Iran J Sci Technol Trans Electr Eng
https://doi.org/10.1007/s40998-018-0122-0

RESEARCH PAPER

New and Efficient Method for Extending Cycle Length of Digital Chaotic Systems

Lahcene Merah[1] · Adda Ali-Pacha[2] · Naima Hadj-Said[2] · Mecheri Belkacem[1]

Received: 29 July 2017 / Accepted: 18 July 2018
© Shiraz University 2018

Abstract
Implementing chaotic systems using digital computers with finite arithmetic precision leads to significant degradations on their quality of chaotic dynamics, and the important shortcoming found on digital chaotic systems is their limited cycle length. Notable efforts have been exerted recently to overcome this problem and enhance the quality of digital chaotic generators, and the aim is to generate chaotic sequences with long cycle lengths. Perturbation of chaotic systems orbits is the most efficient technique that has been adopted in this context. In this paper, we propose a new method for perturbing the orbits of chaotic systems. Compared to many proposals, our method does not need an external generator to perturb the chaotic orbit, and it has a self-perturbation mechanism. Evaluation results showed that the proposed method can extremely extend the cycle length of a given chaotic system in which no repeated patterns have been detected even using low arithmetic precision. The results also showed that the perturbed chaotic system has good statistical proprieties in terms of randomness; it passed successfully a set of statistical tests (NIST and Diehard). The whole system has been implemented in FPGA-based hardware, and real-time results are given. Compared with some proposals, the proposed method has provided better results in terms of randomness and hardware performance.

Keywords Chaos · Cryptography · NIST · Diehard · Cycle length · FPGA

1 Introduction

Random numbers play an important role in nowadays digital systems, and they can be found in many digital systems. As digital computers dominate data processing fields today, random number generators implemented in digital computers are known as pseudo-random number generators (PRNGs). The deterministic nature of the process leads to the term pseudo-random. PRNGs algorithms are widely used today thanks to their simplicity of implementation in both software and hardware. They are capable of generating sequences of numbers which appear random-like from many aspects.

Though they are necessarily periodic and their periods are very long, they pass many statistical tests and can be easily implemented with simple software routines (Elsherbeny and Rahal 2012). PRNGs have been widely used in Monte Carlo simulations, test pattern generation, cryptography, and telecommunication systems (Liu and Miao 2015). A good PRNG should have characteristics of: (1) long-period random number sequence; (2) a fit in statistical properties; (3) a high throughput rate; and (4) an unpredictability (Li et al. 2012). Finding all aforementioned characteristics together in one PRNG is a big challenge, due to their fixed linear structure, and most known pseudo-random generators (Linear Feedback Shift Registers, Linear congruential generators, etc.) are not secure enough, especially when used for information security.

✉ Lahcene Merah
l.merah@lagh-univ.dz

Adda Ali-Pacha
a.alipacha@gmail.com

Naima Hadj-Said
naima.hadjsaid@univ-usto.dz

Mecheri Belkacem
b.mecheri@lagh-univ.dz

[1] Department of Electronics, University of Laghouat, Bp 37G route de Ghardaia, Laghouat, Algeria

[2] Department of Electronics, University of Science and Technology of Oran USTO, BP 1505, 31036 El MNaouer Oran, Algeria

Published online: 30 July 2018