NEURAL NETWORK BASED CRYPTOGRAPHY

*Apdullah Yayık, Yakup Kutlu**

Abstract: In this paper, neural network based cryptology is performed. The system consists of two stages. In the first stage, neural network-based pseudo-random numbers (NPRNGs) are generated and the results are tested for randomness using National Institute of Standard Technology (NIST) randomness tests. In the second stage, a neural network-based cryptosystem is designed using NPRNGs. In this cryptosystem, data, which is encrypted by non-linear techniques, is subject to decryption attempts by means of two identical artificial neural networks (ANNs). With the first neural network, non-linear encryption is modeled using relation-building functionality. The encrypted data is decrypted with the second neural network using decision-making functionality.

Key words: *Artificial neural network, asymmetric cryptology, pseudo-random number generator*

Received: November 11, 2013 **DOI:** 10.14311/NNW.2014.24.011
Revised and accepted: April 14, 2014

1. Introduction

Cryptography uses mathematical techniques for information security. Information security is now a compulsory component of commercial applications, military communications and also social media implementation. This is a result of the many threats and attacks that can be made to these networks by people with malicious intent. Cyber-terrorists, crackers, hackers, so-called 'script kiddies' and industrial spies are all masters in the manipulation of information systems [17]. Cryptography is, furthermore, the most significant part of communication security [3]. It maintains the confidentiality that is the core of information security. Any cryptography requires confidentiality, authentication, integrity and non-repudiation from those authorized to have it. Authentication relates to the identification of two parties entering into communication, while integrity addresses the unauthorized modification of an element inserted into the system [23]. To date, there has been a large number of studies intended to advance robust cryptosystems and use them in communications. Some of these studies concerned the usage of neural networks in

*Apdullah Yayık, Yakup Kutlu, Mustafa Kemal University, Department of Computer Engineering, Turkey, E-mail: apdullahyayik@gmail.com, ykutlu@mku.edu.tr

