APLIKASI ENKRIPSI CITRA DIGITAL MENGGUNAKAN ALGORITMA *GINGERBREADMAN MAP*

***Suryadi MT*[1]**
***Tony Gunawan*[2]**

[1]*Departemen Matematika, FMIPA Universitas Indonesia*
[2]*Jurusan Teknik Informatika, FTI Universitas Gunadarma*
[1]*yadi.mt@sci.ui.ac.id,* [2]*newtonyrobertt@gmail.com*

Abstrak

Komunikasi data berbasis digital melalui intenet sangatlah bermanfaat bagi kehidupan manusia. Pada sisi lainnya, hal tersebut dapat menimbulkan kerawanan tersendiri. Untuk itu diperlukan suatu usaha perlindungan atau keamanan terhadap bebrbagai macam data atau informasi digital, agar tidak disalahgunakan oleh berbagai pihak yang tidak bertanggung jawab. Pengamanan yang dilakukan yakni dengan menerapkan algoritma enkripsi. Pada paper ini akan dibuat suatu program aplikasi enkripsi dengan menggunakan algoritma Gingerbreadman Map. Metode yang dilakukan yakni membangkitkan barisan bilangan acak berbasis fungsi chaos Gingerbreadman Map. Hasil dari pembangkitan bilangan acak tersebut berfungsi sebagai key stream, yang digunakan untuk menyandikan data aslinya. Hasil uji coba terhadap data citra digital yang diperoleh bahwa program ini mampu melakukan proses enkripsi dengan baik, sehingga diperoleh citra tersandikan. Demikian pula untuk proses kebalikannya (dekripsi). Rata-rata waktu enkripsi dan dekripsinya relatif sama. Selain itu, waktu proses enkripsi berbanding lurus dengan ukuran citranya.

Kata Kunci: *algoritma enkripsi, citra digital, gingerbreadman map, teori chaos.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang semakin canggih ini tidak terlepas dari semakin pentingnya komunikasi jarak jauh. Sumber informasi terkini, tidak hanya di sekitar kita namun juga informasi yang ada di belahan negara lain. Semua itu dapat dilakukan dengan menggunakan koneksi internet. Dengan adanya koneksi internet ini, kita bisa terhubung dengan banyak orang melalui berbagai macam layanan *social media* yang ada dan mencari informasi yang sangat *up-to-date* melalui *website* penyedia informasi tersebut.

Di sisi lain, dengan adanya koneksi internet ini telah membuat orang-orang yang berniat "buruk" untuk mengetahui data rahasia kita yang terkirim melalui internet maupun yang tersimpan dalam media penyimpanan. Oleh sebab itu diperlukan suatu usaha keamanan yang ketat supaya data/informasi *digital* tidak dibaca dan dipergunakan oleh orang yang tidak bertanggung jawab. Metode tersebut dinamakan kriptografi.

Pengertian secara umum dari kriptografi adalah ilmu dan seni untuk

menjaga kerahasiaan berita (Scheiner, 2006, Stalling, 2011). Pengertian lainya yaitu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, *et. al*, 1996).

Dalam perkembangannya pun, kriptografi telah dipakai untuk mengamankan berbagai tipe data, mulai dari teks, citra, hingga video. Pengiriman data multimedia yang dilakukan oleh *user* hingga saat ini dengan aman menjadi sangat mungkin karena diterapkannya metode kriptografi. Banyak *user* yang hendak mengirimkan citra tertentu ke rekan-rekan mereka namun tidak ingin citra tersebut diketahui atau disalahgunakan oleh pihak ketiga yang tidak diinginkan, sehingga metode kriptografi citra ini merupakan suatu hal yang penting di masa sekarang ini.

Beberapa metode enkripsi citra yang telah banyak dikembangkan yaitu diantaranya dengan metode logistic map, Arnold Cat map (Pareek *et. al*, 2006, Patidar *et. al*, 2009, Kocarev, 2011, Munir, 2012). Pada paper ini metode enkripsinya berbasis *chaos* juga namun menggunakan fungsi *Chaos Gingerbreadman Map,* sebagai alternatif dalam usaha mengamanakan citra digital.

METODE PENELITIAN

Sejalan tujuan dari paper ini yakni membuat program aplikasi enkripsi citra digital berbasis chaos dengan menggunakan *Gingerbreadman Map,* maka usaha yang dilakukan adalah dengan menyandikan data berupa citra digital agar tidak bisa terbaca informasinya oleh pihak ketiga.

Proses enkripsi yang dilakukan dengan enkripsi simetris, yang berarti kunci yang digunakan saat mengenkrip harus sama dengan kunci yang digunakan pada saat mendekrip. Kunci tersebut dimanfaatkan untuk membangkitkan barisan bilangan acak yang disebut sebagai *key stream* menggunakan *Gingerbreadman Map*. Bentuk fungsi *Gingerbreadman Map* yaitu sebagai berikut (Devaney, 1989):

$$\begin{cases} x_{n+1} = 1 - y_n + |x_n| \\ y_{n+1} = x_n \end{cases} \quad \ldots(1)$$

Agar citra yang disandikan dapat dijamin dapat kembali lagi kebentuk aslinya maka dalam hal ini digunakan operator XOR dalam melakukan perubahan seyiap nilai piksel citranya. Adapun persamaan enkripsinya yakni sebagai berikut:

$$C_i = P_i \oplus K_i \quad \ldots(2)$$

Sedangkan persamaan dekripsinya yaitu :

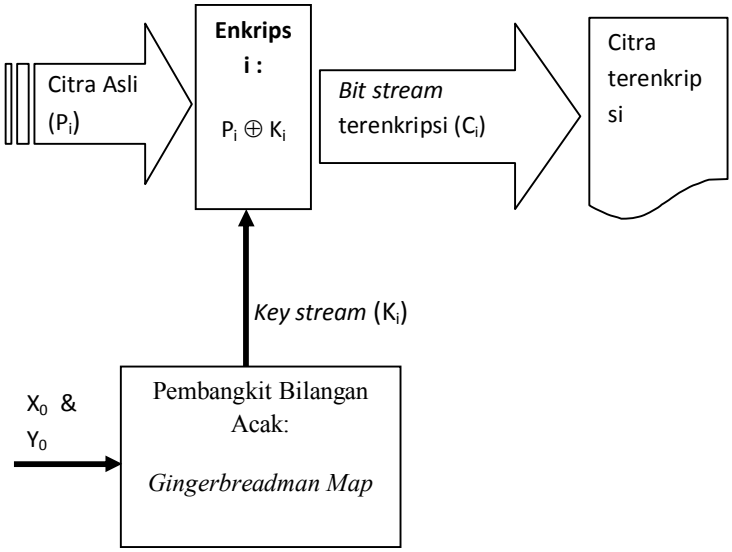
$$P_i = C_i \oplus K_i \quad \ldots(3)$$

dengan P_i merupakan nilai piksel *plaintext* (citra asli) ke-*i*. C_i merupakan nilai piksel *ciphertext* (citra tersandikan) ke-*i*. K_i merupakan nilai *key stream* ke-*i.*

Secara umum proses enkripsi dan dekripsi yang dikembangkan dapat disajikan dalam bentuk diagram blok, sebagaimana tampak pada Gambar 1.

HASIL DAN PEMBAHASAN

Pembangunan program aplikasinya dengan fasilitas tiga menu utama yakni enkripsi citra, dekripsi citra dan perbandingan citra. Tampilan menu utama tampak pada Gambar 2.



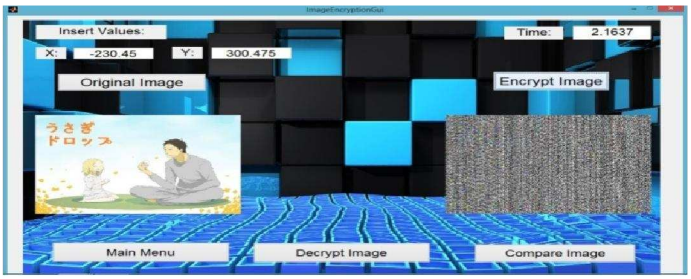
Gambar 1. Diagram proses Enkripsi Menggunakan *Gingerbreadman Map*

Gambar 2. Menu Utama Program Aplikasi Enkripsi Citra

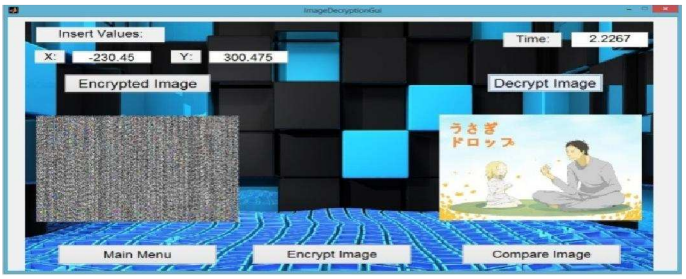
Selanjutnya masing-masing menu utama tersebut bentuk tampilannya tampak pada Gambar 3, Gambar 4 dan Gambar 5.

Gambar 3 dan Gambar 4 memperlihat menu untuk proses enkripsi dan dekripsi citra, dengan memasukkan nama file dan juga dua nilai parameter kunci yang digunakan. Hasil yang diperoleh yaitu berupa file yang sudah terenkrisi atau yang terdekripsi beserta informasi waktu prosesnya. Selain itu juga,
file hasil enkripsi maupun dekripsinya dapat disimpan didalam media penyimpanan yang diinginkan.

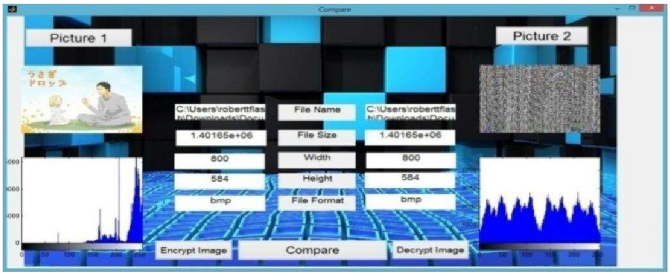
Gambar 5 memperlihatkan hasil proses perbandingan antar file (sebagai inputnya). Hasil berupa informasi hasil perbandingan dalam hal ukuran file, ukuran piksel dan tampilan histogramnya masing-masing. Selanjutnya dilakukan pengujian program terhadap 5 data uji berbeda ukuran dengan tampilan citra warna yang sama, seeperti tampak pada Tabel 1.



Gambar 3. Tampilan Submenu Enkripsi Citra Dan Hasil Prosesnya



Gambar 4. Tampilan Submenu Dekripsi Citra dan Hasil Prosesnya



Gambar 5. Tampilan Submenu Dekripsi Citra dan Hasil Prosesnya

Tabel 1. Citra Data Uji

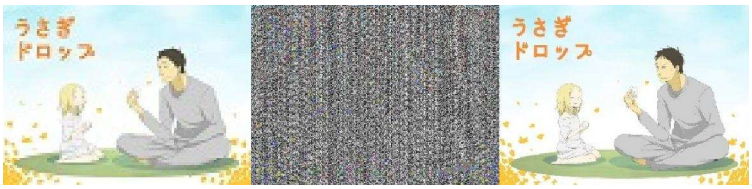
Data Uji ke	Nama File	Tampilan Gambar	Ukuran Citra (piksel)	Ukuran Citra (byte)
1.	Usa1. bmp		300x219	193 KB
2.	Usa2. bmp		600x438	770 KB
3.	Usa3. bmp		800x584	1369 KB
4.	Usa4. bmp		1270x958	3455 KB
5.	Usa5. bmp		1500x1097	4821 KB

Semua data uji pada Tabel 1, dilakukan pengujian proses enkripsi dan dekripsi dengan beberapa nilai kunci X = -230.45 dan Y = 300.475, diperoleh hasil enkripsi dan dekripsinya berupa file, sebagaimana tampak pada Gambar 6

Waktu rata-rata enkripsi dan dekripsi untuk setiap data uji
citra yang digunakan (Tabel 1) beserta grafiknya dengan nilai kunci yang sama, tampak pada Tabel 2 dan Gambar 7.

Tampak dari Tabel 2 dan Gambar 7, menujukkan bahwa rata-rata waktu proses enkripsi dan dekripsi relatif tidak jauh berbeda.

Selain itu, tampak bahwa rata-rata waktu proses enkripsi dan dekripsi berbanding lurus terhadap ukuran citra inputnya.

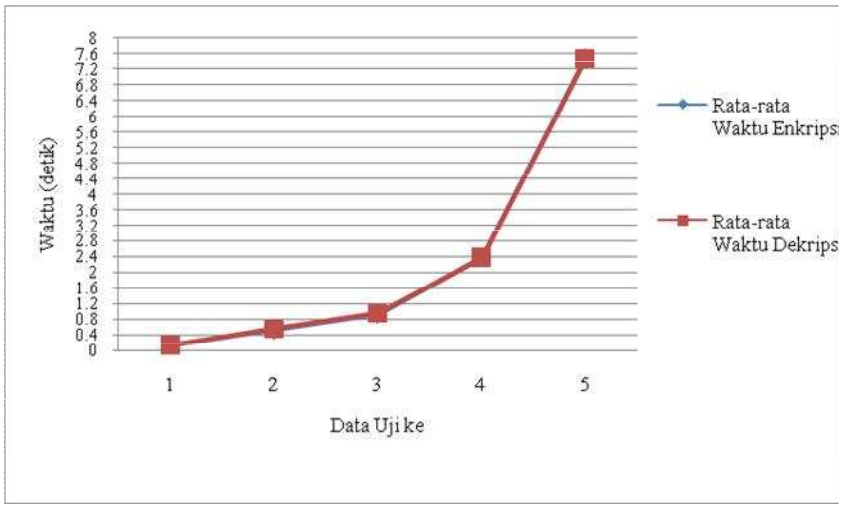


a b c

Gambar 6. (a) Citra asli, (b) Citra terenkripsi (c) Citra terdekripsi

Tabel 2. Waktu rata-rata Proses Enkripsi dan Dekripsi

Data Uji Ke-	Nama File	Ukuran Citra (piksel)	Rata-rata Waktu Enkripsi (detik)	Rata-rata Waktu Dekripsi (detik)
1.	Usa1.bmp	300x219	0.131926	0.131821
2.	Usa2.bmp	600x438	0.518059	0.555059
3.	Usa3.bmp	800x584	0.929696	0.954899
4.	Usa4.bmp	1270x928	2.38195	2.38676
5.	Usa5.bmp	1500x1097	7.49028	7.47278



Gambar 7. Rata-rata Waktu Enkripsi dan Dekripsi Data Uji Usa.bmp

SIMPULAN

Berdasarkan semua hal yang telah diuraikan sebelumnya dapat diambil kesimpulan :

a. Program aplikasi enkripsi berbasis fungsi chaos dengan menggunakan *Gingerbreadman Map* dapat dikembangan dan mampu melakukan proses enkripsi dan dekripsi bersifat simetris 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 berbanding lurus terhadap ukuran citra inputnya.

DAFTAR PUSTAKA

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

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

Menezes, Alfred J., van Orschot, Paul C., and Vanstone, Scott A., (1996), *Handbook of Applied Cryptography*, CRC Press.

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 map*s". *Journal of Commun Nonlinear Sci Numer Simulat,* 14, 3056-3075.

Stallings, W., (2011), *Computer and Network Security: Principle and Practice* (5th *ed*.). Prentice hall, New York..