Pengembangan Algoritma Enkripsi Selektif Citra Digital dalam Ranah Spasial dengan Mode *CBC-like* Berbasiskan *Chaos*

Rinaldi Munir[1)]

1) Sekolah Teknik Elektro dan Informatika ITB, Bandung 40132, email: rinaldi-m@stei.itb.ac.id

Abstrak **–** *Sebuah citra umumnya bervolume data yang besar, oleh karena itu teknik enkripsi secara selektif bertujuan mengurangi volume komputasi selama proses enkripsi/dekripsi. Makalah ini membahas metode enkripsi selektif yang hanya mengenkripsi 4-bit most significant bit (MSB) pada setiap pixel dan mengoperasikannya dalam mode CBC-like. Bit-bit kunci dibangkitkan dari fungsi chaos untuk memperoleh efek confusion dan diffusion. Hasil eksperimen pada citra grayscale dan citra berwarna memperlihatkan algoritma ini mempunyai kualitas yang bagus: (1) Histogram cipher-image secara visual terlihat datar, (2) algoritma sensitif terhadap perubahan kecil pada kunci. Kedua faktor ini menyulitkan penyerang memecahkan cipher-image.*

Kata Kunci*: citra, enkripsi selektif, n-bit MSB, CBC-like, chaos.*

1. PENDAHULUAN

Enkripsi citra bertujuan melindungi konten di dalam citra dari pengaksesan ilegal. Obyektif dari enkripsi citra adalah mentransformasikan citra ke dalam bentuk lain yang tidak bermakna sehingga konten di dalam citra tidak dapat dipahami lagi secara visual.

Mengenkripsi citra dengan algoritma enkripsi konvensional untuk data teks seperti *DES*, *AES*, *Blowfish*, dan lain-lain kurang cocok untuk aplikasi komunikasi yang *real-time*, sebab citra umumnya bervolume data sangat besar sehingga proses enkripsinya menjadi lambat. Oleh karena itu, solusi untuk masalah ini adalah dengan menggunakan konsep enkripsi selektif (atau sebagian) sebagai lawan dari enkripsi total [2]. Dengan teknik enkripsi selektif hanya sebagian komponen citra yang perlu dienkripsi namun sebagai efeknya citra dienkripsi secara keseluruhan. Tujuan enkripsi selektif jelas untuk meminimalkan volume komputasi selama proses enkripsi dan dekripsi.

Enkripsi selektif dapat dilakukan dalam ranah spasial atau dalam ranah frekuensi. Klasifikasi dan ringkasan beberapa algoritma enkripsi selektif dapat ditemukan di dalam [5], sedangkan performansi algoritmanya dapat dibaca di dalam [3].

Menurut [6], kebanyakan algoritma enkripsi citra dapat dikelompokkan menjadi dua golongan: (a) algoritma enkripsi selektif non-*chaos*, dan (b) algoritma enkripsi selektif atau non-selektif yang berbasis *chaos*. *Chaos* menjadi topik yang atraktif di dalam kriptografi karena tiga alasan: (1) sensitivitas terhadap kondisi awal, (2) berkelakuan acak, dan (3) tidak memiliki periode berulang. Penggunaan *chaos* di dalam kriptografi dapat menghasilkan efek *confusion* dan *diffusion* seperti yang disyaratkan oleh Shanon [8].

Kebanyakan skema enkripsi berbasis *chaos* menggunakan fungsi *chaos* (*chaotic map*) sebagai pembangkit barisan bilangan semi-acak (*pseudo-random*) yang panjang, kemudian barisan bilangan acak tersebut digunakan untuk mengenkripsi plainteks. *Review* beberapa algoritma enkripsi citra yang berbasis *chaos* dapat ditemukan di dalam [4].

Makalah ini membahas sebuah usulan algoritma enkripsi selektif citra digital pada ranah spasial berbasis *chaos*. Untuk memperoleh *cipher-image* yang tahan terhadap serangan analisis frekuensi, maka digunakan mode *seperti CBC* (*cipher block chaining*) sehingga dinamakan *CBC-like*. Mode *CBC* adalah salah satu modus di dalam algoritma *block cipher* sehingga blok cipherteks tidak hanya bergantung pada blok plainteksnya saja tetapi juga bergantung pada blok-blok plainteks sebelumnya. Dengan mode ini maka blok plainteks yang sama tidak menghasilkan blok cipherteks yang sama. Jika diterapkan pada citra, maka *pixel-pixel* di dalam *plain-image* dan *pixel-pixel* di dalam *cipher-image* tidak mempunyai hubungan statistik sehingga menyulitkan kriptanalis untuk mendeduksi kunci atau *plain-image*.

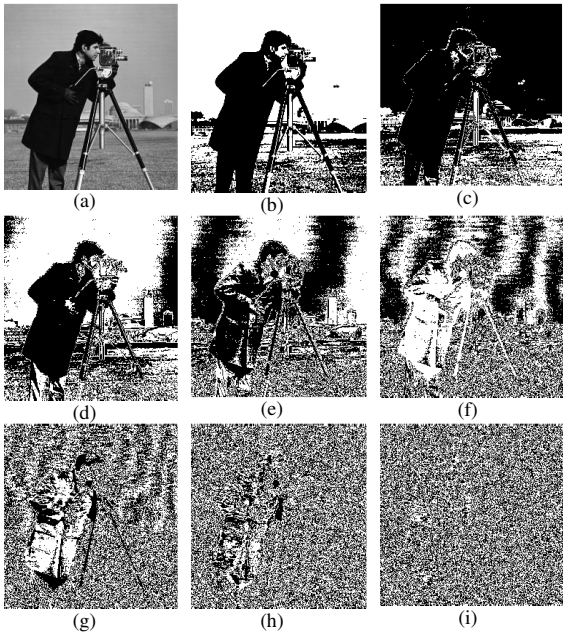
Makalah ini disusun menjadi lima bagian. Yang pertama adalah pendahuluan, bagian kedua adalah enkripsi selektif pada bit-bit *MSB*, bagian ketiga membahas usulan algoritma enkripsi selektif, bagian keempat eksperimen dan pembahasan hasil-hasil, dan bagian terakhir adalah kesimpulan.

2. ENKRIPSI SELEKTIF PADA BIT-BIT MSB

Di nilai *pixel* pada koordinat (*x*, *y*) menyatakan intensitas nilai keabuan pada posisi tersebut. Pada citra *grayscale* nilai keabuan itu dinyatakan dalam *integer* berukuran 1 *byte* sehingga rentang nilainya antara 0 sampai 255. Pada citra berwarna 24-bit setiap *pixel* tediri atas kanal *red*, *green*, dan *blue* (*RGB*) sehingga setiap *pixel* berukuran 3 *byte* (24 bit).

Di dalam setiap *byte* bit-bitnya tersusun dari kiri ke kanan dalam urutan yang kurang berarti (*least significant bits* atau *LSB*) hingga bit-bit yang berarti

(*most significant bits* atau *MSB*). Susunan bit pada setiap *byte* adalah $b_7b_6b_5b_4b_3b_2b_1b_0$. Jika setiap bit ke-*i* dari *MSB* ke *LSB* pada setiap *pixel* diekstrak dan diplot ke dalam setiap *bitplane image* maka diperoleh delapan buah citra biner. Misalnya bila dilakukan pada citra 'cameraman' (Gambar 1(a)) maka setiap *bitplane image* ditunjukkan pada Gambar 1(b) hingga 1(i). Gambar 1(b) hingga 1(f) yang diambil dari bit-bit *MSB* masih dapat memperlihatkan wujud objek di dalam citra sedangkan Gambar 1(g) hingga 1(i) yang diambil dari bit-bit *LSB* sudah terlihat seperti citra acak.



Gambar 1 *Bitplane* pada citra *cameraman*

Berdasarkan hasil ekstraksi bit-bit tersebut dapat disimpulkan bahwa pengubahan bit-bit *MSB* dapat membuat citra menjadi "rusak" atau tidak dapat dikenali lagi, sedangkan pengubahan bit-bit *LSB* tidak mempengaruhi citra secara keseluruhan. Oleh karena itu hanya bit-bit *MSB* saja yang dipilih untuk dienkripsi sebab dengan hanya mengenkripsi bit-bit tersebut maka keseluruhan citra menjadi tidak dapat dikenali lagi.

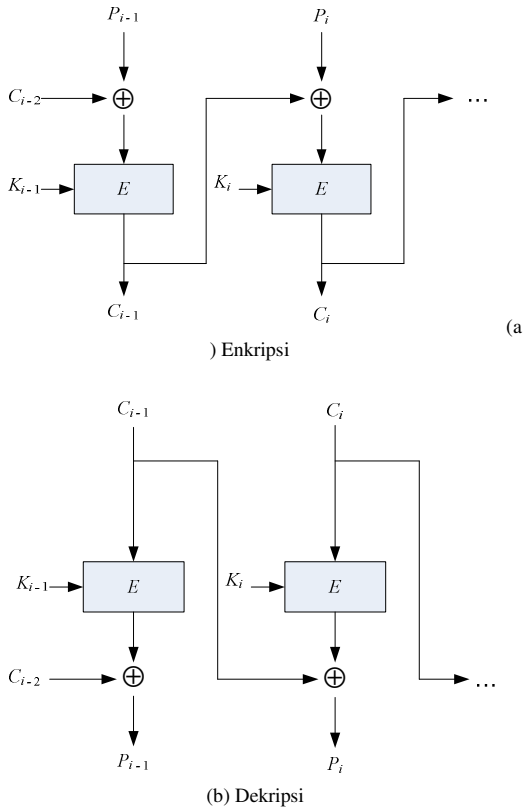
Jumlah bit *MSB* yang dienkripsi mempengaruhi tingkat keamanan. Jika hanya satu bit yang dienkripsi, maka tujuh bit sisanya (yang tidak ikut dienkripsi) masih dapat memperlihatkan wujud objek di dalam citra, sehingga tingkat keamanannya rendah. Oleh karena itu setelah enkripsi 1-bit *MSB* masih diperlukan prosedur permutasi tambahan untuk mengacak *pixel* agar diperoleh efek *confusion* [7].

Tao Xiang di dalam makalahnya menyebutkan bahkan enkripsi lebih dari dua bit *MSB* (tanpa prosedur pengacakan sesudahnya) masih tetap belum menjamin *confidentiality* citra. Untuk memperoleh keseimbangan antara tingkat keamanan dan pertimbangan performansi komputasi, maka enkripsi empat bit *MSB* (yaitu $b_7b_6b_5b_4$)merupakan pemilihan yang optimal [1]. Dengan mengenkripsi hanya 4-bit *MSB* berarti cukup hanya dienkripsi 50% saja dari keseluruhan citra untuk memperoleh citra terenkripsi namun tingkat keamanannya tetap terjamin.

2. USULAN ALGORITMA

Algoritma enkripsi selektif yang diusulkan di dalam makalah ini mengenkripsi citra dalam ranah spasial. Jumlah bit *MSB* yang dienkripsi adalah empat bit sesuai hasil penelitian di dalam [1]. Untuk memperoleh *cipher-image* yang tidak mempunyai hubungan statistik dengan *plain-image*, maka digunakan mode *CBC-like*. Setiap blok data berukuran empat bit yaitu 4-bit *MSB* dari setiap *pixel*.

Gambar 2(a) memperlihatkan skema algoritma enkripsi dengan mode *CBC-like*. Tinjau terlebih dahulu enkripsi-dekripsi pada citra *grayscale*. Misalkan citra berukuran $N \times M$, maka terdapat $n = NM$ buah *pixel*. Ekstraklah 4-bit *MSB* dari setiap *pixel* lalu nyatakan setiap blok berukuran 4-bit tersebut sebagai P_i (i = 1,2, .. n), selanjutnya operasikan blok seperti diagram *CBC* pada Gambar 2.



Gambar 2. Skema enkripsi dan dekripsi dengan *CBC*

Secara matematis, enkripsi dengan mode *CBC* dapat dinyatakan sebagai

$$C_i = E_{K_i}(P_i \oplus C_{i-1}) \quad (1)$$

dan dekripsi sebagai

$$P_i = E_{K_i}(C_i) \oplus C_{i-1} \quad (2)$$

Untuk melakukan enkripsi/dekripsi pada blok pertama diperlukan C_0 yang dalam hal ini C_0 adalah *initialization vector* atau *IV* (pada algoritma ini *IV* = '0000'). *IV* tidak perlu rahasia tetapi harus sama nilainya pada proses dekripsi.

Fungsi *E* yang digunakan di dalam Gambar 2 adalah fungsi sederhana yaitu operasi *XOR* antara bit-bit kunci K_i dengan hasil peng-XOR-an sebelumnya:

$$E_{K_i}(X_i) = X_i \oplus K_i \quad (3)$$

yang dalam hal ini $X_i = P_i \oplus C_{i-1}$ pada skema enkripsi dan $X_i = C_i$ pada skema dekripsi.

Mode yang digunakan di dalam algoritma ini disebut *CBC-like* karena untuk setiap blok menggunakan kunci yang berbeda-beda (pada mode *CBC* yang asli kunci pada setiap blok adalah sama yaitu kunci eksternal *K*).

Kunci K_i pada setiap blok data disebut *internal key* yang panjangnya juga 4-bit. Kunci internal ini dibangkitkan dari fungsi *chaos logistic map*,

$$x_{i+1} = r\, x_i\, (1 - x_i) \quad (4)$$

dengan $0 \le x_i \le 1$, $i = 0, 1, 2, \ldots$ dan $0 \le r \le 4$. Nilai awal (*seed*) iterasi adalah x_0 yang berperan sebagai kunci rahasia. Empat bit kunci internal diperoleh sebagai berikut [10]: nilai *chaos* x_i dikalikan dengan 10 berulangkali sampai ia mencapai panjang angka (*size*) yang diinginkan, selanjutnya potong hasil perkalian tersebut untuk mengambil bagian *integer*-nya saja. Secara matematis, nilai *chaos x* dikonversi ke *integer* dengan menggunakan persamaan berikut:

$$T(x, size) = \left\| x * 10^{count} \right\|, x \neq 0 \quad (5)$$

yang dalam hal ini *count* dimulai dari 1 dan bertambah 1 hingga $x * 10^{count} > 10^{size-1}$. Hasilnya kemudian diambil bagian *integer* saja (dilambangkan dengan pasangan garis ganda pada persamaan 5). Sebagai contoh, misalkan $x_i = 0.003176501$ dan *size* = 4, maka dimulai dari *count* = 1 sampai *count* = 6 diperoleh

$$0.003176501 * 10^6 = 3176.501 > 10^3$$

kemudian ambil bagian *integer*-nya dengan

$$\left\| 3176.501 \right\| = 3176$$

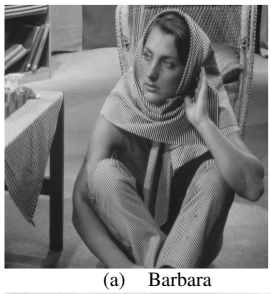
Empat bit terakhir dari representasi biner 3176 dijadikan sebagai K_i yaitu '1000'.

C_1, C_2, …, C_n dari hasil enkripsi selanjutnya menggantikan 4-bit *MSB* dari setiap *pixel* yang diproses. Hasil enkripsi terjadap seluruh *pixel* adalah citra terenkripsi (*cipher-image*). Untuk proses dekripsi dilakukan proses berkebalikan seperti yang ditunjukkan pada Gambar 2(b).

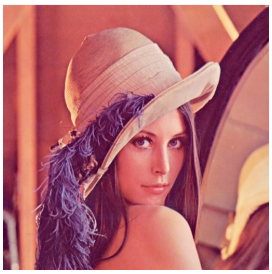
Algoritma di atas dapat dirampatkan untuk citra berwarna. Prosesnya dilakukan tiga kali, masing-masing untuk kanal *red* (*R*), *green* (*G*), dan *blue* (*B*). Jadi, pada setiap *byte* kanal warna diambil 4-bit *MSB* kemudian dioperasikan dengan mode *CBC* secara terpisah.

3. HASIL DAN PEMBAHASAN

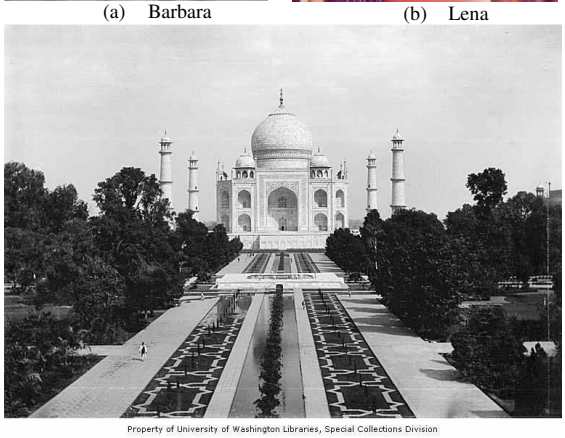
Algoritma enkripsi selektif yang diusulkan ini disimulasikan pada citra uji, baik citra *graysscale* maupun citra berwarna. Dua buah citra standard yang digunakan adalah 'Barbara' (*grayscale*) dan 'Lena' (berwarna) yang keduanya berukuran 512 × 512 (Gambar 3), dan citra ketiga adalah 'Taj Mahal' yang berukuran 768× 573. Parameter kunci yang digunakan adalah $x_0 = 0.376$ (*external key*) dan $r = 3.999$.



(a) Barbara



(b) Lena

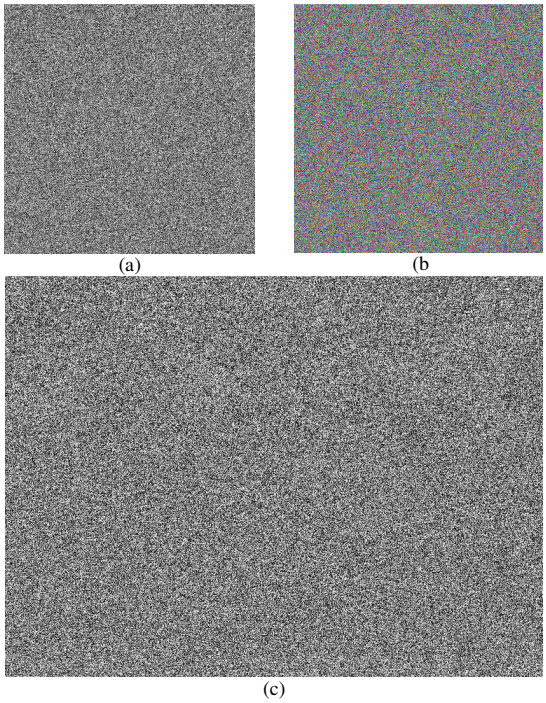


(c)

Gambar 3. Tiga buah citra uji yang digunakan di dalam simulasi enkripsi dan dekripsi.

3.1 Enkripsi

Citra hasil enkripsi (*cipher-image*) untuk ketiga citra uji di atas diperlihatkan pada Gambar 4. Citra hasil enkripsi terlihat sebagai citra acak dan sudah tidak bisa dikenali lagi.



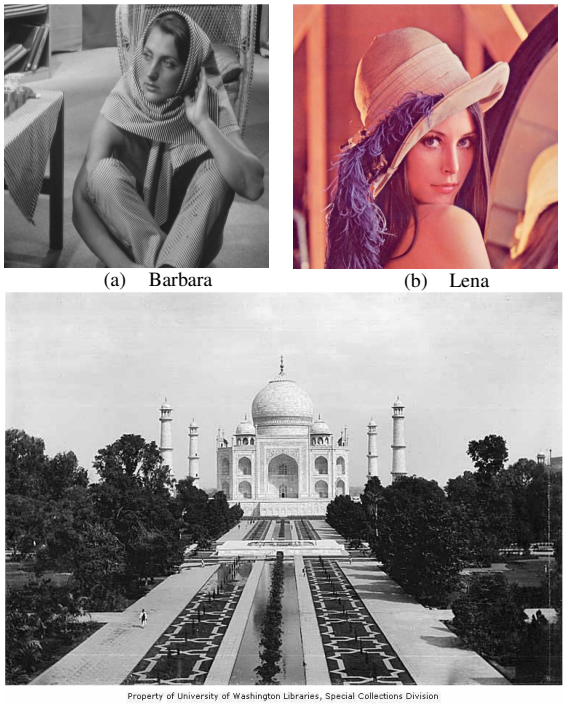
(a) (b

(c)

Gambar 4. Citra hasil enkripsi. Ketiga buah citra *plain-image* sudah tidak dapat dikenali lagi.

3.2 Dekripsi

Dekripsi terhadap *cipher-image* menghasilkan kembali tepat seperti citra semula (Gambar 5).



(a) Barbara (b) Lena

(c)

Gambar 5. *Cipher-image* didekprisi menjadi citra semula.

Selanjutnya hasil-hasil eksperimen di atas didiskusikan pada bagian di bawah ini, meliputi analisis histogram dan analisis sensitivitas.

3.3 Analisis Histogram

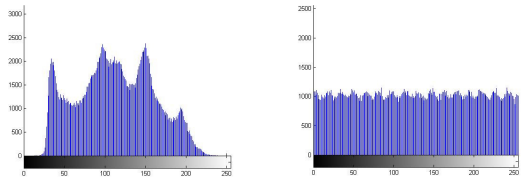
Histogram merupakan properti citra yang penting sebab sebuah histogram memperlihatkan distribusi intensitas *pixel* di dalam citra tersebut. Untuk citra *plain-image* histogramnya membentuk suatu pola yang khas, yaitu ada puncak-puncak dan lembah-lembah. Untuk mencegah penyerang menggunakan histogram untuk melakukan analisis freluensi, maka histogram *plain-image* dan histogram *cipher-image* seharusnya tidak memiliki kemiripan secara statistik. Oleh karena itu, histogram *cipher-image* seharusnya relatif datar (*flat*) sehingga tahan terhadap serangan statistik. Distribusi yang relatif *uniform* pada *cipher-image* adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki kualitas yang bagus [9].

Gambar 6(a) memperlihatkan histogram citra 'Barbara' sebelum dienkripsi, dan Gambar 6(b) adalah histogram *cipher-image*-nya. Dapat dilihat bahwa histogram *cipher-image* memiliki distribusi *uniform* yang mana berbeda dengan histogram *plain-image*.

Gambar 7(a) sampai 7(c) memperlihatkan histogram citra 'Lena' (*plain-image*) untuk setiap kanal warna *RGB* dan Gambar 7(d) sampai 7(f) adalah histogram masing-masang kanal warna pada *cipher-image*. Sama seperti citra 'Barbara', histogram *cipher-image* pada setiap kanal *RGB* juga terlihat *flat* atau terdistribusi *uniform*.

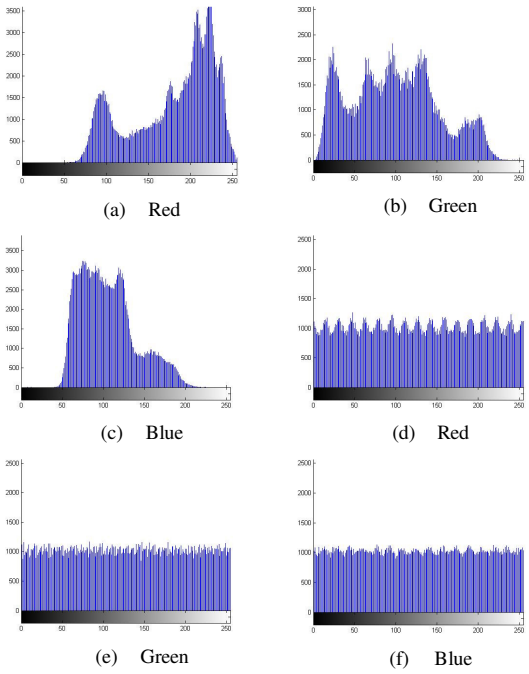
Gambar 8(a) memperlihatkan histogram citra 'Taj Mahal' (*plain-image*) dan Gambar 8(b) adalah histogram *cipher-image*-nya. Sedikit berbeda dengan histogram *cipher-image* dari dua citra sebelumnya, histogram *cipher-image* dari 'Taj Mahal' memiliki distribusi yang relatif *uniform*.

Berdasarkan hasil-hasil analisis histogram di atas dapat disimpulkan bahwa *cipher-image* memiliki histogram yang (relatif) *flat* sehingga menyulitkan penyerang melakukan analisis statistik untuk mendeduksi *pixel* atau kunci. Hasil ini menunjukkan bahwa algoritma enkripsi citra yang diusulkan ini memiliki keamanan yang bagus.



(a) (b)

Gambar 6. (a) Histogram citra 'Barbara' (*plain-image*) dan (b) histogram *cipher-image*.

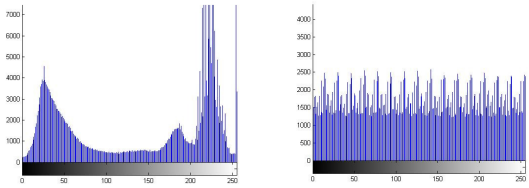


(a) Red (b) Green

(c) Blue (d) Red

(e) Green (f) Blue

Gambar 7. (a)-(c) Histogram citra 'Lena' (*plain-image*) untuk masing-masing kanal *RGB* dan (d)-(f) histogram *cipher-image* untuk setiap kanal *RGB*.



(a) (b)

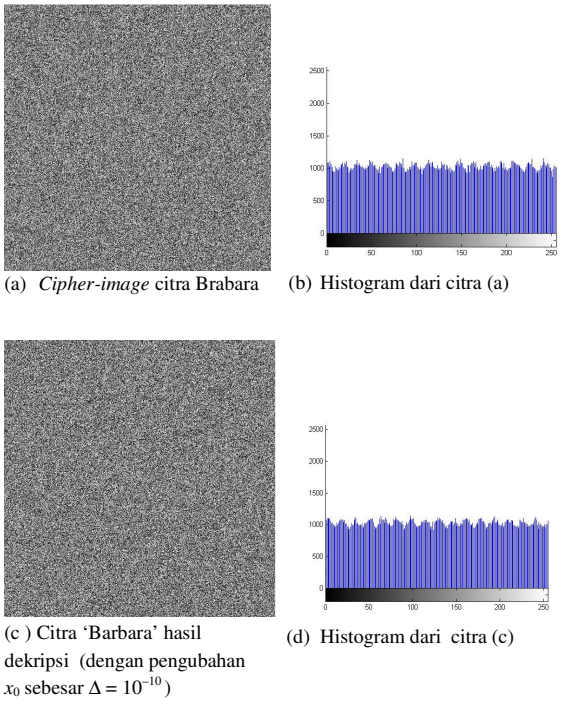
Gambar 8 (a) Histogram citra 'Taj Mahal' (*plain-image*) dan (b) histogram *cipher-image*.

3.2 Analisis Sensitivitas

Algoritma enkripsi citra seharusnya sensitif terhadap kunci. Sensitif artinya jika kunci diubah sedikit saja maka hasil dekripsi terhadap *cipher-image* menghasilkan cipher-image lain yang berbeda signifikan. Karena algoritma yang diusulkan ini menggunakan sistem *chaos*, maka sifat *chaos* yang sensitif terhadap perubahan kecil nilai awal (x_0) merupakan properti keamanan yang penting. Nilai x_0 berperan sebagai kunci yang diberikan oleh pengguna.

Pada eksperimen ini nilai awal *logistic map* diubah sebesar Δ sehingga menjadi $x_0 + \Delta$, kemudian citra didekripsi dengan kunci $x_0 + \Delta$. Dalam eksperimen ini diambil $\Delta = 10^{-10}$ sehingga nilai awal *logistic map* menjadi 0.376000001. Gambar 9 memperlihatkan hasil dekripsi terhadap *cipher-image* dari citra 'Barbara'. Hasilnya adalah *cipher–image* lain yang ternyata tetap teracak (tidak kembali menjadi citra semula). Perubahan kecil nilai awal *chaos* membuat nilai chaotik yang dihasilkan berbeda signifikan. Karena nilai-nilai ini dipakai sebagai kunci maka hasilnya adalah hasil dekripsi yang tidak benar dan *cipher-image* tetap teracak.

Hasil eksperimen ini menunjukkan bahwa karakteristik *chaos* yang sensitif terhadap nilai awal memberikan keamanan yang bagus dari serangan *exhaustive attack*. Eksperimen ini juga menyiratkan bahwa perubahan sangat kecil pada kunci menyebabkan hasil dekripsi tetap salah.



(a) *Cipher-image* citra Brabara (b) Histogram dari citra (a)

(c) Citra 'Barbara' hasil dekripsi (dengan pengubahan x_0 sebesar $\Delta = 10^{-10}$) (d) Histogram dari citra (c)

Gambar 9. Hasil ekperimen dekripsi dengan pengubahan x_0 sebesar $\Delta = 10^{-10}$.

4. KESIMPULAN

Di dalam makalah telah disajikan sebuah usulan algoritma enkripsi selektif citra pada ranah spasial. Untuk menyeimbangkan antara tingkat keamanan dengan performansi komputasi, maka dari setiap *pixel* hanya dienkripsi 4-bit *MSB* saja. Jadi, hanya 50% saja dari keseluruhan citra yang diproses untuk memperoleh citra terenkripsi secara keseluruhan. Untuk memperoleh *cipher-image* yang tidak mempunyai kemiripan secara statistik dengan *plain-*

image, maka 4-bit *MSB* tersebut dioperasikan dengan mode *CBC-like*.

Hasil eksperimen memperlihatkan algoritma ini dapat mengenkripsi sembarang citra (baik citra grayscale maupun citra berwarna) dengan baik. *Cipher-image* yang dihasilkan dari proses enkripsi sudah tidak dapat dikenali lagi meskipun yang dienkripsi hanya 4-bit *MSB* saja.

Pixel-pixel di dalam *cipher-image* mempunyai distribusi relatif *uniform*, hal ini diperlihatkan dengan bentuk histogramnya yang relatif datar. Histogram *cipher-image* yang datar tidak memungkinkan penyerang melakukan serangan dengan menggunakan analisis statistik.

Eksperimen dengan mengubah sedikit nilai awal *chaos* memperlihatkan bahwa algoritma ini sensitif terhadap perubahan kecil pada kunci sehingga aman dari serangan *exhaustive attack*.

5. *ACKNOWLEDGMENT*

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

DAFTAR REFERENSI

[1] Tao Xiang, Kwok-wo Wong, Xiaofeng Liao, *Selective Image Encryption Using a Spatiotemporal Chaotic System*, Chaos Volume 17, 2007.

[2] Nidhi S Kulkarni, Balasubrmanian Raman, Indra Gupta, *Selevtive Encryption of Multimedia Image*s, Proc. Of XXXII National Systems Conference, NSC 2008, December 17-19, 2008.

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

[4] Monisha Sharma, Manoj Kumar Kowar, *Image Encryption Techniques Using Chaotic Schemes: A Review*, International Journal of Engineering Science and Technology, Vol. 2(6), 2010

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

[6] Mohammad Ali Bani Younes, Aman Jantan, *Image Encryption Using Block-based Transformation Algorithm*, IAENG International Journal of Computer Science, 35: 1, IJCS_32_1_03, 2008.

[7] Rinaldi Munir, *Enkripsi Selektif Citra Digital dengan Stream Cipher Berbasiskan pada Fungsi* Chaotik Logistic Map, Seminar Nasional dan Expo Teknik Elektro Univeristas Syiah Kuala, Banda Aceh, Oktober 2011.

[8] Bruce Schneier, *Applied Cryptography 2nd Edition*, Wiley & Sons, 1996.

[9] Alireza Jolfaei, Abdul Rasoul Mirghadri, *An Image Encryption Approach Using Chaos and Stream Cipher*, Journal of Theoretical and Applied Information Technology, 2010.

[10] James Lampton, *Chaos Cryptography: Protecting data Using Chaos,* Missisippi School for Mathematics and Science.

.