Universitas Indonesia Library >> UI - Skripsi Membership

Pengembangan sistem enkripsi citra berbasis chaos dengan menggunakan Arnold's cat map dan henon map = Development of chaos-based image encryption system using Arnold's cat map and henon map.

Frenzel Timothy Surya, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20505159&lokasi=lokal

---

Abstrak

Pada penelitian ini, dirancang suatu sistem enkripsi citra yang berfokus di bidang teledermatologi, secara khusus untuk mengamankan data-data berupa gambar penyakit kulit. Mekanisme enkripsi dan dekripsi citra dilakukan di sisi klien menggunakan program enkripsi berbasis chaos dengan menerapkan gabungan teknik confusion dan diffusion. Model chaotic map yang digunakan pada teknik confusion adalah Arnold’s cat map, sedangkan model yang digunakan pada teknik diffusion adalah Henon map. Initial values dari kedua chaotic map tersebut didapatkan dari secret key sepanjang 30-digit numerik yang dihasilkan melalui pertukaran kunci Diffie-Hellman. Pada Arnold’s cat map digunakan nilai p dan q yang berbeda-beda pada setiap iterasinya, sedangkan pada Henon map digunakan nilai x dan y dengan tingkat presisi hingga 10^-14. Dari pengujian yang telah dilakukan, didapatkan histogram dengan persebaran piksel yang menyeluruh. Selanjutnya didapatkan juga rata-rata koefisien korelasi sebesar 0.003877 (horizontal), -0.00026 (vertikal), -0.00049 (diagonal), dan rata-rata nilai entropi sebesar 7.950304. Dari segi sensitivitas kunci, perbedaan satu angka pada secret key menyebabkan hasil enkripsi hanya memiliki indeks kesamaan sebesar 0.005337 (0.5%). Sedangkan perbedaan kunci pada dekripsi citra tidak bisa kembali ke bentuk semula, dan justru menghasilkan citra acak lain dengan rata-rata nilai entropi hasil dekripsi sebesar 7.964909333 (perbedaan secret key) dan 7.994861667 (perbedaan private key).

.....This research designed an image encryption system that focused on securing teledermatology data, in the form of skin disease images. The encryption and decryption process of this system is done on the client side using chaos-based encryption with confusion and diffusion techniques. The chaotic map model that is being used for confusion is Arnold’s cat map, meanwhile Henon map is used for the diffusion. Initial values of both chaotic maps are obtained from 30-digits secret key which is generated using Diffie-Hellman key exchange. During Arnold’s cat map generation, different p and q values are used for every iteration. On the other side, the precision of Henon map’s x and y values are 10^-14. From the tests that have been done, histograms of the encrypted images are relatively flat and distributed through all the gray values. Moreover, the encrypted images have an average correlation coefficient of 0.003877 (horizontal), -0.00026 (vertical), -0.00049 (diagonal), and average entropy of 7.950304. From key sensitivity test, a difference of just one number on the secret key causes big differences as both results only have similarity index of 0.005337 (0.5%). Meanwhile in decryption process, that little key difference cannot be used to restore the encrypted image to its original form and generate another chaotic image with an average entropy of 7.964909333 (secret key difference) and 7.994861667 (private key difference).