

Article



An Oscillator without Linear Terms: Infinite Equilibria, Chaos, Realization, and Application

Othman Abdullah Almatroud¹, Victor Kamdoum Tamba², Giuseppe Grassi³ and Viet-Thanh Pham^{4,*}

- ¹ Department of Mathematics, Faculty of Science, University of Ha'il, Ha'il 2440, Saudi Arabia; o.almatroud@uoh.edu.sa
- ² Department of Telecommunication and Network Engineering, Fotso Victor University Institute of Technology, University of Dschang, Bandjoun P.O. Box 134, Cameroon; victor.kamdoum@univ-dschang.org
- ³ Dipartimento Ingegneria Innovazione, Universita del Salento, 73100 Lecce, Italy; giuseppe.grassi@unisalento.it
- ⁴ Nonlinear Systems and Applications, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam
- Correspondence: phamvietthanh@tdtu.edu.vn

Abstract: Oscillations and oscillators appear in various fields and find applications in numerous areas. We present an oscillator with infinite equilibria in this work. The oscillator includes only nonlinear elements (quadratic, absolute, and cubic ones). It is different from common oscillators, in which there are linear elements. Special features of the oscillator are suitable for secure applications. The oscillator's dynamics have been discovered via simulations and an electronic circuit. Chaotic attractors, bifurcation diagrams, Lyapunov exponents, and the boosting feature are presented while measurements of the implemented oscillator are reported by using an oscilloscope. We introduce a random number generator using such an oscillator, which is applied in biomedical image encryption. Moreover, the security and performance analysis are considered to confirm the correctness of encryption and decryption processes.

Keywords: chaos; nonlinear oscillations; bifurcation diagram; analog circuit; random number generator; biomedical image encryption

1. Introduction

Nonlinear systems are studied widely because of their complex dynamics [1–5]. It is a challenge to analyze the solutions of such systems. In fact, numerical approaches have been attempted in numerous studies. In addition to limit cycles, chaos can appear in nonlinear systems [6]. Chaos become famous after Lorenz's investigations [7]. Chaos was reported in various systems such as the spherical system [8], the plasma model [9], the jerk circuit [10], the modified logistic map [11], the complex Rikitake model [12], and the glucose-insulin system [13]. Interestingly, the application areas were promoted by the irregular dynamics of a chaotic system [14–16]. Recent applications include the steganography protocol [17], the substitution box [18], secure smart grids [19], the pseudo-random generator [20], communication for IoT [21], liquid mixtures [22], and Hash function realization [23].

Recent years have seen the emergence of systems with special equilibria [24]. Typically, we can refer to systems with infinite equilibria [25]. Jafari and Sprott used quadratic terms to propose line equilibium [25]. In the work [26], the authors applied absolute and quadratic terms to get a gallery of systems, in which equilibria are located on lines and curves. Li et al. utilized a memristor to design a memristive circuit with infinite equilibria [27]. By adding a memristive device into a system with one stable equilibrium, Pham et al. obtained a system having infinite equilibria [28]. Equilibrium points on a butterfly-like curve and two circles were explored by Sambas et al. [29,30]. Although the presence of infinite equilibria has received considerable critical attention [31,32], there are still issues which should be considered further [24].



Citation: Almatroud, O.A.; Tamba, V.K.; Grassi, G.; Pham, V.-T. An Oscillator without Linear Terms: Infinite Equilibria, Chaos, Realization, and Application. *Mathematics* **2021**, *9*, 3315. https://doi.org/10.3390/ math9243315

Academic Editors: Kehui Sun, Sajad Jafari, Bocheng Bao and Daniel-Ioan Curiac

Received: 8 November 2021 Accepted: 15 December 2021 Published: 20 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/). The purpose of this investigation is to explore an oscillator with infinite equilibria. Interestingly, there is an absence of linear terms in such an oscillator. The dynamics and feasibility of the oscillator are explored by using simulations and an electronic circuit. In addition, the application of the oscillator is illustrated via biomedical image encryption. The novelty and contribution of our work is summarized as follows.

- We introduce an oscillator without linear terms.
- There are infinite equilibria in the oscillator.
- The oscillator displays the boosting feature, which is useful for generating a signal with flexible amplitudes.
- Physical realization of the oscillator is reported.
- Special features of the oscillator are suitable for secure applications.

2. Oscillator and Oscillator's Dynamics

By applying nonlinear elements (quadratic, absolute, and cubic ones), we introduce an oscillator in the following form:

$$\begin{cases} \dot{x} = yz \\ \dot{y} = x^3 - y^3 \\ \dot{z} = -ay^3 - bxy + c|x| \end{cases}$$
(1)

In Equation (1), positive parameters are *a*, *b*, and *c*. We set

$$yz = 0 \tag{2}$$

$$x^3 - y^3 = 0 (3)$$

$$-ay^3 - bxy + c|x| = 0 (4)$$

for finding oscillator's equilibrium. From Equations (3) and (4) we have

$$ax^3 + bx^2 - c|x| = 0 (5)$$

It is simple to see that the root of Equation (5) depends on the parameters *a*, *b*, *c*. For a = 0.1 and c = 0.5 and $b \in [1, 2.5]$, Equation (5) has three real roots. As a result, the oscillator has two symmetrical equilibria $(E_{1,2}^*)$ and a line of equilibria (E_3^*) :

$$E_1^*(\alpha, \alpha, 0) \tag{6}$$

$$E_2^*(-\alpha, -\alpha, 0) \tag{7}$$

$$E_3^*(0,0,z^*)$$
 (8)

The bifurcation diagram is presented in Figure 1 for the parameter *b*. We fixed a = 0.1, c = 0.5 and the initial conditions (0.1, 0.1, 0.1). The oscillator displays chaos for some windows of *b*. Figure 2 illustrates chaotic attractor when b = 1. We observe the coexisting of chaotic attractors as shown in Figure 3. Such attractors are asymmetric.

In Equation (1), the state z appears one time on the right side of equations. Therefore, a parameter k can be included into Equation (1) to control the state z as follows:

$$\begin{cases} \dot{x} = y(z+k) \\ \dot{y} = x^3 - y^3 \\ \dot{z} = -ay^3 - bxy + c|x| \end{cases}$$
(9)

Boosting feature is, in fact, linear shift of coordinates of the state space. For example, boosting feature is reported for k = 0, 5, -5 (see Figure 4). Obviously, by changing the value of k the attractors are varied along the z axis. It is noted that the linear term ky is only appeared in Equation (9) when we include the parameter k into the Equation (1). Is this case, the oscillator can generate a signal with flexible amplitudes or a positive-amplitude signal (z).



Figure 1. Changing the value of parameter *b* (**a**) Bifurcation diagram, and (**b**) Lyapunov exponents of the oscillator.



Figure 2. Chaotic attractors displayed for b = 1 (**a**) *x*-*y* plane, (**b**) *x*-*z* plane, and (**c**) *y*-*z* plane.

2





Figure 3. Coexisting attractors (a) *x*-*y* plane, (b) *x*-*z* plane, and (c) *y*-*z* plane for b = 2.3 with (x(0), y(0), z(0)) = (0.1, 0.1, 0.1) (black) and (x(0), y(0), z(0)) = (0, -1, 0) (red).



Figure 4. (a) Boosting bifurcation and boosting attractors in (b) *z*-*x* plane, and (c) *z*-*y* plane. Here colors for k = 0, 5, -5 are black, blue, and red, respectively.

Moreover, in order to choose the parameter values according to a desired behavior and explore well the dynamics of the investigated system, we provide two-parameter bifurcation diagrams computed respectively in (a - b) and (a - c) planes in Figure 5. The initial conditions are fixed by (0.1, 0.1, 0.1) and the used parameter step is 0.005.

Figure 5 shows the various dynamical behaviors exhibited by the investigated oscillator (1) according to the value of the Largest Lyapunov Exponent (LLE). The lowest values of LLE are marked with blue, while the highest ones are indicated with dark red. The system in these ranges of parameters displays globally periodic and chaotic behaviors. Periodic oscillations are located in blue regions where LLE ≤ 0 , while chaotic ones are positioned in green, red and black regions where LLE > 0. The white regions correspond to the unbounded solutions. Figure 5 plays an important role in the engineering system. Indeed, it helps the designer to choose the values of the system parameters according to the desired behavior. It also supports the understanding of the dynamical behavior of the system for the set of initial conditions (0.1, 0.1, 0.1). However, other types of coexisting attractors are out of the scope of Figure 5.



Figure 5. Dynamical behaviors map. (a) $0 \le a \le 0.2$ and $1 \le b \le 2.5$ for c = 0.5, (b) $0 \le a \le 0.2$ and $0 \le c \le 0.8$ for b = 1. The initial conditions are (0.1, 0.1, 0.1).

3. Oscillator Implementation

The mathematical model of a system can be transformed to its equivalent electronic circuit using basic modules (addition and integration). We design and implement an electronic circuit to reproduce the dynamics of an oscillator (1) and confirm the numerical analyses carried out in the preceding section. The proposed electronic circuit diagram for system oscillator (1) is given in Figure 6.

Considering the voltage across the capacitor V_x , V_y , V_z , the corresponding circuit state equations can be expressed as

$$\begin{cases} \frac{dV_x}{dt} = \frac{1}{10R_1C} V_y V_z \\ \frac{dV_y}{dt} = \frac{1}{100R_2C} V_x^3 - \frac{1}{100R_3C} V_y^3 \\ \frac{dV_z}{dt} = -\frac{1}{100R_aC} V_y^3 - \frac{1}{10R_bC} V_x V_y + \frac{1}{R_cC} |V_x| \end{cases}$$
(10)



Figure 6. (a) Circuit diagram of oscillator (1), (b) absolute function circuit. The circuit includes quadruple operational amplifiers (TL084), and analog multiplier chips (AD 633JN) which are used to realize the cubic and quadrature nonlinearities, capacitors and resistors.

For the selected parameters of oscillator (1) a = 0.1, b = 1, c = 0.5 and the initial voltages of capacitors (V_x , V_y , V_z) = (0.1V, 0.1V, 0.1V), the circuit elements are C = 10 nF, $R = 10 \text{ k}\Omega$, $R_1 = 1 \text{ k}\Omega$, $R_2 = R_3 = 100 \Omega$, $R_a = 1 \text{ k}\Omega$, $R_b = 1 \text{ k}\Omega$, and $R_c = 20 \text{ k}\Omega$. The chaotic attractors of the circuit are captured from the breadboard by using an analog oscilloscope (see Figure 7).

The experimental results in Figure 7 confirm that the proposed electronic circuit reproduces well the dynamics of oscillator (1). In addition, it is also possible to use the integrator-based oscillator design in the case of the boosting feature. By adding a resistor and an operational amplifier, the value of parameter k can be realized.



(a)



Figure 7. Chaotic attractors (**a**) V_x - V_y , (**b**) V_x - V_z , and (**c**) V_y - V_z captured from the electronic circuit of oscillator (1) implemented in breadboard for the following values of electronic components C = 10 nF, R = 10 k Ω , $R_1 = 1$ k Ω , $R_2 = R_3 = 100$ Ω , $R_a = 1$ k Ω , $R_b = 1$ k Ω , and $R_c = 20$ k Ω . The initial voltage of the capacitors are (V_x , V_y , V_z) = (0.1V, 0.1V, 0.1V).

4. Random Number Generator (RNG) Using the Oscillator

In this section, we use the oscillator (1) to design random number generators (RNG) for biomedical image encryption applications. RNGs are aperiodic, more complex and have high entropy values. Therefore, the prediction of long-term solutions is not possible. These features are very suitable for chaos-based secure communications. The obtained numbers from an RNG process must pass the NIST-800-22 statistical tests before being used for an engineering application such as image encryption. Random number generators are commonly exploited in some relevant applications including authentication, game programming, data hiding, secure communication and encryption [33–36]. The random number generators are designed to be used for biomedical image encryption algorithms. The block diagram in Figure 8 shows the main steps in the designing process of random number generators based on oscillator (1).

The procedure of RNG starts by considering oscillator (1) as a source of chaotic generator. The system parameters (a = 0.1, b = 1, and c = 0.5) and initial conditions (0.1, 0.1, 0.1) are used. After that, oscillator (1) is discretized via fourth-order Runge Kutta algorithm with time step $\Delta t = 0.001$. The output results (x, y and z) are presented as float numbers. To increase the possibility to receive more successful test results in RNG, the float numbers are converted into 32 bits binary format. This conversion is done using the following MATLAB command: dec2bin(typecast(single(floatnumber),'uint32'),32). The binary numbers from the outputs signals x, y and z are used to obtain RNG. Bits of low digits with high sensitivity are selected to construct the RNG. The following formulas are used: rngx+ = x(8LSBs), rngy+ = y(8LSBs) and rngz+ = z(8LSBs) and 1 Mbit binary sequence for NIST-800-22 statistical tests is generated.



Figure 8. Block diagram explaining the main steps of the designing process of random number generators based on oscillator (1).

NIST-800-22 tests are performed to verify the randomness of the random number generation's results. The NIST-800-22 test consists to 16 different tests, including frequency, runs, rank, serial and random excursions tests. A sequence of bits is therefore valid for engineering applications when it passes all the NIST tests. Note that a test will be counted successful when the *p*-value is greater than 0.01. The generated random numbers from the outputs (*x*, *y*, *z*) passed all tests, which are recorded in Table 1. Considering the results of Table 1, the generated random numbers are effectively random and can be used for biomedical image encryption with high quality and good security. It is noted that "Nooverlapping templates", in NIST tests "Random Excursions", and "Random Excursions Variant" contains 148, 8, and 18 sub items, respectively. All the sub items have passed the NIST test. The value of "Nooverlapping templates" given in Table 1 has been selected randomly. The values of "Random Excursions", and "Random Excursions Variant" in Table 1 are selected for x = -1.

Test-Name	<i>p</i> -Value			Dessile
	X	Ŷ	Z	- Kesult
Frequency	0.01736	0.50790	0.49918	Passed
Block-frequency	0.18189	0.14409	0.18861	Passed
Runs	0.96599	0.15381	0.21472	Passed
Longest runs of ones	0.06335	0.65267	0.74264	Passed
Rank	0.49885	0.49928	0.44669	Passed
DFT	0.79219	0.30442	0.02589	Passed
No overlapping templates	0.05985	0.07790	0.00453	Passed
Overlapping templates	0.28548	0.37728	0.79657	Passed
Universal	0.07618	0.99902	0.35890	Passed
Linear complexity	0.79980	0.22241	0.94489	Passed
Serial test 1	0.08187	0.68489	0.22395	Passed
Serial test 2	0.03409	0.70814	0.11562	Passed
Approximate entropy	0.43162	0.72734	0.61123	Passed
Cumulative sums (forward) Cumulative sums (reverse)	0.02610 0.01303	0.82875 0.55867	0.45276 0.49918	Passed Passed
Random excursions $x = -1$	0.53667	0.68853	0.46270	Passed
Random excursions variant $x = -1$	0.83784	0.44510	0.53585	Passed

Table 1. Results of NIST-800-22 tests.

5. Biomedical Images Encryption Based on RNG Obtained from the Oscillator

Based on the developed RNG in preceding section, a biomedical images encryption algorithm is proposed. The security and performance analysis of the proposed encryption algorithm are performed.

5.1. Proposed Biomedical Images Encryption Algorithm

The main objective here is to combine the RNG obtained from oscillator (1) with the corresponding bits numbers of each pixel provided from the biomedical image. The cipher image does not need to be decrypted by anyone who is not authorized to discover a part or full information contained by the original biomedical image. The biomedical images are used here to illustrate the importance of the personal medical data protection during the transmission of these data for a medical diagnostic. The proposed biomedical image encryption process is presented in Figure 9.



Figure 9. The proposed biomedical image encryption process.

In Figure 9, the parameters and initial conditions of oscillator (1) are used as keys. The RNG bits are used in the encryption and decryption processes. The original biomedical image is converted into a pixel-based binary format. The bit array of the RNG process and the biomedical image are transferred to an XOR operation to produce the cipher image. The decryption process is realized by performing the same XOR operation of the RNG bits with the cipher image. Therefore, the decrypted biomedical image is obtained.

5.2. Computational Results

The designed encryption method is analyzed by using three different biomedical images, namely "Chest", "Brain", and "Lung" (256 × 256 size). The computational results of the proposed encryption and decryption processes are provided in Figure 10 (see Figure 10a–c for original biomedical images, Figure 10d–f for cipher biomedical images and Figure 10g–i for decrypted biomedical images). We can see from Figure 10 that there is no relationship between the original images (see Figure 10a–c) and their corresponding encrypted ones (see Figure 10d–f). The decrypted images (see Figure 10g–i) seem to be the same as the original ones. This means that the encryption processes are realized successfully with high quality and good security.



Figure 10. Computational results of the proposed encryption process: (**a**–**c**) are original biomedical images; (**d**–**f**) are encrypted biomedical images and (**g**–**i**) are decrypted biomedical images.

5.3. Security and Performance Analysis

5.3.1. Key Space Analysis

The key space size must be greater than 2^{100} [37]. The oscillator (1) consists of three parameters and three initial conditions which are used as key as mentioned above. Fixing the precision of the system to 2^{-17} , the key space size will be $10^{17*6} = 10^{102}$, which is much larger than 2^{100} . It is sufficient to withstand brute force attacks because of the large key space.

5.3.2. Key Sensitivity Analysis

The system under scrutiny is very sensitive to initial conditions and parameter variations. The slight change of the key makes the chaotic sequence completely different, and generates two different encrypted images. Hence, the encrypted image cannot be decrypted correctly. Figure 11 presents the test when changing the secret key 10^{-17} . Results show the high sensitivity of the algorithm for secret key.



(g)

Figure 11. Test results of key sensitivity, (a) $x(0) + 10^{-17}$, (b) $y(0) + 10^{-17}$, (c) $z(0) + 10^{-17}$, (d) $a + 10^{-17}$, (e) $b + 10^{-17}$, (f) $c + 10^{-17}$, (g) correct key.

5.3.3. Information Entropy

An excellent parameter indicating randomness of a signal is information entropy. Its evaluation uses the following expression

$$H(m) = -\sum_{i=1}^{N} P(m_i) \log_2(P(m_i))$$
(11)

where *N* represents the total number of all possible occurrence of signal m_i and $P(m_i)$ represent the probability that the symbol m_i appears. If the gray-scale source $m = \{m_1, m_2, \ldots, m_{256}\}$ emits 256 symbols with equivalent probability, then the entropy value should be equal to 8 [38] which is the ideal value of entropy for true-random information. The results of information entropy of the algorithm are displayed in Table 2. The information entropy of the cipher image is closed to 8. This serves to conclude that the cipher image is very random. Thus, the proposed algorithm has very good security performance.

Entropy		Greyscale Images	
	Chest	Brain	Lung
Original image	7.6578	5.8389	6.8364
Encrypted version	7.9965	7.9952	7.9955

Table 2. Assessment of information entropy for original and encrypted images.

5.3.4. Noise Attacks

Noise attack is studied using Gaussian as well as Salt and Pepper noises. The mean value of 0 and variance of 0.01, 0.03 and 0.05 (Gaussian noise) is added to the cipher images. The recovery images are reported in Figure 12. Likewise, by introducing the noise intensity of Salt and Pepper as 0.1, 0.3 and 0.5 in the cipher image, we obtain the recovery images in Figure 13. The results of Figures 12 and 13 confirm the ability of the algorithm to avoid noise attacks.



Figure 12. Gaussian noise attacks test. (**a**,**e**,**i**) encrypted images of Chest, Brain and Lung; (**b**,**f**,**j**) decrypted image (variance 0.01); (**c**,**g**,**k**) decrypted image (variance 0.03) and (**d**,**h**,**l**)decrypted image (variance 0.05) respectively for Chest, Brain and Lung images.



Figure 13. Salt and pepper noise attacks test. (**a**,**e**,**i**) encrypted images of Chest, Brain and Lung; (**b**,**f**,**j**) decrypted image (density 0.1); (**c**,**g**,**k**) decrypted image (density 0.3) and (**d**,**h**,**l**) decrypted image (density 0.5) respectively for Chest, Brain and Lung images.

6. Conclusions

In this work, we have introduced an oscillator in which there are infinite equilibria. It is worth noting that all terms in the oscillator are nonlinear. By investigating the oscillator, we reported different oscillator features such as chaos, multistability, and boosting attractors. moreover, the circuital attractors illustrated the oscillator's feasibility, which is useful for applications. We have implemented a random number generator using the oscillator's chaotic behavior. The random number generator showed good results when applying it to the encryption of biomedical images.

Author Contributions: Conceptualization, O.A.A.; Formal analysis, O.A.A.; Funding acquisition, G.G.; Investigation, V.K.T.; Methodology, V.K.T.; Resources, V.-T.P.; Software, V.-T.P.; Supervision, G.G.; Validation, V.K.T.; Visualization, O.A.A.; Writing—original draft, V.-T.P.; Writing—review & editing, G.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by Scientific Research Deanship at University of Ha'il - Saudi Arabia through project number RG-21067.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Ikeda, K.; Daido, H.; Akimoto, O. Optical turbulence: Chaotic behavior of transmitted light from a ring cavity. *Phys. Rev. Lett.* 1980, 45, 709–712. [CrossRef]
- Ikeda, K.; Matsumoto, K. High-dimensional chaotic behaviour in system with time-delayed feedback. *Physics D* 1987, 29, 223–235. [CrossRef]
- Shilnikov, L.P.; Shilnikov, A.L.; Turaev, D.V.; Chua, L.O. Methods of Qualitative Theory in Nonlinear Dynamics; World Scientific: Singapore, 1998.
- 4. Ando, B.; Graziani, S. Stochastic Resonance: Theory and Applications; Kluwer: Norwel, MA, USA, 2000.
- 5. Sanjuan, M.A.F.; Grebogi, C. Recent Progress in Controlling Chaos; World Scientific: Singapore, 2010.

- 6. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
- 7. Lorenz, E.N. Deterministic non-periodic flow. J. Atmos. Sci. 1963, 20, 130-141. [CrossRef]
- 8. Nunez-Perez, J.C.; Adeyemi, V.A.; Sandoval-Ibarra, Y.; Perez-Pinal, F.J.; Tlelo-Cuautle, E. FPGA realization of spherical chaotic system with application in image transmission. *Math. Probl. Eng.* **2021**, *2021*, 5532106. [CrossRef]
- 9. Natiq, H.; Ariffin, M.R.K.; Asbullah, M.A.; Mahad, Z.; Najah, M. Enhancing chaos complexity of a plasma model through power input with desirable random features. *Entropy* **2021**, *23*, 48. [CrossRef]
- 10. Li, F.; Tai, C.; Bao, H.; Luo, J.; Bao, B. Hyperchaos, quasi-period and coexisting behaviors in second-order-memristor-based jerk circuit. *Eur. Phys. J. Spec. Top.* **2020**, 229, 1045–1058. [CrossRef]
- 11. Moysis, L.; Tutueva, A.; Volos, C.; Butusov, D.; Munoz-Pacheco, J.M.; Nistazakis, H. A two-parameter modified logistic map and its application to random bit generation. *Symmetry* **2020**, *12*, 829. [CrossRef]
- 12. Pang, W.; Wu, Z.; Xiao, Y.; Jiang, C. Chaos control and synchronization of a complex Rikitake dynamo model. *Entropy* **2020**, 22, 671. [CrossRef]
- 13. Rajagopal, K.; Bayani, A.; Jafari, S.; Karthikeyan, A.; Hussain, I. Chaotic dynamics of a fractional order glucose-insulin regulatory system. *Front. Inf. Technol. Electron. Eng.* **2020**, *21*, 1108–1118. [CrossRef]
- 14. Strogatz, S.H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering; Perseus Books: Boston, MA, USA, 1994.
- 15. Chen, G.R. Controlling Chaos and Bifurcations in Engineering Systems; CRC Press: Boca Raton, FL, USA, 1999.
- Buscarino, A.; Fortuna, L.; Frasca, M.; Muscato, G. Chaos does help motion control. Int. J. Bifurc. Chaos 2007, 17, 3577–3581. [CrossRef]
- 17. Abd-El-Atty, B.; Iliyasu, A.M.; Alaskar, H.; El-Latif, A.; Ahmed, A. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based e-healthcare platforms. *Sensors* **2020**, *20*, 3108. [CrossRef]
- El-Latif, A.A.A.; Abd-El-Atty, B.; Belazi, A.; Iliyasu, A.M. Efficient chaos-based substitution-box and its application to image encryption. *Electronics* 2021, 10, 1392. [CrossRef]
- Varan, M.; Akgul, A.; Kurugollu, F.; Sansli, A.; Smith, K. A Novel Security Methodology for Smart Grids: A Case Study of Microcomputer-Based Encryption for PMU Devices. *Complexity* 2021, 2021, 2798534. [CrossRef]
- 20. Tutueva, A.V.; Karimov, T.I.; Moysis, L.; Nepomuceno, E.G.; Volos, C.; Butusov, D.N. Improving chaos-based pseudo-random generators in finite-precision arithmetic. *Nonlinear Dyn.* **2021**, *105*, 727–737. [CrossRef]
- 21. Fataf, N.A.A.; Rahim, M.F.A.; He, S.; Banerje, S. A Communication Scheme based on Fractional Order Chaotic Laser for Internet of Things. *Internet Things* **2021**, *15*, 100425. [CrossRef]
- 22. Kalayci, O.; Pehlivan, I.; Akgul, A.; Coskun, S.; Kurt, E. A New Chaotic Mixer Design Based on the Delta Robot and Its Experimental Studies. *Math. Probl. Eng.* 2021, 6615856. [CrossRef]
- 23. la Fraga, L.G.D.; Mancillas-Lopez, C.; Tlelo-Cuautle, E. Designing an authenticated Hash function with a 2D chaotic map. *Nonlinear Dyn.* **2021**, *104*, 4569–4580. [CrossRef]
- 24. Wang, Z.; Wei, Z.; Sun, K.; Shaobo He, H.W.; Xu, Q.; Chen, M. Chaotic flows with special equilibria. *Eur. Phys. J. Spec. Top.* 2020, 229, 905–919. [CrossRef]
- 25. Jafari, S.; Sprott, J.C. Simple chaotic flows with a line equilibrium. Chaos Solitons Fractals 2013, 57, 79-84. [CrossRef]
- 26. Pham, V.T.; Jafari, S.; Volos, C.; Kapitaniak, T. A gallery of chaotic systems with an infinite number of equilibrium points. *Chaos Solitons Fractals* **2016**, *93*, 58–63. [CrossRef]
- 27. Li, Q.; Zeng, H.; Li, J. Hyperchaos in a 4D memristive circuit with infinitely many stable equilibria. *Nonlinear Dyns.* 2015, 79, 2295–2308. [CrossRef]
- 28. Pham, V.T.; Jafari, S.; Kapitaniak, T. Constructing a chaotic system with an infinite number of equilibrium points. *Int. J. Bifurc. Chaos* **2016**, *26*, 1650225. [CrossRef]
- Sambas, A.; Vaidyanathan, S.; Bonny, T.; Zhang, S.; Hidayat, Y.; Gundara, G.; Mamat, M. Mathematical Model and FPGA Realization of a Multi-Stable Chaotic Dynamical System with a Closed Butterfly-Like Curve of Equilibrium Points. *Appl. Sci.* 2021, 11, 788. [CrossRef]
- Sambas, A.; Vaidyanathan, S.; Tlelo-Cuautle, E.; Zhang, S.; Guillen-Fernandez, O.; Hidayat, Y.; Gundarat, G. A novel chaotic system with two circles of equilibrium points: Multistability, electronic circuit and FPGA realization. *Electronics* 2019, *8*, 1211. [CrossRef]
- Bao, B.; Zou, X.; Liu, Z.; Hu, F. Generalized memory element and chaotic memory system. Int. J. Bifurc. Chaos 2013, 23, 1350135. [CrossRef]
- 32. Bao, H.; Wang, N.; Bao, B.; Chen, M.; Jin, P.; Wang, G. Initial condition-dependent dynamics and transient period in memristorbased hypogenetic jerk system with four line equilibria. *Commun. Nonlinear Sci. Numer. Simul.* **2018**, *57*, 264–275. [CrossRef]
- 33. Karakaya, B.; Gulten, A.; Frasca, M. A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation. *Chaos Solitons Fractals* **2019**, *119*, 143–149. [CrossRef]
- 34. Tuncer, S.A.; Kaya, T. True random number generation from bioelectrical and physical signals. *Comput. Math. Methods Med.* **2018**, 2018, 3579275.
- 35. Tuncer, T. The implementation of chaos-based PUF designs in field programmable gate array. *Nonlinear Dyn.* **2016**, *86*, 975–986. [CrossRef]

- 36. Kaya, T. A true random number generator based on a Chua and RO-PUF: Design, implementation and statistical analysis. *Analog Integr. Circuits Signal Process.* **2020**, *102*, 415–426. [CrossRef]
- 37. Seyedzadeh, S.M.; Mirzakuchaki, S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Process.* 2012, *92*, 1202–1215. [CrossRef]
- 38. Tsafack, N.; Kengne, J.; Abd-El-Atty, B.; Iliyasu, A.; Hirota, K.; El-Latif, A. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Inf. Sci.* **2020**, *515*, 191–217. [CrossRef]