

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

COMPLEXITY LEADS TO RANDOMNESS IN CHAOTIC SYSTEMS

RENÉ LOZI

Laboratory J. A. Dieudonné, UMR CNRS 6621, University of Nice Sophia-Antipolis, Parc Valrose, 06108 Nice Cedex 02, France

and

Institut Universitaire de Formation des Maîtres Célestin Freinet-académie de Nice, University of Nice-Sophia-Antipolis, 89 avenue George V, 06046 Nice Cedex 1, France

Abstract— Complexity of a particular coordinated system is the degree of difficulty in predicting the properties of the system if the properties of the system's correlated parts are given. The coordinated system manifests properties not carried by individual parts. The subject system can be said to emerge without any "guiding hand". In systems theory and science, emergence is the way complex systems and patterns arise out of a multiplicity of relatively simple interactions. Emergence is central to the theories of integrative levels and of complex systems. The emergent property of the ultra weak multidimensional coupling of p 1-dimensional dynamical chaotic systems for which complexity leads from chaos to randomness has been recently pointed out.

Pseudorandom or chaotic numbers are nowadays used in many areas of contemporary technology such as modern communication systems and engineering applications. Efficient Chaotic Pseudo Random Number Generators (CPRNG) have been recently introduced. They use the ultra weak multidimensional coupling of p 1-dimensional dynamical systems which preserves the chaotic properties of the continuous models in numerical experiments. Together with chaotic sampling and mixing processes, the complexity of ultra weak coupling leads to families of CPRNG which are noteworthy. In this paper we improve again these families using a double threshold chaotic sampling instead of a single one. A window of emergence of randomness for some parameter value is numerically displayed. Moreover we emphasize that a determining property of such improved CPRNG is the high number of parameters used and the high sensitivity to the parameters value which allows choosing it as cipher-keys.

1. Introduction

Characterizing complexity is not easy and there are in science a number of approaches to do it. Many definitions tend to postulate or assume that complexity expresses a condition of numerous elements in a system and numerous forms of relationships among the elements. Some others definitions relate to the algorithmic basis for the expression of a complex phenomenon or model or mathematical



Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011)* pp. 93-125.

expression. Warren Weaver [1] has posited that the (organized) complexity of a particular system is the degree of difficulty in predicting the properties of the system if the properties of the system's parts are given. In Weaver's view organized complexity, resides in nothing else than the non-random, or correlated, interaction between the parts. These correlated relationships create a differentiated structure which can, as a system, interact with other systems. The coordinated system manifests properties not carried by individual parts. The organized aspect of this form of complexity versus other systems than the subject system can be said to emerge without any "guiding hand". The number of parts does not have to be very large for a particular system to have emergent properties.

In systems theory and science, emergence is the way complex systems and patterns arise out of a multiplicity of relatively simple interactions. Emergence is central to the theories of integrative levels and of complex systems (M. A. Aziz-Alaoui *et al.* [2]).

In this paper we use the emergent property of the ultra weak multidimensional coupling of p 1-dimensional dynamical chaotic systems for which complexity leads from chaos to randomness. Efficient Chaotic Pseudo Random Number Generators (CPRNG) have been recently introduced (Lozi [3, 4, 5, 6]) and their properties analyzed (Hénaff *et al.* [7, 8, 9, 10]). The idea of applying discrete chaotic dynamical systems, intrinsically, exploits the property of extreme sensitivity of trajectories to small changes of initial conditions. The ultra weak multidimensional coupling of p 1-dimensional dynamical systems preserves the chaotic properties of the continuous models in numerical experiments. The process of chaotic sampling and mixing of chaotic sequences, which is pivotal for these families, works perfectly in numerical simulation when floating point (or any multi-precision) numbers are handled by a computer.

It is noteworthy that these families of ultra weakly coupled maps are more powerful than the usual formulas used to generate chaotic sequences mainly because only additions and multiplications are used in the computation process; no division being required. Moreover the computations are done using floating point or double precision numbers, allowing the use of the powerful Floating Point Unit (FPU) of the modern microprocessors (built by both Intel and Advanced Micro Devices (AMD)). In addition, a large part of the computations can be parallelized taking advantage of the multicore microprocessors which appear on the market of laptop computers.

In this paper we improve the properties of these families using a double threshold chaotic sampling instead of a single one. The genuine map f used as one-dimensional dynamical systems to generate them is henceforth perfectly

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

hidden. A window of emergence of randomness for some parameter value is numerically displayed.

A determining property of such improved CPRNG is the high number of parameters used ($p \times (p-1)$ for p coupled equations) which allows to choose it as cipher-keys due to the high sensitivity to the parameters values. We call these families multi-parameter chaotic pseudo-random number generators (M-p CPRNG).

Several applications can be found for these families as for example producing Gaussian noise, computing hash function or in chaotic cryptography.

In Sec. 2 we review some of the most popular chaotic mappings in low dimension in the scope of their use in numerical algorithms and PRNG.

In Sec. 3 we improve the properties of ultra weak multidimensional coupled of p 1-dimensional dynamical chaotic systems using a double threshold chaotic sampling instead of a single one.

In Sec. 4 we describe the emergence of randomness from complexity in a particular window of parameter value. We point out the parameter sensitivity in Sec. 5, with some applications of the M-p CPRNG and we give a conclusion in Sec. 6.

2. Discrete Dynamical Systems in Low Dimension

Chaotic dynamical systems in low dimension are often used since their discovery in the 70' in order to generate chaotic numbers, because they are very easy to implement in numerical algorithms [11]. However, as we point out in this section the computation of numerical approximation of their periodic orbits leads to very different results from the theoretical ones. Then they are unable to generate Pseudo Random Numbers (PRN). We review some of the most used maps in dimension from 1 to 3 in this scope.

2.1. 1-Dimensional Chaotic Dynamical Systems

2.1.1. Logistic map

The very well known logistic map $g_a : [0, 1] \rightarrow [0, 1]$ is simply defined as

$$g_a(x) = ax(1-x) \quad (1)$$

and generally considered for $a \in [0, 4]$ (see Fig. 1). It is associated to the discrete dynamical system [12]

$$x_{n+1} = g_a(x_n) \quad (2)$$

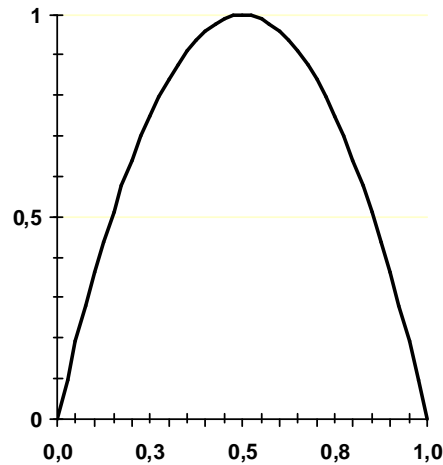


Figure 1. Graph of the logistic map for $a = 4$.

This dynamical system which has excellent ergodic properties on the real interval $[0, 1]$ has been extensively studied especially by R. M. May [13], and J. Feigenbaum [14] who introduced what is now called the Feigenbaum's constant $\delta = 4.66920160910299067185320382\dots$ explaining by a new theory (period doubling bifurcation) the onset of chaos.

For every value of a there exist two fixed points: $x = 0$ which is always unstable and $x = \frac{a-1}{a}$ which is stable for $a \in]1, 3[$ and unstable for $a \in]0, 1[\cup]1, 4[$.

When $a = 4$, the system is chaotic. The set $\left\{ \frac{5-\sqrt{5}}{8}, \frac{5+\sqrt{5}}{8} \right\} = \{0.3454915028, 0.9045084972\}$ is the period-2 orbit. In fact there exist infinity of periodic orbits and infinity of periods. This dynamical system possesses an invariant measure $P(x) = \frac{1}{\pi\sqrt{x(1-x)}}$ (see Fig. 2).

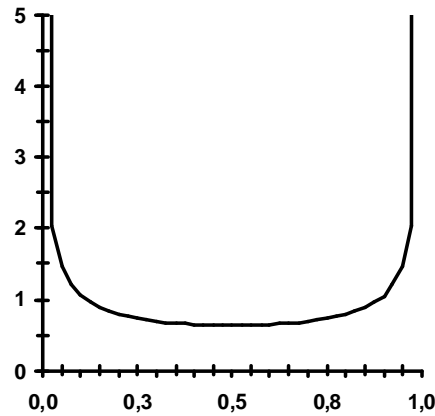


Figure 2. Graph of the invariant measure $P(x)$ of the logistic map for $a = 4$.

2.1.2. Numerical approximation of the logistic map

In order to compute longer periodic orbits the use of computer is required, as it is equivalent to find roots of polynomial equation of degree greater than 4 for which Galois theory teaches that no closed formula is available. However, numerical computation uses ordinarily double precision numbers (IEEE-754) so that the working interval contains roughly 10^{16} representable points. Doing such a computation in Eq. (2) with 1,000 randomly chosen initial guesses, 596, *i.e.*, the majority, converge to the unstable fixed point $x = 0$, and 404 converge to a cycle of period 15,784,521. (see Table 1) [15].

Table 1. Coexisting periodic orbits found using 1,000 random initial points for double precision numbers

Period	Orbit	Relative Basin size
1	$x = 0$ unstable fixed point	596 over 1,000
15,784,521	Scattered over the interval	404 over 1,000

Thus, in this case at least, the very long-term behaviour of numerical orbits is, for a substantial fraction of initial points, in flagrant disagreement with the true behaviour of typical orbits of the original smooth logistic map.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

In others numerical experiments we have performed, the computer working with fixed finite precision is able to represent finitely many points in the interval in question. It is probably good, for purposes of orientation, to think of the case where the representable points are uniformly spaced in the interval. The true logistic map is then approximated by a discretized map, sending the finite set of representable points in the interval to itself.

Describing the discretized mapping exactly is usually complicated, but it is roughly the mapping obtained by applying the exact smooth mapping to each of the discrete representable points and "rounding" the result to the nearest representable point. In our experiments [16, 17], uniformly spaced points in the interval with several order of discretization (ranging from 9 to 2,001 points) are involved, the results for 2,000 and 2,001 points are displayed in Table 2. In each experiment the questions addressed are:

- how many periodic cycles are there and what are their periods ?
- how large are their respective basins of attraction, *i.e.* , for each periodic cycle, how many initial points give orbits with eventually land on the cycle in question ?

Table 2. Coexisting periodic orbits for the discretization with regular meshes of $N = 2,000$ and $2,001$ points.

N	Period	Orbit	Relative Basin Size
2,000	1	{0}	2 over 2,000
2,000	2	{1,499}	14 over 2,000
2,000	2	{691;1,808}	138 over 2,000
2,000	3	{276;1,221;1,900}	6 over 2,000
2,000	8	{3;11;43;168;615;1,703.1,008.1,998}	1,840 over 2,000
2,001	1	{0}	5 over 2,001
2,001	1	{1500}	34 over 2,001
2,001	2	{91; 1809}	92 over 2,001
2,001	8	{3;11;43;168;615;1,703;1,011;1,999}	608 over 2,001
2,001	18	{35;137;510;1,519;1,461;1,574;...}	263 over 2,001
2,001	25	{27;106;401;1,282;1,840;588;...}	1,262 over 2,001

The existence of very short periodic orbit (see Table 1), the existence of a non constant invariant measure (see Fig. 2) and the easily recognized shape of the function in the phase space (x_n, x_{n+1}) avoid the use of the logistic map as a PRN generator. However, its very simple implementation in computer program led some authors to use it as a base of cryptosystem [18, 19].

2.1.3. Symmetric tent map

Another often studied dynamical system is defined by the symmetric tent map on the interval $J = [-1, 1]$, $f_a : J \rightarrow J$

$$f_a(x) = 1 - a|x| \quad (3)$$

$$x_{n+1} = f_a(x_n) \quad (4)$$

Despite its simple shape (see Fig. 3), it has several interesting properties. First, when the parameter value $a = 2$, the system possesses chaotic orbits. Because of its piecewise-linear structure, it is easy to find those orbits explicitly. More, owing to its simple definition, the symmetric tent map's shape under iteration is very well understood. The invariant measure is the Lebesgue measure. Finally, and perhaps the most important, the tent map is conjugate to the logistic map, which in turn is conjugate to the Hénon map for small values of b [12].

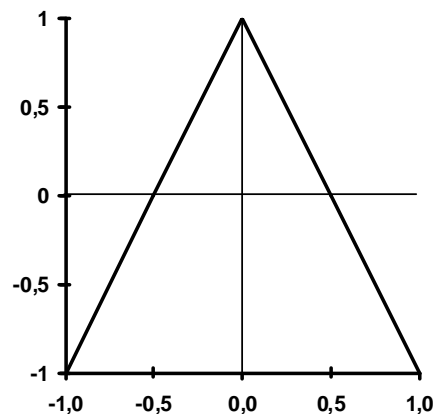


Figure 3. Graph of the symmetric tent map on J for $a = 2$.

However the symmetric tent map is dramatically numerically unstable: Sharkovskii's theorem applies for it [20]. When $a = 2$ there exists a period three orbit, which implies that there is infinity of periodic orbits. Nevertheless the orbit of almost every point of the interval J of the discretized tent map converges to the (unstable) fixed point $x = -1$ (this is due to the binary structure of floating points) and there is no numerical attracting periodic orbit [11].

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

The numerical behaviour of iterates with respect to chaos is worse than the numerical behaviour of iterates of the approximated logistic map. This is why the tent map is never used to generate numerically chaotic numbers. However in Sec. 3 we will show that it is possible to preserve its chaotic properties when several logistic maps are ultra weakly coupled.

2.2. 2-Dimensional System Chaotic Dynamical Systems

2.2.1. Hénon map

In order to study numerically the properties of the Lorenz attractor [11], M. Hénon in 1976 [21] introduced a simplified model of the Poincaré map [12] of this attractor. The Lorenz attractor being in dimension 3, the corresponding Poincaré map is a map from \mathbb{R}^2 to \mathbb{R}^2 . The Hénon map is then also defined in dimension 2 as

$$F : \begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} y + 1 - ax^2 \\ bx \end{pmatrix} \quad (5)$$

It is associated to the dynamical system

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \quad (6)$$

For the parameter value $a = 1.4$, $b = 0.3$ Hénon pointed out numerically that there exists an attractor with fractal structure (see Fig. 4). This was the first example of strange attractor (previously introduced by D. Ruelle and F. Takens [22]) for a mapping defined by an analytic formula.

Nowadays hundreds of research papers have been published on this prototypical map in order to fully understand its innermost structure. However as in dimension 1, there is a discrepancy between the mathematical properties of this map in the plane \mathbb{R}^2 and the numerical computations done using (IEEE-754) double precision numbers.

If we call Megaperiodic orbits [23], those whose length of the period belongs to the interval of natural numbers $[10^6, 10^9[$ and Gigaperiodic orbits, those whose length of the period belongs to the interval $[10^9, 10^{12}[$, Hénon map possesses Gigaperiodic orbits. On a Dell computer with a Pentium IV microprocessor running at the frequency of 1.5 Gigahertz, using a Borland C compiler and computing with ordinary (IEEE-754) double precision numbers, one can find for $a = 1.4$ and $b = 0.3$ one attracting period of length 3,800,716,788

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

i.e. two hundred forty times longer than the longest period of the one-dimensional logistic map (see Table 1).

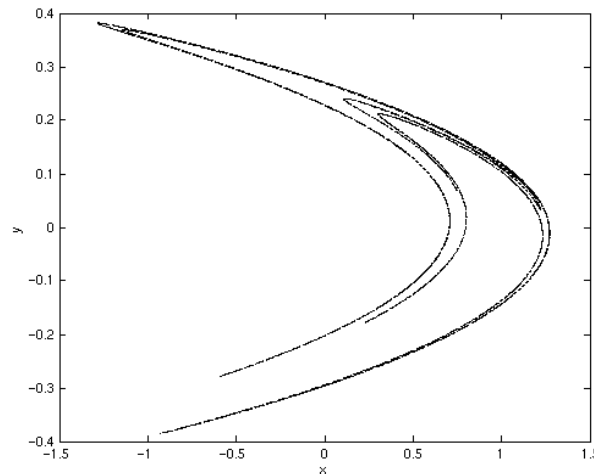


Figure 4. The strange attractor of the Hénon map for $a = 1.4$ and $b = 0.3$.

This periodic orbit (we call it here Orbit 1) is numerically slowly attracting. Starting with the initial value

$$(x_0, y_0)_1 = (-0.35766, 0.14722356) \text{ one obtains:}$$

$$(x_{11,574,730,767}, y_{11,574,730,767})_1 = (x_{15,375,447,555}, y_{15,375,447,555})_1 \\ = (1.27297361350955662, -0.0115735710153616837)$$

The length of the period is obtained subtracting

$$15,375,447,555 - 11,574,730,767 = 3,800,716,788.$$

However this periodic orbit is not unique: starting with the initial value

$(x_0, y_0)_2 = (0.4725166, 0.25112222222356)$ the following periodic orbit (which is a Megaperiodic orbit of period 310,946,608 (Orbit 2)) is computed.

$$(x_{12,935,492,515}, y_{12,935,492,515})_2 = (x_{13,246,439,123}, y_{13,246,439,123})_2 \\ = (1.27297361350865113, -0.0115734779561870744)$$

This orbit can be reached more rapidly starting from the other initial value

$$(x_0, y_0) = (0.88187775591, 0.0000322222356), \text{ then}$$

$$(x_{4,459,790,707}, y_{4,459,790,707}) = (1.27297361350865113, -0.0115734779561870744).$$

It is possible that some others periodic orbits coexist with both Orbit 1 and Orbit 2.

The comparison between Orbit 1 and Orbit 2 gives a perfect idea of the sensitive dependence on initial conditions of chaotic attractors: Orbit 1 passes

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

through the point (**1.27297361350955662**, – **0.0115735710153616837**) and Orbit 2 passes through the point (**1.27297361350865113**, – **0.0115734779561870744**). The same digits of these points are bold printed, they are very close.

Nevertheless, as displayed in Fig. 4 the orbit are not uniformly distributed on the phase space, then it is not possible to use this map as a PRN generator.

Beside the problem of PRN generator, logistic and Hénon maps are recently used together with a secret key, by N. Pareek *et al.* [24], in order to build a chaotic block cipher which is extremely robust, due to the excellent confusion and diffusion properties of these maps. The results of the statistical analysis show that the chaotic cipher possesses all features needed for a secure system and useable for the security of communication system.

L. dos Santos Coelho *et al.* [25], introduced a chaotic particle swarm optimisation (PSO) which is a population-based swarm intelligence algorithm driven by the stimulation of a social psychological metaphor instead of the survival of the fittest individual. Based on the chaotic systems theory (using Hénon map sequences which increase its convergence rate and resulting precision) the novel PSO combined with an implicit filtering allows solving economic dispatch problems.

2.2.2. Lozi map

The Lozi map [26] is a linearized version of the Hénon map, built in order to simplify the computations, mainly because it is possible to compute explicitly any periodic orbits solving a linear system. It is defined as

$$\begin{cases} x_{n+1} = y_n + 1 - a|x_n| \\ y_{n+1} = bx_n \end{cases} \quad (7)$$

or equivalently

$$x_{n+1} = 1 - a|x_n| + bx_{n-1} \quad (8)$$

For $a = 1.7$ and $b = 0.5$ there exists a strange attractor. The particularity of this strange attractor is that it has been rigorously proved by Misiurewicz in 1980 [27].

In the same conditions of computation as for Hénon map, running the computation during nineteen hours, one can find a Gigaperiodic attracting orbit of period 436,170,188,959 more than one hundred times longer than the period of Orbit 1 found for the Hénon map.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

Starting with $(x_0, y_0) = (0.88187777591, 0.0000322222356)$ one obtains

$$\begin{aligned} (x_{686,295,403,186}, y_{686,295,403,186}) &= (x_{250,125,214,227}, y_{250,125,214,227}) \\ &= (1.34348444450739479, -2.07670041497986548 \cdot 10^{-7}). \end{aligned}$$

There is a transient regime before the orbit is reached. It seems that there is no periodic orbit with a smaller length. This could be due to the quasihyperbolic nature of the attractor. However, the orbit-shifted shadowing property of Lozi map (and generalized Lozi map), which is the property which ensures that pseudo-orbits of a homeomorphism f can be traceable by actual orbits even if rounding errors in computing are not inevitable has been recently proved [28].

Hence this attractor is very efficient, in order to generate chaotic numbers without repetition for standard simulation using either the first or the second component. However they are not equally distributed on the plane (see Fig. 5). The non constant density forbids its direct use as a PRN generator. Nevertheless there are some U.S. patents for “method of generating pseudo-random numbers in an electronic device, and a method of encrypting and decrypting electronic data” in which the Lozi map is involved [29, 30].

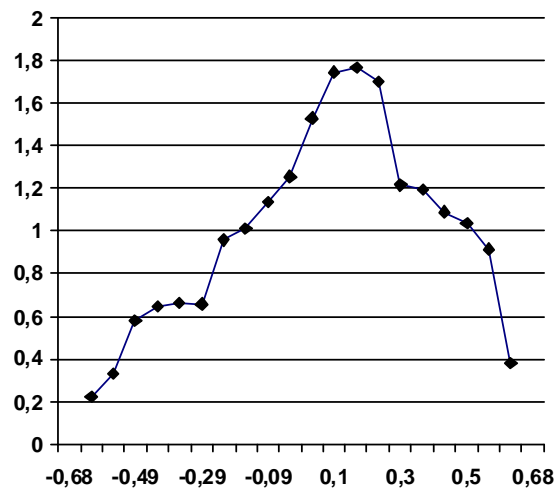


Figure 5. Invariant density of the second component y of Eq. (7) computed using 10^{10} iterations.

Nevertheless Lozi map is now widely used in chaotic optimisation which belongs to a new class of algorithms: the evolutionary algorithms (EA). In a

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

founding paper, R. Caponetto et al. [31] propose an experimental analysis on the convergence of EA. The effect of introducing chaotic sequences instead of random ones during all the phases of the evolution process is investigated. The approach is based on the substitution of the PRNG with chaotic sequences. Several numerical examples are reported in order to compare the performance of the EA using random and chaotic generators as regards to both the results and the convergence speed. The results obtained show that chaotic sequences obtained from Lozi map are always able to increase the value of some measured algorithm-performance indexes with respect to random sequences.

Several authors following this idea use Lozi map in chaotic optimization in order to avoid local optima stagnation and embed a superior search strategy [32 – 40].

2.3. 3-Dimensional System Chaotic Dynamical Systems

In order to generalize in higher dimension the tent map, G. Manjunath *et al.* [41] introduce a three-dimensional map $F : I^3 \rightarrow I^3$ where $I = [0, 1]$ (see Fig. 6) which is continuous in the Euclidian topology and prove its chaotic properties:

$$F(x, y, z) = \begin{pmatrix} \left| I - \left| 2x + \frac{y+z}{2} - I \right| \right| \\ \left| I - \left| 2y + \frac{x+z}{2} - I \right| \right| \\ \left| I - \left| 2z + \frac{x+y}{2} - I \right| \right| \end{pmatrix} \quad (9)$$

The related dynamical system is

$$(x_{n+1}, y_{n+1}, z_{n+1}) = F(x_n, y_n, z_n) \quad (10)$$

They emphasize that most of the well known examples of higher dimensional chaotic dynamical systems belong to the class of hyperbolic diffeomorphisms on a n -torus. These higher dimensional maps on the torus are not continuous on the standard topology of the Euclidean space since they exhibit jump discontinuities. The realization of such jump discontinuities in an electronic circuit implementation is not reliable. They prove the following theorem:

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

Theorem (G. Manjunath *et al.*) The map defined in (9) is topologically transitive and exhibits sensitive dependence on initial conditions with any real

number $\delta \in \left(0, \frac{\sqrt{3}}{2}\right)$ as sensitivity constant.

Once again the sequence of iterated points (x_n, y_n, z_n) obtained from the dynamical system (10) is not equally distributed on the volume I^3 . The invariant density of the first component x_n is displayed in Fig. 7. The relative discrepancy of this invariant density versus the uniform one lies between 4% and 5%.

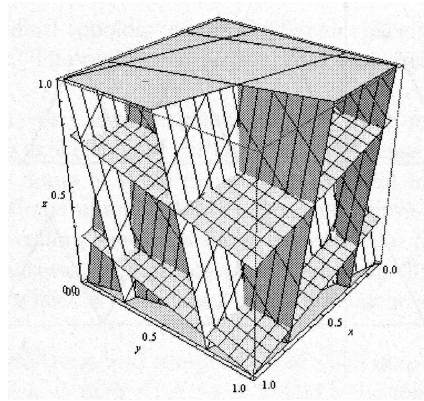


Figure 6. Tessellation of I^3 into 3^3 regions by parallel set of critical planes $\bar{T}_{y,z}(z) = 0$ and 1 , $\bar{T}_{x,z}(y) = 0$ and 1 , $\bar{T}_{x,z}(z) = 0$ and 1 , pertaining to the map (9).

To allow the generation of PRN using complexity and emergence theory we consider in the next section how to generate these numbers with uniform repartition on a given interval, or on a given square of the plane or more generally in a given hypercube of \mathbb{R}^n involving the ultra weak multidimensional coupling of p l -dimensional chaotic dynamical systems.

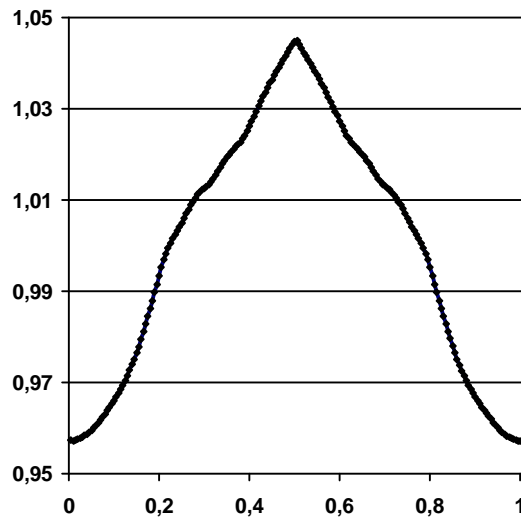


Figure 7. Invariant density of the first component x of Eq. (10) computed using 10^{11} iterations.

3. Multi-parameter Chaotic Pseudo-Random Number Generator (M-p CPRNG)

As previously seen, when a dynamical system is realized on a computer using floating point or double precision numbers, the computation is of a discretization, where finite machine arithmetic replaces continuum state space. For chaotic dynamical systems, the discretization often has collapsing effects to a fixed point or to short cycles [15, 42]. In order to preserve the chaotic properties of the continuous models in numerical experiments we consider an ultra weak multidimensional coupling of p one-dimensional dynamical systems.

3.1. System of p -Coupled Symmetric Tent Map

In order to simplify the presentation of the M-p CPRNG we introduce, we use as an example the symmetric tent map previously defined (3), even though others chaotic map of the interval (as the logistic map, the baker transform, ...) can be used for the same purpose (as a matter of course, the invariant measure of the chaotic map chosen is preserved).

The considered system of the p -coupled dynamical systems is described by

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

$$X_{n+1} = F(X_n) = A \cdot \underline{f}(X_n) \quad (11)$$

with

$$X_n = \begin{pmatrix} x_n^1 \\ \vdots \\ x_n^p \end{pmatrix}, \quad \underline{f}(X_n) = \begin{pmatrix} f(x_n^1) \\ \vdots \\ f(x_n^p) \end{pmatrix} \quad (12)$$

and

$$A = \begin{pmatrix} \varepsilon_{1,1} = I - \sum_{j=2}^{j=p} \varepsilon_{1,j} & \varepsilon_{1,2} & \cdots & \varepsilon_{1,p-1} & \varepsilon_{1,p} \\ \varepsilon_{2,1} & \varepsilon_{2,2} = I - \sum_{j=1, j \neq 2}^{j=p} \varepsilon_{2,j} & \cdots & \varepsilon_{2,p-1} & \varepsilon_{2,p} \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots \\ \varepsilon_{p,1} & \cdots & \cdots & \varepsilon_{p,p-1} & \varepsilon_{p,p} = I - \sum_{j=1}^{j=p-1} \varepsilon_{p,j} \end{pmatrix} \quad (13)$$

F is a map of $J^p = [-1, 1]^p \subset \mathbb{R}^p$ into itself.

Considering $\varepsilon_{i,i} = I - \sum_{j=1, j \neq i}^{j=p} \varepsilon_{i,j}$, the matrix A is always a stochastic matrix

iff the coupling constants verify $\varepsilon_{i,j} > 0$ for every i and j .

If $\forall i, j \quad \varepsilon_{i,j} = 0$ the maps are totally decoupled, instead they are fully

crisscross coupled when for example $\varepsilon_{i,j} = \frac{I}{p-1}$ for $i \neq j$. Generally, researchers do

not consider very small values of $\varepsilon_{i,j}$ because it seems that the maps are quasi-decoupled with those values and no special effect of the coupling is expected. In fact it is not the case and ultra small coupling constants (as small as 10^{-7} for floating point numbers or 10^{-16} for double precision numbers), allows the construction of very long periodic orbits, leading to sterling chaotic generators. This is the way in complexity leads to randomness from chaos.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

Moreover each component of these numbers belonging to \mathbb{R}^p is equally distributed over the finite interval $J \subset \mathbb{R}$, when one chooses a function f with uniform invariant measure. Numerical computations (up to 10^{13} numbers) show that this distribution is obtained with a very good approximation. They have also the property that the length of the periods of the numerically observed orbits is very large [23].

3.2. Chaotic Sampling and Mixing

However chaotic numbers are not pseudo-random numbers because the plot of the couples of any component (x_n^l, x_{n+1}^l) of iterated points (X_n, X_{n+1}) in the corresponding phase plane reveals the map f used as one-dimensional dynamical systems to generate them *via* Eq. (11).

Nevertheless we have recently introduced a family of enhanced Chaotic Pseudo Random Number Generators (CPRNG) in order to compute very fast long series of pseudorandom numbers with desktop computer [3, 4, 5]. This family is based on the previous ultra weak coupling which is improved in order to conceal the chaotic genuine function.

In order to hide f in the phase space (x_n^l, x_{n+1}^l) two mechanisms are used. The pivotal idea of the first one mechanism is to sample chaotically the sequence $(x_0^l, x_1^l, x_2^l, \dots, x_n^l, x_{n+1}^l, \dots)$ generated by the l -th component x^l , selecting x_n^l every time the value x_n^m of the m -th component x^m , is strictly greater (or smaller) than a threshold $T \in J$, with $l \neq m$, for $1 \leq l, m \leq p$.

That is to say to extract the subsequence $(x_{n_{(0)}}^l, x_{n_{(1)}}^l, x_{n_{(2)}}^l, \dots, x_{n_{(q)}}^l, x_{n_{(q+1)}}^l, \dots)$ denoted here $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ of the original one, in the following way

Given $1 \leq l, m \leq p, l \neq m$

$$\begin{cases} n_{(-1)} = -1 \\ \overline{x_q} = x_{n_{(q)}}^l, \text{ with } n_{(q)} = \underset{r \in \mathbb{N}}{\text{Min}} \{ r > n_{(q-1)} \mid x_r^m > T \} \end{cases} \quad (14)$$

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

The sequence $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ is then the sequence of chaotic pseudo-random numbers.

The mathematical formula (14) can be best understood in algorithmic way. The pseudo-code, for computing iterates of (14) corresponding to N iterates of (11) is:

$$X_0 = (x_0^1, x_0^2, \dots, x_0^{p-1}, x_0^p) = \text{seed}$$

$$n = 0; q = 0$$

do { while $n < N$

do { while $(x_n^m \leq T)$

compute $(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p); n++$

compute $(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p);$

then $n(q) = n; \overline{x_q} = x_{n(q)}^1; n++; q++$

This chaotic sampling is possible due to the independence of each component of the iterated points X_n vs. the others [3].

Remark 1: Albeit the number $NSampl_{iter}$ of pseudo-random numbers $\overline{x_q}$ corresponding to the computation of N iterates is not known *a priori*, considering that the selecting process is again linked to the uniform distribution of the iterates of the tent map on J , this number is equivalent to $\frac{2N}{1-T}$.

A second mechanism can improve the unpredictability of the pseudo-random sequence generated as above, using synergistically all the components of the vector X_n , instead of two. Given $p-1$ thresholds

$$T_1 < T_2 < \dots < T_{p-1} \in J \quad (15)$$

and the corresponding partition of J

$$J = \bigcup_{k=0}^{p-1} J_k \quad (16)$$

with $J_0 = [-1, T_1]$, $J_1 =]T_1, T_2[$, $J_k = [T_k, T_{k+1}[$ for $1 < k < p-1$ and $J_{p-1} = [T_{p-1}, 1[$, this simple mechanism is based on the chaotic mixing of the $p-1$ sequences

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

$$\left(x_0^1, x_1^1, x_2^1, \dots, x_n^1, x_{n+1}^1, \dots\right), \quad \left(x_0^2, x_1^2, x_2^2, \dots, x_n^2, x_{n+1}^2, \dots\right), \dots, \\ \left(x_0^{p-1}, x_1^{p-1}, x_2^{p-1}, \dots, x_n^{p-1}, x_{n+1}^{p-1}, \dots\right), \dots$$

using the last one $\left(x_0^p, x_1^p, x_2^p, \dots, x_n^p, x_{n+1}^p, \dots\right)$ in order to distribute the iterated points with respect to this given partition defining the subsequence $\left(x_{n_{(0)}}^l, x_{n_{(1)}}^l, x_{n_{(2)}}^l, \dots, x_{n_{(q)}}^l, x_{n_{(q+1)}}^l, \dots\right)$ here denoted $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots\right)$ by

$$\left\{ \begin{array}{l} n_{(q-1)} = -1 \\ \overline{x_q} = x_{n_{(q)}}^k, \text{ with } n_{(q)} = \underset{1 \leq k \leq p-1}{\text{Min}} \left\{ s_k(q) = \underset{r_k \in \mathbb{N}}{\text{Min}} \left\{ r_k > n_{(q-1)} \mid x_{r_k}^p \in J_k \right\} \right\} \end{array} \right\} \quad (17)$$

The pseudo-code, for computing the iterates of (17) corresponding to N iterates of (11) is:

$X_0 = \left(x_0^1, x_0^2, \dots, x_0^{p-1}, x_0^p\right) = \text{seed}$
 $n = 0; q = 0$
do { while $n < N$
do { while $\left(x_n^p \in J_0\right)$ compute
 $\left(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p\right); n++$
compute $\left(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p\right)$
let k be such that $x_n^p \in J_k$
then $n(q) = n; \overline{x_q} = x_{n(q)}^k; n++; q++$ }

Remark 2: In this case also, $NSampl_{iter}$ is not known *a priori*, however, considering that the selecting process is linked to the uniform distribution of the iterates of the tent map on J , one has $NSampl_{iter} \approx \frac{2N}{1-T_1}$.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

Remark 3: This second mechanism is more or less linked to the whitening process [43, 44].

Remark 4: Actually, one can choose any of the components in order to sample and mix the sequence, not only the last one.

3.3. Double Threshold Chaotic Sampling

One can eventually improve the CPRNG previously introduced with respect to the infinity norm instead of the L_1 or L_2 norms because the L_∞ norm is more sensitive than the others ones to reveal the concealed function f [5]. For this purpose we introduce a second kind of threshold $T' \in \mathbb{N}$, together with $T_1, \dots, T_{p-1} \in J$ such that the subsequence $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ is defined by

$$\left\{ \begin{array}{l} n_{(-1)} = -1 \\ \overline{x_q} = x_{n_{(q)}}^k, \text{ with } n_{(q)} = \text{Min}_{1 \leq k \leq p-1} \left\{ s_k(q) = \text{Min}_{r_k \in \mathbb{N}} \left\{ r_k > n_{(q-1)} + T' \mid x_{r_k}^p \in J_k \right\} \right\} \end{array} \right\} \quad (18)$$

In pseudo-code Eq. (18) is then:

$$X_0 = (x_0^1, x_0^2, \dots, x_0^{p-1}, x_0^p) = \text{seed}$$

$$n = 0, q = 0$$

do { while $n < N$

do { while $(n \leq n_{(q-1)} + T' \text{ and } x_n^p \in J_0)$

compute $(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p); n++$

compute $(x_n^1, x_n^2, \dots, x_n^{p-1}, x_n^p)$

let k be such that $x_n^p \in J_k$

then $n(q) = n; \overline{x_q} = x_{n(q)}^k; n++; q++$

Remark 5: In this case also, $NSampl_{iter}$ is not known a priori, it is more complicated to give an equivalent to it. However, considering that the selecting

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

process is linked to the uniform distribution of the iterates of the tent map on J , and to the second threshold T' , it comes that $NSampl_{iter} \leq \text{Min} \left\{ \frac{2N}{1-T_1}, \frac{N}{T'} \right\}$.

Remark 6: the second kind of threshold T' can also be used with only the chaotic sampling, without the chaotic mixing.

4. Emergence of Randomness

Numerical results about chaotic numbers produced by (11) — (17) show that they are equally distributed over the interval J with a very good precision [3, 4].

In this section we emphasize that when the parameters $\mathcal{E}_{i,j}$ belong to a special window (called the window of emergence) the M-p CPRNG defined above behaves well.

4.1. Approximated Invariant Measures

In order to perform numerical computation, we have to define some numerical tools: the approximated invariant measures.

First we define an approximation $P_{M,N}(x)$ of the invariant measure also called the probability distribution function linked to the 1-dimensional map f when computed with floating numbers (or numbers in double precision). In this scope we consider a regular partition of M small intervals (boxes) r_i of J defined by:

$$\begin{aligned} s_i &= -I + \frac{2i}{M}, \quad i = 0, M \\ r_i &= [s_i, s_{i+1}[, \quad i = 0, M - 2 \\ r_{M-1} &= [s_{M-1}, I] \\ J &= \bigcup_0^{M-1} r_i \end{aligned}$$

the length of each box is

$$s_{i+1} - s_i = \frac{2}{M}$$

(note that this regular partition of J is different from the previous one linked to the threshold values T_i (16)).

All iterates $f^{(n)}(x)$ belonging to these boxes are collected (after a transient regime of Q iterations decided *a priori*, *i.e.* the first Q iterates are neglected). Once

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

the computation of $N + Q$ iterates is completed, the relative number of iterates with respect to N/M in each box r_i represents the value $P_N(s_i)$. The approximated $P_N(x)$ defined in this article is then a step function, with M steps. As M may vary, we define

$$P_{M,N}(s_i) = \frac{1}{2} \frac{M}{N} (\#r_i)$$

where $\#r_i$ is the number of iterates belonging to the interval r_i and the constant $1/2$ allows the normalisation of $P_{M,N}(x)$ on the interval J .

$$P_{M,N}(x) = P_{M,N}(s_i) \quad \forall x \in r_i$$

In the case of p -coupled maps, we are more interested by the distribution of each component $(x^1, x^2, x^3, \dots, x^p)$ of X rather than the distribution of the variable X itself in J^p . We then consider the approximated probability distribution function $P_{M,N}(x^j)$ associated to one among several components of $F(X)$ defined by (11) which are one-dimensional maps. In this paper we use equally N_{disc} for M and N_{iter} for N when they are more explicit.

The discrepancies E_1 (in norm L_1), E_2 (in norm L_2) and E_∞ (in norm L_∞) between $P_{N_{disc}, N_{iter}}(x)$ and the Lebesgue measure which is the invariant measure associated to the symmetric tent map, are defined by

$$E_{1, N_{disc}, N_{iter}}(x) = \left\| P_{N_{disc}, N_{iter}}(x) - 0.5 \right\|_{L_1}$$

$$E_{2, N_{disc}, N_{iter}}(x) = \left\| P_{N_{disc}, N_{iter}}(x) - 0.5 \right\|_{L_2}$$

$$E_{\infty, N_{disc}, N_{iter}}(x) = \left\| P_{N_{disc}, N_{iter}}(x) - 0.5 \right\|_{L_\infty}$$

In the same way an approximation of the correlation distribution function $C_{M,N}(x, y)$ is obtained numerically building a regular partition of M^2 small squares (boxes) of J^2 imbedded in the phase subspace (x^1, x^m)

$$s_i = -1 + \frac{2i}{M}, \quad t_j = -1 + \frac{2j}{M}, \quad i, j = 0, M$$

$$r_{i,j} = [s_i, s_{i+1}] \times [t_j, t_{j+1}], \quad i, j = 0, M-2$$

$$r_{i, M-1} = [s_i, s_{i+1}] \times [t_{M-1}, 1], \quad j = 0, M-2$$

$$r_{M-1, M-1} = [s_{M-1}, I] \times [t_{M-1}, I]$$

the measure of the area of each box is

$$(s_{i+1} - s_i) \times (t_{i+1} - t_i) = \left(\frac{2}{M}\right)^2$$

Once $N + Q$ iterated points (x_n^l, x_n^m) belonging to these boxes are collected the relative number of iterates with respect to N/M^2 in each box $r_{i,j}$ represents the value $C_N(s_i, t_j)$. The approximated probability distribution function $C_N(x, y)$ defined here is then a 2-dimensional step function, with M^2 steps. As M can take several values in the next sections, we define

$$C_{M,N}(s_i, t_j) = \frac{1}{4} \frac{M^2}{N} (\# r_{i,j}) \quad (19)$$

where $\# r_{i,j}$ is the number of iterates belonging to the square $r_{i,j}$ and the constant $1/4$ allows the normalisation of $C_{M,N}(x, y)$ on the square J^2

$$C_{M,N}(x, y) = C_{M,N}(s_i, t_j) \quad \forall (x, y) \in r_{i,j} \quad (20)$$

The discrepancies E_{C_1} (in norm L_1), E_{C_2} (in norm L_2) and E_{C_∞} (in norm L_∞) between $C_{N_{disc}, N_{iter}}(x, y)$ and the uniform distribution on the square, are defined by

$$\begin{aligned} E_{C_1, N_{disc}, N_{iter}}(x, y) &= \left\| C_{N_{disc}, N_{iter}}(x, y) - 0.25 \right\|_{L_1} \\ E_{C_2, N_{disc}, N_{iter}}(x, y) &= \left\| C_{N_{disc}, N_{iter}}(x, y) - 0.25 \right\|_{L_2} \\ E_{C_\infty, N_{disc}, N_{iter}}(x, y) &= \left\| C_{N_{disc}, N_{iter}}(x, y) - 0.25 \right\|_{L_\infty} \end{aligned}$$

Finally let $AC_{N_{disc}, N_{iter}}(x, y)$ be the autocorrelation distribution function which is the correlation function $C_{N_{disc}, N_{iter}}(x, y)$ of (20) defined in the phase space (x_n^l, x_{n+1}^l) instead of the phase space (x^l, x^m) . In order to control that the enhanced chaotic numbers $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ are uncorrelated, we plot them in the phase subspace $(\overline{x_q}, \overline{x_{q+1}})$ and we check if they are uniformly distributed in the square J^2 and if f is concealed (*i.e.*

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011)* pp. 93-125.

$E_{AC_1, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1}), E_{AC_2, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1}), E_{AC_{\infty}, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$ vanish).

4.2. A window of Emergence of Randomness

In order to point out the usefulness of the double threshold chaotic sampling with simply consider the case of only 4 coupled equations, and such that $\varepsilon_{i,j} = \varepsilon_i \forall i \neq j$ and $\varepsilon_{i,i} = 1 - 3\varepsilon_i$. Eq. (11) becomes

$$\begin{cases} x_{n+1}^1 = (1 - 3\varepsilon_1)f(x_n^1) + \varepsilon_1 f(x_n^2) + \varepsilon_1 f(x_n^3) + \varepsilon_1 f(x_n^4) \\ x_{n+1}^2 = \varepsilon_2 f(x_n^1) + (1 - 3\varepsilon_2)f(x_n^2) + \varepsilon_2 f(x_n^3) + \varepsilon_2 f(x_n^4) \\ x_{n+1}^3 = \varepsilon_3 f(x_n^1) + \varepsilon_3 f(x_n^2) + (1 - 3\varepsilon_3)f(x_n^3) + \varepsilon_3 f(x_n^4) \\ x_{n+1}^4 = \varepsilon_4 f(x_n^1) + \varepsilon_4 f(x_n^2) + \varepsilon_4 f(x_n^3) + (1 - 3\varepsilon_4)f(x_n^4) \end{cases} \quad (21)$$

Moreover we assume that $\varepsilon_i = i\varepsilon_1$

For the shake of simplicity we consider only the chaotic sampling method (*i.e.* we use only one threshold T), without the chaotic mixing. We then compute $E_{1, N_{disc}, N_{iter}}(\bar{x}), E_{2, N_{disc}, N_{iter}}(\bar{x}), E_{\infty, N_{disc}, N_{iter}}(\bar{x})$ and $E_{AC_{\infty}, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$ $E_{AC_1, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1}), E_{AC_2, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$, for $N_{disc} = 1,024$ and $N_{iter} = 10^{11}$. We choose, $T = 0.9$ and $T' = 20$. We display on Fig. 8 the values of the six computed error when $\varepsilon_1 \in [10^{-17}, 10^{-1}]$. The seed (initial values) being

$$x_0^1 = 0.330000, x_0^2 = 0.338756, x_0^3 = 0.504923, x_0^4 = 0.324082.$$

A window of emergence comes clearly into sight for the values $\varepsilon_1 \in [10^{-15}, 10^{-7}]$ if one considers all together the six errors.

The errors $E_{\infty, N_{disc}, N_{iter}}(\bar{x}), E_{AC_{\infty}, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$ narrowing this window in which $340,753,095 \leq NSampl_{iter} \leq 340,768,513$ out of $N_{iter} = 10^{11}$.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

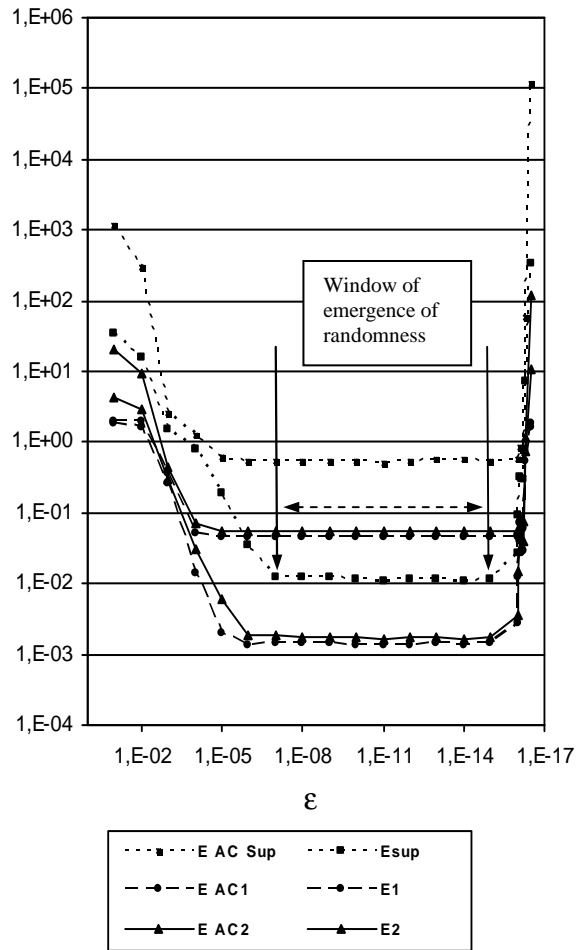


Figure 8. The window of emergence of randomness

4.3. The Underneath of Randomness

The double threshold chaotic sampling is very efficient because its aim is mainly to conceal f in the most drastic way. In order to understand the underneath mechanism consider first that in the phase space (x_n^I, x_{n+1}^I) the graph of the

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

chaotically sampled chaotic numbers is a mix of the graphs of the $f^{(r)}$ for all $r \in \mathbb{N}$ (see Fig. 9).

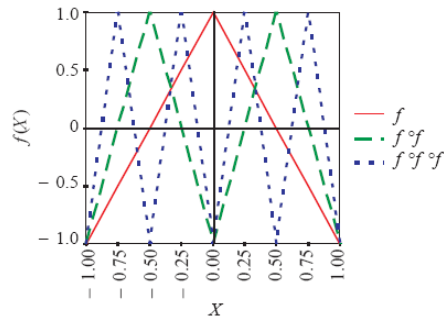


Figure 9. Graphs of the symmetric tent map $f, f^{(2)}$ and $f^{(3)}$ on the interval $[-1, 1]$.

It is obvious as showed on Fig. 10 that for $r = 1$ if $M = 1$ or 2 , $AC_{M,N}(x, y)$ is constant and normalized on the square hence $E_{AC_1, N_{disc}, N_{iter}}(x, y) = E_{AC_2, N_{disc}, N_{iter}}(x, y) = E_{AC_{\infty}, N_{disc}, N_{iter}}(x, y) = 0$

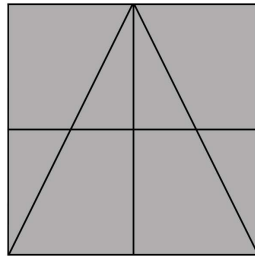


Figure 10. In shaded regions the autocorrelation distribution $AC_{M,N}(x, y)$ is constant for the symmetric tent map f on the interval $[-1, 1]$ for $M = 1$ or 2 .

The autocorrelation function is different from zero only if $M > 2$ (see Fig. 11). In the same way as displayed on Fig. 12, 13 and 14, $E_{AC_1, N_{disc}, N_{iter}}(x, y) = E_{AC_2, N_{disc}, N_{iter}}(x, y) = E_{AC_{\infty}, N_{disc}, N_{iter}}(x, y) = 0$ for $f^{(i)}$ iff $M < 2^i$. Hence for a given M , if we cancel the contribution of all the $f^{(i)}$ for $2^i < M$, it is not possible to identify the genuine function f .

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

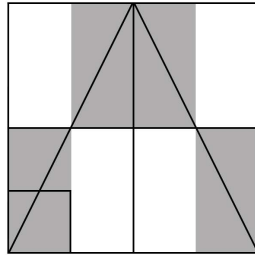


Figure 11. Regions where the autocorrelation distribution $AC_{M,N}(x, y)$ is constant for the symmetric tent map f are shaded, for $M = 4$. (The square on the bottom left hand side of the graph shows the size of the r_{ij} box). $AC_{M,N}(x, y)$ vanishes on the white regions.

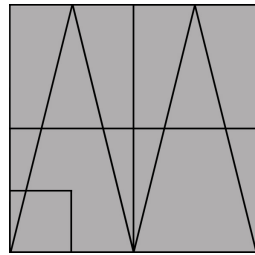


Figure 12. In shaded regions the autocorrelation distribution $AC_{M,N}(x, y)$ is constant for the symmetric tent map $f^{(2)}$ on the interval $[-1, 1]$ for $M = 1, 2$ and 4 .

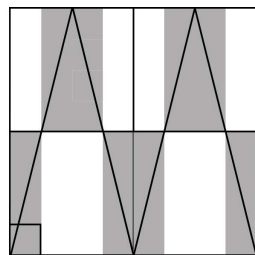


Figure 13. Regions where the autocorrelation distribution $AC_{M,N}(x, y)$ is constant for the symmetric tent map $f^{(2)}$ are shaded for $M = 8$.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

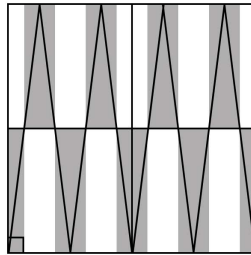


Figure 14. Regions where the autocorrelation distribution $AC_{M,N}(x,y)$ is constant for the symmetric tent map $f^{(3)}$ are shaded for $M = 16$.

4.4. Testing the Randomness

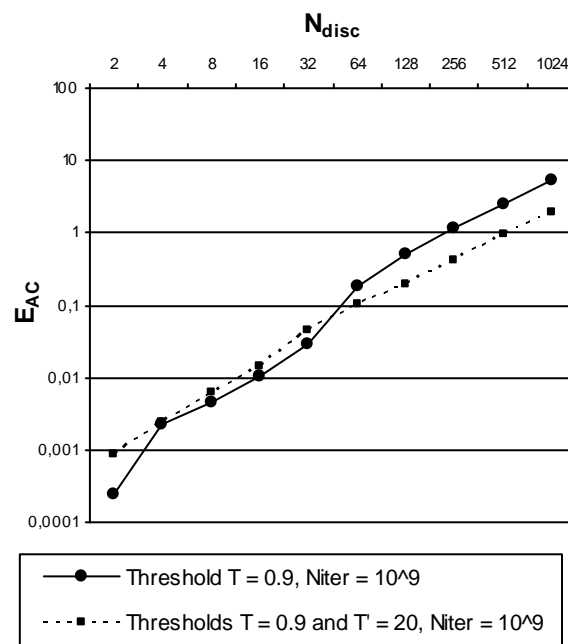


Figure 15. Error of $E_{AC^\infty, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$, $N_{disc} = 2^1$ to 2^{10} , $N_{iter} = 10^9$, thresholds $T = 0.9$ and $T' = 20$, $\varepsilon_i = i \varepsilon_1$, $\varepsilon_i = 10^{-14}$.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

Computations are done using double precision numbers (~14-15 digits).

As shown previously [3] the errors in L_1 or L_2 norms decrease with the number of chaotic points (as in the law of large numbers) and conversely increase with the number M of boxes used to define $AC_{M,N}(x, y)$. It is the same for the error in L_∞ norm. Fig. 15 shows that when M is greater than 2^5 , the sequence defined by (18) behaves better than the one defined by (14) or (17) when applied to Eq. (21).

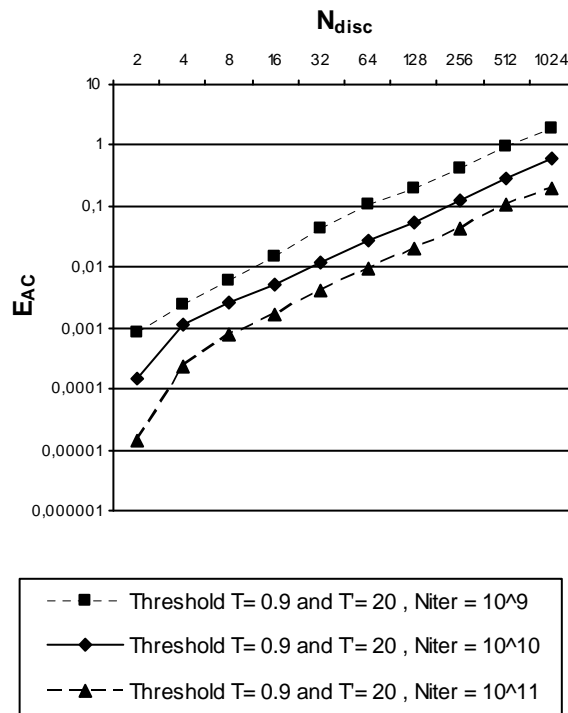


Figure 16. Error of $E_{AC^\infty, N_{disc}, N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$ $N_{disc} = 2^1$ to 2^{10} , $N_{iter} = 10^9$ to 10^{11} , thresholds $T = 0.9$ and $T' = 20$, $\varepsilon_i = i \varepsilon_1$, $\varepsilon_i = 10^{-14}$. Computations are done using double precision numbers (~14-15

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.
 digits).

Fig. 16 shows that when the number of chaotic points increases the error $E_{AC^\infty, N_{disc} \cdot N_{iter}}(\bar{x}_q, \bar{x}_{q+1})$ decreases drastically. If for example $T' > 100$, it is necessary to use a huge grid of $2^{100} \times 2^{100}$ boxes splitting the square J^2 in order to find a trace of the genuine function f . This is numerically impossible with double precision numbers. Then the chaotic numbers emerge as random numbers.

5. Applications

Generation of random or pseudorandom numbers, nowadays, is a key feature of industrial mathematics. Pseudorandom or chaotic numbers are used in many areas of contemporary technology such as modern communication systems and engineering applications.

More and more European or US patents using discrete mappings for this purpose are obtained by researchers of discrete dynamical systems [29, 30].

When an efficient M-p CPRNG is defined, there exists a huge number of applications for the pseudo-random numbers it can generate, as for example chaotic masking, chaotic modulation or chaotic shift keying in the fields of secure communications [7, 8, 9, 10].

5.1. Parameter sensitivity

A determining property of the M-p CPRNG we have improved in this paper via Eq. (21) and double threshold chaotic sampling (18) is the high number of parameters used ($p \times (p-1)$ for p coupled equations) which allows to choose it as cipher-keys however this achievement is possible only if there is a high sensitivity to the parameters values.

In order to point up this sensitivity, it is enough to consider the simplest case of 2-coupled equations with two sets of slightly different parameters $(\varepsilon_1, \varepsilon_2)$ and $(\varepsilon_1^*, \varepsilon_2^*)$ $\varepsilon_1 = 0.000,001$, $\varepsilon_1^* = 0.000,001,000,000,000,000,3$, and $\varepsilon_2 = 0.000,002$.

$$\begin{cases} x_{n+1}^1 = (1 - \varepsilon_1)f(x_n^1) + \varepsilon_1 f(x_n^2) \\ x_{n+1}^2 = \varepsilon_2 f(x_n^1) + (1 - \varepsilon_2)f(x_n^2) \end{cases} \quad (22)$$

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

$$\begin{cases} x_{n+1}^{*1} = (I - \varepsilon_1)f(x_n^{*1}) + \varepsilon_1^* f(x_n^{*2}) \\ x_{n+1}^{*2} = \varepsilon_2 f(x_n^{*1}) + (I - \varepsilon_2)f(x_n^{*2}) \end{cases} \quad (23)$$

The double threshold sampling is done using $T = 0.9$ and $T' = 20$ and the same seed is taken

$$X_0 = (x_0^1, x_0^2) = X_0^* = (x_0^{*1}, x_0^{*2})$$

Despite the fact that the difference between ε_1 and ε_1^* is tiny:

$\frac{|\varepsilon_1 - \varepsilon_1^*|}{\varepsilon_1} = 3 \times 10^{-13}$ the sequences $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ and $(\overline{x_0^*}, \overline{x_1^*}, \overline{x_2^*}, \dots, \overline{x_q^*}, \overline{x_{q+1}^*}, \dots)$ differ completely as displayed in Table 3 (In fact all the components $(x_{n(q)}^1, x_{n(q)}^2)$ and $(x_{n(q)}^{*1}, x_{n(q)}^{*2})$ are different).

ε_1	0.000,001	ε_1^*	0.000,001,000, 000,000,000,3
x_0^1	0.330,000,013, 113,021,851	x_0^{*1}	0.330,000,013, 113,021,851
$x_{n(q)}^1$	-0.959,214,817, 207,605,153	$x_{n(q)}^{*1}$	-0.058,536,729, 173,974,455,5
$x_{n(q)}^1$	0.657,775,688, 600,752,417	$x_{n(q)}^{*1}$	0.386,129,403, 866,398,935
$x_{n(q)}^1$	-0.784,600,935, 471,051,031	$x_{n(q)}^{*1}$	0.471,824,729, 381,262,631

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

ε_1	0.000,001	ε_1^*	0.000,001,000, 000,000,000,3
x_0^2	0.338,756,413, 113,021,848	x_0^{*2}	0.338,756,413, 113,021,848
$x_{n(0)}^2$	0.914,472,270, 898,123,885	$x_{n(0)}^{*2}$	-0.646,249,812, 458,326,023
$x_{n(1)}^2$	0.915,684,412, 995,676,6	$x_{n(1)}^{*2}$	0.894,262,910, 879,751,405
$x_{n(2)}^3$	0.910,813,705, 361,448,345	$x_{n(2)}^{*2}$	0.820,811,987, 022,524,114

Table 3. Sequences $(x_{n(q)}^1, x_{n(q)}^{*1})$ and $(x_{n(q)}^2, x_{n(q)}^{*2})$ of Eq. (22) and (23) with $\varepsilon_1 = 0.000,001$, $\varepsilon_1^* = 0.000,001,000,000,000,000,3$ and $\varepsilon_2 = 0.000,002$. $X_0 = (x_0^1, x_0^2) = X_0^* = (x_0^{*1}, x_0^{*2})$

Then rather than a unique CPRNG which is introduced here, there is a quasi-infinite family of CPRNG that the M-p CPRNG define allowing several possibilities of applications.

5.2. Gaussian Noise

As an example of such application, the generation of Gaussian noise from the sequences $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ is very easy when a Box-Muller transform is applied.

A Box-Muller transform [45] is a method of generating pairs of independent standard normally distributed (zero expectation, unit variance) random numbers, given a source of uniformly distributed random numbers. The polar form [46] of such a transform takes two samples from a different interval, $[-1, 1]$ and maps them to two normally distributed samples without the use of sine or cosine functions. This form of the polar transform is widely used, in part due to its inclusion in Numerical Recipes.

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

As the sequences $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ are uniformly distributed in $J = [-1, 1] \subset \mathbb{R}$, the application is straightforward.

5.3. Hash Function

Another example of application could be the computation of hash function. A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small one. The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

Hash functions are mostly used to speed up table lookup or data comparison tasks — such as finding items in a database, detecting duplicated or similar records in a large file, finding similar stretches in DNA sequences, and so on.

A hash function may map two or more keys to the same hash value. In many applications, it is desirable to minimize the occurrence of such collisions, which means that the hash function must map the keys to the hash values as evenly as possible. Depending on the application, other properties may be required as well. Although the idea was conceived in the 1950s, the design of good hash functions is still a topic of active research.

Although hash function generally involve integers, one can consider that the application which maps the initial seed $X_0 = (x_0^1, x_0^2, \dots, x_0^{p-1}, x_0^p)$ into any predetermined term of the sequence $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \dots, \overline{x_q}, \overline{x_{q+1}}, \dots)$ is a hash function working on floating point numbers.

We will explore this application in a forthcoming paper.

Others applications show the high-potency of such M-p CPRNG. Due to limitation of this article, they will be published elsewhere.

6. Conclusion

Using a double threshold in order to sample a chaotic sequence, we have improved with respect to the infinity norm the M-p CPRNG previously introduced. When the value of the second threshold T' is greater than 100, it is impossible to find the genuine function used to generate the chaotic numbers. The new M-p CPRNG family is robust versus the choice of the weak parameter of the system for $10^{-14} < \epsilon < 10^{-5}$, allowing the use of this family in several applications as

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

for example producing Gaussian noise, computing hash function or in chaotic cryptography.

References

1. W. Weaver, *American Scientist* **36**, (4), 536 (1948).
2. M. A. Aziz-Alaoui and C. Bertelle, *From System Complexity to Emergent Properties (Understanding Complex Systems)* Springer-Verlag, Berlin (2009).
3. R. Lozi, *Indian Journal of Industrial and Applied Mathematics* Vol.1, n° 1, 1 (2008).
4. R. Lozi, *Proceedings of 6th EUROMECH Non Linear Dynamics Conference, Saint-Petersburg, ENOC 2008, IPACS Open Access Electronic Library*, 1715 (2008).
5. R. Lozi, *Conference Proceedings of ICCSA 2009* 20 (2009).
6. R. Lozi, *Intern. J. Bifurcation & Chaos* to appear (2011).
7. S. Hénaff, I. Taralova and R. Lozi, *Conference Proceedings of ICCSA 2009* 47 (2009).
8. S. Hénaff, I. Taralova and R. Lozi, *Indian Journal of Industrial and Applied Mathematics* Vol.2, No 2, 1 (2009).
9. S. Hénaff, I. Taralova and R. Lozi, *Proceedings of the Physics and Control Conference, Catania 2009, IPACS Open Access Electronic Library*, 1939 (2009).
10. S. Hénaff, I. Taralova and R. Lozi, *Journal of Nonlinear Systems and Applications* Vol.1, (3-4), 87 (2010).
11. J. C. Sprott, *Chaos and Time-Series Analysis* Oxford University Press, Oxford, UK (2003).
12. K. T. Alligood, T. D. Sauer and J. A. Yorke, *Chaos. An introduction to dynamical systems* Springer, Textbooks in mathematical sciences, New-York (1996).
13. R. M. May, *Science, New Series* Vol. 186, No 4164, 645 (1974).
14. M. J. Feigenbaum, *J. Stat. Phys* 21, 669 (1979).
15. O. E. Lanford III, *Experimental Mathematics* Vol. 7, **4**, 317 (1998).
16. R. Lozi and C. Fiol, *Grazer Math. Bericht* Nr 354, 112 (2009).
17. R. Lozi and C. Fiol, *Conference Proceedings A.I.P.* **1146**, 303 (2009).
18. M. S. Baptista, *Phys. Lett. A* 240, 50 (1998).
19. M. R. K. Ariffin and M. S. M. Noorani, *Phys. Lett. A* 372, 5427 (2008).
20. A. N. Sharkovskii, *Intern. J. Bifurcation & Chaos* Vol. 5, **5**, 1263 (1995).
21. M. Hénon, *Comm. Math. Phys.* **50**, 69 (1976).
22. D. Ruelle and F. Takens, *Comm. Math. Phys.* **20**, 167 (1971).

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011) pp. 93-125*.

23. R. Lozi, in *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, eds. A. H. Siddiqi, I. S. Duff and O. Christensen, Anamaya Publishers, New Delhi, India, 80 (2006).
24. N. K. Pareek, V. Patidar and K. K. Sud, *Int. J. Information and Communication Technology* Vol. 2, n°3, 244 (2010).
25. L. dos Santos Coelho, *Chaos, Solitons and Fractals* **39**, 510 (2009).
26. R. Lozi, *J. Phys. Colloques* **39**, C5 (1978).
27. M. Misiurewicz, *Ann. N. Y. Acad. Sci.* **375**, 348, (1980).
28. A. Sakurai, *Taiwanese J. of Math.* Vol. 14, N° 4, 1609 (2010).
29. M. V. Petersen & H. M. Sorensen, *United States Patent* 7170997 (2007).
30. D. Ruggiero, D. Mascolo, I. Pedaci and P. Amato, *United States Patent Application* 20060251250 (2006).
31. R. Caponetto, L. Fortuna, S. Fazzino and M. G. Xibilia, *IEEE Transactions on Evolutionary Computation* Vol. 7, Iss. 3, 289 (2003).
32. L. dos Santos Coelho, *Chaos, Solitons and Fractals* **39**, 1504 (2009).
33. L. dos Santos Coelho, *Chaos, Solitons and Fractals* **41**, 594 (2009).
34. L. dos Santos Coelho and D. L. de Andrade Bernet, *Chaos, Solitons and Fractals* **42**, 634 (2009).
35. S. Jalilzadeh, H. Shayeghi, A. Safari and E. Aliabadi, *Proceedings of ECTI-CON 2009, 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* 24 (2009).
36. H. Shayeghi, S. Jalilzadeh, H. A. Shayanfar and A. Safari, *Proceedings of ECTI-CON 2009, 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* 40 (2009).
37. H. Shayeghi, H. A. Shayanfar, S. Jalilzadeh and A. Safari, *Energy Conversion and Management* **51**, No 7, 1572 (2010).
38. H. Shayeghi, H. A. Shayanfar, S. Jalilzadeh and A. Safari, *Energy Conversion and Management* **51**, No 12, 2678 (2010).
39. A. Safari, H. Shayeghi and H. A. Shayanfar, *International Journal on Technical and Physical Problems of Engineering* Vol. 1, Number 3, Issue 4, 44 (2010).
40. D. Davendra, I. Zelinka and R. Senkerik, *Computers and Mathematics with Applications* 60, 1088 (2010).
41. G. Manjunath, D. Fournier-Prunaret and A.-K. Taha, *Grazer Math. Bericht* Nr 354, 145 (2009).
42. P. Gora, A. Boyarsky, Md. S. Islam and W. Bahsoun, *SIAM J. Appl. Dyn. Syst. (electronic)* 5:1, 84 (2006).
43. J. Viega, *Proceedings of 19th Annual Annual Computer Security Applications Conference*, 129 (2003).

Published In *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*. Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Editors), *World Scientific Publisher, Singapore (2011)* pp. 93-125.

44. J. Viega, and M. Messier, *Secure programming cook book for C and C++* O'Reilly, Sebastopol CA (2003).

45. G. E. P. Box and M. E. Muller, *Ann. Math. Statist.* Vol. 29, No 2, 610 (1958).

46. R. Knop, *Comm. of ACM* Vol. 12, Issue 5, 28 (1969).