Sekilas *Image Watermarking* untuk Memproteksi Citra Digital dan Aplikasinya pada Citra Medis

Oleh: Rinaldi Munir
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
E-mail: rinaldi@informatika.org

Abstrak

Image watermarking merupakan solusi untuk melindungi citra digital dari masalah seperti perlindungan *copyright*, kepemilikan, otentikasi, *fingerprinting*, dan sebagainya. *Watermark* dapat disisipkan ke dalam citra dalam dua domain: domain spasial atau domain *transform*. Makalah ini membahas dua metode *image watermarking* untuk kedua *domain* tersebut. Studi *image watermarking* untuk citra medis ditinjau untuk mengenalkan aplikasinya di bidang kedokteran.

Kata kunci: *image watermarking*, domain spasial, domain *transform*, citra medis.

1. Pendahuluan

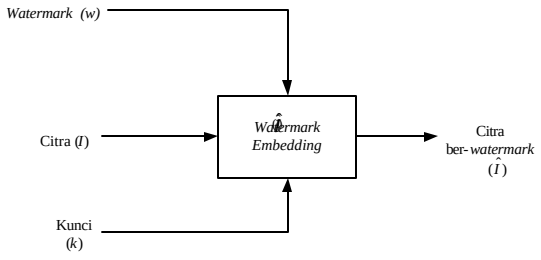
Saat ini kebanyakan data dan informasi disajikan dalam bentuk format digital, baik berupa teks, citra, audio, maupun video. Citra digital, sebagaimana produk digital lainnya, mempunyai beberapa karakteristik, antara lain: (1) Penggandaan (*copy*) terhadap data digital juga mudah dilakukan dan hasilnya tepat sama dengan aslinya; (2) Mudah didistribusikan melalui *magnetic disk* maupun internet. Penyebaran data digital meningkat secara luar biasa seiring dengan perkembangan teknologi internet; (3) Perubahan yang sedikit pada citra tidak mudah dipersepsi oleh indera penglihatan.

Masalah muncul jika citra digital tersebut merupakan karya yang perlu dilindungi, misalnya citra hasil seni fotografi, citra hasil penginderaan jauh, citra medis, dan sebagainya. Contoh-contoh masalah yang muncul misalnya masalah kepemilikan (*ownership*), pelanggaran *copyright*, dan masalah keaslian. Permasalahan semacam di atas dapat diatasi dengan menggunakan *digital watermarking*. *Digital watermarking* adalah teknik untuk menyisipkan informasi tertentu ke dalam data digital yang disebut *watermark*. *Watermark* dapat berupa teks seperti informasi *copyright*, gambar berupa logo, data audio, atau rangkaian bit yang tidak makna. Penyisipan *watermark* dilakukan sedemikian rupa sehingga *watermark* tidak merusak data digital yang dilindungi. Selain itu *watermark* yang telah disisipkan tidak dapat dipersepsi oleh indra manusia, namun ia dapat dideteksi oleh komputer dengan menggunakan kunci yang benar. *Watermark* yang telah disisipkan tidak dapat dihapus dari dalam data digital, sehingga bila data digital ber-*watermark* disebar dan digandakan, maka otamatis *watermark* di dalamnya ikut terbawa. *Watermark* di dalam data digital dapat dideteksi atau diekstraksi kembali. *Watermarking* berguna untuk membuktikan kepemilikan, copyright protection, otentikasi, fingerprinting tamper profing, distribution tracing, dan sebagainya.

Watermarking dapat diterapkan baik pada data digital berupa teks, citra, audio, maupun video. Makalah ini hanya membahas *watermarking* pada citra digital (*image watermarking*).

2. Sekilas Mengenai *Digital Watermarking*

Teknik *watermarking* pada citra secara umum terdiri dari 2 tahapan: 1) penyisipan *watermark* (*watermark embedding*), dan 2) ekstraksi atau pendeteksian *watermark* (*watermark detection*). Penyisipan *watermark* dapat dipandang sebagai superposisi data *watermark* pada citra dengan suatu cara sedemikian sehingga superposisi tersebut tidak mempengaruhi persepsi visual terhadap citra. Gambar 1 memperlihatkan sebuah *encoder* yang melakukan penyisipan *watermark*. *Encoder E* menerima masukan berupa citra *I*, *watermark w*, kunci penyisipan *k*, dan menghasilkan citra ber-*watermark*, $\hat{I}$.

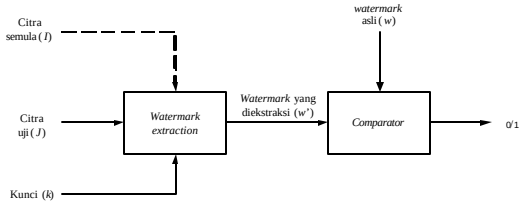


Gambar 1 Proses penyisipan *watermark*

Citra asal I dan citra ber-*watermark* $\hat{I}$ hampir mirip secara statisik, atau secara visual mempunyai persepsi yang sama. Secara matematis, penyisipan *watermark* ditulis sebagai

$$E_k(I, w) = \hat{I} \quad (1)$$

Watermark harus dapat diekstraksi atau dideteksi kembali bergantung pada *nature* algoritma *watermarking*. Pada beberapa algoritma *watermarking*, *watermark* dapat diekstraksi dalam bentuk yang eksak, sedangkan pada sebagian algoritma yang lain, kita hanya dapat mendeteksi apakah *watermark* terdapat di dalam citra, sehingga prosedurnya dinamakan pendeteksian *watermark* [20].



Gambar 2 Proses ekstraksi/verifikasi *watermark*

Gambar 2 memperlihatkan prosedur untuk melakukan ekstraksi dan selanjutnya verifikasi *watermark*. Prosedur terdiri dari sebuah *decoder* untuk mengekstraksi *watermark* dan komparator untuk melakukan pembandingan. *Decoder D* menerima masukan berupa citra J (J bisa berupa citra ber-*watermark* $\hat{I}$ atau citra tanpa *watermark*, bahkan mungkin citra yang sudah mengalami distorsi. Jika tidak ada distorsi, $J = \hat{I}$), kunci k, dan menghasilkan *watermark* terekstraksi *w*'. Secara matematis proses ini ditulis sebagai

$$D_k(J) = w' \quad (2)$$

Decoder dapat mengikutsertakan citra asal yang belum diberi *watermark* (*non-blind watermarking*) atau tidak sama sekali (*blind watermarking*), karena beberapa skema *watermarking* memang menggunakan citra asal dalam proses ini untuk meningkatkan hasil ekstraksi yang lebih baik. Selanjutnya, *watermark* terekstraksi *w*' dibandingkan dengan *watermark* asli *w* dengan fungsi komparator *C* (umumnya sebuah *correlator*) untuk menghasilkan keputusan berupa keluaran biner (1 menyatakan cocok, 0 menyatakan sebaliknya):

$$C_t(w, w') = \begin{cases} 1, & c \le t \\ 0, & c > t \end{cases} \quad (3)$$

yang dalam hal ini, t adalah nilai ambang, dan $c = C_t(w, w')$ adalah nilai korelasi antara dua buah sinyal *watermark*.

Sebuah teknik *watermarking* yang bagus harus memenuhi persyaratan berikut [4]:

1) *Imperceptibility*: keberadaan *watermark* tidak dapat dipersepsi oleh indera visual. Hal ini bertujuan untuk menghindari gangguan pengamatan visual.
2) *Key uniqueness*: kunci yang berbeda seharusnya menghasilkan *watermark* yang berbeda. Ini berarti penggunaan kunci yang salah dapat menyebabkan hasil ekstraksi/deteksi *watermark* yang salah pula.
3) *Noninvertibility*: secara komputasi sangat sukar menemukan *watermark* bila diketahui hanya citra ber-*watermark* saja.
4) *Image dependency*: satu kunci menghasilkan sebuah *watermark* tunggal, tetapi *watermark* bergantung pada isi citra. Salah satu pendekatan yang digunakan adalah membangkitkan *watermark* dari nilai *hash* (*message digest*) citra asli, sebab nilai *hash* bergantung pada isi citra.
5) *Robustness*: *watermark* seharusnya tetap kokoh terhadap berbagai serangan yang dilakukan pada citra ber-*watermark*. Ini berarti manipulasi yang dilakukan terhadap citra ber-*watermark* tidak merusak *watermark* (*watermark* masih dapat dideteksi). Manipulasi citra meliputi operasi seperti penambahan derau aditif (Gaussian atau non-Gaussian), kompresi (seperti *JPEG*), transformasi geometri (seperti rotasi, perbesaran, perkecilan), penapisan (baik penapisan lanjar maupun nirlanjar, konversi digital-ke-analog (*D*/*A*) atau *A*/*D*, seperti pemindaian citra

Gambar 3 (lihat lampiran) memperlihatkan contoh *watermarking*. Gambar 3(a) adalah citra asli yang belum diberi *watermark*. Gambar 3(b) adalah citra yang sudah disisipkan *watermark*, *watermark*-nya adalah gambar logo *Hewlett-Packard* (*Hp*) seperti pada Gambar 3(c) Perhatikan bahwa citra ber-*watermark* hampir tidak dapat dibedakan dengan citra aslinya. Jika kita mengekstraksi *watermark* dengan kunci yang benar, maka hasilnya adalah *watermark* yang sama dengan Gambar 3(c). Dengan membandingkan *watermark* terekstraksi dengan *watermark* yang asli, pemilik citra dapat membutikan bahwa citra ber-*watermark* adalah miliknya. Sebaliknya, jika kunci yang dimasukkan salah, maka hasil ekstraksinya

adalah gambar yang berisi pola-pola acak seperti pada Gambar 3(d).

Gambar 3(d) memperlihatkan citra ber-*watermark* yang sudah dimanipulasi dengan menambahkan sedikit derau berupa bintik-bintik putih di dekat kepala (bagian atas). Jika kita mengekstraksi *watermark* dengan menggunakan kunci yang benar terhadap citra ini, maka hasilnya adalah gambar logo seperti pada Gambar 3(e). Gambar logo ini mengalami distorsi pada bagian atas, namun *watermark* ini masih dapat dikenali mendekati aslinya. Kerusakan pada *watermark* digunakan untuk membuktikan bahwa citra ber-*watermark* sudah mengalami manipulasi (*tamper proofing*).

3. Jenis-jenis *Image Watermarking*

Image watermarking dapat dibedakan menjadi beberapa kategori [2]:

(a) Berdasarkan persepsi manusia, *image watermarking* dibedakan menjadi *visible watermarking* dan *invisible watermarking*. *Watermarking* tak-tampak (*invisible*) sudah ditunjukkan pada Gambar 3 dimana *watermark* tidak dapat dipersepsi oleh indera visual. *Watermarking* tak-tampak ini dimungkinkan karena sistem visual manusia yang tidak dapat mendeteksi perubahan kecil pada citra. Selain itu, sebuah citra mengandung banyak redundansi yang dapat dimanfaatkan untuk menyisipkan *watermark*.

(b) Berdasarkan tingkat kokokohan *watermark*, *image watermarking* dibedakan menjadi *secure watermarking*, *robust watermarking*, dan *fragile watermarking* [2]. *Secure watermarking* berarti *watermark* harus tetap bertahan terhadap *non-malicious attack* dan *malicious attack*. Suatu serangan digolongkan sebagai *non malicious attack* yaitu manipulasi yang normal terjadi selama penggunaan citra ber-*watermark*, misalnya kompresi, operasi penapisan, penambahan derau, penskalaan, penyuntingan, operasi geometri, dan *cropping*. Serangan tersebut dapat merusak atau menghancurkan *watermark* di dalam data digital. Jika akibat serangan tersebut *watermark* masih dapat diekstraksi, maka skema *watermarking* yang digunakan dikatakan kokoh (*robust*). Serangan digolongkan sebagai *malicious attack*, yaitu serangan yang tujuan utamanya adalah menghilangkan atau membuat *watermark* tidak dapat dideteksi. Dalam membahas *malicious attack*, penyerang diasumsikan mengetahui algoritma *watermarking*. Aplikasi *secure watermarking* misalnya untuk perlindungan *copyright*, karena *watermark* tidak boleh hancur atau dihapus dari citra. *Robust watermarking* berarti *watermark* harus tetap bertahan terhadap *non-malicious attack*. Pada *fragile watermarking*, *watermark* dikatakan mudah rusak (*fragile*) jika ia berubah, rusak, atau malah hilang jika citra dimodifikasi. *Fragile watermarking* ditujukan pada aplikasi yang tujuannya untuk memverifikasi isi (*content*) citra, misalnya untuk otentikasi data dan bukti kepemilikan (*ownership*) citra, dimana *watermark* yang hilang atau berubah adalah pertanda bahwa citra sudah dirusak (*tamper*), dan verifikasi *watermark* di dalam citra dapat digunakan untuk menunjukkan kepemilikan citra.

4. Aplikasi *Image Watermarking*

Image watermarking mempunyai banyak penggunaan dalam kehiduan sehari-hari, di bawah ini disebutkan beberapa diantaranya:

a. Memberi label kepemilikan (*ownership*) atau *copyright* pada citra digital.
Watermark menyatakan informasi yang menyatakan pemilik citra atau pemegang hak penggandaan (*copyright*). Informasi tersebut bisa berupa identitas diri (nama, alamat, dsb), atau gambar yang menspesifikasikan pemilik. Klaim pihak lain yang mengaku sebagai pemilik citra tersebut dapat dibantah dengan membandingkan *watermark* yang diekstrak dengan *watermark* pemilik citra. Persyaratan yang dibutuhkan untuk aplikasi semacam ini adalah *watermark* harus tak-tampak (*invisible*) dan kokoh (*robust*).

b. Otentikasi atau *tamper proofing*.
Pemilik citra menyisipkan *watermark* ke dalam citra untuk membuktikan apakah citra yang disimpan atau yang beredar masih asli atau sudah berubah (*tamper proofing*). Jika *watermark* yang diekstraksi tidak tepat sama dengan *watermark* asli, maka disimpulkan citra sudah tidak otentik lagi (lihat contoh Gambar 3(f)). Keotentikan pemilik juga dapat ditunjukkan karena hanya pemilik yang mengetahui kunci. Kunci yang salah akan menghasilkan ektraksi *watermark* yang salah pula, seperti contoh pada Gambar 3(d).

Persyaratan yang dibutuhkan untuk aplikasi semacam ini adalah *watermark* harus tak-tampak dan *fragile*.

c. *Fingerprinting* (*traitor-tracing*)
Pemilik citra mendistribusikan citra yang sama ke berbagai distributor. Sebelum didistribusikan, setiap citra disisipkan *watermark* yang berbeda untuk setiap distributor, seolah-olah cetak jari distributor terekam di dalam citra. Karena *watermark* juga berlaku sebagai *copyright*, maka distributor terikat aturan bahwa ia tidak boleh menggandakan citra tersebut dan menjualnya ke pihak lain. Misalkan pemilik citra menemukan citra ber-*watermark* tersebut beredar secara ilegal di tangan pihak lain. Ia kemudian mengekstraksi *watermark* di dalam citra ilegal itu untuk mengetahui distibutor mana yang telah melakukan penggandaan ilegal, selanjutnya ia dapat menuntut secara hukum distributor nakal ini. Persyaratan yang dibutuhkan untuk aplikasi semacam ini adalah *watermark* harus tak-tampak (*invisible*) dan kokoh (*robust*).

d. Aplikasi medis
Citra medis seperti foto sinar-X diberi *watermark* berupa *ID* pasien dengan maksud untuk memudahkan identifikasi pasien. Informasi lain yang dapat disisipkan adalah hasil diagnosis penyakit. Lebih lanjut mengenai aplikasi ini akan dijelaskan pada bagian tersendiri sebagai studi kasus. Persyaratan yang dibutuhkan untuk aplikasi semacam ini adalah *watermark* harus tak-tampak (*invisible*) dan *fragile*.

e. *Covert communication*
Untuk sistem komunikasi di negara-negara di mana kriptografi tidak dibolehkan, *watermarking* dapat digunakan untuk menyisipkan informasi rahasia. Informasi tersebut disisipkan ke dalam citra, citra dikirim melalui saluran komunikasi publik, dan penerima mengekstraksi informasi di dalamnya. Aplikasi semacam ini sama seperti steganografi [4].

f. *Piracy protection*
Watermark di dalam citra digunakan untuk mencegah perangkat keras melakukan penggandaan yang tidak berizin. Aplikasi semacam ini membutuhkan kolaborasi dengan perangkat keras [4].

5. Metode *Image Watermarking*

Penyisipan *watermark* dapat dilakukan dalam dua ranah, yaitu ranah spasial dan ranah *transform*. Keduanya melahirkan dua macam metode *watermarking*, waitu metode spasial dan metode *transform*. Penyisipan dalam *domain* spasial berarti menyisipkan *watermark* secara langsung ke dalam *pixel* citra. Keuntungan cara ini adalah murah (cepat) tetapi umumnya *watermark* tidak kokoh terhadap manipulasi pada citra.

Kekokohan *watermark* dapat diperoleh jika penyisipan *watermark* dilakukan dalam ranah *transform*, artinya *watermark* disisipkan ke dalam koefisien transformasi. Umumnya yang menjadi ranah *transform* adalah ranah frekuensi dan transformasi yang digunakan misalnya *DFT* (*Discrete Fourier Transform*), *DCT* (*Discrete Cosine Transform*), dan *DWT* (*Discrete Wavelet Transform*). Kekokohan terhadap manipulasi *cropping* dapat diperoleh jika *watermark* disebar (*spread*) di antara seluruh komponen frekuensi. Kekokohan terhadap operasi geometri (seperti penskalaan, rotasi, atau pergeseran) dapat diperoleh dalam ranah *tranform* karena ranah transform dapat dirancang sedemikians ehingga invariant terhadap sekumpulan transformasi tertentu. Misalnya, teknik yang menggunakan tranformasi *DFT* kokoh terhadap operasi pergseran karena pergeseran dalam ranah spasial tidak mempunyai pengaruh terhadap magnitodo *DFT*.

Di bawah ini dijelaskan secara ringkas dua buah metode *watermarking* dalam ranah spasial dan sebuah metode dalam ranah *transform*.

5.1 Metode LSB

Metode *LSB* (*Least Significant Bit*) merupakan metode *watermarking* dalam ranah spasial yang paling sederhana. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*most significant bit* atau *MSB*) dan bit yang paling kurang berarti (*least significant bit* atau *LSB*). Dengan menggunakan metode ini, *LSB* dari citra diganti dengan bit data *watermark*. Sebagai ilustrasi, di bawah ini dijelaskan metode modifikasi *LSB* untuk menyisipkan *watermark* pada citra (gambar) digital.

Misalkan segmen *pixel-pixel* citra sebelum penambahan bit-bit *watermark* adalah

00110011 10100010 11100010 01101111

Misalkan sebagian *watermark* (yang telah dikonversi ke sistem biner) adalah 0111. Setiap bit dari *watermark* menggantikan posisi *LSB* dari segmen data citra menjadi:

00110010 10100011 11100011 01101111

Misalkan susunan *byte* tersebut di dalam gambar menyatakan warna tertentu, maka perubahan satu bit *LSB* tidak mengubah warna tersebut secara berarti. Lagi pula, dan ini keuntungan yang dimanfaatkan, mata manusia tidak dapat membedakan perubahan yang kecil.

Untuk memperkuat penyisipan data, bit-bit *watermark* tidak digunakan untuk mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka *byte* yang diganti bit *LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49. Pembangkit bilangan acak dapat digunakan untuk menentukan lokasi penyisipan. Nilai awal atau umpan (*seed*) yang digunakan untuk membangkitkan bilangan acak berlaku sebagai kunci penyisipan *watermark*. Pada proses ekstraksi *watermark*, kunci yang sama digunakan kembali untuk membangkitkan bilangan acak yang sama seperti pada saat penyisipan.

Sayangnya, metode *LSB* tidak kokoh terhadap perubahan yang dilakukan pada citra ber-*watermark*. Jika citra ber-*watermark* dimodifikasi, maka bit *LSB* citra juga berubah, akibatnya watermark yang diesktraksi juga rusak. Selain itu, metode *LSB* tidak aman, karena diketahui dimana watermark disisipkan pada bit *LSB*, maka *wartermark* mudah dihilangkan dengan cara mengganti semua bit *LSB* dengan nilai kebalikan (0 menajdi 1 atau 1 menjadi 0). Oleh karena itu, metode ini tidak cocok digunakan untuk aplikasi *robust watermarking*, namun cocok untuk aplikasi *fragile watermarking*.

5.2 Metode Bender-Nikolaidis-Pitas

Bender, Nikolaidis, dan Ioanis Pitas [5] mengusulkan metode *watermarking* dengan cara membagi *pixel-pixel* citra menjadi dua himpunan, *A* dan *B*. Pembagian ini didasarkan pada pengamatan bahwa pada kebanyakan citra, $\sum_A pixel - \sum_B pixel \approx 0$.

Penyisipan *watermark* dilakukan dengan memilih nilai *k* yang cukup kecil. Setiap nilai *pixel* di dalam himpunan *A* ditambah dengan *k*, sedangkan setiap nilai *pixel* di dalam himpunan *B* dikurangi dengan *k*. Gabungan *pixel-pixel* di himpunan *A* dengan *pixel-pixel* di himpunan *B* menghasilkan citra ber-*watermark*.

Pendeteksian *watermark* dilakukan dengan mula-mula membagi citra menjadi himpuna *A* dan *B*, lalu menghitung $x = \sum_A pixel - \sum_B pixel$. Jika niali *x* dekat ke nol, maka disimpulkan *watermark* tidak ada di dalam citra, tetapi jika *x* dekat ke nilai $N*k$, maka disimpukkan *watermark* ada.

5.3 Metode *Spread Spectrum Watermarking*

Metode *spread spectrum watermarking* melakukan penyisipan dan pendeteksian *watermark* dalam ranah *tranform*. Mula-mula citra ditransformasikan kedalam ranah frekuensi, lalu bit *watermark* disisipkan pada koefisein transformasi (misalnya koefisien *DCT*, *FFT*, *DWT*). Istilah "*spread spectrum*" muncul karena penyisipan *watermark* ke dalam citra menggunakan teknik yang analog dengan komunikasi *spread spectrum*, yaitu *watermark* disebar (*spread*) di antara banyak komponen frekuensi. Secara umum, *spread sepctrum watermarking*, sebagaimana metode wateramrking lain dalam ranah transform, menghasilkan metode yang lebih kokoh terhadap serangan seperti kompresi, *cropping*, dan penapisan lolos-rendah.

Cox [2, 6] mengusulkan teknik *watermarking* yang kokoh dengan pendekatan *spread spectrum*. *Watermark w* adalah rangkaian nilai yang mempunyai distribusi normal atau Gaussian, $N(0, \sigma^2)$, yang dalam hal ini distribusi normal mempunyai rerata 0 dan variansi σ^2. Rumus distribusi normal:

$$p(w) = \frac{1}{\sqrt{2ps^2}} \exp\left(-\frac{w^2}{2s^2}\right) \qquad (4)$$

Watermark berdistribusi Gaussian dipilih karena ia lebih kokoh terhadap perubahan dibandingkan dengan menggunakan distribusi *uniform*. *Watermark* juga berlaku sebagai kunci, karena hanya pemilik citra yang mengetahui *watermark* ini. *Watermark* harus disisipkan di dalam komponen sinyal yang signifikan secara persepsi (*perceptually significant region*), meskipun perubahan pada komponen ini dapat menyebabkan kerusakan yang tampak pada citra.

Skema penyisipan *watermark* adalah sebagai berikut:

1. Citra asli dianggap sebagai sebuah blok, lalu ditansformasi ke dalam ranah frekuensi dengan menggunakan *DCT*. Tranformasi citra $I(i, k)$ yang berukuran $N \times N$ dihitung dengan menggunakan rumus:

$$C(u,v) = C(u)c(v)\frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j)\cos\left(\frac{p}{N}u(i+\frac{1}{2})\right)\cos\left(\frac{p}{N}v(j+\frac{1}{2})\right) \quad (5)$$

dengan

$$\begin{cases} c(w) = 2^{-\frac{1}{2}} & w = 0 \\ c(w) = 1 & w > 0 \end{cases}$$

2. Temukan komponen sinyal yang signifikan secara persepsi. Cox menggunakan 1000 koefisien terbesar. Inilah yang dinamakan *frequency spreading*.
3. *Watermark* $W = w_1, w_2, \ldots, w_n$ dibangkitkan sedemikian sehingga w_i mempunyai distribusi $N(0, 1)$, yaitu distribusi normal dengan rerata 0 dan variansi 1.*Watermark* disisipkan ke dalam koefisien *DCT* dengan cara mengubah komponen frekuensi v_i dari citra asal menjadi $\hat{v}_i$ dengan menggunakan persamaan:

$$\hat{v}_i = v_i(1 + \alpha w_i) \quad (6)$$

yang dalam hal ini α adalah faktor skalar. Cox memilih $\alpha = 0.1$.

4. Lakukan transformasi *DCT* inversi terhadap hasil langkah 4 untuk menghasilkan citra ber-*watermark*. Persamaan *DCT* inversi adalah:

$$I(i,j) = \frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} c(u)c(v)C(u,v)\cos\left(\frac{p}{N}u(i+\frac{1}{2})\right)\cos\left(\frac{p}{N}v(j+\frac{1}{2})\right) \quad (7)$$

Skema ekstraksi *watermark* adalah sebagai berikut:

1. Citra ber-*watermark* dianggap sebagai sebuah blok, lalu ditansformasi ke dalam ranah frekuensi dengan menggunakan *DCT*.
2. Lakukan tranformasi *DCT* terhadap citra asli (yang belum diberi *watermark*).
3. Selisih langkah 1 dan 2 adalah *watermark* yang diekstraksi, *W** , dengan kata lain *W** diperoleh dengan menghitung w_i* kembali berdasarkan persamaan 6 menghasilkan persamaan berikut:

$$w_i^* = \frac{\frac{\hat{v}_i}{v_i} - 1}{a} \quad (8)$$

4. *Watermark* *W** dibandingkan dengan watermark asli W dengan menggunakan persamaan berikut:

$$sim(W, W^*) = \frac{W \cdot W^*}{\sqrt{W \cdot W^*}}$$

Untuk memutuskan apakah *W* dan *W** sama, digunakan nilai ambang *T*, yaitu keduanya sama jika $sim(W, W^*) > T$.

Metode Cox mempunyai kelemahan karena ekstraksi *watermark* membutuhkan citra asal yang belum diberi *watermark*. Meskipun demikian, *watermark* kokoh terhadap operasi penglahan citra yang umum seperti konversi analog-ke-digital dan digital-ke-analog, *dithering*, *resampling*, kompresi, rotasi, translasi, dan pensakalaan [2].

6. Aplikasi *Watermarking* pada Citra Medis

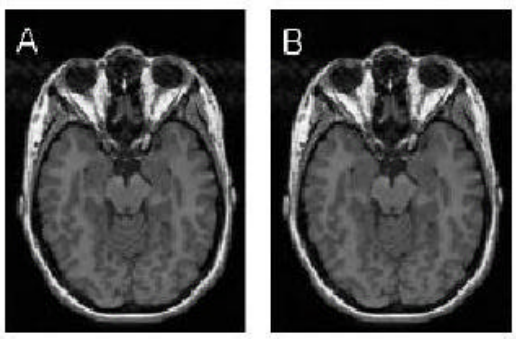
Citra medis (seperti citra sinar-X) disimpan untuk tiga tujuan [7], yaitu diagnosis, basis data, dan penyimpanan jangka panjang. *Watermarking* sudah digunakan pada citra medis untuk tujuan otentikasi, integritas citra dan perlindungan HAKI. Seseorang yang dapat mengakses citra medis mungkin melakukan modifikasi pada citra medis, oleh karena itu integritas citra harus dilindungi dengan menggunakan *watermark*, ini disebut *integrity watermark*. Ini berarti metode *fragile watermarking* dapat digunakan untuk tujuan ini. Selain itu, sistem basis data citra yang berbasis *web* mengandung sumberdaya citra medis yang berharga tidak hanya untuk riset tetapi juga untuk tujuan komersil, oleh karena itu *copyright* dan properti intelektual citra juga harus dilindungi dengan *watermark*, ini disebut *copyright watermark* [7]. Untuk kasus ini metode *robust watermarking* dapat digunakan.

Sejumlah studi sudah dilakukan pada *watermarking* untuk citra medis. Anand, seperti disebutkan di dalam [8], mengusulkan metode yang menyisipkan versi enkripsi EPR (*Electronic Patient Records*) ke dalam bit *LSB* dari *pixel-pixel* citra medis. Meskipun kerusakan pada kualitas citra minimal, fragilitas *LSB watermarking* ini dapat diketahui untuk memeriksa integritas citra. Zhou dkk, seperti disebutkan di dalam [9], mempresentasikan metode *watermarking* dengan cara yang mirip Anand untuk memverifikasi otentikasi dan integritas citra mammografi. Chao dkk, seperti disebutkan di dalam [9], mengusulkan metode yang berbasis *DCT* untuk menyembunyikan *EPR*.

Persyaratan umum *watermarking*, yaitu tidak dapat dipersepsi (*invisibility*), aman (tidak dapat diakses oleh orang yang tidak berhak), dan kokoh terhadap usaha untuk merusak atau menghilangkan *watermark* juga berlaku pada citra medis, tetapi ada persyaratan tambahan lain, yaitu *reversible*. Seperti diketahui, tradisi medis sangat ketat dengan kualitas citra biomedis, yaitu tidak dibolehkan mengubah bit di dalam citra karena dapat memepngaruhi diagnosis. Oleh karena itu, metode *watermarking* harus *reversible*, yaitu citra asal harus dapat dikembalikan lagi secara tepat [9]. Skema *reversible watermarking* terdiri dari penyisipan *watermark* ke dalam citra asal dan suatu cara sedemikian sehingga bila *watermark* diekstraksi, citra asal dapat diperoleh kembali. Riset mengenai *reversible watermarking* telah dilakukan. Misalnya, Trichili, seperti disebutkan di dalam [9] mengusulkan pinggir semu (*virtual border*) di dalam citra sebagai area *watermarking*. *EPR* disisipkan pada bit *LSB* pinggiran tersebut.

Beberapa metode *watermarking* pada citra medis menerapkan alternatif penyisipan pada bagian yang bukan termasuk ke dalam *region of interest* (*ROI*). *ROI* adalah bagian yang paling penting di dalam citra medis. Bagian ini harus dilindungi dari *watermark*. Bagian ini tidak boleh berubah oleh penyisipan, oleh karena itu bagian ini dibiarkan utuh, sementara penyisipan dilakukan pada bagian non-*ROI* (umumnya bagian latar belakang). Jadi, kita harus mendefinisikan mana bagian *ROI* dan mana bagian untuk penyisipan *watermark*.

Yongho Cho dkk di dalam [10] mengusulkan metode *watermarking* yang cocok untuk citra medis. Penyisipan *watermark* dapat dilakukan dalam ranah spasial dan dalam ranah frekuensi. Dalam ranah spasial, mula-mula tentukan bagian non-*ROI*, yaitu bagian latar belakang di dalam citra. Bagian latar belakang ini tidak berarti (*meaning-less*), sehingga kita mencegah kerusakan pada citra. Penyisipan *watermark* dilakukan dalam ranah spasial pada bagian ini. Caranya, hitung nilai *hash* bagian non-*ROI*, lalu nilai *hash* ditambahkan pada bagian non-*ROI*. Dalam ranah frekuensi, kita menyisipkan *watermark* satu dimensi *w* pada koefisien *DCT* citra tersebut. Penyisipan dan ekstraksi *watermark* dalam ranah frekuensi mirip dengan skema yang diusulkan oleh Cox (lihat upabab 5.3), bedanya citra asal dibagi ke dalam blok-blok yang berukuran 8 x 8, lalu koefisien *DCT* setiap blok dihitung, dan penyisipan *watermark* dihitung dengan rumus yang dikemukakan oleh Cox. *Watermark* berupa barisan bilangan riil yang mempunyai distribusi normal dengan $N(0, 1)$. Faktor skala α dipilih hati-hati sehingga tidak merusak citra. Gambar 4 memperlihatkan watermarking pada citra *MRI*. Gambar a adalah citar asli dan gambar b adalah citra yang diberi *watermark*.



Gambar 4 (A) citra asli, (B) citra ber-*watermark*

Referensi

1. Mauro Barni dan Franco Bartolini, *Watermarking Systems Engineering*, Marcel Dekker Publishing, 2004.
2. Saraju P. Mohanty, *Digital Watermarking: A Tutorial Review*, Dept. of Computer Scieence and Engineering, University of South Florida.
3. Athanasios Nikolaidis dan Ioannis Pitas, *Region-Based Image Watermarking*, IEEE Transaction on Image Processing, Vol. 10, No. 11, Novemebr 2001.
4. William Stalling, *Cryptography and Network Security, Principle and Practice 3rd Edition*, Pearson Education, Inc., 2003.
5. Doug Tygar, Watermarking.
6. Young K Hwang, *Secure Spread Spectrum Watermarking for Multimedia*.
7. Akiyoshi Wakatani, *Digital Watermarking for ROI Medical Images by Using Compressded Signature Image*, Proc. Of th 35th Annual Hawaii International Conference on System Science, 2002.
8. G. Coatrieux dkk, *Relevance of Watermarking in Medical Imaging*.
9. Jasni Zain, *Security in Telemedicine*: *Watermarking Medical Images*
10. Yongho Cho dkk, *A Study for Watermark Methods Apprpriate to Medical Image*

Lampiran

(a)

(b)

(c)

(d)

(e)

(f)

Gambar 3 Demo *watermarking*. Keterangan gambar: (a) Citra asli; (b) Citra ber-*watermark* (c) *watermark*; (d) *watermark* yang salah jika kunci untuk deteksi salah; (e) citra ber-*watermark* yang ditambahkan sedikit derau; (f) *watermark* yang diekstraksi dari gambar (e).
(Sumber: http://www.europe4drm.com)