

An Opamp-Based Coexisting Chaotic Attractors Used in IoT Secure Data Communication

Dr.M. Anbarasan^{1*}, Dr. Gobalakrishnan Natesan², and Dr.S. Prakash³

^{1*}Professor, Department of Computer Science Engineering, Saveetha Engineering College, Tamil Nadu, India. anbarasan.cse@gmail.com, <https://orcid.org/0000-0002-2828-9016>

²Professor, Department of Computer Science Engineering, Saveetha Engineering College, Tamil Nadu, India. gobalakrishnanse@gmail.com, <https://orcid.org/0000-0003-3820-6744>

³Professor, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Tamil Nadu, India. prakash.sav4@gmail.com, <https://orcid.org/0000-0001-7799-4582>

Received: September 22, 2025; Revised: October 27, 2025; Accepted: December 23, 2025; Published: February 27, 2026

Abstract

In this research paper, an opamp-based simple chaotic circuit is designed exhibiting coexisting chaotic attractors with application in IoT secure data communication is presented. It is interestingly, that this circuit with, only three multipliers and with a few opamps was implemented with OrAD-Pspice, which displays a chaotic attractor. And the coexisting phenomena were also observed by varying initial conditions. This implies it increases the encryption space for IoT secure communication. Finally, an application in IoT for secure data communication, an analog circuit was implemented using the chaotic Masking method. The proposed chaotic masking was verified for single encryption, and double encryption and the original data was decrypted at the receiver successfully using OrAD-Pspice. However, we also prove that when the encrypted signal was decrypted with a different encryption signal other than the transmitted encryption signal, the original signal was not decrypted successfully at the receiver. Also, the proposed coexisting chaotic circuit can be easily manufactured at low cost because of simple circuit implementation compared to nano-based devices such as memristor.

Keywords: OPAMP, Data Communication, Encryption, and Decryption.

1 Introduction

The IoT-based devices have tremendously increased nowadays are predicted to grow over \$69 billion by 2024 (Hedayatipour et al., 2020). These types of IoT devices are interfaced with Transducers for sensing information from the environment and transmitting the information for analysis to the receiver side for further processing of signals. Also, with Smart wearables (Wang et al., 2022), heart rhythm devices, and both bio-fluidic and On-body devices are concerned with production and their privacy and security (Wen et al., 2021). Therefore, for robust communication against security attacks. Hence, device duplication poses risk-sensitive challenges that must be carefully managed. In communication-based chaos techniques, systems have unpredictable signals, a wide spectrum, and a self-synchronization property widely utilized to transmit secure communication (Al Momin, 2022; Zhong & Ayrom, 1985).

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 311-322.
DOI: 10.58346/JISIS.2026.11.018

*Corresponding author: Professor, Department of CSE, Saveetha Engineering College, Tamil Nadu, India.

Also, these systems are much cheaper compared to spread spectrum techniques used in wireless communication (Volkovskii et al., 2005). It is considered a preferred option for ensuring robust communication (Duan et al., 2022; Vishwakarma et al., 2023) in the presence of eavesdroppers. Furthermore, chaos-based methods have been proposed as potential alternatives in the realm of post-quantum cryptography (Onuki et al., 2022). While advancements have been made in chaos-based communication such as the development of hyperchaos (Xianhui et al., 2024; Nataliya et al., 2024) and systems with coexisting attractors (Shi et al., 2025; Subbulaxmi et al., 2024; Prabu et al., 2024) limited attention has been given to securing the design and production of Chaotic hardware communication circuits fabricated by potentially unreliable foundries (Rezaei et al., 2019; Anand et al. 2025). Chaotic system synchronization helps toward improvement in the application of IoT-based secure communication (Rahul et al., 2023). Many encryption standards are available for digital transmission, such as AES, RSA, and Lorenz masking (Kaplan & Yorke, 1979), which require complex circuits to be implemented. Furthermore, compared to AES and RSA, the proposed op-amp-based chaotic system offers lower hardware complexity, reduced cost, and continuous-time operation suitable for analog domains. Unlike Lorenz masking, it uses a custom chaotic attractor, increasing resistance to system identification. Although it does not match the formal security guarantees of AES or RSA, it provides a lightweight and low-power alternative for secure data masking, key stream generation, or random number production in resource-constrained or real-time analog environments. Hence, we have the unique advantage of our coexisting attractor over the above-mentioned cryptography, such as highly customizable, simple structure, no digital logic needed, fast to prototype, and unpredictability of chaos. Motivated by the above issues and research perspective, the following objectives are decided for this work (Ganesh et al., 2025; Stankevich et al., 2024).

1. To investigate a simple opamp-based autonomous chaotic system and also increase encryption space because of its sensitivity to initial conditions.
2. Analog circuit design and implementation in the OrCAD-PSpice platform.
3. Synchronization between the proposed chaotic system and its use in IoT data communication with single and double encryption using the OrCAD-PSpice platform.

The following paper is arranged as: the introduction and dynamical behaviors of the proposed coexisting attractor system and its sensitivity to initial conditions are presented in Section 2. In Section 3, the analog circuit is designed for the proposed chaotic system using OrCAD-PSpice. In Section 4, application to IoT secure communication is explored using OrCAD-PSpice for the proposed coexisting attractor system. Finally, conclusions are summarized.

2 Chaotic System Description

The dynamic system of equations and its description

$$\dot{x}_1 = 0.2x_1 + x_2 \quad (1)$$

$$\dot{x}_2 = -\frac{1}{3}x_1 - \frac{1}{3}x_2x_3^2 \quad (2)$$

$$\dot{x}_3 = -0.4x_2 - 0.4x_3 + x_2x_3 \quad (3)$$

2.1 Stability Analysis

The stability of the proposed coexisting attractor is obtained by equating $\dot{x}_1 = 0, \dot{x}_2 = 0, \dot{x}_3 = 0$. Three equilibria are given as

$$\begin{cases} E_1 = [0,0,0]^T \\ E_2 = [-2.4357, 0.4871, 2.2361]^T \\ E_3 = [-1.6965, 0.3393, -2.2361]^T \end{cases}$$

At $E_1 = (0, 0, 0)$, the Jacobian linearization of the system is achieved as:

$$J_{E_1} = \begin{bmatrix} 0.2 & 1 & 0 \\ -\frac{1}{3} & -\frac{1}{3}x_3^2 & -\frac{2}{3}x_2x_3 \\ 0 & -0.4 + x_3 & -0.4 + x_2 \end{bmatrix}$$

Eigen values are calculated as $\lambda_{1,2} = 0.1 + 0.5686i$, $\lambda_3 = -0.4$. Therefore, the equilibrium point has saddle focus. Similarly, the equilibrium point E_2 is calculated as $\lambda_{1,2} = -0.7796 + 0.9368i$, $\lambda_3 = 0.1795$, and the equilibrium point E_3 is determined. Eigen values are $\lambda_{1,2} = -0.8427 + 0.9892i$, $\lambda_3 = 0.1579$, which also exhibit a saddle focus nature about the equilibrium points E_2 and E_3 . It is concluded that the system has three saddle focus behaviors.

2.2 Lyapunov Exponents and Dimension

The coexisting attractor system are verified for chaotic behaviour using lyapunov exponents. As shown in Figure 1, the Lyapunov exponents are $L_1 = 0.031556$, $L_2 = 0.006926$, and $L_3 = -0.401371$. The signa of LE as $[+, 0, -]$ signifies chaotic behaviour. The Lyapunov dimensions [16] indicated below

$$L_D = 2 + \frac{1}{(L_3)} \sum_{i=1}^2 L_i = 2 + \frac{0.03155}{0.40137} = 2.0786$$

The fractional value of the Lyapunov dimension confirms chaotic behavior.

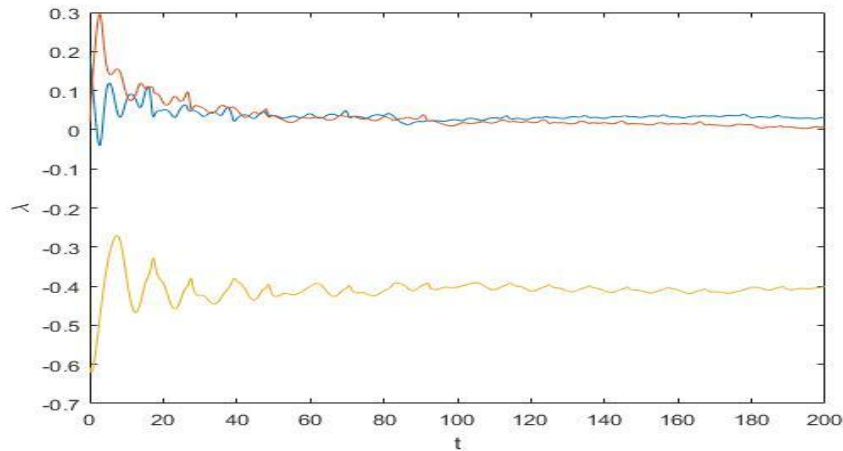


Figure 1: Dynamical behavior of lyapunov exponents (LEs)

Table 1: Varying initial conditions, the proposed system exhibits chaotic behavior

S. No	x1, x2, x3	S. No	x1, x2, x3	S. No	x1, x2, x3
1	(0, -0.1, -0.1)	6	(-0.1, -0.1, 0)	11	(-0.1, 0, 0.1)
2	(0, 0.1, -0.1)	7	(-0.1, 0.1, 0)	12	(-0.1, 0, 0.1)
3	(0, -0.1, 0.1)	8	(0.1, -0.1, 0)	13	(0.1, 0, 0.1)
4	(0, 0.1, 0.1)	9	(0.1, 0.1, 0)	14	(-0.1, -0.1, -0.1)
5	(0, 0.1, 0)	10	(0.1, 0, 0)	15	(0, 0, -0.1)
				16	(0, -0.1, 0)
				17	(-0.1, 0, 0)

Chaotic systems are susceptible to slightly varying the initial conditions and may result in significantly diverse outputs in the state behaviors. Two very close initial conditions are considered as $[0 \ -0.1 \ -0.1]^T$ and $[0 \ -0.10001 \ -0.10001]^T$. Figure 2 shows the MATLAB-simulation of the proposed chaos system. The change of the initial condition is made in the fifth decimal place, and the simulation result shown in Figure 3 reveals that the two behaviors excited at different initial conditions are identical till $t=220$ seconds, and after that, the chaotic behaviors are quite different from each other. Furthermore, from the different initial conditions as listed in Table 1. Whereas in Figure 4, the simulation result reveals that the two behaviors excited at different initial conditions, say for example $([0 \ 0.1 \ 0.1], [0 \ -0.1 \ -0.1])$ show the chaotic behavior deviation starts at $t=0$ itself. These phenomena are also called coexisting chaotic attractors (Prabu et al., 2024). This, implies that the encryption space gets enhanced for use in IoT secure communication for the same proposed chaotic system (Zhou et al., 2024).

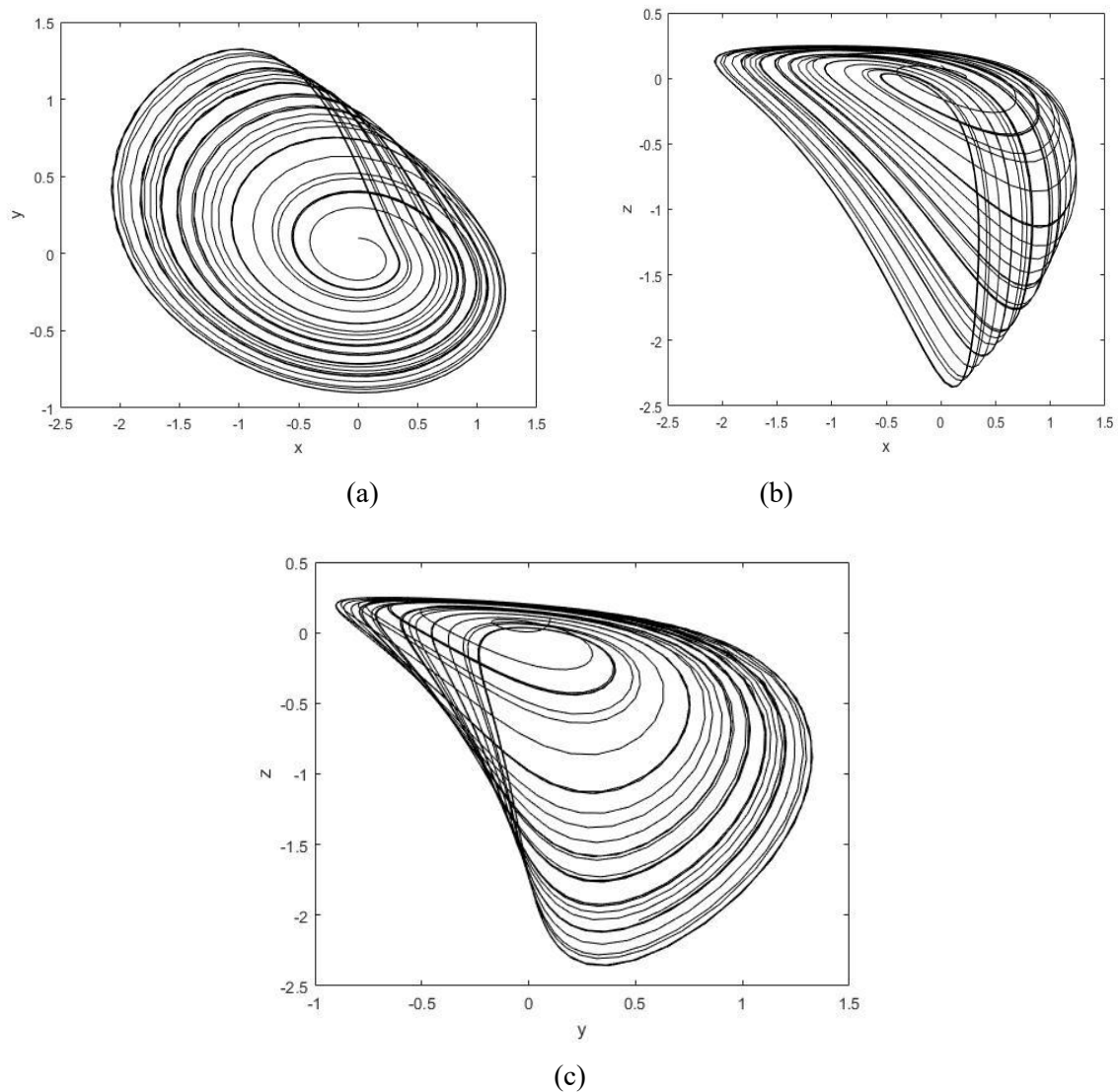


Figure 2: Phase diagram plots using MATLAB simulated for (a) $x_1 - x_2$ phase, (b) $x_2 - x_3$ phase, and (c) $x_1 - x_3$ phase

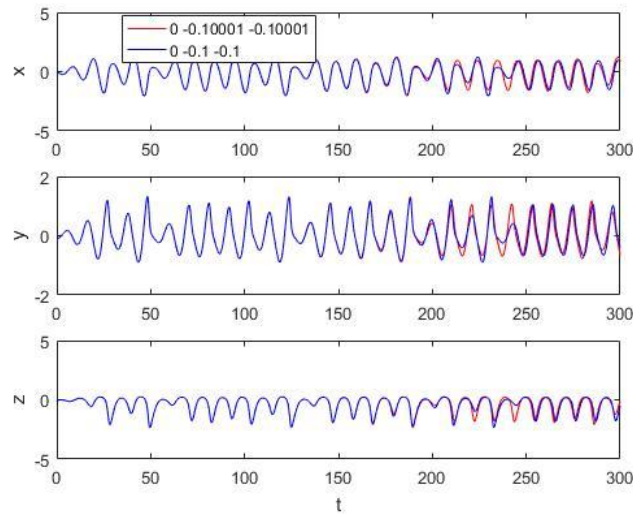


Figure 3: Shows sensitivity in the initial condition. There are changes the time response of $x(t)$ after $t=220s$ with a small change in initial conditions

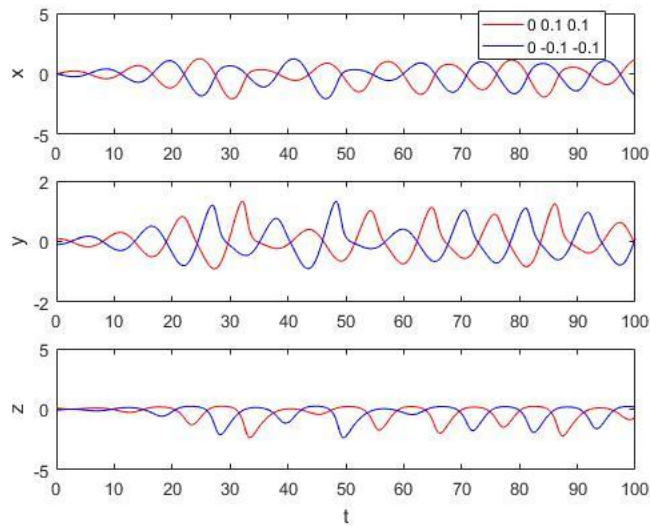


Figure 4: Shows sensitivity in the initial condition. There are abrupt changes in the time response of $x(t)$ from $t=0s$ with different initial conditions

3 Circuit Design

The proposed chaotic system is designed using analog components, i.e., resistances, capacitances, and opamps of different values in OrCAD-PSpice.

$$\begin{cases} \frac{dx_1}{dt} = \frac{1}{R_1 C_1} x_1 + \frac{1}{R_2 C_1} x_2 \\ \frac{dx_2}{dt} = \frac{-1}{R_3 C_2} - \frac{1}{R_4 C_2} x_2 x_3^2 \\ \frac{dx_3}{dt} = \frac{-1}{R_5 C_3} x_2 - \frac{1}{R_6 C_3} x_3 + \frac{1}{R_7 C_3} x_2 x_3 \end{cases}$$

The analog implementation is shown in Figure 5. The component values are given as: $C_i = 10\text{nF}$ ($i=1, 2, 3$). $R_1=100\text{ k}\Omega$, $R_2=R_7=20\text{ k}\Omega$, $R_3=R_4=60\text{ k}\Omega$, $R_5=R_6=50\text{ k}\Omega$. Phase plane behaviors of the coexisting attractor system are shown in OrCAD-PSpice, as given in Figure 6. Furthermore, the coexisting proposed attractor system displayed in OrCAD-PSpice, as given in Figure 7. The simulated phase plots are very similar to the MATLAB-simulated ones.

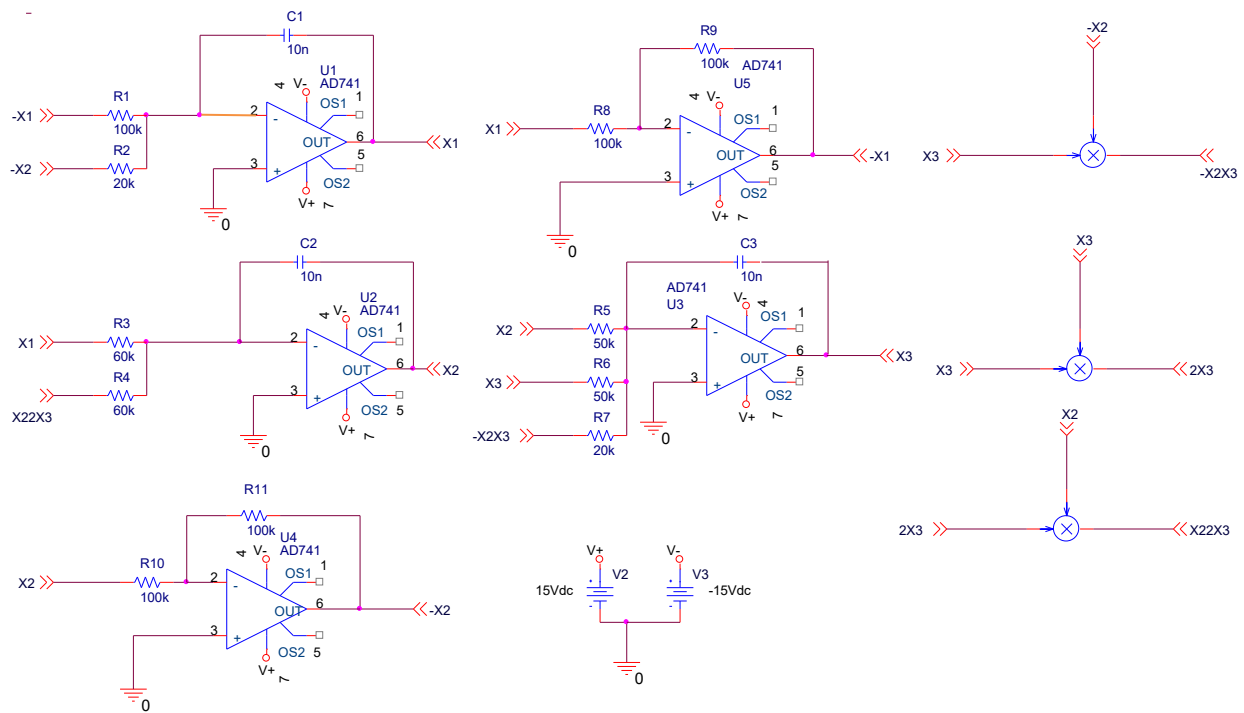


Figure 5: Analog circuit diagram of the proposed chaotic oscillator

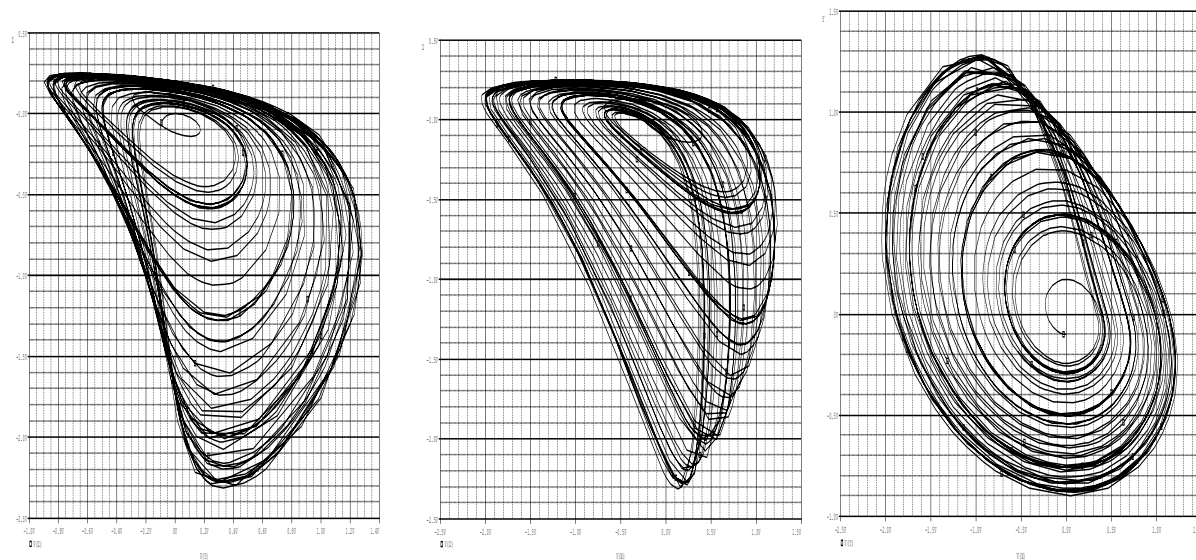


Figure 6: Phase diagram plots using ORCAD-PSpice for (a) x_1 - x_2 phase, (b) x_2 - x_3 phase, and (c) x_1 - x_3 phase plane

4 Chaotic Secure Communication

The proposed communication setup using the chaotic masking method (Ouannas et. al., 2021; Liu & Zhang, 2011) is shown in Figure 7. The masking of the message with a carrier chaos signal at the transmission side. Unmasking of the original signal can be achieved, if synchronization between the chaotic systems is achieved at the receiver end. A information signal $m(t)=1v$ with a square pulse of 50% duty cycle is added with x_2 state at the transmitter end and termed as transmitted content $i_T = (x_2 + m)$. At the reception side, the received message is decrypted successfully as $\hat{m}(t) = i_T - x_2$ synchronization The original signal and recovered message signal are shown in Figure 8. However, it should be observed when the transmitted signal (i_T) was recovered with a different state signal, for example, with x_3 , i.e. $\hat{m}(t) = i_T - x_3$. The original message was not decrypted successfully at the receiver, as shown in Figure 9.

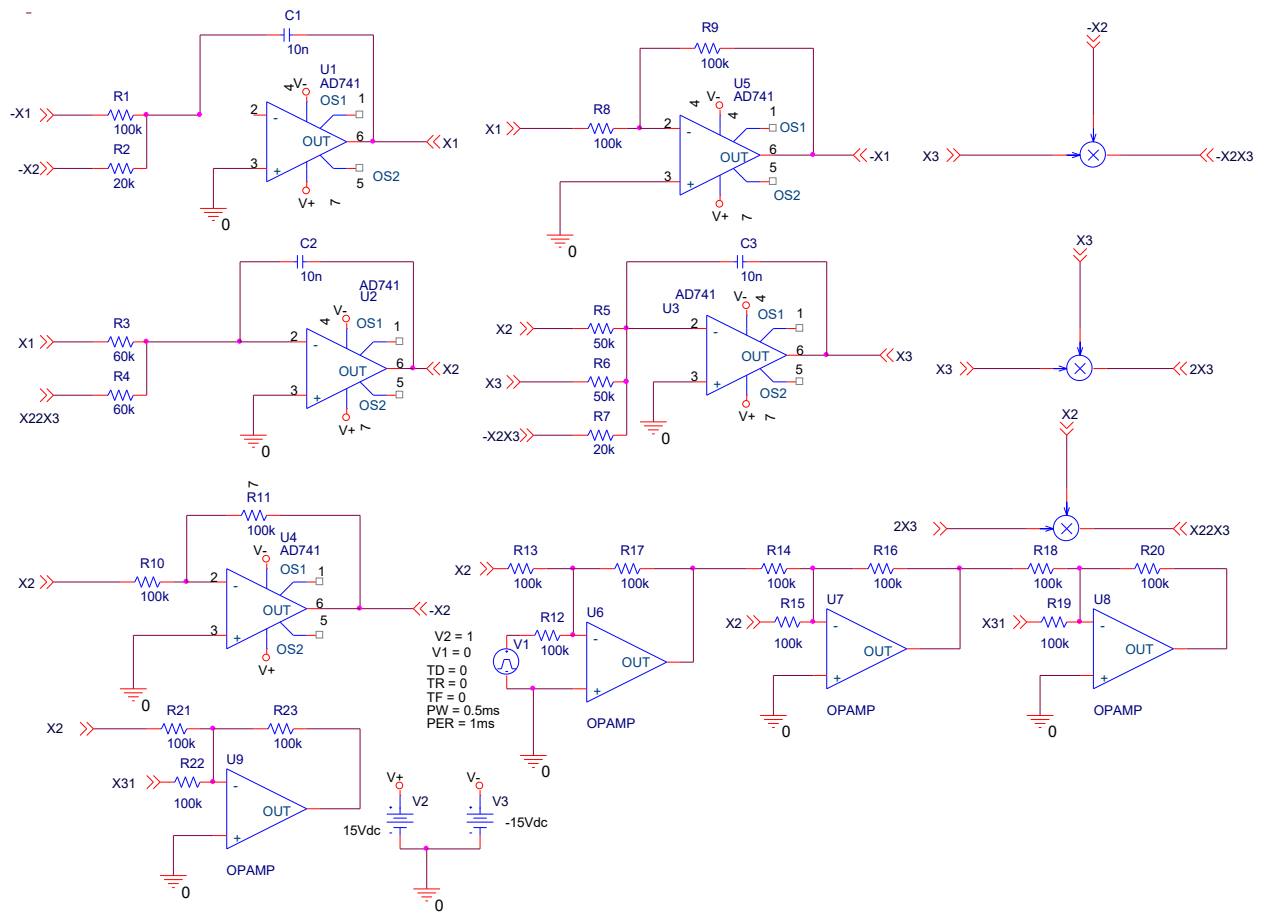


Figure 7: Analog circuit diagram of the chaotic masking method for secure communication in an IoT application using ORCAD-PSpice

Furthermore, the proposed communication setup for the double encryption chaotic masking method synchronization is shown in Figure 10. The information signal $m(t)=1v$ square wave pulse of 50% duty cycle was added with two state signals, and the transmitted signal $i_T = (x_2 + x_3 + m)$. At the receiver end, the received message is decrypted successfully, as synchronization $\hat{m}(t) = i_T - x_2 - x_3$ shown in

Figure 11. The proposed double encryption makes it difficult for an intruder to decipher two different chaotic signals, facilitating powerful encryption of the information or message signal during IoT secure communication. Figure 12 proved that the transmission $I(t)$ and reception $R(t)$ are truly match each other. Also, the difference error is nearly zero as displayed in Figure 12.

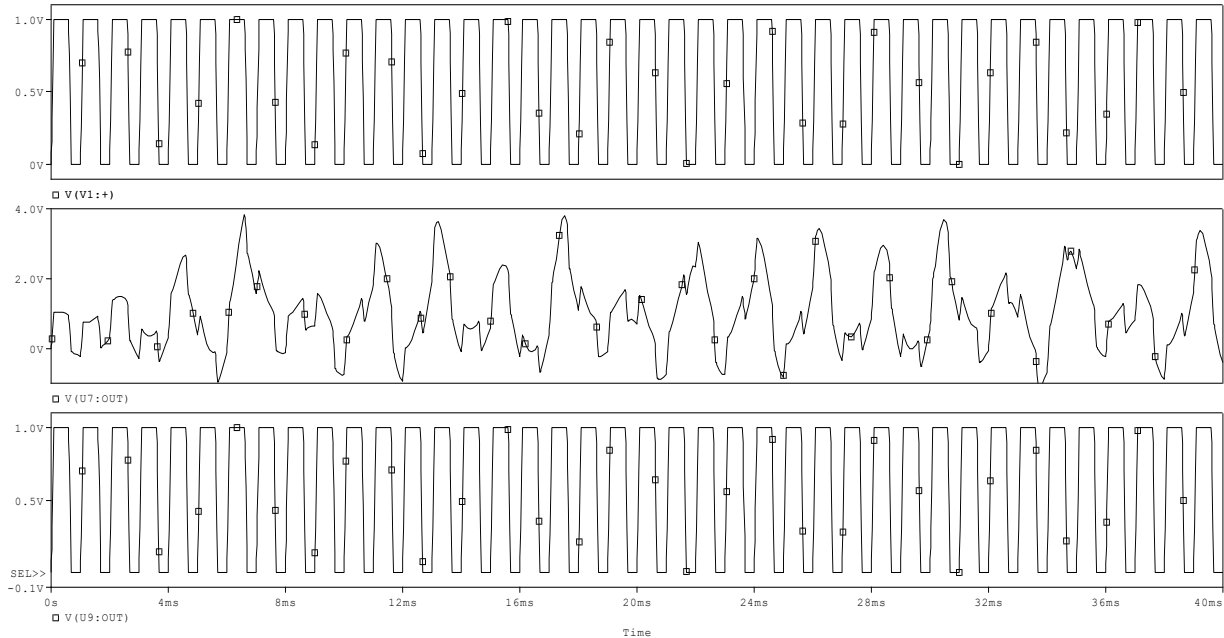


Figure 8: Shows chaotic secure communication (a) Original Information (b) Transmission chaotic signal, and (c) Decrypted at the receiver successfully

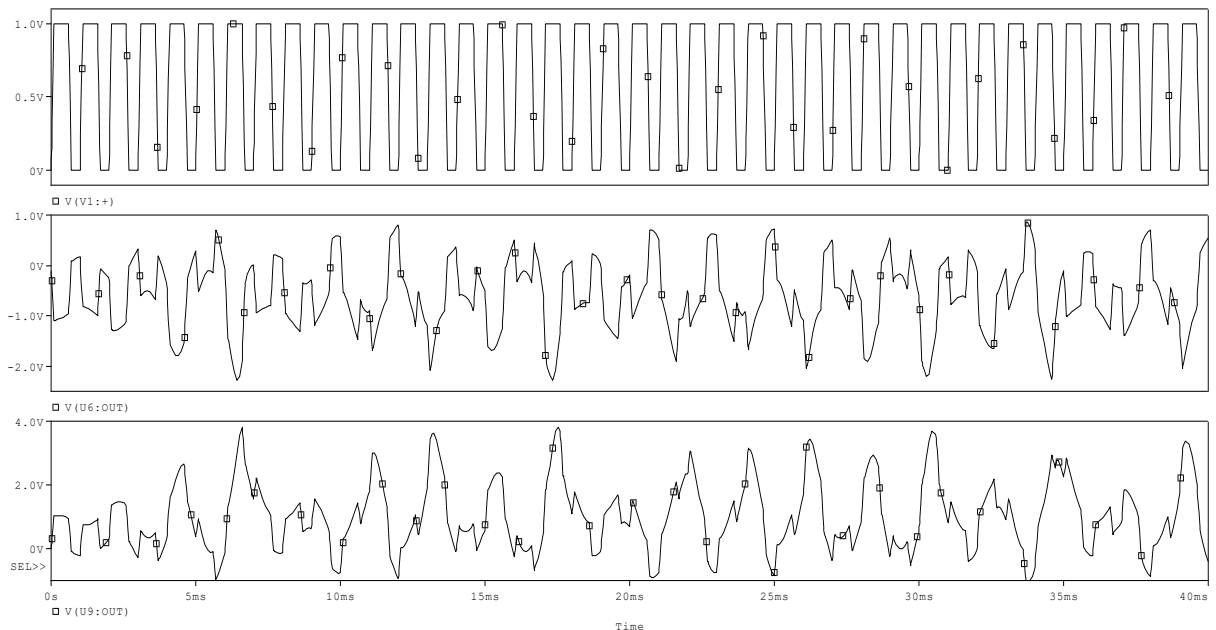


Figure 9: Shows chaotic secure communication (a) Original Information bearing signal, (b) Transmitted signal, and (c) Decrypted the transmitted signal with different encryption key, and the original information was not successfully received at the receiver

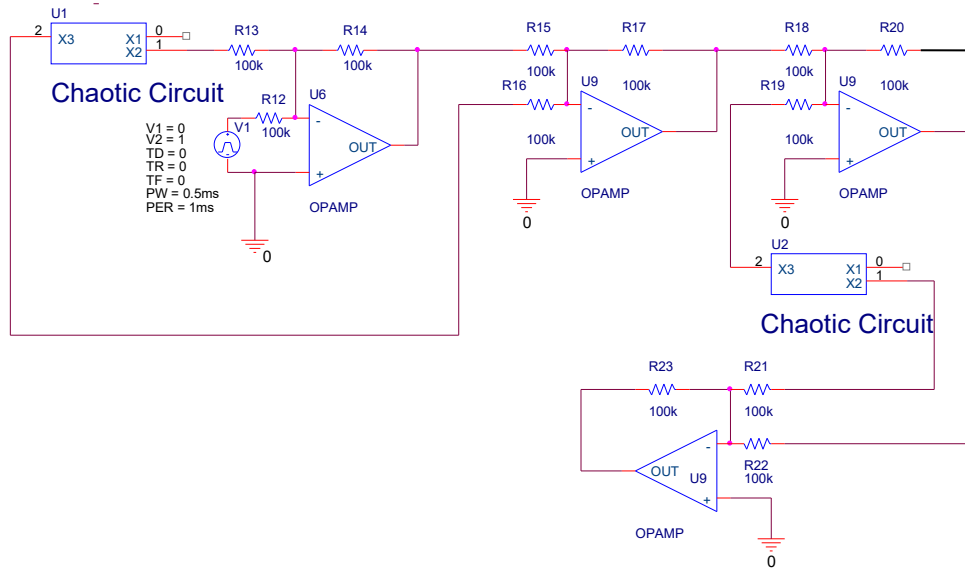


Figure 10: Schematic block diagram for double encryption secure communication for IoT application

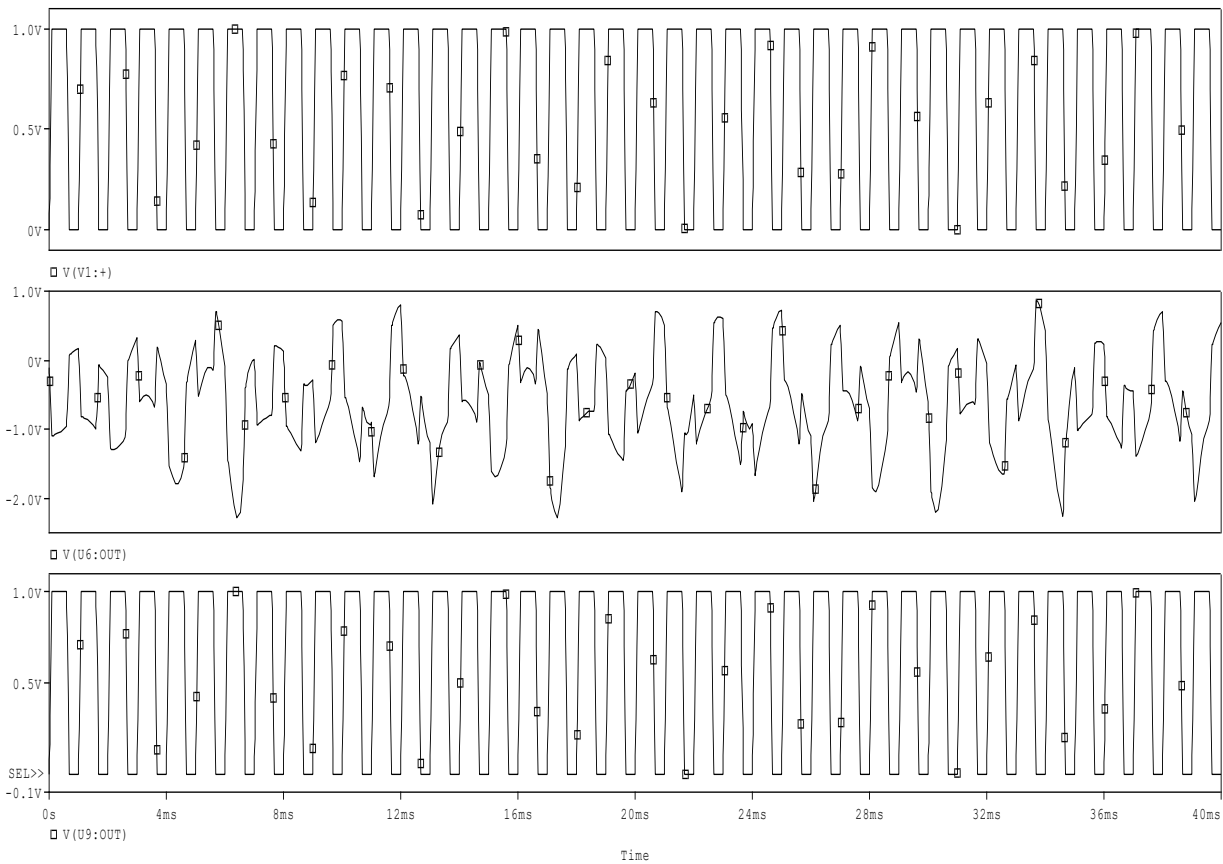


Figure 11: Shows chaotic secure communication (a) Original Information bearing signal, (b) Double encrypted (x2 + x3) transmitted signal, and (c) Double decrypted message signal at the receiver successfully

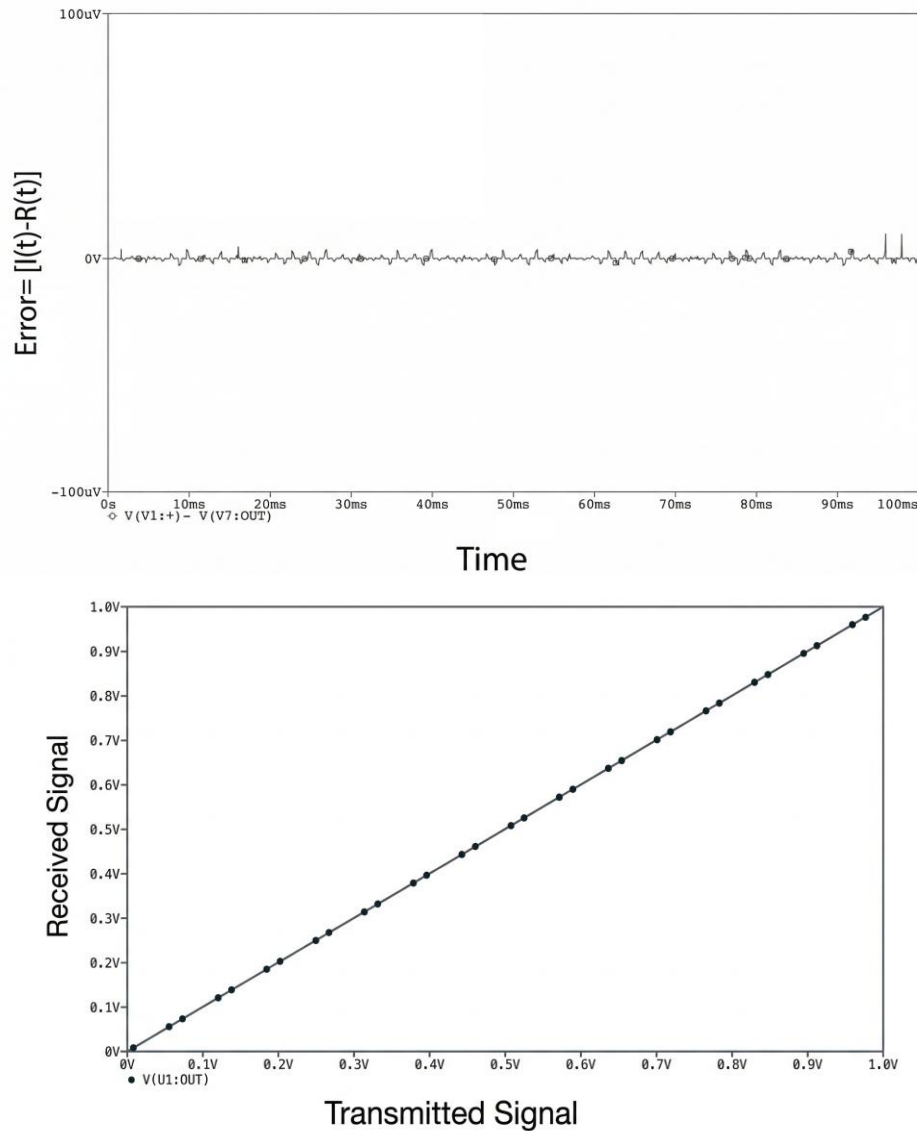


Figure 12: The of chaos masking communication method modeling of the proposed coexisting chaos attractor (a) Difference $I(t)/R(t)$, and (b) $e(t)=I(t)-R(t)$

5 Conclusion

In this research paper, a coexisting attractor system with saddle focus equilibria is proposed. The system exhibits chaotic behavior. The dynamical behavior was analyzed using Lyapunov exponents and dimension. Also, its sensitivity to initial conditions was verified because it enhances the encryption space of the same chaotic system for IoT secure communication. Further, an analog circuit is designed to realize the coexisting attractor, and its synchronization. The circuit simulation corresponds to the MATLAB simulation results. Analog circuit simulation results are in good qualitative agreement. Both single and double encryption were performed using the chaotic masking method, and the original information was decrypted at the receiver successfully. Double encryption enabled more secure encryption of the information signal during communication to achieve high performance, secure communication for use in IoT applications, and demonstrated. Furthermore, it was proved that when the

transmitted signal was decrypted with a different state signal than the encrypted state, the original message signal was not recovered at the receiver successfully. Hence, communication security in complex dynamical communication networks is a dire need and trending research nowadays.

References

- [1] Al Momin, M. A. (2022). Medical device security. In *Security, data analytics, and energy-aware solutions in the IoT* (pp. 173–191). IGI Global.
- [2] Anand, M. V., Krishnamurthy, A., Kannan, A., & Govindarajan, N. (2025). Secure Routing in Mobile Ad Hoc Networks with Hybrid Tasmanian Gazelle Optimization. *IETE Journal of Research*, 1-12.
- [3] Duan, Z., Wang, H., He, S., Li, S., Yan, S., Zhao, X., ... & Tan, H. (2022). A fully integrated chaos generator based on voltage-controlled oscillator. *Microelectronics Journal*, 126, 105514. <https://doi.org/10.1016/j.mejo.2022.105514>
- [4] Ganesh, N. G., Balasubramanian, V., Prasad, D. V. V., & Velan, S. S. (2025). Deep learning-based user authentication with hybrid encryption for secured blockchain-aided data storage and optimal task offloading in mobile edge computing. *Wireless Networks*, 31(3), 2389-2417.
- [5] Hedayatipour, A., & Mcfarlane, N. (2020). Wearables for the next pandemic. *IEEE Access*, 8, 184457-184474. <https://doi.org/10.1016/j.mejo.2022.105514>
- [6] Kaplan, J. L., & Yorke, J. A. (1979). In *Functional differential equations and approximations of fixed points: Proceedings, Bonn, July 1978* (H.-O. Peitgen & H. O. Walther, Eds., pp. 204–220). Springer-Verlag.
- [7] Liu, J., & Zhang, Y. (2011, July). The application of Chaotic masking and chaotic switching in communication. In *2011 Second, International Conference on Mechanic Automation and Control Engineering* (pp. 7781-7784). IEEE.
- [8] Onuki, K., Cho, K., Horio, Y., & Miyano, T. (2022). Secret-key exchange through synchronization of randomized chaotic oscillators aided by logistic hash function. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(4), 1655-1667. 10.1109/TCSI.2022.3140762
- [9] Ouannas, A., Karouma, A., Grassi, G., Pham, V. T., & Luong, V. S. (2021). A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Engineering Journal*, 60(1), 1873-1884. <https://doi.org/10.1016/j.aej.2020.11.035>
- [10] Prabu, R., Dhinakar, P., Prakash, S., & Gayathri, N. (2024, November). Study of Generating 4D and 5D Coexisting Hyper Chaotic Autonomous Systems for Application in Cryptography. In *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)* (pp. 1-5). IEEE. 10.1109/DELCON64804.2024.1086696
- [11] Rezaei, A., Gu, J., & Zhou, H. (2019, July). Hybrid memristor-CMOS obfuscation against untrusted foundries. In *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 535-540). IEEE.
- [12] Shi, F., Cao, Y., Xu, X., & Mou, J. (2025). A novel memristor-coupled discrete neural network with multi-stability and multiple state transitions. *The European Physical Journal Special Topics*, 1-17. <https://doi.org/10.1140/epjs/s11734-024-01440-8>
- [13] Stankevich, N. V., Bobrovskii, A. A., & Shchegoleva, N. A. (2024). Chaos and hyperchaos in two coupled identical Hindmarsh–Rose systems. *Regular and Chaotic Dynamics*, 29(1), 120-133.
- [14] Subbulaxmi, S., Valarmathi, G., Hema, R., Prakash, S., Kalaivani, K., & Sundararajan, M. (2024, April). A Memristive IoT based device third dimensional order exhibiting co-existing chaotic behavior for information processing. In *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)* (pp. 1-6). IEEE. 10.1109/IC3IoT60841.2024.10550270

- [15] Vishwakarma, R., Monani, R., Hedayatipour, A., & Rezaei, A. (2023). Reliable and secure memristor-based chaotic communication against eavesdroppers and untrusted foundries. *Discover Internet of Things*, 3(1), 2. <https://doi.org/10.1007/s43926-023-00029-2>
- [16] Volkovskii, A. R., Tsimring, L. S., Rulkov, N. F., & Langmore, I. (2005). Spread spectrum communication system with chaotic frequency modulation. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 15(3). <https://doi.org/10.1063/1.1942327>
- [17] Wang, Z., Gong, L., Yang, J., & Zhang, X. (2022). Cloud-assisted elliptic curve password authenticated key exchange protocol for wearable healthcare monitoring system. *Concurrency and Computation: Practice and Experience*, 34(9), e5734. <https://doi.org/10.1002/cpe.5734>
- [18] Wen, H., Zhang, C., Chen, P., Chen, R., Xu, J., Liao, Y., ... & Ke, J. (2021). A quantum chaotic image cryptosystem and its application in IoT secure communication. *IEEE access*, 9, 20481-20492. <https://doi.org/10.1109/ACCESS.2021.3054952>
- [19] Zhong, G. Q., & Ayrom, F. (1985). Experimental confirmation of chaos from Chua's circuit. *International journal of circuit theory and applications*, 13(1), 93-98. <https://doi.org/10.1002/cta.4490130109>
- [20] Zhou, X., Sun, K., Wang, H., & Yao, Z. (2024). Coexisting hyperchaos and multistability in a discrete memristor-coupled bi-neuron model. *Nonlinear Dynamics*, 112(11), 9547-9561.

Authors Biography



Dr. M. Anbarasan received the B.E. degree in Computer Science and Engineering from Anna University, India, in 2005 and the M.E degree in Computer Science and Engineering from Anna University, India, in 2011. His Doctorate from Anna University, Chennai in 2019. He has got teaching, Research, and administrative experience of more than 18 years in various Engineering Colleges and Autonomous Institutions. He is currently working as a Professor at Saveetha Engineering College. He has worked as a Lecturer, Assistant Professor, and Associate Professor in various Institutions. He has published more than 25 Papers in National and International Conferences and International Journals. He is working as a scientific and editorial board member of many journals. He is reviewed dozens of papers in many journals. He is the author of two book chapters. He is a Life member of the ISTE (India), Life Member IAENG (Hong Kong), Member of IAES, and Life-time member of CSI. He has given many national and international conferences and chaired many sessions. His research interests include Ad hoc Networks, Network security, and Machine Learning.



Dr. Gobalakrishnan Natesan pursued his Bachelor's degree in Information Technology at Anna University, Tamil Nadu, India in 2005. He then obtained his Master's degree in Software Engineering from Bharathidasan University, Tamil Nadu, India, in 2008. He completed his Ph.D., in 2019 and is currently working as a Professor in the Department of Computer Science and Engineering, Saveetha Engineering College, Tamil Nadu, India. He is a Life Member of ISTE and IAENG. His current research interests are Cloud computing, Image Processing, and Big Data.



Dr. S. Prakash obtained his Bachelor's degree (B.E) in Electronics & Communication Engineering from Madurai Kamaraj University, India, in 1990, Master's degree (M.E) in Instrumentation and Control from BIT, Mesra, India, in 1992, and Ph. D from IISc, Bangalore, in 1997 from the Department of Instrumentation. Then, continued research on ohmic contact studies in GaN materials at the NUS, Singapore. Further, research in the area of thin film transistors at the University of Waterloo, Canada. He has got teaching, Research, and administrative experience of more than 29 years in various Engineering Colleges and Deemed Institutions. Also, worked in the capacity as a Lecturer, Assistant Professor, and Associate Professor in various Institutions. Currently, working as a professor in the department of electronics and communication engineering at Bharath Institute of Higher Education and Research, Tamil Nadu, India. He has authored or co-authored 51 international journal research papers. And has presented in many national and international conferences and chaired many sessions. Under his guidance, seven have received their Ph.D. degree from the faculty of information and communication engineering, Anna University, India. He is a life member of ISTE and a Fellow Member of IETE. His fields of research are Nanodevices, Embedded systems, Dynamical systems, Communication systems, and Computer networks.