

Enkripsi citra digital dengan menggunakan fungsi chaos skew tent map = Digital image encryption using chaos function skew tent map

Siti Wahyuningsih, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20387925&lokasi=lokal>

Abstrak

Pengamanan terhadap citra digital guna menghindari berbagai bentuk kejahatan dunia teknologi menjadi aspek yang sangat penting dan mendesak untuk diperhatikan. Salah satu teknik pengamanan yang sering digunakan adalah teknik kriptografi. Salah satu teknik kriptografi yang sedang berkembang saat ini adalah teknik kriptografi berbasis fungsi chaos. Fungsi chaos yang akan digunakan dalam skripsi ini adalah skew tent map dengan dua proses yang akan dilakukan, yaitu proses permutasi dan difusi. Proses permutasi akan mengubah posisi piksel sedangkan proses difusi akan mengubah nilai piksel.

Analisis hasil uji coba dilakukan dengan cara analisis waktu proses enkripsi dan dekripsi, analisis ruang kunci, analisis sensitivitas nilai kunci, koefisien korelasi antara plaintext dan ciphertext, uji goodness of fit, dan uji NIST (National Institute of Standard and Technology).

Adapun hasil yang diperoleh yakni waktu proses enkripsi dan dekripsi hampir sama, ruang kuncinya mencapai 1030, sensitivitas kuncinya mencapai 10-16, koefisien korelasi antara plaintext dan ciphertext mendekati nol, nilai-nilai piksel ciphertext berdistribusi uniform, dan keystream yang digunakan acak. Sehingga hasil enkripsi dengan algoritma yang diusulkan dalam skripsi ini sulit untuk dipecahkan dengan serangan brute force dan known plaintext.

.....

Securing the digital image in order to avoid various forms of world's crime technology aspect is a very important issue and needs to be discussed. The security techniques which are often used are cryptography techniques. One of the cryptography techniques which is being developed today is cryptography technique based on chaos function. Chaos function, which is used on this research, is the skew tent map with two processes applied, the permutation and diffusion processes. Permutation process will change the position of pixels while the diffusion process will change the value of pixels.

Test Analysis results are done by encryption and decryption time analysis, key space analysis, key value sensitivity analysis, correlation coefficient between plaintext and ciphertext, the goodness of fit test, and the NIST (National Institute of Standard and Technology) test.

The results are encryption and decryption time are almost same, the key space reach 1030, the key value sensitivity reach 10-16, correlation coefficient between plaintext and ciphertext near to zero, the ciphertext pixel values distributed uniformly and keystream which is randomly used. So the result of this proposed encryption algorithm is difficult to be solved with brute force attack and known plaintext attack.