A Novel Random Number Generator Based on Fractional Order Chaotic Chua System

Fatih Ozkaynak
Department of Software Engineering, Firat University,
23119 Elazig, Turkey
ozkaynak@firat.edu.tr

***Abstract*—One of the practical applications of chaotic systems is the design of a random number generator. In the literature, generally random number generators are designed using discrete time chaotic systems. The reason for the use of the discrete time chaotic systems in the design architecture is that the latter have a simpler structure than the continuous time chaotic systems. In order to observe chaos in continuous time systems, the system must have at least three degrees. It is shown that for fractional order chaotic systems chaos can be observed even in a lower system degree. The aim of this study is to develop a random number generator using a fractional order chaotic Chua system. The proposed generator is analysed using various randomness tests. The analysis results show that the proposed generator passes the random requirements successfully. On the one hand, this study is important because it demonstrates the practical application of fractional order chaotic systems. On the other hand, it provides an alternative to designs based on discrete time chaotic systems.**

***Index Terms*—Chaos; Fractional order chaos; Chua system; Random number generator.**

I. INTRODUCTION

Chaotic behaviors are the dynamics observed in nonlinear systems. Many nature systems or man-made systems are nonlinear. Therefore, the probability of encountering chaotic behaviors and systems is very high [1]–[4]. In recent years, Chaos theory and Chaotic dynamics, which are observed in nonlinear systems and called as strange attractors, have been intensively studied by researchers. Describing the term ‘Chaos’ roughly, it is irregular behavior in a nonlinear deterministic system showing sensitive dependent behavior to initial conditions. Deterministic systems are systems, in which system behavior is determined by its parameters and initial conditions. Chaotic systems have a deterministic behavior. This behavior is the most important characteristic difference between noise and chaos [4]. In a system, the requirements for observing the complex dynamics, defined as strange attractors, are listed below:

– The system must have nonlinear elements;

– The system must be sensitive to the initial condition.

These conditions are necessary for the chaos in a system to exist, but it is not enough. If the system is a continuous time system, it must have at least three degrees. Chaos is not observed in nonlinear systems where the system degree is less than three. For discrete time systems, such a condition is not required. Chaos can be observed even in a first order system, e.g., logistic map. Therefore, in many practical applications of chaos, discrete time chaotic systems are preferred. The most important reason for such a choice is that the discrete time chaotic systems have a simpler structure than the continuous time chaotic systems. On the other hand, both in fractional models of the existing chaotic systems and in newly defined fractional systems chaotic behaviour in the system is observed even though the system degree is less than three [5]–[12].

In this study, a random number generator is proposed using these advantageous features of fractional order chaotic systems. The randomness properties of the proposed generator are tested using chi-square and monobit tests. The analysis results shows that the proposed generator passes the random requirements successfully. The study is important because it demonstrates the practical application of fractional order chaotic systems and offers an alternative to designs based on discrete time chaotic systems.

The rest of the study is organized as follows. In Section II, fractional order chaotic systems are briefly described. The properties of the fractional order Chua system used in the study are demonstrated to show the chaotic behaviour through parameter values. In Section III, the operation of the proposed algorithm for converting fractional chaotic system outputs to random numbers is detailed. In Section IV, the random number generator based on fractional order Chua system is tested and the results are analysed. In Section V, the advantages of the proposed method compared to the other methods in the literature are discussed. The obtained results are summarized and suggestions for future studies are made in the last section of the paper.

II. FRACTIONAL ORDER CHAOTIC SYSTEM

Since fractional calculation is not a matter of pure mathematics, it has opened up various applications in parallel with theoretical developments. Fractional calculation helps to express and successfully solve many physical problems. Recent research shows that fractional order differential equations are an effective tool to define complex dynamics and can model many physical and engineering-related systems more effectively [4], [12].

The existence of chaotic dynamics in fractional systems

Manuscript received 11 May, 2019; accepted 19 November, 2019.
This paper is supported by the Firat University Scientific Research Project (TEKF.18.02).

becomes an issue to be investigated in parallel with the intense work of dynamics that is observed in nonlinear systems called chaos [5], [6], [11]. Many chaotic systems, such as Rössler, Chen, and Chua, that are widely known in the literature, are studied by researchers. Although the degree of these systems is less than 3, there are still three state variables in the system and the degree of at least one of these three state variables is less than one, and none of them have a delay element. In this study, Chua system is used as a fractional order chaotic system [4]. Chua system is widely known in chaos theory and its practical applications. This system known as the Chua circuit is a third-order system, and show classic chaotic behaviour [1]. Unlike the usual Chua system, in this system, instead of the nonlinear element in the partial linear structure, cubic type nonlinearity is used. The state space representation of the Chua system is expressed as given in (1):

$$\begin{cases} \dfrac{dx}{dt} = \sigma\left[y + \dfrac{x - 2x^3}{7} \right], \\ \dfrac{dy}{dt} = x - y + z, \\ \dfrac{dz}{dt} = -\beta y. \end{cases} \tag{1}$$

The x, y, and z state variables are the σ and β system parameters. In the study, β = 100/7 is taken. The state space representation of the fractional model of the Chua system described in (1) is given in (2):

$$\begin{cases} \dfrac{d^q x}{dt} = \sigma\left[y + \dfrac{x - 2x^3}{7} \right], \\ \dfrac{d^q y}{dt} = x - y + z, \\ \dfrac{d^q z}{dt} = -\beta y. \end{cases} \tag{2}$$

Here, q corresponds to the fractional degree of each state variable. The block diagram equivalent to the state space representation is given as in Fig. 1, so that the fractional model can be simulated in a comfortable manner.

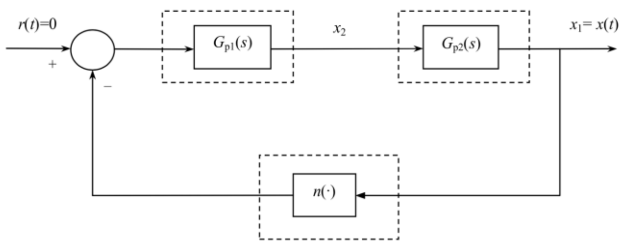


Fig. 1. Block diagram of fractional order chaotic Chua system.

In the block diagram of Fig. 1, fractional integral, linear subsystem, and non-linear subsystem are given in (3)–(5):

$$G_{p1}(s) = \frac{1}{s^a}, \tag{3}$$

$$G_{p2}(s) = \frac{\sigma(s^2 + s + \beta)}{s^2 + s + (\beta - \sigma)}, \tag{4}$$

$$n(x) = \frac{2x^3 - x}{7}. \tag{5}$$

The σ = 9.5 and β = 100/7 values and the state space diagram of system for α = 1 are obtained as given in Fig. 2.

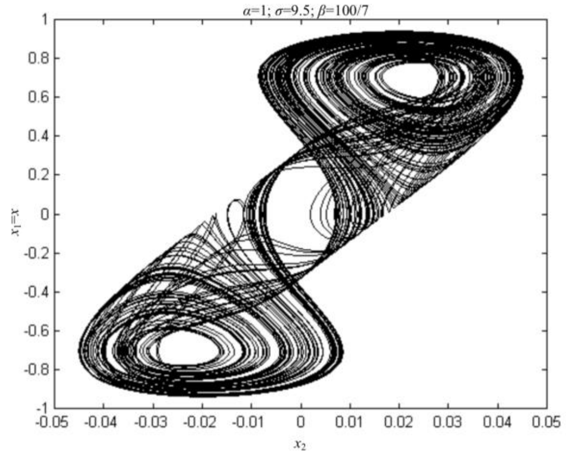
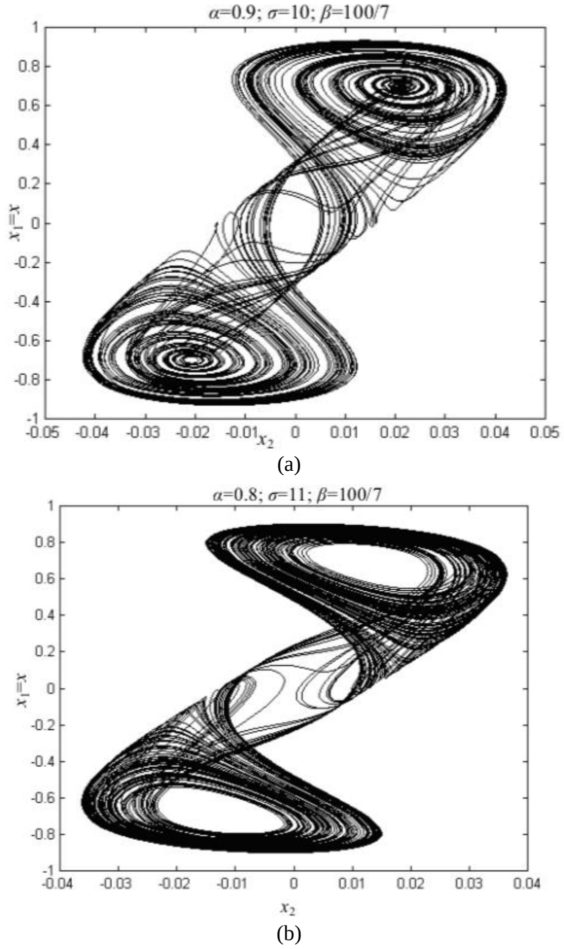


Fig. 2. Phase space diagram for Chua system.

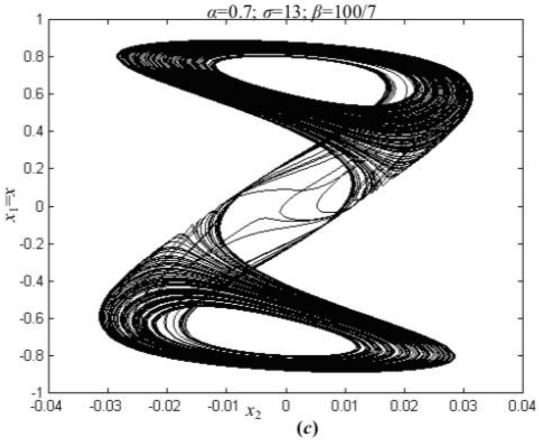
In the fractional model of the Chua system, the integral degree of the block diagram (Fig. 1) is examined for the presence of the chaos in the system for α = 0.9, α = 0.8, and α = 0.7. In this case, the system degree is going to be 2.9, 2.8, and 2.7, respectively. State space diagrams of the systems corresponding to these cases are obtained in Fig. 3.

In Fig. 2 and Fig. 3, the chaotic behaviour is shown qualitatively.



(a)

(b)



(c)

Fig. 3. State space diagrams of fractional order Chua system for the integral degree of a) α = 0.9, b) α = 0.8, and c) α = 0.7.

In Fig. 4, the time variation of x state variable for α = 0.9, α = 0.8, and α = 0.7 is obtained. From the time responses, it can be observed that the system is chaotic [4].

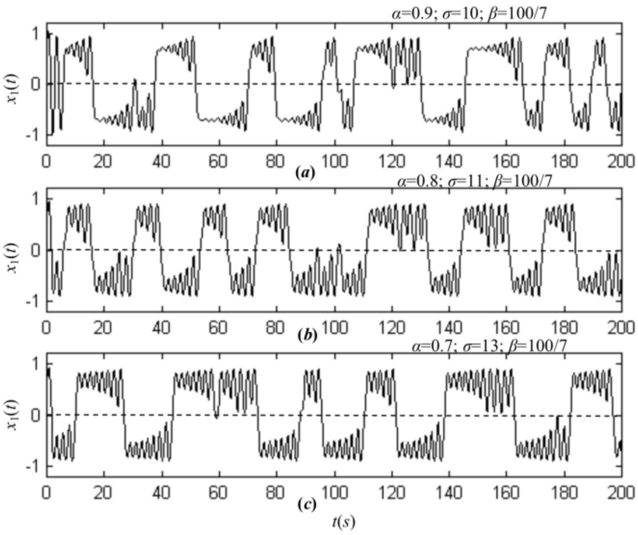


Fig. 4. State space diagrams of fractional order Chua system for the integral degree of a) α = 0.9, b) α = 0.8, and c) α = 0.7.

Another chaos analysis method, Lyapunov exponents, is a quantitative method of chaos analysis. The presence of at least one positive Lyapunov exponent indicates the chaotic behaviour. In Table I, the maximum Lyapunov exponents are calculated for α = 0.9, α = 0.8 and α = 0.7. The calculations are obtained according to two different initial conditions very close to each other (x_{01}(0.1, 0, 0) and x_{02}(0.1 001, 0, 0). All of the maximum Lyapunov exponents have a positive value indicating that there is chaos in the system [4].

TABLE I. MAXIMUM LYAPUNOV EXPONENTS.

Degree of Integral (q)	System parameters (σ, β)	Maximum Lyapunov Exponent (λ_{max})
0.9	(10, 100/7)	0.00190
0.8	(11, 100/7)	0.00032
0.7	(13, 100/7)	0.00008

III. PROPOSED ALGORITHM FOR RANDOM NUMBER GENERATOR

Randomness is the absence of a specific pattern or predictability in the events. Non-random systems are deterministic. Random numbers are numbers that are defined for a given interval and their probability of occurrence being equal to each other, and there is no specific relationship between these numbers. Random numbers are used in many areas, such as simulation, sampling, numerical analysis, entertainment, and cryptography [2], [7], [13]–[23].

Random number generators are divided into two classes: Deterministic Random Number Generator (DRNG) and True Random Number Generator (TRNG). DRNG is an algorithm that generates sequence arrays that resemble the random number properties. DRNG is calculated using the seed value [2]. Therefore, the structure used as a seed value is of a great importance. Structures, which are usually a strong source of the entropy, should be selected as the seed value. Since chaotic systems are a powerful source of entropy, they are widely used in the literature in the random number generator designs.

In this study, chaotic system outputs are converted to random numbers between 0–15. The mode operation for this convertion is used [24]. In this way, a very simple process is obtained with a robust generator. The details of the proposed algorithm are described step-by-step below:

Step 1. Select fractional order chaotic system. Chen system is used in this study;

Step 2. The system outputs are calculated for the parameter values for the selected system. α = 0.7, σ = 9.5, and β = 100/7 are used in this study;

Step 3. Select one of the state variables. In this study *x* state variable is used.

Step 4. The values of the chaotic system output after the comma are converted to the values between 0 and 15 by applying the mode 16 operation.

The random numbers obtained for the first 10 values of the x state variable of the fractional order chaotic Chua system are shown in Table II.

TABLE II. AN EXEMPLARY USE OF THE PROPOSED ALGORITHM.

No	Chaotic Output	Operation	Random Number
1	-0.8051	8051 mod 16	3
2	-0.8046	8046 mod 16	14
3	-0.7904	7904 mod 16	0
4	-0.7326	7326 mod 16	14
5	-0.4406	4406 mod 16	6
6	0.1528	1528 mod 16	8
7	0.5351	5351 mod 16	7
8	0.5188	5188 mod 16	4
9	0.4946	4946 mod 16	2
10	0.4663	4663 mod 16	7

If the numbers in the last column are converted to the bit array, the 40-bit length array to be obtained is going to be as follows: 0011111000001110011010000111010000100111.

IV. ANALYSIS RESULTS FOR PROPOSED DRNG

256 values are taken for use from the fractional order chaotic Chen system output in the analysis. These values are converted to numbers between 0–15 using the method described in Section III.

Two different statistical randomness test are used in this study. First statistical randomness test is known as the monobit (frequency) test [3]. Definition of this test is that "Monobit test measures whether the number of 0 s and 1 s produced by the generator are approximately the same as would be expected for a truly random sequence." [3].

Since 256 numbers are generated from 0 to 15, a random sequence with a length of 1024 bits is obtained. An ideal random number generator characteristic is that the expected 512-bit value is 0 and the 512-bit value is 1. Monobit test results are given in Table III. As can be seen from the Table III, the proposed generator meets the Monobit randomness requirements. That is, the difference between the number of zeros and the number of one for the 1024-bit value is only 10.

Another statistical randomness test is the chi-square test. Definition of this test is that "A chi-square statistic compares these substring proportions to the ideal 1/2. The statistic is referred to a chi-squared distribution with the degrees of freedom equal to the number of substrings. The chi-squared distribution is used to compare the goodness-of-fit of the observed frequencies of a sample measure to the corresponding expected" [3].

TABLE III. MONOBIT TEST RESULTS.

	Expected	Observed
Number of 0 s	512	502
Number of 1 s	512	522

According to the chi-square test, the expected frequency values are 256/16 = 16 for each number from 0 to 15. Observed values are given in Table IV.

TABLE IV. CHI-SQUARE TEST RESULTS.

Number	Expected	Observed
0	16	13
1	16	15
2	16	19
3	16	14
4	16	14
5	16	18
6	16	20
7	16	21
8	16	19
9	16	13
10	16	15
11	16	17
12	16	14
13	16	12
14	16	11
15	16	21

Random numbers are generated between 0 and 15. Therefore, the degree of freedom (DF) of the chi-square test is 16. All confidence values for the degree of freedom 16 are given in Table V.

TABLE V. DEGREE OF FREEDOM TABLE.

	P-values					
DF	0.20	0.10	0.05	0.025	0.01	0.001
16	20.465	23.542	26.296	28.845	32.000	39.252

In order to be able to say that the random numbers produced are statistically random, the calculated chi-square value should be smaller than the values in the Table V. The calculated chi-square value is 10.125.

Analysis studies are performed on the 1024-bit obtained using the proposed method. The reason why tests are performed on 1024-bit lengths random numbers sequence is to show the practical usability of proposed method in conventional encryption algorithms, such as AES and RSA. The key length of the AES algorithm, which is a secret key encryption algorithm, is 256 bits and the key length of the RSA algorithm, which is an public key encryption algorithm, is 1024 bits.

One of the most commonly used examples to explain randomness is to generate a random bit sequence using coin tossing. In this experiment, heads are converted to 1 and tails are converted to 0. If this experiment is repeated a few times, it is going to be unbalance between the #0 and #1 distribution. However, if the experiment is repeated sufficiently, this unbalance is going to be lost because the experiment is random and the coin is fair. When the experimental results in Table III and Table IV are analysed, the small unbalance between the #0 and #1 is observed. This small unbalance is lost when the same tests are performed on the random number sequences greater than 1024-bit length to be obtained using the proposed algorithm. This analysis shows that the entropy source (outputs of fractional order chaotic Chua system) used in the proposed method has a random structure.

V. PERFORMANCE COMPARISONS AND DISCUSSION

In this section, a detailed comparison of the proposed method with the other chaos based RNG published in the last three years in the literature is given. In Table VI, RNG type, chaotic system class used as an entropy source, number of control parameters in chaotic system, number of initial conditions in the chaotic system, complexity of the algorithm used to convert outputs of chaotic system to random bits (numbers), and output bit rate are used as the comparison metric. Advantageous and disadvantageous aspects of the proposed method for each comparison metric are discussed in detail below.

The random number generators are divided into two general classes as described in Section III. In this paper, DRNG structure is proposed. However, it is planned to show that the proposed method can be implemented on FPGA for TRNG structure in future studies. In the proposed method, only mode operation is used to convert chaotic data to random outputs. Therefore, it is thought that the proposed method can be used without any problems in both DRNG and TRNG structures.

A serious problem of TRNG structures is that they require post-processing [8], [14], [25]–[28]. The aim of the post-processing is to eliminate the statistical dependence between the obtained data. In the TRNG structures given in Table VI, XOR operation is used as the post-processing. This operation reduces output bit rate by half. So half of the generated bits cannot be used. In the proposed method, it is claimed that this problem will not occur due to the uniform distribution provided by the mode operation. There is no post-processing step in DRNG structures. Therefore, such a problem is not going to be experienced.

The most striking parameter in RNG design is the chaotic system class. There are two basic approaches in the literature related to the choice of chaotic systems. The first approach is based on discrete time chaotic systems. As it can be seen in [8], [13]–[15], [18], [19], [29]–[32], the systems used in these RNG designs are low-dimensional chaotic systems. These designs are faster, but their reliability is questionable. Various cryptanalysis studies related to RNG designs based on low-dimensional chaotic systems makes this problem more evident [17], [20], [21]. The proposed approaches in [30]–[32] suggest several additional procedures to address these problems. However, this additional workload eliminates the advantageous aspect of the discrete time chaotic systems. As an alternative to these RNG based on discrete time chaotic systems, various designs based on continuous time chaotic systems are proposed [9], [10], [16], [22], [28]. However, these systems have serious problems. They are slow and requires post-processing. The dimension of the proposed method is lower than continuous time systems. It also has a structure as simple as discrete time chaotic systems.

At the end of this section, the conversion method of the other chaos based RNG in the literature is compared with the conversion method of proposed chaos based RNG. In the proposed method, mode operation is used. The advantages of the proposed method are both simple nature and good statistical characteristics of the mode operation.

TABLE VI. PERFORMANCE COMPARISION FOR CHAOS BASED RNG.

Reference	**RNG Type**	**Type of Chaotic system**	**Number of control parameters**	**Dimension**	**Method**	**The output bit rate**
[13]	DRNG	One-dimensional discrete chaotic map	1	1	Composition of permutations Virtually unlimited key space Dynamical degradation	1:1
[15]	DRNG	Sawtooth chaotic map	1	1	Mod and convert float to binary	1:1
[18]	DRNG	Coupled map lattice with time-varying delay Spatiotemporal chaotic system				1:1
[19]	DRNG	Coupling the piecewise and logistic maps	1	1	Selection of chaotic map and mod	1:1
[29]	DRNG	Single skew tent map	1	1	Comparison with a threshold value and dominant period property	1:1
[30]	DRNG	Polynomial combination of one-dimensional chaotic maps	Depending on the number of chaotic maps		Comparison with a threshold value	1:!
[31]	DRNG	Logistic map	4	4	Convert float to 32-bit binary selection combination	1:1
[32]	DRNG	Ikeda system with delay differential equation	4	4	Decimal digital discarding method	1:1
[8]	TRNG	Logistic map	1	1	GPU realization	2:1
[14]	TRNG	Tanh map	1	1	LFSR and Quantization	2:!
Proposed Method	DRNG	Fractional Chaotic Chua System	3	2.7	Mode operation	1:1
[9]	DRNG	New proposed chaotic system	5	4	Convert float to 32-bit binary	1:1
[10]	DRNG	New proposed chaotic system	4	3	Convert float to 32-bit binary	1:1
[16]	DRNG	Novel three-dimensional quadratic continuous autonomous chaotic system	1	3	Convert float to 32-bit binary	1:1
[22]	DRNG	Chaotic hyperjerk system	4	4	Convert float to 32-bit binary	1:1
[28]	TRNG	Memristive canonical Chua's oscillator and Logistic map	(4 + 1) = 5	(4 + 1) = 5	Comparison with a threshold value	2:1

VI. CONCLUSIONS

Fractional calculation and systems have become increasingly important. In parallel with this interest, in many applications, this calculation technique and systems have been widely studied. In this study, a random number generator based on fractional order chaotic systems is proposed. It is shown that the proposed generator meets the randomness requirements and can be used practically.

The original and advantageous aspects of the proposed method can be listed as follows. One of the most important results of the study is that fractional order chaotic systems may be an alternative to discrete time chaotic systems in the literature. This result may be the basis for many future studies. In the many applications based on discrete time chaotic systems, the latter are preferred to continuous time chaotic systems. The reason for this type of preference is explained by many designers: discrete time systems have a simpler structure (lower system degree) than continuous time systems. In this study, a practical application of the lower degree Chua system is carried out and the necessity of re-evaluating this view is revealed. It is thought that the future studies will bring new insights for applications, where discrete-time chaotic systems, such as design of optimization and encryption algorithms, are widely preferred [25], [26].

ACKNOWLEDGMENT

The author gratefully thanks to the Referee for the constructive comments and recommendations, which definitely helped to improve the readability and quality of the study.

REFERENCES

[1] L. O. Chua, "Chua's circuit: An overview ten years later", *Journal of Circuits, Systems and Computers*, vol. 4, no. 2, pp. 117–159, 1994. DOI: 10.1142/S0218126694000090.

[2] W. Schindler, "Random number generators for cryptographic applications", C .K. Koc (ed.): *Cryptographic Engineering*. Springer, Signals and Communication Theory, Berlin, 2009. DOI: 10.1007/978-0-387-71817-0_2.

[3] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication, Report no. 800–22rev1a, 2010.

[4] J. Sprott, *Elegant chaos: Algebraically simple chaotic flows*. World Scientific, 2010. DOI: 10.1142/7183.

[5] D. Mozyrska and M. Wyrwas, "Systems with fractional variable-order difference operator of convolution type and its stability", *Elektronika ir Elektrotechnika*, vol. 24, no. 5, pp. 69–73, 2018. DOI: 10.5755/j01.eie.24.5.21846.

[6] A. Dumlu, "Practical position tracking control of a robotic manipulator based on fractional order sliding mode controller", *Elektronika ir Elektrotechnika*, vol. 24, no. 5, pp. 19–25, 2018. DOI: 10.5755/j01.eie.24.5.21838.

[7] M. Stipčević and Ç. K. Koç, "True random number generators", in Koç Ç. K. (eds) *Open Problems in Mathematics and Computational Science*. Springer, Cham, 2014. DOI: 10.1007/978-3-319-10683-0_12.

[8] M. Al-Mazrooie, A. Akhavan, J. S. Teh, and A. Samsudin, "GPUs and chaos: a new true random number generator", *Nonlinear Dynamics*, vol. 82, pp. 1913–1922. DOI 10.1007/s11071-015-2287-7.

[9] S. Kacar, "Analog circuit and microcontroller based RNG application of a new easy realizable 4D chaotic system", *Optik*, vol. 127, no. 20, pp. 9551–9561, 2016. DOI: 10.1016/j.ijleo.2016.07.044.

[10] Ü. Çavus, A. Akgül, A. Zengin, and I. Pehlivan, "The design and implementation of hybrid RSA algorithm using a novel chaos based RNG, Chaos", *Solitons and Fractals*, vol. 104, pp. 655–667, 2017. DOI: 10.1016/j.chaos.2017.09.025.

[11] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system", *Signal, Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017. DOI: 10.1007/s11760-016-1007-1.

[12] E. Zambrano-Serrano, J. M. Muñoz-Pacheco, and E. Campos-Cantón, "Chaos generation in fractional-order switched systems and its digital implementation", *AEU - International Journal of Electronics and Communications*, vol. 79, pp. 43–52, 2017. DOI: 10.1016/j.aeue.2017.05.032.

[13] D. Lambic and M. Nikolic, "Pseudo-random number generator based on discrete-space chaotic map", *Nonlinear Dynamics*, vol. 90, pp. 223–232, 2017. DOI 10.1007/s11071-017-3656-1.

[14] J. V. C. Evangelist, J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, "Emitter-coupled pair chaotic generator circuit", *International Journal of Electronics and Communications (AEÜ)*, vol. 77, pp. 112–117, 2017. DOI: 10.1016/j.aeue.2017.04.029.

[15] M. A. Dastgheib and M. Farhang, "A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period", *Nonlinear Dynamics*, vol. 89, pp. 2957–2966, 2017. DOI 10.1007/s11071-017-3638-3.

[16] A. Ozdemir, I. Pehlivan, A. Akgul, and E. Guleryuz, "A strange novel chaotic system with fully golden proportion T equilibria and its mobile microcomputer-based RNG application", *Chinese Journal of Physics*, vol. 56, no. 6, pp. 2852–2864, 2018. DOI: 10.1016/j.cjph.2018.09.021.

[17] D. Lambic, A. Jankovic, and M. Ahmad, "Security analysis of the efficient chaos pseudo-random number generator applied to video encryption", *Journal of Electronic Testing*, vol. 34, pp. 709–715, 2018. DOI: 10.1007/s10836-018-5767-0.

[18] X. Lv, X. Liao, and B. Yang, "A novel pseudo-random number generator from coupled map lattice with time-varying delay", Nonlinear Dynamics, vol. 94, pp. 325–341, 2018. DOI: 10.1007/s11071-018-4361-4.

[19] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption", *Nonlinear Dynamics*, vol. 94, pp. 723–744, 2018. DOI: 10.1007/s11071-018-4390-z.

[20] D. Lambic, "Security analysis and improvement of the pseudo-random number generator based on quantum chaotic map", *Nonlinear Dynamics*, vol. 94, pp. 1117–1126, 2018. DOI: 10.1007/s11071-018-4412-x.

[21] D. Lambic, "Security analysis of the pseudo-random bit generator based on multi-modal maps", *Nonlinear Dynamics*, vol. 91, pp. 505–513, 2018. DOI: 10.1007/s11071-017-3885-3.

[22] S. Vaidyanathan, A. Akgul, S. Kacar, and U. Cavusoglu, "A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography", *The European Physical Journal Plus*, vol. 133, no. 2, pp. 46, 2018. DOI 10.1140/epjp/i2018-11872-8.

[23] M. Bakiri, C. Guyeux, J. Couchot, and A. K. Oudjida, "Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses", *Computer Science Review*, vol. 27, pp. 135–153, 2018. DOI: 10.1016/j.cosrev.2018.01.002.

[24] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption", *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, 2018. DOI: 10.1007/s11071-018-4056-x.

[25] Y. Mousavi and A. Alfi, "Fractional calculus-based firefly algorithm applied to parameter estimation of chaotic systems", *Chaos, Solitons & Fractals*, vol. 114, pp. 202–215, 2018. DOI: 10.1016/j.chaos.2018.07.004.

[26] Z. Liu and T. Xia, "Novel two dimensional fractional-order discrete chaotic map and its application to image encryption", *Applied Computing and Informatics*, vol. 14, no. 2, pp. 177–185, 2018. DOI: 10.1016/j.aci.2017.07.002.

[27] Z. M. Shah, M. Y. Kathjoo, F. A. Khanday, K. Biswas, and C. Psychalinos, "A survey of single and multi-component Fractional-Order Elements (FOEs) and their applications", *Microelectronics Journal*, vol. 84, pp. 9-25, 2019. DOI: 10.1016/j.mejo.2018.12.010.

[28] B. Karakayaa, A. Gülten, and M. Frasca, "A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation", *Chaos, Solitons and Fractals*, vol. 119, pp. 143–149, 2019. DOI: 10.1016/j.chaos.2018.12.021.

[29] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation", *Chaos, Solitons and Fractals*, vol. 118, pp. 134–144, 2019. DOI: 10.1016/j.chaos.2018.11.019.

[30] M. Asgari-Chenaghlu, M. Balafar, and M. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation", *Signal Processing*, vol. 157, pp. 1–13, 2019. DOI: 10.1016/j.sigpro.2018.11.010.

[31] A. M. Hemdan, O. S. Faragallah, O. Elshakankiry, and A. Elmhalaway, "A fast hybrid image cryptosystem based on random generator and modified logistic map", *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16177–16193, 2019. DOI: 10.1007/s11042-018-6948-7.

[32] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on improved random number generator and its implementation", *Nonlinear Dynamics*, vol. 95, no. 1, 2018. DOI: 10.1007/s11071-018-4659-2.