DSTA 2021
dys-ta.com
16th INTERNATIONAL CONFERENCE
Dynamical Systems – Theory and Applications
December 6-9, 2021, On-line

Continuous Dynamical Systems as Pseudo Random Number Generator

ENGİN KANDIRAN[1*], AVADIS HACINLIYAN[2]

1. Yeditepe University, School of Applied Sciences, Software Development Department, Ataşehir, Turkey [ORCID: 0000-0002-6171-1346]
2. Yeditepe University, Faculty of Arts and Science, Department of Physics, Ataşehir, Turkey [ORDCID:0000-0002-4667-9659]

* Presenting Author

Abstract:. Random number generators are very crucial for both security applications and numerical simulations. There are two main categories of random numbers: those generated by Pseudo Random Generators (PRNGs) and True Random Number Generators (TRNGs). Chaotic systems have been recently used as a random number generator especially in cryptography and data encryption. Researchers prefer to use chaotic dynamical systems as PRNG due to their non-periodic behavior and usability as fast random number generators. ne important characteristic of chaotic systems is their sensitive dependence on initial conditions which implies that in integrating equations of motion of such a system, the effect of even an infinitesimal change in the initial conditions will increase exponentially over time and will easily collapse the accuracy of the prediction In this study, we have proposed a pseudo random number generator (PRNG) based on well-known two chaotic dynamical systems: Rössler system and Duffing oscillator. We test our PSRNGs using statistical test suite NIST and we have shown that both systems pass the test and they are feasible for cryptographic usage. Finally, as application we use our PRNGs in image encryption and presents the performance of them in encryption.

Keywords: pseudo random number generators, image encryption, chaos