Abstract

In this paper an algorithm for one-way hash function construction based on a two layer feed forward neural network along with the piece-wise linear (pwl) chaotic map is proposed. Where SHA-2 is cryptographic hash function designed by NSA(National Security Agency). Based on chaotic neural networks, a SHA-2 Hash function is constructed, which makes use of neural
networks' diffusion property and chaos' confusion property. This function encodes the plaintext of arbitrary length into the hash value of fixed length (typically, 128-bit, 256-bit or 512-bit). Theoretical analysis and experimental results show that this hash function is one-way, with high key sensitivity and plaintext sensitivity, and secure against birthday attacks or meet-in-the-middle attacks. These properties make it a suitable choice for data signature or authentication.

Reference

- Neural Network by Christos Stergiou and Dimitrios Siganos.

Index Terms

Computer Science

Artificial Intelligence

Key words

Artificial Neural Network

Hash Function

Feed Forward

Plaintext Sensitivity