

INTISARI

MODEL KOMPRESI-ENKRIPSI CITRA DIGITAL BERBASIS GENERATIVE ADVERSARIAL NETWORK (GAN) DAN CHAOTIC MAP

Oleh

Mulkiah

19/448720/PPA/05803

Permasalahan pertukaran data berbentuk digital, termasuk data citra, adalah ukurannya yang cenderung semakin besar dan pemenuhan aspek kerahasiaannya pada saat ditransmisikan melalui jalur yang tidak aman. Untuk menyelesaikan permasalahan tersebut digunakan model kriptosistem yang menggunakan penggabungan metode kompresi dan kriptografi. Salah satu metode kompresi yang berkembang akhir-akhir ini adalah kompresi berbasis *neural network*, sedangkan metode enkripsi yang banyak digunakan untuk pengamanan citra digital adalah enkripsi berbasis chaos. Dalam penelitian ini, dilakukan pengembangan dan pengukuran kinerja model kompresi-enkripsi citra digital menggunakan algoritme kompresi berbasis *neural network* yaitu Generative Adversarial Network yang bersifat lossy dan algoritme enkripsi berbasis chaos. Terdapat dua chaotic map yang digunakan, yaitu Logistic Map yang berbasis substitusi dan Arnold Cat Map yang berbasis permutasi. Pengujian terdiri dari dua aspek pengujian yaitu aspek pengujian kinerja kompresi, dan pengujian aspek efektifitas keamanan. Pada pengujian kompresi digunakan analisis PSNR, SSIM, dan rasio kompresi. Dan pada pengujian aspek keamanan dilakukan pengujian dengan menggunakan analisis ruang kunci, histogram, nilai entropi, nilai korelasi, nilai NPCR dan nilai UACI. Hasil pengujian menunjukkan bahwa skema GAN-Logistic map unggul dari segi rasio kompresi, ruang kunci, histogram, entropi, korelasi, NPCR, UACI, dan waktu proses dibandingkan GAN-Arnold Cat Map. Hasil pengujian juga menunjukkan skema ini juga unggul dibandingkan algoritme kompresi-enkripsi lain, dengan nilai SSIM yang tinggi yaitu di atas 0,87 dan presentase rasio kompresi rata-rata 88 % untuk skema GAN-ACM dan 95 % untuk skema GAN-LM.

Kata-kata kunci : Kompresi-Enkripsi, citra digital, Chaos, lossy compression, symmetric cryptography, Generative Adversarial Network

ABSTRACT

Compression-Encryption Model for Digital Images Based on Generative Adversarial Network (GAN) and Chaotic Map

By

Mulkiah

19/448720/PPA/05803

The problem of data transmission, including images, tends to get bigger in size also fulfill its confidentiality aspects when transmitted through unsecured channels. To solve this problem, a cryptosystem model that combines compression and cryptography methods is implied. One of the advanced compression methods developed recently is Neural Network-based compression, while the most widely used encryption method for securing digital images is chaos-based encryption. In this study, the development and performance measurement of the digital image compression-encryption model using a neural network-based compression algorithm, namely the lossy Generative Adversarial Network and a chaos-based encryption algorithm, was conducted. There are two chaotic maps used, namely the Logistic Map based on substitution and the Arnold Cat Map based on permutations. Testing is conducted by two aspects: compression performance and security performance. In the compression performance test, PSNR, SSIM, and compression ratio analysis were implied, and in security performance, testing is implemented using key space analysis, histogram analysis, entropy, correlation coefficient, UACI, and NPCR value. The test results show that the GAN-Logistic map scheme is outperform GAN-Arnold Cat Map in compression ratio, key space analysis, histogram, entropy, correlation, NPCR, UACI and processing time. The test results also show that this scheme is also better than other compression-encryption algorithms, with a high SSIM value in average is 0.97 and percentage of compression ratio in average for GAN-ACM scheme is 88%, and GAN-LM is 95 %.

Keywords : compression-encryption, digital image, Chaos, lossy compression, symmetric cryptography, Generative Adversarial Network