Heun Algorithm based FPGA Realization of Chaotic Generator

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 chaotic systems have an important role in secure communication and cryptography. As FPGA implementation have certain advantages over analog one, different chaotic system like chaotic oscillator, True random number generators and chaotic systems used in image processing, optical circuits for secure communications were successfully realized in FPGA. This paper presents FPGA implementation of Autonomous Pandey-Baghel-Singh chaotic signal generators using Heun algorithm. Numerical solution of Differential equation system is obtained and coded in 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 maximum operating frequency achieved up to 359.71 MHz.**

Key Words - Chaotic Generators, Heun algorithm, FPGA

I. INTRODUCTION

Chaos generator is a fundamental block of any chaos based system. Basically chaos based system are used in secure communication and cryptography. Recently implementation of FPGA based real time chaotic oscillator using different numerical algorithm were presented and it was shown that the processing speed of FPGA is much higher due to parallel processing capabilities. Hence it may be interesting to see the performance of FPGA based different chaotic systems as the analog based design of chaos based generators is sensitive to initial conditions and acquires a large chip area. To avoid these problems Digital based design chaotic systems using FPGA can be implemented as FPGA implementation is more flexible architecture and have low cost test cycle and found more useful in chaos based engineering applications [1-7].

In II section of the paper presented the Pandey-Baghel-Singh Chaos System (PBSCS) is presented along with their x, y and z signals and their phase portraits [8]. In the III section the mathematical models of PBSCS is numerically obtained with Heun algorithm and FPGA model of PBSCS is introduced. In the IV section simulation results has been presented and analyzed. In section V conclusion is given.

II. INTRODUCTION TO PANDEY- BAGHEL-SINGH CHAOS SYSTEM

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

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

In the system two equilibrium points as (0, 0, 0) and (-1, 0, 0) were shown for the constants a = 1, b = 1.1, and c = 0.4. The equilibrium point (0, 0, 0) have the Eigen values -0.745, 0.162+j1.147 and 0.162-j1.147. For the equilibrium point (-1, 0, 0) the Eigen values shown are 0.589, -0.504+j1.20, and -0.504-j1.20. The system is designed for the initial condition x = 0.1, y = 0 and z = 0. The time series results and phase portraits of this system are shown in Fig. 1 and Fig. 2 (a-c) respectively.

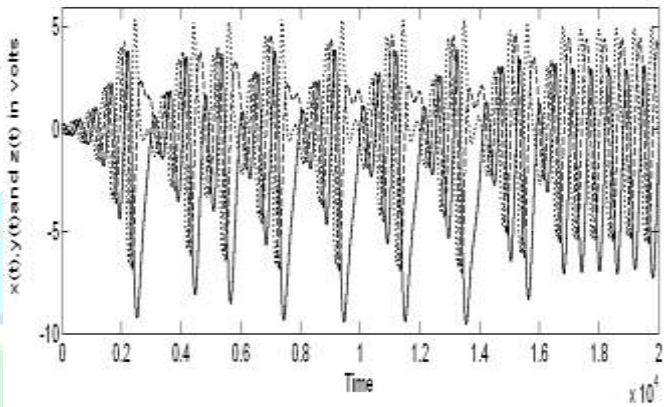
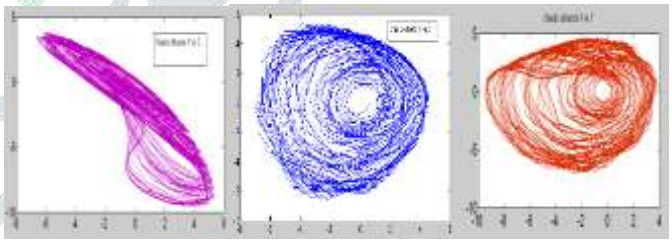


Fig 1: Time domain representation of x, y and z signals of PBSCS.



(a) (b) (c)

Fig 2: (a) x-y phase portrait, (b) y-z phase portrait, (c) x-z phase portrait

III. HEUN BASED NUMERICAL MODEL OF PBSCS AND ITS FPGA IMPLEMENTATION

For FPGA implementation of the system the numerical model is obtained using Heun algorithm and coded in Verilog.

A. Numerical model using Heun algorithm

For the numerical model using Heun algorithm initial value of x (n), y (n) and z (n) are taken as x (t_0) = x (n) = 0.1, y (t_0) = y (n) = 0 and z(t_0) = z(n) = 0,

The Heun algorithm have two successive stages. In the first stage $x(n^0+1)$ is calculated and $x(n+1)$ the value after steps h is calculated using previous values $x(n^0+1)$ and$x(n)$. The

mathematical model of PBS chaotic system is described by the following Eq.2.

$$x(n^0+1) = x(n) + h.y(n)$$
$$x(n+1) = x(n) + h\{y(n) + x(n^0+1)\}/2 \quad (2)$$
$$y(n^0+1) = y(n) + h.z(n)$$
$$y(n+1) = y(n) + h\{z(n) + y(n^0+1)\}/2$$
$$z(n^0+1) = z(n) + h\{-a.x(n) - b.y(n) - c.z(n) - x(n)^2\}$$
$$z(n+1) = z(n) + h.[\{-a.x(n) - b.y(n) - c.z(n) - x(n)^2\} + z(n^0+1)]/2$$

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

The PBSCS has been modeled using Heun algorithm and implemented with 32- bit IEEE 754-1985 standard on FPGA. Verilog modeling have been generated from IP core in Vivado design suite for the floating point multiplication, addition and subtraction modules. Top-level diagram of Heun based units have been shown in Fig. 3. 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. Three 32-bit output signals (Xn_out), (Yn_out) and (Zn_out) are there and ready is taken as three one bit control signals for the proposed Heun based chaotic generators.

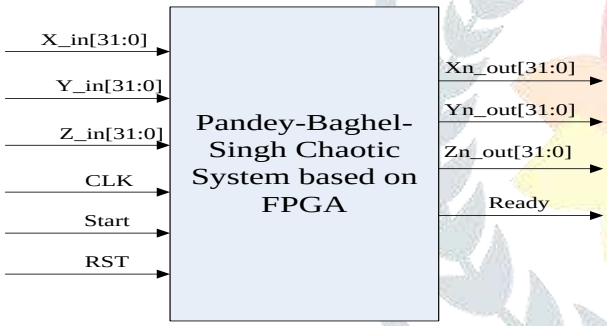


Fig.3 Top level design of PBS Chaotic System based on FPGA

The second level block diagram of the Heun based chaotic generator is presented in Fig. 4 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.

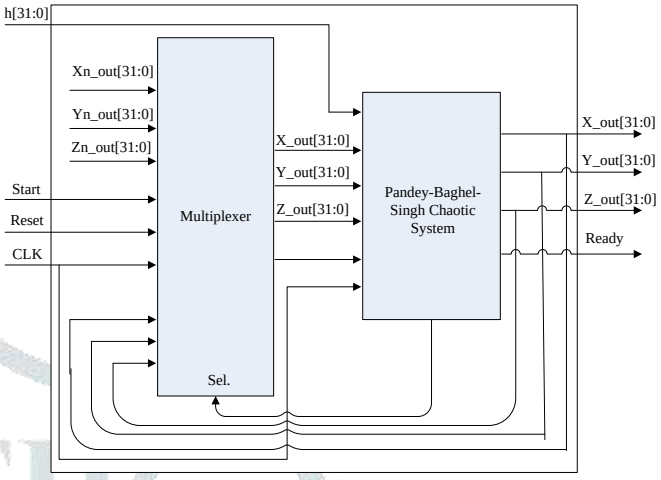


Fig.4 second level design of PBSCS based on FPGA

The third level block diagram of the Heun based chaotic generator is given in Fig. 5. The proposed generator consist of multiplexer, function f^0, multiplier, adder, f, Divider and filter stages. The PBSCS equation are calculated by f^0 stage with the help of MUX unit which provides control signal. After multiplication with h the output is added with the previous generated signal $x(n), y(n)$ *and* $z(n)$ by the generator unit. The output of this adder stage is applied to f stage which calculate the equation of PBSCS. The output of this stage and output of f^0 are adder-II stage. Further the output of the adder-II stage divided in the divider stage. In adder-III stage output of the chaotic generator from MUX stage and divider stage are added. The Heun based chaotic generator works in sequential order which generates the first value after 118 clock cycles.

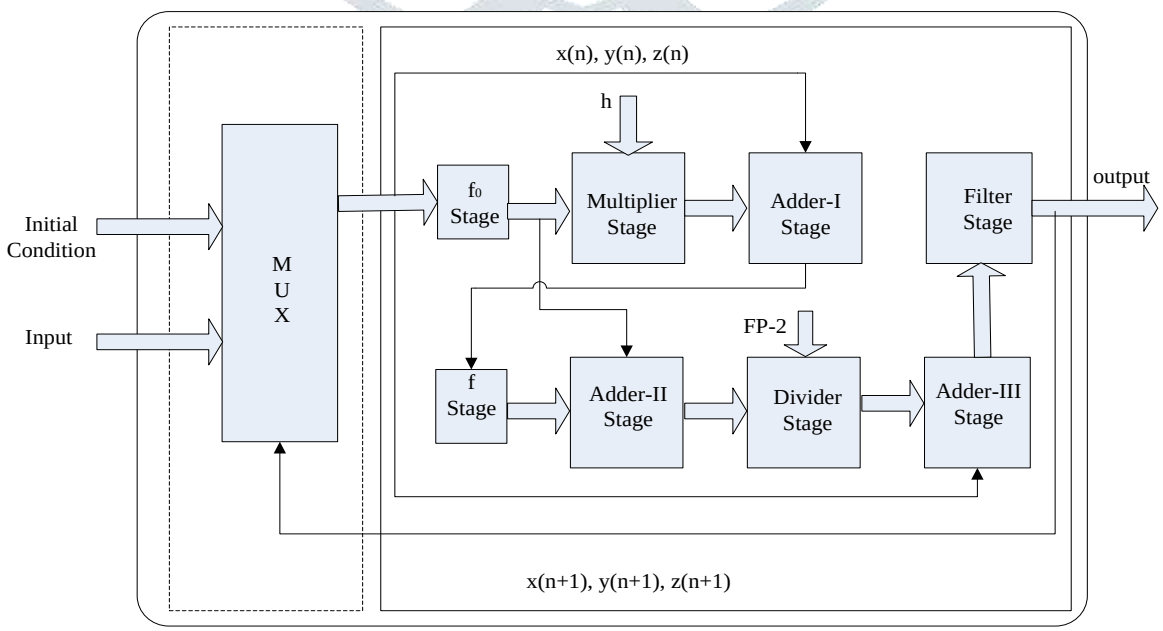


Fig. 5 Third Level design of Heun based PBSCS Generator Unit

IV. SIMULATION RESULTS OF PBS CHAOTIC GENERATOR

The Heun 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 Heun 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 Heun algorithm is given in table 1. For the optimize result with the use of 2973 LUT's and 4979 registers the fastest clock period of the Heun based chaotic generator is 2.78 ns and the maximum frequency achieved is 359.71 MHz.

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

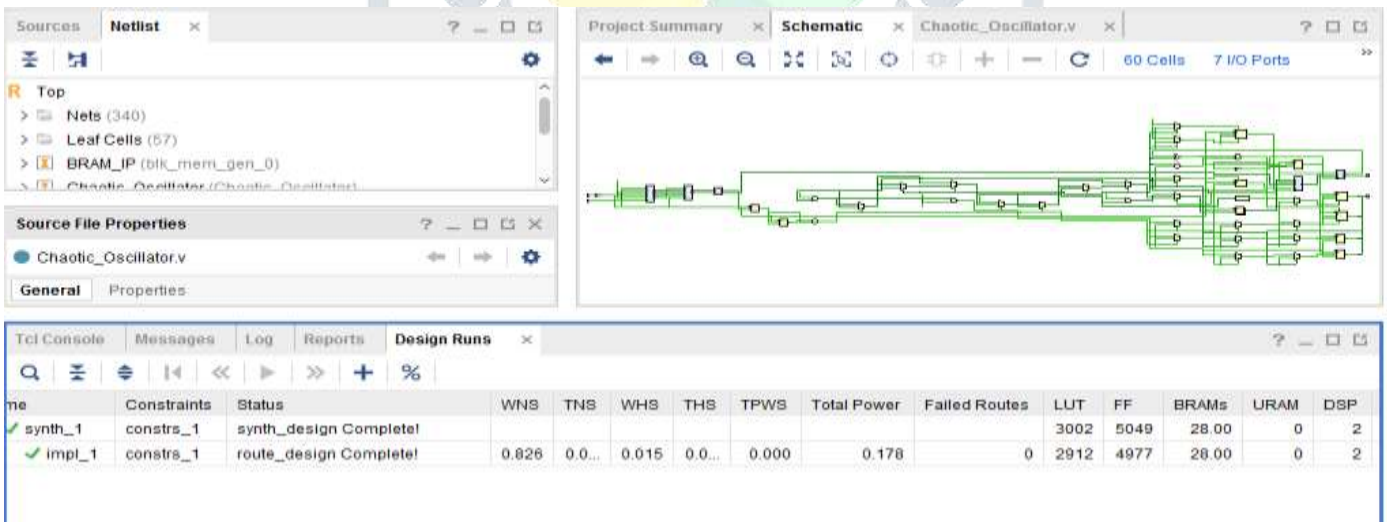
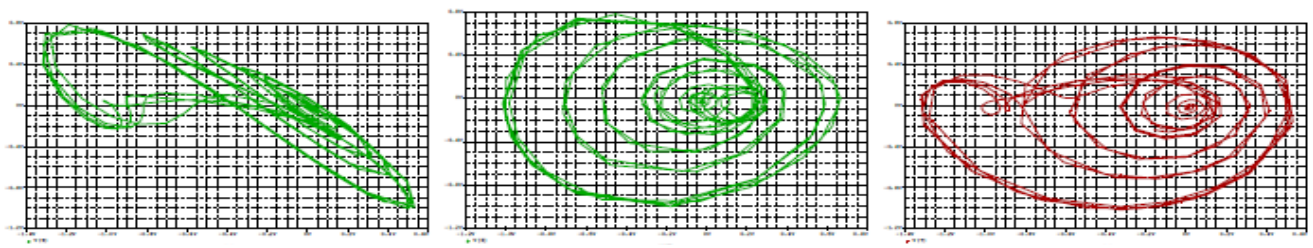


Fig.7 Simulation result of PBSCS on Vivado 17.3



(a) (b) (c)

Fig. 8 (a) x-y phase portrait, (b) y-z phase portrait, (c) x-z phase portrait

Maximum frequency (MHz)	359.71
No. of DSP	2
Number of 4 input LUTs	2912
Number of bonded IOBs	32
Number of BRAMs	28
Number of Slice Flip Flops	4977
Total On-chip Power(W)	0.178
Worst Negative Slack	0.826

Table 1: Final report of the resources consumption

V. CONCLUSION

The Heun 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 2912 LUT's and 4977 registers the fastest clock period of the Heun 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.