IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL MENGGUNAKAN SKEMA TRANPOSISI BERBASIS FUNGSI *CHAOS*

***Suryadi MT*[1]**
***Zuherman Rustam*[2]**
***Wiwit Widhianto*[3]**

[1,2,3]*Departemen Matematika, FMIPA, Universitas Indonesia*
[1]*yadi.mt@sci.ui.ac.id,* [2]*rustam@ui.ac.id,* [3]*wiwit.widhianto@sci.ui.ac.id*

Abstrak

Algoritma enkripsi citra digital yang dikembangkan dalam paper ini ditujukan sebagai alternatif dalam mengamankan informasi citra tersebut. Lenaha yang dilakukan adalah dengan menggunakan skema transposisi yang berbasis fungsi chaos, yaitu fungsi Arnold's cat map. Fungsi tersebut berfungsi sebagai bentuk transposisi atau pertukaran posisi dari informasi data aslinya. Akan ditetapkan skema transposisi tertentu untuk mengacak informasi asli sehingga sulit untuk dibaca kembali oleh pihak ketiga. Selanjutnya dilakukan pengujian secara praktis. Pengujian dilakukan untuk beragam data berupa citra digital dengan berbagai ukuran. Hasil analisis pengujian secara praktis menunjukkan bahwa ruang kunci yang dihasilkan sangat jauh lebih besar dan tingkat sensitivitasnya sangat jauh lebih kecil.

Kata Kunci: *Algoritma enkripsi, citra digital, Arnold's cat map, fungsi chaos.*

PENDAHULUAN

Fenomena pada era masya-rakat informasi saat ini dengan mudahnya kita mendapatkan banyak informasi yang tersebar dan tersedia dari beragam bentuk khususnya dalam bentuk citra. Padahal informasi tersebut tanpa disadari memiliki nilai yang sangat tinggi (berharga) bagi pribadi, institusi atau organisasi, sehingga sangat rentan akan dimanfaatkan oleh pihak-pihak yang tidak

bertanggung jawab bagi kepentingan pribadi atau kelompoknya. Apalagi dengan tersedianya program aplikasi yang sangat mudah dioperasikan sehingga para pelaku dapat memanipulasi citra sesuai de-ngan niat jahatnya, yang akan berakibat pada perubahan infor-masi yang tampak dari citra tersebut guna mendapatkan keuntungan bagi pelaku.

Jika kita perhatikan dalam kenyataannya, penggunaan tek-nologi informasi dan komunikasi (TIK) khususnya terkait dengan usaha penyimpanan maupun perlindungan bagi data atau informasi yang ada saat ini masih memiliki keterbatasan yang cukup signifikan. Keter-batasan yang dimaksud dalam hal ini terlihat pada tingkat keamanan atau perlindungan data atau informasi yang relatif masih lemah. Sehingga peluang terjadinya pencurian data atau informasi oleh orang yang tidak berhak semakin besar seiring dengan penggunaan jaringan komputer

saat ini. Dengan demikian diperlukan usaha untuk meningkatkan keamanan data atau informasi.

Untuk mencegah pengak-sesan data atau informasi oleh pihak ketiga, diperlukan teknik pengamanan data atau informasi, salah satunya dengan cara mengenkripsi data atau infor-masi, sehingga hanya orang yang tertentu saja yang dapat mengakses data atau informasi tersebut.

Metode enkripsi citra telah banyak dikembangkan diantara-nya yaitu yang umum digunakan dengan metode Arnold Cat map, logistic map, (Pareek *et. al*, 2006, Patidar *et. al*, 2009, Huang, *et.al*, 2010, Kocarev & Lian, 2011, Munir, 2012). Pada paper ini metode enkripsinya menggunakan fungsi *Chaos* Arnold Cat map, yang diimplementasikan mengguna-kan bahasa pemrograman Python dan citra digital berekstensi bmp.

METODE PENELITIAN

Chaos adalah tipe dari perilaku suatu sistem ataupun fungsi yang bersifat acak, peka terhadap nilai awal dan *ergodicity*. Fungsi yang memi-liki sifat *chaos* dinamakan fungsi *chaos*. Fungsi *chaos* sudah dibuktikan sangat cocok untuk merancang sarana untuk proteksi data (Kocarev & Lian, 2011, Alvares & Li, 2006). Dengan sifat tersebut, fungsi *chaos* dapat digunakan sebagai pembangkit bilangan acak. Salah satu fungsi sederhana yang memunculkan sifat *chaos* adalah persamaan *Arnold's cat map*. *Arnold's cat map* didefinisikan secara umum sebagai berikut (Huang, *et.al*, 2010, Kocarev & Lian, 2011) :

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \quad \ldots (1)$$

dengan syarat nilai determinan dari matriks :

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} = 1 \ldots\ldots\ldots\ldots\ldots (2)$$

Parameter inputnya yaitu p, q, merupakan bilangan bulat poitif dan $[x_i, y_i]$ dan $[x_{i+1}, y_{i+1}]$ merupakan bilangan bulat *non negative* yaitu {0,1, 2, 3, …, N – 1}. Adapun yang dimaksud dengan $[x_i, y_i]$ menunjukkan posisi piksel dari citra aslinya dan $[x_{i+1}, y_{i+1}]$ menunjukkan posisi baru dari piksel $[x_i, y_i]$. Sedangkan N menunjukkan ukuran dari citra inputnya berupa citra square yaitu $N \times N$.

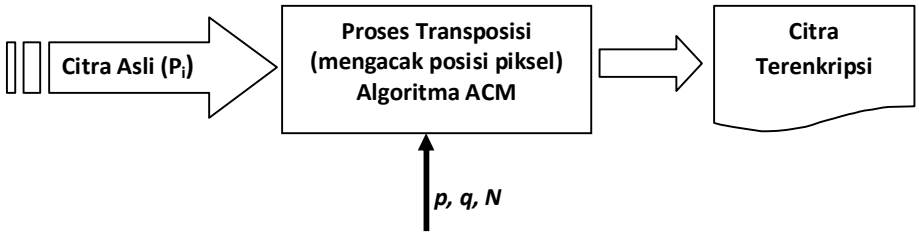
Secara umum proses enkripsi dan dekripsi yang dikembangkan dapat disajikan dalam bentuk diagram blok, sebagaimana tampak pada Gambar 1. Proses enkripsi sebagaimana tampak pada Gambar 1, menggunakan tiga parameter kunci p, q dan N. Hal tersebut akan mempengaruhi proses pengacakan posisi piksel dari citra asli menjadi citra yang terenkripsi.

HASIL DAN PEMBAHASAN

Implementasi algoritmanya menggunakan bahasa pemro-graman Python. Program apli-kasi tersebut diuji cobakan terhadap 5 data uji berbeda namun dengan tampilan gambar yang sama. Adapun kelima data uji tersebut tampak pada Tabel 1.

Proses pengujiannya dilakukan dengan memasukan nilai parameter kunci p, q dan N. Untuk nilai p dan q nya pada setiap uji coba bernilai sama,

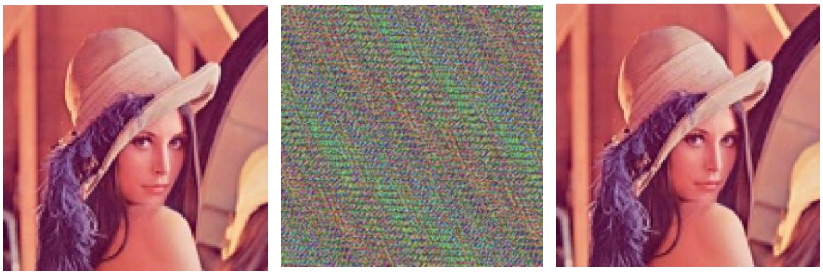
dalam hal ini yaitu $p = 157$ dan $q = 37$. Sedangkan nilai N tergantung pada ukuran piksel data uji yang digunakan. Adapun hasil dari enkripsi dan dekripsinya terhadap satu uji coba untuk *file* Lena1.bmp, tampak pada Gambar 2.



Gambar 1. Bentuk Umum Proses Enkripsi Menggunakan Arnold's Cat Map

Tabel 1. Citra Data Uji

Data Uji ke	Nama File	Tampilan Gambar	Ukuran Citra (piksel)
1.	Lena1 .bmp		128 x 128
2.	Lena2 .bmp		256 x 256
3.	Lena3 .bmp		512 x 512
4.	Lena4 .bmp		1024 x 1024
5.	Lena5 .bmp		2048 x 2048



a b c

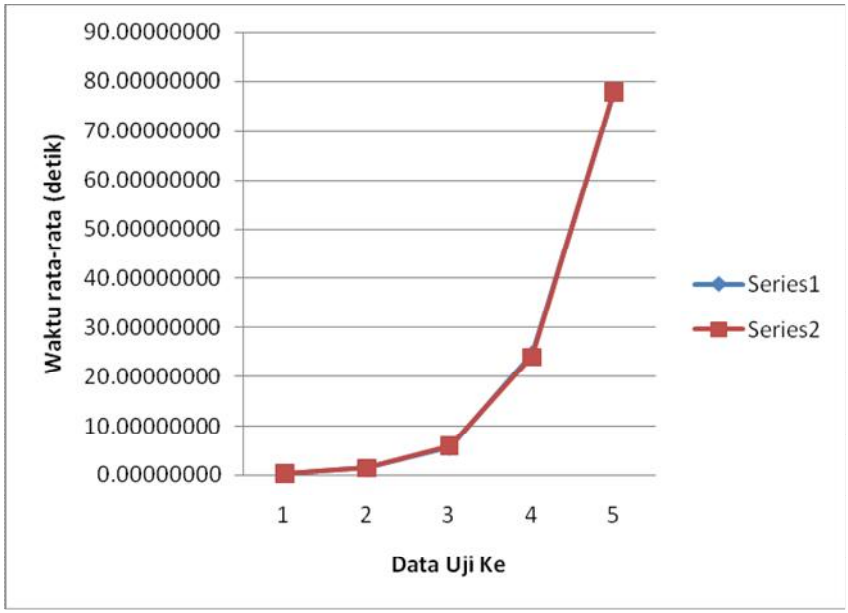
Gambar 2. (a) Citra asli, (b) Citra terenkripsi, (c) Citra terdekripsi

Sedangkan rata-rata waktu enkripsi dan dekripsi dari hasil uji coba untuk setiap data uji citra yang digunakan (Tabel 1), dapat dilihat pada Tabel 2 dan Gambar 3. Adapun penyajian secara grafik dari hasil rata-rata waktu proses enkripsi dan proses dekripsi sebagaimana Tabel 2, dapat dilihat pada Gambar 3. Tampak dari Tabel 2 dan Gambar 3, menujukkan bahwa rata-rata

waktu proses enkripsi dan dekripsi relatif sama. Selain itu, tampak bahwa rata-rata waktu proses enkripsi dan dekripsi berbanding lurus terhadap ukuran piksel citra inputnya. Semakin besar ukuran piksel suatu citra maka akan semakin lama rata-rata waktu yang dibutuhkan untuk proses enkripsi dan dekripsinya.

Tabel 2. Rata-rata Waktu Proses Enkripsi dan Dekripsi

Data Uji Ke-	Nama File	Ukuran Citra (piksel	Rata-rata Waktu Enkripsi (detik)	Rata-rata Waktu Dekripsi (detik)
1.	Lena1.bmp	128 x 128	0.354699979	0.345399973
2.	Lena2.bmp	256 x 256	1.471900007	1.506399962
3.	Lena3.bmp	512 x 512	5.833900035	5.984700119
4.	Lena4.bmp	1024 x 1024	24.53229999	23.96350004
5.	Lena5.bmp	2048 x 2048	77,89499998	77,97300004



Gambar 3. Rata-rata Waktu Enkripsi dan Dekripsi Data Uji Lena.bmp

SIMPULAN DAN SARAN

Kesimpulan dari uraian yang telah disampaikan sebelumnya yaitu :

a. Implementasi algoritma Arnold's Cat Map dalam enkripsi data citra digital dapat dikembangan melalui bahasa pemrograman Python dengan hasilnya sesuai yang diharapkan.

b. Rata-rata waktu proses enkripsi dan dekripsi relatif sama untuk masing-masing citra.
c. Rata-rata waktu proses enkripsi dan dekripsi sangat bergantung terhadap ukuran citra. Semakin besar ukuran citranya maka semakin lama rata-rata waktu yang dibutuhkan untuk proses enkripsi dan proses dekripsinya.

DAFTAR PUSTAKA

Alvarez, Gonzalo., Li, Shujun 2006 "Some Basic Cryptography Requirements Chaos-Base Cryptosystems" *International Journal of Bifurcation and Chaos*, Vol. 16, No. 8, pp. 2129-2151

Devaney, R.L 1989 *An introduction to chaotic dynamical systems* (2nd *ed*.). Addison-Wesley Publishing company, Inc.

Huang, Mao-Yu., Huang, Yueh-Min., Wang, Ming-Shi 2010 "Image Encryption Algorithm Based on Chaotic Map", *Computer Symposium (ICS) International*, *IEEE Xplore*, 154-158.

Kocarev, L., & Lian, S. 2011 *Chaos-based cyrptography*, Springer-Verlag, Berlin Heidelberg.

Munir, Rinaldi 2012 "Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi Dan Teknik Substitusi Menggunakan Arnold Cat Map Dan Logistic Map", *Prosiding Seminar Nasional Pendidikan Teknik Informatika (SENAPATI)*, 107-124.

Pareek, N.K., Patidar, V., Sud, K.K 2006 "Image encryption using chaotic logistic map" *Journal of Image and Vision Computing,* 24, 926-934.

Patidar, V., Pareek, N.K., Sud, K.K. 2009 "A new subtitution-diffusion based image cipher using chaotic standard and logistic maps". *Journal of Commun Nonlinear Sci Numer Simulat,* 14, 3056-3075