FPGA Implementation of an Autonomous Chaotic System using Euler Algorithm

Subodh Kumar Pandey
Research Scholar
Department of Electronics & Communication Engineering
Rabindranath Tagore University, Chiklod Road,
Raisen-464993 (M.P.)

Sanjeev Kumar Gupta
Professor and Dean
Department of Electronics & Communication Engineering
Rabindranath Tagore University, Chiklod Road,
Raisen-464993 (M.P.)

ABSTRACT: ***Now a days Chaos based systems plays an important role specifically in secure communication and cryptography. Chaotic systems have wide applications in random numbers generators, image encryption, Optical secure circuits, and quantum applications. This paper presents FPGA implementation of Autonomous Pandey-Baghel-Singh chaotic signal generators using Euler's algorithm. Numerical algorithm is implemented using Verilog and tested with Xilinx vivado 17.3 design suite in Artix-7 Nexus 4 DDR and Basys 3. Performance of the FPGA based chaotic generators is analyzed using 10^6 data sets with the operating frequency up to 359.71 MHz.***

Key Words - Chaotic Generators, Euler algorithm, FPGA

I. INTRODUCTION

Presently chaos systems are playing an important role specifically in secure communication and cryptography. Chaos generators is a fundamental structure of a chaos based systems and may be implemented in analog or digital form. The analog based design of chaos based generators is sensitive to initial conditions and acquires a large chip area. Digital based design chaotic systems eliminates these problems and can be better synchronized. FPGA implementation is more flexible architecture so have low cost test cycle and found more useful in chaos based engineering applications [1-7].

In the II section of the study the numerical model of Pandey-Baghel-Singh Chaos System (PBSCS) is presented using Euler algorithm and FPGA model of PBSCS is introduced. In the III section simulation results has been presented and analyzed. In section IV conclusion is given.

II. FPGA IMPLEMENTATION OF PBSCS

Pandey-Baghel-Singh Chaos System (PBSCS) [8] is defined by the set of differential equation (1).

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -ax - by - cz - x^2 \end{aligned} \quad (1)$$

The initial condition for the PBSCS is x = 0.1, y = 0 and z = 0.

A. Numerical model using Euler algorithm

For the numerical model using Euler algorithm initial value of x (n), y (n) and z (n) are taken as x (n) = x (t_0) = 0.1, y (n) = y (t_0) = 0 and z(n) = z(t_0) = 0, and the numerical model for PBSCS is described in the Eq.2.

$$\begin{aligned} x(n+1) &= x(n) + h.y(n) \\ y(n+1) &= y(n) + h.z(n) \\ z(n+1) &= z(n) + h.\{-a.x(n) - b.y(n) - c.z(n) - x(n)^2\} \end{aligned} \quad (2)$$

.

Euler based chaotic generator's 2nd level diagram is presented in Fig. 2 It have one multiplexer and a chaotic generator unit which is FPGA based. The multiplexer is used to provide initial condition signals. For successive operation it is provided by the output signals. When enable is at logic high, the output generates chaotic signal.

B. FPGA Implementation of Autonomous Chaotic Generator based on Euler algorithm

For all mathematical operations Verilog codes has been generated and the PBSCS has been modeled using Euler algorithm with 32- bit IEEE 754-1985 standard on FPGA. Top-level diagram of Euler based units have been shown in Fig. 1. A 32-bit input has been used and initial conditions are set in the beginning phase. The 32-bit signal are used as input parameter. There are three output signals of 32-bit each and ready is taken as one bit control signals for the proposed Euler based chaotic generators.

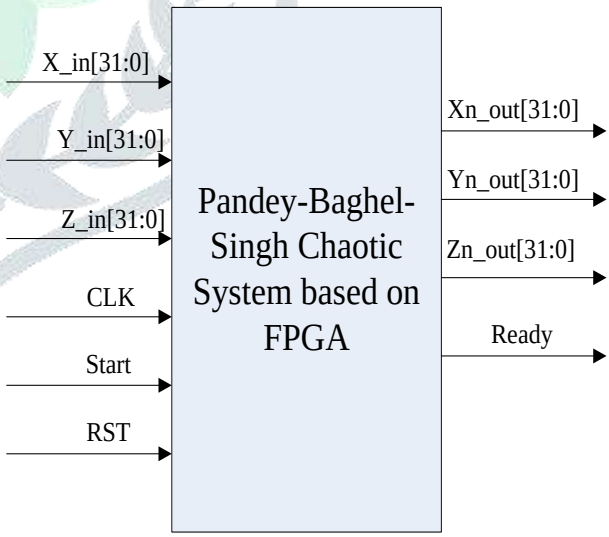

Fig.1 Top level design of PBS Chaotic System based on FPGA

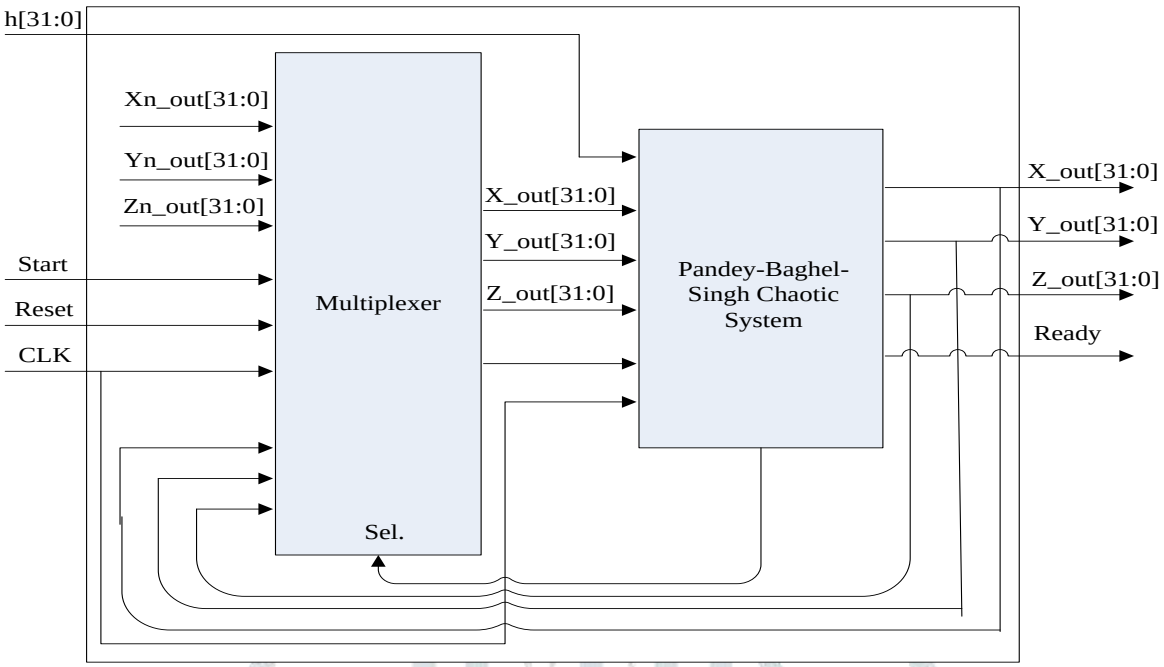

Fig.2 second level diagram of PBSCS

Euler based third level diagram of the chaotic generator is presented in Fig. 3. The system consist of multiplexer, function f, multiplier, adder/subtracter and filter. The system equations are calculated in the f unit and the output is multiplied by h in the multiplier. The output of the multiplier and previously generated signals by the generators are added in the adder unit. The undesired signal are eliminated at the filter stage.

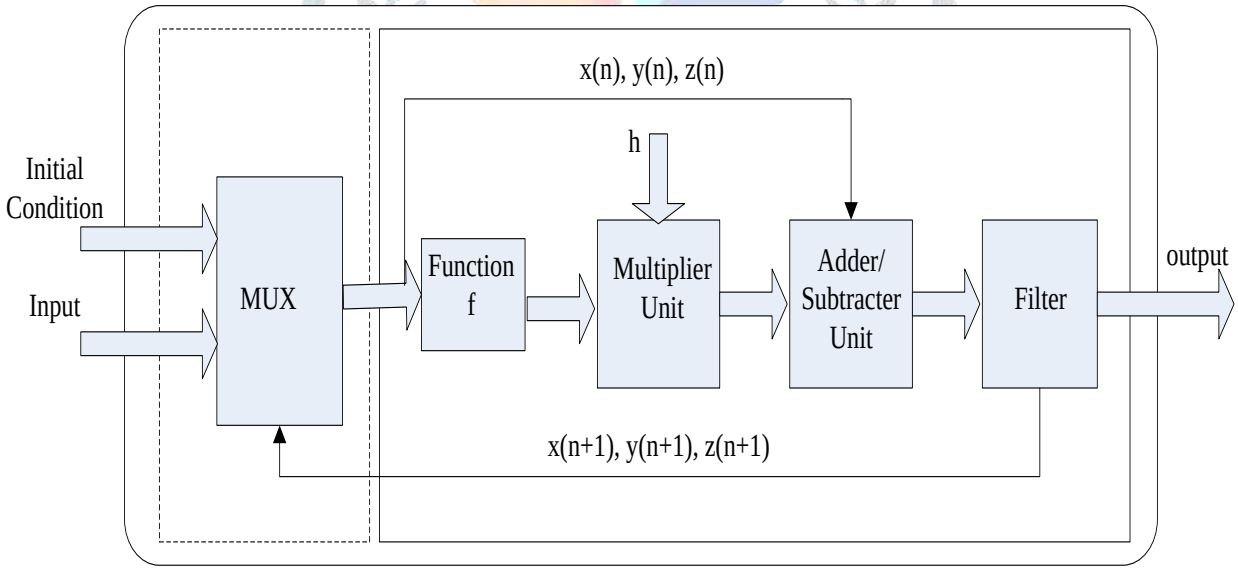

Fig. 3 Third level diagram of PBSCS

III. SIMULATION RESULTS OF PBSCS

The Euler algorithm based PBS Chaotic generator have been synthesized for the Nexus 4 DDR XC7A100TCSG-1 (Artix7) and Basys3 (Artix7) from the Xilinx vivado v.2017.3 design suite. FPGA chip related Parameters and clock speed of the system have been analysed. The simulation results of the Euler based PBSCS is presented in the Fig. 6 and Fig. 7. The simulation results are presented in hexadecimal format to analyse the results. The phase portraits of the system is generated by the data set are given in fig. 8 (a-c). The Nexus 4 DDR XC7A100TCSG-1 (Artix7) and Basys3 (Artix7) chip speed and other statistics which are obtained for the Euler algorithm is given in table 1. For the optimize result with the use of 2181 LUT's and 3907 registers the fastest clock period of the Euler based chaotic generator is 2.78 ns and the maximum frequency achieved is 359.71 MH

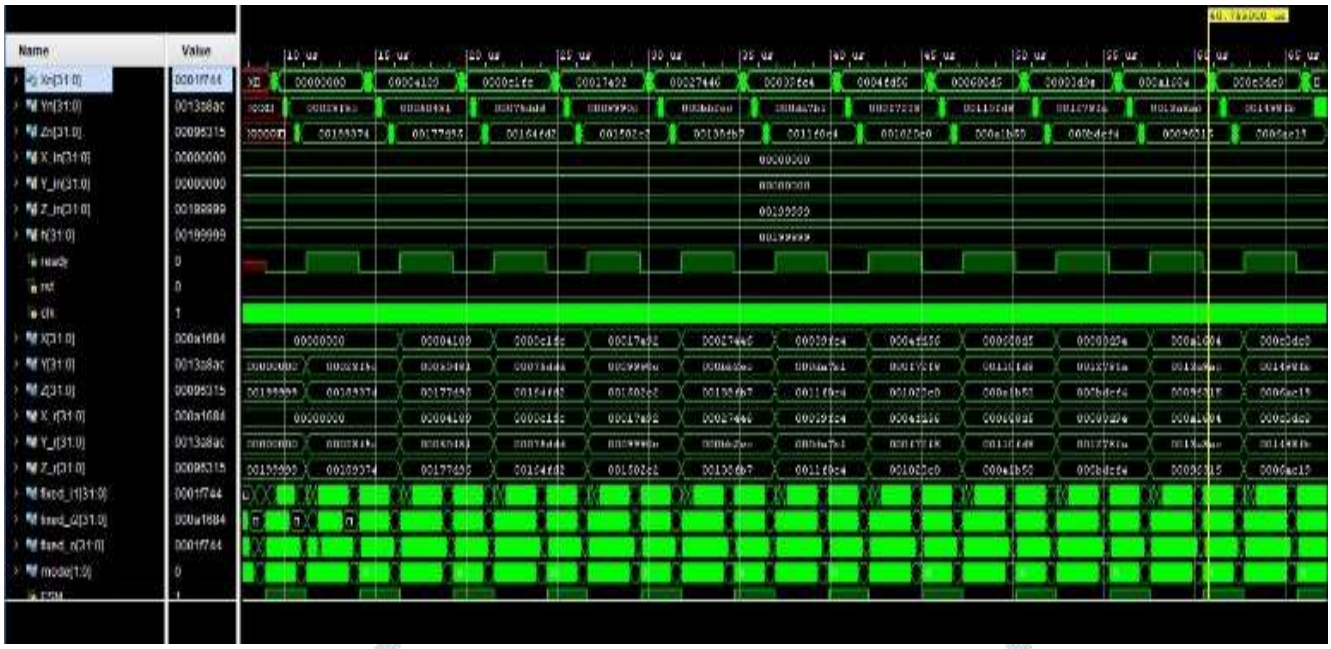

Fig.6 Timing simulation results of EULER based PBSCS obtained from Xilinx Vivado 17.3

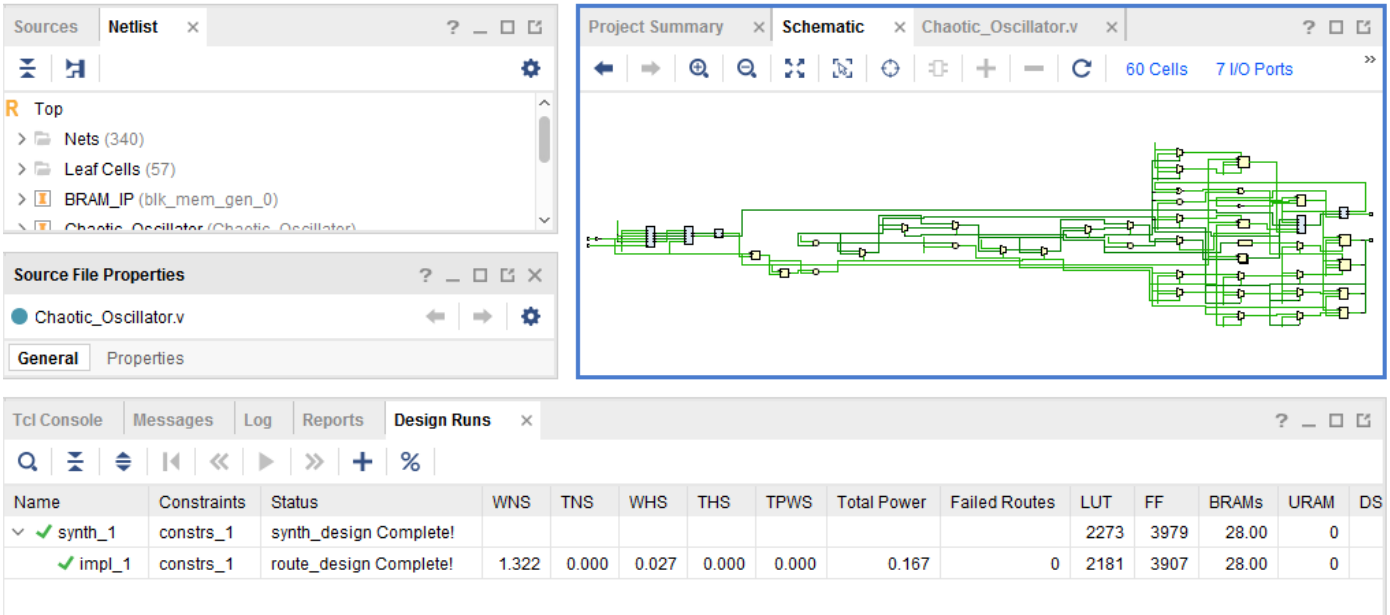

Fig.7 Simulation result of PBSCS on Vivado 17.3

Table 1: Final report of the resources consumption

Resource	No.
No. of DSP	2
LUT's used	2181
bonded IOBs used	32
BRAMs used	28
Flip Flops used	3907
Total On-chip Power(W)	0.167
Worst Negative Slack	1.322

V. CONCLUSION

The Euler algorithm based PBS Chaotic generator have been synthesized using the Nexus 4 DDR XC7A100TCSG-1 (Artix7) and Basys3 (Artix7) from the Xilinx Vivado v.2017.3 design suite. For the optimize result with the use of 2181 LUT's and 3907 registers the fastest clock period of the Euler based chaotic generator is 2.78 ns and the maximum frequency achieved is 359.71 MHz. The phase portraits generated for the FPGA based generator are similar to PBSCS designed on analog platform.

REFERENCES

[1] Ismail K., A. Tuaran O, Ihsan Pehlivan, "Implementation of FPGA-based real time novel chaotic oscillator", Nonlinear dynamics (2014) ; pp. 49-59.

[2] Murat Tunaa, Can Bülent Fidan, "Electronic circuit design, implementation and FPGA-based realization of a new 3D chaotic system with single equilibrium point", Optic Elsevier Optik (2016) pp. 11786–11799.

[3] S. Banerjee, J. Kurths, "Chaos and cryptography: a new dimension in secure communications", Eur. Phys. J. Spec. Top. , (2014) pp. 1441–1445.

[4] I. Koyuncu, A.T. Ozcerit, I. Pehlivan, "An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system", Optoelectron. Adv. Mater. Rapid Commun. (2013) pp. 635–638.

[5] L. Merah, A. Ali-pacha, N.H. Said, "A pseudo random number generator based on the chaotic system of Chua's circuit and its real time", FPGA Implementation (2013) pp. 2719–2734.

[6] S. C¸ ic¸ ek, A. Ferikog˘lu, I˙. Pehlivan, "A new 3D chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application", Optik – Int. J. Light Electron Opt. (2016) pp. 4024–4030.

[7] M. Tuna, I. Koyuncu, C.B. Fidan, I. Pehlivan, "Real time implementation of a novel chaotic generator on FPGA", in: 2015 23rd Signal Processing and Communications Applications Conference (SIU), IEEE, 2015, pp. 698–701.

[8] Alpana Pandey, R. K. Baghel, R.P. Singh, "Analysis and Circuit Realization of a New Autonomous Chaotic System", International Journal of Electronics and Communication Engineering. ISSN 0974-2166 Volume 5, Number 4 (2012), pp. 487-495