Chaotic Oscillators as the Pseudo-Random Numbers Generators

Roman Senkerik, Michal Pluhacek, Jakub Janostik and Zuzana Kominkova Oplatkova

Abstract—This paper investigates the utilization of the time-continuous chaotic system as the chaotic pseudo random number generators. (CPRNGs) Two selected chaotic oscillators are simulated, statistically analyzed and compared within this research study. Complex chaotic systems of interests are well known and widely studied UEDA oscillator and Van der Pol oscillator. Furthermore this paper also shows complex analysis of the influence of sampling rates to the distribution and dynamical sequencing during the generating of pseudo number numbers by means of both studied chaotic systems.

Keywords—Deterministic Chaos; Chaotic Oscillators, PRNG.

I. INTRODUCTION

GENERALLY speaking, the term “chaos” can denote anything that cannot be simply predicted deterministically. The deterministic chaos is an interesting phenomenon that is not based on the presence of random or any stochastic effects. It is clear from the structure of the chaotic systems equations (see the section 4), that no mathematical term expressing randomness is present there. The seeming randomness in deterministic chaos is related to the extreme sensitivity to the initial conditions, popularly known as the “butterfly effect” [1].

Till now, the chaos has been observed in many of various dynamical systems. Systems exhibiting deterministic chaos include, for example, economy models, air flows, weather, biological systems, many electronic circuits (Chua’s circuit), mechanical systems, such as double pendulum, magnetic pendulum, or so called billiard problem.

The idea of using chaotic systems instead of random processes (pseudo-number generators - PRNGs) has been presented recently in many research fields and in many applications with interesting results [2], [3].

Another research joining deterministic chaos and pseudorandom number generator has been done for example in [4]. Possibility of generation of random or pseudorandom numbers by use of the ultra weak multidimensional coupling of p 1-dimensional dynamical systems is discussed there.

Another paper [5] deeply investigate logistic map as a possible pseudorandom number generator and is compared with contemporary pseudo-random number generators. A comparison of logistic map results is made with conventional methods of generating pseudorandom numbers. The approach used to determine the number, delay, and period of the orbits of the logistic map at varying degrees of precision (3 to 23 bits). Another paper [6] proposed an algorithm of generating pseudorandom number generator, which is called (couple map lattice based on discrete chaotic iteration) and combine the couple map lattice and chaotic iteration. Authors also tested this algorithm in NIST 800-22 statistical test suits and for future utilization in image encryption. In [7] authors exploit interesting properties of chaotic systems to design a random bit generator, called CCCBG, in which two chaotic systems are cross-coupled with each other. A new binary stream-cipher algorithm based on dual one-dimensional chaotic maps is proposed in [8] with statistic proprieties showing that the sequence is of high randomness. Similar studies are also done in [9], [10] and [11].

II. MOTIVATION

Till now the deterministic chaos was observed in many of various dynamical systems (including evolutionary one) and in the last few years, it is also widely used to replace pseudo-number generators (PRNGs) in evolutionary algorithms (EAs) as well as many swarm based algorithms (SAs).

Recent research in chaos driven heuristics has been fueled with the predisposition that unlike stochastic approaches, a chaotic approach is able to bypass local optima stagnation. This is very important for successful utilization of evolutionary algorithms or any related heuristic. A chaotic approach generally uses the chaotic system in the place of a pseudo random number generator [12]. This causes the heuristic to map unique regions, since the chaotic system iterates to new regions. The very difficult task is then to select a very good chaotic system (either discrete map or time-continuous system) as the chaotic pseudo random number generator (CPRNG).

The initial concept of embedding chaotic dynamics into the evolutionary algorithms is given in [13]. Later, the initial study [14] was focused on the simple embedding of chaotic
systems in the form of chaos pseudo random number generator (CPRNG) for DE (Differential Evolution) and SOMA [15] in the task of optimal PID tuning

Several papers have been recently focused on the connection of heuristic and chaotic dynamics either in the form of hybridizing of DE with chaotic searching algorithm [16] or in the form of chaotic mutation factor and dynamically changing weighting and crossover factor in self-adaptive chaos differential evolution (SACDE) [17]. Also the PSO (Particle Swarm Optimization) algorithm with elements of chaos was introduced as CPSO [18] or CPSO combined with chaotic local search [19].

This idea was later extended with the successful experiments with chaos driven DE (ChaosDE) [20] - [24]. The concept of Chaos DE has proved itself to be a powerful heuristic also in combinatorial problems domain [25].

At the same time the chaos embedded PSO with inertia weigh strategy was closely investigated [26], followed by the introduction of a PSO strategy driven alternately by two chaotic systems [27] and novel chaotic Multiple Choice PSO strategy (Chaos MC-PSO) [28].

The primary aim of this work is not to develop a new type of pseudo random number generator, which should pass many statistical tests, but to try to test, analyze and compare the implementation of different natural chaotic dynamics as the CPRNGs, thus to analyze and highlight the different influences to the system, which utilizes the selected CPRNG (including the evolutionary computational techniques).

III. THE CONCEPT OF CPRNG

The general idea of CPRNG is to replace the default PRNG with the chaotic system. As the chaotic system is a set of equations with a static start position, we created a random start position of the system, in order to have different start position for different experiments. This random position is initialized with the default PRNG, as a one-off randomizer. Once the start position of the chaotic system has been obtained, the system generates the next sequence using its current position.

Generally there exist many other approaches as to how to deal with the negative numbers as well as with the scaling of the wide range of the numbers given by the chaotic systems into the typical range 0 – 1:

- Finding of the maximum value of the pre-generated long discrete sequence and dividing of all the values in the sequence with such a maxval number.
- Shifting of all values to the positive numbers (avoiding of ABS command) and scaling.
- Rotation of negative values around y axis (also avoiding ABS command).

IV. CHAOTIC OSCILLATORS

This section contains the description of time-continuous chaotic system (flows or oscillators), which were used as the chaotic pseudo random generators. In this research, direct sampled output iterations of the chaotic systems were used for the generation of real numbers scaled into the typical range for random function: <0 - 1>. Following chaotic systems were used: unmodified UEDA oscillator (1) and Driven Van der Pol Oscillator (2).

The x, y parametric plots of the chaotic systems are depicted in Fig. 1 (UEDA osc.) and Fig. 4 (Vander Pol osc.). The typical chaotic behavior of the utilized chaotic systems, represented by the examples of direct output for the variable x and y is depicted in Figures 2 and 3 (UEDA osc.) and Fig. 5 and 6 (Vander Pol osc.). Whereas Figures 7 and 8 represent the complex analysis of the influence of sampling rates to the distribution and dynamical sequencing during the generating of pseudo number numbers by means of both studied CPRNGs. These two aforementioned figures contain the chaotic dynamics from the range <0 - 1> sampled with the particular sampling rate – variable x and the histograms of the distribution of real numbers transferred into the range <0 - 1>.

A. UEDA Oscillator

UEDA oscillator is the simple example of driven pendulums, which represent some of the most significant examples of chaos and regularity.

The UEDA system can be simply considered as a special case of intensively studied Duffing oscillator that has both a linear and cubic restoring force. Ueda oscillator represents the both biologically and physically important dynamical model exhibiting chaotic motion. It can be used to explore much physical behavior in biological systems. [29]

The UEDA chaotic system equations are given in (1). The parameters are: \( a = 1.0 \), \( b = 0.05 \), \( c = 7.5 \) and \( \omega = 1.0 \) as suggested in [30].

\[
\begin{align*}
\frac{dx}{dt} &= y \\
\frac{dy}{dt} &= -ax^3 - by + c \sin \omega t
\end{align*}
\]

(1)

Fig. 1 x, y parametric plot of the UEDA oscillator
B. Van der Pol Oscillator

Van der Pol oscillator is the simple example of the limit cycles and chaotic behavior in electrical circuits employing vacuum tubes. Similarly to the UEDA oscillator, it can be used to explore physical (unstable) behaviour in biological sciences. [31].

In this paper, the forced, or commonly known as driven, Van der Pol oscillator is investigated. This system consist of the original Van der Pol oscillator definition with the added driving function $a \sin(\omega t)$, thus the differential equations have the form (2). The parameters are: $\mu = 0.2 \gamma = 8.0$, $a = 0.35$ and $\omega = 1.02$ as suggested in [30].

$$\begin{align*}
\frac{dx}{dt} &= y \\
\frac{dy}{dt} &= \mu(1 - x^2)y - x^3 + a \sin(\omega t)
\end{align*}$$

(2)
Fig. 7 Comparison of the influence of sampling rate to the distribution of numbers given by UEDA CPRNG; Left: Histogram of the distribution of real numbers transferred into the range <0 - 1>; Right: Example of the chaotic dynamics: range <0 - 1> generated by means of UEDA oscillator sampled with the particular sampling rate – variable x; Sampling rates from up to down: 0.1s, 0.5s, 1.0s, 2.0s.
Fig. 8 Comparison of the influence of sampling rate to the distribution of numbers given by Van der Pol oscillator; Left: Histogram of the distribution of real numbers transferred into the range $<0$ - $1>$; Right: Example of the chaotic dynamics: range $<0$ - $1>$ generated by means of Van der Pol oscillator sampled with the particular sampling rate – variable $x$; Sampling rates from up to down: 0.1s, 0.5s, 1.0s, 2.0s.
This paper was investigating the utilization of the time-
continuous chaotic system as the chaotic pseudo random
number generators. (CPRNGs) Totally two different chaotic
systems (oscillators) were simulated, statistically analyzed and
compared within this initial research study.

From the graphical comparisons, it follows that through
the utilization of different chaotic systems; entirely different
statistical characteristics of CPRNGs can be achieved. Thus
the different influence to the system, which utilizes the
selected CPRNG, can be chosen through the implementation
of particular inner chaotic dynamics given by the particular
time-continuous chaotic system.

Another important phenomenon was discovered – Only
sampling rate of 0.1s (and partially also 0.5s) keeps the
information about the chaotic dynamics (as in Figures 7 and
8). And as aforementioned in the motivation section of this
paper, by using of such chaotic dynamics driving the
heuristics (EAs and SAs), their performance, selection of
individual solutions for crossover and mutation process may
be significantly influenced by inner complex dynamics and
the overall heuristic algorithm may work better.

Another important fact was discovered – changing of
sampling rate for time-continuous systems, do not affect the
statistical distribution of pseudo-random numbers (for long
time generating – i.e. several thousands of samples), but it
strongly affect the existence of the complex chaotic dynamics
nature in the dynamical sequencing.

Furthermore chaotic systems have additional parameters,
which can by tuned. This issue opens up the possibility of
examining the impact of these parameters to generation of
random numbers, and thus influence on the results obtained by
means of either evolutionary techniques or different systems
from the softcomputing/computational intelligence field.

REFERENCES

Algorithms Researchers," in Evolutionary Algorithms and Chaotic
Systems, vol. 267, I. Zelinka, S. Celikovsky, H. Richter, and G. Chen,

systems engineering," Journal of Process Control, vol. 6, pp. 71-87,
1996.

water quality time series prediction," Environmental Modelling &


pseudoarandom number generators for periodicity induced by finite
precision floating-point representation," Chaos, Solitons & Fractals,

on CML and chaotic iteration," Nonlinear Dynamics, vol. 70, pp. 1589-
1592, 2012/10/01 2012.


