INTISARI

SISTEM KRIPTOGRAFI MEMANFAATKAN *NEURAL NETWORK MULTILAYER PERCEPTRON* DENGAN AUDIO SEBAGAI PEMBANGKIT KUNCI ASIMETRI

Oleh

Ayu Vina Waluyantari
13/356460/PPA/04426

Masalah keamanan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi yang harus dapat dijaga kerahasiaan dan keautentikannya. Salah satu metode pengamanan yang dapat dilakukan adalah dengan menggunakan pemodelan sistem kriptografi kunci asimetri. Seiring berkembangnya teknologi, penggunaan *neural network* dapat dikombinasikan pada banyak aspek termasuk kriptografi. Komputasi *neural network* memiliki beberapa kesamaan dengan komputasi kriptografi yaitu sama-sama memiliki keterkaitan antara data masukan dan data keluaran. Plainteks dapat direpresentasikan oleh *input layer*, chiperteks direpresentasikan oleh *hidden layer* dan hasil dekripsi cipherteks direpresentasikan oleh *output layer*. Selain itu *neural network* memiliki kemampuan untuk beradaptasi dan kemampuan proses belajar yang dapat dimanfaatkan saat proses pembangkitan kunci asimetri sistem kriptografi.

Penelitian ini dilakukan untuk mengetahui kinerja pemanfaatan *neural network multilayer perceptron* dengan algoritma *Levenberg-Marquardt* pada sistem kriptografi. Sistem dapat menggunakan nilai ekstraksi ciri data audio sebagai pembangkit kunci asimetri. Pemilihan audio didasarkan karena angka acak memainkan peran penting saat proses enkripsi untuk berbagai aplikasi keamanan jaringan. Angka acak dapat diperoleh dari ekstraksi ciri data audio dengan mencari nilai amplitudo, *short time energy* dan *zero crossing rate*.

Hasil penelitian menunjukkan sistem kriptografi yang dibangun telah berhasil menyandikan pesan dan mengembalikannya kebentuk semula. Keberhasilan dalam enkripsi dan dekripsi pesan dipengaruhi oleh jumlah *node hidden* yang pada penelitian ini berhasil mencapai nilai akurasi 100% dengan menggunakan 17 *node hidden*, total nilai audio yang digunakan diatas 4 dengan nilai awal acak kecil (nilai pecahan bilangan desimal positif yang baru memiliki nilai pada 3 angka dibelakang koma). Penyerangan dengan metode *brute force* berdasarkan kunci membutuhkan waktu 3.7577E + 226 tahun untuk dapat memecahkan pesan.

Kata kunci : Sistem kriptografi, *Levenberg-Marquardt*, ekstraksi ciri data audio.

ABSTRACT

CRYPTOGRAPHIC SYSTEM USING NEURAL NETWORK MULTILAYER PERCEPTRON WITH AUDIO AS ASYMMETRIC KEY GENERATOR

By

Ayu Vina Waluyantari
13/356460/PPA/04426

A security issue is one of the important aspects of a message, data, or information that should be kept confidential and authenticity. One of the security methods can use modeling cryptographic system of asymetric key. As the development of technology, the use of neural network can be combined in many aspects, including cryptography. Computational cryptography has some similarities with neural network computing that is equally has the link between data input and data output. Plaintext can be represented by the input layer, chipertext represented by the hidden layer and decrypt ciphertext results represented by the output layer. Besides neural network has the ability to adapt and the ability of the learning process that can be used when the key generation process cryptographic systems of asymmetry.

This research to determine how performance the multilayer perceptron neural network with Levenberg-Marquardt algorithm on cryptographic systems. The system can use the value of feature extraction of audio data as a asymmetry key generator. Selection was based audio because of random numbers play an important role during the process of encryption for various network security applications. Random numbers can be obtained from the feature extraction audio data to find the value of the amplitude, short-time energy and zero crossing rate.

The results showed cryptographic systems has been built successfully encrypt a message and return to forms previously. Success in the encryption and decryption of messages is affected by the number of nodes hidden that in this study it achieves 100% accuracy using 17 nodes hidden, the total value of the audio used above 4 with the initial value of the small random (fractional value decimals new positive value at 3 decimal places). Assault with a brute force method based 3.7577E + 226 years to be able to be able to dechiper the message.

Keywords : Cryptographic system, *Levenberg-Marquardt*, feature extraction of audio data.