Abstract

Cryptography is a skill of sending the data in such a form that only those for whom it is intended can read it. There are number of methods to perform cryptography, one of such methods is Chaos theory which studies the behavior of a dynamical systems that are highly sensitive to initial conditions. Even slight changes in initial conditions result in extensively deviating outcomes for such dynamical systems, hence making long-standing estimate unmanageable. The limitations of applying Chaos Theory are choosing the input parameters and synchronization. The computation of these input parameters lies on the dynamics underlying the data and the highly complex analysis, not always accurate. Artificial neural networks (ANN) well known for learning and generalization are hence used to model the dynamics of Chua’s circuit viz. x, y and z. The designed ANN was trained by varying its structures and using different learning algorithms. ANN was trained using 9 different sets which were formed with the initial conditions of Chua’s circuit and each set consisted of about 1700 input-output data. A feed-forward Multi-Layer Perceptron (MLP) network structure, trained with Levenberg-Marquardt backpropagation algorithm, produced best outcome. Further a case study
in which a plain text was first encoded and then decoded by both the chaotic dynamics obtained from the proposed ANN and the numerical solution of Chua's circuit and are compared with each other.

References


Index Terms

Computer Science

Networks

Keywords
Encryption, decryption, chaos theory, chaotic dynamics.