Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption

Lazaros Moysis [1] [iD]**, Christos Volos** [1,*] [iD]**, Sajad Jafari** [2]**, Jesus M. Munoz-Pacheco** [3] [iD]**, Jacques Kengne** [4] [iD]**, Karthikeyan Rajagopal** [5,6] [iD] **and Ioannis Stouboulos** [1]

[1] Laboratory of Nonlinear Systems—Circuits & Complexity (LaNSCom), Physics Department, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece; lmousis@physics.auth.gr (L.M.); stouboulos@physics.auth.gr (I.S.)

[2] Nonlinear Systems and Applications, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam; sajad.jafari@tdtu.edu.vn

[3] Faculty of Electronics Sciences, Autonomous University of Puebla, Puebla 72000, Mexico; jesusm.pacheco@correo.buap.mx

[4] Department of Electrical Engineering, University of Dschang, Dschang P.O. Box 134, Cameroon; kengnemozart@yahoo.fr

[5] Center for Nonlinear dynamics, Defence University, Mekelle 1020, Ethiopia; rkarthiekeyan@gmail.com

[6] Institute of Energy, Mekelle University, Mekelle 6330, Ethiopia

* Correspondence: volos@physics.auth.gr

Abstract: A modification of the classic logistic map is proposed, using fuzzy triangular numbers. The resulting map is analysed through its Lyapunov exponent (LE) and bifurcation diagrams. It shows higher complexity compared to the classic logistic map and showcases phenomena, like antimonotonicity and crisis. The map is then applied to the problem of pseudo random bit generation, using a simple rule to generate the bit sequence. The resulting random bit generator (RBG) successfully passes the National Institute of Standards and Technology (NIST) statistical tests, and it is then successfully applied to the problem of image encryption.

1. Introduction

The field of chaos theory expands to numerous applications related to cryptography, secure communications, engineering, physics, economics, robotics, control, and many more; see, for example, References [1–5] and the references therein. Chaotic systems, being deterministic systems with a high sensitivity to initial conditions and parameter changes, constitute an excellent basis for efficiently modelling complex natural phenomena, as well as adding complexity to security related applications.

Due to the aforementioned applicability of chaotic systems, there is an ongoing demand for introducing novel chaotic systems. This is usually done by considering an existing chaotic system and modifying it, either by slightly altering a term in the system's differential/difference equations, or by adding more nonlinear terms, or even by adding more variables and changing the system to a higher dimension.

The logistic map [6] is one of the most well-known one-dimensional discrete time chaotic systems and one of the most heavily modified chaotic systems; see, for example, References [7–17]. The map has only one parameter and a simple structure, which makes it suitable for many applications. In this work, we propose a modified version of the classic logistic map by employing fuzzy triangular numbers to

modify its behavior. The idea of passing the values of the logistic map through a fuzzy number is mathematically very simple, yet it leads to a significant improvement of the chaotic behavior of the map, with many chaos related phenomena appearing, like antimonotonicity and crisis. Fuzzy logic and fuzzy sets are themselves a large field of study with innumerable applications in engineering and more [18–20]. Specifically in dynamical systems, fuzzy sets have been combined with chaotic systems in fuzzy dynamical systems; see, for example, References [15,21–28]. In the proposed modification of the logistic map, the values of the map in each iteration are passed through a triangular fuzzy number, which is a simple linear function that takes values on the interval $[0, 1]$. The resulting map presents more complex chaos related phenomena compared to the classic map as mentioned above, as well as achieves a higher value for its Lyapunov exponent. Furthermore, to showcase the applicability of the map to chaos related applications, the problems of pseudo random bit generation [4,5,10,11,13,29–43] and image encryption [4,7,9,14,15,33,35,39,44–48] are considered. It is seen that the bit sequence generated from the modified map using a simple rule passes all 15 tests of the National Institute of Standards and Technology (NIST) statistical test suite [49]. The bit sequence generated is then applied to the problem of image encryption, and the resulting encrypted image is analysed for security using methods like histogram analysis, correlation, and information entropy.

It is important to note that this approach can be easily applied to any other one-dimensional chaotic system, as well as further modified by considering different types of fuzzy numbers, like trapezoidal, Gaussian, quadratic, exponential, or their combination. Thus, it is our belief that this approach for modifying a chaotic system will lead to more interesting works in the future.

The rest of the work is structured as follows: Section 2 presents some preliminaries on fuzzy numbers and the logistic map. In Section 3, the modified logistic map is proposed and its dynamical behavior is explored. Section 4 studies the application of the map in random number generation. The use of the produced bit sequence to the problem of image encryption is presented in Section 5. Finally, Section 6 concludes the paper with a discussion on future works.

2. Mathematical Preliminaries

2.1. Fuzzy Numbers

This section presents some preliminaries on fuzzy numbers; see [18–20] for a full presentation. There are slightly varying definitions for a fuzzy number, but in this work we consider a fuzzy number as a function $f : X \rightarrow [0, 1]$ defined over a set $X \subseteq \mathbb{R}$, such that:

- It is a normal fuzzy set, that is, there exists at least one $x \in X$, such that $f(x) = 1$.
- Its a-cuts $f^a = \{x, f(x) \geq a\}$ are closed intervals $\forall a \in [0, 1]$.
- f is piecewise continuous.

Note that some works define fuzzy numbers as having exactly one x_0, such that $f(x_0) = 1$.

The fuzzy numbers considered here are defined as $f : [0, 1] \rightarrow [0, 1]$ and have the following triangular form:

$$f_z(x) = \begin{cases} \frac{x}{z}, & 0 \leq x \leq z \\ \frac{1-x}{1-z}, & z \leq x \leq 1, \end{cases} \tag{1}$$

where z denotes the peak of the triangular fuzzy number. Examples for different values of z are shown in Figure 1. For example, for the fuzzy number $f_{0.5}(x)$, it holds that $f_{0.5}(0.4) = 0.8$, which can be interpreted as the number 0.4 being equal to 0.5 with truth index 0.8.
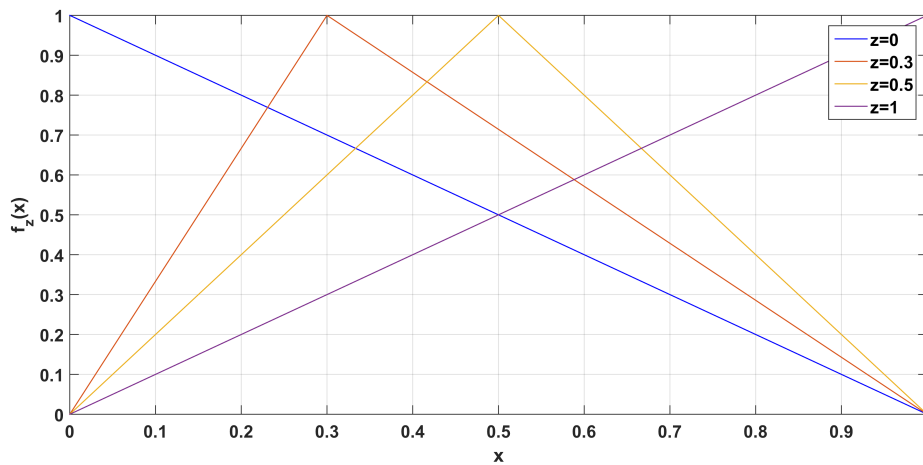
Figure 1. Examples of fuzzy trigonometric numbers for $z = 0, 0.3, 0.5, 1$.

2.2. The Logistic Map

The logistic map [6] is one of the most well-known discrete time 1D chaotic systems with a single parameter, described by

$$x_{i+1} = rx_i(1 - x_i), \quad i = 0, 1, ..., \tag{2}$$

where r is the system parameter that takes values in the interval $[0, 1]$, as well as $x_0 \in [0, 1]$. For different values of the parameter r, the following three dynamics are observed:

- For $r < 1$, x decays to a fixed point $x \to 0$.
- For $1 \leq r \leq 3$, the previous point loses its stability and another fixed point appears $x = 1/r$.
- For $3 \leq r \leq 4$ the system exhibits a rich behavior, going to chaos following a period doubling route.

Figure 2 shows the bifurcation diagram of the logistic map, and Figure 3 shows the diagram of its Lyapunov exponent, given by [50]

$$LE = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \ln |f'(x_i)|, \tag{3}$$

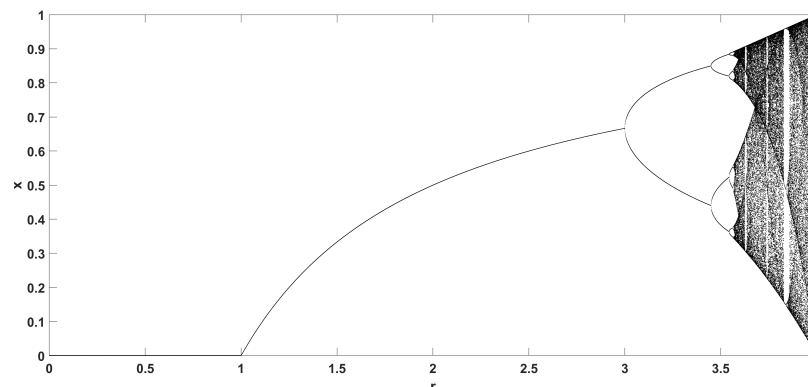which confirms the aforementioned dynamical behavior for various values of parameter r.

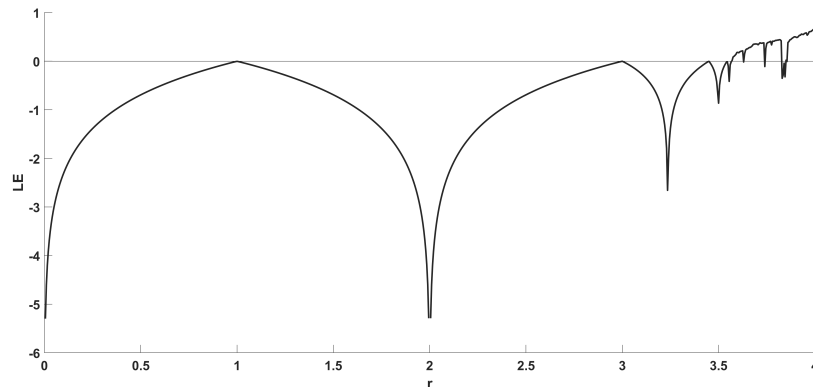**Figure 2.** Bifurcation diagram of the logistic map.

Figure 3. Diagram of Lyapunov exponent of the Logistics map.

3. Implementation of Fuzzy Numbers to Logistic Map

We propose the following fuzzy number logistic map, described by

$$x_{i+1} = f_z \left(r x_i (1 - x_i) \right), \tag{4}$$

where r the bifurcation parameter, and f_z denotes the fuzzy triangular function described above, centered at z. Thus, this modified logistic map has two parameters that can be tuned to affect the system's behavior.

To unmask the dynamical behavior of the system, its bifurcation diagram is plotted with respect to parameter r. Examples for various values of z are given in Figures 4–8, where many interesting phenomena are observed. First, it is easily seen in Figure 4 that for the two end values $z = 0$ and $z = 1$, the behavior of the system is very similar to the classic logistic map, having periodic behavior for values up until around 3.7, and then traversing to chaos through a period doubling route. For intermediate values of the parameter z, the system exhibits chaotic behavior for a range of parameter values r. The phenomenon of period doubling route to chaos appears in all cases, but also crisis phenomena are observed, where the system exits from chaos abruptly. The chaotic behavior is verified by the corresponding diagram of the Lyapunov Exponent (LE) of the system. Note that for $z = 0$ and $z = 1$, the diagram of the LE is the same as with the classic logistic map.

It is also very important to note that in many cases the Lyapunov exponent achieves a maximum value that is higher than 1, which is a lot higher than the value of the classic logistic map, which achieves a maximum value of around 0.7. This is clearly seen in Figure 9, which depicts the Lyapunov exponents of the system for various parameter values.

Similarly, considering the bifurcation diagrams of the system (4) with respect to parameter z unveils even more interesting phenomena, as seen in Figures 10–15. Again, crisis phenomena appear where the system suddenly enters to, or exists from, chaos. In addition, for some values of the parameter r, the phenomenon of antimonotonicity appears, where the system enters chaos through a period doubling route and also exits from chaos following a reverse period halving route (Figures 13 and 14). Lastly, the phenomenon of constant chaos appears when the bifurcation parameter is set to $r = 4$ (Figure 15). This means that the system will be chaotic for all values of the triangular fuzzy number chosen.

In addition, Figures 16 and 17 give a closer look at the bifurcation diagrams with respect to z, for $r = 3.98$ and $r = 1.4$, where the chaotic regions are interrupted by small windows of periodic behavior.
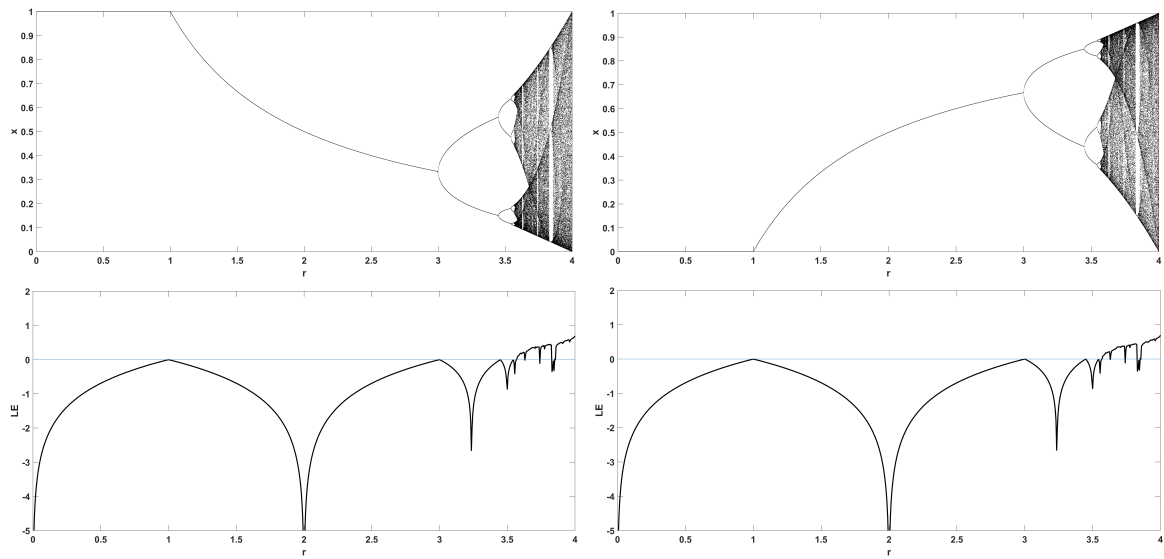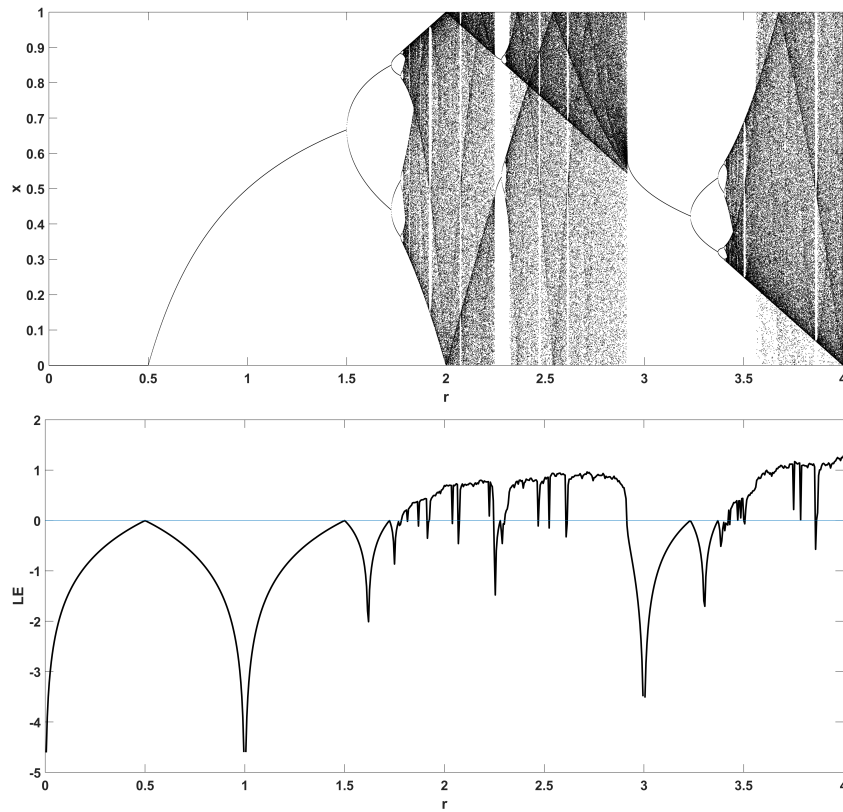
Figure 4. Bifurcation diagram of x versus the bifurcation parameter r and corresponding diagram of Lyapunov exponent for $z = 0$ (**left**) and $z = 1$ (**right**).
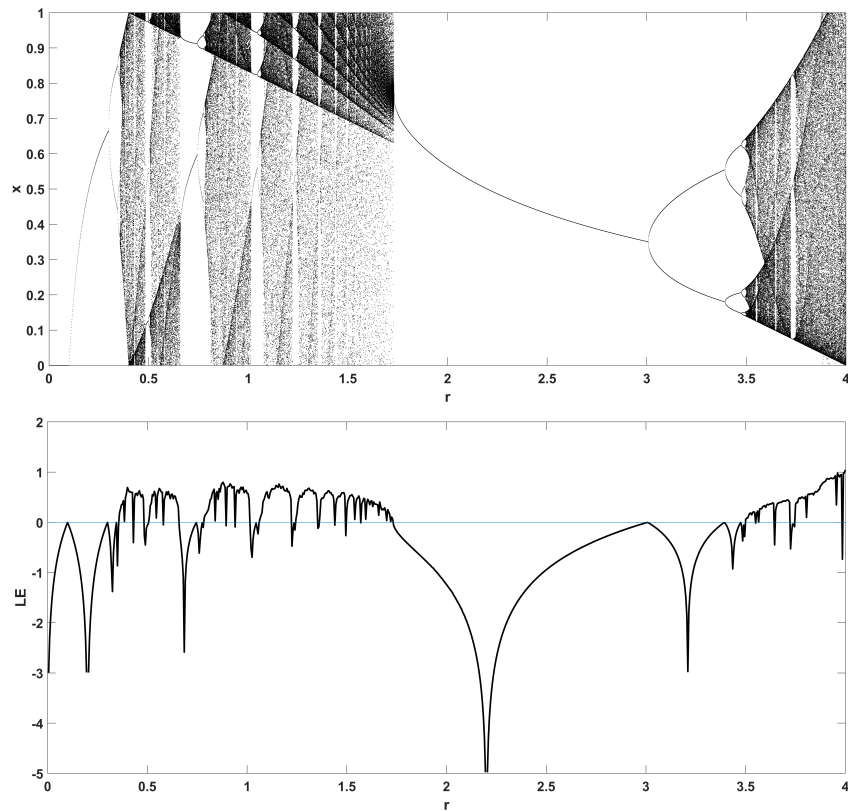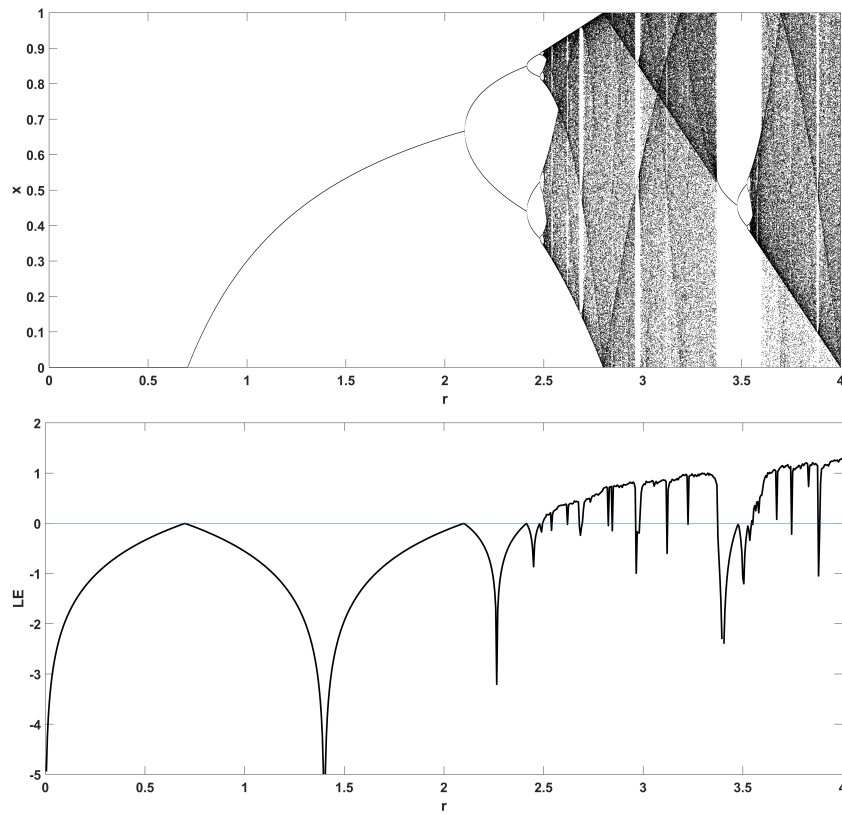

Figure 5. Bifurcation diagram of x versus the bifurcation parameter r and corresponding diagram of Lyapunov exponent for $z = 0.1$.
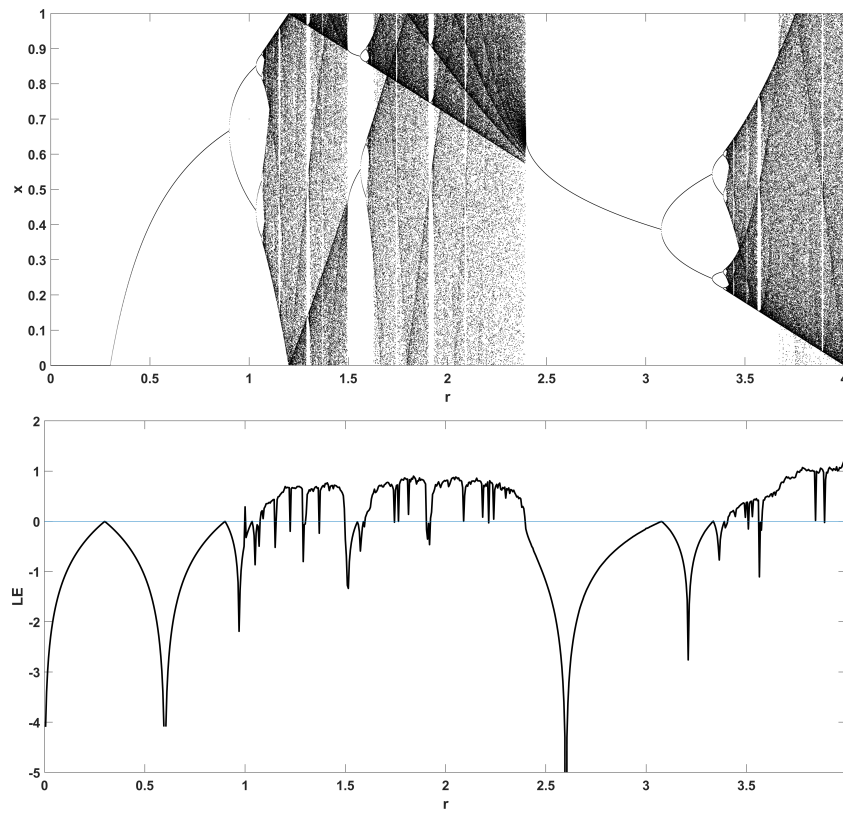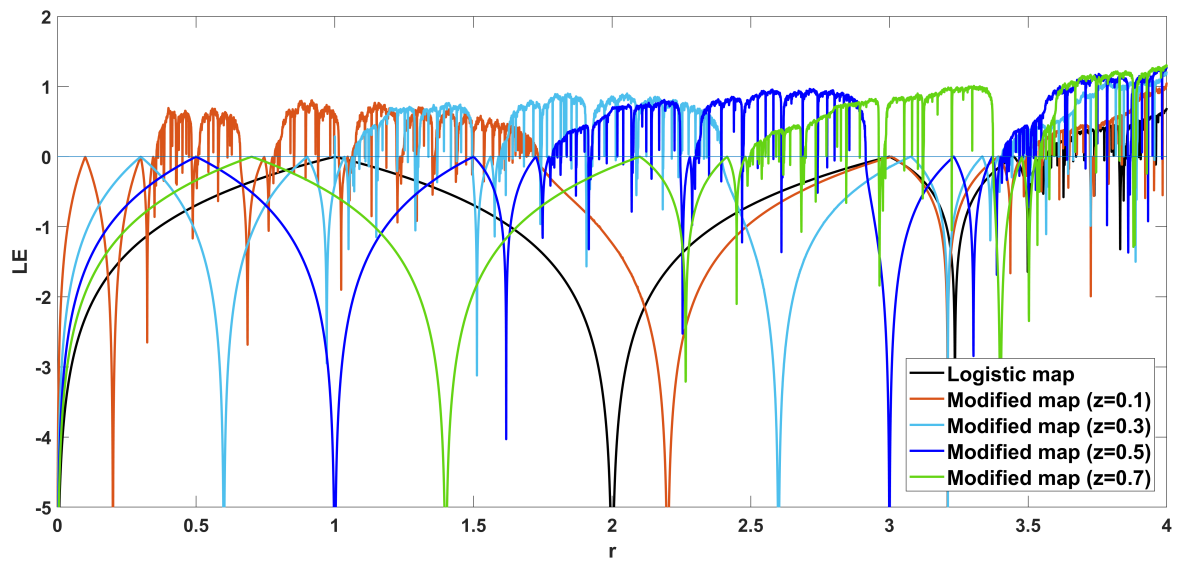
Figure 6. Bifurcation diagram of x versus the bifurcation parameter r and corresponding diagram of Lyapunov exponent for $z = 0.3$.
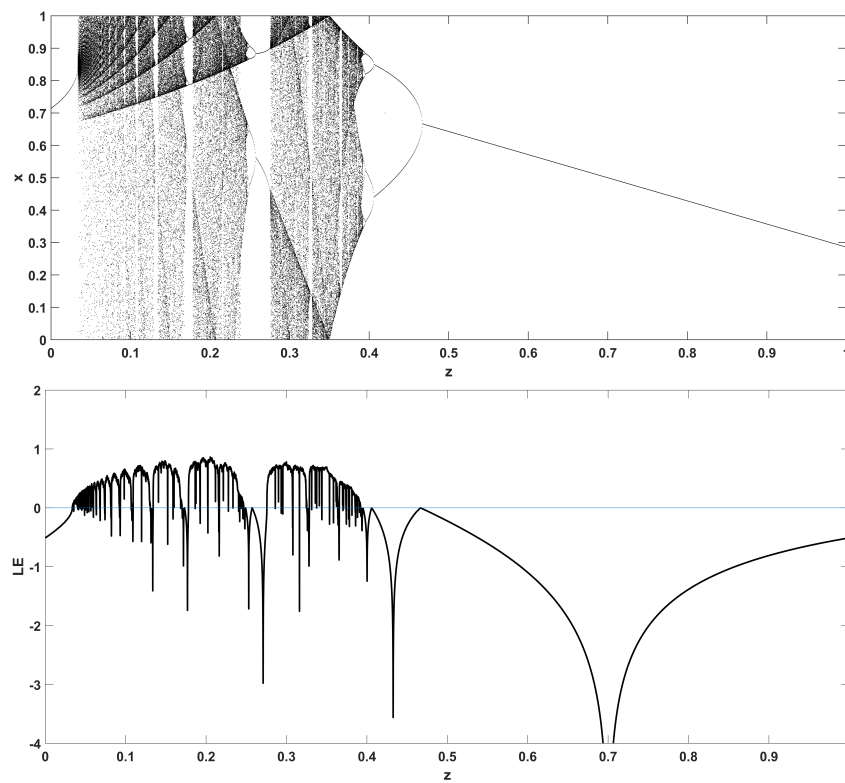

Figure 7. Bifurcation diagram of x versus the bifurcation parameter r and corresponding diagram of Lyapunov exponent for $z = 0.5$.
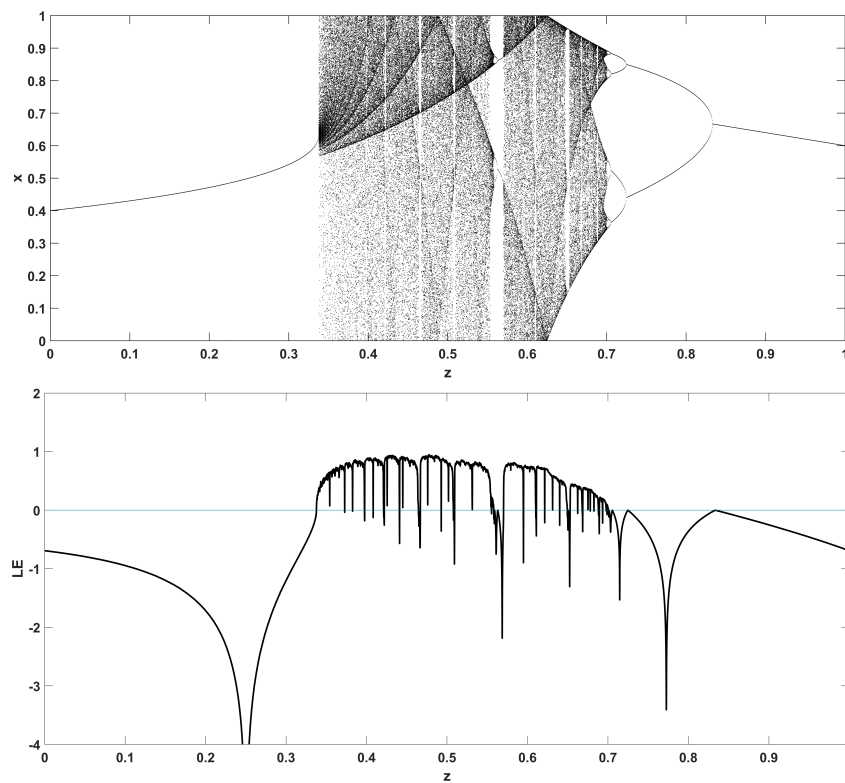
Figure 8. Bifurcation diagram of *x* versus the bifurcation parameter *r* and corresponding diagram of Lyapunov exponent for $z = 0.7$.

Figure 9. Diagram of Lyapunov exponents.

Figure 10. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 1.4$.

Figure 11. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 2.5$.

Figure 12. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 3$.

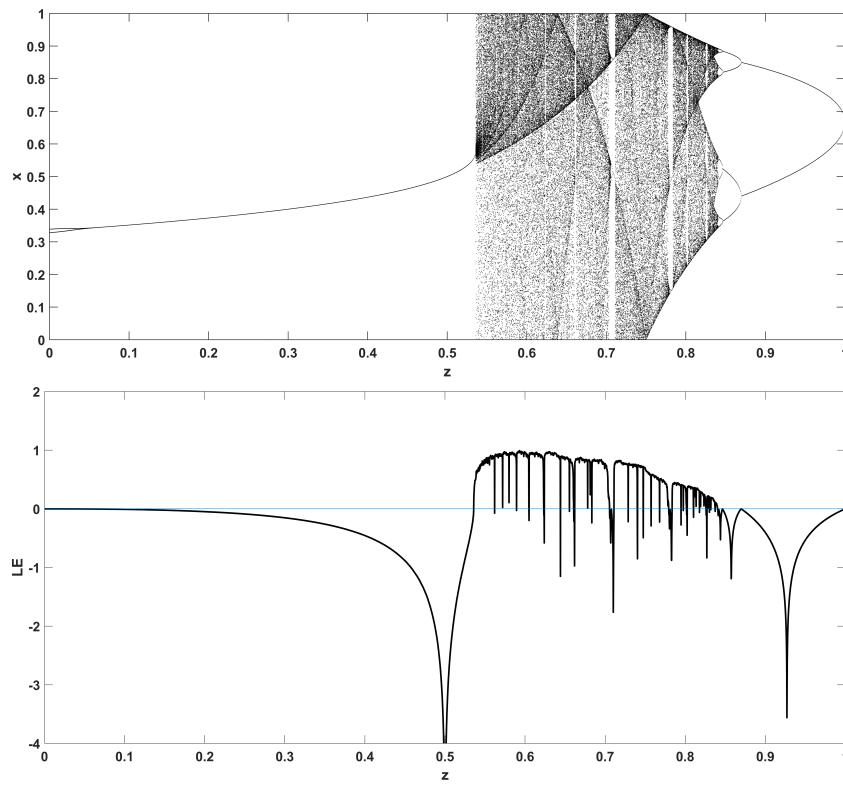
Figure 13. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 3.4$.

Figure 14. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 3.87$.
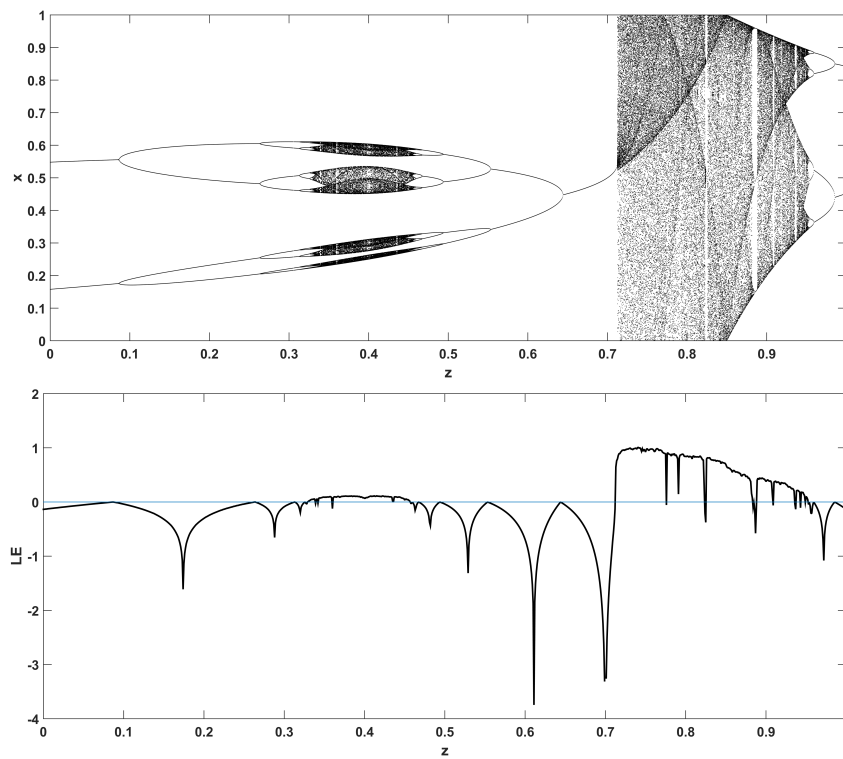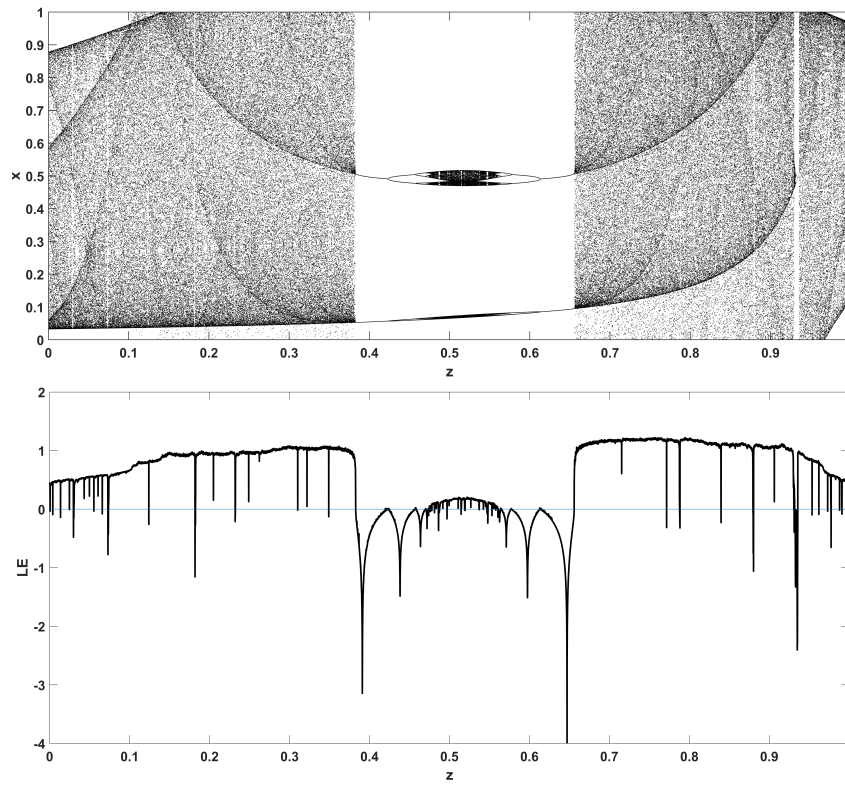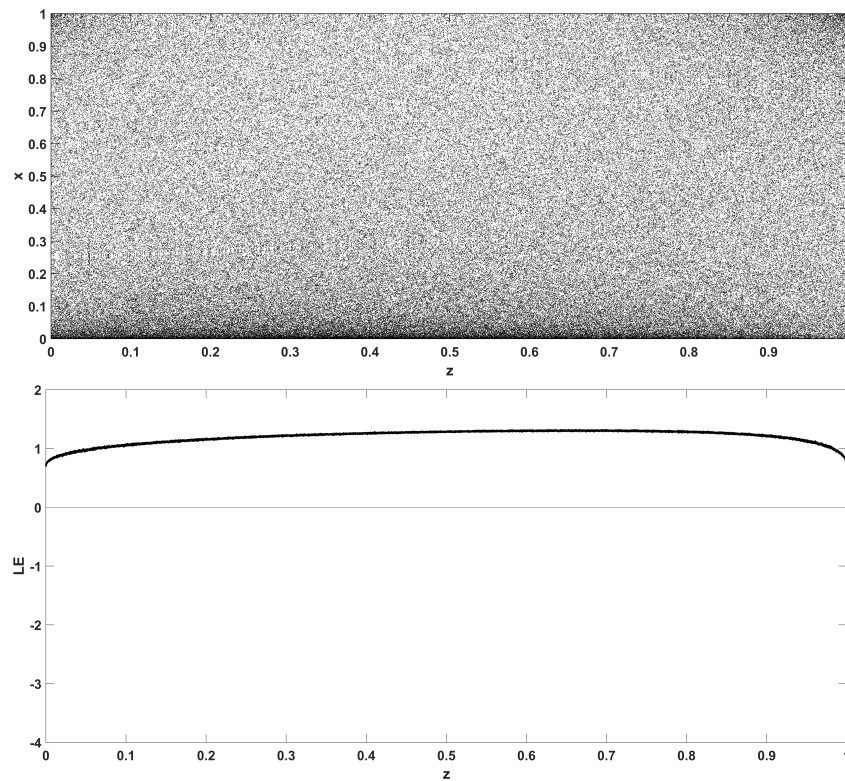

Figure 15. Bifurcation diagram of *x* versus the bifurcation parameter *z* and corresponding diagram of Lyapunov exponent for $r = 4$.
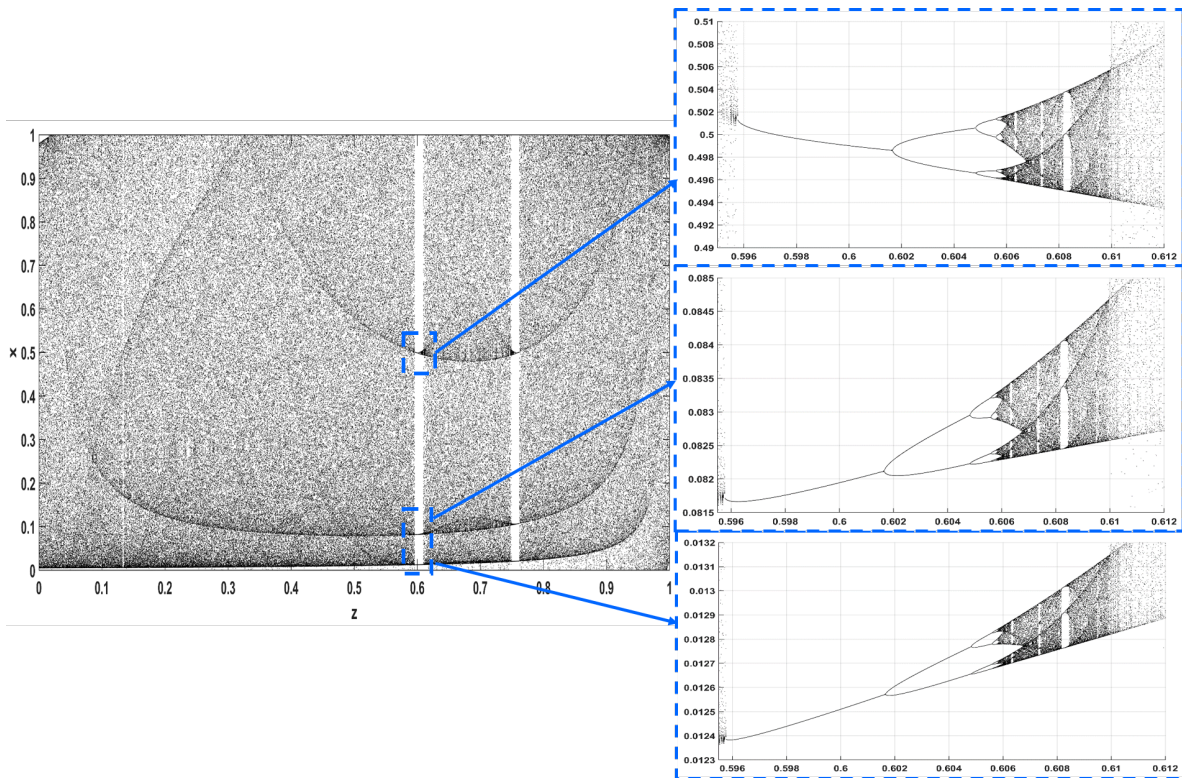
Figure 16. Bifurcation diagram of (4) with respect to parameter *z* for *r* = 3.98.
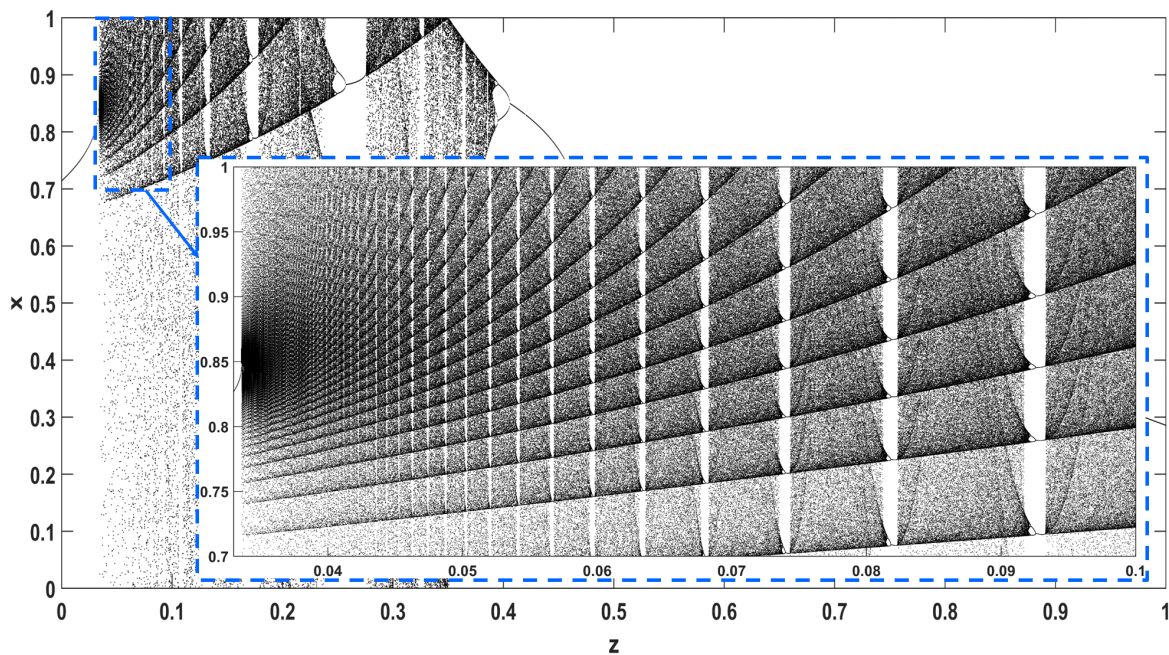
Figure 17. Bifurcation diagram of (4) with respect to parameter *z* for *r* = 1.4.

4. Application to Random Bit Generation

To showcase the high implementability and robustness of the proposed chaotic system, the application to random bit generation is considered. The proposed chaotic random bit generator is created by taking the value of x_i in each iteration, discarding its first 10 decimal digits, and then comparing the resulting number with a threshold value, chosen here as 0.5. The bit value 1 is produced

if the number is greater or equal to the threshold, and the bit value 0 is produced if it is not. Thus, the RBG tactic has the following form:

$$d_i = 10^{10} x_i \mod 1 \tag{5}$$

$$b_i = \begin{cases} 1, & \text{if } d_i \geq 0.5 \\ 0, & \text{if } d_i < 0.5. \end{cases} \tag{6}$$

To test if the generated sequence is truly random, the FIPS (Federal Information Processing Standards) tests of the National Institute of Standards and Technology (NIST 800-22) are used [49]. All 15 given tests are considered. Each test results in a p-value, for which if $p \geq a$ the test is considered successful, where a is the level of significance chosen.

The tests were applied to 20 sequences of 1.000.000 bits each, for $a = 0.01$, generated for three different parameter values: $(r = 4, z = 0.5)$, $(r = 2, z = 0.3)$, and $(r = 3.4, z = 0.8)$. The results are shown in Tables 1–3, where it is seen that the sequence passes all tests for all three cases. For tests that have multiple case runs, the result of the last run is printed. The choice of multiple parameter values further showcases the versatility of the map.

In addition, Figure 18 shows the sensitivity of the system to initial conditions and parameters. It is seen that small changes lead to different trajectories and bit sequence after a very short number of iterations. In addition, Figure 19 depicts the autocorrelation and cross-correlation plots for a bit sequence of length 10^4, generated for parameter values $(r = 4, z = 0.5)$. For random sequences, the auto-correlation should have a delta like form, and the cross-correlation should be close to zero [5,13]. This is indeed verified. For the cross-correlation, two random bit sequences were generated, where the initial conditions of the two chaotic maps used are chosen as x_0 and $y_0 = x_0 + 10^{-16}$. Finally, Figure 20 depicts the percentage of 1s in the bit sequence, with respect to the sequence length. This diagram shows that there exits 0–1 balancedness in the sequence, which is another desired property.

Table 1. National Institute of Standards and Technology (NIST) statistical test results, with $a = 0.01$, and $r = 4, z = 0.5$.

	If $p \geq \alpha$, the Test Is Successful			
No.	**Statistical Test**	**p-Value**	**Proportion**	**Result**
1	Frequency	0.437274	20/20	success
2	Block Frequency	0.964295	20/20	success
3	Cumulative Sums	0.534146	20/20	success
4	Runs	0.911413	20/20	success
5	Longest Run	0.534146	19/20	success
6	Rank	0.834308	19/20	success
7	FFT	0.534146	20/20	success
8	Non-Overlapping Template	0.534146	20/20	success
9	Overlapping Template	0.534146	19/20	success
10	Universal	0.964295	19/20	success
11	Approximate Entropy	0.534146	19/20	success
12	Random Excursions	0.911413	10/10	success
13	Random Excursions Variant	0.066882	10/10	success
14	Serial	0.437274	20/20	success
15	Linear Complexity	0.964295	20/20	success

**Table 2.** NIST statistical test results, with $a = 0.01$, and $r = 2, z = 0.3$.

	If $p \geq \alpha$, the Test Is Successful			
No.	**Statistical Test**	**p-Value**	**Proportion**	**Result**
1	Frequency	0.637119	19/20	success
2	Block Frequency	0.122325	20/20	success
3	Cumulative Sums	0.090936	19/20	success
4	Runs	0.964295	20/20	success
5	Longest Run	0.350485	20/20	success
6	Rank	0.350485	20/20	success
7	FFT	0.275709	20/20	success
8	Non-Overlapping Template	0.066882	20/20	success
9	Overlapping Template	0.739918	20/20	success
10	Universal	0.834308	20/20	success
11	Approximate Entropy	0.275709	20/20	success
12	Random Excursions	0.437274	11/11	success
13	Random Excursions Variant	0.637119	11/11	success
14	Serial	0.637119	19/20	success
15	Linear Complexity	0.090936	20/20	success

**Table 3.** NIST statistical test results, with $a = 0.01$, and $r = 3.4, z = 0.8$.

	If $p \geq \alpha$, the Test Is Successful			
No.	**Statistical Test**	**p-Value**	**Proportion**	**Result**
1	Frequency	0.275709	18/20	success
2	Block Frequency	0.437274	20/20	success
3	Cumulative Sums	0.637119	19/20	success
4	Runs	0.275709	20/20	success
5	Longest Run	0.122325	20/20	success
6	Rank	0.437274	20/20	success
7	FFT	0.090936	20/20	success
8	Non-Overlapping Template	0.213309	20/20	success
9	Overlapping Template	0.834308	19/20	success
10	Universal	0.437274	20/20	success
11	Approximate Entropy	0.004301	20/20	success
12	Random Excursions	0.035174	14/14	success
13	Random Excursions Variant	0.066882	14/14	success
14	Serial	0.437274	20/20	success
15	Linear Complexity	0.964295	20/20	success
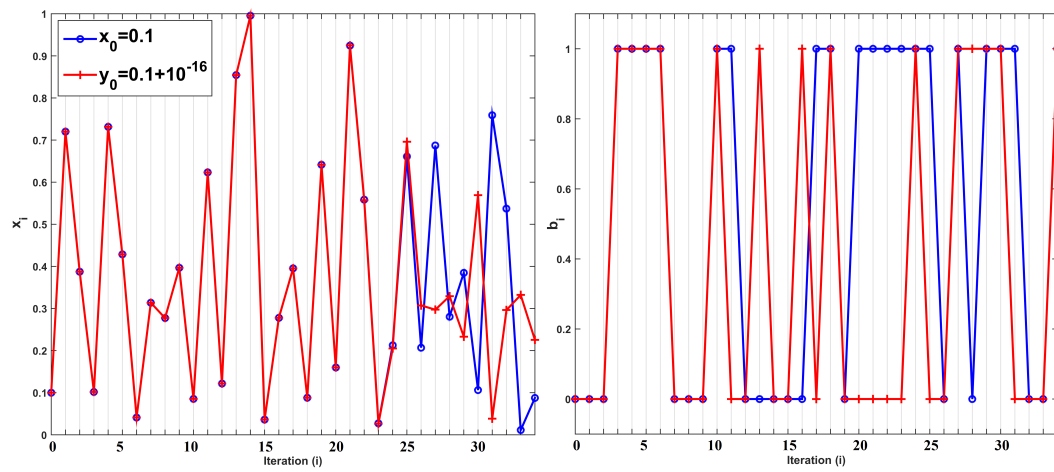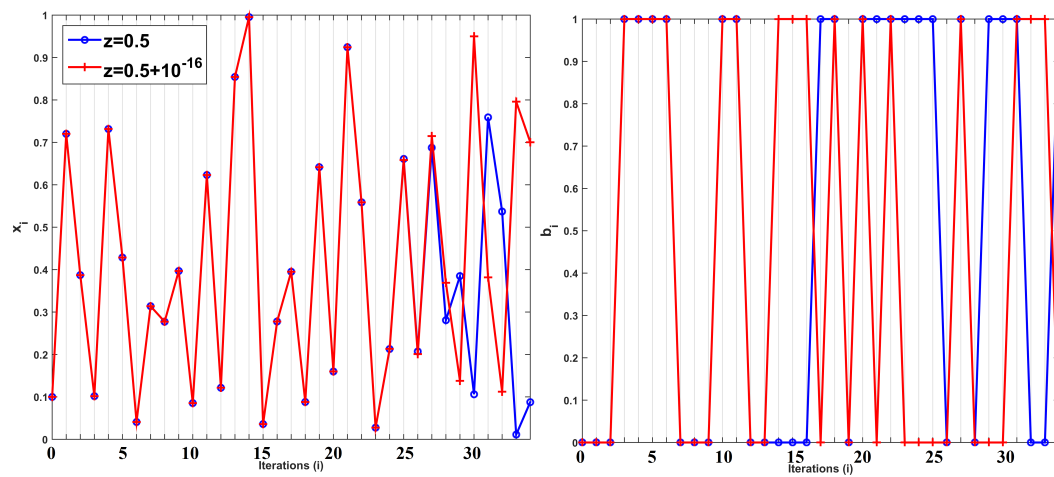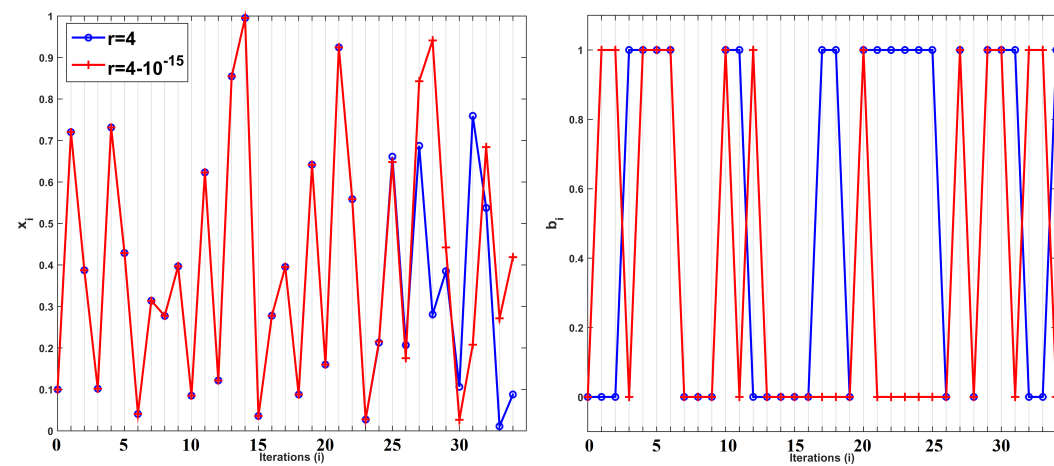
Figure 18. Sensitivity to initial conditions and parameter changes for (**a**) different initial conditions ($r = 4, z = 0.5$), (**b**) different z, ($x_0 = y_0 = 0.1, r = 4$), and (**c**) different r, ($x_0 = y_0 = 0.1, z = 0.5$).
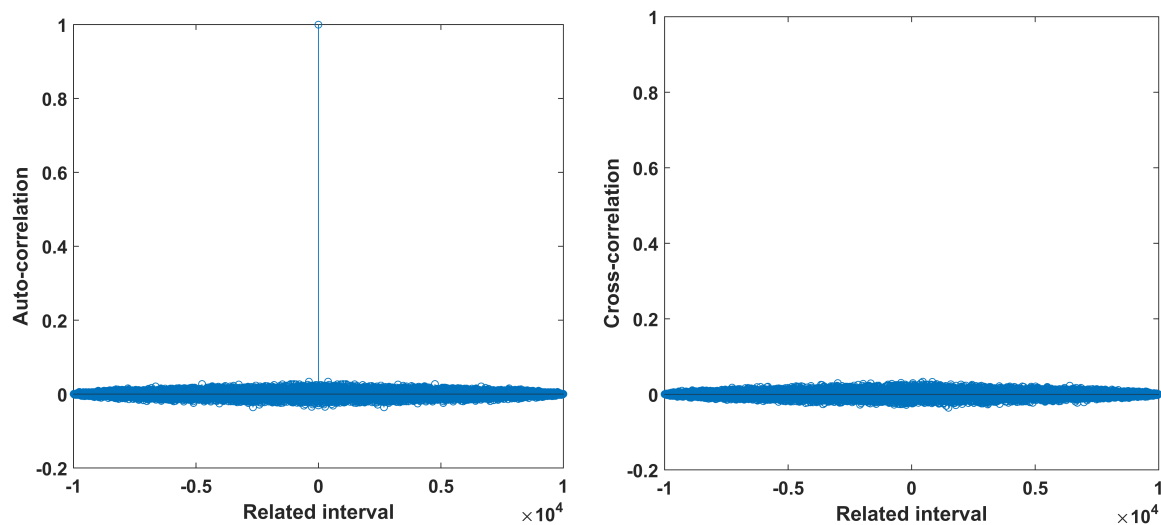
Figure 19. Auto-correlation and cross-correlation of the proposed RBG, for $(r = 4, z = 0.5)$.
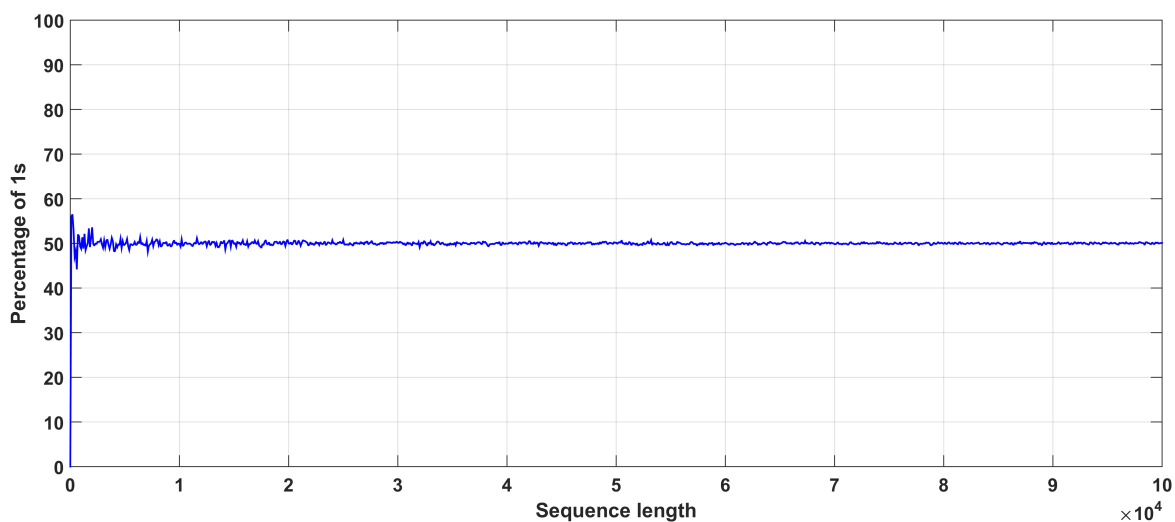

Figure 20. Occurrence of 1's in the sequence the proposed PRBG, for $(r = 4, z = 0.5)$.

As for the key space, it is known that a system should have a key space larger than 2^{100} to resist brute force attacks [51], although some more recent works require a lower bound of 2^{128} [5,38,48]. The proposed system has two key parameters r and z, as well as the initial value x_0. Assuming $z = 4$, for which the system exhibits constant chaos, the key space for a 16-digit accuracy is $10^{16} \times 10^{16} = 10^{32} \approx (10^3)^{10.6} \approx (2^{10})^{10.6} = 2^{106}$, which is higher than the minimum value 2^{100}, but lower than 2^{128}. An upper bound for the key space though can be computed by considerinrg the full spectrum of both parameters, which gives $10^{16} \times 10^{16} \times 10^{16} \approx 2^{160}$. Since the system is not chaotic for every combination of r, z, the real key space is between these two values.

5. Application to Image Encryption

The proposed RBG is further applied to the problem of image encryption, using the method proposed in [4]. The design consists of the following steps:

Step 1. An $m \times n$ grayscale image is read as a matrix whose elements represent the gray value of each pixel, taking integer values in 0-255. The values are then converted to binary numbers and the matrix columns are reshaped to a single row vector A.

Step 2. The resulting binary row vector A is combined with a binary vector B of equal length produced by the proposed RBG using the XOR command, resulting in the encrypted message $C = A \oplus B$.

Step 3. The encrypted sequence C can be transmitted safely and the original image can be reconstructed at the receiver end by taking $A = C \oplus B$ and following the reverse procedure of Step 1.

The above procedure is showcased using a 512×512 image of Lenna. The original image and the encrypted and decrypted ones are shown in Figure 21.

In order to study the security of the encryption design, several tests are performed on the encrypted image. First, the histograms of the original and encrypted images are computed, as shown in Figure 22. In contrast to the original image, the encrypted image has a uniform histogram, which makes it strong against statistical attacks.

Next, the correlation between adjacent vertical, horizontal and diagonal pixels is tested for the original and encrypted images and the results are shown in Figure 23. Here, 10000 randomly selected pairs of adjacent pixels are taken, and it is seen that in contrast to the original image, adjacent pixels in the encrypted one are uncorrelated. This is also verified by the values of the correlation coefficient γ shown in Table 4, were it is observed that for the encrypted image the value is close to zero. The correlation coefficient is computed using the following formulas:

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \tag{7}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2, \tag{8}$$

$$cov(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{9}$$

$$\gamma(x,y) = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{10}$$

where x, y are the gray values of two adjacent pixels, and N the number of adjacent pairs of pixels considered.

Finally, the information entropy is computed, which measures the randomness of a given signal, given by

$$H(S) = - \sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i), \tag{11}$$

where $p(s_i)$ is the possibility of appearance for the symbol s_i. The information entropy of an encrypted image should be close to 8. The information entropy of the original image is 7.4450, while for the encrypted image is 7.9670, so the encrypted image has a value closer to 8, which means that the information signal is safer against entropy attacks.
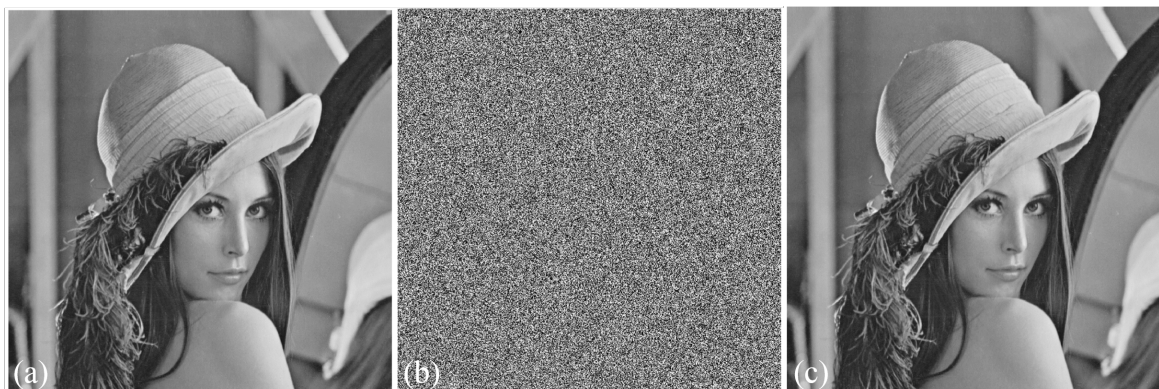

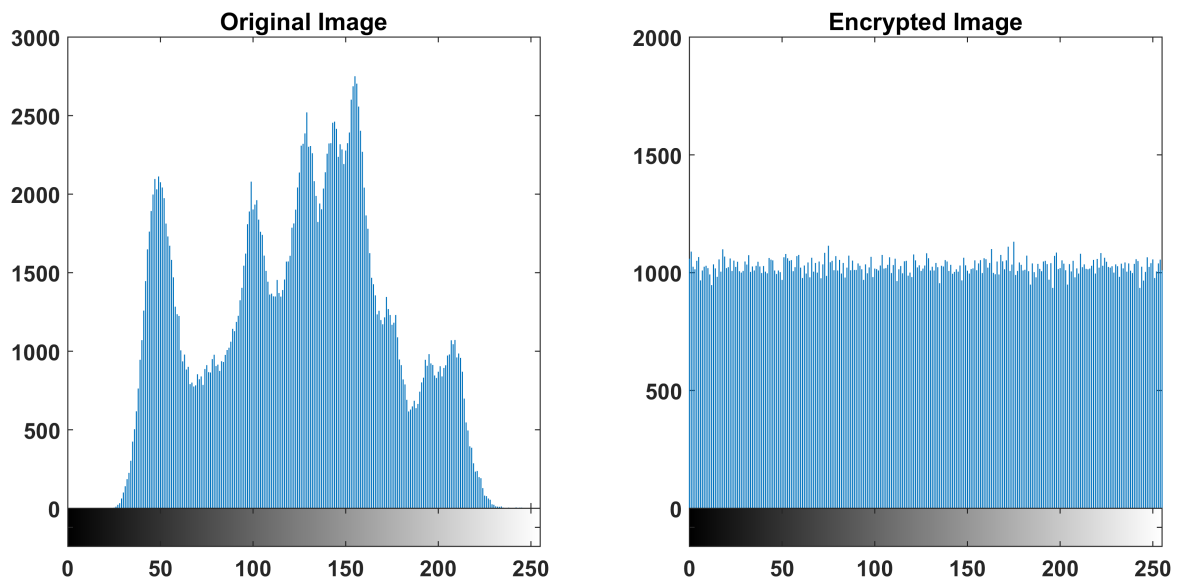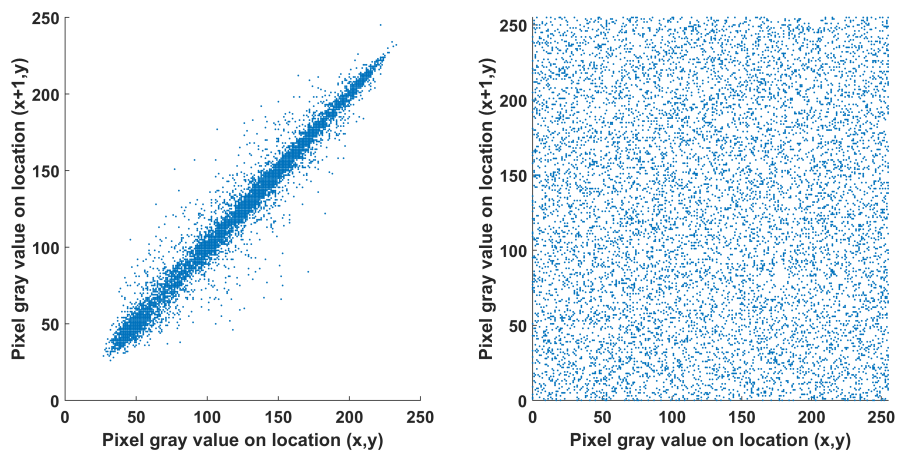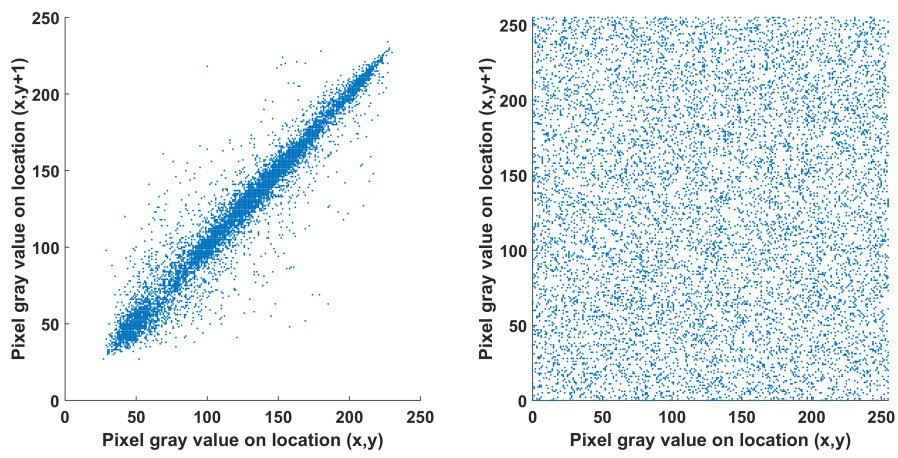**Figure 21.** (**a**) Original image, (**b**) encrypted, and (**c**) decrypted.
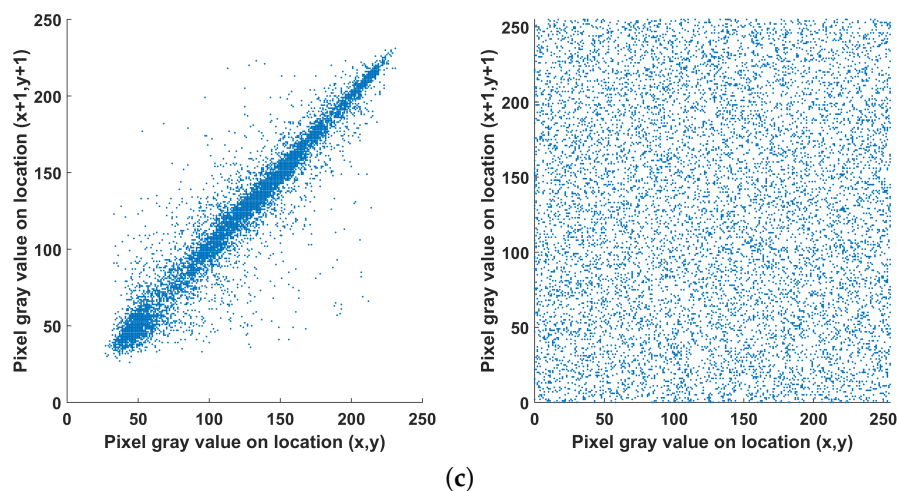
Figure 22. Histograms of the plain and encrypted image.

Figure 23. *Cont.*

(c)

Figure 23. Correlation analysis of two (**a**) horizontal, (**b**) vertical and (**c**) diagonal adjacent pixels for the original (**left**) and encrypted (**right**) image.

Table 4. Correlation coefficients of two adjacent pixels in the original and encrypted image.

	Original	Encrypted
Horizontal	0.9843	0.0046
Vertical	0.9724	0.0063
Diagonal	0.9573	0.0023

6. Conclusions

In this work, the logistic map was modified through the use of fuzzy triangular numbers, to give a new modified logistic map that exhibits a plethora of chaos related phenomena, for different parameter values. It was shown that the modified logistic map also reaches a higher Lyapunov exponent compared to the logistic map. The map was then applied to the problem of random bit generation, yielding positive results. It is important to note that this simple technique to increase the complexity of a chaotic map can easily be implemented to many other chaotic systems. In addition, using different fuzzy numbers other than triangular can lead to many modifications of this technique. These are both promising research topics for future works.

Author Contributions: Conceptualization, L.M.; Formal analysis, L.M., C.V.; Methodology, L.M., C.V.; Software, L.M., C.V.; Supervision, C.V., I.S., S.J., J.M.M.-P., J.K., K.R.; Validation, L.M., C.V., I.S., S.J., J.M.M.-P., J.K., K.R.; Visualization, L.M., C.V.; Writing, L.M., C.V. All authors have read and agreed to the published version of the manuscript.

References

1. Strogatz, S.H. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*; CRC Press: Boca Raton, FL, USA, 2018.
2. Azar, A.T.; Vaidyanathan, S. *Advances in Chaos Theory and Intelligent Control*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 337.

3.   Fradkov, A.L.; Evans, R.J. Control of chaos: Methods and applications in engineering. *Annu. Rev. Control.* **2005**, *29*, 33–56. [CrossRef]

4.   Volos, C.K.; Kyprianidis, I.M.; Stouboulos, I.N. Image encryption process based on chaotic synchronization phenomena. *Signal Process.* **2013**, *93*, 1328–1340. [CrossRef]

5.   Huang, X.; Liu, L.; Li, X.; Yu, M.; Wu, Z. A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics. *Complexity* **2019**, *2019*, 6567198. [CrossRef]

6.   May, R.M. Simple mathematical models with very complicated dynamics. *Nature* **1976**, *261*, 459–467. [CrossRef]

7.   Sun, Y.; Wang, G. An image encryption scheme based on modified logistic map. In Proceedings of the 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications, Hangzhou, China, 19–22 October 2011; pp. 179–182.

8.   Wu, G.C.; Baleanu, D. Discrete fractional logistic map and its chaos. *Nonlinear Dyn.* **2014**, *75*, 283–287. [CrossRef]

9.   Han, C. An image encryption algorithm based on modified logistic chaotic map. *Optik* **2019**, *181*, 779–785. [CrossRef]

10. Wang, Y.; Liu, Z.; Ma, J.; He, H. A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dyn.* **2016**, *83*, 2373–2391. [CrossRef]

11. Murillo-Escobar, M.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn.* **2017**, *87*, 407–425. [CrossRef]

12. Radwan, A.G. On some generalized discrete logistic maps. *J. Adv. Res.* **2013**, *4*, 163–171. [CrossRef]

13. Liu, L.; Miao, S.; Cheng, M.; Gao, X. A pseudorandom bit generator based on new multi-delayed Chebyshev map. *Inf. Process. Lett.* **2016**, *116*, 674–681. [CrossRef]

14. Liu, L.; Miao, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus* **2016**, *5*, 289. [CrossRef] [PubMed]

15. Valandar, M.Y.; Ayubi, P.; Barani, M.J. A new transform domain steganography based on modified logistic chaotic map for color images. *J. Inf. Secur. Appl.* **2017**, *34*, 142–151. [CrossRef]

16. Chen, S.L.; Hwang, T.; Lin, W.W. Randomness enhancement using digitalized modified logistic map. *IEEE Trans. Circuits Syst. II Express Briefs* **2010**, *57*, 996–1000.

17. Borujeni, S.E.; Ehsani, M.S. Modified logistic maps for cryptographic application. *Appl. Math.* **2015**, *6*, 773. [CrossRef]

18. Zimmermann, H.J. *Fuzzy Set Theory—And Its Applications*; Springer Science & Business Media: Berlin, Germany, 2011.

19. Chakraverty, S.; Sahoo, D.M.; Mahato, N.R. *Concepts of Soft Computing: Fuzzy and ANN with Programming*; Springer: Berlin/Heidelberg, Germany, 2019.

20. Hanss, M. *Applied Fuzzy Arithmetic: An Introduction with Engineering Applications*; Springer: Berlin/Heidelberg, Germany, 2005.

21. Li, Z.; Zhang, X. On Fuzzy Logic and Chaos Theory: from an Engineering Perspective. In *Fuzzy Logic: A Spectrum of Theoretical & Practical Issues*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 79–97.

22. Oliva, G.; Panzieri, S.; Setola, R. Fuzzy chaotic logistic maps. In Proceedings of the World Automation Congress 2012, Puerto Vallarta, Mexico, 24–28 June 2012; pp. 1–6.

23. Molaeezadeh, S.F.; Moradi, M.H. Bifurcating fuzzy sets: Theory and application. *Neurocomputing* **2013**, *118*, 268–278. [CrossRef]

24. Hong, L.; Sun, J.Q. Bifurcations of fuzzy nonlinear dynamical systems. *Commun. Nonlinear Sci. Numer. Simul.* **2006**, *11*, 1–12. [CrossRef]

25. Porto, M.; Amato, P. A fuzzy approach for modeling chaotic dynamics with assigned properties. In Proceedings of the Ninth IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2000 (Cat. No. 00CH37063), San Antonio, TX, USA, 7–10 May 2000; Volume 1, pp. 435–440.

26. Nieto, J.J.; Otero-Espinar, M.V.; Rodríguez-López, R. Dynamics of the fuzzy logistic family. *Discret. Contin. Dyn. Syst. B* **2010**, *14*, 699. [CrossRef]

27. Fridrich, J. On chaotic systems: fuzzified logistic mapping. *Int. J. Gen. Syst.* **1994**, *22*, 369–380. [CrossRef]

28. Stefanini, L.; Sorini, L.; Guerra, M.L. Simulation of fuzzy dynamical systems using the LU-representation of fuzzy numbers. *Chaos Solitons Fractals* **2006**, *29*, 638–652. [CrossRef]

29. Patidar, V.; Sud, K.K.; Pareek, N.K. A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica* **2009**, *33*, 441–452.

30. Stojanovski, T.; Kocarev, L. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **2001**, *48*, 281–288. [CrossRef]

31. Volos, C.; Kyprianidis, I.; Stouboulos, I. Experimental investigation on coverage performance of a chaotic autonomous mobile robot. *Robot. Auton. Syst.* **2013**, *61*, 1314–1322. [CrossRef]

32. Volos, C.K.; Kyprianidis, I.; Stouboulos, I. Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator. *J. Eng. Sci. Technol. Rev.* **2013**, *6*, 9–14. [CrossRef]

33. Hamza, R. A novel pseudo random sequence generator for image-cryptographic applications. *J. Inf. Secur. Appl.* **2017**, *35*, 119–127. [CrossRef]

34. Irfan, M.; Ali, A.; Khan, M.A.; Ehatisham-ul Haq, M.; Mehmood Shah, S.N.; Saboor, A.; Ahmad, W. Pseudorandom Number Generator (PRNG) Design Using Hyper-Chaotic Modified Robust Logistic Map (HC-MRLM). *Electronics* **2020**, *9*, 104. [CrossRef]

35. Nepomuceno, E.G.; Nardo, L.G.; Arias-Garcia, J.; Butusov, D.N.; Tutueva, A. Image encryption based on the pseudo-orbits from 1D chaotic map. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 061101. [CrossRef]

36. Tutueva, A.V.; Nepomuceno, E.G.; Karimov, A.I.; Andreev, V.S.; Butusov, D.N. Adaptive chaotic maps and their application to pseudo-random numbers generation. *Chaos Solitons Fractals* **2020**, *133*, 109615. [CrossRef]

37. Akgül, A.; Arslan, C.; Arıcıoğlu, B. Design of an Interface for Random Number Generators based on Integer and Fractional Order Chaotic Systems. *Chaos Theory Appl.* **2019**, *1*, 1–18.

38. François, M.; Grosges, T.; Barchiesi, D.; Erra, R. Pseudo-random number generator based on mixing of three chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 887–895. [CrossRef]

39. Khanzadi, H.; Eshghi, M.; Borujeni, S.E. Image encryption using random bit sequence based on chaotic maps. *Arab. J. Sci. Eng.* **2014**, *39*, 1039–1047. [CrossRef]

40. Wang, X.Y.; Xie, Y.X. A design of pseudo-random bit generator based on single chaotic system. *Int. J. Mod. Phys. C* **2012**, *23*, 1250024. [CrossRef]

41. Andrecut, M. Logistic map as a random number generator. *Int. J. Mod. Phys. B* **1998**, *12*, 921–930. [CrossRef]

42. Ahmad, M.; Doja, M.; Beg, M.S. A new chaotic map based secure and efficient pseudo-random bit sequence generation. In *International Symposium on Security in Computing and Communication*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 543–553.

43. Wang, L.; Cheng, H. Pseudo-Random Number Generator Based on Logistic Chaotic System. *Entropy* **2019**, *21*, 960. [CrossRef]

44. Pak, C.; Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **2017**, *138*, 129–137. [CrossRef]

45. Farhan, A.K.; Al-Saidi, N.M.; Maolood, A.T.; Nazarimehr, F.; Hussain, I. Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder. *Entropy* **2019**, *21*, 958. [CrossRef]

46. Xie, Y.; Yu, J.; Guo, S.; Ding, Q.; Wang, E. Image encryption scheme with compressed sensing based on new three-dimensional chaotic system. *Entropy* **2019**, *21*, 819. [CrossRef]

47. Natiq, H.; Al-Saidi, N.; Said, M.; Kilicman, A. A new hyperchaotic map and its application for image encryption. *Eur. Phys. J. Plus* **2018**, *133*, 6. [CrossRef]

48. François, M.; Grosges, T.; Barchiesi, D.; Erra, R. A new image encryption scheme based on a chaotic function. *Signal Process. Image Commun.* **2012**, *27*, 249–259. [CrossRef]

49. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A statistical Test Suite for Random and Pseudorandom Number Generators for cRyptographic Applications*; Technical Report; Booz-Allen and Hamilton Inc.: Mclean, VA, USA, 2001.

50. Wolf, A.; Swift, J.B.; Swinney, H.L.; Vastano, J.A. Determining Lyapunov exponents from a time series. *Phys. D Nonlinear Phenom.* **1985**, *16*, 285–317. [CrossRef]

51. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]