Pamukkale Univ Muh Bilim Derg, 28(5), 701-709, 2022

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

A novel analysis and applications of an introduced hyperchaotic system

Tanıtılmış bir hiperkaotik sistemin yeni bir analizi ve uygulamaları

Emrah TELLİ[1], *Zehra Gülru ÇAM TAŞKIRAN*[2*]

[1]Department of Electrical-Electronics Engineering, Faculty of Engineering, Mugla Sitki Kocman University, Mugla, Turkey.
emrahtelli@mu.edu.tr

[2]Department of Electronics-Communication Engineering, Fac. of Elect-Elec. Engineering, Yildiz Tech. Univ., Istanbul, Turkey.
zgcam@yildiz.edu.tr

Received/Geliş Tarihi: 30.04.2021 Revision/Düzeltme Tarihi: 02.09.2021 doi: 10.5505/pajes.2021.66178
Accepted/Kabul Tarihi: 22.10.2021 Research Article/Araştırma Makalesi

Abstract

In this study, the new analysis of the introduced hyperchaotic equation set was handled. The equation set was firstly analyzed mathematically and then the results were proven by designing a more efficient circuit with active elements. The aim of the study is offering an effective secure communication application and random number generator application. Hence, based on the new analysis of equation set, secure communication system and random number generation application were proposed. Accordingly, creating a Pseudorandom Number Generator is the halfway house in this study. The signals received from the chaotic oscillator were sampled at low frequency and with a simple post-processing, a bit stream was created. The resulting bit stream passed the NIST test successfully. The other halfway of the study is creating a secure communication system by the synchronization of two chaotic oscillators that are in transmitter and receiver. An identical noise-like signals are generated in both transmitter and receiver parts. At the transmitter part adding a noise-like chaotic signal to the information is done. At the receiver, this same noise-like signal is subtracted from the perceived signal. Thus, the information can be transmitted securely. Spice simulations of both proposed applications have been made and it has been shown that they are compatible with mathematical analysis. The proposed circuits are suitable for realization with commercially available circuit elements.

Keywords: Chaotic system, Chaotic synchronization, Circuit implementation, CCII+, Secure communication system, Pseudo-Random number generator.

Öz

Bu çalışmada, tanıtılmış bir hiperkaotik denklem setinin yeni bir analizi ele alınmıştır. Denklem seti önce matematiksel olarak analiz edilmiş, ardından aktif elemanlarla daha verimli bir devre tasarlanarak sonuçlar kanıtlanmıştır. Çalışmanın amacı, etkili bir güvenli iletişim uygulaması ve rastgele sayı üreteci uygulaması sunmaktır. Bu nedenle, denklem setinin yeni analizi temel alınarak güvenli iletişim sistemi ve rastgele sayı üretme uygulaması önerilmiştir. Bu bağlamda, bir Sözde Rastgele Sayı Üreticisi oluşturmak, bu çalışmadaki yolun yarısıdır. Kaotik osilatörden alınan sinyaller düşük frekansta örneklenmiş ve basit bir post-processing ile bit dizileri oluşturulmuştur. Elde edilen bit dizisi NIST testinden başarı ile geçmiştir. Çalışmadaki yolun diğer yarısı ise verici ve alıcıda bulunan iki kaotik osilatörün senkronizasyonu ile güvenli bir iletişim sistemi oluşturmaktır. Hem verici hem de alıcı parçalarda özdeş bir gürültü benzeri sinyal üretilir. Verici kısmında bilgiye gürültü benzeri kaotik bir sinyal eklenmektedir. Alıcıda, bu aynı gürültü benzeri sinyal algılanan sinyalden çıkarılır. Böylece bilgiler güvenli bir şekilde iletilebilir. Önerilen iki uygulamanın da SPICE benzetimleri yapılmış, matematiksel analizler ile uyumlu olduğu gösterilmiştir. Önerilen devreler, ticari olarak bulunan devre elemanları ile gerçeklenmeye uygundur.

Anahtar kelimeler: Kaotik sistem, Kaotik senkronizasyon, Devre uygulaması, CCII+, Güvenli haberleşme sistemi, Sözde-Rassal sayı üreteci.

1 Introduction

1.1 Analysis and applications of a hyperchaotic system

Nowadays, everything is demanded to be fast. This approach has made powerful progress in digitalization. Today, from bank accounts to social security issues, everything has found its place in the digital world. Even food or market orderings are possible while staying seated on the couch. Although this transformation makes daily life easier, there are also some disadvantages brought by digitalization. At the same time that they have digitalized, they became open to some risks. The risks are mainly related to information security. All verification and payment process depends on some personal information. Card numbers, passwords need to transmit in the process. As mentioned above lots of information is transmitted through communication channels, and sometimes this information can be very confidential. Like in all communication methods, channels can be reached from multiple receivers. Sometimes, especially in this case, it can be a digital eavesdropper. Considering the information is confidential, it is completely undesirable. Thus, the increasing security requirements in communication and data storage has pushed developers to find new solutions. Chaos theory has applications that can meet these requirements. The application examples can be given as secure chaotic communication systems which are proposed as the secure way to transmit information and random number generators (RNGs) which stand a good way of data encryption [1]-[3]. Correspondingly, chaos theory has specific implementations as chaotic image encryption applications [4]-[6], industrial internet of things (IoT) [7], communication of interconnected embedded devices [8], extinguishment of the security drawbacks of Vigenère cipher algorithm used by cryptography systems [9], and besides data encryption, chaos theory has some applications to do with biological modelling [10], financial estimations [11], industry management [12].

*Corresponding author/Yazışılan Yazar

In the referred image encryption application [4], Liu et al. suggested a method based on chaos theory and public-key cryptography (double random phase encoding) for a system that is capable to make optical encryption and decryption respectively in 0.0245s and 0.072s. It is an illustrative example of chaos theory usage in optical communication systems. In the referred industrial IoT application [7], thanks to chaos theory two HR-coupled neuron systems were synchronized better with good stability to be used in industrial IoT. Similarly, in the communication of embedded devices [8], chaos theory meets the requirements of confidentiality for information transmission used in Wireless Sensor Networks (WSN) and IoT. For data encryption chaos theory offers fast, reliable solutions either in optical transmission or WSN applications.

As it is seen from the referred studies chaos is a very part of life. For the reason that chaos theory exhibits unpredictability, similarity to randomness, reproducibility, synchronization and, sensitivity to initial conditions, it suits well to the all referential applications [13].

In this study, secure communication and random number generation applications were focused. In secure chaotic communication systems / applications, a transmitted signal is encoded and hidden, and for this reason, it is very important to obtain the data as close to its original by decoding it correctly. Also, since chaotic systems are very sensitive, the system must be well synchronized [14],[15]. There are many methods proposed for the synchronization of chaotic systems in the literature [16]-[18].

Random number generators have two types: Pseudorandom Number Generators (PRNGs) and True Random Number Generators (TRNGs). Generators that produce a sequence seems random at the end of a certain algorithmic process are called PRNG, while the hardware entropy sources that include the noise in the system are called TRNG. In RNGs, the system must ensure some specific tests as autocorrelation, bitmap, frequency, cumulative sums, etc. [19]. The success of a random number generator is scaled by the amount of test accomplished. There are test suites that used for testing random number generators, like NIST and Diehard [19]-[21].

For creating these applications, chaotic systems that create strange attractors were proposed. Chaotic systems are nonperiodic, inherently unpredictable, and highly sensitive to their initial conditions [22]. These unique properties make chaotic systems useful for applications like secure communication and data encryption.

Chaotic systems are given as differential equation sets, and with some specific coefficients that make them behave chaotically. The first chaotic system that creates chaotic attractors found in 1963 by Edward Lorenz [23]. It is a three-dimensional chaotic system found while studying atmospheric convection. The equation set which is named by Lorenz is given below as Equation (1).

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \end{cases} \quad (1)$$

Lorenz equation set which is given by Equation (1) behaves chaotically with coefficients a=10, b= 8/3, c=28.

Following studies in this field have made available many chaotic system equation sets and electronic circuits depended on them. In 1990, the synchronization idea of two chaotic systems is suggested by Pecora and Carroll [24]. According to Pecora and Carroll synchronization of chaotic oscillator circuits may create an opportunity for secure communication. It was an essential step to form a chaotic communication system. The first chaotic system that is used to transmit information securely is defined in 1993 by K. M. Cuomo et al. [25]. Cuomo et al. used two chaotic oscillator circuits created by using the Lorenz equation set as transmitter and receiver with the synchronization idea. In 1992, Parlitz et al. used Chua's circuit to create a communication system [26]. In 1997, A. Iglesias et al. similarly used the Chua's circuit to create a secure communication system, they have achieved to send a masked picture with this system [27]. In 2009, Arman et al. defined a new fractional chaotic communication system based on extended fractional Kalman [28]. This is a different approach that uses the fractional Lorenz equation set. Lately, there are popular studies on chaotic secure communication systems implemented by electronic components using active elements as op-amps [29],[30], current conveyor (CCII+) [31],[32], DVCCs [33] etc. In 2020 Alçın et al. used CCII+ while designing Sundarapandian-Pehlivan Chaotic Oscillator (SPCO) to create FPGA for secure communication implementation [14].

The first attempt to create random numbers happened in 1927. L.H.C. Tippett developed a table that includes 41.600 random numbers and this table is published in Cambridge University Press [34]. In May 1947, RAND corporation started creating random numbers by using an electronic simulation of a roulette wheel, and this study was published in 1955 as a random number book named A Million Random Digits with 100,000 Normal Deviates [35]. In 2018, circuit designs and applications of 4D hyperchaotic equation set is done. In this study PRNG is created to mask an image [36]. Soon, generating RNGs which are ensuring tests and giving response fast in real-time applications are important. In 2020, B. Widynski explained a counter-based method named Squares RNG. Widynski defines the method as one of the fastest counter-based RNG of all time [37].

In this study, the hyperchaotic system, which is defined by Bao Bocheng, Liu Zhong & Xu Jianping in 2009 is handled to accomplish given applications [38]. Bocheng et al. explained both three-dimensional and four-dimensional chaotic systems in their study. The Equation set of the hyperchaotic system is given below by Equation (2).

$$\begin{cases} \dot{x} = a(x - y) \\ \dot{y} = xz - cy + w \\ \dot{z} = xy - bz \\ \dot{w} = d(x + y) \end{cases} \quad (2)$$

Bocheng equation set behaves chaotically with coefficients a=20, b=4, c=32, d=70. Equation set behaves periodically if d=92 with the same other conditions. Chaotic behaving signals generates chaotic attractors when the signals are plotted according to each other. Chaotic attractor is composed of two or three non-intersecting, non-periodic chaotic signals. According to the number of signals, shape is called 2D or 3D chaotic attractor and the graph is named Phase portraits. The three-dimensional chaotic attractor shape of Bocheng equation set is given in the Figure 1.

Bao Bocheng et al. defined chaotic and hyperchaotic systems in their study and they proposed applications of chaotic systems by using operational amplifiers by LM741 or LF347, and multipliers by AD633 [39]-[41]. The handled study was

including a parallel synthesis method while designing the circuit and extra numbers of elements were used. In this study, the suggested structure includes active elements like analog amplifiers and current conveyors to reduce noise and cost in circuit through reducing element numbers.

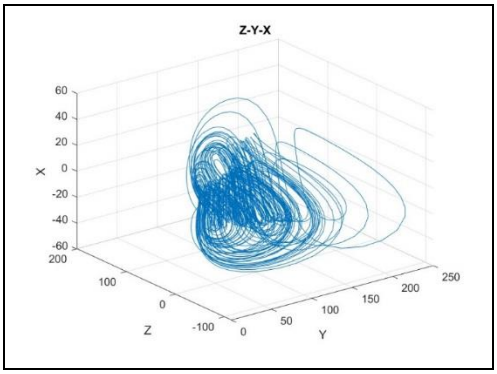


Figure 1. Phase portraits of Z-Y-X variables of bocheng equation set.

2 Analysis of dynamical differential equation set

Clearly, the origin (0,0,0,0) is the unique equilibrium of the differential equation set that is given by Equation (2). The handled equation set behaves chaotic with the initial conditions x(0)=1, y(0)=1, z(0)=1 and w(0)=0 and parameters a=20, b=4, c=32, d=70. The analysis of the differential equation set was done to acquire chaotic behavior of variables. Time series and phase portraits were obtained theoretically by solving differential equations with giving chaotic parameters and chaotic initial conditions using MATLAB [42]. Time series is the time-based plotted signals. If the examined signal is chaotic, time-based plotted signal shouldn't be periodic or repetitive at any time. Time series of X and Z variable in the equation set is given in Figure2.

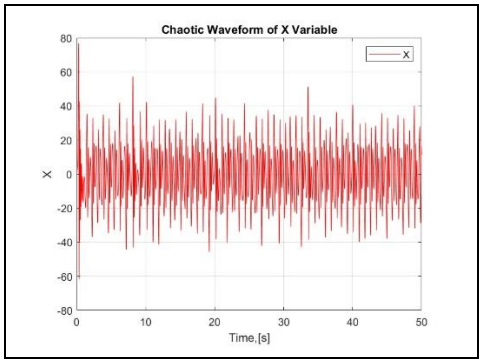


Figure 2. Time series of X variable.

As it was explained before, phase portraits were generated by plotting instantaneous state of two or three chaotic variables according to each other. They are famous for generating shapes like the wings of butterflies which is given by Figure 3.

These oscillations were obtained with chaotic parameters, on the other hand by using periodic parameters (a=20, b=4, c=32, d=92) a shape drawn by a singular line should be obtained as illustrated by Figure 4.

Figure 4 is the same phase portrait given in Figure 1 with the exception of changing parameters from chaotic to periodic. As reported before, phase portraits of the periodic signals need to be close to the single-line shape. In the Figure 4 the gathered shape is almost a single line.

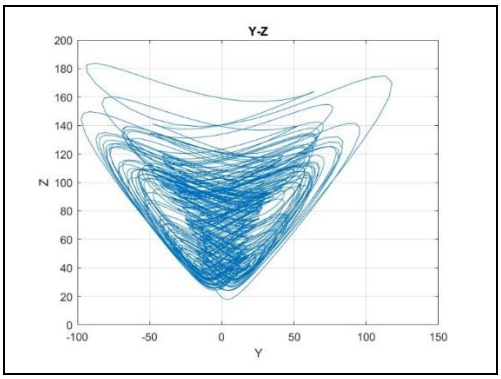


Figure 3. Phase portraits of Y - Z variables.

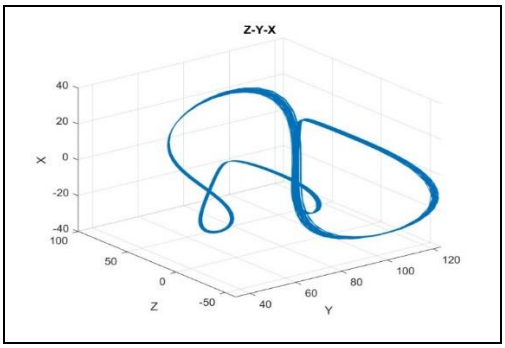


Figure 4. Phase portrait of Z-Y-X variables with periodic parameters.

2.1 Lyapunov Exponentials and Bifurcation Diagram

The divergence of the system can be calculated as given in Equation (3).

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = a - b - c \tag{3}$$

By using the chaotic parameters Equation (3) becomes $\nabla V = 20 - 32 - 4 < 0$. Because the divergence is negative, the system is dissipative and support the chaotic attractors.

The Lyapunov exponents were calculated as L_1=0.936, L_2=0.078, L_3=-0.723 and L_4=-16.291 with parameters a=20, b=32, c=4, d=70 [43]. By using these exponents, the Lyapunov dimension or Kaplan - Yorke dimension [44] can be calculated as given in Equation (4).

$$D_{ky} = j + \frac{1}{|L_{j+1}|}\sum_{i=1}^{j} L_i \tag{4}$$

Here '*j*'is the largest integer for which $L_1 + \cdots + L_n \geq 0$. For the system $L_1 + L_2 + L_3 > 0$ and *j=3*. Thus, the Kaplan - Yorke dimension was acquired by solving Equation (4) as,

$$D_{ky} = 3 + \frac{L_1 + L_2 + L_3}{|L_4|} = 3.0186.$$

Lyapunov exponentials are standards for being chaotic. When variables are plotted as Lyapunov exponentials according to time if the highest exponential is positive (>0) equation set is accepted to be chaotic. If there are no positive exponentials, this equation set converges to a constant value. If there are more than one positive exponential, the equation set is accepted as

hyperchaotic [43]. In this study, there are two positive Lyapunov exponents (L1 and L2) and the sum of Lyapunov exponents are negative, which means this equation set is hyperchaotic. Lyapunov exponents obtained mathematically of the Bocheng equation set were given by Figure 5.

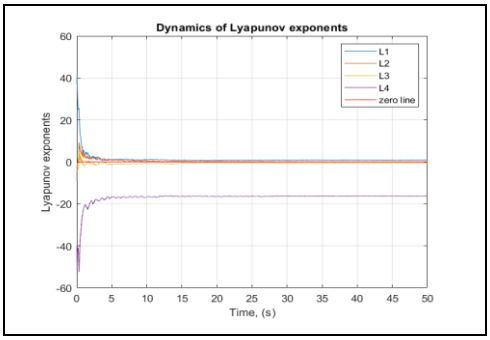


Figure 5. Lyapunov exponents.

A bifurcation diagram is the plotting of one variable according to one parameter of the equation set. Here is 'd' parameter was chosen for adjustment. According to changing values of 'd', peak values of Z are obtained. Classifying the equation set's behaviour as regards parameter values is possible. Considering the given plotting, line-like parts of the graph give the 'd' parameters for the periodic or quasi-periodic behaviour. The points on the graph that have a lot of dots show chaotic behaviour parameters. As this number increases, chaotic oscillations of the equation set increase as well. Bifurcation diagram is shown in Figure 6.

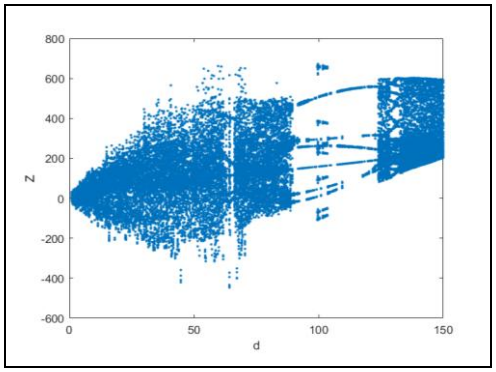


Figure 6. Bifurcation diagram.

As it is seen from the given Figure 6 at the point d=92, there is a periodic or quasi-periodic appearance. Also, at the point d=70, chaotic behaviour can be seen. After the given analyses were done, modelling these chaotic variables by capacitors, and modelling these equations with required circuit elements like analog multipliers, current conveyors should be done to process real-life implementations.

3 Circuit design of hyper chaotic oscillator

Each chaotic variable was modeled through capacitor voltages. Thus, each equation in the equation set has become a node equation in accordance with the current-voltage definition relation of the capacitor element. The circuit design has been made by connecting one terminal of the grounded capacitors to these nodes. Chaotic parameters were provided with passive element values in the circuit. At this stage, coefficients of equations were modelled by elements as capacitors and resistors. Thus, the chaotic oscillator which is given by Figure 7 circuit was composed.

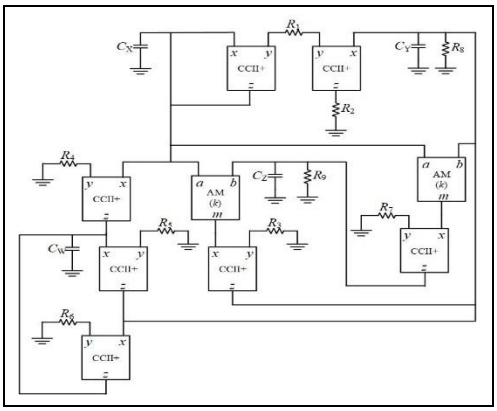


Figure 7. Chaotic oscillator circuit design.

After the analyses were done with chaotic parameter values, some element values were acquired using MATLAB. These element values needed to be normalized first to be expanded to applicable values. Therefore, element values were normalized first then the mathematical analyses were done with these normalized element values. Next, the values were changed to applicable denormalized values by extending them proportionally. Thus, applicable denormalized element values were acquired. For the purpose of getting optimum results, some optimization was done to the values experimentally. The used element values can be found in Table 1.

Table 1. Denormalized element values

Element	Value	Element	Value
C_x	$5x10^{-9}$ F	R_4	160 Ω
C_y	$6.25x10^{-9}$ F	R_5	5 kΩ
C_z	$25x10^{-9}$ F	R_6	5 kΩ
C_w	$2.86x10^{-9}$ F	R_7	5 kΩ
R_1	10 kΩ	R_8	40 Ω
R_2	10 kΩ	R_9	160 kΩ
R_3	10 kΩ	k (AM)	0.1

Applying this extended element values to equations denormalized parameter values were obtained as in Table 2.

Table 2. Denormalized parameter values.

Parameter	Formula	Value
a	$1/(C_x*R_1)$	20000
b	$1/(C_z*R_3)$	4000
c	$1/(C_y*R_7)$	32000
d	$1/(C_w*R_6)$	70000

When the same time series and phase portraits with the theoretical solutions were achieved through OrCAD simulations given by Figure 8 and Figure 9 the design of an applicable chaotic oscillator is completed. In all simulations, the commercially available AD844 integrated circuit was used as CCII + by leaving the w port open, and the AD633 integrated circuit was used as an analog multiplier.

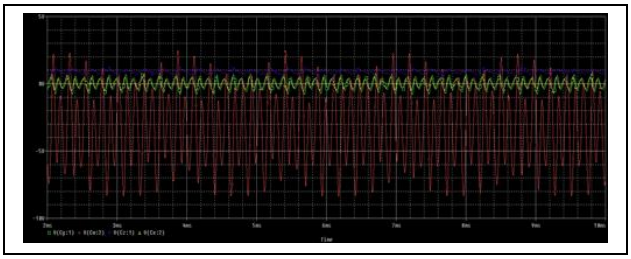


Figure 8. Time series of the four variables.

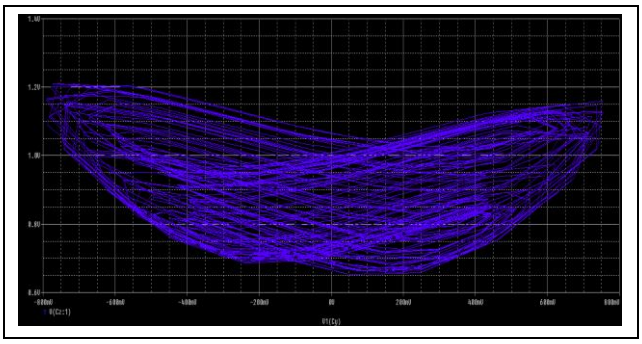


Figure 9. Phase portrait of Y - Z variables.

4 Applications of dynamical differential equation set

As reported before, chaotic oscillators have some applications in secure communication systems through synchronization and in safe data storage systems through the pseudorandom number/bit sequence generation.

4.1 Secure communication system

Chaotic oscillators and their circuits have some usage in terms of modulation of the information signal. This modulation creates unpredictability and safety of the information signal, it adds irregular appearance to the information signal. The classical method in chaotic communication is to add a chaotic variable to the information signal to be transmitted in the transmitter part, to ensure that the transmitted signal has a noise-like structure. In this way, a perception is created that the transmitted signal does not carry any information. In the receiver part, it must be the same as the chaotic signal added, so that the information can be retrieved with a simple subtraction process. For this reason, the synchronization of the receiver and transmitter is very important. The method for synchronization was provided through difference addition by connecting two variables/capacitors with a current conveyor and a resistance [8]. This method requires to add a difference term or an error term. Therefore, an error term has been added to the equation on the receiver side of the 'z' variable selected for synchronization. The value $\varepsilon = {}^{1}/_{500C_y}$ was determined as the error term coefficient.

Related equations for both transmitter and receiver circuits were given respectively by Equation (5) and Equation (6).

$$\begin{cases} \dot{x_t} = \dfrac{1}{C_x R_1}(x_t - y_t) \\ \dot{y_t} = x_t z_t - \dfrac{1}{C_y R_7} y_t + w_t \\ \dot{z_t} = x_t y_t - \dfrac{1}{C_z R_3} z_t \\ \dot{w_t} = \dfrac{1}{C_w R_6}(x_t + y_t) \end{cases} \tag{5}$$

In the Equation (5) all parameters were identified as (x_t, y_t, z_t, w_t) for transmitter.

In the Equation (6) all parameters were identified as (x_r, y_r, z_r, w_r) for receiver. As an error term '$\varepsilon(z_t$-$z_r)$' was added to the equation for variable Z.

$$\begin{cases} \dot{x_r} = \dfrac{1}{C_x R_1}(x_r - y_r) \\ \dot{y_r} = x_r z_r - \dfrac{1}{C_y R_7} y_r + w_r \\ \dot{z_r} = x_r y_r - \dfrac{1}{C_z R_3} z_r - \varepsilon(z_t - z_r) \\ \dot{w_r} = \dfrac{1}{C_w R_6}(x_r + y_r) \end{cases} \tag{6}$$

These two chaotic signals must be generated at the same time, in other words, these oscillators need to be synchronized for addition in the transmitter and subtraction in the receiver at the same moment with the same value.

In this sense, the circuit given by Figure 10. was composed theoretically.

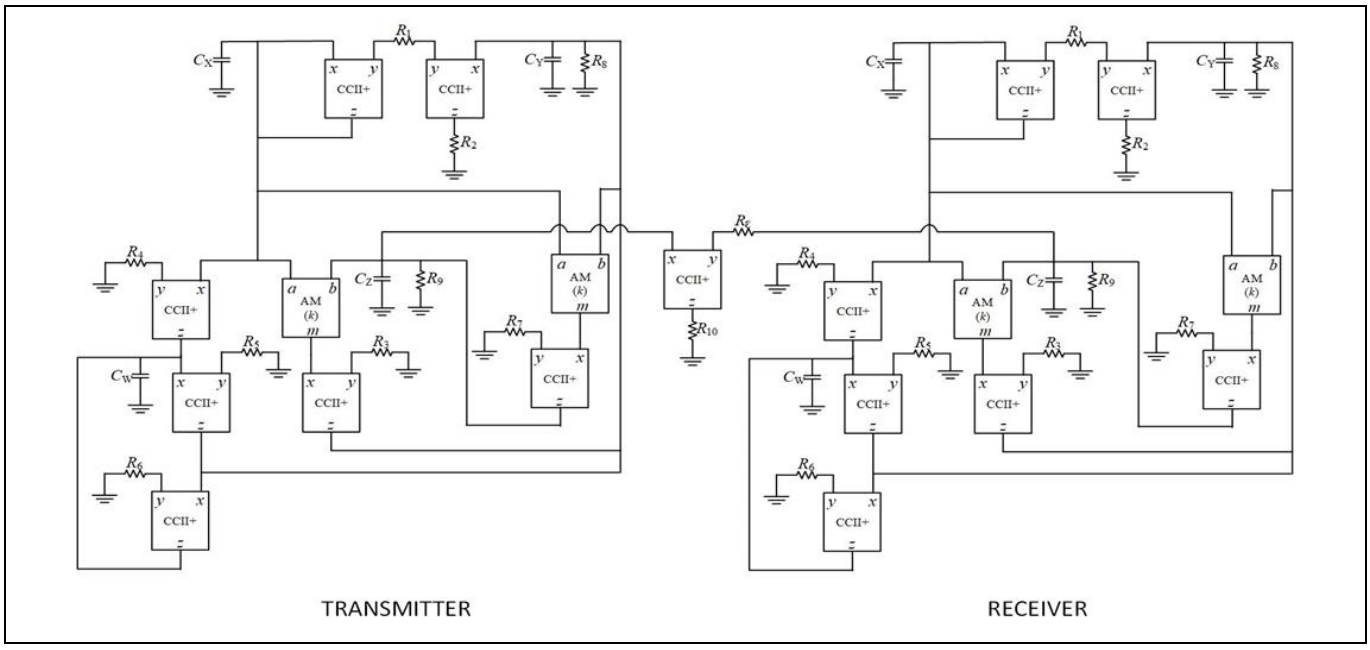


Figure 10. Secure communication system circuit design.

Then, by using OrCAD software, circuits were simulated and executed. The same results with theoretical solutions and OrCAD simulations for secure communication system were obtained using denormalized design parameters in Table 2.

Synchronization of two identical chaotic oscillators in the transmitter and in the receiver was achieved. Figure 11 shows the synchronization of X variables/capacitor voltages in approximately 1.1 ms. Figure 12 shows the synchronization of Z variables/capacitor voltages in the same small-time.

In this example, a sinusoidal signal which has 1 kHz frequency, and 0.1 V amplitude was used as information signal. By the addition of this synchronized signal to the information signal, an information-carrying signal with a noise-like appearance was obtained. This signal was shown in Figure 13 As can be seen, the signal transmitted from the transmitter to the receiver is of an unpredictable structure, similar to noise.

In the receiver part, this identical noise-like signal was subtracted from the received signal. It can be seen from Figure 14 that after the synchronization was achieved, the information signal, in this case, it is a sinus signal was obtained purely.

4.2 Pseudorandom number generator

The other application of this study is the pseudorandom number generator. This PRNG can have applications like frequency modulation so, again a secure communication system can exist through software. But the primary application of PRNG is the encryption of stored data. Unpredictable chaotic bit sequences generated from PRNG can be added to any digital signal. And this chaotic signal becomes the key to the stored data.

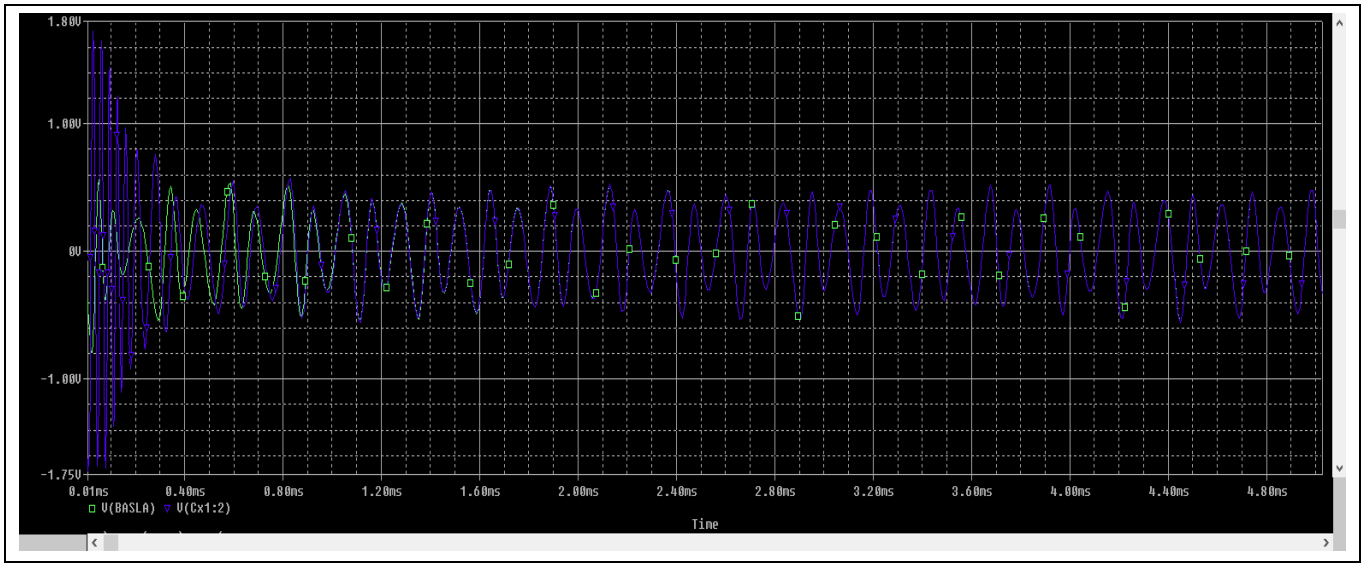


Figure 11. Synchronization of X variables in simulation with applicable parameters.

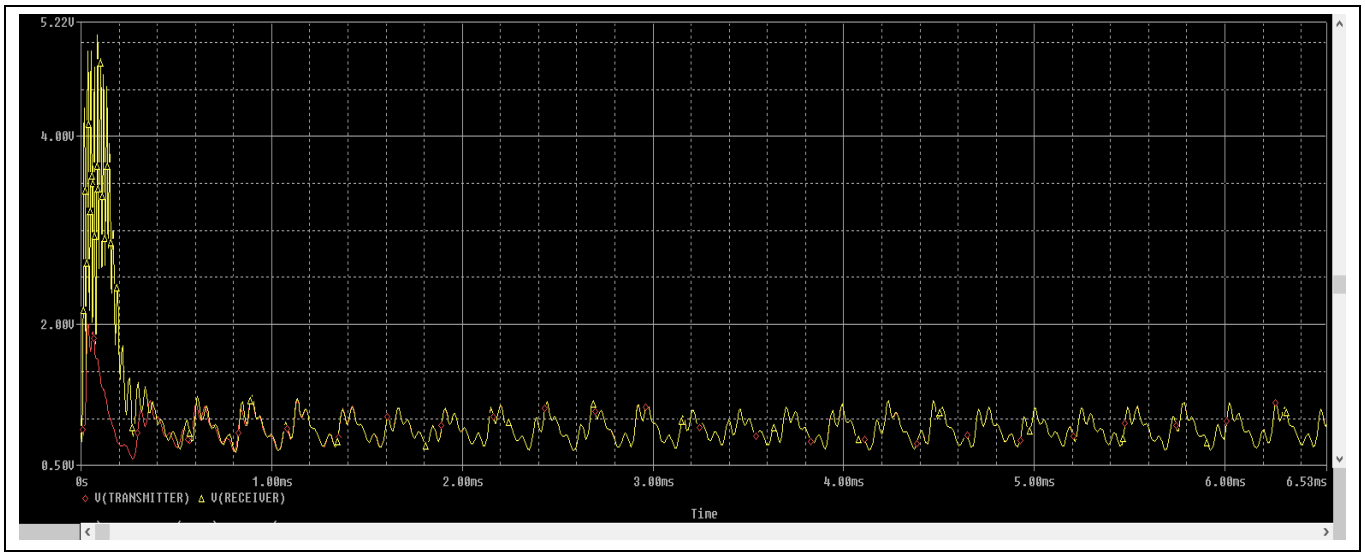
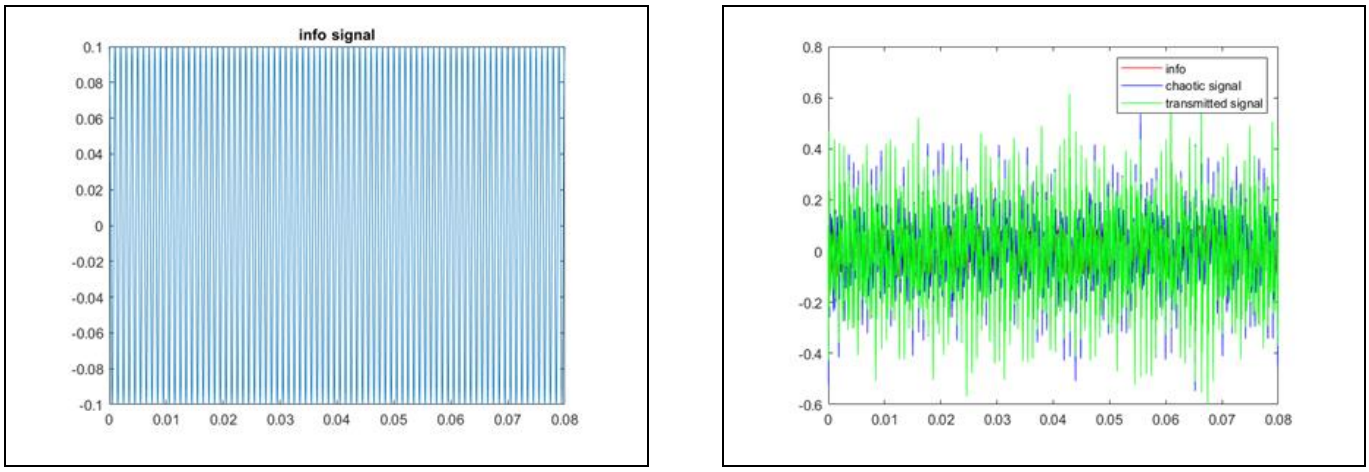
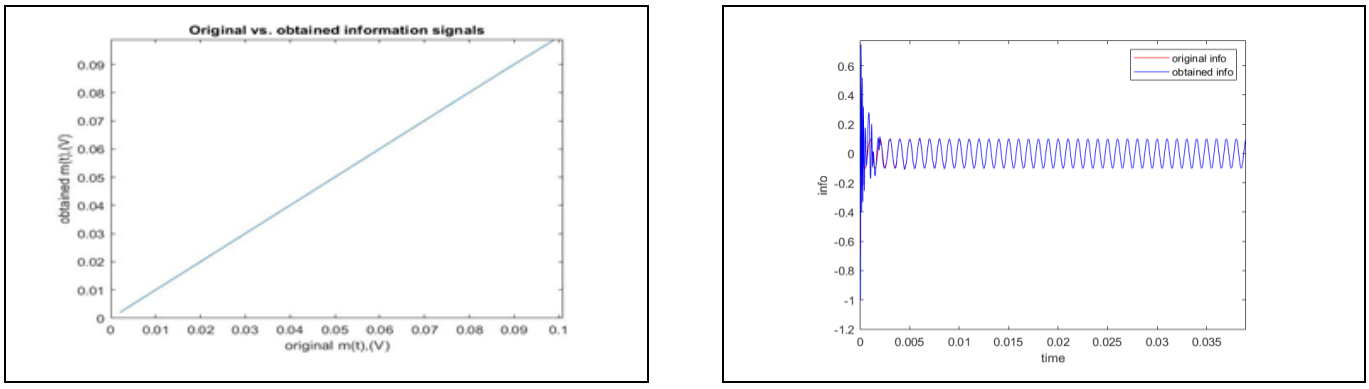


Figure 12. Synchronization of Z variables in simulation with applicable parameters.



(a) (b)

Figure 13. Masking of the information signal by chaotic signal. (a): Information signal. (b): Info, chaotic and masked info (transmitted) signals.



(a) (b)

Figure 14. Comparing obtained information signal with original information signal after the subtraction of synchronized chaotic signal. (a): Obtained info signal vs. original info signal. (b): Obtained info signal with original info signal.

In this study, the PRNG was generated by examining the voltage of the X capacitor. Samples taken from the X channel of the chaotic oscillator were sampled for 818 seconds at a sampling frequency of 600 Hz. After the sampled data was converted into float type numbers, the second digits after the comma were examined. If this number is an odd number, logic'1 ', if it is an even number, logic'0' is recorded to create a bit sequence. The size of the generated bit sequence is 490772.

4.2.1 Test results obtained from NIST

After the bit sequence was generated, to approve the randomness of the sequence, the sequence was applied to NIST tests as a 10-bit stream, and the results were obtained.

In the results shown in Table 3, P-value should be greater than 0.01 to be considered random in each category like Frequency, Cumulative sums, Linear complexity, etc. This is the number of bits that are rejected in the percentage. Considering obtained P-value results from NIST tests given in Table 3, the bit-stream deserves to be named random. Thus, for the applications of frequency modulation and safe data storage 490772 pieces of random bits were generated in this study. These bits were passed the randomness tests of NIST successfully.

5 Conclusion

In the study in which the examined and applied equation set was introduced [29], a circuit that realizes this set of equations was also proposed. The circuit proposed in the original article is opamp-based and contains 12 active elements. The CCII+ based circuit proposed in this study contains 9 active elements. The reduction of the number of elements is an advantage considering noise reduction and compactness of communication devices. Consequently, with the different approach, the circuit application of a secure communication system was achieved by synchronizing two identical chaotic oscillators. This circuit was composed of applicable element values to prove that it can be implemented in real life.

Also, for safe data storage applications and secure communication systems pseudorandom 490772 bits were generated in 818 seconds. This bit sequence has passed from NIST randomness tests, it deserves the 'random' title. The proposed receiver and transmitter configurations can be realized with commercially available elements. Since the proposed PRNG has the same structure, it can be converted into a TRNG by the physical implementation of the oscillator.

Table 3. Test results obtained from NIST.

C1-C10	P-Value	P-Value(KS)	Proportion	Statistical Test
1102200202	0.534146	0.870255	1.0	Frequency
3000120112	0.350485	0.727604	1.0	Block Freq.
0111211111	0.991468	0.882752	1.0	Cum. Sums
2200200022	0.350485	0.518107	1.0	Cum. Sums
0201204010	0.066882	0.720258	1.0	Runs
0021112111	0.911413	0.547014	1.0	Longest Run
2001212101	0.739918	0.829654	1.0	Rank
1012020004	0.066882	0.221796	0.9	FFT
1113101110	0.739918	0.648186	1.0	NonOverlappingTemp.
0001031203	0.122325	0.047416	1.0	NonOverlappingTemp.
1201111201	0.911413	0.987851	1.0	NonOverlappingTemp.
0020103121	0.350485	0.218509	1.0	NonOverlappingTemp.
0210111211	0.911413	0.857053	1.0	Serial
0211110022	0.739918	0.681475	1.0	Serial
2111011030	0.534146	0.806425	1.0	Linear Complexity

Also, for proposed PRNG, the bit stream can be extended with longer generation times. On the secure communication side, the proposed scheme effectively ensures security with a synchronization time of 1.1 ms. It is suitable for commercial consumer electronics. The simulation results of the proposed circuit and test results of random number generation demonstrate the productiveness and effectiveness of the study. The security issue of frequently transmitted information can be solved by further implementations in real life thanks to the applicable circuit proposed in this study.

6 Acknowledgments

The author would like to thank the anonymous reviewers whose comments and feedback have improved the text significantly.

7 Author contribution statements

In the scope of this study, Emrah TELLİ contributed data collection, conducting the analyses, literature review, writing and assessment of the obtained results, Zehra Gülru ÇAM TAŞKIRAN formation of the idea, design, supplying the materials, writing and assessment of the obtained results.

8 Ethics committee approval and conflict of interest statement

There is no need to obtain permission from the ethics committee for the article prepared. There is no conflict of interest with any person / institution in the article prepared.

9 References

[1] Corron NJ, Hahs DW. "A new approach to communications using chaotic signals". *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applictions*, 4(5), 373-382, 1997.

[2] Aydos M, Ugur A. "Chaotic image encryption with random shuffling of data". *Pamukkale University Journal of Engineering Sciences*, 20(2), 31-35, 2014.

[3] Aydın Ö, Kösemen C. "XORSHIFTUL+: A novel hybrid random number generator for internet of things and wireless sensor network applications". *Pamukkale University Journal of Engineering Sciences*, 26(5), 953-958, 2020.

[4] Liu Y, Jiang Z, Xu X, Zhang F, Xu J. "Optical image encryption algorithm based on hyper-chaos and public-key cryptography". *Optics & Laser Technology*, 127(1), 1-10, 2020.

[5] Wang X, Zhao M. "An image encryption algorithm based on hyperchaotic system and DNA coding". *Optics & Laser Technology*, 143(1), 21-28, 2021.

[6] Gao X. "A color image encryption algorithm based on an improved Hénon map". *Physica Scripta,* 96(6), 12-20, 2021.

[7] Wang T, Wang D, Wu K. "Chaotic adaptive synchronization control and application in chaotic secure communication for industrial internet of things". *IEEE Access*, 6(1), 8584-8590, 2018.

[8] Zirem A, Senouci MR. "Efficient lightweight chaotic secure communication system for WSNs and IoT". *2018 International Conference on Smart Communications in Network Technology SaCoNeT 2018*, 43-48, El Oued, Algeria, 27-31 October 2018.

[9] Triandi B, Ekadiansyah E, Puspasari R, Iwan LT, Rahmad F. "Improve security algorithm cryptography vigenere cipher using chaos functions". *2018 6th International Conference on Cyber and IT Service Management CITSM 2018*, Parapat, Indonesia, 7-9 August 2018.

[10] Çetin M, Beyhan S. "State and parameter estimation of uncertain brain cortex model". *University Journal of Engineering Sciences*, 24(8), 1425-1434, 2018.

[11] Klioutchnikov I, Sigova M, Beizerov N. "Chaos theory in finance". *Procedia Computer Science*, 119(2017), 368-375, 2017.

[12] Levy D. "Chaos theory and strategy: theory, application, and managerial implications". *Strategic Management Journal*, 15(2), 167-178, 1994.

[13] Hilborn RC. *Chaos and Nonlinear Dynamics: An Introduction For Scientists and Engineers*. 2nd ed. New York, USA, Oxford University Press, 2000.

[14] Alçın M, Tuna M, Pehlivan İ, Koyuncu İ. "CCII current conveyor and dormand-prince-based chaotic oscillator designs for secure communication applications". *International Advanced Researches and Engineering Journal*, 4(3), 217-225, 2020.

[15] Kolumbán G, Kennedy MP, Chua LO. "The role of synchronization in digital communications using chaos-Part II: Chaotic modulation and chaotic synchronization". *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications*, 45(11), 1129-1140, 1998.
[16] Sambas A, Mada Sanjaya WS, Mamat M, Tacha O. "Design and numerical simulation of unidirectional chaotic synchronization and its application in secure communication system". *Journal of Engineering Science and Technology Review*, 6(4), 66-73, 2013.
[17] Chen HC, Chang JF, Yan JJ, Liao TL. "EP-based PID control design for chaotic synchronization with application in secure communication". *Expert Expert Systems with Applications*, 34(2), 1169-1177, 2008.
[18] Wen G, Wang QG, Lin C, Li G, Han X. "Chaos synchronization via multivariable PID control". *International Journal of Bifurcation and Chaos*, 17(5), 1753-1758, 2007.
[19] Rukhin A, Soto J, Nechvatal J. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, Maryland, USA, 2010.
[20] Lü J, Chen G, Cheng D. "A new chaotic system and beyond: The generalized lorenz-like system". *International Journal of Bifurcation and Chaos*, 14(5), 1507-1537, 2004.
[21] Zhang Z. A Multi-threaded Cryptographic Pseudorandom Number Generator Test Suite, MSc Thesis, Naval Postgraduate School, Monterey, United States, 2016.
[22] Jiang ZP. "A note on chaotic secure communication systems". *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 49(1), 92-96, 2002.
[23] Lorenz EN. "Deterministic nonperiodic flow". *Journal of Atmospheric Sciences*, 20(2), 130-141, 1963.
[24] Pecora LM, Carroll TL. "Synchronization in chaotic systems". *Physical review letters, 64(8),* 821-824, 1990.
[25] Cuomo KM, Oppenheim AV. "Circuit implementation of synchronized chaos with applications to communications". *Physical Review Letters*, 71(1), 65-68, 1993.
[26] Parlitz U, Chua LO, Kocarev L, Halle KS, Shang A, "Transmission of digital signals by chaotic synchronization". *International Journal of Bifurcation and Chaos*, 2(4), 973-977, 1992.
[27] Iglesias A, Gutierrez JM, Ansotegui D, Carnicero MA. "Transmission of digital signals by chaotic synchronization. Application to secure communications". *WIT Transactions on Engineering Sciences*, 15(1), 1-8, 1997.
[28] Kiani-B A, Fallahi K, Pariz N, Leung H. "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter". *Communications in Nonlinear Science and Numerical Simulation*, 14(3), 863-879, 2009.
[29] Tchitnga R, Nguazon T, Fotso PHL, Gallas JAC. "Chaos in a single op-amp-based jerk circuit: Experiments and simulations". *IEEE Transactions on Circuits and Systems II: Express Briefs*, 63(3), 239-243, 2015.
[30] Emiroglu S, Akgül A, Adıyaman Y, Gümüş TE, Uyaroglu Y, Yalçın MA. "A new hyperchaotic system from T chaotic system: dynamical analysis, circuit implementation, control and synchronization". *Circuit World*, 2021(2), 1-13, 2021.
[31] Sahin ME, Cam Taskiran ZG, Guler H, Hamamci SE. "Application and modeling of a novel 4D memristive chaotic system for communication systems". *Circuits, Systems and Signal Processing*, 39(7), 3320-3349, 2020.
[32] Yu F, Shen H, Liu L, Zhang Z, Huang Y, He B, Cai S, Song Y, Yin B, Du S, Xu Q. "CCII and FPGA realization: A multistable modified fourth-order autonomous Chua's chaotic system with coexisting multiple attractors". *Complexity*, 2020(1), 1-17, 2020.
[33] Joshi M, Ranjan A. *Realization of Novel Multi-scroll 2D Chaotic Oscillator Using DVCC*. Editors: Mishra S, Sood YR, Tomar A. Applications of Computing, Automation And Wireless Systems İn Electrical Engineering, 1093-1101, Cham, Switzerland, Springer, 2019.
[34] Tippett LHC. *Random Sampling Numbers*. Editors: Pearson K. Tracts For Computers, 8-26, London, UK, Cambridge University Press, 1927.
[35] The Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. 1st ed. Santa Monica, CA, USA, RAND Corporation, 1955.
[36] Vaidyanathan S, Akgul A, Kaçar S, Çavuşoğlu U. "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*, 133(2), 1-18, 2018.
[37] Widynski B. "Squares: A Fast Counter-Based RNG". *arXiv Preprint*, https://arxiv.org/abs/2004.06278 (16.03.2022).
[38] Bao B, Liu Z, Xu J. "New chaotic system and its hyperchaos generation". *Journal of Systems Engineering and Electronics*, 20(6), 1179-1187, 2009.
[39] Texas Instruments. "LM741 Operational Amplifier Datasheet". Dallas, Texas, USA, Rev. D, 2015.
[40] Texas Instruments. "LF347, LF347B JFET-Input Quad Operational Amplifiers". Dallas, Texas, USA, 2016.
[41] Analog Devices, "AD633 Low Cost Analog Multiplier Datasheet". Norwood, MA, USA, Rev. K, 2015.
[42] MATLAB. "MathWorks Announces Release 2019b of MATLAB and Simulink". https://www.mathworks.com/company/newsroom/mathworks-announces-release-r2019b-of-matlab-and-simulink.html (16.03.2022).
[43] Wolf A, Swift JB, Swinney HL, Vastano JA. "Determining Lyapunov exponents from a time series". *Physica D: Nonlinear Phenomena*, 16(3), 285-317, 1985.
[44] Grassberger P, Procaccia I. *Measuring The Strangeness of Strange Attractors.* Editors: Hunt BR, Li TY, Kennedy JA, Nusse HE. The Theory of Chaotic Attractors, 170-189, New York, USA, Springer,2004.