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 (PRGNs) 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

R.Senkerik, M. Pluhacek, J. Janostik and Z. Kominkova Oplatkova are with the Department of Informatics and Artificial Intelligence, Tomas Bata University in Zlin, Nad Stranemi 4511, 760 05 Zlin, Czech Republic, (phone: +420576035189; fax: +420576035279; e-mail: senkerik@fai.utb.cz).

This work was supported by Grant Agency of the Czech Republic - GACR P103/15/06700S, further by financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic and also by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089, partially supported by Internal Grant Agency of Tomas Bata University under the projects No. IGA/FAI/2015/057 and IGA/FAI/2015/061.

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].

$$\begin{aligned} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= -ax^3 - by + c\sin\omega t \end{aligned} \tag{1}$$

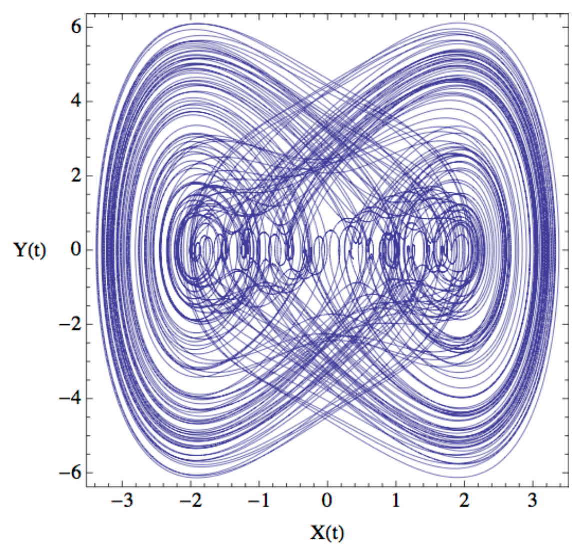

Fig. 1 x, y parametric plot of the UEDA oscillator

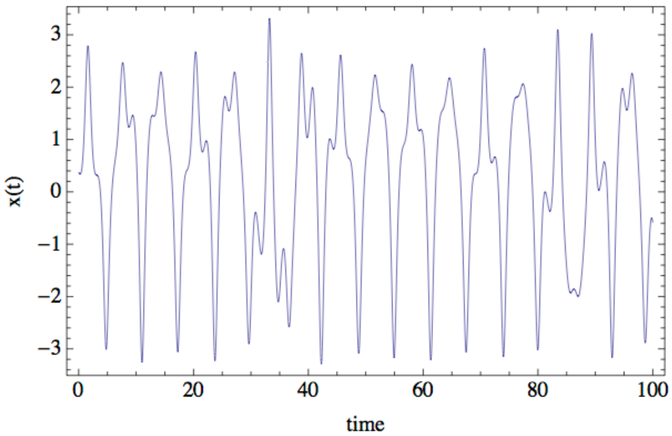

Fig. 2 Simulation of the UEDA oscillator (variable x – line-plot)

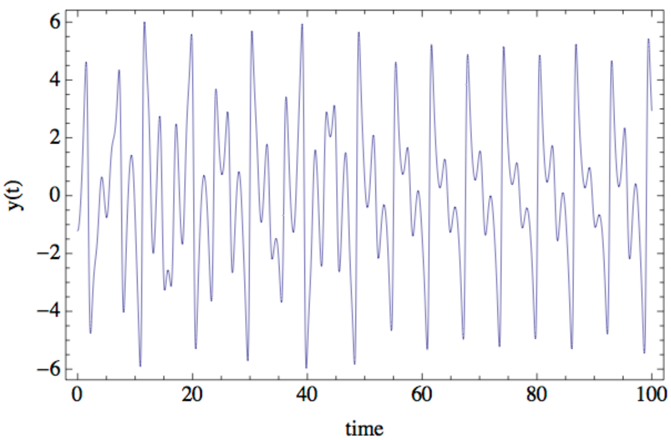

Fig. 3 Simulation of the UEDA oscillator (variable y – line-plot)

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(ωt), 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].

$$\begin{aligned} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= \mu\left(1-\gamma x^2\right)y - x^3 + a\sin\omega t \end{aligned} \tag{2}$$

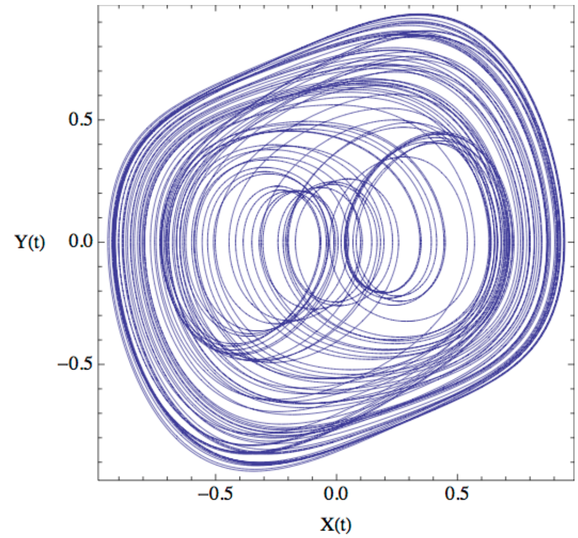

Fig.4 x, y parametric plot of the Van der Pol oscillator

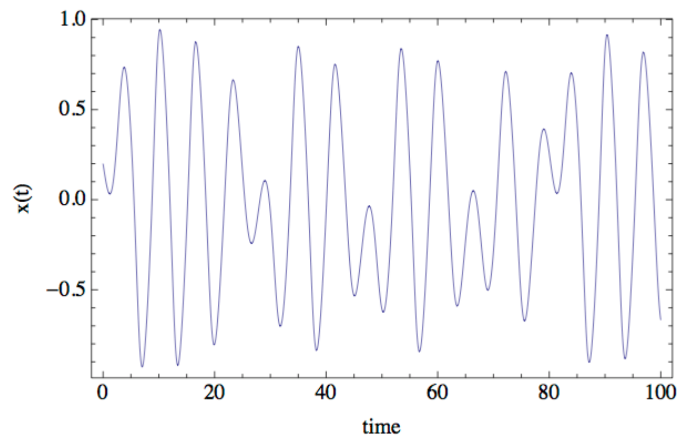

Fig. 5 Simulation of the Van der Pol oscillator (variable x – line-plot)

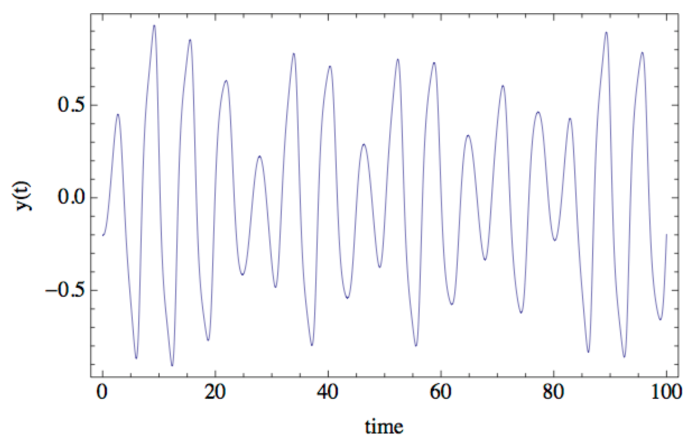

Fig. 6 Simulation of the Van der Pol oscillator (variable y – line-plot)

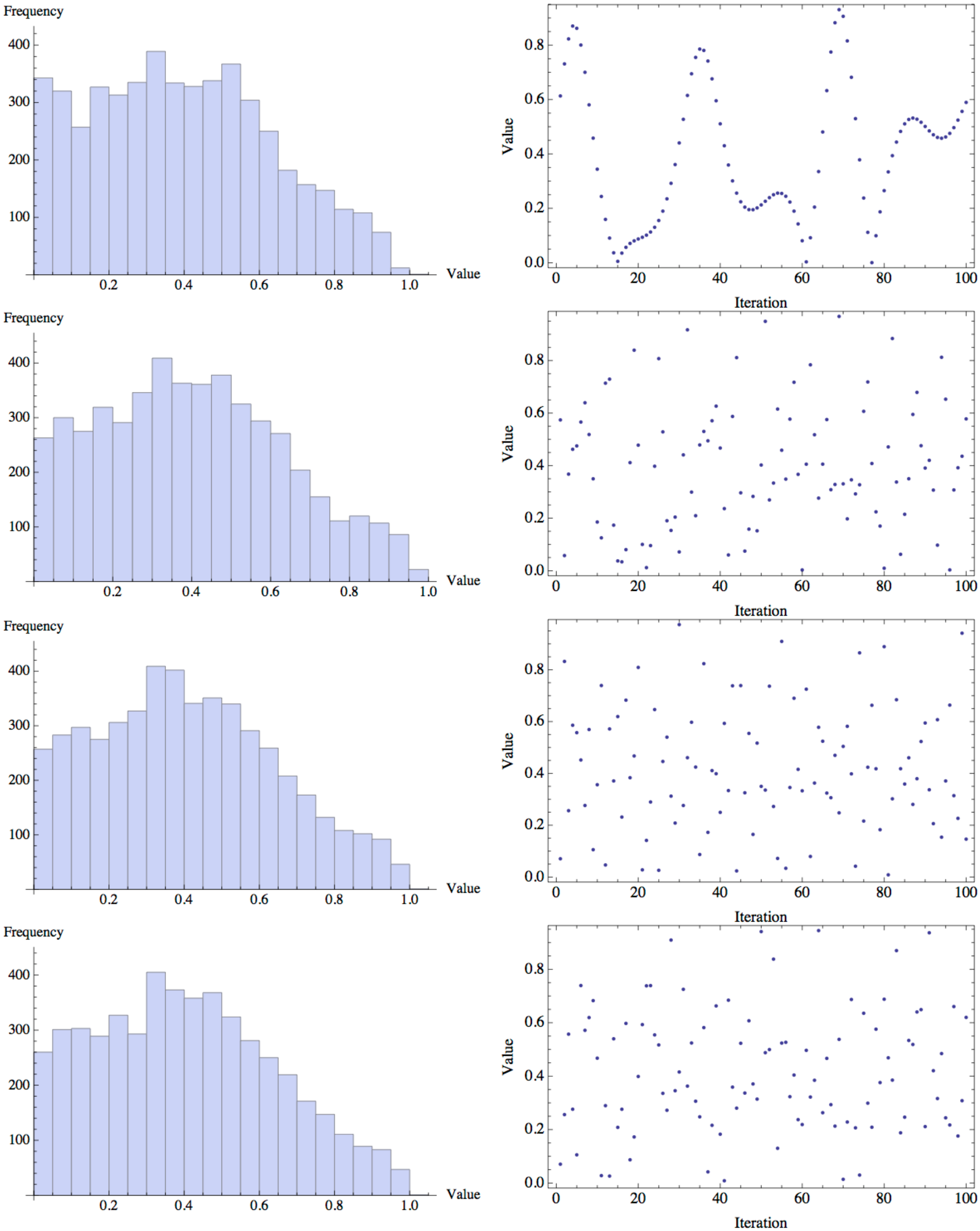

Fig. 7 Comparison of the influence of sampling rate to the distribution of numbers given by UEDA CPRNG; Left: Histogram of the distribution of real numbers transferred into the range <0 - 1>; Right: Example of the chaotic dynamics: range <0 - 1> generated by means of UEDA oscillator sampled with the particular sampling rate – variable x ; Sampling rates from up to down: 0.1s, 0.5s, 1.0s, 2.0s.

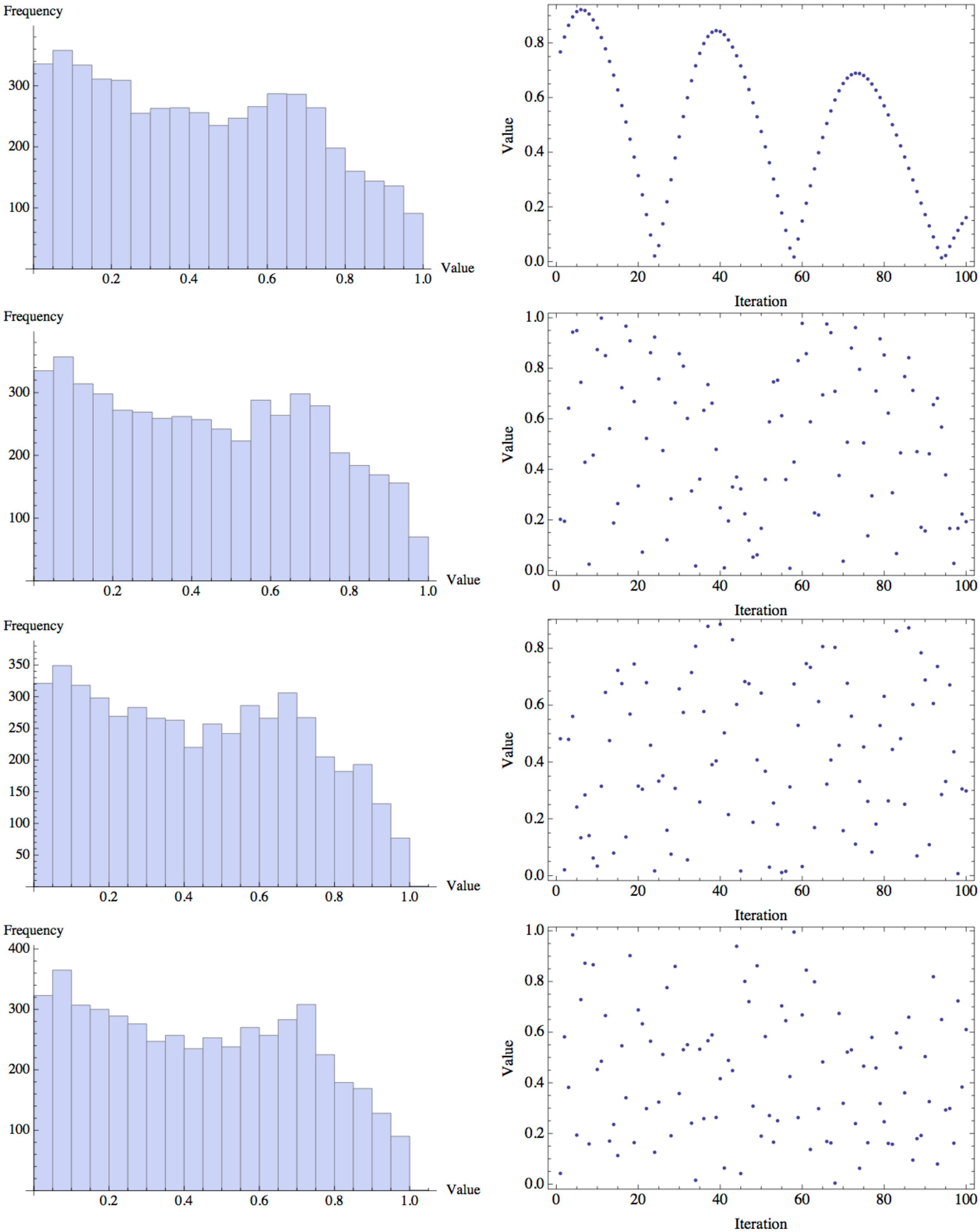

Fig. 8 Comparison of the influence of sampling rate to the distribution of numbers given by Van der Pol oscillator; Left: Histogram of the distribution of real numbers transferred into the range <0 - 1>; Right: Example of the chaotic dynamics: range <0 - 1> generated by means of Van der Pol oscillator sampled with the particular sampling rate – variable x ; Sampling rates from up to down: 0.1s, 0.5s, 1.0s, 2.0s.

V. Conclusion

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

[1] S. Celikovsky and I. Zelinka, "Chaos Theory for Evolutionary Algorithms Researchers," in *Evolutionary Algorithms and Chaotic Systems*. vol. 267, I. Zelinka, S. Celikovsky, H. Richter, and G. Chen, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 89-143.

[2] J. S. Lee and K. S. Chang, "Applications of chaos and fractals in process systems engineering," *Journal of Process Control,* vol. 6, pp. 71-87, 1996.

[3] J. Wu, J. Lu, and J. Wang, "Application of chaos and fractal models to water quality time series prediction," *Environmental Modelling & Software,* vol. 24, pp. 632-636, 2009.

[4] R. Lozi, "Emergence of Randomness from Chaos," *International Journal of Bifurcation and Chaos,* vol. 22, p. 1250021, 2012.

[5] K. J. Persohn and R. J. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," *Chaos, Solitons & Fractals,* vol. 45, pp. 238-245, 2012.

[6] X.-y. Wang and X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration," *Nonlinear Dynamics,* vol. 70, pp. 1589-1592, 2012/10/01 2012.

[7] K. P. Narendra, P. Vinod, and K. S. Krishan, "A Random Bit Generator Using Chaotic Maps," *International Journal of Network Security,* vol. 10, pp. 32 - 38, 2010.

[8] L. Yang and X.-Y. Wang, "Design of Pseudo-random Bit Generator Based on Chaotic Maps," *International Journal of Modern Physics B,* vol. 26, p. 1250208, 2012.

[9] M. Bucolo, R. Caponetto, L. Fortuna, M. Frasca, and A. Rizzo, "Does chaos work better than noise?," *Circuits and Systems Magazine, IEEE,* vol. 2, pp. 4-19, 2002.

[10] H. Hu, L. Liu, and N. Ding, "Pseudorandom sequence generator based on the Chen chaotic system," *Computer Physics Communications,* vol. 184, pp. 765-768, 2013.

[11] A. Pluchino, A. Rapisarda, and C. Tsallis, "Noise, synchrony, and correlations at the edge of chaos," *Physical Review E,* vol. 87, p. 022910, 2013.

[12] I. Aydin, M. Karakose, and E. Akin, "Chaotic-based hybrid negative selection algorithm and its applications in fault and anomaly detection," *Expert Systems with Applications,* vol. 37, pp. 5285-5294, 2010.

[13] R. Caponetto, L. Fortuna, S. Fazzino, and M. G. Xibilia, "Chaotic sequences to improve the performance of evolutionary algorithms," *IEEE Transactions on Evolutionary Computation,* vol. 7, pp. 289-304, 2003.

[14] D. Davendra, I. Zelinka, and R. Senkerik, "Chaos driven evolutionary algorithms for the task of PID control," *Computers & Mathematics with Applications,* vol. 60, pp. 1088-1104, 2010.

[15] I. Zelinka, "SOMA — Self-Organizing Migrating Algorithm," in *New Optimization Techniques in Engineering*. vol. 141, ed: Springer Berlin Heidelberg, 2004, pp. 167-217.

[16] W. Liang, L. Zhang, and M. Wang, "The chaos differential evolution optimization algorithm and its application to support vector regression machine," *Journal of Software,* vol. 6, pp. 1297- 1304, 2011.

[17] G. Zhenyu, C. Bo, Y. Min, and C. Binggang, "Self-Adaptive Chaos Differential Evolution," in *Advances in Natural Computation*. vol. 4221, L. Jiao, L. Wang, X.-b. Gao, J. Liu, and F. Wu, Eds., ed: Springer Berlin Heidelberg, 2006, pp. 972-975.

[18] L. d. S. Coelho and V. C. Mariani, "A novel chaotic particle swarm optimization approach using Hénon map and implicit filtering local search for economic load dispatch," *Chaos, Solitons & Fractals,* vol. 39, pp. 510-518, 2009.

[19] W.-C. Hong, "Chaotic particle swarm optimization algorithm in a support vector regression electric load forecasting model," *Energy Conversion and Management,* vol. 50, pp. 105-117, 2009.

[20] R. Senkerik, M. Pluhacek, I. Zelinka, Z. Oplatkova, R. Vala, and R. Jasek, "Performance of Chaos Driven Differential Evolution on Shifted Benchmark Functions Set," in *Proc. International Joint Conference SOCO'13-CISIS'13-ICEUTE'13*. vol. 239, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A. C. P. L. F. Carvalho*, et al.*, Eds., ed: Springer International Publishing, 2014, pp. 41-50.

[21] R. Senkerik, D. Davendra, I. Zelinka, M. Pluhacek, and Z. Kominkova Oplatkova, "On the Differential Evolution Drivan by Selected Discrete Chaotic Systems: Extended Study," in *Proc. 19th International Conference on Soft Computing, MENDEL 2013*, 2013, pp. 137-144.

[22] R. Senkerik, M. Pluhacek, Z. K. Oplatkova, D. Davendra, and I. Zelinka, "Investigation on the Differential Evolution driven by selected six chaotic systems in the task of reactor geometry optimization," in *Proc. 2013 IEEE Congress on Evolutionary Computation (CEC)*, 2013, pp. 3087-3094.

[23] R. Senkerik, M. Pluhacek, D. Davendra, I. Zelinka and Z. Oplatkova, " Chaos Driven Evolutionary Algorithm: A New Approach for Evolutionary Optimization," *International Journal of Mathematics and Computers in Simulation*, vol. 7, pp. 363-368, 2013.

[24] R. Senkerik, I. Zelinka, M. Pluhacek, and Z. Oplatkova, "Evolutionary Control of Chaotic Burgers Map by means of Chaos Enhanced Differential Evolution," *International Journal of Mathematics and Computers in Simulation*, vol. 8, pp. 39-45, 2014.

[25] D. Davendra, M. Bialic-Davendra, and R. Senkerik, "Scheduling the Lot-Streaming Flowshop scheduling problem with setup time with the chaos-induced Enhanced Differential Evolution," in *Proc. 2013 IEEE Symposium on Differential Evolution (SDE)*, 2013, pp. 119-126.

[26] M. Pluhacek, R. Senkerik, D. Davendra, Z. Kominkova Oplatkova, and I. Zelinka, "On the behavior and performance of chaos driven PSO algorithm with inertia weight," *Computers & Mathematics with Applications,* vol. 66, pp. 122-134, 2013.

[27] M. Pluhacek, R. Senkerik, I. Zelinka, and D. Davendra, "Chaos PSO algorithm driven alternately by two different chaotic maps - An initial study," in *Proc. 2013 IEEE Congress on Evolutionary Computation (CEC)*, 2013, pp. 2444-2449.

[28] M. Pluhacek, R. Senkerik, and I. Zelinka, "Multiple Choice Strategy Based PSO Algorithm with Chaotic Decision Making – A Preliminary Study," in *Proc. International Joint Conference SOCO'13-CISIS'13-ICEUTE'13*. vol. 239, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A. C. P. L. F. Carvalho*, et al.*, Eds., ed: Springer International Publishing, 2014, pp. 21-30.

[29] L. Bharti and M. Yuasa. Energy Variability and Chaos in Ueda Oscillator.
Available: http://www.rist.kindai.ac.jp/no.23/yuasa-EVCUO.pdf

[30] J. C. Sprott, *Chaos and Time-Series Analysis*: Oxford University Press, 2003.

[31] T. Kanamaru, "Van der Pol oscillator," *Scholarpedia,* vol. 2, p. 2202, 2007.