PENGEMBANGAN METODE BEAUFORT CIPHER MENGGUNAKAN PEMBANGKIT KUNCI CHAOS

Naniek Widyastuti
Jurusan Teknik Informatika
Institut Sains & Teknologi AKPRIND
Jl. Kalisahak 28 Yogyakarta
Email: naniek_wid@yahoo.com

ABSTRACT

Cryptography world have implemented a variety of methods for encoding messages today. The more complicated the method used, the resulting level of security would be better. In order to increase the level of security in the cryptographic algorithms, chaos theory is used. The chaos theory is a branch of mathematics that studies how to generate random numbers.Chaos theory is very sensitive to the initial value (initial condition), it is very useful and can be applied in the world of cryptography to generate a random key that will be processed as a tool in the process of encryption and descryption. More random numbers are generated, the better the security level of a ciphertext.

This study specifically discusses/investigates how chaos theory applied for encoding using beaufort cipher encryption methods to increase the security on the keywords used. Based on the results of tests performed on the tested images show that the beaufort cipher algorithm using a key generated using chaos functions proved to be effective and safe.This is evidenced/proved by the average processing time required to perform the encryption and descryption process is quite fast which is about 0.7 seconds. And visually based testing and statistical test used encryption algorithms cannot provide any clues to do statistical attack by cryptanalist.
Key words: cryptography, beaufort cipher, chaos function

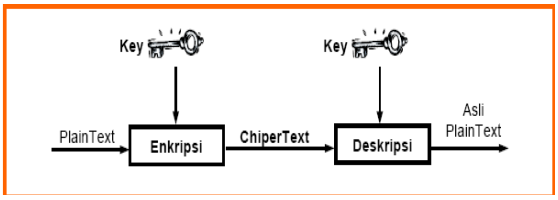
INTISARI

Dunia kriptografi saat ini telah menerapkan berbagai metode untuk penyandian pesan. Semakin rumit metode yang digunakan, maka tingkat keamanan yang dihasilkan pun akan semakin baik pula. Dalam rangka meningkatkan tingkat keamanan dalam algoritma kriptografi, digunakanlah teori chaos. Teori chaos ini merupakan cabang dari matematika yang mempelajari bagaimana membangkitkan bilangan secara acak. Teori chaos ini sangat sensitive pada nilai awal (initial condition), hal ini sangat berguna dan dapat diterapkan di dalam dunia kriptografi sebagai pembangkit kunci acak yang nantinya akan diolah sebagai sarana dalam melakukan proses enkripsi dan dekripsi. Semakin acak bilangan yang dihasilkan, semakin baik pula tingkat keamanan dari suatu cipherteks.

Penelitian ini secara khusus membahas tentang bagaimana teori chaos diterapkan pada penyandian menggunakan metode *Beaufort Cipher* untuk meningkatkan keamanan pada kunci yang digunakan. Berdasarkan hasil pengujian yang dilakukan terhadadap citra yang diujikan menunjukkan bahwa algoritma *Beaufort Cipher* yang menggunakan kunci yang dibangkitkan menggunakan fungsi chaos terbukti efektif dan aman. Hal ini dibuktikan dengan rata-rata waktu proses yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi cukup cepat yaitu sekitar 0,7 detik. Dan berdasarkan pengujian secara visual dan uji statistik algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan *statistical attack* oleh kriptanalis.
Kata kunci: kriptografi, *beaufort cipher,* fungsi chaos*.*

PENDAHULUAN

Nilai informasi sangat penting, oleh karena itu informasi memerlukan pengamanan yang baik saat didistribusikan ataupun saat disimpan. Salah satu metode pengamanan data adalah dengan proses penyandian terhadap data yang akan dikirimkan. Pada penelitian ini proses penyandian yang dilakukan adalah dengan menggunakan kriptografi. Kriptografi melingkupi proses transformasi informasi yang berlangsung dua arah, yang terdiri dari proses enkripsi dan dekripsi. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia (Gambar 1).



Gambar 1. Blok Diagram Teknik Kriptografi Berbasis Kunci

Keamanan dari sebuah kriptografi diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan chiperteks menjadi plainteksnya tanpa mengetahui kunci yang digunakan, . semakin kuat algoritma kriptografi tersebut, yang berarti semakin aman digunakan untuk menyandikan data. Selain itu proses penyandian harus menggunakan kunci yang memenuhi sifat acak dan tanpa pola atau hanya dipakai sekali saja.

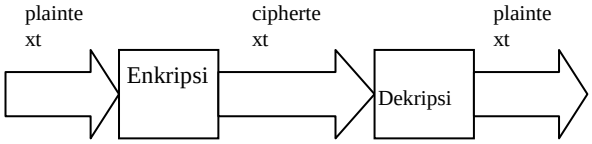
Perumusan masalahnya adalah bagaimana merancang sebuah cipher yang dikembangkan dari salah satu algoritma kriptografi klasik yaitu Beaufort cipher menggunakan pembangkit kunci chaos yang berpotensi untuk menjadi *unbreakable cipher*selanjutnya digunakan untuk menyandikan data citra. Sedang batasan masalah dalam penelitian ini meliputi: data yang digunakan adalah citra warna dengan ukuran 256 x 256 pixel dan analisis serta pengujian implementasi algoritma enkripsi dilakukan pada aspek korelasi, entropi, histogram warna, serta waktu proses dengan bantuan perangkat lunak Matlab.

Saroj Kumar Panigrahy - Bibhudendra Acharya - Debasish Jena (2008), yang meneliti penyandian data citra menggunakan algoritma Hill Cipher, hasil penelitian yang diperoleh menunjukkan bahwa metode Hill Cipher tidak akan berhasil apabila digunakan untuk menyandikan citra yang mempunyai background dengan warna yang sama atau grayscale.

Setyaningsih, E(2010) melakukan penelitian untuk mengamankan data image menggunakan metode vigenere cipher. Metode *vigenere cipher* akan semakin baik hasilnya apabila menggunakan kunci dengan ukuran minimal 0,2% dari ukuran pixel citra yang akan dienkripsi. Setyaningsih E, Iswahyudi C, dan Widyastuti N(2012) melakukan penelitian untuk mengamankan data citra yang diimplementasikan pada telepon seluler. Pada penelitian ini digunakan konsep kriptografi superenkripsi dengan menggabungkan 2 (dua) metode kriptografi yaitu metode playfair cipher dan vigenere cipher. Dari keseluruhan hasil pengujian dan analisis algoritma super enkripsi ini dapat dikatakan efektif dan aman sehingga layak digunakan untuk mengamankan data citra.Dari ketiga penelitian tersebut membuktikan bahwa metode kriptografi klasik bisa digunakan untuk menyandikan tidak hanya pesan dalam bentuk teks namun juga pesan dalam bentuk image. Penelitian Setyaningsih(2010) yang menggunakan metode vigenere cipher mempunyai kelemahan apabila kunci yang digunakan sangat pendek, karena mempunyai celah berupa perulangan kunci yang digunakan untuk mengenkripsi plainteks yang berupa citra, untuk mengatasi perulangan kunci yang digunakan pada proses panyandian dapat digunakan pembangkit kunci berbasis chaos.

Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan, keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi. Sistem kriptografi (*kryptosystem*) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Fungsi-fungsi yang mendasar dalam kriptografi adalah *enkripsi* dan *dekripsi. Enkripsi* adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (*plainteks*) menjadi sebuah kode yang tidak bisa dimengerti (*cipherteks*). Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut *dekripsi*. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



Gambar 2. Mekanisme kriptografi

Beaufort cipher

Beaufort cipher merupakan salah satu varian dari metode *vigenere cipher*. Pada *beaufort cipher* kunci K adalah urutan huruf-huruf K= k_1 … k_d dimana k_i didapat dari banyak penggeseran pada alfabet ke-I sama seperti pada vegenere cipher.

Formula *beaufort cipher* :

Misalkan *m* menentukan beberapa nilai integer positive. Diberikan P= C = K = $(Z_{26})^m$.

untuk sebuah kunci K = (k_1, k_2, …, k_m), kita definisikan :

$e_K(x_1, x_2, \ldots, x_m) = (k_1 - x_1, k_2 - x_2, \ldots, k_m - x_m)$ (2.1)

dan

$d_K(y_1, y_2, \ldots, y_m) = (k1 - y1, k_2 - y_2, \ldots, k_m - y_m)$ (2.2)

dimana semua operasi adalah berbasis pada Z_{26}

Rumus enkripsi yang digunakan untuk menghitung nilai cipher image tiap pixel adalah sebagai berikut :

$$E_{ki}(a) = (a - ki) \bmod 256 \quad (2.3)$$

Sedangkan rumus yang digunakan untuk mendapatkan kembali plainteks yang berupa image tiap pixel yang telah terenkripsi (dekripsi) adalah:

$$E_{ki}(a) = (a + ki) \bmod 256 \quad (2.4)$$

Pembangkit Bilangan Acak Berbasis Chaos

Teori chaos ini merupakan cabang dari matematika yang mempelajari bagaimana membangkitkan bilangan secara acak. Fenomena umum di dalam teori *chaos*, yaitu peka terhadap perubahan nilai awal (*sensitive dependence on initial condition*). Satu masalah yang muncul dari bilangan acak dengan chaos adalah nilai yang berupa bilangan riil antara 0 dan 1, sedangkan kriptografi yang digunakan unutk menyandikan data image menggunakan derajad keabuan 256 yang terdiri dari nilai 0 – 255. Agar barisan nilai chaos dapat digunakan untuk enkripsi dan dekripsi data image maka nilai chaos dikonversi ke integer. Teknik konversi dapat dilakukan dengan mengambil 3 angka terakhir pada bagian mantissa bilangan riil. Sebagai contoh dari 0.024568 diambil 3 angka terakhir dari bagian mantissanya yaitu 568.

Konversi nilai chaos ke integer dilakukan dengan menggunakan fungsi pemotongan. Caranya nilai chaos dikalikan dengan 10 berulangkali sampai ia mencapai panjang angka (size) yang diinginkan, lalu memotong hasil perkalian tersebut untuk mengambil bagian integer-nya saja. Secara matematis nilai chaos x dikonversikan ke integer dengan menggunakan persamaan 2.5 (Lampton, 2002) :

$$T(x, size) = \left\| x * 10^{count} \right\|, \quad x \neq 0 \quad (2.5)$$

Analisis Enkripsi

Untuk mengetahui apakah algoritma enkripsi yang diusulkan cukup aman untuk diimplementasikan, dilakukan analisis dan pengujian algoritma enkripsi menggunakan beberapa parameter korelasi, entropi, histogram warna, waktu proses dan kualitas enkripsi.

Penghitungan korelasi dan entropi dilakukan untuk menilai kualitas citra hasil enkripsi. Semakin rendah korelasi antar piksel dan semakin tinggi entropinya, maka sistem enkripsi dapat dikatakan aman.

Untuk menghitung korelasi digunakan rumus (Younes, 2008) :

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{\left[n\sum(x^2) - (\sum x)^2\right]\left[n\sum(y^2) - (\sum y)^2\right]}} \quad (2.6)$$

Entropi.

Teori informasi merupakan teori matematik dalam komunikasi data yang dikemukakan oleh Shannon pada tahun 1949 (Stinson, 1995). Teori informasi modern peduli dalam hal koreksi kesalahan, kompresi data, kriptografi, serta sistem komunikasi.

Entropi dari pesan dapat dihitung dengan rumus (Younes, 2008) :

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2(P(k)) \quad (2.7)$$

Dalam praktek, jika sebuah informasi dienkripsi dan dalam kondisi teracak, nilai entropi yang ideal adalah 7,99902 (≈8). Dengan demikian sistem enkripsi yang dirancang aman dari serangan entropi. Namun jika nilai entropi lebih kecil dari 8, dapat dikatakan sistem enkripsi masih dapat ditebak (Jolfaei dan Mirghadri, 2011).

Analisis histogram.

Teknik analisis histogram warna digunakan untuk melihat kesesuaian distribusi warna antara *plain image* dengan *cipher image*. Jika nilai histogram *cipher image* memiliki distribusi keragaman dan memiliki perbedaan yang signifikan dengan histogram *plain image*-nya, maka dapat dikatakan *cipher image* tidak memberikan petunjuk apa-apa untuk melakukan *statistical attack* pada algoritma enkripsi yang digunakan. Dengan histogram dapat dicari citra yang memiliki kemiripan komposisi warna.

Kualitas Enkripsi.

Pengukuran kualitas enkripsi dilakukan dengan membandingkan nilai piksel citra sebelum dan sesudah dienkripsi. Semakin tinggi tingkat perubahan piksel, maka enkripsi citra dikatakan lebih efektif dan oleh sebab itu dinyatakan lebih aman (Jolfaei dan Mirghadri, 2011). Ukuran kualitas enkripsi dinyatakan sebagai deviasi antara *plain image* dan *cipher image*. Kualitas enkripsi merepresentasikan jumlah rata-rata perubahan setiap derajat keabuan.Untuk

mengukur kualitas enkripsi digunakan rumus (Jolfaei dan Mirghadri, 2011):

$$EQ = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \qquad (2.8)$$

Analisis waktu proses.

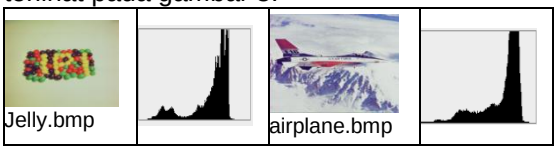
Analisis waktu proses dilakukan dengan cara membandingkan *initial process* dengan akhir proses pada saat dilakukan enkripsi dan dekripsi.

Penelitian ini bertujuan untuk membangun penyandian citra menggunakan metode *Beaufort cipher* menggunakan pembangkit kunci chaos dan diharapkan dapat memberikan kontribusi bagi keamanan data citra. Secara garis besar manfaat dari penelitian ini adalah memberikan kontribusi dalam pengembangan iptek, terutama pada keamanan data, menguji kehandalan metode kriptografi *beaufortcipher* menggunakan pembangkit kunci chaos, mengembangkan pengajaran ilmu di bidang penyandian data, pengolahan citra dan keamanan data.

Bahan Penelitian

Percobaan dilakukan dengan menggunakan citra dengan format bmp berukuran 256x256 piksel, yang dibedakan berdasarkan karakteristik tingkat kecerahan dan tingkat kontras dari citra. Citra yang digunakan pada pengujian dikelompokkan menjadi dua kelompok yaitu :

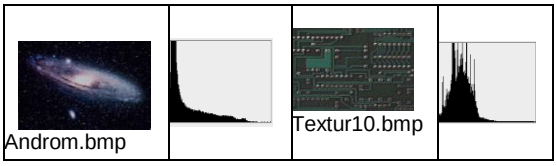
Berdasarkan tingkat kecerahan citra (*brightnes*). Tingkat kecerahan dari suatu citra dapat dilihat dari histogram warna yang mengelompok di salah satu sisi saja. Citra yang mewakili citra cerah. Pada pengujian diambil contoh citra yang histogramnya mengelompok di sisi sebelah kanan seperti terlihat pada gambar 3.



Gambar 3 Contoh citra yang mewakili citra cerah

Citra yang mewakili citra gelap. Pada pengujian diambil contoh citra yang histogramnya mengelompok di sisi sebelah kiriseperti terlihat pada gambar 4

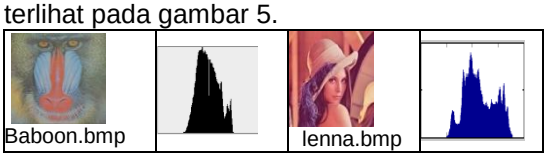
.



Gambar 4. Contoh citra yang mewakili citra gelap

Berdasarkan kekontrasan citra (*contrast*)

Tingkat kekontrasan dari suatu citra dapat dilihat dari histogramnya yang menyempit di bagian tengah atau melebar. Citra yang mewakili kontras rendah. Pada pengujian diambil contoh citra yang histogramnya menyempit seperti terlihat pada seperti terlihat pada gambar 5.



Gambar 5. Contoh citra yang mewakili citra dengan kontras rendah

Citra yang mewakili kontras tinggi. Pada citra jenis ini apabila dilihat dari histogramnya terlihat melebar seperti terlihat pada gambar 6

Gambar 6 Contoh citra yang mewakili citra dengan kontras tinggi

Alat Penelitian

Pada penelitian ini konfigurasi system yang digunakan untuk mengimplementasikan perangkat lunak yang akan dibangun adalah menggunakan bahasa pemrograman Matlab versi. R2009a menggunakan GUI *(Graphical User Interface)* dan system operasi Windows Seven dengan spesifikasi komputer sebagai berikut :Processor Core2 Duo T7100 1.8 GHz, RAM 4 Gigabytes

Tahap-tahap yang akan dilakukan terdiri dari tahap inisiasi, pembangunan prototype, pengujian, verifikasi dan analisis.Pada tahap verifikasi dilakukan verifikasi terhadap aplikasi program setelah dilakukan perbaikan-perbaikan atas dasar hasil pengujian pada aspek pemrograman maupun konfigurasi progam yang digunakan untuk memastikan bahwa program tersebut siap diterapkan untuk aplikasi pengamanan data citra yang akan dikirimkan melalui jalur komunikasi. Kemudian menganalisis hasil enkripsi dan dekripsi untuk berbagai contoh citra yang diujikan.

Tabel 1. Kunci berbasis chaos yang dibangkitkan dengan nilai awal xo yang berbeda

xo awal	10 Kunci Berbasis Chaos									
0.5105502	179	45	162	20	78	34	136	135	228	32
0.51055	212	41	187	126	142	209	51	116	132	221
0.5105	251	204	247	123	228	188	76	210	253	102
0.51	182	233	226	114	229	230	77	183	187	214
0.5	99	225	52	211	211	231	185	182	120	62
5	216	160	225	75	195	232	82	204	36	232
51	210	135	35	24	217	232	19	136	166	100
5105	8	126	52	247	134	153	245	103	212	211
51055	47	188	88	79	126	148	92	69	228	237
5105502	53	129	109	49	66	116	20	121	26	172

Dari tabel 1 terlihat bahwa apabila terdapat perubahan data meskipun sangat kecil menyebabkan perubahan yang sangat signifikan pada kunci yang dibangkitkan.

Algoritma pada gambar 7. menjelaskan langkah-langkah proses enkripsi data citra menggunakan metode *Beufort cipher* menggunakan kunci berbasis chaos.

Langkah untuk proses enkripsi sebagai berikut

Inputkan plain image yang akan dilakukan proses enkripsi.

Inputkan kunci yang telah disepakati antara pengirim dan penerima. Pada algoritma ini inputan kunci minimal adalah angka 1 sedangkan maksimalnya tidak ditentukan namun lebih baik tidak terlalu panjang sehingga mudah diingat.

Bangkitkan kunci chaos sebanyak m x n piksel berdasarkan nilai kunci yang diinputkan sehingga nantinya akan terbentuk matrik kunci ukuran m x n piksel sesuai dengan ukuran plain image.

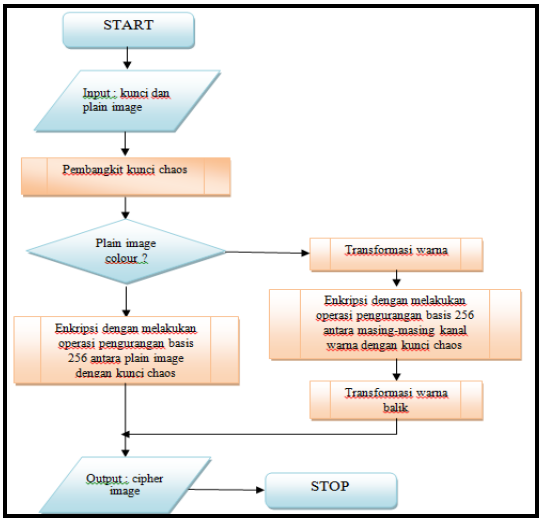
Untuk citra warna dilakukan proses transformasi warna sehingga nilai RGB tiap piksel terpisah. Pada aplikasi MATLAB untuk memisahkan komponen warna citra menggunakan perintah

Red =citra(:,:,1); Green = citra(:,:,2) ; Blue = citra(:,:,3).

Selanjutnya dilakukan operasi pengurangan berbasis 256 pada masing-masing komponen warna (Red, Green, Blue) dengan matrik kunci.

Vektor hasil enkripsi dikembalikan sebagai nilai RGB menggunakan transformasi warna balik sehingga menghasilkan citra baru yang sudah tersandikan.

Untuk citra grayscale proses selanjutnya adalah melakukan pengurangan berbasis 256 antara plain image dengan matrik kunci. Hasil dari proses ini adalah cipher baru yang telah tersandikan.



Gambar 7. Algoritma Enkripsi Menggunakan Metode*Beufort Cipher*

AlgoritmaDekripsi Citra

Algoritma pada gambar 8. menjelaskan langkah-langkah proses dekripsi data citra menggunakan metode *Beufort cipher* menggunakan kunci berbasis chaos.

Langkah untuk **proses enkripsi** sebagai berikut :

Inputkan cipher image yang akan dilakukan proses enkripsi.

Inputkan kunci yang telah disepakati antara pengirim dan penerima.

Bangkitkan kunci chaos sebanyak m x n piksel bedasarkan nilai kunci yang diinputkan sehingga nantinya akan terbentuk matrik kunci ukuran m x n piksel sesuai dengan ukuran cipher image.

Untuk citra warna

Dilakukan proses transformasi warna sehingga nilai RGB tiap piksel terpisah.

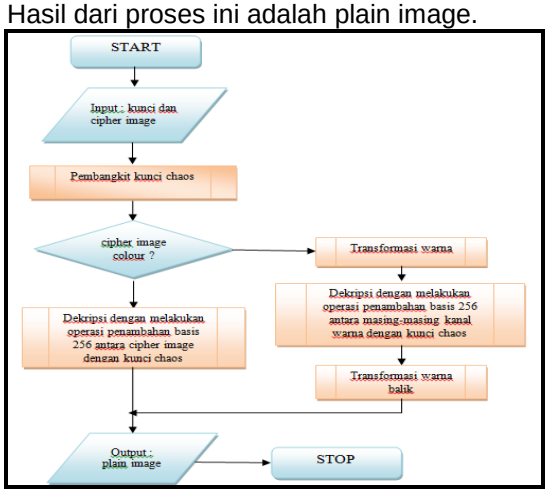
Pada aplikasi MATLAB untuk memisahkan komponen warna citra menggunakan perintah

Red =citra(:,:,1); Green = citra(:,:,2) ; Blue = citra(:,:,3).

Selanjutnya dilakukan operasi penjumlahan berbasis 256 pada masing-masing komponen warna (Red, Green, Blue) dengan matrik kunci.

Vektor hasil dekripsi dikembalikan sebagai nilai RGB menggunakan transformasi warna balik sehingga menghasilkan plain image.Untuk cipher image grayscale proses selanjutnya adalah melakukan penambahan berbasis 256 antara cipher image dengan matrik kunci.

Hasil dari proses ini adalah plain image.



Gambar 8. Algoritma Dekripsi Menggunakan Metode*Beufort Cipher*

Perancangan Sistem

Perangkat lunak penyandian citra yang nantinya akan digunakan untuk menganalisa hasil penyandian citra ini terdiri dari dari 2 bagian, yaitu :

Bagian untuk melakukan proses enkripsi *citra*

Masukannya adalah berupa *citra* berwarna ataupun grayscale (*.bmp) dan kunci.Outputnya berupa citra hasil penyandian, nilai parameter yang digunakan untuk menganalisis kekuatan algoritma yang digunakan, yang terdiri dari nilai entropi, kualitas enkripsi, analisis korelasi dan waktu proses enkripsi . Pada system ini juga dapat dilakukan untuk menyimpan kunci yang digunakan untuk mengenkripsi dengan format kunci (*.key), mengambil kunci yang tersimpan di media penyimpanan, sertadapat digunakan untuk menyimpan citra yang telah dienkripsi dengan mengunakan format bmp (*.bmp). Selain itu aplikasi ini juga menampilkan informasi histogram hasil penyandian menggunakan metode *Beufort cipher*.

Bagian untuk proses dekripsi.

Masukan berupa cipher image, citra yang telah tersandikan menggunakan metode *Beufort cipher,* serta kunci yang akan digunakan untuk melakukan dekripsi. Selain itu aplikasi juga dapat mengambil kunci yang akan digunakan untuk melakukan dekripsi pada media penyimpanan, menampilkan hasil dekripsi citra menggunakan kunci yang digunakan, serta waktu proses.

Rancangan Sistem Halaman Depan

Antarmuka grafis pada halaman depan yang dibuat dalam bentuk menu toolbar seperti terlihat pada gambar 9

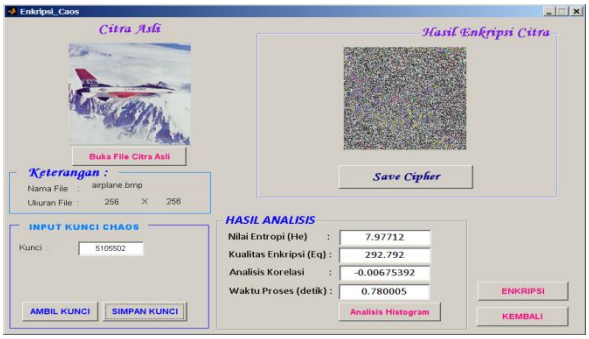
Gambar 9. Tampilan halaman depan

Antarmuka tersebut terdiri dari 3 tombol, yaitu :

Tombol untuk proses Enkripsi, Tombol untuk proses Dekripsi, dan Tombol Keluar.

Rancangan Aplikasi Proses Enkripsi Citra

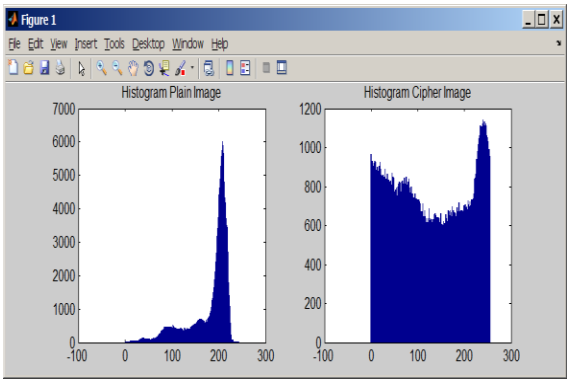
Antarmukapada proses enkripsi dibuat dalam bentuk desktop seperti terlihat pada gambar 10



Gambar 10. Tampilan proses enkripsi citra

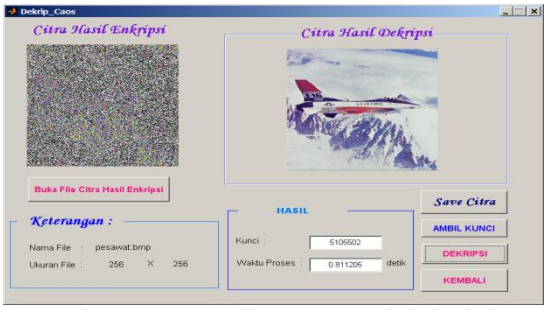
Antarmuka proses enkripsi citra terdiri dari :

Tombol Buka File Citra Asli, Editor text, Tombol Ambil Kunci, Tombol Simpan, TombolSave Cipher, Tombol Enkripsi,Tombol Analisis Histogram seperti terlihat pada gambar 11.



Gambar 11. Tampilan histogram plain image dan cipher image

Rancangan Aplikasi Proses Dekripsi Citra Antarmukapada proses dekripsi dibuat dalam bentuk desktop seperti terlihat pada gambar 12



Gambar 12. Tampilan proses dekripsi citra

Antarmuka proses dekripsi citra terdiri dari Tombol Buka File Citra Hasil Enkripsi, Tombol Save Citra, Tombol Ambil Kunci, Tombol Dekripsi, dan Tombol Kembali.

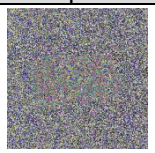
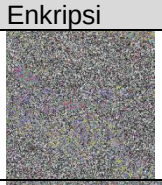
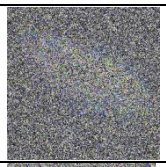
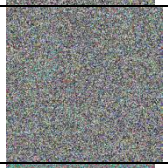
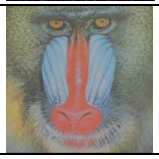
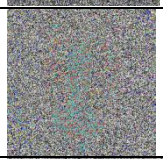
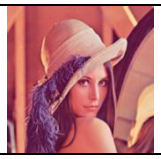
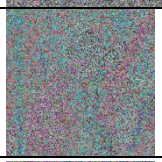
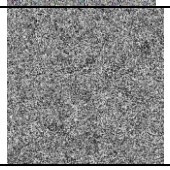
HASIL DAN PEMBAHASAN

Penelitian ini dilakukan pengujian dan analisis pada beberapa contoh citra sebagaimana ditampilkan pada gambar 3, gambar 4, gambar 5, dan gambar 6 dengan menggunakan Kunci 5105502 dengan nilai r = 4 dengan size = 3 yang menyatakan panjang digit angka hasil konversi chaos ke nilai integer karena kunci yang diijinkan adalah angka 0 sampai 255.

Uji Visual dan Analisis Histogram

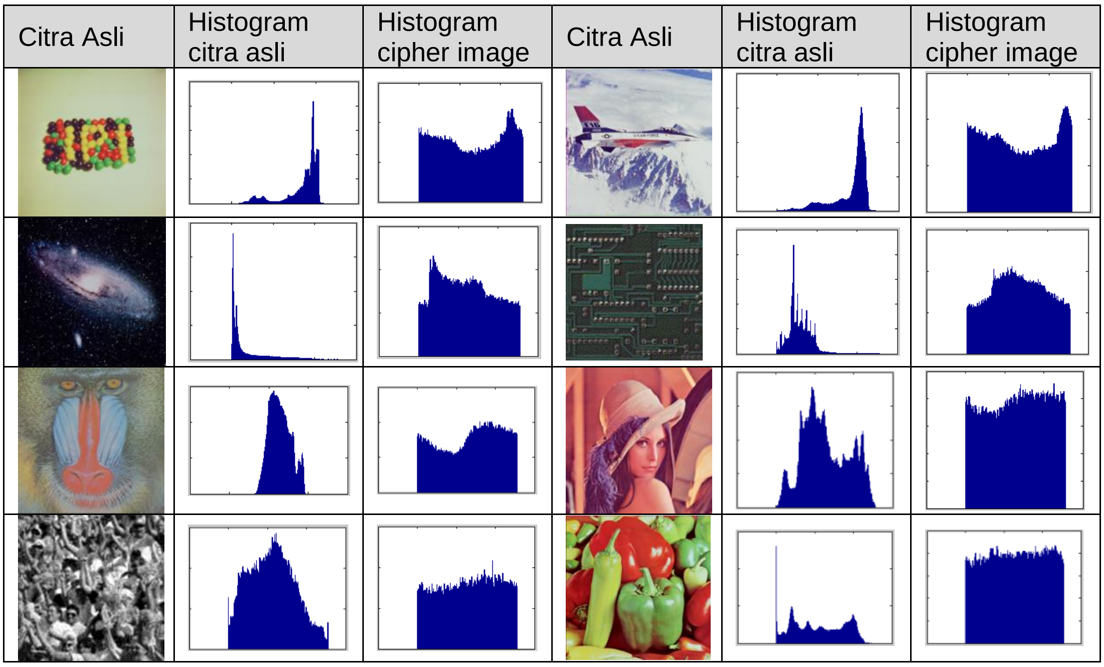
Dari hasil pengujian 2 kelompok citra yang berbeda tingkat kecerahan citra (*brightness*) dan kekontrasan citra (*contrast*) menggunakan kunci yang sama, maka berdasarkan uji secara visual dapat dilihat hasilnya pada tabel 2

Tabel 2. Hasil uji visual citra

Kelompok citra	Citra Asli	Citra Hasil Enkripsi	Citra Asli	Citra Hasil Enkripsi
Cerah				
Gelap				
Kontras Rendah				
Kontras Tinggi				

Dari Tabel 2 terlihat bahwa citra asli tidak dapat terlihat setelah dilakukan proses enkripsi. Hasil penyandian citra menunjukkan keteracakan warna dan perubahan intensitas warna yang cukup signifikan. Hal ini menunjukkan bahwa proses enkripsi berhasil dengan baik untuk semua kelompok citra yang diujikan.

Tabel 3. Hasil analisis histogram



Berdasarkan pengamatan secara visual dari histogram *plain image* dengan histogram dari *cipher image* pada tabel 3, terlihat histogram *cipher image* memiliki perbedaan yang cukup signifikan dengan histogram *plain image*-nya, hal ini menunjukkan distribusi keragaman intensitas warna yang cukup baik. Hasil uji visual pada histogram *cipher image* terlihat relatif datar hal ini memperlihatkan bahwa distribusi kemunculan setiap intensitas relatif sama, hal ini menunjukkan bahwa algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan *statistical attack* oleh kriptanalis.

Uji Statistik

Parameter uji statistik yang digunakan dalam pengujian algoritma enkripsi adalah korelasi, entropi, kualitas enkripsi dan waktu proses enkripsi dan dekripsi. Hasil dari pengujian statistik dapat dilihat pada tabel 4.

Tabel 4. Hasil uji statistik

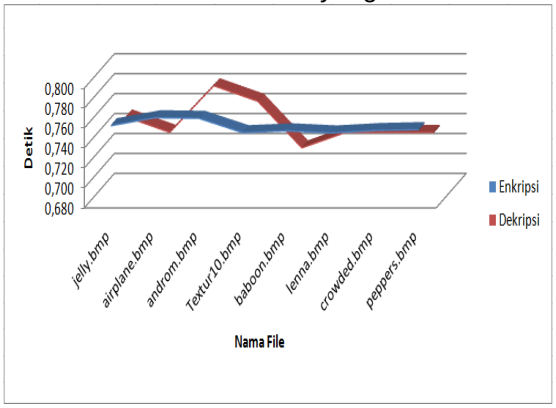
Nama File	Ukuran Piksel	Ukuran File (KB)	Hasil Pengukuran Nilai			Waktu Proses (detik)	
			He	Eq	Ic	Enkripsi	Dekripsi
jelly.bmp	256 x 256	193	7,9561	353,471	-0,000753	0,757	0,749
airplane.bmp	256 x 256	193	7,9771	292,792	-0,006754	0,765	0,733
androm.bmp	256 x 256	193	7,9661	303,151	0,091281	0,765	0,780
Textur10.bmp	256 x 256	193	7,9556	338,487	0,020862	0,750	0,764
baboon.bmp	256 x 256	193	7,9706	313,979	-0,002980	0,752	0,718
lenna.bmp	256 x 256	193	7,9880	212,596	-0,000995	0,750	0,733
crowded.bmp	256 x 256	193	7,9934	110,984	0,004590	0,752	0,733
peppers.bmp	256 x 256	193	7,9854	205,536	0,013126	0,753	0,733
Rata-rata			7,9740	266,375	0,014797	0,756	0,743

Dari tabel 4 terlihat rata-rata nilai untuk 2 kelompok citra yang diujikan rata-rata nilai entropinya (He) adalah 7.9740. Berdasarkan teori yang dikemukakan oleh Jolfae dan Mirghadri (2011) bahwa jika sebuah informasi dienkripsi dan dalam kondisi teracak maka nilai entropi yang ideal adalah ≈ 8. Berdasarkan teori tersebut maka algoritma enkripsi yang dirancang ini aman dari serangan entropi atau

sulit ditebak oleh kriptanalis karena nilainya sangat dekat dengan 8.

Kekuatan dari suatu algoritma enkripsi selain diukur dari nilai entropi juga diukur berdasarkan nilai korelasinya (Ic) dengan skala 0 sampai 1. Variabel yang dimaksud pada penelitian ini adalah intensitas citra pada plain image terhadap cipher image. Dari tabel 5.3 terlihat bahwa nilai korelasi antara *plain image* dengan *cipher image* rata-rata bernilai 0,014797. Karena rata-rata nilai korelasinya mendekati nol maka keterhubungan antara plain image dan cipher image tidak ada. Hal ini menunjukkan bahwa sistem enkripsi yang diusulkan sesuai dengan teori *perfect secrecy* yang dikemukakan oleh Shannon, yaitu semakin rendah korelasi antar piksel dan semakin tinggi entropinya, maka sistem enkripsi dapat dikatakan aman (Stinson, 1995).

Untuk mengukur kualitas enkripsi citra dilakukan dengan membandingkan nilai piksel citra sebelum dan sesudah dienkripsi. Dari hasil pengujian 2 kelompok citra seperti terlihat pada tabel 5.3. diperoleh rata-rata kualitas enkripsi sebesar 266,375. Nilai kualitas enkripsi ini cukup tinggi yang artinya tingkat perubahan piksel-nya pun juga tinggi sehingga sistem ini dapat dikatakan efektif dan aman. Rata-rata waktu enkripsi untuk citra dengan ukuran 256 x 256 adalah 0,756 detik. Sedangkan rata-rata waktu dekripsi citra dengan ukuran 256 x 256 adalah 0,743 detik. Grafik waktu proses enkripsi dan dekripsi secara terinci disajikan dalam gambar 13. Dari hasil tersebut dapat dinyatakan bahwa algoritma ini cukup efektif untuk penyandian data citra warna, karena rata-rata waktu proses yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi tidak membutuhkan waktu yang lama.



Gambar 13. Grafik waktu proses enkripsi dan dekripsi

Hal ini disebabkan pembangkit kunci chaos berhasil menambahkan panjang kunci yang nilainya acak, sehingga metode ini cukup aman.

KESIMPULAN

Berdasarkan pengujian yang dilakukan secara visual citra hasil enkripsi tidak terlihat lagi yang disebabkan karena keteracakan warna dan perubahan intensitas warna yang cukup signifikan. Histogram *cipher image* memiliki perbedaan yang cukup signifikan dengan histogram *plain image*-nya, hal ini menunjukkan distribusi keragaman intensitas warna yang cukup baik. Hasil uji visual pada histogram *cipher image* terlihat relatif datar hal ini memperlihatkan bahwa distribusi kemunculan setiap intensitas relatif sama, hal ini menunjukkan bahwa algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan *statistical attack* oleh kriptanalis Berdasarkan uji statistik didapatkan rata-rata nilai entropinya (He) adalah 7.9740, nilai korelasi antara *plain image* dengan *cipher image* bernilai 0,014797, dan kualitas enkripsi sebesar 266,375, hal ini menyatakan bahwa algoritma enkripsi yang dirancang ini aman.Algoritma ini cukup efektif untuk penyandian data citra warna, karena rata-rata waktu proses yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi tidak membutuhkan waktu yang lama yaitu sekitar 0,7 detik.

Saran

Algoritma ini cukup simple, efektif dan aman untuk itu penelitian lanjutan perlu dilakukan untuk diimplementasikan padatelepon seluler yang mampu menghasilkan kombinasi yang baik antara kecepatan, pengamanan yang tinggi, kompleksitas, *reasonable computational overhead*, dan *computational power*.

DAFTAR PUSTAKA

Jolfaei, A. Dan Mirghadri, A., 2011, “Image Encryption Using Chaos and Block Cipher”, *Computer and Information Science, Vol. 4., No.1., January 2011.*

Lampton, J., 2002, “Chaos Cryptography: Protecting Data Using Chaos”, Missisippi School for Mathematics and Science.

Panigrahy, S.K., Acharya, B., and Jena, D., 2008, “Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm”, *1st International Conference on Advances in Computing,* Chikhli, India, 21-22 February 2008.

Setyaningsih, E., 2010, “Konsep Superenkripsi Untuk Penyandian Citra Warna Menggunakan Kombinasi Hill Cipher dan Playfair Cipher”, *Jurnal Ilmiah Nasional SITRORIKA,* Januari 2010

Setyaningsih, E., 2010, “Pengembangan Metode Vigenere Cipher Untuk Pengamanan Data Citra”,Laporan Penelitian, Lembaga Penelitian IST AKPRIND Yogyakarta, Februari 2010.

Setyaningsih, E. Iswahyudi, C., Widyastuti, N. (2012) Image Encryption on Mobile Phone using Super Encryption Algorithm. *National Journal TELKOMNIKA.* 2012.10(4): 599-608

Stinson, R Douglas, 1995, *Cryptography Theory and Practice*, CRC Press, Inc, Boca Raton, London

Younes, M.A.B., Jantan, A., 2008,”Image Encryption Using Block-Based Transformation Algorithm”, *IAENG International Journal of Computer Science, 35:1,* Februari 2008