Information Security System Based on Chaotic Signals

Volodymyr Rusyn[a], Aceng Sambas[b] and Mujiarto[b]

[a] *Yuriy Fedkovych Chernivtsi National University, Kotsybynsky str. 2, Chernivtsi, 58012, Ukraine*
[b] *Universitas Muhammadiyah Tasikmalaya, Jl. Tamansari No. KM 2,5, Mulyasari, Kec. Tamansari, Tasikmalaya, Jawa Barat, 46196, Indonesia*

Abstract

In this paper, we present computer modelling and analysis of the chaotic Arneodo system. For demonstrate of these results was used modern software environment LabView. Created programming interface allows to generating, analysis and research of the main information properties of chaotic Arneodo system, focusing on time series of the three chaotic coordinates, phase portraits and Lyapunov exponents. Another programming interface demonstrates the algorithm of masking and decrypt of the information.

Keywords 1

Nonlinear, Arneodo, LabView, FPGA, security system

1. Introduction

Chaotic signals are used in different technical scientific areas such as engineering, optics, radio electronics, telecommunications, robotics, cybersecurity [1-19]. Chaos theory is a branch of mathematics and physics that studies systems whose dynamics, under certain conditions, largely depend on the initial conditions, making long-term prediction impossible [20, 21]. Because, on the one hand, the dynamics of behavior of such systems corresponds to the laws of physics, and, on the other hand, looks irregular, it is called deterministic chaos. Chaotic systems are nonlinear dynamical systems.

Chaotic signals have the following characteristics: sensitive dependence on the initial conditions, unpredictability, similarity to the noise, and difficulty to be deciphered. Therefore, it is especially suitable to be applied to the secure communication field. In many physical systems and their deterministic models, it has been confirmed that in addition to typical behaviors such as reduction to constant, periodic or quasiperiodic behaviors, in some cases trajectories become aperiodic (chaotic) if their parameters, internal variables, or external signals are selected.

A great interest is the simulation of the main information properties of chaotic systems. For modelling of these properties and demonstrate results was selected software LabView (LabView-2020 (64-bit version for Windows).

2. Modeling of a chaotic Arneodo system

Chaotic Arneodo system is described by equations

$$\begin{cases} \dot{x} = y; \\ \dot{y} = z; \\ \dot{z} = -ax - by - cz + dx^3 \end{cases} \quad (1)$$

where a,b,c,d – system parameters, x,y,z – initial conditions [22].

Figure 1 shows the block diagram that implements of chaotic Arneodo system. The main functional part is a formula node, in which would include the equation (1). In the input formula node fed values

ITTAP'2021: 1st International Workshop on Information Technologies: Theoretical and Applied Problems, November 16–18, 2021, Ternopil, Ukraine
EMAIL: rusyn_v@ukr.net (A. 1); acenx.bts@gmail.com (A. 2); mujiarto@umtas.ac.id (A. 3)
ORCID: 0000-0001-6219-1031 (A. 1); 0000-0002-1623-0770 (A. 2); 0000-0002-4825-8436 (A. 3)

of system parameters (*a*,*b*,*c*,*d*) and the value of the initial conditions (*x*,*y*,*z*). At the output assigned equations (1). Also, the output is an opportunity to demonstrate the solution of equations in three dimensions.

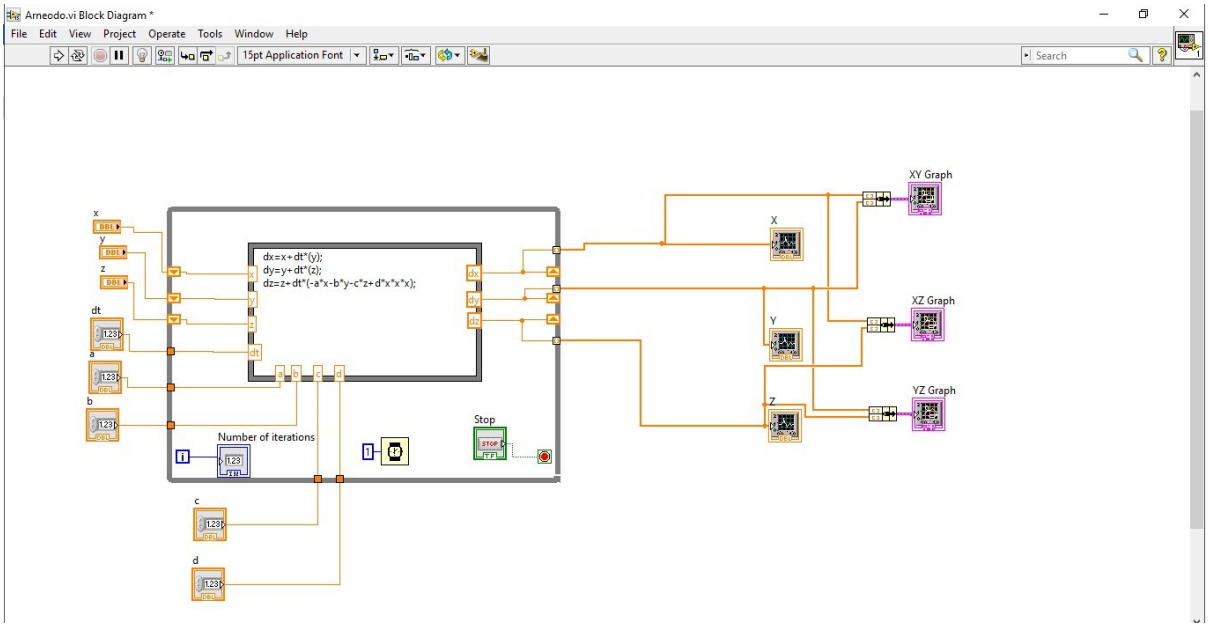

Figure 1: Block diagram of chaotic Arneodo system

Figure 2 and Figure 3 shown chaotic attractor in XY, XZ and YZ projection and time series for X, Y and Z coordinates for the following set of parameters: a = -5.5, b = 3.5, c = 1, d = -1; x = 0.5, y = -1, z = 0.5, dt = 0.01, number of iterations N = 10000.

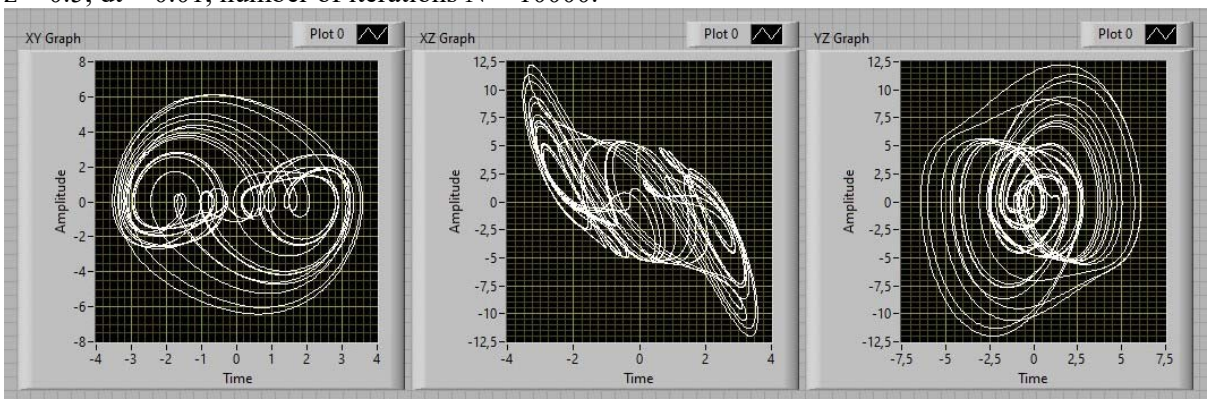

Figure 2: Chaotic attractor in XY, XZ and YZ projection

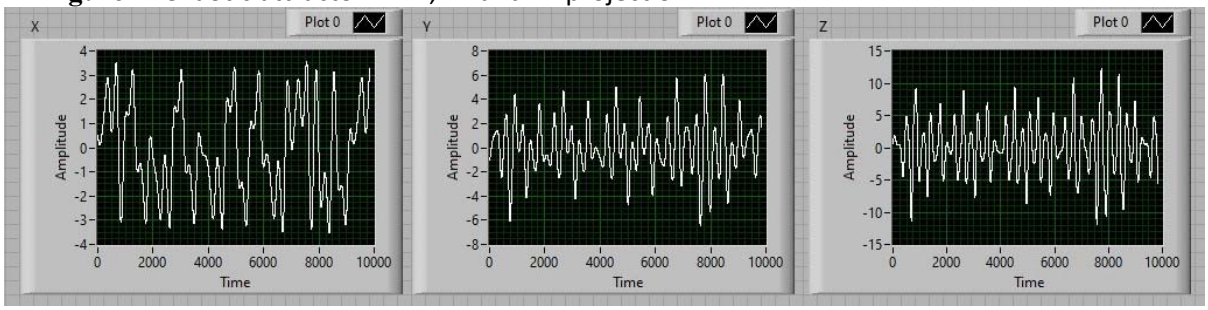

Figure 3: Time series for X, Y and Z coordinates

To demonstrate of chaotic behavior of the different nonlinear systems can be used Field-Programable Gate Array (FPGA) [23-25]. Figures 4-6 shows chaotic attractor in XY, XZ and YZ projection using FPGA.

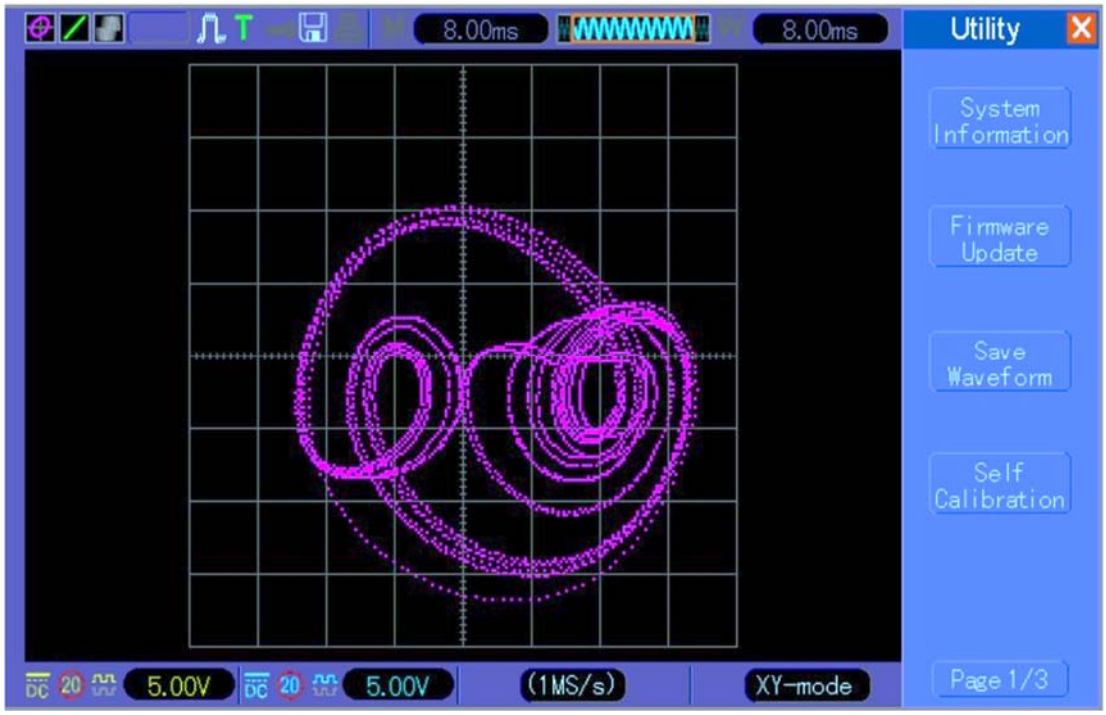

Figure 4: Chaotic attractor in XY projection

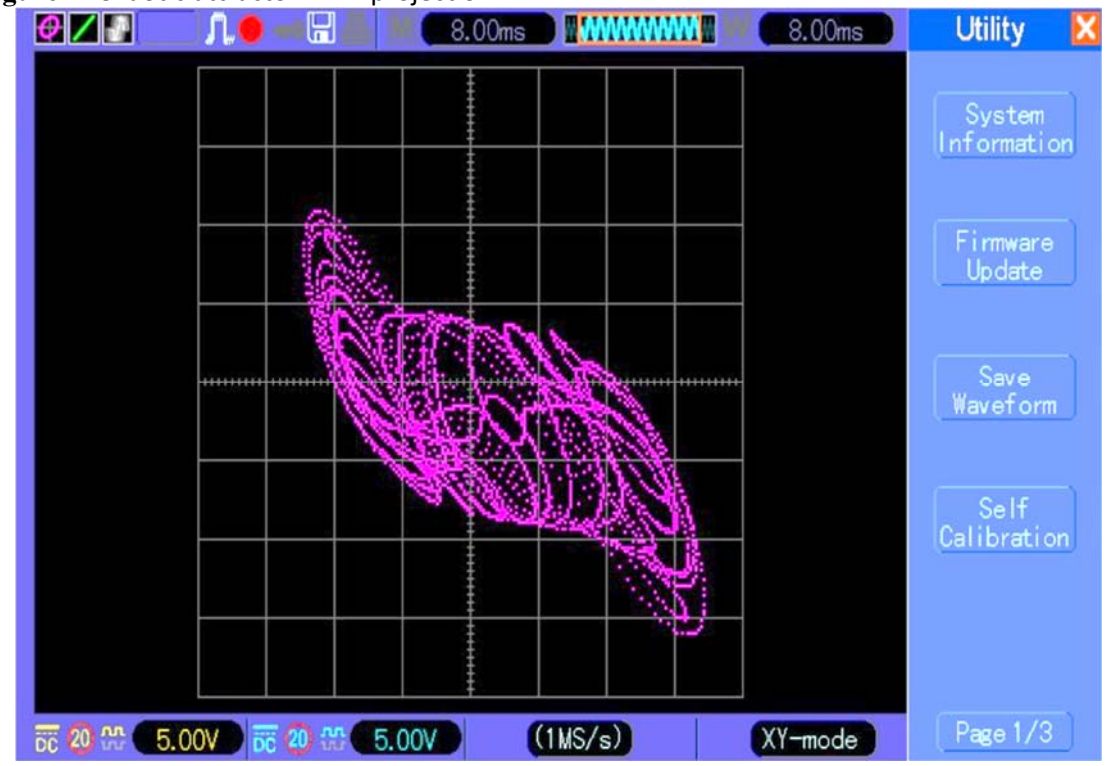

Figure 5: Chaotic attractor in XZ projection

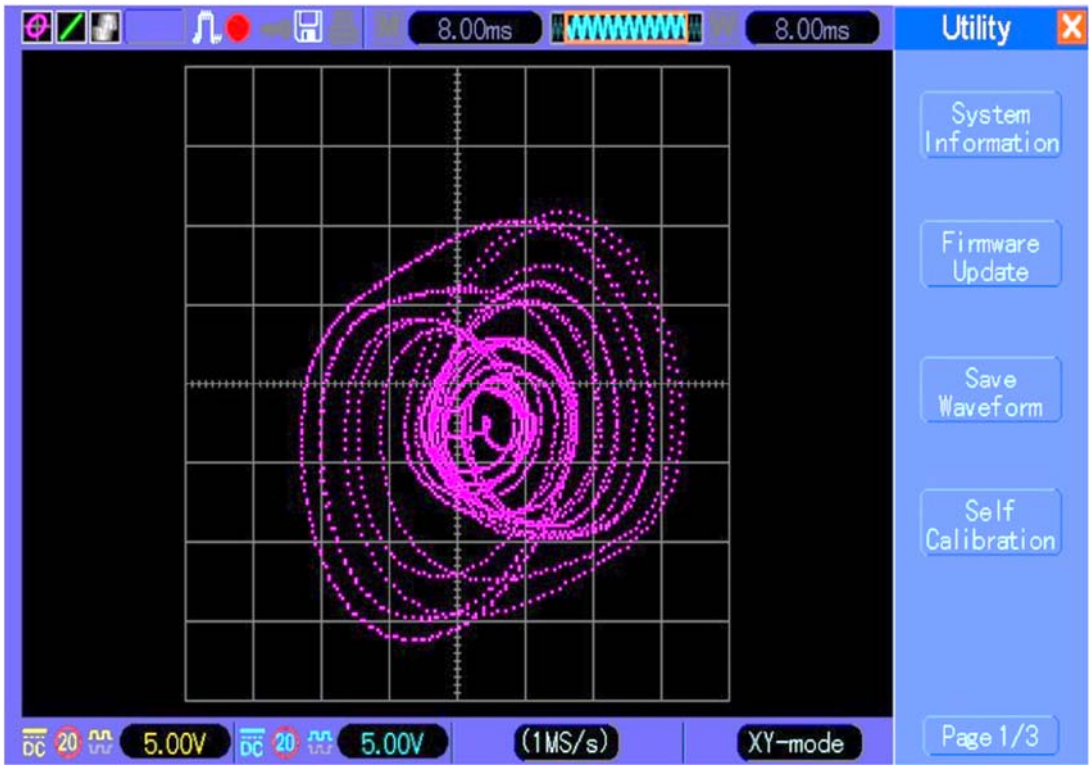

Figure 6: Chaotic attractor in YZ projection

The Lyapunov exponents of the Arneodo attractor are 0.232, 0, and -1.232.

3. Chaotic masking and decryption of the information carrier

The coherent receivers usually are dynamical systems that resemble the chaos producing transmitters. They achieve synchronization with the transmitter, enabling the synchronization to extract the information signal from the received chaotic signal. In order to achieve synchronization, the parameters of the transmitter have to be known. They can be considered as the encryption key of the message; thus, coherent receptions allows for some privacy of the information transmission.

Figure 7 demonstrates the presence of the chaotic signal between the transmitter and receiver. In this case, the use of chaos in secure communication systems has been proposed. The design of these systems depends on the self-synchronization property of the chaotic attractor. As shown in Figure 7, the transmitter and the receiver systems are identical.

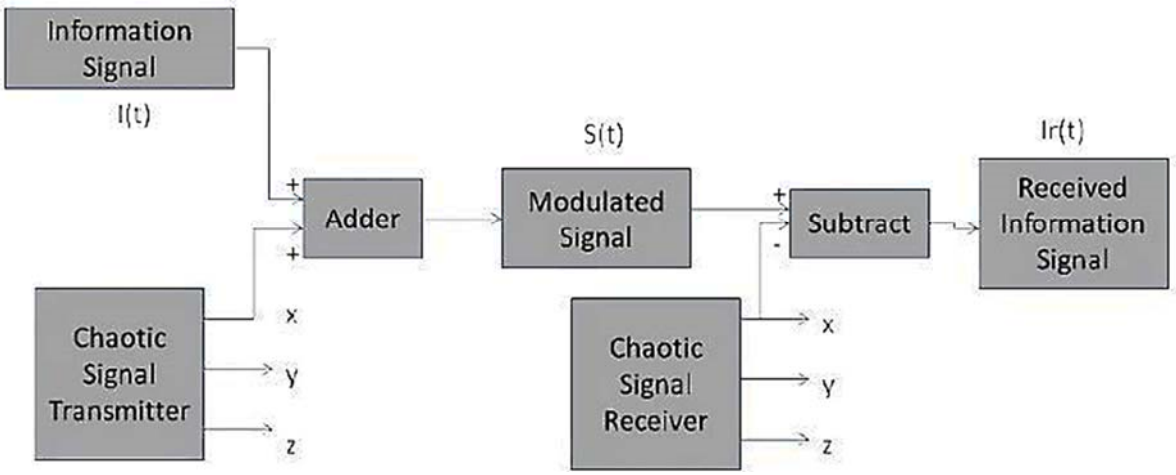

Figure 7: Transmitter and receiver systems

Figure 8 presents the program interface, which demonstrates the masking of the information carrier based on a chaotic Arneodo system (1).

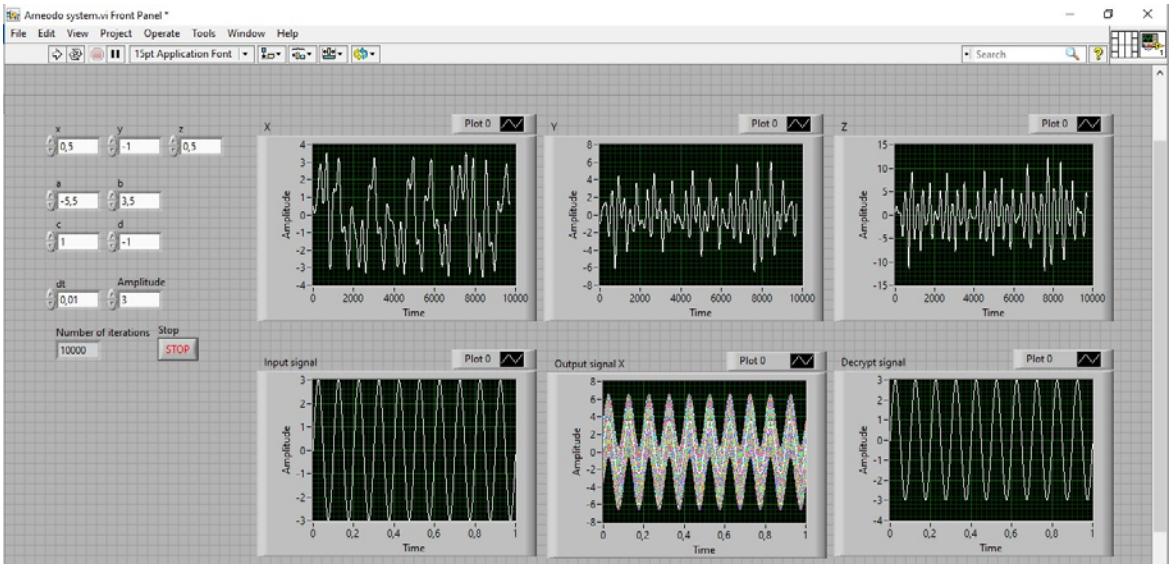

Figure 8: Software interface show's masking and decryption of the information carrier

The masking of the information carrier based on chaos is provided by blending information with the chaotic signal. A sinusoidal signal (useful signal) was used as information (input) with amplitude of *3 V* and system parameters $a = -5.5$, $b = 3.5$, $c = 1$, $d = -1$, dynamic variables $x = 0.5$, $y = -1$, $z = 0.5$. System parameters and dynamic variables are the keys for the masking information.

Algorithm for the decryption has opposite effect.

4. Conclusions

For modelling of information properties of the chaotic Arneodo system and demonstrate computer modelling results was selected software LabView (LabView-2020 (64-bit version for Windows). The main information properties of chaotic Arneodo system such as a time series of the three chaotic coordinates, phase portraits and Lyapunov exponents are presented. The programming interface demonstrates the algorithm of masking and decrypt of the information carrier.

5. References

[1] S. Vaidyanathan, A. Sambas, S. Zhang, Mujiarto, M. Mamat, Subiyanto, A Chaotic Jerk System with Three Cubic Nonlinearities, Dynamical Analysis, Adaptive Chaos Synchronization and Circuit Simulation. Journal of Physics: Conference Series 1179, (2019) art.no 012083. URL: http://dx.doi.org/10.1088/1742-6596/1764/1/012205.

[2] V. Rusyn, S. Subbotin, A. Sambas, Analysis and experimental realization of the logistic map using Arduino Pro Mini. CEUR Workshop Proceedings 2608, (2020) 300-310.

[3] V. Rusyn, A. Samila, Ch. Skiadas, Computer modeling and practical realization of chaotic circuit with a light-emitting diode, in: Proceedings of the Fourteenth International Conference on Correlation Optics, 2019, pp. 113690D. http://dx.doi.org/10.1117/12.2550813.

[4] V. Rusyn, S. Khrapko, Memristor: modeling and research of information properties, in: Ch. H. Skiadas, I. Lubashevsky (Eds.), Springer Proceedings in Complexity. Springer, Cham, 2019, pp. 229-238. http://dx.doi.org/10.1007/978-3-030-15297-0_21.

[5] S. Vaidyanathan, M. Feki, A. Sambas, C. H. Lien, A new biological snap oscillator: its modelling, analysis, simulations and circuit design. International Journal of Simulation and Process Modelling, 13(5), (2018) pp. 419-432. https://doi.org/10.1504/IJSPM.2018.10015882.

[6] Z.F. Wang, L. Shi, H. Wu, N. Helian, O.L. Chua, Fractional memristor. Applied Physics Letter 111, (2017), art.no. 243502. https://doi.org/10.1063/1.5000919.

[7] D. Yu, C. Zheng, H. H. C. Iu, T. Fernando, L.O. Chua, A new circuit for emulating memristors using inductive coupling. IEEE Access 5, (2017), pp. 1284-1295. https://doi.org/10.1109/ACCESS.2017.2649573.

[8] V. Rusyn, Ch.H. Skiadas, A. Sambas, M. Mamat, S. Vaidyanathan, Process of pulse transformation of the analog nonlinear signals. Telecommunications and Radio Engineering, 79(13), (2020), pp. 1141–1147. DOI: 10.1615/TelecomRadEng.v79.i13.40.
[9] S. Vaidyanathan, A. Sambas, S. Kacar, Ü. Çavuşoğlu, A new three-dimensional chaotic system with a cloud-shaped curve of equilibrium points, its circuit implementation and sound encryption. International Journal of Modelling, Identification and Control, 30(3), (2018), pp. 184-196. http://dx.doi.org/10.1504/IJMIC.2018.095334.
[10] V. Rusyn, Modeling and Research Information Properties of Rucklidge Chaotic System Using LabView, in: Proceedings of 10th Chaotic Modeling and Simulation International Conference, Barcelona, 2017, pp. 739-744.
[11] P. Milicka, P. Cížek, J. Faigl, On Chaotic Oscillator-based Central Pattern Generator for Motion Control of Hexapod Walking Robot. CEUR Workshop Proceedings 1649, (2016), pp. 131-137.
[12] I.N. Stouboulos, I.M. Kyprianidis, M.S. Papadopoulou, Chaotic dynamics and coexisting attractors in a modified Chua's circuit. WSEAS Transactions on Circuits and Systems, 5(11) (2006), pp. 1640-1646.
[13] L. Chua, A zoo of strange attractors from the canonical Chua's circuits, in: Proceedings of the IEEE 35th Midwest Symposium on Circuits and Systems, Cat. No. 92CH3099-9, Vol. 2, (1992), pp. 916-926. https://doi.org/10.1109/MWSCAS.1992.271147.
[14] V. Rusyn, M.A. Mohamed, D. Purwandari, M. Mamat, J. Titaley, B. Pinontoan, Chaotic and Controlling Regimes of a New Modified Chua's Generator. Journal of Advanced Research in Dynamical and Control Systems, 12(2) (2020), pp. 556-561. DOI:10.5373/JARDCS/V12I2/S20201077.
[15] M.S. Papadopoulou, I.M. Kyprianidis, I.N. Stouboulos, Study of the behavior of a 4th order non driven circuit. Chaotic synchronization of two identical circuits. WSEAS Transactions on Circuits and Systems, 5(7) (2006), pp. 993-1000.
[16] I.N. Stouboulos, I.M. Kyprianidis, M.S. Papadopoulou, Experimental study of antimonotonicity in a 4th order nonlinear autonomous electric circuit. WSEAS Transactions on Circuits and Systems, vol. 5(11) (2006), pp. 1662-1668.
[17] V. Rusyn, M. Sadli, M. Mamat, Mujiarto, W.S. Mada Sanjaya, Computer Modelling of a New Simple Chaotic Generator. Journal of Physics: Conference Series, 1477 (2020), art.no. 022010. https://doi.org/10.1088/1742-6596/1477/2/022010.
[18] M.S. Papadopoulou, I.M. Kyprianidis, I.N. Stouboulos, A.N. Anagnostopoulos, Chaos Synchronization and its Application to Secure Communication. Journal of Concrete and Applicable Mathematics, 9 (2011), pp. 205-212.
[19] V. Rusyn, Mujiarto, M. Mamat, F. Azharul, W.S. Mada Sanjaya, A. Sambas, E. Dwipriyoko, A. Sutoni, Computer Modelling of the Information Properties of Hyper Chaotic Lorenz System and Its Application in Secure Communication System. Journal of Physics: Conference Series, 1764, (2021), art.no. 012205. http://dx.doi.org/10.1088/1742-6596/1764/1/012205
[20] C.H. Skiadas, C. Skiadas, Chaotic Modelling and Simulation: Analysis of Chaotic Models, Attractors and Forms. In: Taylor & Francis Group, (2008), pp. 1-345.
[21] C.H. Skiadas, Exact solutions of stochastic differential equations: Gompertz, generalized logistic and revised exponential. Methodology and Computing in Applied Probability 12(2) (2010), pp. 261-270.
[22] Hua Changchun, Guan Xinping, Adaptive control for chaotic systems. Chaos, Solitons and Fractals, 22 (2004), pp. 55-60. https://doi.org/10.1016/j.chaos.2003.12.071
[23] Xuenan, Peng, Yicheng, Zeng, Mengjiao, Wang, Zhijun, Li, Generating Multi-layer Nested Chaotic Attractor and Its FPGA Implementation. Chinese Physics B, 30(6) (2021), art. no. 060509. https://doi.org/10.1088/1674-1056/abda34.
[24] A. Sambas, S. Vaidyanathan, T. Bonny, S. Zhang, Sukono, Y. Hidayat, G. Gundara, M. Mamat, Mathematical Model and FPGA Realization of a Multi-Stable Chaotic Dynamical System with a Closed Butterfly-Like Curve of Equilibrium Points. Appl. Sci., 11(2) (2021), p. 788. https://doi.org/10.3390/app11020788
[25] Dong Enzeng, Yuan Mingfeng, Han Fangfang, Tong Jigang, Du Shengzhi, Topological Horseshoe Analysis and FPGA Implementation of a Classical Fractional Order Chaotic System. IEEE Access, 7 (2019), pp. 129095-129103. https://doi.org/10.1109/ACCESS.2019.2938556.