Penerapan DES dalam Skema Watermarking Berdasarkan Kuantisasi Warna

Hari Bagus Firdaus – NIM: 13506044

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
Email: if16044@students.if.itb.ac.id

Abstrak

Watermarking digital saat ini sudah sangat luas digunakan untuk memecahkan masalah perlindungan hak cipta dari konten media terkait penggunaan dan distribusi ilegal. *Watermarking* dilakukan dalam 2 tahap: 1) penyisipan *watermark* (*watermark embedding*), dan 2) ekstraksi atau pendeteksian *watermark* (*watermark detection*). Penyisipan *watermark* akan menghasilkan citra ber-*watermark*. Ekstraksi citra ber-*watermark* akan menghasilkan kembali citra asli, sedangkan deteksi *watermark* hanya digunakan untuk mengetahui apakah *watermark* terdapat atau tidak dalam citra.

Di sisi lain, *Data Encryption Standard* (DES) adalah sistem kriptografi simetri dan tergolong jenis *cipher* blok yang sudah populer karena dijadikan standar algoritma kunci-simetri, meskipun saat ini sudah digantikan dengan *Advanced Encryption Standard* (AES). DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit *plainteks* menjadi 64 bit *cipherteks* dengan menggunakan 56 kunci internal (*internal-key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*exteral-key*) yang panjangnya 64 bit.

Makalah ini membahas tentang penerapan dari *Data Encryption Standard*, yaitu sebuah standar kriptografi yang menggunakan algoritma-algoritma cipher blok (*Data Encryption Algorithm*), dalam suatu proses pemberian *watermark* terhadap suatu *image*/citra berdasarkan kuantisasi warna. Makalah ini akan menekankan pada penjelasan tentang *Data Encryption Standard*, penjelasan skema *watermarking* berbasis kuantisasi warna, *watermark embedding*, *watermark extraction*, dan hasil *watermarking* dengan skema ini.

Kata kunci: *watermarking* citra, kuantisasi warna, pemetaan pixel, *Data Encryption Standard*

1. Pendahuluan

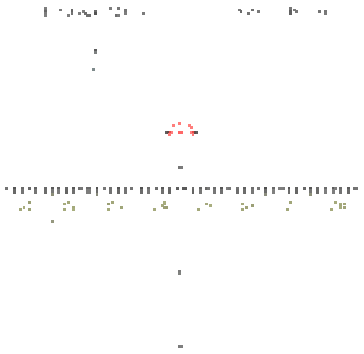
Perkembagan media digital dan semakin populernya internet, semakin banyak pula kegiatan-kegiatan ilegal seperti duplikasi, modifikasi, dan pemalsuan yang dilakukan terhadap media-media digital tersebut secara mudah dan cepat. Operasi ilegal ini berdampak pada motivasi para penciptanya dan akan menghambat kreatifitas. Oleh karena itu, perlindungan terhadap hak properti intelektual pada media-media digital tersebut adalah sebuah *urgent matter*. Diantara jenis-jenis digital media yang ada, citra atau gambar adalah yang paling rentan terhadap operasi-operasi ilegal tersebut, karena data berupa citra dapat dengan mudah ditangkap oleh mata manusia.

Dari semua metode yang diperkenalkan untuk memproteksi hak kekayaan intelektual dari citra digital, pengembangan dari *waternarking* digital adalah pendekatan yang paling umum digunakan. Dalam skema *watermarking* digital, beberapa tipe dari data digital seperti logo, label atau nama, yang disebut *watermark*, ditanam ke dalam citra yang diinginkan. Watermark ini digunakan untuk merepresentasikan kepemilikan dari citra tersebut.

Skema *watermark* dapat diklasifikasikan ke dalam dua kategori: *watermark* domain/ranah spasial dan *watermark* domain/ranah transform. Pada domain spasial, *watermark* disisipkan ke dalam citra dengan memodifikasi secara langsung nilai pixel dari citra asli tanpa menimbulkan perubahan yang signifikan pada representasi citra. Pada domain transform, dilakukan sebuah prosedur trnasformasi domain dengan fungsi transformasi seperti *discrete cosine transformation* (DCT), *discrete fourier transformation* (DFT), *discrete wavelet transformation* (DWT), dll. Lalu, koefisien frekuensi yang sudah dikenai transformasi tadi dimodifikasi untuk menyisipkan *watermark*. Dan terakhir, citra akan dikenai invers dari fungsi transformasi yang digunakan untuk menyisipkan *watermark* tadi.

Keuntungan utama dari skema *watermarking* domain frekuensi adalah mereka lebih kuat/kokoh daripada skema domain spasial. Akan tetapi, biasanya skema transformasi ienis ini akan melibatkan lebih banyak biaya komputasional karena transformasi forward tambahan dan invers transformasi harus dilakukan.

Data Encryption Standard (DES) sendiri adalah sebuah algoritma sandi kunci blok simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit. Maksud ukuran kunci adalah panjang kunci eksternal yang dimasukkan pengguna adalah sebesar 64 bit, namun hanya 56 bit saja yang digunakan (8 bit pasitas tidak digunakan). DES ini adalah standar umum enkripsi data yang dahulu sempat populer, dikembangkan oleh IBM pada 1972 berdasarakan algoritma Lucifer yang dibuat oleh Horst-Feistel dan kemudian disetujui oleh NSA dan NBS Amerika Serikat setelah menilai kekuatannya.



Gambar 1 Garis besar proses operasi DES

Pada praktiknya, beberapa monitor dan *display device* lainnya memiliki *frame buffer* yang terbatas yang hanya dapat menampilkan sejumlah kecil warna secara simultan. Contohnya, sebuah monitor dengan 8 bits *frame buffer* hanya mampu menampilkan 256 warna. Sedangkan sebuah gambar RGB dengan 24 bits/pixel mengandung total 16.777.216 warna. Untuk menampilkan gambar seperti itu pada *display device* sejenis diatas, dikembagkanlah teknik kuantisasi warna. Pada teknik ini, sebuah set atau kumpulan dari warna-warna representatif, yang disebut palet atau palet warna, dipilih untuk merepresentasikan warna asli dari citra. Setiap pixel pada citra RGB dipetakan ke warna yang paling dekat menyerupai warna aslinya pada palet. Biasanya, sejumlah distorsi akan muncul pada citra dengan warna terkuantisasi.

Keuntungan penggunaan *frame buffer* yang terbatas dan waktu transmisi yang rendah akan membuat teknik kuantisasi warna ini secara luas dapat diaplikasikan dalam animasi komputer, *pseudocoloring*, *color adjustment*, dll. Untuk menyediakan proteksi hak cipta pada citra-citra yang mengalami kuantisasi warna ini, sebuah skema *watermarking* berdasarkan teknik ini diperkenalkan, yang akan mempeluas penelitian tentang sekma *watermarking* terhadap citra yang secara langsung menyisipkan *watermark* ke dalam citra asli yang sudah terkompres. Skema *watermark* ini akan menggunakan bantuan DES dalam proses penyisipan *watermark* tersebut.

2. Data Encryption Standard

DES adalah algoritma *cipher* blok yang populer karena dijadikan standar algoritma enkripsi kunci-simetri, meskipun aat ini sudah digantikan algoritma yang baru, AES. DES mengenkripsikan 4 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal atau upa-kunci. Kunci internal dibangkitkan dari kunci eksternal yang panjannya 64 bit. [2]

Skema global DES pertama-tama adalah melakukan permutasi terhadap blok plainteks dengan matriks permutasi awal (*Initial Permutation* atau IP). Hasil permutasi awal kemudian di-enciphering sebanyak 16 kali (16 putaran) dimana setiap putarannya menggnakan kunci internal yang berbeda. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers IP atau IP-1) menjadi blok cipherteks.

Dalam proses enkripsi, blok plainteks terbagi menjadi dua, kiri (L) dan kanan (R), masing-masing 32 bit. Secara matematis, satu putaran DES dinyatakan sebagai:

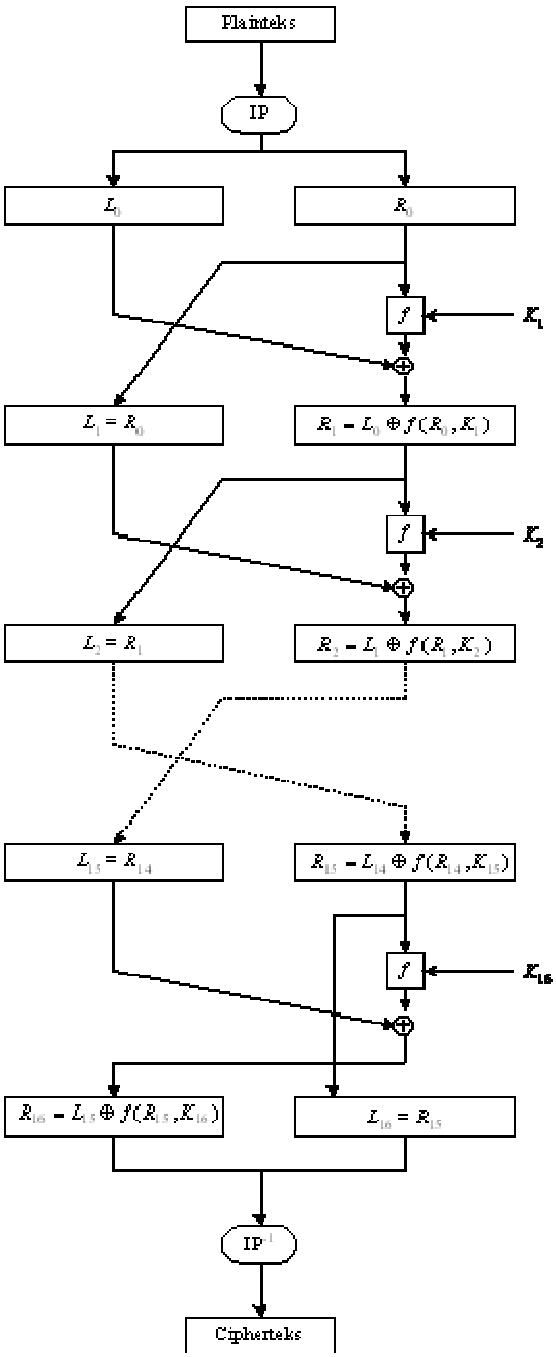
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dar fungsi f di-XOR kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelumnya.

Permutasi awal dilakukan untuk mengacak plainteks sehingga urutan bit-nit didalamnya berubah. Pembangkitan kunci internal dilakukan sebanyak 16 kali karena ada 16 putaran dalam sebuah jaringan feistel. Kunci internal ini dibangkitkan dari knci eksternal yang diberikan oleh pengguna yang panjangnya 64 bit atau 8 karakter. Selanjutnya dilakukan permutasi, tiap bit kedelapan (*parity bit*) dari delapan byte kunci diabaikan, sehingga hasil permutasinya adalah 56 bit. Permutasi terakhir dilakukan setelah 16 kali putaran abungan blok kiri dan blok kanan. Proses ini menggunakan matriks permutasi awal balikan atau invers dari IP.

Dekripsi terhadap cipherteks pada DES merupakan kebalikan dari enkripsi dan tetap menggunakan algoritma yang sama. Jika pada enkripsi urutan kunci internal adalah K1,K2,...K16, maka pada

dekripsi urutan kunci yang digunakan adalah K16,K15...,K1.



Gambar 2 Algoritma enkripsi DES

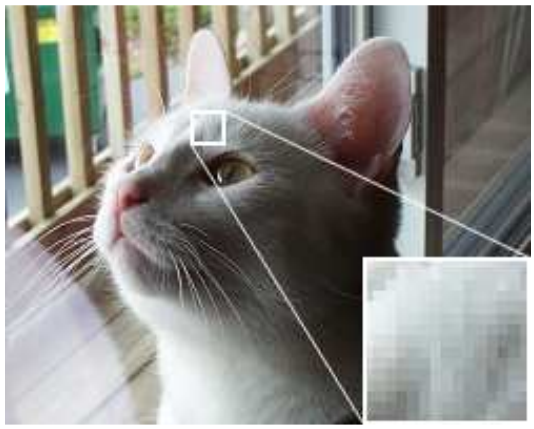
3. Skema Watermarking dengan Teknik Kuantisasi Warna

3.1 Teknik Kuantisasi Warna

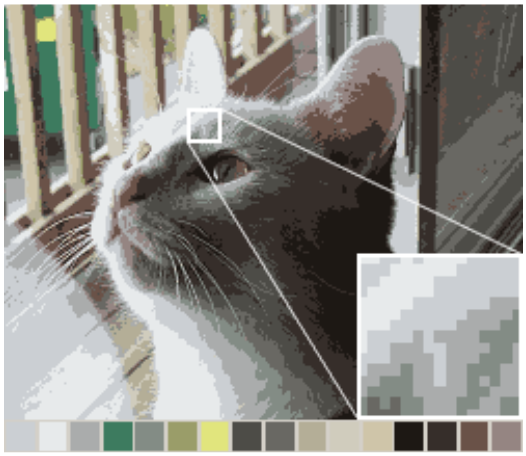
Pada awalnya, tujuan dari teknik kuantisasi warna adalah untuk menyediakan detail citra yang berbeda untuk *display device* yang berbeda yag memiliki *frame buffer* yang terbatas. Operasi utama teknik kuantisasi warna terletak pada prosedur pendesainan palet dan prosedur pemetaan pixel.

Tugas dari prosedur pendesainan palet adalah untuk memilih warna-warna representatif untuk citra-citra tertentu. Secara umum, setiap warna-warna representatif terpilih mengandung tiga dimensi untuk mode warna Red-Green-Blue (RGB) yang bisa dianggap sebagai kata-kata kode pada sebuah buku kode, dimana palet merupakan buku kodenya. Pendesainan palet ini membutuhkan sebuah algoritma khusus yang bertujuan untuk memilih warna representatif yang paling baik dengan sedikit biaya komputasi dan seminimal mungkin distorsi.

Setelah desain palet warna selesai, pemetaan pixel dari citra dilakukan. Tujuan pemetaan pixel ini adalah untuk menemukan warna yang sesuai yang paling dekat dari palet untuk merepresentasikan pixel dari suatu citra dengan menimbulkan seminimal mungkin distorsi warna. Setiap pixel pada citra berwarna asli dipetakan ke warna terdekat yang ada di palet.



Gambar 3 Citra 24-bit RGB



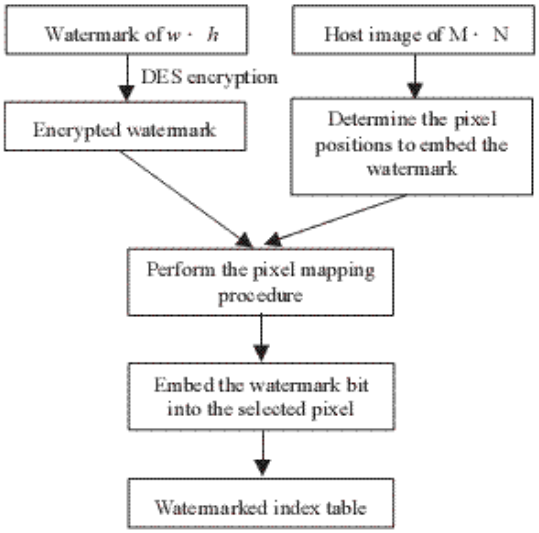
Gambar 4 Citra dengan warna terkuantisasi oleh palet 16 warna terdekat warna citra asli; warna pada palet ditunjukkan oleh kotak-kotak diatas [3]

Squared Euclidean Distance (SED) adalah salah satu cara yang paling banyak digunakan dalam menemukan warna terdekat yang berada di palet. SED antara pixel asli (h_i) dan warna pada palet (cj) dapat dihitung dengan rumus berikut [1]:

$$SED(hi, cj) = \sum_{i=1}^{k} (\text{hi} - \text{cji})^2$$

dimana *k* adalah dimensi dari setiap warna pada palet dan c_{ji} adalah dimensi ke-$_i$ dari kode c_j. Setelah menemukan index dari warna terdekat pada palet untuk setiap pixel dari citra asli, index tersebut lalu disimpan dan digunakan untuk menampilkan citra masukan tadi.

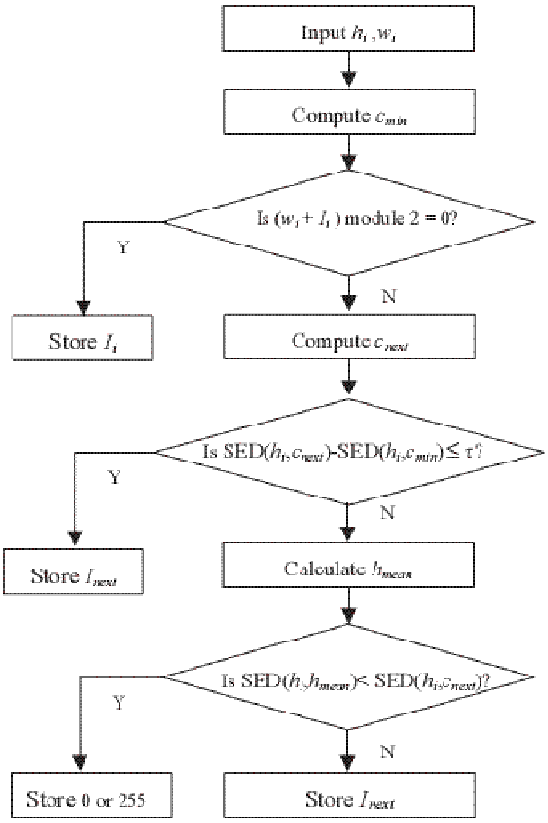
3.2 Prosedur Penyisipan Watermark



Gambar 5 Skema umum penyisipan *watermark*

Sebuah citra yang akan disisipi *watermark* (host image) H adalah sebuah citra berwarna RGB berukuran *M* x *N* pixel, dimana H = (h_1,h_2,...,$h_M x_N$). Watermark W adalah sebuah citra biner yang terdiri dari *w* x *h* bit, dimana W = (w_1,w_2,...,$w_w x_h$) dan W_i Є (0,1). Palet dengan pilihan optimal yang digunakan dapat di-*generate* langsung oleh program-program pengolah grafis seperti Adobe Photoshop.

Setelah melakukan pendesainan palet, prosedur yang akan dilakukan kemudian adalah melakukan pemetaan pixel untuk mengkuantisasi warna. Ketika prosedur pemetaan ini dilakukan, pada saat inilah proses penyisipan *watermark* juga dilakukan. Untuk keamanan, bit-bit *watermark* yang akan disisipkan akan terlebih dahulu dienkripsi dengan prosedur DES, sebelum *watermark* benar-benar disisipkan. Sebagai tambahan, sebuah *pseudorandom number generator* (PRNG) digunakan untuk menentukan posisi-posisi pixel yang akan dipergunakan untuk menyisipkan bit-bit *watermark* tadi.



Gambar 6 Flow chart proses penyisipan *watermark*

Algoritma penyisipan *watermark* akan dijelaskan sebagai berikut:

1. Lakukan ekripsi DES terhadap *watermark* W dan tentukan PNRG untuk menghasilkan kumpulan posisi dari *w* x *h* pixel untuk *watermark* yag akan disisipkan.
2. Untuk setiap pixel h_i, warna terdekat cmin dengan index I_i dipilih menggunakan prosedur pemetaan pixel.
3. Ketika pixel h_i merupakan satu dari pixel-pixel yang terpilih, jika (w_i+I_i) modulo 2 adalah 0, I_i akan secara langsung disimpan. Pergi ke langkah 7.
4. Temukan warna terdekat lainnya c_{next} dengan index I_{next} pada palet, yang memenuhi (w_i+I_{next}) modulo 2 adalah 0. Apabila SED(h_i,c_{next}) − SED(h_i,c_{min}) ≤ τ, I_{next} akan disimpan. Pergi ke langkah 7.
5. Hitung nilai rata-rata h_{mean} dari h_1 pixel kiri dan langsung diatas h_a pixel dari h_i. Jika SED(h_i,h_{mean}) < SED(h_i,c_{next}), 2 buah index spesial 0 dan 255 akan disimpan untuk x_i = 0 dan 1 secara berurutan. Pergi ke langkah 7.

6. Jika SED(h_i,h_{mean}) ≥ SED(h_i,c_{next}), Inext akan disimpan.
7. Apabila masih ada bit *watermark* untuk disisipkan, pergi ke langkah 2.

Pada skema diatas, bit-bit *watermark* disisipkan ke dalam tabel index warna, dimana ukuran dari tabel index tidak dimodifikasi. Selain itu, penggunaan prosedur enkripsi DES dan PRNG akan meningkatkan keamanan dari skema *watermarking* ini.

3.3 Proses Ekstraksi Watermark

Prosedur ekstraksi *watermark* dengan teknik kuantisasi warna dimasukkan dalam struktur dari prosedur pendekodean citra. Pertama, PRNG menentukan posisi dari pixel-pixel citra yang digunakan untuk menyisipkan bit-bit *watermark*.

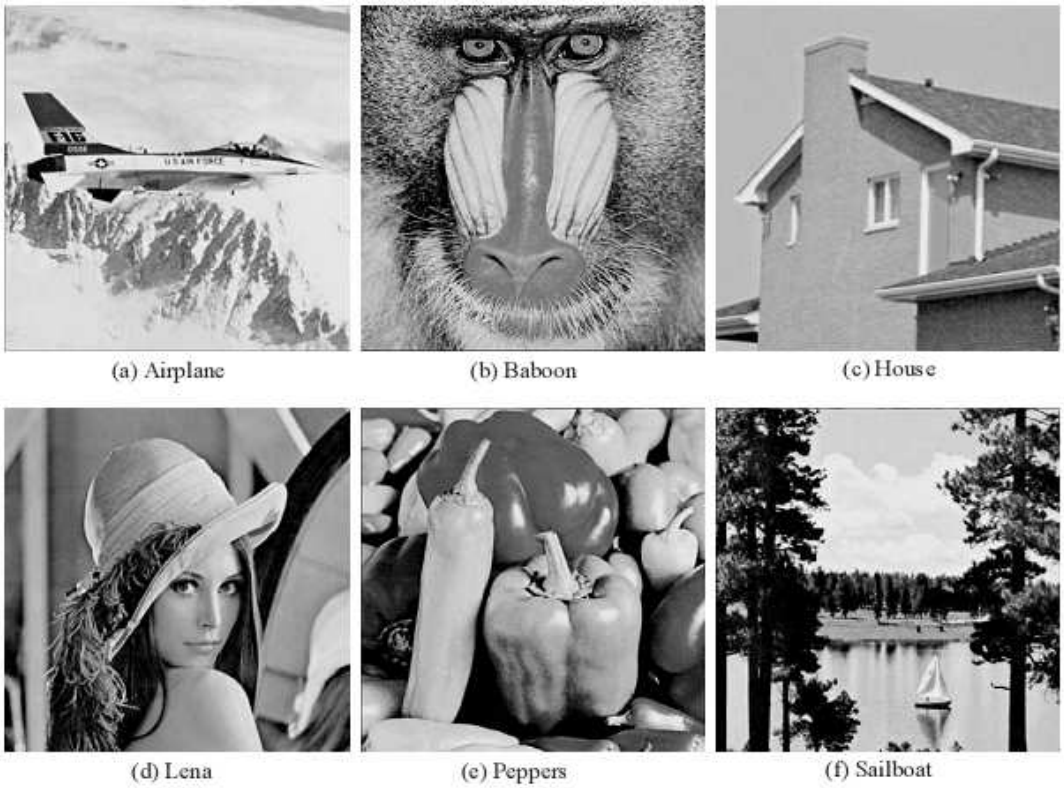
Pada prosedur pendekodean citra ini, setiap masukan atau *entry* dalam tabel index warna akan digantikan oleh warna yang bersesuaian atau berkorespondensi pada palet. Ketika sebuah *entry* mengadung *watermark* ditemukan, bit *watermark* yang bersesuaian diekstrak sebelum penggantian warna dilakukan. Apabila nilai *entry* adalah ganjil, itu berarti bahwa bit *watermark* yang disisipkan tersebut diberikan nilai satu. Apabila nilai *entry* adalah genap, itu berarti bahwa bit *watermark* yang disisipkan tersebut diberikan nilai nol. Bit-bit *watermark* yang sudah diektrak tadi lalu didekripsikan dengan prosedur deksipsi *Data Encryption Standard*.

Algoritma ekstraksi *watermark*:

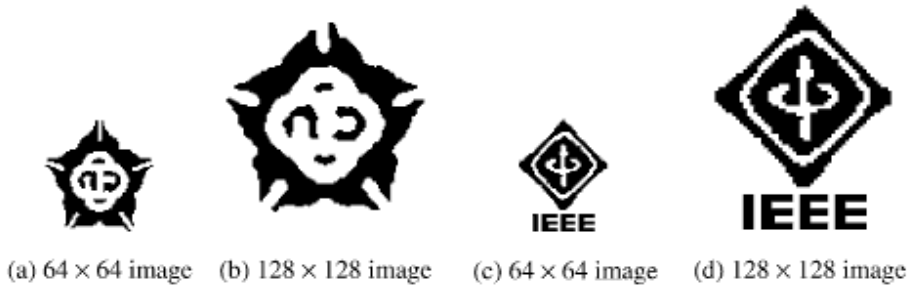
1. Gunakan PRNG untuk menentukan posisi dari entry pada tabel index warna yang mengandung bit-bit *watermark*.
2. Apabila nilai dari *entry* yang dipilih adalah ganjil, nilai bit *watermark* yang diekstrak akan diset menjadi satu. Apabila nilai *entry* adalah genap, nilai bit *watermark* yang diekstrak akan diset menjadi nol.
3. Lakukan prosedur dekripsi DES untuk mengembalikan *watermark*.

4. Hasil Percobaan

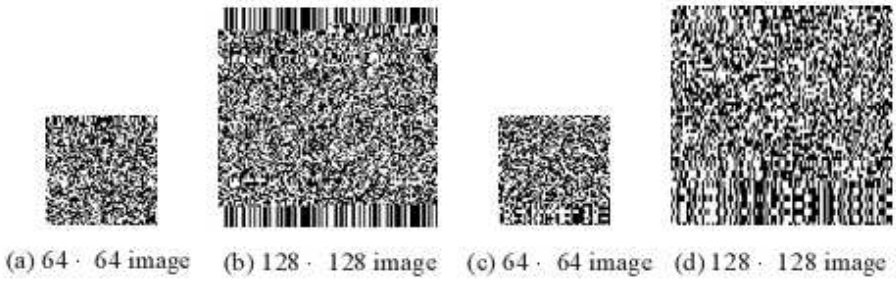
Beberapa percobaan telah dilakukan pada sejumlah komputer. Simulasi yang telah dicobakan dengan mengambil sebuah kumpulan citra RGB dengan ukuran 512 x 512 pixel, “Airplane”, “Baboon”, “House”, “Lena”, “Peppers”, dan “Sailboat” sebagai citra asli yang akan disisipkan *watermark*. Dua buah citra biner, “CCU” dan “IEEE”, masing-masing dengan ukuran 64 x 64 dan 128 x 128 bit, digunakan sebagai citra *watermark* pada simulasi.



Gambar 7 Enam citra asli 512 x 512 pixel



Gambar 8 Empat citra *watermark*



Gambar 9 Citra *watermark* terenkripsi DES

Untuk setiap citra asli, sebuah palet yang berkorespondensi di-*generate* oleh *software* Adobe Photoshop versi 5.0 dengan pilihan palet optimal. Setiap palet mengandung 256 warna dan terindeks mulai dari 0 sampai dengan 255. Setiap warna pada palet memiliki *channel* RGB.

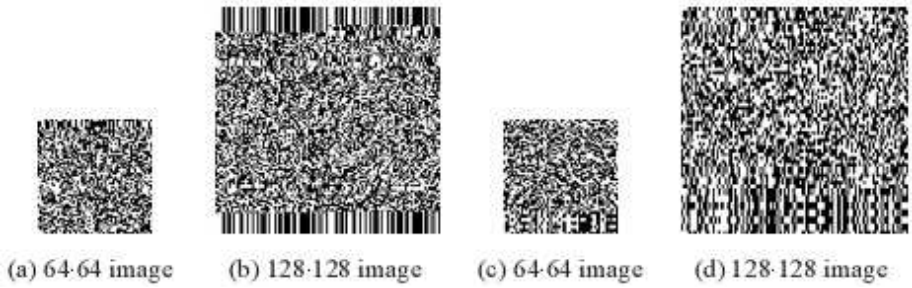
Gambar 10 Citra "Lena" hasil *watermarking* dengan keempat citra *watermark* terenkripsi

Selanjutnya adalah melakukan prosedur enkripsi DES untuk megenkripsi citra *watermark* dan PRNG digunakan untuk menentukan posisi pixel untuk menyisipkan *watermark*. Gambar 9 menunjukkan citra *watermark* pada Gamabar 8 yang sudah terenkripsi. Dapat dilihat bahwa pixel-pixel pada setiap citra *watermark* terenkripsi sangat berbeda.

Gambar 10 menunjukkan empat buah citra “Lena” yang sudah dikenai proses *watermark* dengan teknik kuantisasi warna. Disini, empat citra *watermark* yang sudah terenkripsi seperti pada Gambar 9 digunakan untuk meghasilkan keempat gambar “Lena” tersebut. Menurut pengamatan dari hasil yang didapat, dapat terlihat bahwa kualitas visual dari setap citra ber-*watermark* cukup bagus.

Untuk mengidentifikasi kepemilikan dari citra ber-*watermark*, prosedur estraksi *watermark* dengan teknik kuantisasi warna dilakukan. Gambar 11 menunjukkan keempat citra *watermark* terenkripsi yang sudah diektrak. Keempat citra *watermark* tersebut kemudian diproses lebih lanjut oleh prosedur dekipsi DES. Citra-citra *watermark* hasil dari proses dekripsi tersebut ditunjukkan oleh Gambar 12.

Untuk mengetahui apakah prosedur penyisipan *watermark* yang dilakukan mungkin saja menyebabkan degradasi citra, suatu set simulasi yang melakukan pemetaan dasar dari pixel-pixel dieksekusi. Keenam gambar yang terkuantisasi dari keenam gambar asli ditunjukkan dalam Gambar 13. Menurut hasil pengamatan, tidak ada degradasi warna karena sangat susah untuk mata manusia dapat menemukan perbedaan diantaranya.

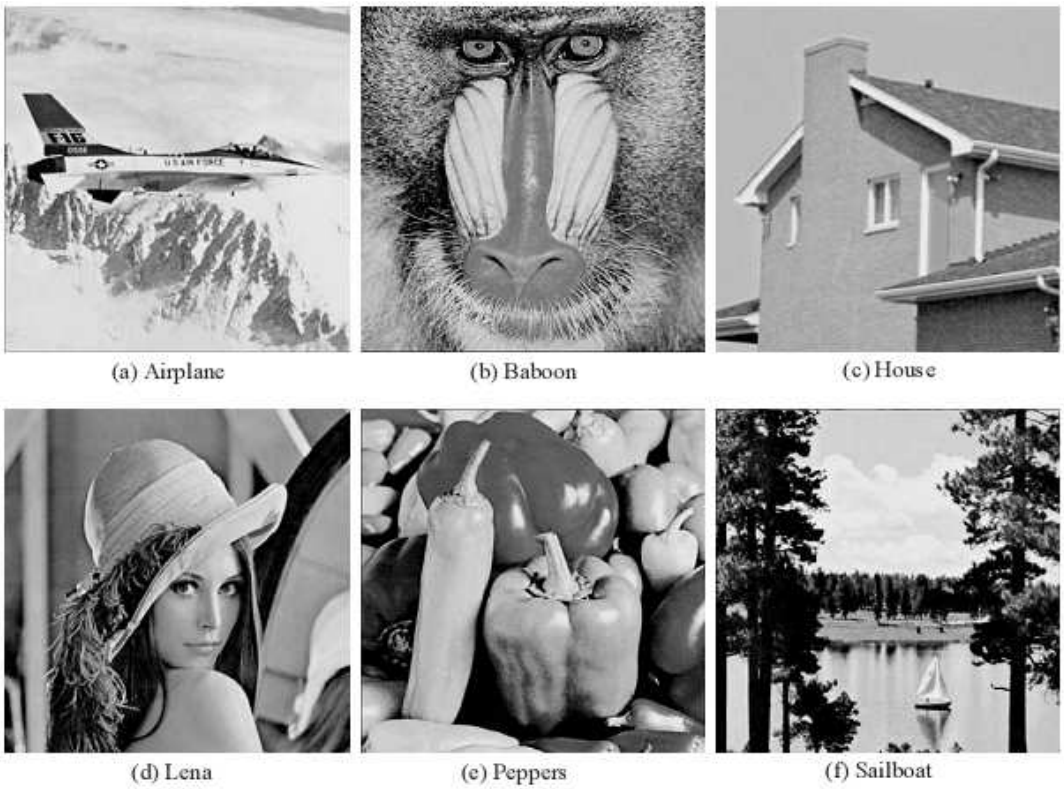


(a) 64·64 image (b) 128·128 image (c) 64·64 image (d) 128·128 image

Gambar 11 Hasil ekstrak citra *watermark* terenkripsi DES

(a) 64 × 64 image (b) 128 × 128 image (c) 64 × 64 image (d) 128 × 128 image

Gambar 12 Hasil dekripsi DES citra *watermark*



(a) Airplane (b) Baboon (c) House

(d) Lena (e) Peppers (f) Sailboat

Gambar 13 Citra asli yang warnanya terkuantisasi

5. Kesimpulan

Watermarking sangat penting diperlukan untuk melindungi hak-hak cipta pada suatu media digital. Makalah ini membahas salah satu contoh watermarking pada citra/gambar yang berbasiskan teknik kuantisasi warna, yaitu warna citra asli akan dipetakan pada suatu palet sehingga warna yang akan ditampilkan nantinya adalah warna dari palet yang paling dekat menyerupai warna aslinya.

Pemberian watermark pada citra dengan warna yang terkuantisasi ini dapat dilakukan dengan menambahkan suatu prosedur penyisipan watermark yang dilakukan pada saat proses kuantisasi warna berlangsung, tepatnya ketika proses pemetaan pixel dilakukan. Watermark akan disisipkan ke dalam tabel index warna. Sedangkan untuk mengekstrak watermark dari citra, diperlukan suatu prosedur ekstraksi watermark yang dilakukan pada saat proses pendekodean citra terkuantisasi.

Untuk meningkatkan keamanan, suatu cipher harus diimplementasikan pada skema ini, yaitu Data Encryption Standard. Enkripsi DES pada citra watermark ini berfungsi untuk menukar urutan bit-bit dari citra watermark. Hasil enkripsi akan disisipkan pada pixel-pixel dari citra asli, yang ditentukan oleh PRNG. Hal ini akan menyediakan keamanan yang lebih baik dari sekedar proses *watermarking* biasa.

Menurut hasil percobaan, terlihat bahwa skema watermarking berbasis kuantisasi warna ini tidak hanya menyediakan kualitas citra yang baik, tetapi juga membutuhkan biaya komputasi yang sangat kecil. Selain itu, skema ini juga memperkenalkan suatu pendekatan watermarking efektif yang dapat diaplikasikan kepada media digital lain berbasis kuantisasi warna.

DAFTAR PUSTAKA

[1]Tsai, Piyu, Yu-Chen Hu, Chin-Chen Chang. (2003). A color image watermarking scheme based on color quantization. *http://www.sciencedirect.com*. Tanggal akses: 2 April 2009 pukul 19.00.

[2] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[3] *http://*en.wikipedia.org/wiki/Color_quantization Tanggal akses: 2 April 2009 pukul 20.00.