Algoritma Enkripsi Selektif Citra Digital dalam Ranah Frekuensi Berbasis Permutasi *Chaos*

Rinaldi Munir
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung (ITB)
email: rinaldi-m@stei.itb.ac.id

Abstract—Di dalam makalah ini dipresentasikan algoritma enkripsi selektif pada citra digital dalam ranah frekuensi. Citra ditransformasikan ke ranah frekuensi dengan Discrete Cosine Transform (DCT), kemudian koefisien-koefisien DCT dipindai secara zigzag, dan elemen-elemen pada sub-band frekuensi rendah diambil. Enkripsi dilakukan hanya pada sebagian elemen berfrekuensi rendah dengan cara mempermutasikannya menggunakan chaos map 2D, yaitu Arnold Cat Map, selanjutnya IDCT diterapkan untuk memperoleh citra terenkripsi. Algoritma enkripsi ini termasuk ke dalam lossy encryption. Eksperimen terhadap citra grayscale maupun citra berwarna memperlihatkan bahwa citra dapat dienkripsi dengan baik. Histogram citra hasil enkripsi berbeda signifikan dengan histogram citra semula, dan pixel-pixel di dalamnya tidak lagi berkorelasi.

Kata Kunci. Citra, enkripsi selektif, ranah frekuensi, DCT, Arnold Cat Map, chaos.

Abstract—This paper presents a selective image encryption in frequency domain. At first, the image is transformed into frequency domain with Discrete Cosine Transform (DCT), and then DCT coefficients are scanned in zigzag, and elements of the low-frequency sub-band are extracted. Encryption is performed only on selected elements by scrambling them using 2D chaos map, namely Arnold Cat Map. Next, IDCT is applied to obtain the encrypted image. The encryption algorithm is included in lossy encryption. Experiments on both grayscale images and color images show that the images can be encrypted succesfully. Histograms of the encrypted images differ significantly from histogram of the original images, and the pixels in the encrypted images are not longer correlated.

Kata Kunci. Image, selective encryption, frequency domain, DCT, Arnold Cat Map, chaos

I. PENDAHULUAN

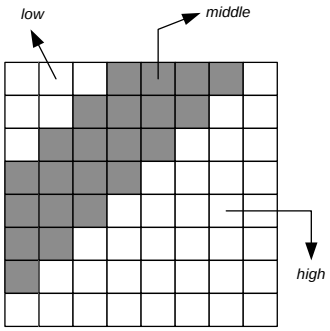
Perkembangan teknologi informasi telah membuat penyimpanan dan pengiriman media digital seperti citra dan video menjadi lebih mudah dan efisien. Persoalan yang timbul dari kemudahan itu adalah keamanan informasi seperti privasi dan kerahasiaan. Citra yang disimpan atau didistribusikan dalam bentuk *plain-image* rentan terhadap penyadapan atau pengaksesan oleh pihak-pihak yang tidak berhak (*unauthorized party*). Salah satu teknik untuk melindungi informasi di dalam citra adalah dengan mengenkripsinya menjadi informasi yang tidak bermakna (*cipher-image*).

Algoritma enkripsi konvensional untuk pesan teks seperti *DES*, *AES*, *Blowfish*, *RSA*, dan lain-lain kurang cocok untuk mengenkripsi citra karena karakteristik citra yang mempunyai volume data yang besar dan redundansi yang tinggi pada *pixel-pixel*-nya. Karena alasan itu, maka para ilmuwan mengembangkan algoritma enkripsi khusus untuk citra digital. Algoritma enkripsi citra dapat digolongkan menjadi dua kelompok: enkripsi selektif dan enkripsi total (non-selektif). Algoritma enkripsi selektif – sebagai lawan dari enkripsi total [1] -- hanya mengenkripsi sebagian elemen saja di dalam citra namun efeknya keseluruhan citra terenkripsi. Tujuan algoritma enkripsi selektif adalah meminimalkan volume komputasi (yang artinya menghemat waktu komputasi), sehingga ia cocok diterapkan untuk aplikasi yang mensyaratkan kebutuhan *real-time* seperti *teleconference*, *live video streaming*, yang jelas-jelas jelas memerlukan *delay* yang rendah.

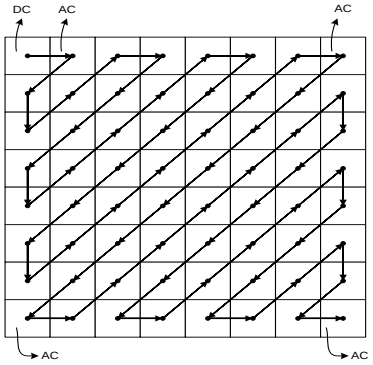
Enkripsi citra (baik selektif maupun non-selektif) dapat dilakukan baik dalam ranah spasial, ranah frekuensi, maupun gabungan keduanya. *Review* dan performansi beberapa algoritma algoritma enkripsi selektif dapat ditemukan di dalam [2, 3].

Kebanyakan enkripsi citra menerapkan teknik permutasi – atau istilah lainnya pengacakan (*scrambling*) – di dalam algoritmanya. Pengacakan bertujuan untuk mentransformasikan citra ke dalam bentuk yang tidak berarti, membuat informasi di dalamnya menjadi tidak terurut dan tidak sistematis, sehingga meningkatkan kompleksitas komputasi terhadap serangan *chosen-plaintext attack* [4].

Permutasi dalam ranah spasial, yang dilakukan dengan mengacak posisi *pixel-pixel* citra, memiliki kelemahan, yaitu *cipher-image* tetap mempertahankan karakteristik statistik citra setelah pengacakan. Hal ini ditunjukkan pada histogram *plain-image* dan *cipher-image* yang tetap sama.



Gambar 1. Pembagian tiga kanal frekuensi pada ranah *DCT*



Gambar 2. Pemindaian zig-zag

Kelemahan ini dapat digunakan oleh penyerang untuk mengungkapkam kembali *pixel-pixel* di dalam *plain-image.*

Untuk mengatasi kelemahan tersebut, maka pengacakan sebaiknya dilakukan dalam ranah frekuensi. Citra dalam ranah spasial terlebih dahulu ditransformasikan ke ranah frekuensi dengan sejumlah kakas antara lain *Fourier Transform*, *Discrete Cosine Transform*, *Fourier-Mellin Transform*, *Wavelet Trabsform*. Setelah elemen-elemen citra di dalam ranah frekuensi diacak, hasil transformasi balik ke ranah spasial menghasilkan *cipher-image* yang berbeda dan memiliki kerakteristik statistik yang tidak sama dengan *plain-image.* Jadi, pengubahan susunan elemen frekuensi dapat mengubah posisi *pixel* dan nilai-nilai *pixel* sekaligus.

Beberapa fungsi *chaos* (*chaos map*) sering digunakan untuk pengacakan, yaitu *Baker Map*, *Arnold Cat Map*, *Chen Map*, *Henon Map*, dan lain-lain. Penelitian tentang *chaos* merupakan topik yang atraktif di dalam kriptografi. *Chaos* dipakai di dalam kriptografi karena *chaos* berkelakukan acak, sensitivitas pada kondisi awal, dan tidak memiliki periode perulangan.

Di dalam makalah ini dipresentasikan usulan algoritma enkripsi selektif citra digital pada ranah frekuensi. Transformasi citra ke ranah frekeunsi dilakukan dengan menggunakan kakas Discrete Cosine Transform (DCT). Pemilihan DCT adalah karena kompatibalitasnya dengan standard JPEG untuk pengkodean citra digital. Enkripsi selektif pada ranah DCT dilakukan dengan menerapkan Arnold Cat Map pada elemen-elemen DCT yang dipilih.

Makalah ini dibagi menjadi lima bagan. Bagian pertama adalah pendahuluan ini yang menjelaskan state-of -the-art penelitian. Bagian kedua adalah konsep teoritis yang digunakan dalam penyusunan algoritma. Bagian ketiga adalah usulan algoritma enkripsi selektif. Bagian keempat adalah eksperimen dan pembahasan hasil-hasil, dan bagian kelima ditutup dengan kesimpulan.

II. STUDI PUSTAKA

Discrete Cosine Transform (*DCT*) dan *Arnold Cat Map* (*ACM*) adalah dua teori yang mendasari usulan algoritma enkripsi selektif dalam ranah frekuensi. *DCT* sebagai fungsi transformasi citra dari ranah spasial ke ranah frekuensi dan *ACM* sebagai fungsi permutasi. Keduanya dibahas dalam dua sub-bab terpisah berikut ini.

A. Discrete Cosine Transform

Jika citra digital dipandang sebagai sinyal dua dimensi, maka *DCT* 2D mentransformasikan citra *I* (yang berukuran $M \times N$) dari ranah spasial (x, y) ke ranah frekuensi (u, v) dengan persamaan berikut:

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N} \quad (1)$$

yang dalam hal ini

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}} & ,u = 0 \\ \sqrt{\frac{2}{M}} & ,1 \le u \le M-1 \end{cases} \quad ; \quad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}} & ,v = 0 \\ \sqrt{\frac{2}{N}} & ,1 \le v \le N-1 \end{cases}$$

Tranformasi DCT balik (invers DCT atau IDCT) mengembalikan data sinyal dari ranah frekuensi ke ranah spasial dengan persamaan

$$I(x,y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u,v) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N} \quad (2)$$

C(u, v) dinamakan koefisien DCT dari citra I. Elemen C(0,0) yang terletak di pojok kiri atas dinamakan koefisien DC, sedangkan sisanya dinamakan koefisien AC.

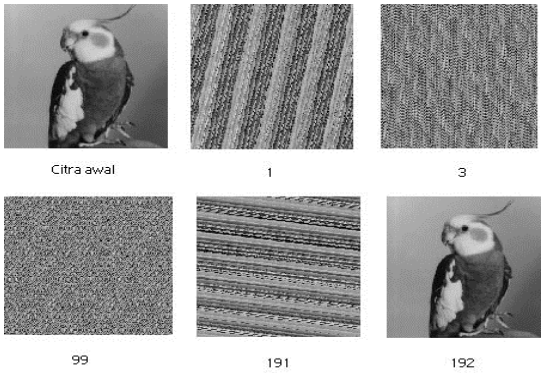
Transformasi *DCT* menempatkan koefisien-koefisien hasil transformasi ke dalam tiga *sub-band* frekuensi (*low*, *middle*, dan *high*), seperti ditunjukkan pada Gambar 1. Karakteristik visual citra yang paling penting berada pada *sub-band* frekuensi yang rendah, sedangkan informasi detil ditentukan oleh frekuensi yang tinggi [5]. Untuk mengekstrak *sub-band* frekuensi tertentu, maka matriks koefisien *DCT* dipindai secara *zig-zag* sebagaimana yang dilakukan di dalam algoritma kompresi *JPEG* (Gambar 2).

Karena *DCT* beroperasi dalam bilangan *floating point* yang menggunakan skema pembulatan dalam operasinya, maka *DCT* adalah transformasi yang *lossy*, artinya citra hasil *IDCT* tidak persis sama dengan citra semula.

B. Arnold Cat Map

Arnold Cat Map (*ACM*) adalah fungsi *chaos* dwimatra yang mentransformasikan koordinat (x, y) dari citra berukuran $N \times N$ ke koordinat baru (x', y'). Persamaan iterasinya adalah

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N)$$



Gambar 3. Hasil iterasi ACM pada citra 'bird'[7]

CM bersifat *reversible*, yaitu citra hasil transformasinya dapat dikembalikan ke citra semula dengan persamaan:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(N) \quad (4)$$

parameter *b* dan *c* adalah *integer* positif sembarang, dan determinan matriks $\begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}$ harus sama dengan 1 agar hasil transformasinya bersifat *area-preserving*, yaitu tetap berada di dalam area citra yang sama. *ACM* diiterasikan sebanyak *m* kali dan setiap kali iterasi menghasilkan citra yang terlihat seperti acak. Makin banyak jumlah iterasinya, makin acak citra hasil transformasi. Nilai *b*, *c*, dan *m* dapat dianggap sebagai kunci rahasia. Setelah diiterasi sejumlah *p* kali, citra hasil transformasi kembali sama dengan citra semula, seperti yang ditunjukkan pada Gambar 3. Nilai *p* berbeda-beda untuk setiap citra, bergantung pada *b*, *c*, *N*. Menurut [6], penelitian Freeman J. Dyson dan Harold Falk menemukan bahwa $T < 3N$.

Iterasi *ACM* pada citra dalam ranah spasial memiliki kelemahan. Citra acak yang dihasilkannya memiliki karakateristik statistik yang tidak berubah. Hanya lokasi *pixel* yang berubah, tetapi distribusi statistiknya tetap. Gambar 4 (atas) memperlihatkan histogram citra 'bird' dan Gambar 4 (tengah) histogram citra hasil transformasi *ACM* dalam ranah spasial setelah 5 kali iterasi tetap sama.

Hasil berbeda ditunjukkan jika pengacakan dilakukan pada ranah frekuensi. Histogramnya terlihat berbeda dengan histogram citra awal seperti yang diperlihatkan pada Gambar 4 (bawah). Hal ini terjadi karena menurut persamaan (2) nilai *pixel* pada lokasi (*x*, *y*) merupakan hasil resultan dari seluruh koefisien *DCT*. Perubahan susunan koefisien *DCT* akibat pengacakan mengubah hasil

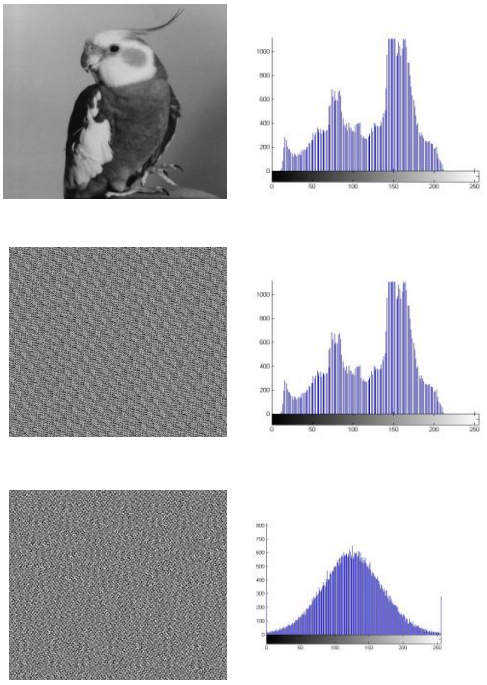
perhitungan pada *term cosinus* di dalam persamaan tersebut, sehingga nilai $I(x, y)$ yang dihasilkan berubah.

III. METODE

Di dalam bagian ini dipresentasikan algoritma enkripsi selektif yang diusulkan. Pembahasan dimulai dengan beberapa penelitian yang terkait dengan enkripsi citra dalam ranah *DCT*.

A. Related Works

Beberapa algoritma enkripsi citra dalam ranah *DCT* sudah pernah diusulkan. Droogenbroeck dan Benedett [4]



Gambar 4. *Atas*: citra 'bird' dan histogramnya; *Tengah*: hasil iterasi *ACM* terhadap citra 'bird' dalam ranah spasial dan histogramnya';
Bawah: hasil iterasi *ACM* terhadap citra 'bird' dalam ranah frekuensi dan histogramnya.

memilih koefisien *AC* untuk dienkripsi dengan algoritma *DES*, *Triple DES*, dan *IDEA*. Koefisien *DC* tidak dienkripsi karena koefisien *DC* membawa informasi visual yang penting.

Tang di dalam [8] mengusulkan metode enkripsi yang dinamakan permutasi zigzag yang diterapkan pada citra dan video berbasis *DCT*. Di satu sisi metode tersebut memberikan kerahasiaan pada gambar, tetapi di sisi lain ia meningkatan *bit rate* secara keseluruhan.

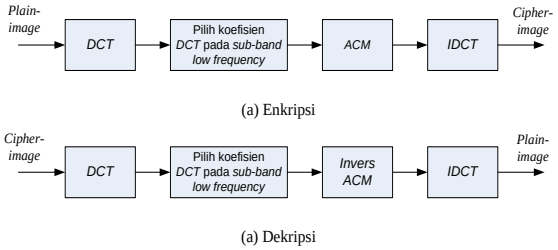
Krikor dkk [5] mempresentasikan metode enkripsi selektif dengan memilih koefisien *DCT* pada *sub-band low frequency* dan mengenkripsinya dengan *stream cipher*.

B. Usulan Algoritma Enkripsi Selektif

Algoritma enkripsi selektif yang diusulkan ini didasarkan pada fakta bahwa *HVS* (*Human Visual System*) sangat sensitif pada frekuensi yang lebih rendah daripada frekuensi yang lebih tinggi. Informasi visual yang penting seperti kerangka obyek, bentuk obyek, dll, terdapat pada *sub-band low frequency*, sedangkan informasi detil gambar terdapat pada *sub-band high frequency*. Dengan mengenkripsi hanya koefisien-koefisien *DCT* pada *sub-band low frequency*, maka informasi visual di dalam citra menjadi "rusak" sehingga citra tidak dapat dikenali lagi (setelah dilakukan *IDCT*), yang berarti citra telah terenkripsi.

Secara garis besar algoritma enkripsi selektif yang diusulkan adalah sebagai berikut:

1. Tranformasikan citra ke ranah frekuensi dengan transformasi *DCT* (persamaan 1)
2. Pindai matriks koefisien *DCT* dengan algoritma zigzag, lalu ekstraksi koefisien-koefisien *AC* pada *sub-band low frequency* sebanyak N^2 elemen. Koefisien *DC* tidak dipilih karena ia menentukan informasi visual yang penting di dalam sebuah citra.



(a) Enkripsi

(a) Dekripsi

Gambar 5. Diagram enkripsi dan dekripsi selektif.

3. Nyatakan koefisien-koefisien *DCT* yang terpilih ke dalam matriks yang berukuran $N \times N$.
4. Terapkan *ACM* (persamaan 3) dengan nilai *b* dan *c* rahasia pada matriks dari langkah 3 di atas sebanyak *m* kali.
5. Tempatkan hasil transformasi *ACM* pada matriks *DCT* semula.
6. Terapkan *IDCT* (persamaan 2) pada matriks hasil langkah 5 di atas untuk mendapatkan *cipher-image*.

Algoritma di atas adalah untuk citra *grayscale*. Untuk citra berwarna prosesnya dilakukan secara terpisah masing-masing untuk setiap komponen *Red* (*R*), *Green* (*G*), dan *Blue* (*B*). Algoritma dekripsi sama dengan algoritma enkripsi kecuali untuk *invers* transformasi *ACM* digunakan persamaan (4). Gambar 5 memperlihatkan diagram proses enkripsi dan dekripsi citra.

Parameter nilai yang menjadi kunci yang harus dirahasiakan adalah *b*, *c*, *m*, dan *N*. Proses dekripsi memerlukan parameter kunci yang sama untuk mendapatkan kembali *plain-image*. Karena *DCT* adalah *lossy transformation*, maka citra hasil dekripsi tidak persis sama dengan citra semula

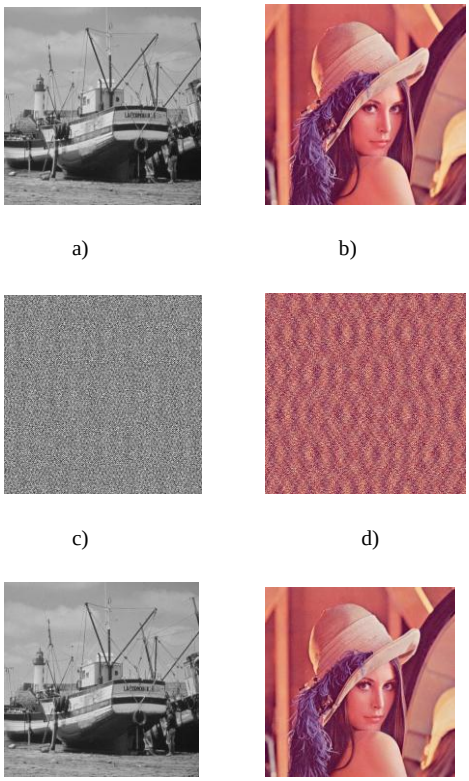
IV. HASIL DAN PEMBAHASAN

Untuk mengetahui kinerja algoritma enkripsi selektif yang diusulkan di atas, maka sejumlah eksperimen dilakukan dengan menggunakan kakas *Matlab*. Citra uji yang digunakan dipilih dari *grayscale* dan citra berwarna. Dua buah citra uji yang dipakai adalah 'boat' (512 × 512) dan citra 'Lena' (512 × 512), seperti ditunjukkan pada Gambar 6(a) dan 6(b). Keduanya merupakan citra standard dalam pengolahan citra. Parameter kunci yang dipakai di dalam eksperimen adalah: $b = 62$, $c = 78$, $m = 5$, $N = 350$. Dua nilai pertama adalah parameter *ACM*, *m* adalah jumlah iterasi *ACM*, dan *N* adalah ukuran matriks $N \times N$ yang dipilih dari N^2 koefisien *DCT* pada *sub-band low frequency*.

Sebagai catatan, perhitungan waktu enkripsi/dekripsi dalam satuan waktu tidak diukur secara spesifik karena metode enkripsi ini tidak bertujuan membandingkannya dengan algoritma enkripsi konvensional. Waktu proses berkaitan dengan banyak faktor seperti optimasi kode program, spesifikasi perangkat keras yang digunakan, manajemen proses di dalam sistem operasi, dan sebagainya. Adapun kinerja algoritma yang diukur dititikberatkan pada segi keamanan dan *fidelity* citra.

A. *Hasil Enkripsi dan Dekripsi*

Algoritma ini berhasil mengenkripsi dan mendekripsi citra dengan baik. Citra hasil enkripsi (*cipher-image*) masing-masing diperlihatkan pada Gambar 6(c) dan 6(d). Citra hasil enkripsi terlihat sudah tidak dapat dikenali lagi karena secara visual terlihat relatif sama seperti citra acak (*random images*).



a) b)

c) d)

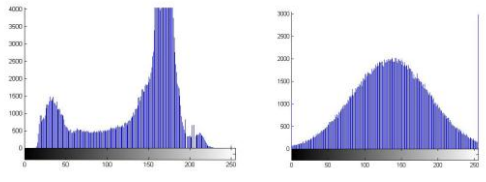
(e) *PSNR* = 38.9444 (f) *PSNR* = 31.0903

Gambar 6. (a) 'boat' (plain-image); (b) Lena (plain-image); (c) cipher-image dari 'boat'; (d) cipher-image dari 'Lena'; (e) citra hasil dekripsi 'boat'; (f) cira hasil dekripsi 'Lena'.

Karena *DCT* adalah transformasi yang *lossy*, maka dekripsi terhadap *cipher-image* menghasilkan citra yang tidak tepat sama dengan citra semula. Hal ini ditunjukkan dengan penurunan kualitas citra hasil dekripsi yang diukur dengan *PSNR*. Citra 'boat' hasil dekripsi memiliki *PSNR* = 38.9444, dan citra 'Lena' hasil dekripsi memiliki *PSNR* = 31.0903.

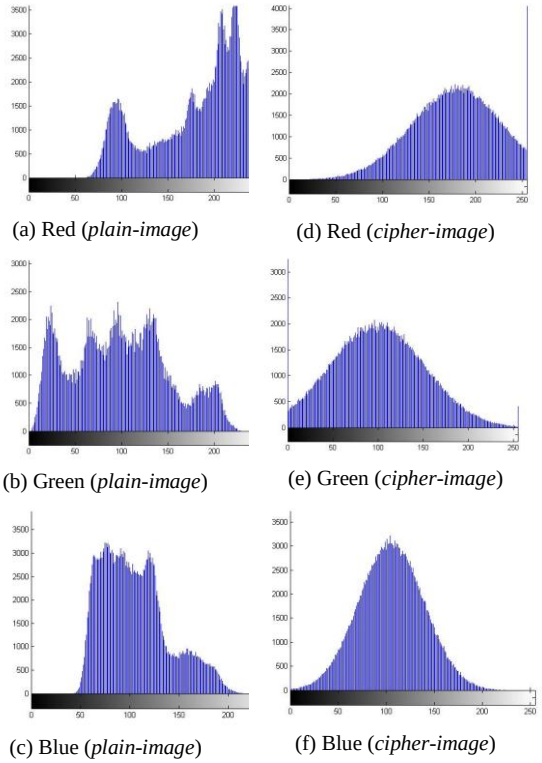
B. *Analisis Histogram*

Histogram memperlihatkan distribusi intensitas *pixel-pixel* di dalam citra tersebut. Penyerang menggunakan histogram untuk menganalisis frekuensi kemunculan intensitas *pixel* untuk mendeduksi kunci atau *pixel-pixel* di dalam *plain-image*. Agar serangan dengan analisis statistik tidak dimungkinkan, maka penting menghasilkan histogram *cipher-image* yang tidak memiliki kemiripan secara statistik dengan histogram *plain-image*. Gambar 7(a) memperlihatkan histogram citra 'boat' dan Gambar 7(b)



a) b)

Gambar 7. (a) Histogram citra 'boat' (*plain-image*) dan (b) histogram *cipher-image* dari 'boat'



(a) Red (*plain-image*) (d) Red (*cipher-image*)

(b) Green (*plain-image*) (e) Green (*cipher-image*)

(c) Blue (*plain-image*) (f) Blue (*cipher-image*)

Gambar 8. (a)-(c) Histogram citra 'Lena' (*plain-image*) untuk masing-masing kanal RGB; dan (d)-(f) histogram *cipher-image* untuk setiap kanal

adalah histogram *cipher-image*-nya. Histogram *cipher-image* berbentuk lonceng dan terlihat seperti memiliki distribusi Gaussian.

Untuk citra berwarna histogramnya dibuat masing-masing untuk komponen warna (*red*, *green*, dan *blue*). Gambar 8(a) sampai 8(c) adalah histogram citra 'Lena' (*plain-image*) untuk setiap kanal warna *RGB*, sedangkan Gambar 8(d) sampai 8(f) adalah histogram masing-masang kanal warna pada *cipher-image*-nya Sama seperti citra 'boat', histogram setiap kanal *RGB* pada *cipher-image* berbentuk lonceng.

Histogram *cipher-image* yang berbeda signifikan dengan histogram *plain-image* menyulitkan pihak lawan melakukan serangan dengan menggunakan analisis frekuensi kemunculan nilai-nilai *pixel*, sebab secara statistik keduanya tidak memiliki hubungan. Dengan kata lain permutasi citra pada ranah frekuensi menghasilkan efek *confusing* bagi pihak lawan.

C. Analisis Korelasi

Di dalam ilmu statistik korelasi merupakan sebuah besaran yang menyatakan kekuatan hubungan linier antara dua peubah acak. Korelasi dari dua buah peubah acak diskrit yang masing-masing beranggotakan n elemen dihitung dengan rumus koefisien korelasi sebagai berikut [10]:

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}} \qquad (5)$$

TABEL 1
PERBANDINGAN KOEFISIEN KORELASI ANTARA DUA *PIXEL* BERTETANGGA

Koefisien korelasi	Horizontal	Vertikal	Diagonal
Plain-image	0.9545	0.9773	0.9465
Cipher-image	0.5032	0.0585	-0.2395

yang dalam hal ini

$$\text{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \quad \text{(kovariansi)} \qquad (6)$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \quad \text{(standard deviasi)} \qquad (7)$$

$$E(x) = \frac{1}{n}\sum^{n} x_i \quad \text{(rata-rata)} \qquad (8)$$

Arti koefisien korelasi adalah sebagai berikut. Nilai koefisien korelasi maksimal 1 dalam harga mutlak. Nilai koefisien korelasi +1 menyatakan hubungan linier (korelasi) sempurna yang menaik, nilai koefisien korelasi -1 menyatakan hubungan linier (korelasi) sempurna yang menurun, sedangkan antara -1 dan +1 menyatakan derajat ketergantungan linier antara dua peubah. Nilai koefisien yang dekat dengan -1 atau +1 menyatakan hubungan linier yang kuat antara x dan y, sedangkan nilai koefisien yang dekat dengan 0 menyatakan hubungan linier yang lemah [7].

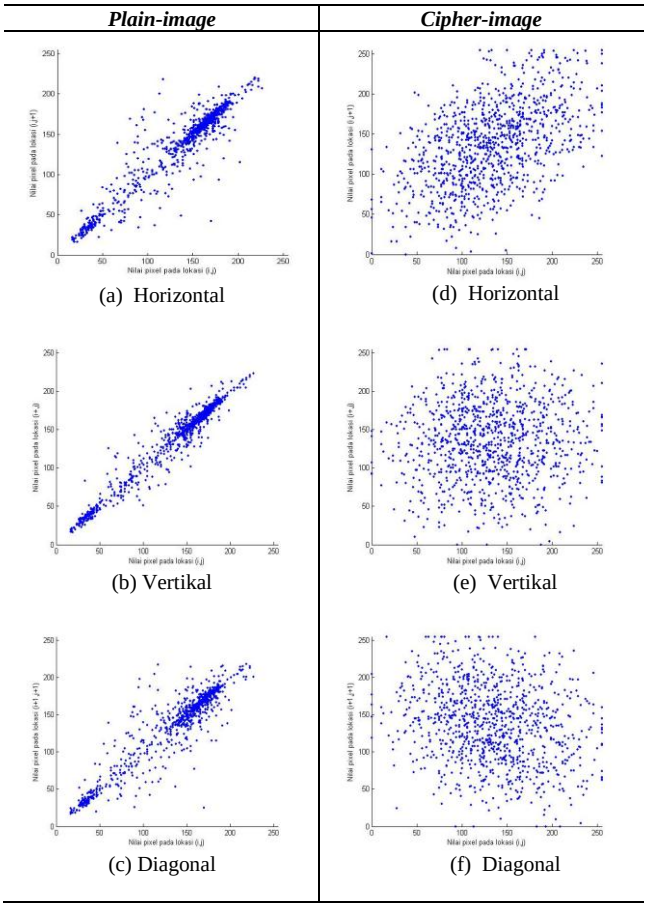
Di dalam *natural image*, *pixel-pixel* yang bertetangga memiliki hubungan linier yang kuat. Ini ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1). Enkripsi citra bertujuan membuat korelasi antara *pixel-pixel* bertetangga menjadi lemah atau koefisien korelasinya sedapat mungkin mendekati nol.

Untuk mengetahui korelasi *pixel-pixel* di dalam *plain-image* maupun *cipher-image*, maka di dalam eksperimen ini dihitung koefisien korelasi antara dua *pixel* bertetangga secara horizontal [$f(i,j)$ dan $f(i, j+1)$], dua *pixel* bertetangga secara vertkal [$f(i,j)$ dan $f(i+1, j)$], dan dua *pixel* bertetangga secara diagonal $f(i,j)$ dan $f(i+1, j+1)$]. Secara acak dipilih 1000 pasang *pixel* bertetangga pada setiap arah (vertikal, horizontal, dan diagonal), masing-masing pada citra 'boat' maupun pada *cipher-image*-nya. Koefisien korelasi dihitung dengan persamaan (5), yang dalam hal ini x dan y adalah nilai keabuan dari dua *pixel* bertetangga. Hasil perhitungan korelasi diperlihatkan pada Tabel 1.

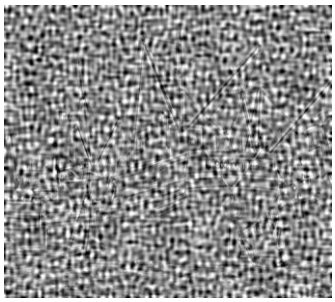
Dari Tabel 1 dapat dilihat bahwa koefisien korelasi pada *pixel-pixel* bertetangga pada setiap arah di dalam *plain-image* nilainya berada di sekitar angka 1, yang mengindikasikan korelasi yang kuat diantara *pixel-pixel* tersebut. Pada *cipher-image* korelasi antar *pixel* bertetangga melemah. Kecuali pada arah horizontal, koefisien korelasi pada arah vertikal dan diagonal mendekati nol, yang mengindikasikan *pixel-pixel* yang bertetangga tidak lagi

berkorelasi dalam arah tersebut. Pada arah horizontal koefisien korelasinya tinggal setengah dari semula.

Agar korelasi antara *pixel-pixel* bertetangga menjadi lebih jelas, maka Gambar 9 memperlihatkan distribusi korelasi *pixel-pixel* bertetangga pada *plain-image* (kolom kiri) dan *cipher-image* (kolom kanan). Pada *plain-image*, *pixel-pixel* yang bertetangga nilai-nilainya berada di sekitar garis diagonal 45°, yang mengindikasikan korelasi yang kuat antara *pixel-pixel* tersebut. Sebaliknya, pada *cipher-image* nilai-nilai *pixel* tersebar merata di seluruh area bidang datar, yang mengindikasikan *pixel-pixe*l di dalamnya tidak lagi berkorelasi atau korelasinya berkurang.



Gambar 9. Distribusi korelasi *pixel-pixel* bertetangga pada *plain-image* dan *cipher-image*



Gambar 10. Rangka obyek di dalam citra masih terlihat karena pemilihan *N* yang kecil.

TABEL 2
PERBANDINGAN PSNR DAN KOEFISIEN KORELASI TERHADAP *N*

N	PSNR citra hasil dekripsi	
	Boat	***Lena***
100	39.0371	31.1732
150	38.7491	31.0239
200	38.6734	31.1400
250	38.9843	30.9922
275	39.0154	31.0974
300	39.0894	30.9387
325	38.9910	30.8321
350	38.9444	31.0903
400	39.1553	31.0656
450	38.9717	31.1298
500	38.8441	31.0375

D. Analisis Ukuran Matriks Permutasi

Kualitas citra hasil dekripsi bergantung pada pemilihan ukuran matriks permutasi (N × N). Sebagaimana yang sudah dijelaskan di atas, permutasi dilakukan pada koefisien-koefisien DCT yang dipilih pada sub-band low frequency. Pemilihan N bergantung pada pengetahuan batas-batas sub-band low frequency. Di dalam eksperimen ini diasumsikan ukuran sub-band low frequency maksimal sepertiga ukuran matriks DCT. Semakin kecil N memang meminimalkan proses komputasi, tetapi cipher-image masih memperlihatkan bentuk obyek (Gambar 9). Jika N dibuat besar, enkripsi menghasilkan cipher-image yang teracak dengan baik dan kualitas citra hasil dekripsi cenderung menaik (diukur dengan PSNR), namun proses komputasi menjadi lebih lama. Dengan kata lain ada timbal balik antara pemilihan N dan kualitas citra hasil dekripsi.

Di dalam eksperimen ini dilakukan pengujian enkripsi dan dekripsi menggunakan nilai *N* yang beragam terhadap citra ‘boat’ dan ‘Lena’. Kualitas citra hasil dekripsi pada citra ‘boat’ dan ‘Lena’ berfluktuatif dengan peningkatan ukuran *N* (Tabel 2). Pemilihan N yang tepat dapat meningkatkan kualitas hasil dekripsi.

E. Ruang Kunci

Serangan *brute-force attack* mencoba menemukan semua kemungkinan kunci untuk mendekripsi *cipher-image*. Agar *brute-force attack* menjadi tidak efisien dilakukan, maka jumlah kemungkinan kunci harus dibuat besar. Ruang kunci menyatakan jumlah total kunci yang berbeda yang dapat digunakan unruk enkripsi/dekripsi.

Parameter kunci rahasia yang digunakan di dalam algoritma enkripsi selektif ini adalah *b*, *c*, *m*, dan *N*. Semua nilai parameter tersebut adalah *integer* positif. *Matlab* mendukung maksimum *unsigned integer* sampai 32 bit, sehingga nilai pilihan *integer* yang mungkin adalah sekitar $2^{32} = 4.3 \times 10^9$. Dengan demikian, ruang kunci seluruhnya adalah

$$H(b, c, m, Nr) \approx (4.3 \times 10^9)^4$$
$$\approx 3.418801 \times 10^{38}$$

Ruang kunci ini terhitung cukup besar agar bertahan terhadap serangan *brute-force attack.*

V. KESIMPULAN

Sebuah algoritma enkripsi selektif citra digital berbasiskan permutasi *chaos* telah dipresentasikan.

Enkripsi dilakukan dalam ranah frekuensi dengan mengacak *sub-band low frequency* pada matriks *DCT* menggunakan *Arnold Cat Map*.

Algoritma ini dapat mengenkripsi citra *grayscale* dan citra berwarna. Histogram *cipher-image* berbeda signifikan dengan histogram plain-image sehingga menyulitkan serangan analisis statistik. Analisis korelasi menunjukkan bahwa *pixel-pixel* di dalam *cipher-image* mempunyai korelasi yang melemah atau mendekati nol sehingga *pixel-pixel* bertetangga tidak berhubungan lagi satu sama lain. Ruang kunci yang cukup besar membuat algoritma ini aman dari serangan *brute force attack*.

Kelemahan algoritma enkripsi ini adalah *lossy encryption*, yakni citra hasil dekripsi tidak tepat sama dengan citra semula. Ada sebagian informasi citra yang hilang karena enkripsi dan dekripsi dilakukan dalam ranah *DCT*. Selain itu, kualitas citra hasil dekripsi juga ditentukan oleh pemilihan ukuran matriks koefisien *DCT* yang diacak dengan *Arnold Cat Map*. Meskipun termasuk *lossy encryption*, tetapi bila kualitas citra hasil dekripsi bukan masalah yang penting, maka algoritma ini tepat digunakan untuk aplikasi yang memerlukan *delay* yang rendah.

VI. UCAPAN TERIMA KASIH

Penelitian yang dipublikasikan di dalam makalah ini sepenuhnya didukung oleh dana **Riset dan Inovasi KK 2012** (Program Riset ITB 2012).

DARTAR PUSTAKA

[1] Nidhi S Kulkarni, Balasubrmanian Raman, and Indra Gupta, "Selevtive Encryption of Multimedia Images", in *Proceeding off XXXII National Systems Conference, NSC 2008*, December 17-19, 2008.

[2] Jolly Shah and Vikas Saxena, "Performance Study on Image Encryption Schemes", in *International Journal of Computer Science Issues*, Vol 8, Issue 4, No 1, July 2011.

[3] Xiliang Liu, "Selective Encryption of Multimedia Contentn in Distribution Networks: Challenges and New Directions", in *Proceeding of Conference of Communications, Internet, and Information Technology*, 2003.

[4] Jonathan M. Blackledge, Musheer Ahmad, and Omar Faruq, "Chaotic Image Encryption on Frequency Domain Scrambling", in *Information Processing Letters*, 2010.

[5] Lala Krikor, Sama Baba, Thawar Arif, and Zyad Shaaban, "Image Encryption Using DCT and Stream Cipher", in *European Journal of Scientific Research*, Vol. 32, No. 1 (2009), pp 47-57

[6] K. Struss, *A Chaotic Image Encryption*, Mathematics Senior Seminar, 4901, University of Minnesota, Morris, 2009.

[7] Rinaldi Munir, "Algoritma Enkripsi Citra dengan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif Terhadap Bit-bit MSB", dalam *Prosiding Seminar Nasional dan Aplikasi Teknologi Informasi (SNATI), Universitas Islam Indonesia Yogyakarta, 2012*.

[8] M. Van Droogenbroek and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images", in Proceedings of Advanced Consepts for Intelligent Vision Systems (ACIVS) 2002, Belgium, Sept. 2002.

[9] L. Tang, "Method for Encrypting and Decrypting MPEG Video Data Efficiency", in *Proceeding of ACM Multimedia*, Vol. 3, pp 219-229, 2006.

[10] T. Hongmei, H. Liying, H. Yu, and W. Xia, "An Improved Compound Image Encryption Scheme", *Proceeding of 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*, 2010