Generalized Fractional Logistic Map Encryption System Based on FPGA

Samar M. Ismail, Lobna A. Said, Ahmed A. Rezk, Ahmed G. Radwan, Ahmed H. Madian, Mohamed F. Abu-Elyazeed, Ahmed M. Soliman

PII: S1434-8411(17)30375-8
DOI: http://dx.doi.org/10.1016/j.aeue.2017.05.047
Reference: AEUE 51918

To appear in: *International Journal of Electronics and Communications*

Received Date: 14 February 2017
Accepted Date: 31 May 2017

Please cite this article as: S.M. Ismail, L.A. Said, A.A. Rezk, A.G. Radwan, A.H. Madian, M.F. Abu-Elyazeed, A.M. Soliman, Generalized Fractional Logistic Map Encryption System Based on FPGA, *International Journal of Electronics and Communications* (2017), doi: http://dx.doi.org/10.1016/j.aeue.2017.05.047

Generalized Fractional Logistic Map Encryption System Based on FPGA

Samar M. Ismail[a], Lobna A. Said[b], Ahmed A. Rezk[b], Ahmed G. Radwan[b,c], Ahmed H. Madian[b,d], Mohamed F. Abu-Elyazeed[e], Ahmed M. Soliman[e]

[a] *Faculty of IET, German University in Cairo (GUC), Egypt*
[b] *Nanoelectronics Integrated Systems Center (NISC), Nile University, Giza, Egypt*
[c] *Engineering Mathematics and Physics Dept, Faculty of Engineering, Cairo University, Giza, Egypt*
[d] *Radiation Engineering Dept., NCRRT, Egyptian Atomic Energy, Authority.*
[e] *Electronics and comm. Eng. Dept., Cairo University,Egypt.*

Abstract

This paper introduces the design of a generalized fractional order logistic map suitable for pseudorandom number key generators and its application in an encryption system based on FPGA. The map is generalized through two parameters (a, b) where complete analysis of their effect on the map is detailed, which gives more control on the map chaotic regions. The vertical map and the zooming map presented in this paper are two special maps extracted from the generalized map with their detailed analysis. Not only the positive bifurcation, but also the negative side is discussed through this paper, covering the complete diagram. The specifications of the introduced special logistic maps are proved to be completely controlled through eight design problems with their Lyapunov exponent. As an application, these eight designs are used for the key generation to encrypt different images through a simple algorithm. The correlation coefficients (horizontal, vertical, and diagonal) of the encryption system proposed, as well as the response to differential attacks are calculated. The sensitivity analysis proves that the encryption algorithm develops high sensitivity to the fractional-order key, which appears from the wrong decryption with 0.001% change of any system parameter. The encryption system is implemented

*Corresponding author
Email address: amadian@nu.edu.eg (Ahmed H. Madian)