis of the oil-dependent economies: Evidence from the west texas intermediate crude oil and the gcc stock markets. Physica A: Statistical Mechanics and its Applications **410**: 154–166.

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

Matia, K., Y. Ashkenazy, and H. E. Stanley, 2003 Multifractal properties of price fluctuations of stocks and commodities. Europhysics letters **61**: 422.

Movahed, M. S., G. Jafari, F. Ghasemi, S. Rahvar, and M. R. R. Tabar, 2006 Multifractal detrended fluctuation analysis of sunspot time series. Journal of Statistical Mechanics: Theory and Experiment **2006**: P02003.

Peng, C.-K., S. V. Buldyrev, S. Havlin, M. Simons, H. E. Stanley, *et al.*, 1994 Mosaic organization of dna nucleotides. Physical review e **49**: 1685.

Peters, E. E., 1994 *Fractal market analysis: applying chaos theory to investment and economics*, volume 24. John Wiley & Sons.

Schmitt, F., D. Schertzer, and S. Lovejoy, 1999 Multifractal analysis of foreign exchange data. Applied stochastic models and data analysis **15**: 29–53.

Scott, A. J. and M. Knott, 1974 A cluster analysis method for grouping means in the analysis of variance. Biometrics pp. 507–512.

Sen, A. and M. S. Srivastava, 1975 On tests for detecting change in mean. The Annals of statistics pp. 98–108.

Stošić, D., D. Stošić, T. Stošić, and H. E. Stanley, 2015 Multifractal analysis of managed and independent float exchange rates. Physica A: Statistical Mechanics and its Applications **428**: 13–18.

Talkner, P. and R. O. Weber, 2000 Power spectrum and detrended fluctuation analysis: Application to daily temperatures. Physical Review E **62**: 150–160.

Tanna, H. and K. Pathak, 2014 Multifractality due to long-range correlation in the l-band ionospheric scintillation s 4 index time series. Astrophysics and Space Science **350**: 47–56.

Telesca, L., V. Lapenna, and M. Macchiato, 2004 Mono-and multifractal investigation of scaling properties in temporal patterns of seismic sequences. Chaos, Solitons & Fractals **19**: 1–15.

Wang, Y., Y. Wei, and C. Wu, 2011a Analysis of the efficiency and multifractality of gold markets based on multifractal detrended fluctuation analysis. Physica A: Statistical Mechanics and its Applications **390**: 817–827.

Wang, Y., Y. Wei, and C. Wu, 2011b Detrended fluctuation analysis on spot and futures markets of west texas intermediate crude oil. Physica A: Statistical Mechanics and its Applications **390**: 864–875.

Xie, C., Y. Zhou, G. Wang, and X. Yan, 2017 Analyzing the cross-correlation between onshore and offshore rmb exchange rates based on multifractal detrended cross-correlation analysis (mf-dcca). Fluctuation and Noise Letters **16**: 1750004.

Yen, G. and C.-f. Lee, 2008 Efficient market hypothesis (emh): past, present and future. Review of Pacific Basin Financial Markets and Policies **11**: 305–329.

Yue, P., H.-C. Xu, W. Chen, X. Xiong, and W.-X. Zhou, 2017 Linear and nonlinear correlations in the order aggressiveness of chinese stocks. Fractals **25**: 1750041.

Zhuang, X., Y. Wei, and F. Ma, 2015 Multifractality, efficiency analysis of chinese stock market and its cross-correlation with wti crude oil price. Physica A: Statistical Mechanics and its Applications **430**: 101–113.

Zhuang, X., Y. Wei, and B. Zhang, 2014 Multifractal detrended cross-correlation analysis of carbon and crude oil markets. Physica A: Statistical Mechanics and its Applications **399**: 113–125.

Zunino, L., A. Figliola, B. M. Tabak, D. G. Pérez, M. Garavaglia, *et al.*, 2009 Multifractal structure in latin-american market indices. Chaos, Solitons & Fractals **41**: 2331–2340.

How to cite this article: Unal, B. Time-Varying Fractal Analysis of Exchange Rates. *Chaos Theory and Applications*, 5(3), 242-255, 2023.

Licensing Policy: The published articles in *Chaos Theory and Applications* are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

e-ISSN: 2687-4539
ERRATUM
Vol.5 / **No.**3 / 2023 / **pp.**256

ERRATUM

Published in Volume 5, Issue 1, 2023; The corrections made in the article titled "**Analysis of Nonlinear Mathematical Model of COVID-19 via Fractional-Order Piecewise Derivative**" are as follows. Affiliations have been corrected due to the request of the authors. You can access the first version of the article from the link below.

Paper URL: https://dergipark.org.tr/en/pub/chaos/issue/75756/1210461

Muhammad Sinan [*,1], **Kamal Shah** [α,β,2], **Thabet Abdeljawad** [β,3] **and Ali Akgül** [§,4]
[*]School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu 611731, China, [β]Department of Mathematics and Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia, [α]Department of Mathematics, University of Malakand, Chakdara Dir (Lower), Khyber Pakhtunkhawa, Pakistan, [§]Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon; Siirt University, Art and Science Faculty, Department of Mathematics, 56100 Siirt, Türkiye; Near East University, Mathematics Research Center, Department of Mathematics, Near East Boulevard, PC: 99138, Nicosia / Mersin-10, Türkiye.

---

[1] sinanmathematics@gmail.com
[2] kamalshah408@gmail.com
[3] tabdeljawad@psu.edu.sa
[4] aliakgul00727@gmail.com (**Corresponding Author**)