Compact Multiplier-less CORDIC-Based on FPGA Implementation of a Sine map for Chaotic Applications

Sara S. Abou Zeid*, Hisham M. Elrefai*, Wafaa S. Sayed**, **Lobna A. Said** *
and Ahmed G. Radwan ***

*Nanoelectronics Integrated Systems Center (NISC), Nile University, Giza, Egypt
**Engineering Mathematics and Physics Dept., Faculty of Engineering, Cairo University, Egypt
***School of Engineering and Applied Sciences, Nile University, Giza, Egypt

Abstract. This paper proposes a new modified sine chaotic map and implements both the conventional sine map and the proposed modified map on hardware. The proposed modified sine map exhibits continuous chaotic behavior against all values of the main system parameter. This is beneficial in pseudo-random number generation and encryption applications regarding system key design and ensuring chaotic behavior. The chaotic behavior of both maps is validated using time series, bifurcation diagrams, and maximum Lyapunov exponent. A reconfigurable CORDIC hardware block is used to compute the transcendental mathematical functions by employing shift-add and sub-operations. While the sin function is computed in circular rotation mode, the multiplication operation is computed in linear vectoring mode. The proposed hardware architecture is multiplier-less and, hence, it does not consume any DSPs. The sine and modified sine maps are realized on Xilinx Artix-7 FPGA board using Verilog HDL, yielding throughputs of 0.342 and 0.312 GBit/s, respectively.

Introduction

Many natural systems, such as fluid movement, rapid heartbeat, weather, and climate, exhibit chaotic behavior. Additionally, it happens on its own in some artificially constructed systems, such as the movement of people in the streets and the movement of air. Chaotic systems have vast importance which gives a focus to trying to implement them to aid in many applications such as encryption (Cryptography) which is mainly based on the unpredictability of the algorithm and output which requires a complex chaotic system to be reliable [1]. also, in [2] two image encryption applications are introduced based on the Sine map. Another use of the chaotic system is in the Robotics field which needs many cases and scenarios for the trial-and-error process to learn how to interact with many use cases [3]. Several research works in the literature presented chaotic maps with trigonometric nonlinearities, yet only a few of them implemented it on Hardware platforms. Zhongyun et al. implemented the Sine Chaotification Model (SCM) on FPGA. SCM increases the chaotic range and improves the dynamic complexity of the one-dimensional (1D) chaotic maps. In addition, it widens the parameters range corresponding to chaotic behavior making the maps more suitable for Pseudo-Random Number Generators [4]. Zhongyun et al. also implemented Sine Transform Based Chaotic System (STBCS), which combines the outputs of two chaotic maps on FPGA. STBCS results in new 1D maps with better complexity, range, and unpredictability [5]. The implementation of CORDIC for the sine function provides a significant improvement in the resource utilization of the FPGA, CORDIC only calculates the function using adders and shifters [6]. In this paper, the proposed solution focuses on implementing a modified sine map based on CORDIC for the design of Pseudo-Random Number Generators (PRNG) and encryption systems.

Results and discussion

The proposed designs for the modified sine map and sine map are interpreted in the hardware language Verilog HDL and are synthesized by using Xilinx Vivado targeting Xilinx Artix-7 FPGA board. The designs achieve a throughput of 0.342 and 0.312 Gbit/s for sin and modified sine maps, respectively. The number of LUTs used in the case of the sine map is 6459 and for the modified sine map is 6918. The proposed implementation uses the Reconfigurable multiplier-less CORDIC in [1] to calculate the sine function and the multiplication. As a result, the proposed architecture does not consume any DSPs. Also in [6] a summary of Reconfigurable CORDIC FPGA result.

References

[1] Ismail, S. M., Said, L. A., Rezk, A. A., Radwan, A. G., Madian, A. H., Abu-Elyazeed, M. F., & Soliman, A. M. (2017). Generalized fractional logistic map encryption system based on FPGA. AEU-International Journal of Electronics and Communications, 80, 114-126.

[2] S. K. Abd-El-Hafiz, A. G. Radwan, and S. H. AbdEl-Haleem, "Encryption applications of a generalized chaotic map," Applied Mathematics & Information Sciences, vol. 9, no. 6, p. 3215, 2015.

[3] Zang X, Iqbal S, Zhu Y, Liu X, Zhao J. Applications of Chaotic Dynamics in Robotics. International Journal of Advanced Robotic Systems. 2016;13(2).

[4] Z. Hua, B. Zhou and Y. Zhou, "Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation," in IEEE Transactions on Industrial Electronics, vol. 66, no. 2, pp. 1273-1284, Feb. 2019.

[5] Z. Hua, B. Zhou and Y. Zhou, "Sine-Transform-Based Chaotic System With FPGA Imple-mentation," in IEEE Transactions on Industrial Electronics, vol. 65, no. 3, pp. 2557-2566, March 2018.

[6] NS. M. Mohamed, W. S. Sayed, A. G. Radwan and L. A. Said, "FPGA Implementation of Reconfigurable CORDIC Algorithm and a Memristive Chaotic System With Transcendental Nonlinearities," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 7, pp. 2885-2892, July 2022.