Discrete one-dimensional piecewise chaotic systems without fixed points

Marcin Lawnik[1*], Lazaros Moysis[2,3*], Murilo S. Baptista[4] and Christos Volos[2]

[1]Department of Mathematics Applications and Methods for Artificial Intelligence, Faculty of Applied Mathematics, Silesian University of Technology, Kaszubska 23, 44-100 Gliwice, Poland.
[2]Laboratory of Nonlinear Systems - Circuits & Complexity, Physics Department, Aristotle University of Thessaloniki, Thessaloniki, Greece.
[3]Department of Mechanical Engineering, University of Western Macedonia, Kozani, 50100, Greece.
[4]Institute for Complex Systems and Mathematical Biology, SUPA, University of Aberdeen, Aberdeen AB24 3UX, UK.

*Corresponding author(s). E-mail(s): marcin.lawnik@polsl.pl; lmousis@physics.auth.gr;
Contributing authors: murilo.baptista@abdn.ac.uk.; volos@physics.auth.gr;

Abstract

This paper presents a new method of generating chaotic maps that do not have fixed points. The method uses an appropriate transformation of functions defined on the unit square in such a way that the newly created projection has no fixed points. In this way, countless new chaotic mappings can be created, both piecewise linear and nonlinear, that belong to the family of systems with hidden attractors. The new family of maps is presented in three examples showing phase diagrams, bifurcation diagrams, and space parameters of the Lyapunov exponent. The discussed examples of mappings were created by appropriate logistic and tent mapping transformations, and their combination. In addition, this paper analyzes the applications of the new families of chaotic mappings in chaotic cryptography. Furthermore, an algorithm for generating pseudorandom bit values (PRBG) is also presented based on the examples of proposed mappings.

Keywords: chaos, piecewise map, equilibrium, fixed point, hidden attractor, logistic map, tent map, chaotification, prbg, encryption

1 Introduction

Chaos theory is one of the great discoveries of the 20th century. Since its discovery, dynamical systems have played a key role in many aspects of science and engineering [1]. Chaotic systems have been reported in various fields, e.g., chemical engineering [2], economics [3], or even medicine [4]. One of the special areas were such systems have found use is the so-called chaotic cryptography. In chaotic cryptography, chaotic systems are a carrier of randomness, that is, using them as a high entropy source, sequences of pseudo-random values are generated, which are then used to ensure security, by masking an information signal. Of course, following the rules prevailing in cryptography, the security of methods and algorithms depends on the so-called unique keys, which in the context of chaotic cryptography, are the values of parameters and initial conditions of the chaotic system. This means that a completely different random stream will be generated by minimally changing the value of the initial condition or parameter of the system. Thus, an uncountable number of different streams of pseudo-random values can be generated. On the other hand, knowing the exact values of such a key allows for fully recreating the generated pseudo-random sequence.

Chaotic cryptography deals with all threads of data security. The resulting algorithms are used to encrypt any type of media, including text [5], image [6], audio [7], and video [8], generating hash functions [9] and S-boxes [10] or even allowing encryption from the context of the so-called asymmetric cryptography [11]. In addition to chaotic cryptography, chaotic systems are used in path planning [12] or optimization algorithms [13]. However, it is clear that for a given chaotic system to be used in such applications, it must meet certain criteria regarding its dynamical behavior. These criteria include sufficiently large ranges of parameter values and initial conditions for which chaos occurs. If the system generates a periodic solution instead of a chaotic solution, then such an algorithm to encrypt information stops working properly, and security is broken.

Several previous works have proposed nonlinear systems that are chaotic and that possess some special property suitable for an encryption method. The proposed systems are either continuous [14–16], systems with derivatives of fractional order [17–20], or discrete [21–23]. It is clear that using a continuous system requires the system to be defined by at least three equations in order to generate chaos. Moreover, the solution of continuous systems is heavily affected by the numerical method used, so accurate reconstruction of the solution across devices is difficult. On the other hand, in the case of discrete systems, only one equation is enough to obtain chaotic solutions, and the time series solution is obtained by a simple iterative function. Moreover, the decay of the correlation of maps is much faster than their continuous analogues. Thus, discrete systems are undoubtedly a better variant, because of the computational cost of generating subsequent solutions.

Among the discrete systems used in chaotic cryptography, such maps as the logistic or asymmetric tent maps are very popular. However, often these systems do not meet the basic criteria of wide parameter ranges of chaos. Another problem associated with chaotic systems is the occurrence of so-called fixed points. The system stops generating chaotic solutions if such a point is chosen as the initial condition. Even worse is the situation when the fixed point is stable. All the points belonging to its basin of

attraction will be attracted to it after a sufficiently large number of iterations. When selecting keys (based on initial conditions), the fixed point and the points belonging to its basin of attraction should be omitted. For this reason, there are works in the literature on the construction of chaotic systems that do not have fixed points. These works concern continuous [24–29] and discrete [30–39] systems, and are generally termed systems with hidden attractors.

Many works deal with the lack of fixed points among the continuous systems. One such work is [24]. Another such work is [25], where a new system was proposed and applied to generate random bit sequences. References [26–28] presents electronic circuits implementations of systems without fixed points. Yet another model is presented in [29].

Also, discrete systems may not have fixed points. This applies to both one-dimensional (1d) and multi-dimensional systems as in paper [30]. Another 2d system was presented in [31], where a memristor was used in its construction. A comparison of different 1d and 2d mappings without fixed points is done in [32] by means of different models with each other, presenting, e.g., bifurcation diagrams, Lyapunov exponents, or entropy calculation. A piecewise-linear mapping is presented in [33], where the authors showed how to use field-programmable gate arrays to implement it. Also, in [34], the dynamics of a discrete linear system were analyzed. A modified logistic map without fixed point is proposed in [35], and its dynamic characterization was presented in [36]. A family of Bernoulli-like maps without fixed points were proposed in [37]. In [38], recursions of the form of the Newton and Euler methods were used to show that mappings of such a form are characterized by chaotic behavior, and at the same time, they do not have fixed points. Yet another family of one-dimensional curves, which is characterized by chaotic behavior and the lack of fixed points, is presented in [39].

Motivated by the constructions of maps in [39], this paper presents a new method of generating countless examples of chaotic maps that do not have fixed points. The new family of mappings is presented in three examples showing phase diagrams, bifurcation diagrams, and space parameters of the Lyapunov exponent. In addition, this paper analyzes the applications of the new family of chaotic mappings in chaotic cryptography. Furthermore, a new algorithm for generating pseudorandom bit values (PRBG) is also presented based on the examples of proposed mappings.

The rest of this article is structured as follows. Section 2 presents the basic preliminaries. Section 3 deals with the derivation and analysis of a new family of maps without fixed points. The next Section 4 shows examples of maps along with their analysis. Section 5 discusses the applications of the proposed family of mappings. The work closes with the Conclusions section, and a discussion on future topics of interest.

2 Preliminaries

Let us consider a one-dimensional (1d) discrete dynamical system of the form

$$x_{k+1} = f(x_k), \tag{1}$$

where f is the mapping function, $x(k)$ is the state of the map and $k = 0, 1, \ldots$ denotes the iteration number. Furthermore, let us assume that the function $f : [0, 1] \to [0, 1]$.

A fixed point, or equilibrium, of the map (1) is a state value of x^* for which the following relation holds

$$f(x^*) = x^*. \tag{2}$$

The graphical interpretation of condition (2) means that the plot of the function $f(x)$ intersects the bisector line at the point (x^*, x^*).

The representation of the form (1) may be characterized by stable or chaotic behavior. The necessary condition for the occurrence of chaos for (1) is the positive value of the Lyapunov exponent λ given by the formula

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|. \tag{3}$$

3 The Proposed Family of Maps

In [39] the authors suggested that the map (1) has no fixed points when it is of the form

$$x_{k+1} = \begin{cases} f_1(x_k), \ 0 \le x_k \le p \\ f_2(x_k), \ p < x_k \le 1 \end{cases}, \tag{4}$$

where

$$f_1(x) > x, \quad \forall x \in [0, p] \tag{5}$$

$$f_2(x) < x, \quad \forall x \in [p, 1]. \tag{6}$$

This geometric approach considered placing each of the 2 sub-functions above and below the bisector in the 2d plane, to guarantee the absence of equilibria.. The problem with (4) is the appropriate definition of the functions f_1 and f_2. This paper shows how to transform the function $f : [0, 1] \to [0, 1]$ to the form (4) fulfilling conditions (5) and (6).

Let us consider a function $f : [0, 1] \to [0, 1]$. Now consider the following function compositions of f:

1°: $(1 - a)\left(-f\left(\frac{x}{p}\right) + 1\right) + a$ for $x \in [0, p]$,

2°: $bf\left(\frac{x-p}{1-p}\right)$ for $x \in (p, 1]$,

where $a, b, p \in (0, 1)$ are parameters.

The composition 1° is a transformation of the domain of the function f into the interval $[0, p]$, then reflection about the x-axis is applied and, finally, its set of values is defined as $[a, 1]$. In turn, composition 2° transforms the domain of the function f into the interval $(p, 1)$ and defines its set of values in the interval $[0, b]$. Both compositions create a new function, which we denote as F. Then $F : [0, 1] \to [0, 1]$ and is in the form

$$F(x) = \begin{cases} (1 - a)\left(-f\left(\frac{x}{p}\right) + 1\right) + a, & x \in [0, p] \\ bf\left(\frac{x-p}{1-p}\right), & x \in (p, 1] \end{cases}. \tag{7}$$

Example function f and its compositions 1° and 2° are shown in the left and right graphs of Figure 1, respectively. The right graph shows that if the appropriate

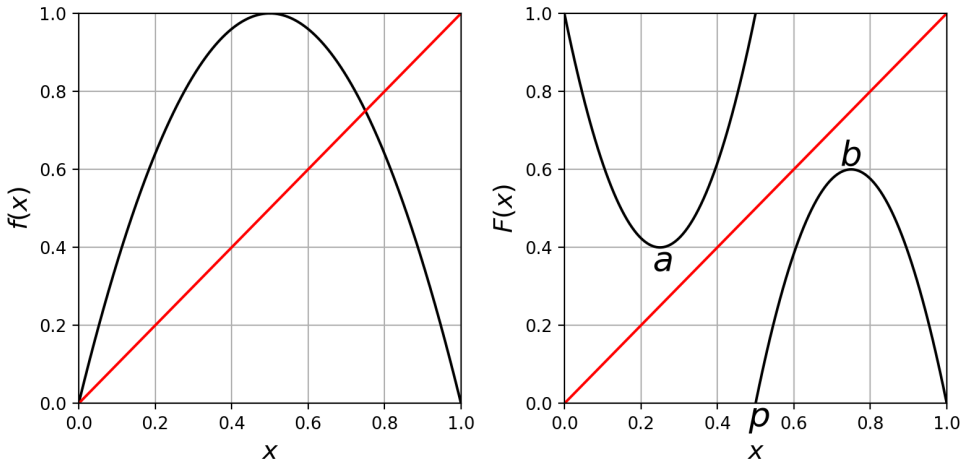


Fig. 1: An example of function f (left) and the corresponding function F of the form (7) (right). The parameters a, b and p in the right figure correspond to the parameters from mapping (7), $a = 0.4,\ b = 0.6,\ p = 0.5$.

relationship between the parameters a, b, and p is maintained, then the function F does not intersect the line $y = x$.

Remark 1. *It is obvious that not every f function is suitable as a base function. A good example is the function shown in Figure 2. This graph shows that if the basis function f is the function that takes the largest values in the neighbourhood of the points $x = 0$ or $x = 1$ (in the case of Figure 2, the relation $f(0) = f(1) = 1$ holds), then the intersection of the line $y = x$ by the function F is very likely.*

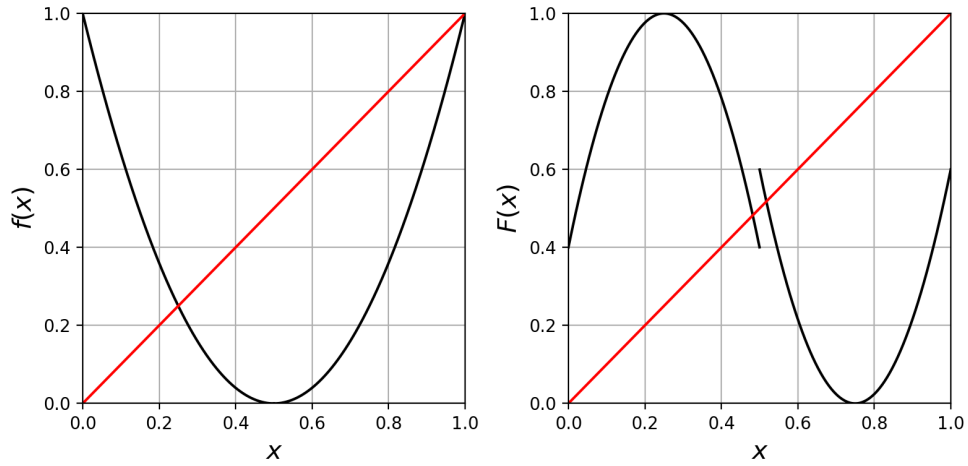


Fig. 2: An example of the base function f (left) and the function F (right) that intersects the line $y = x$, $a = 0.4,\ b = 0.6,\ p = 0.5$.

Let us consider now the following discrete piecewise map

$$x_{k+1} = F(x_k) = \begin{cases} (1-a)\left(-f\left(\frac{x_k}{p}\right)+1\right)+a, & 0 \le x_k \le p \\ bf\left(\frac{x_k-p}{1-p}\right), & p < x_k \le 1 \end{cases}, \tag{8}$$

where $a, b, p \in (0,1)$ and f is a function that $f : [0,1] \to [0,1]$.

The goal is to determine the relationship between the parameters a, b and p in such a way that the mapping (8) does not have fixed points. It should be noted that by controlling the parameters a, b and p, the mapping (8) may not have fixed points, or have a certain number of them.

Remark 2. *In order to facilitate the construction of mappings of the form* (8)*, the following conditions should be met by the f function:*

1. $f(1) = f(0) = 0$,
2. *there is at least one point* $\overline{x} \in (0,1)$ *such that* $f(\overline{x}) = 1$.

Condition 1. means that $F(0) = F(p) = 1$ and $\lim_{x \to p^+} F(p) = F(1) = 0$.

On the other hand, condition 2. means that parameters a and b are in the range $(0,1)$. This results from the fact that the map F, like the function f, is defined on the unit square.

These conditions are conducive for the function F not to intersect the line $y = x$ but still allow for its flexible definition. Examples of such mappings are shown in the next section of this paper. In turn, an example of a function f that does not meet these conditions is shown in Figure 2.

Moreover, it is worth noting that the function f does not have to be continuous for map (8) to have no fixed points.

Remark 3. *Note that the mapping (8) depends directly on the parameters a, b and p. However, the function f can also depend on some other parameters, as is often the case with chaotic mappings. Thus, the number of parameters for mapping (8) can be significantly greater. This situation occurs, for example, in the case of examples of tent maps 4.1.*

Remark 4. *The mapping (8) can be modified to the following form*

$$x_{k+1} = F(x_k) = \begin{cases} (1-a)\left(-f_1\left(\frac{x_k}{p}\right)+1\right)+a, & 0 \le x_k \le p \\ b f_2\left(\frac{x_k-p}{1-p}\right), & p < x_k \le 1 \end{cases}, \tag{9}$$

where f_1 and f_2 are two different functions that satisfy the conditions for the f function.

Remark 5. *With the appropriate selection of parameters a, b, and p, mapping (8) (and also (9)) will not have fixed points. However, nothing more can be said about its dynamics. Everything depends on the function f (or f_1 and f_2 in (9)). Thus, all cases other than fixed points can appear. This also applies to the occurrence of chaos. Regardless of the type of behavior, the mapping trajectories (8) (and (9)) are always bounded — they are contained in the interval $[0, 1]$. This means that both periodic and chaotic solutions will be included in this interval. This is especially important in the context of chaotic behavior, where a positive Lyapunov exponent and a bounded trajectory will guarantee some kind of attractor. However, how complicated the dynamics of maps (8) and (9) are can be seen by defining the function f (or f_1 and f_2 in the case of (9)), as shown by the examples given in Section 4.*

4 Examples

This section shows examples of mappings constructed from various basis functions in the form (8) and (9).

4.1 Tent map

As a first example, consider the well-known asymmetric tent map

$$f(x) = \begin{cases} \frac{x}{r} & 0 \le x \le r \\ \frac{1-x}{1-r} & r < x \le 1 \end{cases}, \tag{10}$$

where $r \in (0, 1)$ and $x \in [0, 1]$.

The tent map function (10) satisfies the assumptions required for the function f in the Remark 2. After substituting (10) to (8) the dynamical system is of the form

$$x_{k+1} = \begin{cases} -\frac{1-a}{pr}x_k + 1 & 0 \le x_k \le pr \\ \frac{1-a}{p(1-r)}(x_k - p) + 1 & pr < x_k \le p \\ \frac{b}{r(1-p)}(x_k - p) & p < x_k \le (1-p)r + p \\ \frac{b}{(1-r)(1-p)}(1-x_k) & (1-p)r + p < x_k \le 1 \end{cases}, \tag{11}$$

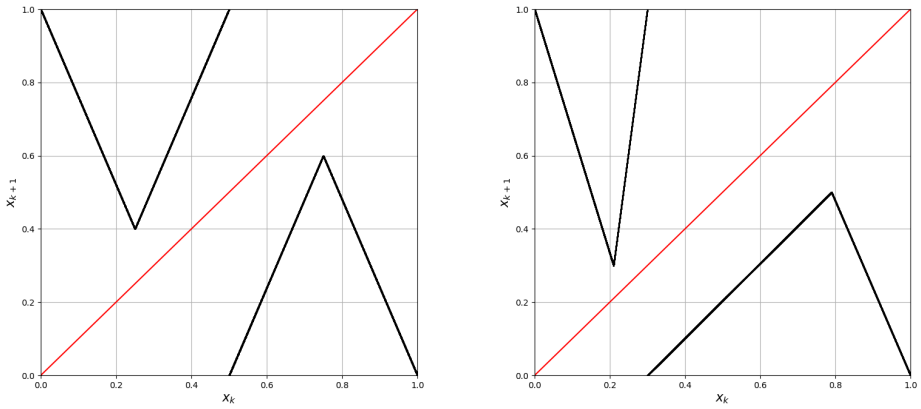
Lemma 1. *When the parameters a, b, p and r meet the conditions*

$$a > pr \text{ and } b < (1-p)r + p, \tag{12}$$

then, the map (11) has no fixed point.

Proof. The mapping (11) has at least one fixed point when there is at least one common point of the mapping with the line $y = x$. In particular, this point is the splicing point of the subfunctions, which can be called the vertex of the mapping for $x \leq p$ and for $x > p$. It is worth noting that the vertices of this mapping are extremum points, that is, the minimum for $x \leq p$ and the maximum for $x > p$. The vertex coordinates are equal to (pr, a) for $x \leq p$ and $((1-p)r + p, b)$ for $x > p$, respectively. From these coordinates, the relationships $a > pr$ and $b < (1-p)r+p$ follow directly. □

The phase diagrams of the mapping (11) for fixed values of the parameters a, b, p and r are shown in Figure 3. The left graph shows a symmetric map, whereas in the right graph, this map is no longer symmetric. However, it is clear from both graphs that these maps do not have fixed points.



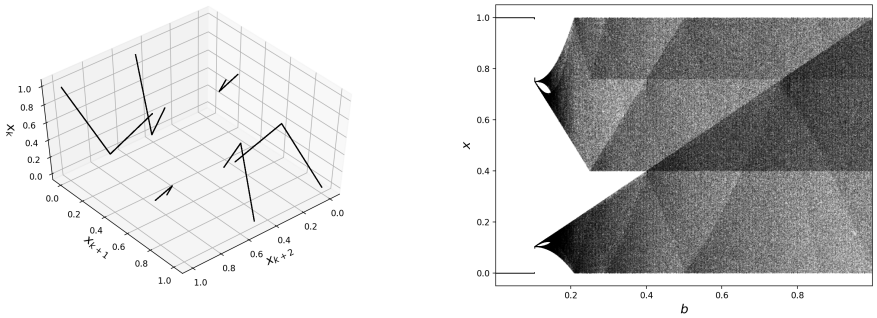
(a) $a = 0.4,\ b = 0.6,\ p = 0.5$ and $r = 0.5$. (b) $a = 0.3,\ b = 0.5,\ p = 0.3$ and $r = 0.7$.

Fig. 3: Phase diagrams of tent maps of the form (11).

In addition, to better illustrate the dynamics of the system, a 3d diagram in the relation (x_k, x_{k+1}, x_{k+2}) for selected parameter values was determined. These results are presented in Figure 4a.

Furthermore, to better show the dynamics of the map (11), depending on the value of the b parameter, a bifurcation diagram was determined, shown in Figure 4b. It clearly shows that the behavior of map (11) is very complicated, including the occurrence of chaos, which will be further investigated. Furthermore, it is worth noting

that the transition to chaos from a two-period orbit does not occur by doubling the period. There is the so-called crisis phenomenon.

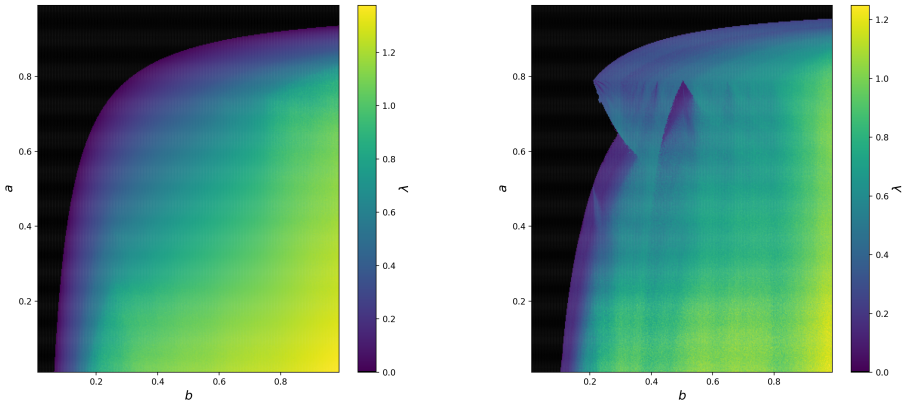


(a) $a = 0.4,\ b = 0.6,\ p = 0.5$ and $r = 0.5$.

(b) $a = 0.4,\ p = 0.5$ and $r = 0.5$.

Fig. 4: 3D phase diagram and bifurcation diagram of logistic-tent maps of the form (11).

Fixed points and periodic solutions are just one of the behaviors that can characterize a dynamical system (11). However, the occurrence of chaos is significant in its behavior. The necessary condition for its occurrence is the positive value of the Lyapunov exponent λ given by the formula (3). Figure 5 shows the parameter space of the Lyapunov exponent obtained for map (11) with different parameter values. The black color in this graph represents parameter values (a, b) for which the system has stable periodic behavior. The other colors, however, represent parameters which lead the system to chaos. It is worth noting that set of parameters leading to chaos is a single open set, i.e., parameters leading to chaos are not close to parameters leading to periodic behavior, except at the boundary between chaotic and periodic parameter regions. In addition, the left graph is symmetrical, resulting from the mapping (11) and the selected parameter values.



(a) $p = 0.5, r = 0.5$.

(b) $p = 0.3, r = 0.7$.

Fig. 5: Parameter spaces showing the Lyapunov exponent of tent maps of the form (11).

4.2 Logistic map

As a second example, let us consider the well-known logistic map

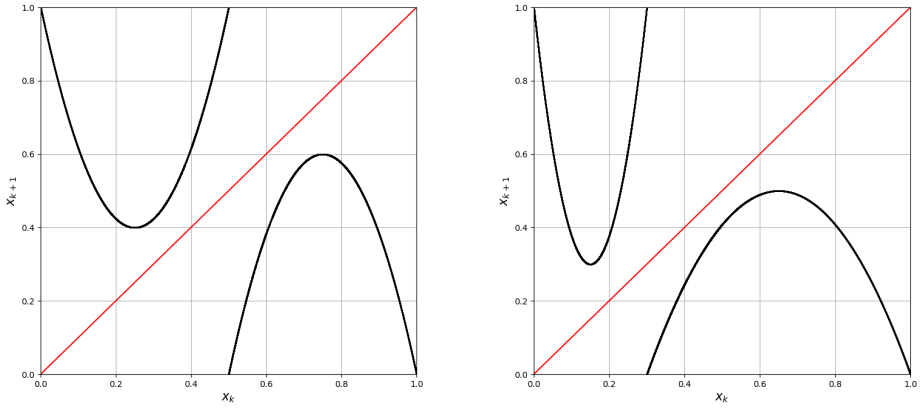
$$f(x) = rx(1 - x), \tag{13}$$

where $r \in [0, 4]$ and $x \in [0, 1]$.

For $r = 4$, the logistic map function (13) satisfies the assumptions required for the function f in the Remark 2. After substituting (13) to (8) the dynamical system is of the form

$$x_{k+1} = \begin{cases} \frac{4(1-a)}{p^2}\left(x_k - \frac{p}{2}\right)^2 + a & 0 \leq x_k \leq p \\ \frac{-4b}{(p-1)^2}\left(x_k - \frac{1+p}{2}\right)^2 + b & p < x_k \leq 1 \end{cases}. \tag{14}$$

The phase diagrams of the mapping (14) for fixed values of the parameters a, b and p are shown in Figure 6. As in the previous example, the left graph shows a symmetric map, whereas in the right graph, this map is no longer symmetric. However, it is clear from both graphs that these projections do not have fixed points.



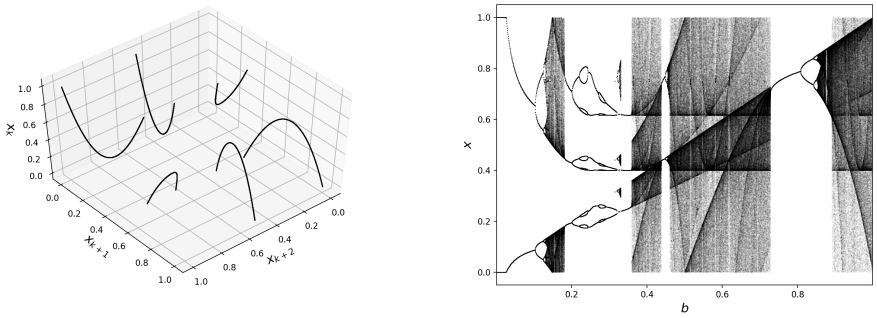
(a) $a = 0.4,\ b = 0.6,\ p = 0.5.$ (b) $a = 0.3,\ b = 0.5,\ p = 0.3.$

Fig. 6: Phase diagrams of logistic maps of the form (14).

In addition, like in the first example, a 3d phase diagram in the relation (x_k, x_{k+1}, x_{k+2}) for selected parameter values was also determined. These results are presented in Figure 7a.

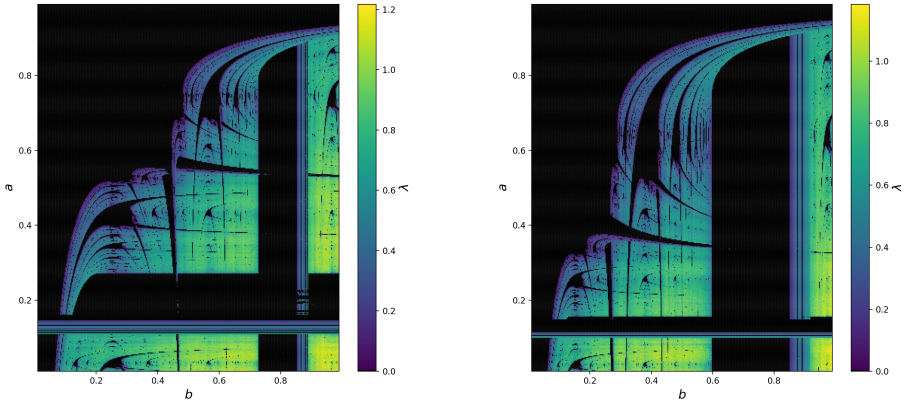
Furthermore, like in the first example, to better show the dynamics of the map (14), depending on the value of the b parameter, a bifurcation diagram was also determined, shown in Figure 7b. It clearly shows that the behavior of map (14) is very complicated, including the occurrence of chaos, which will be further investigated. It is also worth noting that the bifurcation diagram shows the presence of fixed points for a certain range of b parameter values. This case is a consequence of the mapping (14) intersecting the line $y = x$ (a similar situation occurs in the right graph of Figure 2). Another interesting phenomenon can also be observed from this diagram — anti-monotonicity, which occurs when the system follows the path of doubling the period and then switches to a path of halving the period.

As in the first example, using (3), the values of the Lyapunov exponent λ for map (14) were determined. Figure 8 shows the parameter space of the Lyapunov exponent obtained for map (14) with different parameter values. The black color in this graph represent parameter values for which the system has stable periodic behavior. The other colors, however, represent parameters which lead the system to chaos. Contrary to the first example, the region of parameters leading to chaotic behavior is formed by a large number (possibly infinite) of open sets, i.e., parameter regions of chaotic solutions are intertwined with regions of parameters leading to stable solutions. Moreover, the fractal nature of this figure can be observed. The periodic regions form a self-similar set of open sets, the so-called "shrimps" [40–42]. The left graph, as in the first example, is also symmetrical, which results from the form of mapping (14) and selected parameter values.



(a) $a = 0.4,\ b = 0.6,\ p = 0.5.$ (b) $a = 0.4,\ p = 0.5.$

Fig. 7: 3D phase diagram and bifurcation diagram of logistic maps of the form (14).



(a) $p = 0.5.$ (b) $p = 0.3.$

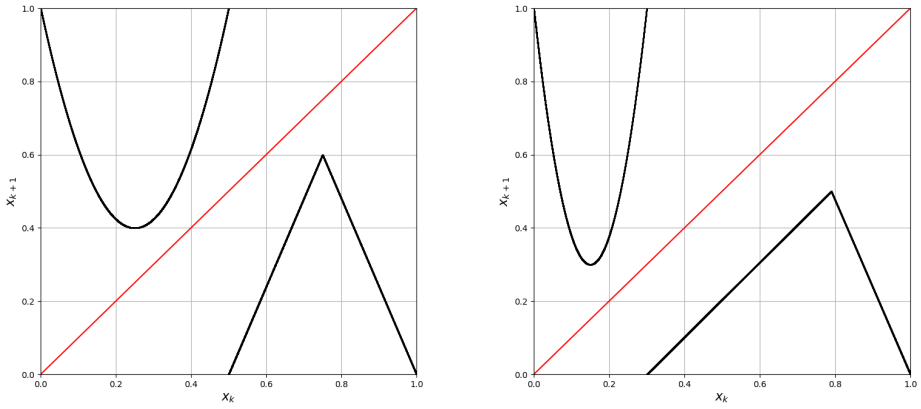
Fig. 8: Parameter spaces showing the Lyapunov exponent of logistic maps of the form (14).

4.3 Logistic-Tent map

As a next example, consider two different functions, f_1 and f_2, where f_1 is the logistic map function (13) and f_2 is the tent map function (10). Then the dynamic system (9) takes the form

$$x_{k+1} = \begin{cases} \frac{4(1-a)}{p^2}\left(x_k - \frac{p}{2}\right)^2 + a & 0 \le x \le p \\ \frac{b}{r(1-p)}(x_k - p) & p < x \le (1-p)r + p \\ \frac{b}{(1-r)(1-p)}(1 - x_k) & (1-p)r + p < x \le 1 \end{cases}, \tag{15}$$

The phase diagrams of the map (15) for fixed values of the parameters a, b, p and r are shown in Figure 9. Both maps shown are not symmetric. However, as the previous examples show, the maps do not have fixed points.

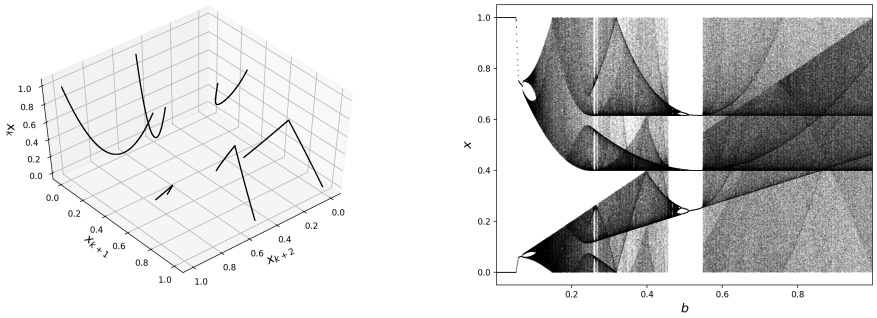


(a) $a = 0.4,\ b = 0.6,\ p = 0.5$ and $r = 0.5$. (b) $a = 0.3,\ b = 0.5,\ p = 0.3$ and $r = 0.7$.

Fig. 9: Phase diagrams of logistic-tent maps of the form (15).

In addition, like in the previous examples, 3d phase diagram in the relation (x_k, x_{k+1}, x_{k+2}) for selected parameter values was also determined. These results are presented in Figure 10a.

Furthermore, like in the previous examples, to better show the dynamics of the map (15), depending on the value of the b parameter, a bifurcation diagram was also determined, shown in Figure 10b. It clearly shows that the behavior of map (15) is very complicated, including the occurrence of chaos, which will be further investigated. Moreover, as in the first example, it can be observed that the transition to chaos from a two-period orbit does not take place by doubling the period. Therefore, also in this mapping there is the so-called crisis phenomenon.



(a) $a = 0.4,\ b = 0.6,\ p = 0.5$ and $r = 0.5$.

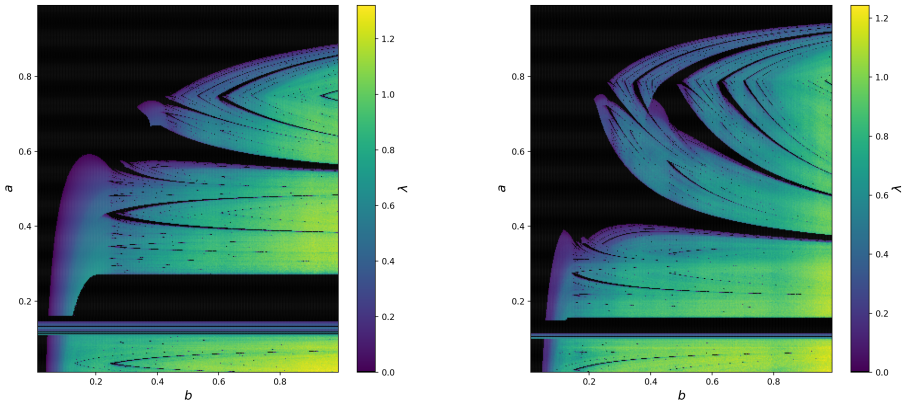
(b) $a = 0.4,\ p = 0.5$ and $r = 0.5$.

Fig. 10: 3D phase diagram and bifurcation diagram of logistic-tent maps of the form (15).

Also, in this example, using (3), the values of the Lyapunov exponent λ for map (15) were determined. Figure 11 shows the parameter space of the Lyapunov exponent obtained for map (15) with different parameter values. The black color in this graph represents parameter values for which the system has stable periodic behavior. The other colors, however, represent parameters which lead the system to chaos. Like in the second example, this parameter space is formed by a number of open sets for parameters that lead to chaos and periodicity. However, different from the shrimps observed in Figure 8, these open sets for the periodic regions seem to be formed along a single convex curve, contrasting the shrimps as in Figure 8 that appear on the "top" of a double set of convex curves. Moreover, the fractal nature of this figure can be observed.

5 Applications

The area where the proposed mappings can find many applications is chaotic cryptography. This type of cryptography uses chaotic mappings as the source of randomness to keep data secret. However, from the point of view of chaotic cryptography, the dynamic system should meet several assumptions, including, among others: a sufficiently large range of parameters and initial conditions for which chaos occurs and a reasonable computational cost of obtaining successive values from the dynamic system. The first criterion for the proposed mappings is met, which is proved by the presented analysis of the Lyapunov exponent. It is worth noting that compared to other dynamical systems, an example in equation (11) has much compact ranges of parameters for which chaos occurs. In addition, unlike other chaotic systems used in cryptography, such as logistic or tent mapping, the proposed mappings can have parameters set so to not have fixed points. So far, only some works in chaotic cryptography have addressed this problem of avoiding systems with fixed points. Finally, it is known that the parameter regions leading a nonlinear system to a fixed point are typically larger



(a) $p = 0.5, r = 0.5$.

(b) $p = 0.3, r = 0.7$.

Fig. 11: Parameter spaces showing the Lyapunov exponent of logistic-tent maps of the form (15).

than the parameter regions leading the same system to higher-period periodic orbits. This can be seen by the Feigenbaum rute to chaos, or by the homoclinic bifurcations [43]. By creating systems that have no fixed point, we are creating systems that can be set to chaos by smaller variations of parameters. Not only that, Figures 4b and 10b show that chaos in these systems appears without the period doubling route. A period 2 orbit looses stability giving rise to the chaotic attractor. All in all, systems with no fixed point enlarge the sets of parameters for which chaotic behavior can be observed. The second criterion means that the computational complexity of the mapping used is such that the computation time of the entire cryptographic system is reasonable. Meeting this criterion may be problematic for continuous systems, where at least three mathematical equations are needed to define the system and require appropriate numerical methods to determine successive values. In addition, one sees that the mappings proposed do not need to use complex mathematical operations.

5.1 PRBG

To illustrate the use of the proposed family of maps in applications, a Pseudo-Random Bit Generator (PRBG) will be designed. The proposed PRBG generates 15 bits per iteration, using the modulo operator for hashing, a transformation to binary representation, and an exclusive or (XOR) operation between the most and least significant bits of the binary hash.

Starting with a given map from the ones proposed, its key parameters and initial condition x_0 are set. Then, in each iteration k, 15 bits are generated from the state x_k of the map, using the following operations,

$$\mathcal{H}_k = \text{rem}\left(\lfloor 10^{12} x_k \rfloor, 2^{30}\right) \tag{16}$$
$$\mathcal{M}_k = \text{de2bi}(\mathcal{H}_k) \tag{17}$$
$$\mathcal{B}_k = \text{XOR}(\mathcal{M}_{k,1:15}, \mathcal{M}_{k,16:30}) \tag{18}$$

were $\lfloor \cdot \rfloor$ denotes the highest integer smaller than its argument, which for positive numbers equals to the integer part of the argument, rem$(\cdot, 2^{30})$ denotes the remainder of division by 2^{30}, de2bi$(\cdot)$ denotes the decimal to binary conversion, and XOR$(\cdot, \cdot)$ denotes the element-wise exclusive OR operation. The de2bi$(\cdot)$ function constitutes a blowup operation, where a single number is transformed into a sequence of 15 bits. Whereas such operation applied directly to the chaotic trajectory would generate strongly correlated binary sequences, the rem$(\cdot, 2^{30})$ operation in (16) is responsible to decorrelate x_k from x_{k-1}. The benefit is obvious, to increase the binary key length. Then, the XOR operation is dedicated to ensure no correlation is present between each block of 15 bits, basically providing the mixing step of the encryption. The notation $a : b$ denotes the elements of a vector in positions $a, a+1, ..., b$, following the notation common to MATLAB. So in each iteration, the value of the chaotic map x_k is multiplied by 10^{12} and its integer part is divided by 2^{30}. The remainder of the division $\mathcal{H}_k$ is an integer in the interval $[0, 2^{30} - 1]$. This integer is then transformed into its binary representation $\mathcal{M}_k$, which has a fixed length of 30 bits. Finally, an exclusive OR operation is performed between the first 15 bits, and the last 15 bits of $\mathcal{M}_k$. So (18) denotes the exclusive or operations XOR$(\mathcal{M}_{k,1}, \mathcal{M}_{k,16})$, XOR$(\mathcal{M}_{k,2}, \mathcal{M}_{k,17})$, ..., XOR$(\mathcal{M}_{k,15}, \mathcal{M}_{k,30})$. The final vector $\mathcal{B}_k$ has a length of 15 bits, which is the output of the PRBG for the k-th iteration. The resulting bitstream is obtained by appending all $\mathcal{B}_k$, as

$$\textbf{Bitstream} = \{\mathcal{B}_1, \mathcal{B}_2, ...\} \tag{19}$$

Since 15 bits are generated per iteration, if a bitstream of length N is required, the chaotic map used must be iterated $k = 1, ..., \lceil \frac{N}{15} \rceil$ times, where $\lceil \cdot \rceil$ denotes the smallest integer higher than its argument.

The PRBG is tested using all three maps (11), (14), (15) as chaotic sources. For each map, a set of 1000 bitstreams of length 10^6 are generated, for random initial condition x_0. This results in an appended bitstream of length 10^9 for each map. The parameters are chosen as $a = 0.4$, $b = 0.6$, $p = 0.5$, $r = 0.5$, for (11), $a = 0.3$, $b = 0.5$, $p = 0.3$, for (14), and $a = 0.3$, $b = 0.7$, $p = 0.3$, $r = 0.7$, for (15). The bitstreams are tested through the National Institute of Standards and Technology (NIST) statistical test suite [44]. This is a common statistical package used to verify if a bitstream can be considered statistically similar to a random sequence, with respect to 15 statistical tests. The tests were performed using their default parameter values. The results are shown in Table 1, and are all positive, meaning that the PRBGs pass all the statistical tests. Thus, the proposed PRBG using the maps developed in the previous section can be a viable option for use in applications relevant to randomness or security.

Finally, Table 2 lists the number of operations required per iteration of the PRBG, as well as the ratio of operations required for a single bit. The number 10^{12} can be precomputed when the PRBG is initialized, and thus is not counted as an additional

Table 1: NIST test results for the proposed PRBG using different maps.

		Map (11)		Map (14)		Map (15)	
No.	**Test**	Ratio	Result	Ratio	Result	Ratio	Result
1	Frequency	993/1000	Pass	989/1000	Pass	988/1000	Pass
2	BlockFrequency	987/1000	Pass	987/1000	Pass	989/1000	Pass
3	CumulativeSums	993/1000	Pass	985/1000	Pass	990/1000	Pass
4	Runs	997/1000	Pass	990/1000	Pass	990/1000	Pass
5	LongestRun	993/1000	Pass	985/1000	Pass	988/1000	Pass
6	Rank	992/1000	Pass	989/1000	Pass	985/1000	Pass
7	FFT	988/1000	Pass	989/1000	Pass	986/1000	Pass
8	NonOverlappingTemplate	990/1000	Pass	988/1000	Pass	989/1000	Pass
9	OverlappingTemplate	986/1000	Pass	989/1000	Pass	987/1000	Pass
10	Universal	990/1000	Pass	987/1000	Pass	988/1000	Pass
11	ApproximateEntropy	989/1000	Pass	986/1000	Pass	994/1000	Pass
12	RandomExcursions	600/609	Pass	606/612	Pass	618/628	Pass
13	RandomExcursionsVariant	603/609	Pass	600/612	Pass	623/628	Pass
14	Serial	991/1000	Pass	989/1000	Pass	993/1000	Pass
15	LinearComplexity	983/1000	Pass	989/1000	Pass	990/1000	Pass

operation. The ratio is 1.27 operations per bit, so around a 30% increase compared to the minimum of 1 operation per bit. Of course, the operations listed all have different complexities, and their execution time is dependent upon the hardware and software used. So this ratio should only be viewed as an index of good balance for the number of operations required per bit, but not as a solid indicator of fast performance, as this would be affected by other implementation parameters. Note that the Table 2 only lists the operations required to generate the bits, after x_k is obtained, so the ratio of 1.27 does not count the operations required to compute the map's value, as different maps can be considered as a source of the PRBG.

Table 2: Number of operations required for a single iteration of the PRBG.

Operation	**Total**
Multiplication	1
$\lfloor \cdot \rfloor$	1
$\mathrm{rem}(\cdot, 2^{30})$	1
$\mathrm{de2bi}(\cdot)$	1
$\mathrm{XOR}(\cdot, \cdot)$	15
Overall	19
Per Bit	$\frac{19}{15} \approx 1.27$

6 Conclusions

In this work, families of piecewise maps without equilibria were proposed. The maps were based on the logistic and tent classic maps, and their phase portraits consisted of two pieces of different curvatures, and thus a single discontinuity, so that no intersections with the bisection appeared. The numerical analysis of their behavior revealed wide chaotic ranges, as well as periodic regions with self-similar patterns, commonly referred to as "shrimps". Other phenomena were also observed, like crisis, antimonotonicity, and a period doubling route to chaos. So overall, the maps exhibited rich dynamics. The maps were also successfully applied to the design of a PRBG that can generate 15 bits per iteration, by mixing the most and least significant bits of a modulo based hash value.

From the numerous bifurcation and Lyapunov exponent diagrams, it can be seen that the proposed maps do indeed showcase compact and predominant areas of chaotic behavior in the space parameters. Still, there are periodic windows of period-2 or higher appearing, but typically the parameter regions leading to those orbits are smaller than the regions of parameters that would lead to a fixed point. In future studies, it is of interest to design maps that will have no N-periodic behavior appearing. To design such maps, one has to consider the absence of intersections with the bisector for all the N-level compositions of the map with itself. This task is more complex to the one considered here, and in previous works that design no-equilibria maps was not significantly analyzed. One way to approach this problem would be to consider nonlinear functions with curves that are easily tunable, like exponential and sinusoidal functions. This task is currently under study by our research group.

Acknowledgments. The authors are thankful to the anonymous reviewers for their constructive feedback.

Declarations

Funding: The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.
Competing Interests: The authors have no relevant financial or non-financial interests to disclose.
Author Contributions: Conceptualization: Marcin Lawnik and Lazaros Moysis; Methodology: Marcin Lawnik; Software: Marcin Lawnik and Lazaros Moysis; Visualization: Marcin Lawnik; Writing—original draft preparation: Marcin Lawnik and Lazaros Moysis; Writing—review and editing: Marcin Lawnik, Lazaros Moysis, Murilo S. Baptista and Christos Volos; Supervision: Murilo S. Baptista and Christos Volos.
Data Availability: Not applicable

References

[1] Strogatz, S.H.: Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering. CRC Press, Boca Raton (2018)

[2] Berezowski, M., Dubaj, D.: Chaotic oscillations of coupled chemical reactors. Chaos, Solitons and Fractals **78**, 22–25 (2015) https://doi.org/10.1016/j.chaos.2015.07.001

[3] Foley, D.: In: Lines, M. (ed.) Complex and Chaotic Dynamics in Economics, pp. 27–66. Springer, Vienna (2005). https://doi.org/10.1007/3-211-38043-4_2

[4] Skinner, J.E., Molnar, M., Vybiral, T., Mitra, M.: Application of chaos theory to biology and medicine. Integr Physiol Behav Sci **27**(1), 39–53 (1992)

[5] Lawnik, M., Moysis, L., Volos, C.: Chaos-based cryptography: Text encryption using image algorithms. Electronics **11**(19) (2022) https://doi.org/10.3390/electronics11193156

[6] Zhang, B., Liu, L.: Chaos-based image encryption: Review, application, and challenges. Mathematics **11**(11) (2023) https://doi.org/10.3390/math11112585

[7] Wu, R., Gao, S., Wang, X., Liu, S., Li, Q., Erkan, U., Tang, X.: Aea-ncs: An audio encryption algorithm based on a nested chaotic system. Chaos, Solitons & Fractals **165**, 112770 (2022) https://doi.org/10.1016/j.chaos.2022.112770

[8] Su, Z., Lian, S., Zhang, G., Jiang, J.: In: Kocarev, L., Lian, S. (eds.) Chaos-Based Video Encryption Algorithms, pp. 205–226. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20542-2_6

[9] Alawida, M., Teh, J.S., Oyinloye, D.P., Alshoura, W.H., Ahmad, M., Alkhawaldeh, R.S.: A new hash function based on chaotic maps and deterministic finite state automata. IEEE Access **8**, 113163–113174 (2020) https://doi.org/10.1109/ACCESS.2020.3002763

[10] Bin Faheem, Z., Ali, A., Khan, M.A., Ul-Haq, M.E., Ahmad, W.: Highly dispersive substitution box (s-box) design using chaos. ETRI Journal **42**(4), 619–632 (2020) https://doi.org/10.4218/etrij.2019-0138

[11] Ye, G., Jiao, K., Wu, H., Pan, C., Huang, X.: An asymmetric image encryption algorithm based on a fractional-order chaotic system and the rsa public-key cryptosystem. International Journal of Bifurcation and Chaos **30**(15), 2050233 (2020) https://doi.org/10.1142/S0218127420502338

[12] Nasr, S., Mekki, H., Bouallegue, K.: A multi-scroll chaotic system for a higher coverage path planning of a mobile robot using flatness controller. Chaos, Solitons & Fractals **118**, 366–375 (2019) https://doi.org/10.1016/j.chaos.2018.12.002

[13] Feng, J., Zhang, J., Zhu, X., Lian, W.: A novel chaos optimization algorithm. Multimedia Tools and Applications **76**(16), 17405–17436 (2017) https://doi.org/10.1007/s11042-016-3907-z

[14] Wang, R., Du, P., Zhong, W., Han, H., Sun, H.: Analyses and encryption implementation of a new chaotic system based on semitensor product. Complexity **2020** (2020) https://doi.org/10.1155/2020/1230804

[15] Liang, B., Hu, C., Tian, Z., Wang, Q., Jian, C.: A 3d chaotic system with multi-transient behavior and its application in image encryption. Physica A: Statistical Mechanics and its Applications **616**, 128624 (2023) https://doi.org/10.1016/j.physa.2023.128624

[16] Guo, Y., Zhang, J., Xie, Q., Hou, J.: Multi-vortex hyperchaotic systems based on memristors and their application to image encryption. Optik **287**, 171119 (2023) https://doi.org/10.1016/j.ijleo.2023.171119

[17] Xu, S., Wang, X., Ye, X.: A new fractional-order chaos system of hopfield neural network and its application in image encryption. Chaos, Solitons & Fractals **157**, 111889 (2022) https://doi.org/10.1016/j.chaos.2022.111889

[18] Hosny, K.M., Kamal, S.T., Darwish, M.M.: Novel encryption for color images using fractional-order hyperchaotic system. Journal of Ambient Intelligence and Humanized Computing **13**(2), 973–988 (2022) https://doi.org/10.1007/s12652-021-03675-y

[19] Khan, N.A., Qureshi, M.A., Akbar, S., Ara, A.: From chaos to encryption using fractional order lorenz-stenflo model with flux-controlled feedback memristor. Physica Scripta **98**(1), 014002 (2022) https://doi.org/10.1088/1402-4896/aca1e8

[20] Lin, L., Zhuang, Y., Xu, Z., Yang, D., Wu, D.: Encryption algorithm based on fractional order chaotic system combined with adaptive predefined time synchronization. Frontiers in Physics **11** (2023) https://doi.org/10.3389/fphy.2023.1202871

[21] Khairullah, M.K., Alkahtani, A.A., Bin Baharuddin, M.Z., Al-Jubari, A.M.: Designing 1d chaotic maps for fast chaotic image encryption. Electronics **10**(17) (2021) https://doi.org/10.3390/electronics10172116

[22] Dua, M., Makhija, D., Manasa, P.Y.L., Mishra, P.: 3d chaotic map-cosine transformation based approach to video encryption and decryption. Open Computer Science **12**(1), 37–56 (2022) https://doi.org/10.1515/comp-2020-0225

[23] Liang, Q., Zhu, C.: A new one-dimensional chaotic map for image encryption scheme based on random dna coding. Optics & Laser Technology **160**, 109033 (2023) https://doi.org/10.1016/j.optlastec.2022.109033

[24] Azar, A.T., Volos, C., Gerodimos, N.A., Tombras, G.S., Pham, V.-T., Radwan, A.G., Vaidyanathan, S., Ouannas, A., Munoz-Pacheco, J.M.: A novel chaotic system without equilibrium: Dynamics, synchronization, and circuit realization. Complexity **2017**, 7871467 (2017) https://doi.org/10.1155/2017/7871467

[25] Wang, Z., Akgul, A., Pham, V.-T., Jafari, S.: Chaos-based application of a novel no-equilibrium chaotic system with coexisting attractors. Nonlinear Dynamics **89**(3), 1877–1887 (2017) https://doi.org/10.1007/s11071-017-3558-2

[26] Tamba, V.K., Pham, V.-T., Hoang, D.V., Jafari, S., Alsaadi, F.E., Alsaadi, F.E.: Dynamic system with no equilibrium and its chaos anti-synchronization. Automatika **59**(1), 35–42 (2018) https://doi.org/10.1080/00051144.2018.1491934

[27] Lai, Q., Wan, Z., Kamdem Kuate, P.D.: Modelling and circuit realisation of a new no-equilibrium chaotic system with hidden attractor and coexisting attractors. Electronics Letters **56**(20), 1044–1046 (2020) https://doi.org/10.1049/el.2020.1630

[28] Zhang, S., Wang, X., Zeng, Z.: A simple no-equilibrium chaotic system with only one signum function for generating multidirectional variable hidden attractors and its hardware implementation. Chaos: An Interdisciplinary Journal of Nonlinear Science **30**(5), 053129 (2020) https://doi.org/10.1063/5.0008875

[29] Wang, X., Chen, G.: In: Wang, X., Kuznetsov, N.V., Chen, G. (eds.) Chaotic Systems With Equilibria, pp. 55–75. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-75821-9_4

[30] Wang, C., Ding, Q.: A new two-dimensional map with hidden attractors. Entropy **20**(5) (2018) https://doi.org/10.3390/e20050322

[31] Almatroud, O.A., Pham, V.-T.: Building fixed point-free maps with memristor. Mathematics **11**(6) (2023) https://doi.org/10.3390/math11061319

[32] García-Grimaldo, C., Campos-Cantón, E.: Comparative analysis of chaotic features of maps without fixed points. In: Huerta Cuéllar, G., Campos Cantón, E., Tlelo-Cuautle, E. (eds.) Complex Systems and Their Applications, pp. 151–176. Springer, Cham (2022)

[33] García-Grimaldo, C., Bermudez-Marquez, C.F., Tlelo-Cuautle, E., Campos-Cantón, E.: Fpga implementation of a chaotic map with no fixed point. Electronics **12**(2) (2023) https://doi.org/10.3390/electronics12020444

[34] García-Grimaldo, C., Campos, E.: Chaotic features of a class of discrete maps without fixed points. International Journal of Bifurcation and Chaos **31**(13), 2150200 (2021) https://doi.org/10.1142/S021812742150200X

[35] Jafari, S., Pham, V.-T., Golpayegani, S.M.R.H., Moghtadaei, M., Kingni, S.T.: The relationship between chaotic maps and some chaotic systems with hidden attractors. International Journal of Bifurcation and Chaos **26**(13), 1650211 (2016)

[36] García-Grimaldo, C., Campos-Cantón, E.: One-dimensional map without fixed

points and with amplitude control. In: 15th Chaotic Modeling and Simulation International Conference, pp. 87–97 (2022). Springer

[37] García-Grimaldo, C., Campos-Cantón, E.: Exploring a family of bernoulli-like shift chaotic maps and its amplitude control. Chaos, Solitons & Fractals **175**, 113951 (2023) https://doi.org/10.1016/j.chaos.2023.113951

[38] Berezowski, M., Lawnik, M.: Hidden attractors in discrete dynamical systems. Entropy **23**(5) (2021) https://doi.org/10.3390/e23050616

[39] Lawnik, M., Moysis, L., Volos, C.: A family of 1d chaotic maps without equilibria. Symmetry **15**(7) (2023) https://doi.org/10.3390/sym15071311

[40] Baptista, M.S., Grebogi, C., Barreto, E.: Topology of windows in the high-dimensional parameter space of chaotic maps. International Journal of Bifurcation and Chaos **13**(09), 2681–2688 (2003) https://doi.org/10.1142/S0218127403008181

[41] Sousa, F.F.G., Rubinger, R.M., Sartorelli, J.C., Albuquerque, H.A., Baptista, M.S.: Parameter space of experimental chaotic circuits with high-precision control parameters. Chaos: An Interdisciplinary Journal of Nonlinear Science **26**(8), 083107 (2016) https://doi.org/10.1063/1.4960582

[42] Maranhão, D.M., Baptista, M.S., Sartorelli, J.C., Caldas, I.L.: Experimental observation of a complex periodic window. Phys. Rev. E **77**, 037202 (2008) https://doi.org/10.1103/PhysRevE.77.037202

[43] Fowler, A., McGuinness, M.: Homoclinic Bifurcations, pp. 99–142. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32538-1_4

[44] 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 (2001)