T – 25

Pemberian Tanda Air Pada Citra Dijital Menggunakan Skema Berbasis Kuantisasi Warna

Soetrisno, Muhammad Irvan
Jurusan Matematika FMIPA ITS
E-mail : soetrisno@matematika.its.ac.id

ABSTRAK

Salah satu penerapan matematika adalah penggunaan matematika dalam proses pemberian tanda air pada sebuah citra dijital.

Pemberian tanda air (*watermarking*) merupakan salah satu teknik pengamanan file citra dijital atau teknik penyembunyian sebuah sandi rahasia dalam sebuah file citra dijital. Proses pemberian tanda air pada citra dijital terdiri dari dua proses utama, yaitu proses pelekatan tanda air kedalam file citra dijital dan proses pemisahan (ekstraksi) tanda air dari file citra dijital. Pemberian tanda air pada file citra dijital telah banyak diterapkan untuk memberi perlindungan hak cipta media dijital. Dalam beberapa tahun terakhir, skema pemberian tanda air pada citra abu-abu (*gray-level*) telah digunakan, tetapi skema pemberian tanda air pada citra berwarna masih merupakan sesuatu yang langka dan biasanya bekerja pada warna pencahayaan. Oleh karena itu, pada makalah ini dibahas sebuah metode pemberian tanda air berbasis kuantisasi warna. Dalam metode ini digunakan citra tanda air (*watermark*) yang dienkripsi DES untuk dilekatkan pada citra asal (*host*). Proses pelekatan tanda air dengan skema berbasis kuantisasi warna menghasilkan sebuah citra ter-*watermark* yang akan digunakan pada proses ekstraksi. Proses ekstraksi tanda air dalam metode ini menggunakan *pseudo random number generator* dan dekripsi DES. Pada makalah ini proses ekstraksi dilakukan pada citra ter-*watermark* yang normal dan pada citra ter-*watermark* yang mengalami gangguan.

Setelah dilakukan pemrograman dari proses ini dan diuji coba, diperoleh hasil bahwa: (i) secara visual tanda air dapat dipersepsikan dengan sangat baik; dan (ii) hasil analisis memberikan simpulan bahwa implementasi sistem memberikan kesalahan estimasi tanda air dalam kisaran 9,1805 %.

Kata kunci: *Watermarking,* DES, Kuantisasi warna, *Pseudo random number generator.*

1. PENDAHULUAN

Perkembangan teknologi komputer dijital dan perangkat-perangkat lainnya semakin cepat, hal ini membuat data dijital banyak digunakan karena mudah diduplikasi, mudah diolah, serta mudah didistribusikan. Dengan berkembangnya internet, distribusi data dijital, salah satunya berupa citra dijital menjadi semakin mudah. Dalam beberapa kasus, citra dijital membutuh-kan pengamanan agar tidak terjadi pelanggaran hak cipta. Citra dijital juga digunakan untuk menyembunyikan suatu kode rahasia yang akan dikirimkan kepihak lain. Banyak metode dikembangkan untuk mengamankan dan melindungi citra digital, salah satunya adalah *watermarking* pada citra dijital.

Selama ini penggandaan atas produk dijital seperti citra dijital dilakukan begitu bebas dan leluasa secara ilegal. Hasil penggandaan tersebut memiliki kualitas yang sama dengan produk dijital aslinya. Namun, pemegang hak cipta produk dijital tidak mendapatkan royalti dari penggandaan tersebut. Akibatnya pemegang hak cipta produk

dijital sangat dirugikan. Hampir semua produk dijital yang tersebar di internet tidak mencantumkan informasi pemiliknya. Khususnya untuk bidang citra dijital, adanya perangkat lunak untuk rekayasa citra seperti *Adobe Photoshop* memungkinkan untuk melakukan berbagai modifikasi terhadap citra dengan bantuan perangkat lunak tersebut. Dengan demikian keamanan terhadap suatu citra dijital menjadi sangat rentan.

Watermarking merupakan salah satu solusi teknis yang diusulkan untuk menangani keamanan materi dijital. *Watermarking* adalah potongan informasi yang disisipkan pada materi data dan berfungsi sebagai alat untuk identi-fikasi kepemilikan, hak penggunaan, kontrol distribusi dan integritas data[4].

Ada beberapa metode *watermarking* pada citra dijital yang telah digunakan dan metode *watermarking* pada citra dijital yang telah digunakan memiliki kelebihan dan kelemahan. . Pada penelitian ini dikemukakan sebuah metode ekstraksi yaitu dengan menggunakan prosedur enkripsi-dekripsi *Data Encrytion Standard* (DES) dan *Pseudo Random Number Generator* (PRNG). Oleh karena itu dalam penelitian ini dikembangkan sebuah metode *watermarking* berdasarkan Skema Kuantisasi Warna [6].

Pada penelitian ini diberikan batasan masalah dan asumsi sebagai berikut :

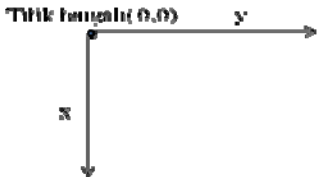
1. Citra *Watermark W* yang digunakan dalam penelitian ini adalah citra biner JPG berukuran *N* x *N*.
2. Citra *Host H* yang akan diproses adalah berupa citra *RGB* dan *grayscale*, bertipe JPG berukuran *M* x *M*.
3. Gangguan yang akan diberikan pada citra ter-*watermark* adalah penambahan *noise* dengan level 1%, level 3% dan 5%.
4. Algoritma yang digunakan adalah *Squared Euclidean Distance* (SED).
5. Ukuran citra *watermark* harus lebih kecil dari pada citra *host.*
6. Warna palet yang digunakan sebatas 862
   warna RGB.

2. DASAR TEORI

2.1 Citra Dijital

Citra adalah gambar pada bidang dua dimensi. Ditinjau dari sudut pandang mate-matika, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi.

Citra dibentuk dari persegi empat yang teratur sehingga jarak horizontal dan vertikal antara piksel satu dengan yang lain adalah sama pada seluruh bagian citra. Indeks x bergerak ke bawah dan indeks y bergerak ke kanan. Untuk menunjukkan koordinat sebuah titik digunakan posisi kanan bawah dalam citra berukuran m x n piksel. Gambar-1 menunjuk-kan sistem koordinat pada suatu citra dijital.



Gambar-1 Koordinat pada citra dijital

Untuk menunjukkan tingkat intensitas cahaya hitam-putih (*grayscale*) suatu piksel, digunakan bilangan bulat dengan rentang selang antara 0-255, dimana 0 untuk warna hitam dan 255 untuk warna putih. Sistem visual manusia dapat membedakan ratusan ribu warna tetapi hanya dapat membedakan 100 *shade* ke-abuan[4].

2.2 Konsep Tetangga Piksel

Pada pengolahan citra dijital dibutuhkan beberapa konsep dasar tentang citra, misalnya untuk mencari rata-rata piksel atau variansi lokal citra dibutuhkan konsep piksel tetangga. Salah satu konsep piksel tetangga yang digunakan adalah 8-tetangga, yang dinotasikan dengan $N8(p)$. Agar piksel tepi dapat di-manipulasi seperti piksel di bagian dalam citra maka dilakukan penambahan satu piksel di sekeliling citra. Piksel tambahan dapat bernilai 0, 1 atau sama dengan piksel tepi dan pemilihannya disesuaikan dengan kebutuhan.

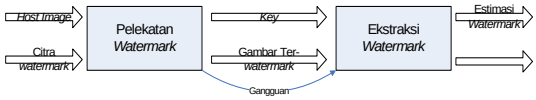
Hubungan piksel $N\ 8(p)$ direpresentasi-kan oleh Gambar-2.

f(x-1,y-1)	f(x-1,y)	f(x-1,y+1)
f(x,y-1)	**f(x,y)**	f(x,y+1)
f(x+1,y-1)	f(x+1,y)	f(x+1,y+1)

Gambar-2. Hubungan piksel $N8(p)$

2.3 Watermarking

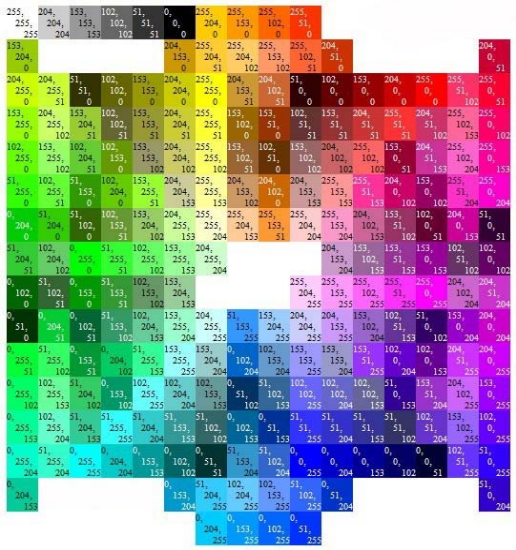
Watermarking dapat diartikan sebagai suatu teknik penyembunyian data (citra dijital) atau informasi rahasia yang berupa citra dijital kedalam suatu data (citra dijital) yang lain untuk ditumpangi, sedemikian hingga orang lain tidak menyadari kehadiran (adanya) data tambahan pada data host-nya. Jadi seolah-olah tidak ada perbedaan antara data host sebelum dan sesudah prosesnya [5]. Secara umum proses watermarking dibagi menjadi dua yaitu proses pelekatan dan proses ekstraksi. Gambar-3 berikut ini menunjukkan skema watermarking.



Gambar-3 Skema *watermarking*

2.4 Palet

File JPG menggunakan warna merah, hijau, dan biru (RGB) untuk warna grafis. Warna RGB juga dikenal sebagai warna penuh. Warna RGB dikenal sebagai warna aditif karena semua warna, merah hijau, dan biru yang ditambahkan bersama-sama pada intensitas penuh mereka akan menciptakan warna keabuan. Campuran kekuatan relatif dari warna-warna, menciptakan jutaan warna yang dapat ditampilkan. Kekuatan warna tersebut diatur dalam rentang dari nol sampai 255 dengan nol menjadi intensitas yang paling rendah mewakili warna hitam dan 255 intensitas tertinggi mewakili warna putih. Ketika merah, hijau dan biru digabungkan pada intensitas nol hasilnya adalah hitam. Pada intensitas tinggi, di mana nilai-nilai ditetapkan pada 255, 255, 255, hasilnya adalah warna putih murni[10].



Gambar-4 Warna palet dalam bentuk desimal

2.5 Data Enksripsi Standar (DES)

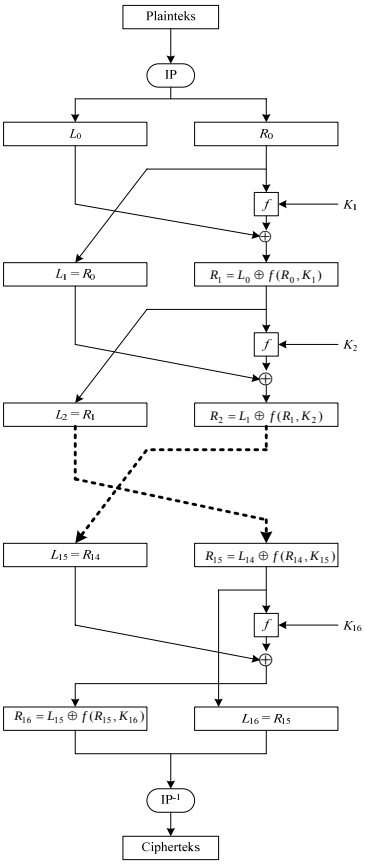
Data Encryption Standard (DES) adalah sistem kriptografi simetri dan tergolong jenis *cipher* blok yang sudah populer karena dijadikan algoritma standar dengan kunci-simetri. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit *plainteks* menjadi 64 bit *cipherteks* dengan menggunakan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

Skema global DES, pertama melakukan permutasi terhadap blok plainteks dengan matriks permutasi awal (inisial permutasi 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[1].

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

$$L_i = R_{i-1} \qquad (1)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \qquad (2)$$



Gambar-5 Proses enkripsi dengan DES

2.6 *Pseudo Random Number Generator* (PRNG)

Bilangan acak (*random*) banyak digunakan di dalam kriptografi, misalnya untuk pembang-kitan elemen-elemen kunci, pembangkitan kunci di dalam sistem kriptografi kunci pembangkit dan sebagainya. Yang dimaksud dengan acak di sini adalah bilangan yang tidak mudah diperdiksi oleh pihak lain. Bilangan acak yang dihasilkan dengan rumus-rumus matema-tika adalah bilangan acak semu (*pseudo*), karena bilangan acak yang dibangkitkan dapat berulang kembali secara periodik. Pembangkit deret bilangan acak semacam itu disebut *pseudo random number generator* (PRNG)[1].

Pembangkit bilangan acak kongruen-lanjar (*linier congruential generator* atau LCG) adalah salah satu pembangkit bilangan acak yang sangat terkenal. LCG didefinisikan dalam relasi rekurensi:

$$x_n = (ax_{n-1} + b) mod\ m \qquad (3)$$

dengan:

x_n = bilangan acak ke-n dari deretnya

x_{n-1} = bilangan acak sebelumnya

a = faktor pengendali

b = *increment*

m = modulus

Kunci pembangkit adalah x_0 yang disebut bilangan awal (*seed*).

2.7 Koefisien Korelasi

Koefisien korelasi $|r_{X,Y}|$ digunakan untuk menghitung kesamaan diantara dua citra, misalkan *X* dan *Y*. Ketika dua citra berbeda secara total nilai $|r_{X,Y}| \approx 0$, dan di sisi lain ketika *X* dan *Y* identik satu sama lain $|r_{X,Y}| \approx 1$. Berikut adalah bentuk umum untuk menghitung koefisien korelasi antara dua citra [3]:

$$|r_{X,Y}| = \frac{|s_{XY}|}{\sqrt{s_{XX} s_{YY}}} \qquad (4)$$

dimana :

$$s_{XY} = \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{(i,j)} - \bar{X})(Y_{(i,j)} - \bar{Y}) \qquad (5)$$

$$s_{XX} = \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{(i,j)} - \bar{X})^2 \qquad (6)$$

$$s_{YY} = \sum_{i=1}^{M} \sum_{j=1}^{N} (Y_{(i,j)} - \bar{Y})^2 \qquad (7)$$

$$\bar{X} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} X_{(i,j)} \qquad (8)$$

$$\bar{Y} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} Y_{(i,j)} \qquad (9)$$

Dalam metode kuantisasi warna koefisien korelasi digunakan untuk mengidentifikasi estimasi citra hasil *watermark*, serta untuk mengukur keidentikan antara citra *watermark* dan estimasi *watermark*.

2.8 Metode *Watermarking* Berdasarkan Kuantisasi Warna

Seperti metode *watermarking* pada umumnya metode Kuantisasi Warna pada citra dijital dapat dibagi menjadi dua bagian yaitu metode pelekatan dan metode ekstraksi.

2.8.1 Metode Pelekatan

Metode pelekatan pada metode kuantisasi warna terdiri dari proses pelekatan citra *watermark W* untuk membentuk citra ter-*watermark I* dan citra *Host H*. Gambar-6 menunjukkan gambaran umum pelekatan menggunakan metode kuantisasi warna.

Masukan berupa citra *watermark W* dan citra *host H*. Mengubah citra *watermark* menjadi chipterteks dengan menggunakan enkripsi DES agar lebih aman sebelum melakukan *color mapping*.

Prosedur desain palet adalah untuk memilih warna-warna representatif untuk citra-citra tertentu. Secara umum, setiap warna-warna representatif terpilih mengandung tiga dimensi untuk warna *Red-Green-Blue* (RGB) yang bisa dianggap sebagai kata-kata kode pada sebuah buku kode, dimana palet merupakan buku kodenya[5].

Setelah palet warna dirancang, pemetaan piksel prosedur dilakukan. Tujuan dari prosedur pemetaan piksel adalah untuk menemukan warna yang sesuai yang paling dekat dari palet untuk merepresentasikan piksel dari suatu citra dengan menimbulkan seminimal mungkin distorsi warna. Setiap piksel dalam warna gambar asli dipetakan ke warna terdekat dalam palet untuk menghasilkan citra terkuantisasi. Secara umum, kuadrat jarak Euclid (SED) adalah yang paling umum digunakan untuk pengukuran jarak warna terdekat. SED antara piksel asli h_i dan c_j warna dalam palet dapat dihitung dengan rumus sebagai berikut[8]:

$$SED(h_i, c_j) = \sum_{i=1}^{k} (h_i - c_{ji})^2 \qquad (10)$$

Langkah-langkah *Embedding Watermark* sebagai berikut:

Langkah 1: Melakukan prosedur untuk enkripsi DES pada *watermark W* dengan *w x h* dan memilih prosedur untuk PRNG untuk pengesetan posisi *w x h* piksel *embedding watermark* tersebut.

Langkah 2: Untuk setiap h_i piksel, yang terdekat dengan warna c_{min} dengan indeks I_i dipilih dengan menggunakan prosedur pemetaan piksel.

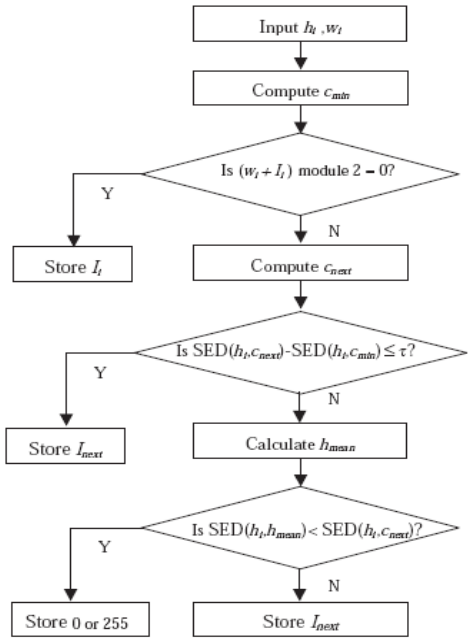
Langkah 3: Ketika piksel h_i merupakan salah satu piksel-piksel yang terpilih, jika $(w_i + I_i)$ maka modulo 2 sama dengan 0, I_i akan disimpan langsung dan berlanjut ke Langkah 7.

Langkah 4: Mencari warna lain c_{next} yang terdekat dengan indeks I_{next} dalam palet yang memenuhi $(w_i + I_{next})$ modul 2 sama dengan 0. Jika SED (h_i, c_{next})- SED $(h_i, c_{min}) \leq \tau$, I_{next} akan disimpan langsung dan berlanjut ke Langkah 7.

Langkah 5: Menghitung nilai rata-rata h_{mean} dari penyandian piksel h_i kiri dan tepat di atas h_a piksel h_i. Jika SED (h_i, h_{mean}) < SED (h_i, c_{next}), dua indeks khusus 0 dan 255 akan disimpan untuk w_i=0 dan 1. Berlanjut ke Langkah 7.

Langkah 6: Jika SED $(h_i, h_{mean}) \geq$ SED (h_i, c_{next}), I_{next} akan disimpan.

Langkah 7: Jika ada bit *watermark* untuk dimasukan maka kembali ke Langkah 2. [6]



Gambar-6 Proses pelekatan *watermark*

2.8.2 Ekstraksi

Proses ekstraksi bertujuan untuk mengekstrak citra *watermark* dari citra yang tersedia. Disamping citra ter-*watermark* I, informasi lain yang tersedia adalah citra *Host* H. Menggunakan *Pseudo Random Number Generator* sebagai *seed* untuk mendapatkan kunci citra *Host* H pada citra *watermark* W. Jadi tujuan dari proses ekstraksi adalah mengekstrak citra *watermark* dari I, citra *Host* H dan *Pseudo Random Number*

Generator. Mengekstrak citra ter-*watermark* I dari citra *watermark* W dan citra *host* H dengan memakai metode Kuantisasi Warna.

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

Pada prosedur pendekodean citra ini, setiap masukan atau *entry* dalam tabel indeks 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 dekripsi *Data*

Encryption Standard. Proses ekstraksi dapat dibagi menjadi beberapa langkah,yaitu :

Algoritma ekstraksi *Watermark*:

Langkah 1: Gunakan PRNG untuk menentukan posisi, masukkan dalam tabel indeks warna yang berisi bit *watermark*.

Langkah 2: Apabila nilai entri yang dipilih adalah ganjil, maka yang diekstraksi bit *watermark* diatur ke satu. Jika tidak, yang diekstraksi bit *watermark* dinilai nol.

Langkah3:Lakukan prosedur untuk deksripsi DES, mengembalikan ke citra watermark.

2.9 Mean Square Error

Mean Square Error (MSE) merupakan suatu metode pengukuran kontrol dan kualitas yang sudah dapat diterima luas (Wikipedia, 2009). MSE dihitung dari sebuah contoh obyek yang kemudian dibandingkan dengan obyek aslinya sehingga dapat diketahui tingkat ketidaksesuaian antara obyek contoh dengan aslinya. Persamaan MSE terhadap deviasi dari target adalah sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{x=1}^{m}\sum_{y=1}^{n}[I(x,y) - I'(x,y)]^2 \quad (11)$$

I(*x*,*y*) adalah nilai piksel di citra asli, I'(*x*,*y*) adalah nilai piksel pada citra hasil modofikasi, dalam hal ini adalah citra ter-*watermark* dan x, y adalah dimensi citra.

3. PENGUJIAN DAN PEMBAHASAN

Pada bagian ini akan dibahas bagaimana sistem program akan berinteraksi dengan pengguna mulai dari memasukkan input data sampai menghasilkan keluaran. Pembahasan mengenai sistem program meliputi langkah-langkah penyelesaian teknik pelekatan *watermark*, langkah-langkah teknik ekstraksi *watermark*, langkah-langkah citra ter-*watermark* reduksi *grayscale* dan langkah-langkah pengujian hasil menggunakan MSE dan koefisien korelasi.

Program *watermarking* pada citra dijital menggunakan metode kuantisasi warna merupakan program utama dalam program ini. Fungsi utamanya adalah membuat chipterteks pada citra *watermark* dan membuat citra ter-*watermark* yang digunakan dalam proses ekstraksi. Proses pelaksanaan sistem dalam program ini ditunjukkan oleh Gambar-7 dan penjelasannya adalah sebagai berikut:

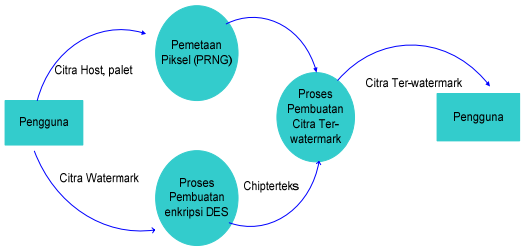
Ketika program dimulai, pengguna mendapat pilihan untuk memasukkan citra masukan langsung dari file citra yang sudah ada. Untuk citra *host* pengguna dapat memilih citra RGB atau *grayscale* berukuran *N* x *N*. Sedangkan untuk *signature* pengguna dapat memilih file citra biner berukuran *M* x *M* yang telah disediakan dengan catatan *M* merupakan faktor yang dapat membagi habis *N* dan ukuran piksel *M* harus lebih kecil dari ukuran piksel *N*.

Program pembuatan enkripsi DES pada citra biner, pengguna mengisi *window image* yang diinginkan. Setelah Enkripsi, sistem akan membuat enkripsi DES dan pengguna dapat menyimpan enkripsi citra *watermark* yang dihasilkan ke folder yang telah dipilih untuk selanjutnya digunakan dalam proses pembuatan citra ter-*watermark*.

Program pembuatan *pseudo random number generator* pada citra *watermark* dan citra *host*, sistem akan membuat *pseudo random number generator* dengan bilangan awal (*seed*) yang telah ditentukan, untuk melakukan pemetaan piksel pada citra *watermark* ke citra *host.*

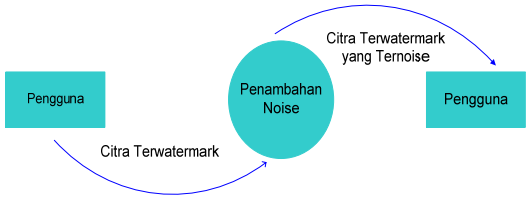
Program pembuatan *watermark*, pengguna diharuskan untuk mengisi *window image* yang diinginkan. Setelah itu proses *watermarking*, sistem akan membuat *watermark* dan

pengguna dapat menyimpan *watermark* yang dihasilkan ke folder yang telah dipilih untuk selanjutnya digunakan dalam proses pembuatan citra ter-*watermark*.



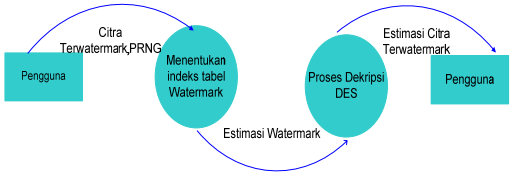
Gambar-7 Diagram alir data proses pelekatan *watermark*

Pada proses ini dilakukan penambahan level *noise* pada citra ter-*watermark* dari level 1% sampai 3% atau 5%. Gambaran proses diagram alir data dapat dilihat pada Gambar-8 berikut:



Gambar-8 Diagram alir data proses penambahan *noise*

Pada proses ini akan dilakukan ekstraksi *signature* dengan menggunakan metode kuantisasi warna. Berikut adalah diagram alir data yang ditunjukkan pada Gambar-9 berikut:



Gambar-9 Diagram alir data proses ekstraksi citra *watermark*

Pada uji coba program akan digunakan citra *host* LenaGREY.jpg dan LenaRGB.jpg, berukuran 512 x 512 piksel. Sedangkan *watermark* akan menggunakan watermark1.jpg dan watermark2.jpg citra biner berupa logo ITS dan tulisan ITS, berukuran 128 x 128 dan 64 x 64 piksel.

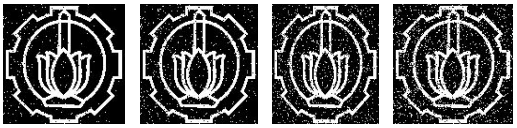
(a)LenaGREY.jgp (b)LenaRGB.jpg

(c)Watermark1.jpg (d)Watermark2.jpg

Gambar-10 Bagian (a) dan (b) **c**itra *host* (asal) dan bagian (c) dan (d) citra watermark

Hasil uji coba secara kasat mata (*visual*) citra ter-*watermark* dan citra asli sulit dibedakan. Selanjutnya akan dibahas hasil numerik dari kualitas citra *watermark* dengan estimasi *watermark* koefisien korelasi.

(a) (b)



(c) (d) (e) (f)

Gambar-11. Masukan dan hasil uji coba pertama

• Masukan citra *host* LenaGREY.jpg dengan watermark citra Watermark1.jpg

Nilai koefisien korelasi pada citra ter-*watermark* dengan Citra *host* LenaGREY.jpg dengan watermark1.jpg. Hasil percobaan pada Tabel-1.

Tabel-1 Nilai koefisien korelasi pada citra ter-*watermark*

No	Jenis Citra Ter-*watermark*	$\lvert\gamma_{x,y}\rvert$
1.	Tanpa Penambahan *noise*	0.957995
2.	Penambahan *noise* Level 1%	0.919936
3.	Penambahan *noise* Level 3%	0.856499
4.	Penambahan *noise* Level 5%	0.817334

(a) (b)

(c) (d) (e) (f)

Gambar-12 Masukan dan hasil uji coba kedua

- Masukan citra *host* LenaGREY.jpg dengan watermark citra watermark2.jpg

Nilai koefisien korelasi pada citra ter-*watermark* dengan Citra *host* LenaGREY.jpg dengan watermark2.jpg. Dapat dilihat pada Tabel-2.

Tabel-2 Nilai koefisien korelasi pada citra ter-*watermark*

No	Jenis Citra Ter-*watermark*	$\lvert r_{x,y} \rvert$
1.	Tanpa Penambahan *noise*	0.990564
2.	Penambahan *noise* Level 1%	0.968386
3.	Penambahan *noise* Level 3%	0.918815
4.	Penambahan *noise* Level 5%	0.856557

(a) (b)

(c) (d) (e) (f)

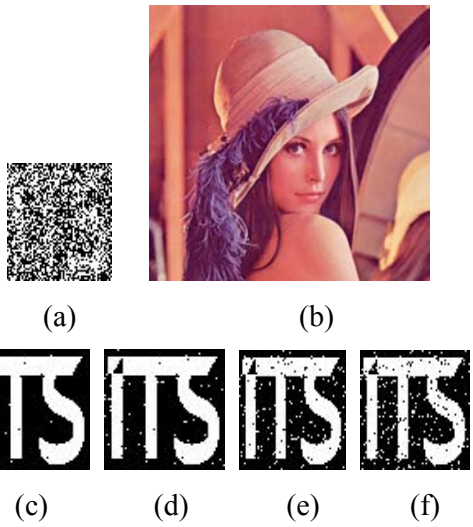
Gambar-13 Masukan dan hasil uji coba ketiga

- Masukan citra *host* LenaRGB.jpg dengan watermark citra watermark1.jpg

Nilai koefisien korelasi pada citra ter-*watermark* dengan Citra *host* LenaRGB.jpg dengan watermark1.jpg. Dapat dilihat pada Tabel-3.

Tabel-3 Nilai koefisien korelasi pada citra ter-*watermark*

No	Jenis Citra Ter-*watermark*	$\lvert r_{X,Y} \rvert$
1.	Tanpa Penambahan *noise*	0.957995
2.	Penambahan *noise* Level 1%	0.926711
3.	Penambahan *noise* Level 3%	0.867904
4.	Penambahan *noise* Level 5%	0.819244



(a) (b)

(c) (d) (e) (f)

Gambar-14 Masukan dan hasil uji coba keempat

- Masukan citra *host* LenaRGB.jpg dengan watermark citra watermark2.jpg

Nilai koefisien korelasi pada citra ter-*watermark* dengan Citra *host* LenaRGB.jpg dengan watermark2.jpg. Hasil percobaan pada Tabel-4.

Tabel-4 Nilai koefisien korelasi pada citra ter-*watermark*

No	Jenis Citra Ter-*watermark*	$\lvert r_{X,Y} \rvert$

1.	Tanpa Penambahan *noise*	0.990564
2.	Penambahan *noise* Level 1%	0.970712
3.	Penambahan *noise* Level 3%	0.918495
4.	Penambahan *noise* Level 5%	0.882817

Pada Gambar-11, 12, 13 dan 14, (a) menyatakan citra *watermark*, (b) citra ter-*watermark*, (c) hasil estimasi citra *watermark* tanpa penambahan *noise*, (d) hasil estimasi *watermark* level 1% penambahan *noise*, (e) hasil estimasi *watermark* level 3% penambahan *noise*, (f) hasil estimasi *watermark* level 5% penambahan *noise*.

Jika melihat nilai koefisien korelasi masing-masing percobaan, dapat kita simpulkan beberapa hal, yaitu :

1. Citra ter-*watermark* dapat diekstraksi dengan baik baik dengan dan tanpa gangguan berupa penambahan *noise*. Meskipun pada beberapa level penambahan *noise* hasil estimasi citra watermark memiliki koefisien korelasi yang relatif kecil.
2. Berdasarkan data yang ada pada Tabel- 1, 2, 3 dan 4 dengan citra *host* yang sama, *watermark* yang berbeda koefisien korelasi mengalami perbedaan yang signifikan. Terlihat bahwa watermark2.jpg memiliki koefisien korelasi yang lebih baik dari watermark1.jpg. Hal ini dikarenakan, kerumitan citra watermark2.jpg yang lebih sederhana, serta ukurannya yang lebih kecil.
3. Dengan menggunakan citra *host* yang berbeda, nilai dari koefisien korelasi juga mengalami perbedaan. Masukan citra *host* LenaRGB.jpg memiliki koefisien korelasi yang lebih baik dibanding LenaGREY.jpg.

4. SIMPULAN DAN SARAN

4.1. Simpulan

Dari hasil pengujian program dapat ditarik beberapa simpulan sebagai berikut:

1. Program *watermarking* menggunakan metode kuantisasi warna dapat meng-ekstraksi citra *watermark* dengan baik tanpa melibatkan citra asli.
2. *Watermark* yang tertanam dalam citra ter-watermark bersifat tak kelihatan dan tahan terhadap gangguan berupa penam-bahan *noise* dengan level 1%, level 3% dan level 5%.

3. Semakin besar ukuran citra *watermark* yang digunakan maka semakin besar pula penurunan kualitas citra ter-*watermark* yang dihasilkan.
4. Semakin rumit citra *watermark* yang ditanamkan semakin rendah pula kualitas citra estimasi *watermark* yang dihasil-kan.

4.2 Saran

Saran yang dapat diberikan dalam peneli-tian ini antara lain adalah:

1. Citra *watermark* yang menjadi input dalam program ini adalah citra biner dan diharapkan dalam penelitian selanjutnya dapat menggunakan citra *grayscale.*
2. Citra *host* dan *watermark* dalam program ini menggunakan format bertipe .jpg, diharap-kan dalam penelitian selanjutnya dapat menggunakan format bertipe .bmp, .gif, .png.
3. Untuk keamanan citra *watermark* dalam program ini menggunakan DES, diharapkan dalam penelitian selanjutnya dapat menggunakan *double* DES atau *triple* DES.
4. Algoritma yang digunakan pada penelitian ini adalah *Squared Euclidean Distance* (SED), dalam penelitian selanjutnya mungkin dapat dicoba algoritma yang lain.
5. Sebagai pengembangan program, dapat dibuat program *watermarking* pada data dijital lainnya misalkan teks, suara, video dan sebagainya.

5. DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2006. **Kriptografi**. PT. Informatika, Bandung.

[2] Murtiyasa, Budi. 2009. **Analisis Keamanan Kriptosistem Kunci Publik Berdasarkan Matriks Invers Tergeneralisasi**. Tugas Akhir FKIP Universitas Muhammadiyah Surakarta, Surakarta.

[3] Pranindya, Yunita. 2010. **Pemberian Tanda Air Pada Citra Dijital Menggunakan Metode Tanda Air Dengan Analisis Komponen Bebas *Transpose* Citra.** . Tugas Akhir Jurusan Matematika Institut Teknologi Sepuluh Nopember, Surabaya.

[4] Prayudi, Yudi. 2002. **Metode Watermarking Ganda Sebagai Teknik Pengamanan Citra Dijital**. Thesis Jurusan Teknik Informatika Institut Teknologi Sepuluh Nopember, Surabaya.

[5] Sirait, Rummi 2006. **Teknologi Watermaking Pada Citra Dijital**.From http://jurnal.bl.ac.id, 18 Oktober 2010.

[6] Tsai, Piyu & Hu, Yu-Chen. 2002. ***A Color Image Watermarking Scheme Based On Color Quantization***. Taiwan journal of Signal Processing (2004) hal. 95-106.

[7] MatWorks, The Math. ***Image Processing Toolbox For Use with MATLAB.*** The Math Works Inc, 1994-2010.

[8] Wikipedia. 2011. **Euclidean Distance**. < http://en.wikipedia.org/wiki/Euclidean_distance >. Di unduh pada tanggal 21 Desember 2010 jam 19.25 WIB.

[9] Wikipedia. 2011. **Web Colors** . < http://en.wikipedia.org/wiki/Web_colors >. Di unduh pada tanggal 22 maret 2011 jam 07.15 WIB.

[10] Wikipedia. 2011. Palette Computing . < http://en.wikipedia.org/wiki/Palette_%28computing%29 >. Di unduh pada tanggal 13 januari 07.30 WIB.