Analisis dan Implementasi Watermark untuk Copyright Image Labelling

Muhammad Luthfi

Program Studi Teknik Informatika,
Sekolah Teknik Elektro Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung 40135

email: luthfi@comlabs.itb.ac.id

Abstrak

Digital watermarking merupakan suatu proses penyisipan data atau informasi tertentu yang sulit untuk dihilangkan. Tujuan penggunaan watermark biasanya adalah untuk menandai atau menjaga originalitas dari suatu data yang disisipkan watermark didalamnya. Perkembangan penelitian dibidang watermarking sudah berkembang cukup pesat. Namun, tidak ada code watermark khusus yang dipulbikasikan secara umum. Hal ini disebabkan keamanan dari system watermak itu sendiri yang bergantung pada algoritma untuk menyisipkan dan mendeteksi watermak, tidak bedasarkan kunci yang digunakan seperti pada algoritma enkripsi pada umumnya

Sebuah watermarking yang baik tentunya harus dapat memenuhi kriteria / persyaratan tertentu. Kriteria tersebut antara lain adalah robustness atau kekuatan watermark yang tertanam dalam image.Pada image labelling hal ini sangat penting untuk menghindari serangan-serangan yang ditujukan untuk menghapus atau membuang watermark yang disisipkan.Selain itu, kerahasiaan penyisipan watermark juga menjadi salah satu pertimbangan dalam menentukan metode apa yang akan digunakan dalam proses penyisipan watermark.

Kata Kunci: *digital watermarking, image labelling, watermarking algorithm*

1. PENDAHULUAN

Dokumen *digital* yang ada saat ini sangat beragam formatnya. Ada format .txt, .rtf, .doc untuk dokumen teks, lalu ada jpg, bmp dan gif untuk bentuk dokumen citra, kemudian .mp3 dan .wav untuk bentuk dokumen audio, serta .mpeg, .mkv dan .avi untuk video dan masih banyak format dokumen *digital* lainnya. Dokumen *digital* tersebut dapat di-*copy* dan didistribusikan dengan mudah. Sehingga diperlukan mekanisme perlindungan terhadap dokumen *digital* tersebut.

Perlindungan ini sangat bermanfaat terutama untuk mengatasi masalah pembajakan atau peng-*copy*-an dokumen *digital* secara illegal. Apalagi bila dokumen yang di-*copy* secara illegal tersebut dijadikan sesuatu yang dikomsumsi publik secara komersil. Hal ini tentu akan sangat merugikan pihak pembuat atau pihak yang memiliki status kepemilikan terhadap dokumen yang dibajak. Salah satu cara yang cukup efektif dan terus dikembangkan saat ini adalah penggunaan *digital watermarking*.

Digital watermarking merupakan cara yang digunakan untuk menyisipkan informasi atau *watermark* pada suatu dokumen *digital*. Salah satu tujuan dilakukannya *digital watermarking* ini adalah untuk menyatakan kepemilikan (*copy*right) dari sebuah dokumen *digital*. *Watermark* yang disisipkan dapat berupa teks, logo, audio, atau pun data biner lainnya. Dalam makalah ini, akan dibahas algoritma *digital watermarking* pada dokumen citra *digital* (*image* labelling).

2.PENGGUNAAN DIGITAL *WATERMARKING*

Digital watermarking saat ini banyak dipergunakan secara luas. Selain sebagai mekanisme perlindungan dokumen *digital* (*copy*right protection), *digital* watermarking juga dipergunakan dalam penelusuran sumber dokumen *digital* (source tracking). Biasanya dokumen *digital* yang diterima pengguna diberi *watermark* yang berbeda. Sehingga bila dokumen *digital* tersebut disebar ulang, dapat diketahui sumbernya. *Digital* watermarking juga digunakan sebagai penanda siaran media massa (broadcast monitoring) serta komunikasi tertutup (rahasia).

2.1 Aplikasi *Watermark*

Watermark telah diterpkan secara luas untuk mengatasi berbagai tindak kejahatan yang berkaitan dengan dokumen *digital*. Fungsi penggunaan *watermark* tersebut antara lain adalah sebagai:

- Identifikasi kepemilikan
  Sebagai identitas dari pemilik dokumen *digital*. identitas ini disisipkan dalam dokumen *digital* dalam bentuk *watermark*. Biasanya identitas kepemilikan seperti ini diterapkan melalui visible *watermarking*. Misal url halaman web tempat suatu gambar didownload.

- Bukti kepemilikan
  Watermark merupakan suatu bukti yang sah yang dapat dipergunakan di pengadilan. Banyak

kasus pemalsuan foto yang akhirnya terungkap karena penggunaan *watermark* ini.

- Memeriksa keaslian isi karya *digital*
  Watermark juga dapat digunakan sebagai teknik untuk mendeteksi keaslian dari suatu karya. Suatu *image* yang telah disisipi *watermark* dapat dideteksi perubahan yang dilakukan terhadapnya dengan memeriksa apakah *watermark* yang disisipkan dalam *image* tersebut rusak atau tidak.

- *User authentication / fingerprinting*
  Seperti halnya bukti kepemilikan, *watermark* juga dapat digunakan sebagai pemeriksaan hak akses atau penanda (sidik jari) dari suatu *image*.

- *Transaction tracking*
  Fungsi transaction tracking ini dapat dilakukan pada *image* yang mengandung *watermark*. Pengimplementasiaanya dilakukan dengan memberikan *watermark* yang berbeda pada sejumlah domain / kelompok pengguna. Sehingga bila *image* tersebar diluar domain tersebut, dapat diketahui domain mana yang menyebarkannya.

- *Piracy protection/copy*
  Untuk dapat melakukan ini, perancang watermark harus bekerjasama tidak hanya pada masalah software, tetapi juga dengan vendor yang membuat hardware. Sehingga sebelum dilakukan peng-*copy*-an, terlebih dahulu dilakukan pemeriksaan apakah *image* tersebut boleh di-*copy* atau tidak.

- *Broadcast monitoring*
  Dalam dunia broadcasting / television news channel, *watermark* biasanya disisipkan sebagai logo dari perusahaan broadcasting yang bersangkutan. Hal ini dilakukan untuk menandai berita yang mereka siarkan. Sehingga bila pihak lain merekam berita tersebut, maka *watermark*-nya akan otomtis terbawa.

2.2 Teknik Penggunaan *Watermark*

Watermark dapat digunakan pada suatu dokumen *digital* dengan dua cara.

1. Cara yang pertama adalah dengan menyisipkan *watermark* tersebut secara langsung ke dalam dokumen *digital* (domain spatial).

2. Cara yang kedua adalah dengan mengintegrasikan *watermark* tersebut dengan dokumen *digital* (domain transform). Masing-masing domain akan dijelaskan kemudian bersamaan dengan algoritma *watermarking*.

Teknik *digital watermarking* yang dilakukan secara terintegrasi jauh lebih kuat (robust) dibandingkan dengan teknik penyisipan. *Watermark* yang berada pada dokumen *digital* yang diberi *watermark* secara terintegrasi tidak akan bisa dihapus atau dibuang. Hal ini disebabkan *watermark* tidak lagi disisipkan pada LSB (Least Significant Bit), namun pada signal yang di-*generate* berdasarkan dokumen *digital* tersebut. Sehingga setiap peng-*copy*-an dokumen *digital* dilakukan, *watermark* akan ikut ter-*copy*.

2.3 Kriteria *Watermark*

Agar suatu *watermark* dapat dikategorikan sebagai *watermark* yang baik, ada beberapa kriteria yang perlu dipenuhi. *Watermark* yang telah disisipkan ke dalam sebuah *image* tentu harus dapat diekstraksi kembali. Namun, *watermark* tersebut juga harus kuat terhadap berbagai jenis serangan. *Watermark* yang baik kriteria sebagai berikut:

1. Imperceptibility:
   Keberadaan *watermark* tidak dapat dipersepsi secara langsung oleh penglihatan manusia.

2. Key uniqueness:
   Kunci yang digunakan pada proses dan penyisipan dan ekstraksi adalah sama dan tidak ada kunci lain yang bisa digunakan untuk membukanya. Perbedaan kunci seharusnya menghasilkan *watermark* yang berbeda pula.

3. Noninvertibility:
   Proses untuk mendeteksi apakah citra tersebut ber-*watermark* atau tidak akan sangat sulit jika hanya diketahui citra ber*watermark* saja.

4. *Image* dependency:
   Watermark yang berada pada suatu *image* bergantung pada isi dari *image* tersebut.

5. Robustness:
   Kekuatan dari *watermark* yang disisipkan, sehingga *watermark* dapat bertahan walaupun telah dilakukan manipulasi terhadap medianya. Teknik yang baik dapat mengatasi manipulasi sehingga tidak merusak *watermark* dan tetap dapat diekstraksi.

2.4 Klasifikasi *Image Watermarking*

Klasifikasi terhadap *image watermarking* dapat dikelompokkan dalam beberapa kategori. Kategori yang pertama berdasarkan kenampakan dari *watermark.*

1. Visible *Watermarking*
   Pada visible *watermarking* ini, *watermark* yang disisipkan pada suatu *image* terlihat dengan jelas. *Watermark* biasanya berbentuk logo atau teks baik transparan atau tidak yang diletakkan tidak mengganggu / menutupi *image* asal. Jenis watermarking ini biasanya diterapkan pada *image* yang memang dimaksudkan untuk disebar secara umum bersama dengan identitas pemilik asal image tersebut.

2. Invisible *Watermarking*
   Sesuai namanya, *watermark* pada invisible watermarking yang disisipkan pada *image* tidak lagi dapat dipersepsi dengan indra. Namun, keberadaannya tetap dapat dideteksi. Penerapan teknik invisible *watermarking* ini lebih sulit dari pada teknik yang digunakan pada visible *watermark*ing.

Selain itu, *watermark* juga dikategorikan berdasarkan kekuatan *watermark* yang ada pada *image*. Berikut penjelasannya:

1. Fragile *Image Watermarking*
   Fragile *Image Watermarking* merupakan jenis *watermark* yang ditujukan untuk menyisipkan label kepemilikan *image*. Pada fragile *watermark*ing ini, *watermark* mudah sekali berubah atau bahkan hilang jika dilakukan perubahan terhadap *image*. Dengan begitu, *image* sudah tidak lagi memiliki *watermark* yang asli. Fragile *image watermarking* ini biasanya digunakan agar dapat diketahui apakah suatu *image* sudah berubah atau masih sesuai aslinya. Jenis *watermark* inilah yang banyak diterapkan pada suatu *image.*

2. Robust *Image watermarking*
   Robust *image watermarking* adalah teknik penggunaan *watermark* yang ditujukan untuk menjaga integritas / orisinalitas *image*. *Watermark* yang disisipkan pada media akan sangat sulit sekali dihapuskan atau dibuang. Dengan Robust *Image*, proses penggandaan *image* yang tidak memiliki izin dapat dihalangai. Kebanyakan aplikasi dari robust *watermarking* ini bukan pada sebuah image, melainkan pada sistem proteksi cd atau dvd.

2.5 Tahap (life-cycle) *Image Watermarking*

Sesuai dengan bahasan dari makalah ini, akan terlebih dahulu dijelaskan secara umum *watermarking* pada suatu dokumen citra *digital* (*image watermarking*). Pada dasarnya, proses *digital watermark* pada suatu *image* bisa dikelompokkan menjadi 3 tahapan. Tahap pertama adalah penyisipan *watermark*, kemudian tahap transmisi dokumen *digital* dan tahap yang ketiga adalah deteksi (extraction) dari *watermark* tersebut.

1. Pada tahap yang pertama, *watermark* akan disisipkan pada suatu *image* melalui suatu algoritma tertentu. *Image* yang disisipi *watermark* ini disebut sebagai host signal, sedangkan *watermark* atau informasi yang disisipkan disebut dengan covered signal. Dalam proses penyisipan ini, suatu algoritma akan menerima host signal dan covered signal ini untuk menjadikannya suatu *watermark*ed signal.

2. *Image* yang telah diberi *watermark* ini kemu-dian dapat disimpan atau disebarkan kepada pengguna. Tahap tansmisi inilah yang dinilai tidak aman. Pada tahap ini dapat terjadi serangan terhadap data yang telah diberi water-mark. Serangan yang dimaksud disini adalah serangan terhadap *copy*right, dimana penyerang berusaha menghilangkan *watermark* me-lalui modifikasi *image*. Modifikasi yang dilakukan dapat berupa penurunan tingkat perubahan geometri *image*, kompresi *image*, cropping atau menambah data lain (noise) terhadap *image* tersebut.

3. Pada tahap terakhir ini, dilakukan deteksi pada *watermark*, apakah *image* yang mengandung watermark itu masih asli atau telah mengalami perubahan. Tahap deteksi ini di-sebut juga dengan tahap ekstraksi, karena pada tahap ini *watermark* akan diekstrak dari *watermark*ed signal. Jika *watermark* yang diekstraksi belum mengalami peru-bahan, be-rarti keaslian *image* tersebut masih terjaga. Pada robust *watermark*, algoritma ekstraksi akan dapat menghasilkan *watermark* yang utuh.

3. METODE PENYISIPAN *WATERMARK*

Berdasarkan domain penyisipannya, metode penyisipan *watermark* kedalam suatu *image* dibagi menjadi dua ranah (domain), yaitu domain spatial dan domain transform. Penyisipan *watermark* dalam domain spatial dilakukan dengan menyisipkan *watermark* langsung pada nilai byte dari pixel *image*. Sedangkan penyisipan pada domain transform dilakukan menyisipkan *watermark* pada koefisien transformasi *image*.

Metode penyisipan *watermark* pada domain spatial memiliki kelebihan dari segi kemudahan dan kecepatan proses penyisipan *watermark*. Tetapi metode penyisipan ini tidak kokoh terhadap serangan dan dikategorikan sebagai fragile *watermarking*. Kelebihan metode penyisipan pada domain transform adalah kekuatan *watermark*nya (robustness). *Watermark* yang disisipkan dengan metode ini tahan terhadap serangan *watermark* seperti kompresi, translasi, penskalaan, pe-rubahan geometri *image* atau pun cropping.

Adapun metode yang sering digunakan dalam proses *image watermarking* adalah sebagai berikut:

3.1 Metode LSB

Metode penyisipan *watermark* yang paling mudah dilakukan adalah dengan menggunakan teknik penukaran LSB (Least Significant Bit). Hal ini dilakukan sama seperti penyisipan informasi rahasia pada steganografi, yakni dengan mengganti bit LSB dengan bit *watermark* yang disisipkan. Cara yang digunakan ialah dengan menambah nilai bit LSB satu bit lebih tinggi atau satu bit lebih rendah dari nilai sebelumnya.

Misalkan sebagian pixel pada *image* adalah
00110011 10100010 11100010 01101111

dan *watermark* yang akan disisipkan : 0111

Maka hasil encodingnya adalah:
00110010 10100011 11100011 01101110

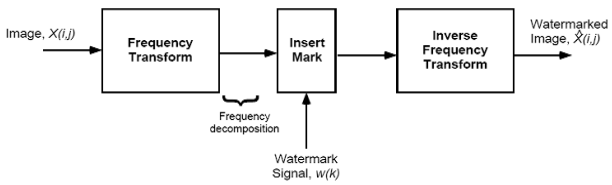
3.2 Metode Spread-Spectrum

Metode pertama kali diperkenalkan oleh Cox dalam makalah "Secure Spread Spectrum *Watermarking* for Multimedia" pada tahun 1997. Konsep utamanya adalah dengan menyebarkan *watermark* di dalam *image*. Spread-spectrum ini dapat dilakukan dalam ke dua-domain. Pada domain spatial, *watermark* disisipkan seca-ra tersebar pada nilai byte dari pixel penyusun *image*. Sedangkan pada domain transform, *watermark* disisip-kan pada koefisien transtformasi dari citra.

Pada metode spread-spectrum ini, *watermark* disisipkan secara additive modification. Spread-spectrum dikenal sebagai metode penyisipan *watermark* yang sangat kokoh (robust), namun, informasi *watermark* yang dapat dimasukkan hanya sedikit karena terjadinya interferensi pada frekuensi *image* serta terdapat trade-off antara robustness itu sendiri dan visibilitynya (α). Penyisipan dalam ranah frekuensi lebih robust dibandingkan dalam ranah spasial.

Konsep utama dari Spread Spectrum ini adalah dengan memodelkan *watermark* sebagai suatu narrowvband signal yang dibandingkan dengan *image* yang disisipi *watermark* di dalamnya (wideband signal). Nilai ketinggian frekuensi tidak selalu berakibat pada kokohnya *watermark*. Trik yang digunakan disini adalah dengan menyebarkan bit *watermark* melalui low frequency channel. Komunikasi spread spectrum menggunakan narrowband signal ditransmisikan dengan bandwidth yang cukup besar sehingga energi sinyal yang ada pada sinyal frekuensi tidak dapat dideteksi.

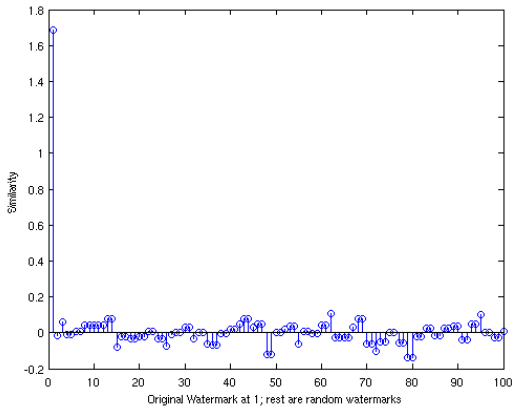
Metode spread spectrum digunakan untuk menyebarkan energi dari *watermark*, sehingga energi pada sebuah frekuensi akan semakin kecil dan menambah kerahasiaan dari penyisipan *watermark*. Spread spectrum juga menjamin robustness dari *watermark* karena untuk mengeliminasi sebuah *watermark* serangan harus dilakukan pada banyak kemungkinan frekuensi. Dengan menggunakan frekuensi sebagai medianya, *watermark* ini kuat terhadap konversi dari anolog ke *digital* dan *digital* ke analog.

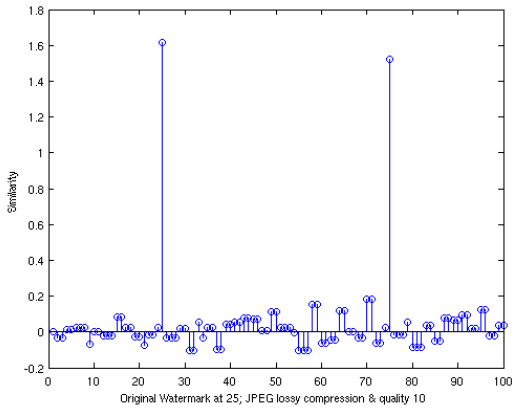


Algoritma penerapan Spread Spectrum dari [COX] adalah sebagai berikut:

1. *Image* ditransformasikan pada ranah frekuensi dengan DCT (Discrete Cosine Transform)
2. Ambil n nilai tertinggi dari koefisien DCT, dimana n adalah panjang dari *watermark*
3. Sebarkan *watermark* diantara nilai-nilai tersebut dengan fungsi invertible
   $v(i) = v(i) * (1+\alpha(i))$ dimana α adalah perbandian koefisien.
4. Kunci dari proses ini adalah setiap perubation dari koefisien DCT bergantung pada variable x(i) dimana variable ini diambil dari disribusi nilai ~N(0,1).
5. Setelah proses penyisipan *watermark* selesai, kemudian dilakukan invers dari DCT sehingga *image* kembali ke semula.

Image sebelum dan setelah kompresi





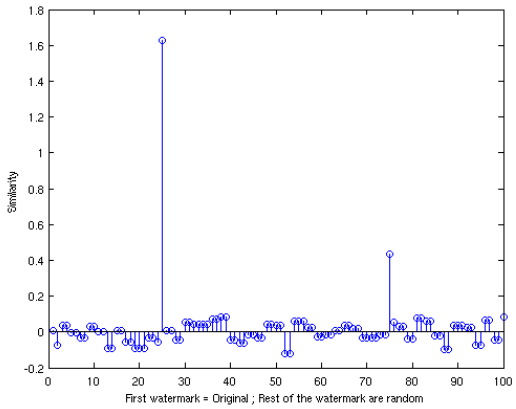


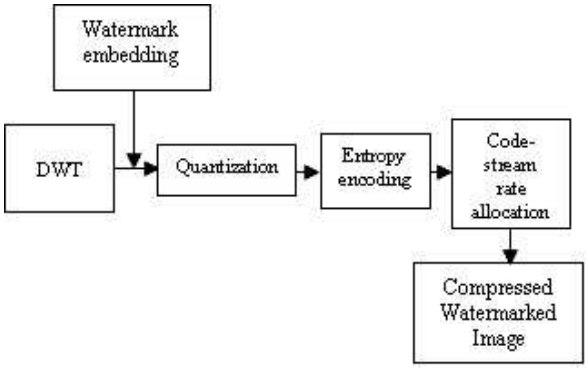
Diagram perbandingan *image* Lena antar sebelum, sesudah kompresi dan setelah dilakukakn perubahan terhadap skala gambar. Terlihat bahwa penyebaran watermark secara umum tidak berubah.

3.3 Metode Quantization

Watermark pada metode ini disisipkan secara terquantisasi. Metode ini dapat menampung informasi yang jauh lebih banyak dari sperad-spectrum untuk ukuran *image* yang sama karena tidak banyak terjadi interferensi. Ada banyak cara yang dapat diterapkan dalam metode quantization *watermarking*. Salah satu implementasi metode ini adalah secara quentization index modulation. Metode ini memproses signal sehingga distorsi antara quantized *image* dan *image* sebelumnya tidak terlalu berbeda.Ada banyak cara yang dapat diterapkan dalam metode quantization watermarking. Salah satu implementasi metode ini adalah secara quentization index modulation. Metode ini memproses signal sehingga distorsi antara quantized *image* dan *image* sebelumnya tidak terlalu berbeda.

Penerapan metode ini dimulai dari dekomposisi *image* menjadi beberapa (n) level. *Image* yang lebih kasar membawa low frequencies yang artinya menjadi bagian yang penting sebagai penyimpan struktur *image* asli. *Image* ini tidak akan di-quantisasi oleh decoder untuk meminimalisasi error saat rekonstruksi *image*.

Image sebelumnya akan ditransformasikan terlebih dahulu dengan menggunakan DWT domain. Kemudian, baru lah *watermark* disisipkan didalamnya, berdasarkan prioritas saat dilakukan quantisasi. Semua koefisien DWT dari *image* yang lebih kasar dipilih dan dikuantisasi berdasarkan metode yang dipiih. Setiap koefisien tersebut kemudian dipilih secara acak sebagai kunci (stream) untuk penempatan *watermark*.



3.4 Metode Amplitude Modulation

Pada metode ini, *watermark* disisipkan seperti pada spread-spectrum, yaitu secara additive modification. Hanya saja proses ini dilakukakan pada domain spatial. Amplitude modulation akan memasukkan bit watermark ke dalam nilai pixel yang telah dimodifikasi. Modifikasi yang dilakukan sebanding dengan luminance dan additive dari nilai bit. Kelebihan metode ini ialah tahan terhadap filtering dan serangan geometris.

Pada saat penyisipan *watermark* dilakukan, satu nilai bit *watermark* akan ditambahkan pada citra berdasarkan kunci yang di*generate* sacara acak sesuai dengan nilai channel yang telah dimodifikasi dengan fraksi luminance tadi. Dengan adanya density parameter, ukuran *image* bisa lebih bebas. Bergantung pada nilai densitinya.

4. ALGORITMA *WATERMARKING*

4.1 Cox Spread Spectrum Algorithm

Salah satu algoritma yang telah lama digunakan dalam watermarking adalah Cox algorithm ini. Sejak diperkenalkan oleh dirinya dalam sebuah paper yang ditulis tahun 1997. Cok algorithm meruapakan alogritma yang sederhana.

Cox Spread Spectrum Algorithm merupakan salah satu algoritma pertama yang menerapkan domain transform dalam *image watermarking*. Algoritma ini memasukkan *watermark* dalam bentuk signal (external file) untuk disisipkan dalam koefisien transformasi image.

Secara umum algoritma dapat dibagai menjadi empat bagian. Bagian pertama merupakan bagian yang digunakan untuk mengenerate signal masukan. Signal ini lah yang menjadi watermark yang akan disisipkan dalam image.

Lalu ada bagian enkripsi sebagai fungsi yang merubah image ke ranah transform melalui DCT, menyebarkan watermark didalamnya berdasarkan koefisien dan nilai variable α. Nilai α digunakan un-tuk memilih tingkat robustness atau visibility pada *image*. Kemudian mengembalikannya ke dalam image melalui invers DCT.

Bagian yang ketiga merupakan bagian untuk mengekstraksi watermark. Watermark yang diesktraksi kemudian dapat dibangdingkan dengan image awal melalui fungsi pembanding (bagian 4). Dengan fungsi ini lah dapat diketahui apakah image masih asli atau telah mengalami modifikasi.

5. KESIMPULAN

Berbagai metode dapat diterapkan untuk menyisipkan *watermark* ke dalam suatu *image*. Dengan disisipkan *watermark* ke dalam *image* ini, maka *image* yang ber*watermark* dapat terjaga orisinalitasnya.

Metode yang dipilih dalam penyisipan *watermark* akan sangat berpengaruh pada seberapa kuat (robust) *watermark* tersebut. Pemilihan metode berdasarkan tingkat kekuatan *watermarking* ini dapat disesuaikan dengan maksud pemberian *watermark*.

Algoritma Cox dalam penerapan Spread Spectrum terhadap *image* labelling sudah cukup robust. Algoritma ini dapat dioptimalisasi lagi dengan pengembangan algoritma lain yang memanfaatkan domain transform untuk menghasilkan algoritma yang lebih kuat.

DAFTAR REFERENSI

[1] Merwald, Peter. *Digital Image Watermarking in Wavelet Transform Domain*, University of Zalsburg.

[2] Munir, Rinaldi. 2005. *Diktat Kuliah IF3038 Kriptografi*, Program Studi Teknik Informatika ITB: Bandung.

[3] Cox J Ingemar, Kilian Joe, Leighton Tem, et al. *Secure spread spectrum watermarking for multimedia.* In Proceedings of the IEEE ICIP '97, California, USA, 1997.