

Pengembangan algoritma enkripsi citra digital dengan menggunakan arnold s cat henon map (ACHM) = Development of digital image encryption alghorithm using arnold s cat henon map (ACHM)

Mohammad Fachruddin, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20455477&lokasi=lokal>

Abstrak

ABSTRAK

Kemajuan bidang kriptografi juga dipengaruhi oleh perkembangan dari fungsi chaos. Dalam tesis ini akan dikembangkan fungsi chaos baru yang merupakan hasil dari komposisi dua fungsi chaos yaitu Henon Map dan Arnold's Cat Map. Dalam tesis ini fungsi chaos baru tersebut dinamakan Arnold's Cat Henon Map ACHM. Proses enkripsi yang dikembangkan dalam tesis ini yaitu dengan menggunakan beberapa parameter yaitu $a, b, p, q \in \mathbb{Z}$ sehingga dapat dihasilkan citra terenkripsi. Selanjutnya dilakukan pengujian kinerja algoritma enkripsi berdasarkan uji keacakan sesuai standar dari National Institute of Standards and Technologies NIST. Uji lainnya dilakukan dengan uji sensitivitas nilai awal, uji distribusi atau uji ergodisitas dan uji PSNR. Dari hasil uji coba maka dihasilkan untuk Uji Keacakan, hasil monobit test adalah tidak acak sedangkan untuk run test mengalami bentuk acak. Nilai uji PSNR = ∞ ; untuk masing-masing data uji beserta chipper image. Uji Sensitivitas Kunci digunakan dengan mengganti nilai parameter $a, b, p, q \in \mathbb{Z}$ sehingga akan terlihat sensitivitas dari hasil enkrip dan dekrip dengan nilai parameter yang berbeda-beda.

ABSTRACT

Progress in cryptography is also influenced by the development of chaos function. This thesis will developed a new functions which are the result of the composition of the two functions, namely chaos Henon Map and Arnold's Cat Map. In this thesis, a new chaos functions are called Arnold's Cat Henon Map ACHM. The encryption process developed in this thesis uses several parameters $a, b, p, q \in \mathbb{Z}$ so it can produce the encrypted image. Further testing the performance of the encryption algorithm by randomness test according to Standards of the National Institute of Standards and Technologies NIST. Other tests done by testing the sensitivity of the initial value, or a distributed test or ergodisitas test and image PSNR. From the results of the trial then generated for the Test of Randomness, the result of monobit test is not random while for the run test has a random form. Test value PSNR ∞ for each test data along with the image chipper. The Key Sensitivity Test is used by replacing parameter values $a, b, p, q \in \mathbb{Z}$ so that the sensitivity of encrypted and decrypted results with different parameter values will be seen.