Makalah Nomor: KNSI-347

ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS *CHAOS* DALAM GABUNGAN RANAH FREKUENSI DAN RANAH SPASIAL

Rinaldi Munir

Program Studi Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
rinaldi-m@stei.itb.ac.id

Abstrak

Makalah ini menyajikan sebuah usulan algoritma enkripsi citra digital yang beroperasi dalam dua ranah, yaitu ranah frekuensi dan ranah spasial. Enkripsi dalam ranah frekuensi dilakukan dengan teknik permutasi dan enkripsi dalam ranah spasial dilakukan dengan teknik substitusi. Permutasi dalam ranah frekuensi bertujuan untuk menyamarkan karakteristik statistik yang biasanya tidak berubah jika permutasi dilakukan dalam ranah spasial. Subsitusi dalam ranah spasial dilakukan dengan operasi XOR antara nilai *pixel* semula dan *keystream*. Dua buah *chaos map* digunakan dalam proses enkripsi/dekripsi, yaitu *Arnold Cat Map* untuk permutasi dan *Logistic Map* untuk substitusi. Hasil eksperimen memperlihatkan algoritma tersebut dapat mengenkripsi sembarang citra *grayscale* dan citra berwarna dengan baik dan mendekripsinya menjadi citra semula. Citra hasil enkripsi terlihat seperti citra acak dan memiliki histogram yang datar sehingga menyulitkan kriptanalis mendeduksi *pixel-pixel* citra semula dengan melakukan analisis statistik.

Kata kunci : enkripsi, citra, ranah frekuensi, ranah spasial, *chaos*, *Arnold Cat map*, *Logistic Map*

15. Pendahuluan

Citra adalah salah satu representasi informasi yang penting karena citra dapat menampilkan informasi secara visual. Penyimpanan citra di dalam media *storage* dan pengiriman citra melalui saluran publik (misalnya internet) rawan terhadap pengaksesan oleh pihak-pihak yang tidak memiliki otoritas. Solusi untuk masalah ini adalah dengan mengenkripsi citra. Mengenkripsi citra artinya menyandikan cira ke dalam bentuk visual yang tidak bermakna.

Algoritma enkripsi konvensional yang sudah ada, misalnya *DES*, *AES*, *RC4*, *RSA*, *Blowfish*, dan sebagainya tidak cocok digunakan untuk mengenkripsi citra digital, karena citra digital memiliki karakteristik yang unik yang membedakannya dengan data tekstual. Citra umumnya memiliki kapasitas data yang besar sehingga algoritma enkripsi konvensional membutuhkan volume komputasi yang besar. Selain itu, sebuah *pixel* di dalam citra digital berkorelasi dengan delapan *pixel* tetangganya, sedangkan pada data tekstual sebuah karakter hanya berkorelasi dengan karakter sebelum dan sesudahnya. Karena karakteristik yang unik itu, maka algoritma enkripsi untk citra perlu didesain secara khusus.

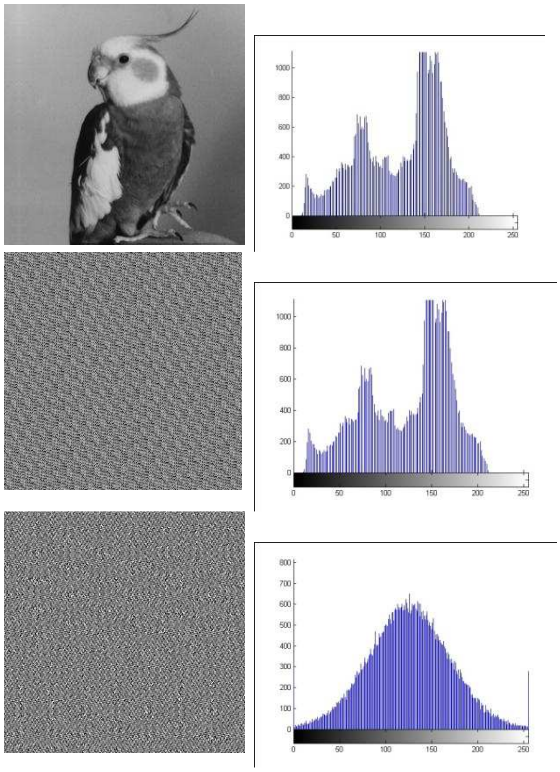
Penelitian mengenai algoritma enkripsi citra menjadi topik riset yang menarik. Secara umum algoritma enkripsi yang sudah dikembangkan peneliti dapat dibagi ke dalam dua kelompok besar: (1) algoritma enkripsi selektif non-*chaos*; (2) algoritma enkripsi selektif dan non selektif yang berbasis *chaos* [1]. Algoritma selektif artinya hanya mengenkripsi sebagian elemen citra namun efeknya keseluruhan citra terenkripsi. Adapun *chaos* menjadi topik penelitian yang intensif karena aplikatif untuk persoalan keamanan data/informasi.

Enkripsi citra dapat dilakukan dalam ranah spasial, ranah frekuensi, atau gabungan keduanya. Dua teknik dasar di dalam enkripsi citra adalah permutasi dan substitusi. Permutasi bertujuan mengacak posisi *pixel-pixel* tetapi tidak mengubah nilainya, sedangkan substitusi mengganti nilai *pixel* dengan nilai yang baru, biasanya merupakan hasil operasi XOR antara nilai *pixel* dengan kunci rahasia.

Karena permutasi dalam ranah spasial tidak mengubah nilai *pixel*, maka histogram *plain-image* dan *cipher-image* tetap sama. Kriptanalis dapat menggunakan histogram yang sama tersebut untuk

mendeduksi *pixel-pixel* dari *plain-image* melalui analisis frekuensi. Oleh karena itu, biasanya permutasi diikuti dengan substitusi untuk membuat *cipher-image* yang teracak dan berbeda nilai *pixel-pixel*-nya dengan *plain-image* semula.

Untuk lebih meningkatkan keamanan algoritma, permutasi sebaiknya dilakukan di dalam ranah frekuensi. Hasil permutasi dalam ranah frekuensi menghasilkan citra baru yang memiliki karakteristik berbeda dengan citra semula. Hal ini ditandai oleh histogram citra hasil permutasi yang berbeda secara signifikan dengan citra plain-image. Gambar 1 memperlihatkan contoh sebuah citra yang diacak masing-masing dalam ranah spasial dan dalam ranah frekuensi [2]. Pengacakan menggunakan sebuah *chaos map* yaitu *Arnold Cat Map*. Permutasi dalam ranah spasial menghasilkan cira acak yang histogramnya tidak berubah, sedangkan permutasi dalam ranah frekuensi menghasilkan citra acak yang histogramnya berbeda dari citra semula.



Gambar 1. *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 [2].

Makalah ini mempresentasikan sebuah usulan algoritma enkripsi kombinasi ranah frekuensi dan ranah spasial. Mula-mula *pixel-pixel* citra dipermutasi dalam ranah frekuensi dengan sebuah *chaos map*, lalu hasilnya ditransformasi kembali ke dalam ranah spasial. Selanjutnya dilakukan proses substitusi nilai *pixel* dengan nilai baru yang diperoleh dari hasil operasi XOR nilai yang lama dengan *keystream* yang dibangkitkan dari *chaos map* yang lain. Permutasi dalam ranah frekuensi didasarkan pada algoritma yang dipresentasikan di dalam [2].

16. Usulan Algoritma

Misalkan I adalah citra *plain-image* yang berukuran $N \times N$ (catatan: citra harus berukuran persegi karena *chaos map* yang digunakan untuk permutasi beroperasi dalam modulo *N*. Jika ukuran citra bukan persegi, maka perlu ditambahkan baris-baris atau atau kolom-kolom *pixel dummy* agar ukurannya menjadi persegi).

2.1 Algoritma Enkripsi

Rincian algoritma enkripsi adalah sebagai berikut:

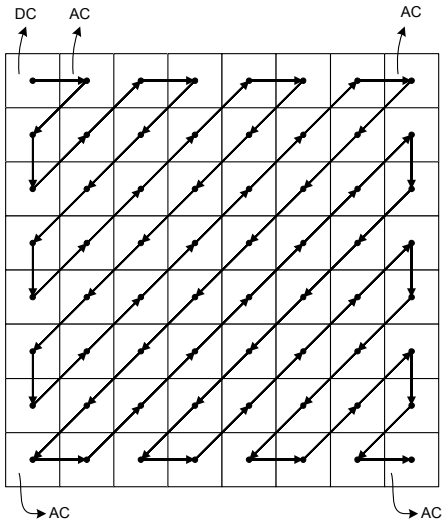
Step 1: Tranformasikan I ke ranah frekuensi dengan transformasi *DCT* berikut:

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

yang dalam hal ini

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

Step 2: Pindai koefisien-koefisien *DCT* di dalam matriks *C* dengan algoritma zig-zag sebagaimana yang diterapkan dalam proses kompresi JPEG (Gambar 2), lalu ekstraksi elemen-elemen *AC* pada *sub-band low frequency* sebanyak r^2 elemen.



Gambar 2. Pemindaian zig-zag

Mengapa hanya elemen *AC* pada *sub-band low-frequency* yang dipilih karena informasi visual yang

penting seperti kerangka obyek ditentukan oleh *sub-band low frequency*, sedangkan informasi detil gambar ditentukan oleh *sub-band high frequency*. Dengan mengenkripsi hanya elemen-elemen *AC* pada *sub-band low frequency*, maka informasi visual di dalam citra menjadi "rusak" sehingga citra menjadi tidak dapat dikenali lagi [2].

Step 3: Permutasikan $r \times r$ elemen *AC* yang terpilih dengan *Arnold Cat Map* (*ACM*) sebanyak *m* kali. Persamaan *ACM* adalah sebagai berikut:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \quad (2)$$

Parameter *ACM* yaitu *b*, *c*, dan jumlah iterasi *m* berperan sebagai kunci rahasia. Setelah permutasi, tempatkan kembali hasil transformasi *ACM* ke dalam matriks *C*.

Step 4: Terapkan *Inverse Discrete Cosine Transform* (*IDCT*) berikut pada matrik *C* untuk memperoleh citra hasil permutasi dalam ranah spasial:

$$I(x,y) = \alpha_u \alpha_v \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u,v) \cos \frac{\pi(2x+1)u}{2N} \cos \frac{\pi(2y+1)v}{2N} \quad (3)$$

Step 5: Misalkan $P = \{p_i\}$, $i = 1, 2, \ldots, N^2$, adalah *pixel-pixel* citra hasil Step 4. Enkripsikan p_i dengan *keystream* k_i dengan operasi XOR sebagai berikut:

$$c_i = p_i \oplus k_i \quad (4)$$

yang dalam hal ini $C = \{c_i\}$, $i = 1, 2, \ldots, N^2$, adalah *pixel-pixel* citra terenkripsi (*cipher-image*).

Kesytream k_i dibangkitkan dari sebuah *chaos-map* bernama *Logistic Map*. Persamaan *Logistic Map* adalah

$$x_{i+1} = \mu\, x_i\, (1 - x_i) \quad (5)$$

yang dalam hal ini $0 \le x_i \le 1$, $i = 0, 1, 2, ...$, dan μ adalah laju pertumbuhan yang nilainya di dalam selang (0, 4]. *Logistic Map* akan bersifat *chaos* bilamana $3.5699456 \le \mu \le 4$ [3]. Nilai awal (*seed*) iterasi (x_0) dan μ berperan sebagai kunci rahasia.

Mengingat nilai-nilai acak dari *Logistic Map* adalah bilangan riil, sedangkan *keystream* harus *integer*, maka harus dilakukan transformasi menjadi *integer*. Metode transformasi yang sederhana diusulkan di dalam [4] dengan persamaan sebagai berikut:

$$T(x, size) = \left\| x * 10^{count} \right\|, x \neq 0 \quad (6)$$

Peubah *count* dimulai dari 1 dan bertambah 1 hingga $x * 10^{count} > 10^{size-1}$. Pasangan garis ganda di dalam persamaan (6) menyatakan operasi pemotongan. Contohnya, bila $x_i = 0.003176501$ dan *size* = 4, maka

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

kemudian ambil bagian *integer*-nya sebagai berikut:

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

Hasil ini menjadi *keystream*. Namun, karena nilai-nilai *pixel* berada di dalam [0, 255], maka *keystream* terlebih dahulu di-modulus-kan dengan 256. Jadi, pada contoh ini $k_i = 3176 \bmod 256 = 104$.

2.2 Algoritma Dekripsi

Algoritma dekripsi merupakan kebalikan dari algoritma enkripsi. Mula-mula citra didekripsi dalam ranah spasial dengan melakukan operasi XOR antara *pixel-pixel* citra terenkripsi (*cipher-image*) dengan *keystream*, menggunakan persamaan

$$p_i = c_i \oplus k_i \quad (7)$$

Selanjutnya, hasil dekripsi ditransformasi ke ranah frekuensi dengan *DCT*, lalu lakukan de-permutasi terhadap koefisien-koefisien *AC* pada *sub-band low frequency* yang terpilih dengan *invers Arnold Cat Map* berikut:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(N) \quad (8)$$

Terakhir, terapkan *IDCT* untuk memperoleh citra *plain-image* semula. Perlu diperhatikan karena *DCT* adalah *lossy transformation*, maka citra hasil dekripsi tidak persis sama dengan citra semula.

17. Eksperimen dan Pembahasan Hasil

Algoritma enkripsi citra di atas diprogram dengan kakas *Matlab*. Dua buah citra uji citra uji standard digunakan di dalam eksperimen, masing-masing sebuah citra *grayscale* dan sebuah citra berwarna, semuanya berukuran 512 × 512 *pixel*. Citra *grayscale* 'couple' diperlihatkan pada Gambar 3, sedangkan citra berwarna 'goldhill' diperlihatkan pada Gambar 4.

Satu set kunci rahasia yang digunakan di dalam eksperimen adalah (b, c, m, x_0, μ, r) = (127, 89, 5, 0.375, 3.9998, 300). Tiga nilai pertama menyatakan parameter *Arnold Cat Map*, dua nilai berikutnya menyatakan parameter *Logistic Map*, dan parameter terakhir menyatakan ukuran matriks koefisien *AC*.

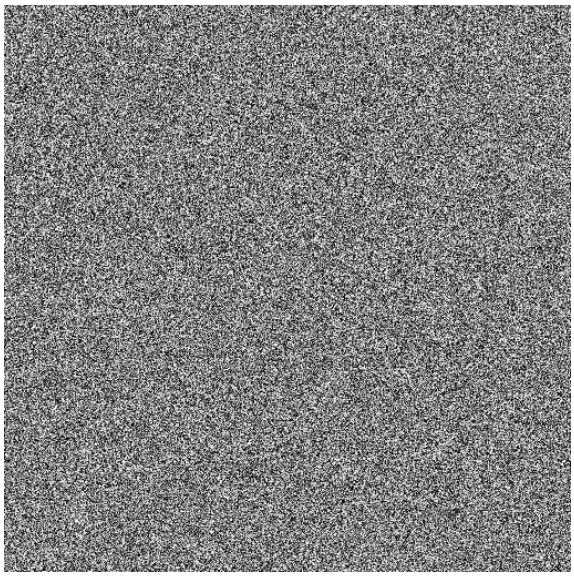
Gambar 3. Citra *grayscale* ‘couple’ (*plain-image*)

Gambar 4. Citra berwarna ‘goldhill’ (*plain-image*)

Hasil-hasil eksperimen terhadap kedua citra masukan di atas dituliskan pada bagian di bawah ini.

3.1 Hasil Enkripsi dan Dekripsi

Gambar 5 memperlihatkan citra ‘couple’ yang sudah dienkripsi (*cipher-image*). Citra hasil enkripsi menyerupai citra acak (*random image*) dan sudah tidak dapat dikenali lagi.

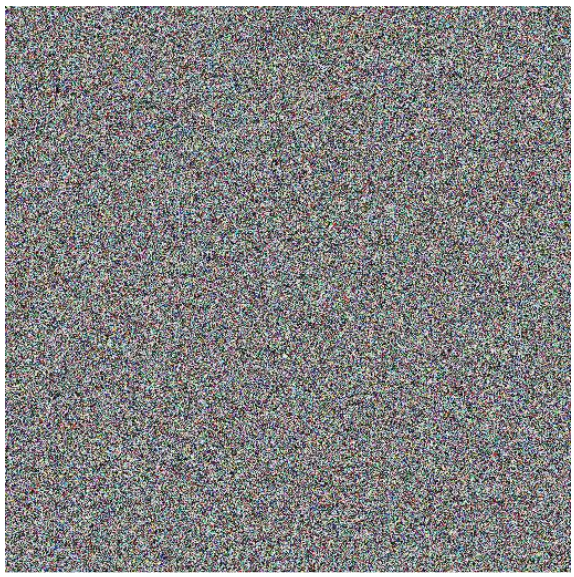


Gambar 5. Hasil enkripsi citra ‘couple’ (*cipher-image*)

Hasil dekripsi terhadap ctra pada Gambar 5 mendapatkan kembali citra ‘couple’ semula (*plain-image*). Gambar 6 adalah citra ‘couple’ hasil dekripsi dengan *PSNR* = 46.3006 dB. *PSNR* (*peak-signal-to-noise-ratio*) dihitung dengan rumus $PSNR = 20 \times \log_{10}\left(\frac{b}{rms}\right)$, yang dalam hal ini *b* adalah sinyal puncak (= 255 untuk citra *grayscale*) dan rms adalah singkatan dari *root mean square*.

Gambar 6. Hasil dekripsi citra ‘couple’ (*PSNR* = 46.3006 dB)

Gambar 7 adalah hasil enkripsi citra ‘goldhill’ (*cipher-image*). Citra tersebut terlihat seperti citra acak dengan campuran tiga komponen warna (*red*, *green*, *blue*). Pada Gambar 8 diperlihatkan hasil dekripsi terhadap citra ‘goldhill dengan *PSNR* = 33.9975 dB. Nilai *PSNR* ini masih di atas 30 dB (batas kualitas citra yang dapat ditoleransi).



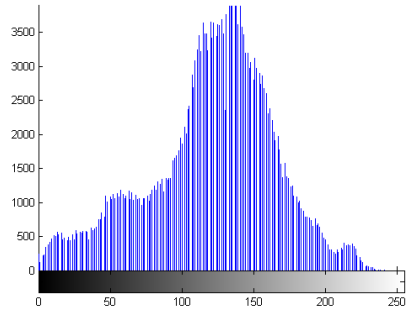
Gambar 7. Hasil enkripsi citra ‘goldhill’ (*cipher-image*)

3.2 Histogram Citra

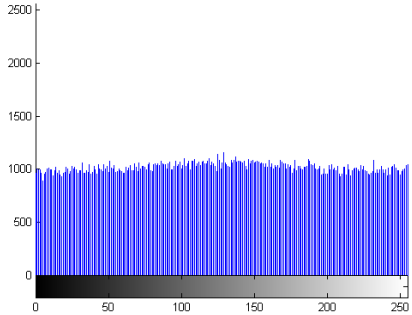
Dalam bidang pengolahan citra, histogram merupakan properti citra yang penting. Sebuah histogram citra menggambarkan distribusi nilai *pixel-pixel* di dalam citra tersebut. Sumbu-*x* menyatakan nilai-nilai *pixel* (0 sampai 255) sedangkan sumbu-*y* menyatakan jumlah *pixel* (atau frekuensi kemunculan *pixel*) yang memiliki nilai tertentu .

Gambar 8. Hasil dekripsi citra ‘goldhill’ (*PSNR* = 33.9975 dB)

Dalam kriptanalisis, penyerang menggunakan berbagai informasi dari *cipher-image* yang dienkripsi untuk menemukan kunci atau mendeduksi *pixel-pixel* di dalam *plain-image*, salah satunya adalah histogram citra. Dengan menganalisis frekuensi kemunculan nilai *pixel* di dalam histogram, penyerang dapat menemukan hubungan antara *pixel-pixel* di dalam *plain-image* dan *cipher-image*.



(a)



(a)

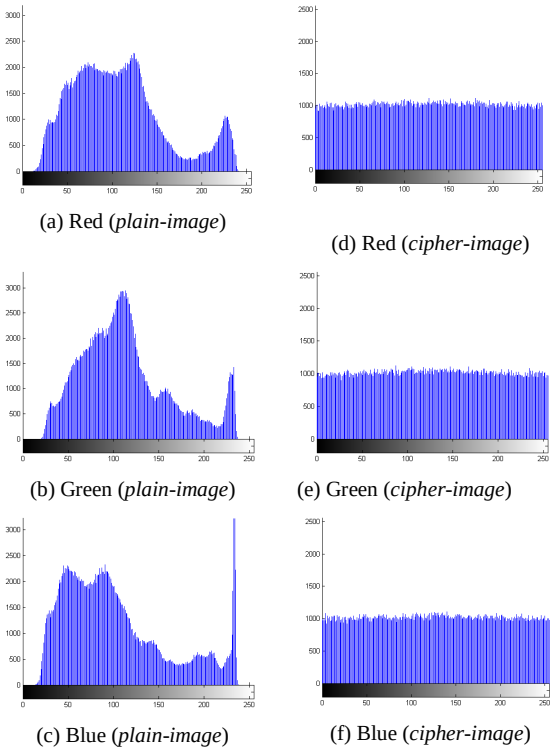
Gambar 9. (a) Histogram *plain-image* dari citra ‘couple’; (b) Histogram *cipher-image* dari citra ‘couple’

Untuk menghambat penyerang melakukan analisis statistik, maka algoritma enkripsi yang bagus seharusnya menghasilkan *cipher-image* yang memiliki histogram berbeda secara signifikan dengan histogram *plain-image*. Dengan kata lain, histogram *cipher-image* tidak memiliki kemiripan secara statistik dengan histogram *plain-image*. Pada citra yang normal, histogram *plain-image* biasanya memperlihatkan lembah dan bukit, maka pada *cipher-image* histogramnya seharusnya datar (*flat*) sehingga tidak memberikan informai bermanfaat bagi kriptanalis. Bentuk histogram citra yang datar menggambarkan *pixel-pixel* di dalam *cipher-image* terdistribusi secara *uniform*.

Gambar 9(a) memperlihatkan histogram citra ‘couple’, sedangkan Gambar 9(b) memperlihatkan histogram *cipher-image*. Histogram *cipher-image* tampak datar yang berarti frekuensi kemunculan *pixel* yang bernilai 0 – 255 adalah relatif seragam.

Histogram untuk citra berwarna dibuat terpisah masing-masing untuk komponen warna (*red*, *green*, dan *blue*). Gambar 10(a) sampai 10(c) adalah histogram citra ‘goldhill’ (*plain-image*) untuk setiap kanal warna *RGB*, sedangkan Gambar 10(d) sampai 10(f) adalah histogram masing-masang kanal warna pada *cipher-image*-nya. Seperti pada citra

sebelumnya, histogram citra *cipher-image* bentuknya relatif datar, dengan kata lain *pixel-pixel* di dalam *cipher-image* terdistribusi secara *uniform.*



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

Eksperimen di atas berhasil memperlihatkan *pixel-pixel* di dalam *cipher-image* memiliki distribusi yang relatif *uniform* sehingga tidak memberikan informasi yang berguna bagi kriptanalis untuk melakukan serangan menggunakan analisis frekuensi. Bentuk histogram yang relatif datar menunjukkan bahwa algoritma enkripsi yang diusulkan ini memiliki tingkat keamanan yang bagus.

18. Kesimpulan

Sebuah usulan algoritma enkripsi citra digital berbasis *chaos* yang beroperasi dalam gabungan ranah frekuensi dan ranah spasial telah dipresentasikan. Hasil eksperimen memperlihatkan citra hasil enkripsi sudah tidak dapat dikenali lagi karena menyerupai citra acak. Citra hasil enkripsi memiliki histogram yang relatif datar sehingga menyulitkan kriptanalis melakukan analisis statistik untuk mendeduksi kunci atau *pixel-pixel* di dalam citra semula.

19. Acknowledgment

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

Daftar Pustaka:

[1] 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.

[2] Rinaldi Munir, *Algoritma Enkripsi Selektif Citra Digital dalam Ranah Frekuensi Berbasis Permutasi Chaos*, Jurnal Rekayasa Elektrika, Jurusan Teknik Elektro Universitas Syiah Kuala, Banda Aceh, Edisi Oktober 2012 (*accepted*)

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

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