World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Main Chaos-Based Image Encryption Algorithm

Authors : Ibtissem Talbi

Abstract : During the last decade, a variety of chaos-based cryptosystems have been investigated. Most of them are based on the structure of Fridrich, which is based on the traditional confusion-diffusion architecture proposed by Shannon. Compared with traditional cryptosystems (DES, 3DES, AES, etc.), the chaos-based cryptosystems are more flexible, more modular and easier to be implemented, which make them suitable for large scale-data encyption, such as images and videos. The heart of any chaos-based cryptosystem is the chaotic generator and so, a part of the efficiency (robustness, speed) of the system depends greatly on it. In this talk, we give an overview of the state of the art of chaos-based block ciphers and we describe some of our schemes already proposed. Also we will focus on the essential characteristics of the digital chaotic generator, The needed performance of a chaos-based block cipher in terms of security level and speed of calculus depends on the considered application. There is a compromise between the security and the speed of the calculation. The security of these block block ciphers will be analyzed.

Keywords : chaos-based cryptosystems, chaotic generator, security analysis, structure of Fridrich
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020