ABSTRAK

Banyak orang berusaha menyiasati bagaimana cara mengamankan informasi, khususnya informasi berupa data berbentuk citra yang dikomunikasikan melalui kanal transmisi atau menyiasati bagaimana cara mendeteksi keaslian dari informasi (citra) yang diterimanya. Salah satu cara yang lazim untuk melindungi data citra digital adalah enkripsi.

Algoritma enkripsi Cat Map mempunyai keunikan tersendiri dalam prosesnya, tetapi parameter kunci yang terdapat pada algoritma ini sangat sedikit, sehingga apabila dilihat dari sisi keamanannya, tentu algoritma ini kurang memuaskan. Algoritma dalam Tugas Akhir ini dirancang untuk memecahkan persoalan tersebut dengan cara menggabungkan algoritma enkripsi Cat Map dengan algoritma enkripsi lainnya. Metoda yang digunakan adalah metoda gabungan Cat Map – SDES (*Simplified Data Encryption Standard*) dan gabungan Cat Map – permutasi blok acak.

Hasil dari implementasi sistem ini adalah bagaimana sistem ini mampu mengenkripsi citra dengan waktu proses yang secepat mungkin dan tingkat keamanan yang tinggi. Dari percobaan untuk masing-masing metode enkripsi pada citra berukuran 200 × 200 *pixel* diperoleh waktu proses enkripsi untuk metode gabungan Cat Map – SDES adalah 16,5973 detik, sedangkan untuk metode gabungan Cat Map – permutasi blok acak jauh lebih cepat yaitu selama 0,91292 detik.

Untuk memecahkan kunci dari metode gabungan Cat Map – SDES dengan menggunakan *brute force attack* (spesifikasi komputer sesuai dengan milik penulis) pada sistem dengan citra input 200 × 200 *pixel* membutuhkan waktu selama 10 tahun, sedangkan untuk metode gabungan Cat Map – permutasi blok acak membutuhkan waktu jauh lebih lama yaitu selama $4{,}56589 \times 10^{371}$ tahun.

Kata kunci: *Image Encryption, Arnold's Cat Map, Simplified DES, cryptography, chaotic maps, random block permutation*.