Enkripsi citra digital dengan skema difusi -transposisi berbasis chaos = Chaos based digital image encryption using diffusion permutation scheme/Wiwit Widhianto

Wiwit Widhianto, author

Abstrak

Perkembangan pesat di bidang teknologi komunikasi saat ini memberikan kemudahan dalam menyimpan maupun mengirimkan informasi digital dengan cepat. Telah banyak metode enkripsi untuk citra digital yang telah diajukan, umumnya menggunakan skema difusi, transposisi, dan difusi-transposisi. Akan tetapi, kesulitan utama dari metode-metode tersebut adalah cara bagaimana mengacak informasi yang terdapat pada citra digital tersebut. Pada tahun 2009, Yong et al. mengajukan algoritma enkripsi dengan skema difusi-transposisi berbasis chaos dengan menggunakan parameter kontrol dimana metode ini membutuhkan waktu komputasi yang lebih cepat tanpa mengorbankan tingkat keamanannya.
Pada tugas akhir ini, akan dibahas mengenai pengamanan citra digital menggunakan skema difusi-transposisi berbasis chaos, dengan fungsi chaos yang digunakan adalah logistic map pada tahap difusi dan Arnold’s cat map pada tahap tranposisi. Ruang kunci dari algoritma ini mencapai 1.84×1049 dengan sensitivitas kunci hingga 1016 yang menjadikannya sulit untuk dipecahkan dengan bruteforce attack. Berdasarkan pengujian dengan menggunakan uji dari National Institute of Standards and Tehcnologies (NIST) keystream yang dihasilkan telah terbukti acak dan distribusi dari nilai intensitas pixel-pixel dari citra yang terenkripsi adalah uniform menjadikannya sulit untuk pecahkan dengan known plaintext attack.
.....
Rapid improvement in technology and communication provides ease in either saving or sending digital information. A number of encryption method on digital images has been proposed in recent years, commonly using diffusion, permutation, and diffusion-permutation scheme. However, the main obstacle in designing encryption algorithm is rather difficult to swiftly shuffle and diffuse the information on digital image. In 2009, Yong et al. proposed a chaos-based encryption algorithm using diffusion-permutation scheme using control parameters which posseses fast encryption speed and high security.
On this skripsi, digital image will be secured by using chaos-based encryption with diffusion-transposition scheme, chaotic function will be employed to generate random number on diffusion is logistic map and Arnold’s cat map on transposition. Key space of this algorithm is 1.84×1049 with sensitivity up to 1016 will provides high resistance from bruteforce attack. Based on National Institute of Standards and Technologies (NIST) test, keystream produced has shown to be random, moreover histogram of pixel value from the chipertext is almost flat which means the distribution of the pixel value is uniform that would provides high resistance from known plaintext attack.