IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 12, No. 1, March 2023, pp. 347~356
ISSN: 2252-8938, DOI: 10.11591/ijai.v12.i1.pp347-356

Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array

Wisal Adnan Al-Musawi, Mohammed Abd Ali Al-Ibadi, Wasan A. Wali
Department of Computer Engineering, Collage of Engineering, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Dec 21, 2021
Revised Aug 8, 2022
Accepted Sep 6, 2022

Keywords:

Artificial neural networks
Chua chaotic systems
Field programmable gate array
Image encryption and decryption
Xilinx system generator

ABSTRACT

Image encryption is an important issue in protecting the content of images and in the area of information security. This article proposes a novel method for image encryption and decryption using the structure of the artificial neural network (ANN)-based chua chaotic system (CCS). This structure was efficiently designed on a field-programmable gate array (FPGA) chip utilizing the xilinx system generator (XSG) tool with the IEEE-754-1985 32-bit floating-point number format. For ANN-based CCS design, a multilayer feed forward neural network (FFNN) structure with three inputs and three outputs was created. This structure consists of one hidden layer with four neurons, each of which has a Tangent Sigmoid activation function. The training of ANN-based CCS yielded a 3.602e-13 mean square error (MSE) value. After successfully training the ANN-based CCS, the design was carried out on FPGA, utilizing the ANN structure's bias and weight values as a reference. The xilinx vivado (2017.4) design suite was used to synthesis and test the ANN-based CCS on the FPGA. The histogram, correlation coefficient, and entropy are used to perform security analysis on various images. Finally, FPGA hardware co-simulation using a Xilinx Artix7 xc7a100t-1csg324 chip was utilized to verify that the encryption and decryption of the images were successful.

Corresponding Author:

Wisal Adnan Al-Musawi
Department of Computer Engineering, University of Basrah
Basrah, Iraq
Email: wisal.eng@gmail.com

1. INTRODUCTION

In recent years, image encryption, being a significant area of information security, has attracted a large number of researchers and scientists. Numerous studies using various methodologies have been implemented, and novel and useful algorithms have been proposed to improve secure image encryption schemes. Digital image encryption approaches based on chaotic systems are novel techniques. This technology encrypts images using random chaos sequences and is a very secure and fast method of image encryption [1]. The use of chaotic systems in cryptography to encrypt images has been proposed as a possible solution to a variety of security problems due to their numerous advantages over random characteristics such as sensitive dependency on initial conditions and parameter settings, simplicity of design, and aperiodic signal, which makes them an ideal option for cryptography systems [2].

This work aims to build a secure cryptographic algorithm that conforms to the following criteria: It is highly resistant to common cryptographic attacks, has a strong key, has a high throughput to meet the demands of large multimedia data volumes, and is simple to implement and consumes little power. The