

EC-5010 Keamanan Sistem Informasi

Partial Watermarking

Teknik dan Implementasinya pada Citra
di World Wide Web menggunakan
Java Script

Disusun oleh:
Elsiawaty / 13201142



INSTITUT TEKNOLOGI BANDUNG
DEPARTEMEN TEKNIK ELEKTRO
FAKULTAS TEKNIK INDUSTRI
2004

ABSTRAK

Telah banyak penelitian yang dilakukan dalam upaya peningkatan keamanan dalam pengiriman data melalui WWW, diantaranya *steganography*, *cryptography*, dan *watemarking*. Ada berbagai macam teknik *watemarking* yang diperkenalkan sampai saat ini, diantaranya menggunakan transformasi, baik di domain spasial maupun frekuensi untuk dokumen berupa citra (*gambar/image*), atau menggunakan modulasi antar kata atau antar huruf dalam dokumen berupa teks. Pembahasan lebih lanjut pada makalah ini adalah teknik *watemarking* untuk citra berwarna.

Indera penglihatan manusia memiliki keterbatasan dalam hal membedakan intensitas pixel yang hanya mengalami sedikit perubahan pada suatu citra ataupun perubahan warna dengan variasi yang sangat kecil. Keterbatasan ini dimanfaatkan untuk menyisipkan *watermark* pada citra, sehingga tanda ini tidak disadari oleh manusia. Beberapa penelitian membuktikan bahwa penglihatan manusia kurang mampu membedakan variasi warna daripada perubahan intensitas. Di samping itu, dari hasil pengamatan penulis, *watermark* lebih sulit dideteksi pada daerah berintensitas sangat rendah (daerah gelap pada citra). Biasanya, informasi *watermark* ditaruh pada seluruh bagian dari citra. Pada makalah ini, penulis mengusulkan untuk menerapkan *watemarking* yang menghasilkan perubahan kecil pada warna di sebagian daerah (parsial) yang memiliki intensitas rendah pada suatu citra, sehingga tanda pada citra tidak dapat dideteksi oleh pengamatan manusia. Namun, perhitungan matematis dan implementasinya belum disertakan dalam makalah ini.

Dengan menggabungkan teknik *watemarking* pada dokumen *Hyper Text Markup Language* melalui *Java Script*, maka informasi yang dikirim dapat menjadi lebih aman. Dalam makalah ini dijelaskan bagaimana caranya *watermark* (berupa informasi dekoder) ditambahkan ke citra *digital* untuk menerjemahkan dokumen yang telah terenkripsi. Implementasi dokumen HMTL adalah dengan menggunakan *Java Script*. Keuntungannya adalah identitas dari pengguna yang melakukan duplikasi dokumen akan dapat dilacak. Teknik menggabungkannya belum dicoba secara langsung. Penulis hanya memberikan usulan ide baru dan memberi gambaran prospek untuk penelitian lebih lanjut.

DAFTAR ISI

Abstrak.....	i
Daftar Isi	ii
Daftar Gambar	iv
1 Pendahuluan.....	1
1.1 Penggunaan <i>World Wide Web</i>	1
1.2 HAKI di Indonesia.....	1
1.3 Kegunaan <i>Watemarking</i>	3
2 Keamanan di <i>World Wide Web</i>	5
2.1 Latar Belakang Keamanan di WWW	5
2.2 Masalah Keamanan di WWW	5
2.3 Salah Satu Solusi Pemecahan Masalah Keamanan di WWW	6
3 Pengenalan <i>Digital Watemarking</i>	7
3.1 Latar Belakang Munculnya <i>Digital Watemarking</i>	7
3.2 Jenis-jenis <i>Watemarking</i>	7
3.2.1 Teknik <i>Robust Watemarking</i> Generasi Pertama	8
3.2.2 Teknik <i>Robust Watemarking</i> Generasi Kedua.....	10
3.2.3 Teknik <i>Robust Watemarking</i> Generasi Ketiga.....	10
3.3 Syarat-syarat Sebuah <i>Digital Watemarking</i> yang Ideal.....	11
4 Penerapan <i>Digital Watemarking</i>	13
4.1 Sekilas Perkembangan Teknik <i>Watemarking</i>	13
4.1.1 <i>Least Significant Bit Coding</i>	13
4.1.2 <i>Patchwork</i> oleh Bender.....	13
4.1.3 Pitas dan Kaskalis	13
4.1.4 Caroni.....	14
4.1.5 Cox.....	14
4.1.6 <i>Randomly Sequenced Pulse Position Modulated Code (RSPPMC)</i>	15
4.2 Perubahan Warna vs. Perubahan Intensitas	16
4.3 Perubahan Warna dengan Transformasi IHS, L^*a^*b , YIQ, atau YUV	16

4.4	Percobaan Menggunakan <i>Software Digimarc</i>	19
4.5	Usulan Teknik Baru untuk <i>Watermarking</i>	19
4.6	<i>Watermarking</i> pada WWW	21
4.5.1	Keamanan di WWW dengan Enkripsi	21
4.5.2	<i>Watermark</i> Berupa Informasi Dekoder yang Digunakan untuk Dekripsi Dokumen HTML.....	23
5	Kesimpulan dan Saran	25
5.1	Kesimpulan	25
5.2	Saran	25
6	Referensi	26

DAFTAR GAMBAR

Gambar 1 Penghilangan label hak cipta	2
Gambar 2 Skema teknik <i>robust watermarking</i> generasi pertama	8
Gambar 3 <i>Watermarking</i> generasi pertama pertama gagal terhadap serangan. (a) citra asli (b) citra yang sudah diberi watermark (c) citra yang sudah terkena serangan (<i>watermark</i> hilang)	9
Gambar 4 Skema teknik <i>robust watermarking</i> generasi kedua.....	10
Gambar 5 Skema teknik <i>robust watermarking</i> generasi ketiga	10
Gambar 6 a dan b menunjukkan keandalan metoda Cox, sedangkan c dan d menunjukkan kelemahan dari Metoda Cox	15
Gambar 7 Algoritma Gilani untuk penambahan <i>watermark</i> ke dalam citra berwarna	17
Gambar 8 Algoritma Gilani untuk pendeteksian watermark	18
Gambar 9 Implementasi algoritma Gilani pada citra; citra asli (kiri), citra yang telah diberi tanda (kanan)	18
Gambar 10 Contoh <i>watermarking</i> : antena parabola; citra asli (kiri) dan hasil <i>embedding watermark</i> (kanan)	19
Gambar 11 Histogram dari gambar antena parabola	20
Gambar 12 Proses segmentasi pada gambar mobil	21
Gambar 13 Contoh dokumen HTML menggunakan <i>Java Script</i>	22
Gambar 14 Tampilan <i>User Prompt</i> untuk meminta <i>user ID</i> ketika <i>file</i> HTML dijalankan.....	22
Gambar 15 Tampilan <i>User Prompt</i> untuk meminta kunci dekripsi ketika <i>file</i> HTML dijalankan.....	23

Bab I

PENDAHULUAN

1.1 Penggunaan *World Wide Web*

Sejak munculnya *World Wide Web* pada tahun 1990-an, yang diperkenalkan oleh Tim Berners-Lee dari CERN High Energy Particle Physics Laboratory di Geneva, Switzerland, orang mulai tertarik untuk menggunakan internet sebagai media pertukaran informasi yang mudah digunakan dan relatif cepat jika dibandingkan pengiriman melalui pos. Saat ini, WWW telah digunakan untuk berbagai kebutuhan, baik untuk kepentingan komersial, misalnya e-commerce, maupun penggunaan secara individual. Namun, masih banyak orang yang kurang menyadari pentingnya aspek keamanan dalam pengiriman informasi melalui WWW. Seiring dengan semakin meluasnya penggunaan WWW, pengiriman informasi semakin rentan terhadap penyadapan, pelanggaran terhadap hak cipta, dan bentuk serangan lain yang dapat mengubah autentikasi dan integritas data.

Salah satu cara untuk mencegah terjadinya pemalsuan ataupun penggunaan secara tidak legal pada dokumen yang didistribusikan menggunakan WWW adalah menandai dokumen tersebut dengan *watermark*.

1.2 HAKI di Indonesia

Sejak tanggal 1 Januari 2000 Indonesia dan negara anggota World Trade Organization telah menerapkan perlindungan Hak Atas Kekayaan Intelektual (HAKI). Indonesia juga termasuk salah satu negara penanda tangan persetujuan TRIPs (*Trade Related Aspects of Intellectual Property Rights*) pada tahun 1994. Namun demikian, di Indonesia tetap saja banyak beredar barang-barang bajakan, berupa *compact disc* (baik berisi program aplikasi kantor, permainan, lagu, film, dan sebagainya), kaset audio, dan media elektronik lain. Barang-barang bajakan ini telah banyak digunakan sebagai media pendistribusi yang berisi informasi, khususnya yang diperoleh dari penyadapan saluran komunikasi data melalui internet

menggunakan WWW. Jika Indonesia mampu memberikan solusi teknik *digital watermarking* yang dapat diandalkan, maka tentunya akan dapat memulihkan nama Indonesia yang sudah terkenal sebagai ‘sarang’ barang bajakan.

Beberapa cara yang pernah dilakukan oleh orang-orang untuk mengatasi masalah pelabelan hak cipta pada data *digital*, antara lain:

❖ *Header Marking*

Pencipta memberikan keterangan atau informasi hak cipta pada *header* dari suatu data *digital*.

Kelemahan :

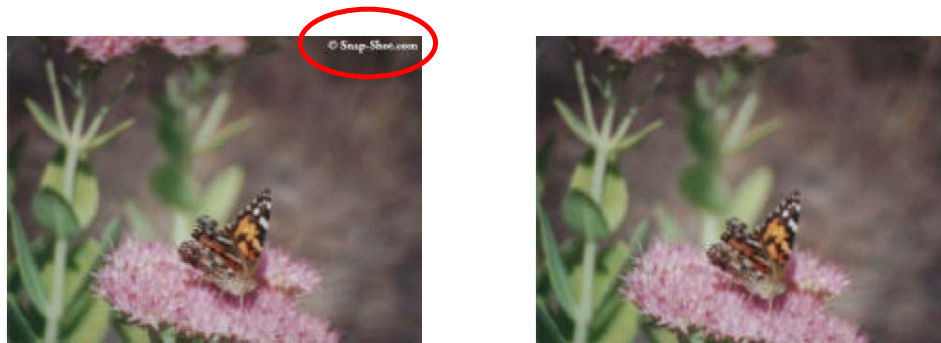
Ada beberapa *software*, seperti Hex Editor dan sejenisnya, yang dapat digunakan untuk membuka dokumen yang berisi data *digital* tersebut (dalam bentuk kode heksadesimal), kemudian menghapus informasi yang berkaitan dengan hak cipta dan sejenisnya yang terdapat di dalam *header* dokumen tersebut.

❖ *Visible Marking*

Pencipta memberikan tanda atau simbol hak cipta pada dokumen *digital* secara eksplisit (terlihat oleh pengamatan manusia).

Kelemahan :

Sama seperti kondisi sebelumnya, dengan tersedianya *software* untuk *image processing*, maka dengan sedikit ketrampilan dan kesabaran untuk memanipulasi citra *digital*, tanda atau simbol tersebut dapat dihilangkan dari data *digitalnya*.



Sumber : snap-shot.com

Gambar 1 Penghilangan label hak cipta

❖ *Encryption*

Pencipta mengkodekan data *digital* ke dalam bentuk representasi lain yang berbeda dengan aslinya, dan untuk mengembalikan ke kondisi semula diperlukan sebuah kunci rahasia tertentu.

Kelemahan :

Kunci rahasia tersebut dapat berupa kunci publik maupun kunci privat. Pemegang kunci publik adalah suatu badan yang dipercaya oleh masyarakat umum (*Key Distribution System*). Jika informasi yang disimpan oleh KDS bocor, maka penyebaran data *digital* secara ilegal dapat dengan mudah dilakukan.

❖ *Copy Protection*

Pencipta memberikan proteksi pada dokumen *digital* miliknya dengan membatasi akses pengguna sedemikian rupa sehingga data *digital* tersebut tidak dapat diduplikasi.

Kelemahan :

Sampai saat ini, proteksi dilakukan secara *hardware*, misalnya proteksi pada DVD, namun dengan adanya internet, proteksi secara *hardware* menjadi tidak lagi bermanfaat.

1.3 Kegunaan *Watermarking*

Ada berbagai tujuan yang ingin dicapai dari penggunaan *watermarking*, sebagai suatu teknik penyembunyian data pada data *digital* lain [3], yaitu:

❖ *Tamper-proofing*

Watermarking digunakan sebagai alat indikator yang menunjukkan apakah data *digital* yang asli telah mengalami perubahan dari aslinya (mengecek integritas data).

❖ *Feature location*

Watermarking sebagai alat identifikasi isi dari data *digital* pada lokasi-lokasi tertentu, misalnya penamaan suatu objek tertentu dari beberapa objek yang ada pada suatu citra *digital*.

❖ *Annotation/caption*

Watermark berisi keterangan tentang data *digital* itu sendiri, misalnya pada *broadcast monitoring* pada penayangan iklan di stasiun TV [4]. Selain itu, *watermark* juga dapat digunakan untuk mengirimkan pesan rahasia.

❖ *Copyright-Labeling*

Watermarking digunakan sebagai metoda untuk menyembunyikan label hak cipta pada data *digital* atau sebagai bukti autentik kepemilikan atas dokumen *digital* tersebut.

Bab II

KEAMANAN DI *WORLD WIDE WEB*

2.1 Latar Belakang Keamanan di WWW

Seluruh isi dari informasi yang dipertukarkan di internet menggunakan *World Wide Web*, disimpan dalam bentuk *digital*. Isi dalam pengkodean *digital* ini memungkinkan untuk dapat dengan mudah diduplikasi dalam jumlah banyak dengan hasil yang sama persis dengan aslinya, kemudian didistribusikan secara tidak legal.

Layanan WWW hanyalah bagian kecil dari keseluruhan sistem yang besar, mencakup internet, program web dari *server* dan klien, sistem operasi, dan LAN. Tingkat keamanan dari keseluruhan sistem yang besar ini akan sebesar tingkat keamanan dari komponen sistem yang paling lemah keamanannya.

Untuk mengevaluasi keamanan dari suatu sistem, perlu diperhatikan titik-titik lemah dari komponen sistem, kebijakan keamanan apa yang harus diadopsi, serta bagaimana caranya memaksakan suatu kebijakan keamanan [7].

Sampai saat ini, tingkat kesadaran (*awareness*) dari pengguna internet di Indonesia dapat dikatakan masih cukup rendah. Biasanya bila belum terjadi permasalahan yang menyangkut keamanan, maka tidak akan dilakukan pencegahan akan terjadinya hal tersebut.

2.2 Masalah Keamanan di WWW

Ada beberapa masalah keamanan di WWW yang sering terjadi [7], diantaranya sebagai berikut :

- ❖ *File-file* penting yang disimpan dalam *server* dicuri oleh pihak yang tidak berwenang. Biasanya ini terjadi ketika *server* mengizinkan akses untuk *file-file* di luar area yang didesain untuk penggunaan WWW.
- ❖ Informasi rahasia, seperti nomor kartu kredit disadap dengan menggunakan berbagai cara. Permasalahan ini muncul pada saat data sedang dikirim melalui media komunikasi.

- ❖ *Server* menampilkan terlalu banyak informasi, seperti jenis software yang digunakan, konfigurasi jaringan, dan sebagainya, yang dapat digunakan oleh penyerang untuk mengetahui kelemahan dari *server* tersebut
- ❖ Berbagai kekurangan yang ada di software web *server* digunakan oleh penyerang untuk mendapatkan akses masuk ke dalam *file* sistem dari *server* tersebut.

Dari uraian di atas, terlihat bahwa letak kunci permasalahan yang paling mendominasi keamanan di WWW adalah data informasi yang sifatnya rahasia dapat dicuri, diduplikasi kemudian didistribusi secara ilegal, atau diubah isinya kemudian dikirim lagi, yang semua hal ini dilakukan oleh orang yang tidak bertanggung jawab.

2.3 Salah Satu Solusi Pemecahan Masalah Keamanan di WWW

Pada awal mulanya, *watermark* digunakan pada surat-surat penting ataupun uang kertas, sebagai contoh *watermark* yang terdapat pada *bank note* (surat hutang bank) akan terlihat memiliki transparansi (daya tembus pandang) yang berbeda ketika dibandingkan dengan bagian kertas yang tidak terdapat *watermark*. Namun, tentunya hal ini tidak dapat diterapkan pada data berbentuk *digital*.

Sampai saat ini, berbagai standar telah diterapkan dalam usulan teknik *watemarking* untuk data *digital* oleh para ahli. Bahkan, Ingemar J. Cox, Matt L. Miller dan Jeffrey A. Bloom [10] menyatakan bahwa tidak akan mungkin untuk menciptakan hanya satu standar untuk diaplikasikan dalam berbagai teknik *watemarking*.

Pembahasan lebih lanjut mengenai teknik *digital watemarking* akan dibahas dalam bab berikut.

Bab III

Pengenalan *Digital Watermarking*

3.1 Latar Belakang Munculnya *Digital Watermarking*

Sebenarnya, konsep atau ide awal dari *watermarking* telah ada sejak tahun 1990-an [1], namun istilah *watermark* baru digunakan pada tahun 1993, diperkenalkan oleh A.Z.Tirkel dan teman-temannya [2].

Digital watermarking didasarkan pada ilmu stenografi, yaitu ilmu yang mengkaji tentang penyembunyian data [5]. Istilah “stenografi “ berasal dari Bahasa Yunani, yang berarti *covered-writing*, atau tulisan tersembunyi. Teknik ini mengambil keuntungan dari keterbatasan indera manusia, khususnya penglihatan dan pendengaran, sehingga *watermark* yang dibubuhkan pada dokumen tidak akan disadari kehadirannya oleh manusia.

3.2 Jenis-jenis *Watermarking*

Secara garis besar, ada dua jenis *watermarking* :

❖ *Robust watermarking*

Jenis *watermark* ini tahan terhadap serangan (*attack*), namun biasanya *watermark* yang dibubuhi ke dokumen masih dapat ditangkap oleh indera penglihatan atau pendengaran manusia.

❖ *Fragile watermarking*

Jenis *watermark* ini akan mudah rusak jika terjadi serangan, namun kehadirannya tidak terdeteksi oleh indera manusia.

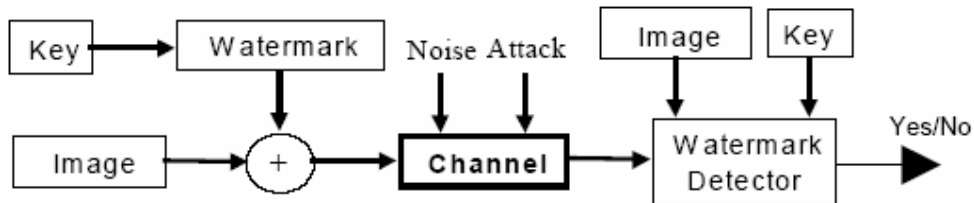
Jika diinginkan untuk membuat suatu algoritma yang dapat mengimplementasikan *watermarking* yang memiliki *fidelity* yang tinggi (adanya *watermark* tidak disadari oleh pengamatan manusia) maka hasilnya akan semakin rentan terhadap serangan.

Ada tiga tahap utama dalam proses *watemarking* :

1. mengintegrasikan *watermark* pada citra (*embedding*)
2. serangan terhadap citra yang telah dibubuhi *watermark*, baik yang disengaja (misalnya dikompresi, dipotong sebagian, di-*filter*, dan sebagainya) ataupun yang tidak disengaja (misalnya disebabkan oleh *noise* atau gangguan dalam saluran transmisi data).
3. proses ekstraksi *watermark* dari dokumen yang akan diuji.

Metoda robust *watemarking* dibagi menjadi 3 tahap generasi oleh Mitrea [6] yang akan dijelaskan lebih lanjut pada sub bab berikut.

3.2.1 Teknik *Robust Watemarking* Generasi Pertama



Gambar 2 Skema teknik *robust watemarking* generasi pertama

Dalam metode *watemarking* generasi pertama, tanda (*mark*) yang diberikan terdiri dari sebuah *pseudo random zero mean Gaussian sequence*, dihasilkan berdasarkan sebuah informasi rahasia (yang selanjutnya disebut kunci / *key*). Tanda ini ditambahkan ke suatu citra. Citra yang sudah ditandai ini dapat mengalami perubahan yang disebabkan oleh dua kemungkinan. Kemungkinan pertama adalah timbulnya gangguan yang muncul ketika citra diproses, biasanya disebut sebagai *noise*. Kemungkinan kedua adalah adanya usaha dari *user* yang tidak bertanggung jawab untuk membuat tanda *watermark* menjadi tidak terdeteksi, gangguan ini biasanya disebut sebagai serangan (*attack*).

Proses deteksi membutuhkan kunci dan citra asli kemudian menyediakan jawaban apakah citra telah ditandai atau tidak (*yes/no answer*) [9]. *Watermark* ditambahkan ke citra pada bit paling tidak signifikan (*least significant bit*) dari tiap pixel pada citra, sehingga penurunan kualitas dari citra akan menjadi minimum. Namun, cara ini sangat mudah terkena serangan, yaitu jika bit yang paling tidak

signifikan diganti secara acak, maka watermark akan hilang. Contoh dari aplikasi ini ditunjukkan pada Gambar 3, suatu panorama dengan kedalaman pixel 512x512 dan derajat keabuan sebanyak 256 level. Gambar 3.a adalah citra asli, 3.b menunjukkan citra yang telah diberi tanda dengan *Gaussian sequence* (zero mean, 1 variance), sedangkan 3.c menunjukkan gambar yang telah diberikan serangan dengan mengganti 3 LSB dengan bilangan acak.



(a)



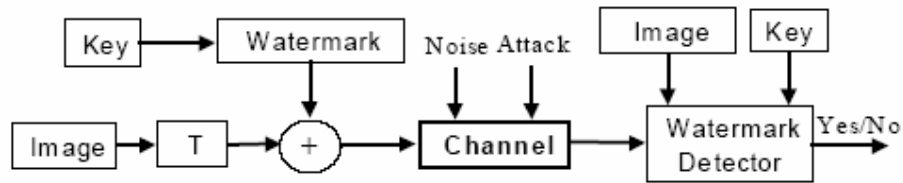
(b)



(c)

Gambar 3 *Watermarking* generasi pertama pertama gagal terhadap serangan. (a) citra asli (b) citra yang sudah diberi watermark (c) citra yang sudah terkena serangan (*watermark* hilang)

3.2.2 Teknik *Robust Watermarking* Generasi Kedua

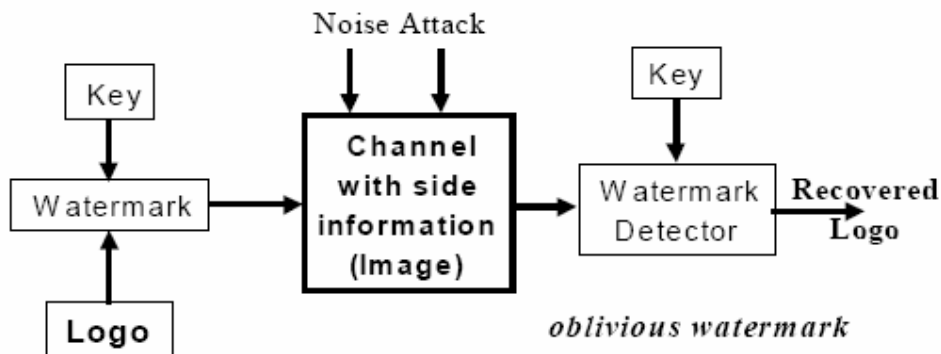


Gambar 4 Skema teknik *robust watermarking* generasi kedua

Pada generasi kedua, metoda *watermarking* tidak secara langsung menambahkan *watermark* ke dalam citra *digital*, tetapi pada citra yang sebelumnya ditransformasi terlebih dahulu (misalnya *Discrete Cosine Transform*, *Hadamard transform*, *Fourier transform*, *Mellin-Fourier transform*, *Wavelet Transform*, dan sebagainya). Masing-masing transformasi memiliki kelebihan dan kekurangannya masing-masing. Misalnya, metoda dengan Transformasi DCT akan tahan terhadap kompresi JPEG, sedangkan Transformasi Mellin-Fourier tahan terhadap proses rotasi. Contoh algoritma generasi kedua ini adalah metoda Cox yang akan dibahas lebih lanjut di sub bab 4.1.5.

Penerapan *watermarking* pada berbagai domain dengan berbagai transformasi turut mempengaruhi berbagai parameter penting dalam *watermarking* [15] (*bitrate*, *invisibility*, dan *robustness*).

3.2.3 Teknik *Robust Watermarking* Generasi Ketiga



Gambar 5 Skema teknik *robust watermarking* generasi ketiga

Teknik *watemarking* generasi ketiga mencoba untuk memanfaatkan citra asli. Saluran pengiriman data (*channel*) juga membawa informasi tambahan (*side information*) [17]. Selain itu, kapasitas saluran transmisi harus ditingkatkan : permasalahannya tidak lagi terletak pada pengiriman informasi 1 bit saja (*yes/no answer*), tetapi juga untuk memulihkan logo, nama, dan sebagainya, yang direpresentasikan dalam beberapa bit, misalnya 60-70 bit. Citra asli tidak digunakan pada waktu proses deteksi.

Untuk mengukur hasil dari metoda *watemarking* ini, Peticolas [18] telah membuat prosedur yang disebut sebagai *Stirmark*. Prosedur ini akan mencoba berbagai transformasi yang akan membuat detektor *watemarking* tidak mampu untuk mendeteksi ada tidaknya watermark pada citra, yaitu kuantisasi ulang (*resampling*), proses geometri : perentangan (*stretching*), pemotongan (*shearing*), pergeseran (*shifting*), dan rotasi, dan *bending* (deviasi kecil pada setiap pixel, yang nilainya bergantung pada posisi di citra). Dari berbagai metoda yang diusulkan para ahli, hanya sedikit yang mampu bertahan oleh serangan *Stirmark*.

3.3 Syarat-syarat Sebuah *Digital Watemarking* yang Ideal

Untuk mendapatkan suatu teknik *digital watemarking* yang baik, maka teknik tersebut harus dapat memenuhi kondisi di bawah ini [8,16] :

1. Elemen dari suatu data *digital* dapat secara langsung dimanipulasi dan informasi dapat ditumpangkan ke dalam data *digital* tersebut
2. Penurunan kualitas dari data *digital* setelah dibubuhkan *watermark*, dapat seminimal mungkin.
3. *Watermark* dapat dideteksi dan diperoleh kembali meskipun setelah data *digital* diubah sebagian, dikompresi, ataupun di-*filter*.
4. Struktur dari *watermark* membuat penyerang sulit untuk mengubah informasi yang terkandung di dalamnya.
5. Proses untuk membubuhkan *watermark* dan mendeteksinya cukup sederhana
6. Jika *watermark* dihapus, maka kualitas dari data *digital* yang ditumpanginya akan berkurang jauh atau bahkan rusak sama sekali.
7. Informasi *watermark* yang diselipkan dalam isi data *digital* dapat dideteksi ketika dibutuhkan.

8. Label hak cipta yang unik mengandung informasi pembuatan, seperti nama, tanggal, dan sebagainya, atau sebuah kode hak cipta seperti halnya ISBN (*International Standard for Book Notation*) pada buku-buku.
9. *Watermark* tidak dapat diubah atau dihapus (*robustness*) secara langsung oleh orang lain atau dengan menggunakan *software* pengolahan sinyal sampai tingkatan tertentu.
10. *Watermarking* yang diberikan lebih dari satu kali dapat merusak data *digital* aslinya. Cara ini dilakukan supaya orang lain tidak dapat melakukan pelabelan berulang terhadap data yang telah dilabel.

Sampai saat ini, belum ada teknik *watermarking* yang dapat memenuhi seluruh kriteria di atas.

Bab IV

PENERAPAN *DIGITAL WATERMARKING*

4.1 Sekilas Perkembangan Teknik *Watermarking*

Semua metoda penggabungan watermark pada dokumen *digital* memiliki keuntungan dan kerugiannya masing-masing, tetapi kekurangan yang paling umum terjadi adalah kesulitan untuk dideteksi kembali setelah mengalami serangan (*attack*) atau gangguan (*noise*).

Beberapa metoda yang pernah diteliti, diantaranya adalah:

4.1.1 *Least Significant Bit Coding*

Teknik ini sangat sederhana, namun tidak mampu bertahan terhadap serangan yang dapat mengubah nilai intensitas pada citra. Caranya adalah dengan mengubah nilai LSB (*Least Significant Bit*) komponen intensitas atau warna menjadi bit dari label yang akan disembunyikan. Hasil citra setelah digabung dengan *watermark* akan sangat mirip dengan aslinya (tingkat *fidelity* yang tinggi). Seperti yang telah dijelaskan sebelumnya, teknik ini termasuk *watermarking* generasi pertama.

4.1.2 *Patchwork oleh Bender*

Caranya adalah dengan menanamkan label 1 bit pada citra *digital* dengan menggunakan pendekatan statistik [3]. Sejumlah n pasang titik (a_i, b_i) pada citra dipilih secara acak, kemudian *brightness* dari a_i dinaikkan 1 (satu) dan *brightness* dari pasangannya b_i diturunkan satu. Nilai harapan dari jumlah perbedaan n pasang titik tersebut adalah $2n$. Teknik ini kurang tahan terhadap kompresi JPEG (hanya sekitar 75%).

4.1.3 *Pitas dan Kaskalis*

Kedua ahli ini mengusulkan metoda yang hampir sama dengan metoda yang diusulkan oleh Bender. Cara yang dilakukan adalah membagi sebuah citra menjadi dua bagian (*subsets*) sama besar (misalnya dengan menggunakan *random generator*)

atau dengan menggunakan *digital signature* yang dikodekan sebagai matriks berordo $m \times n$ dengan jumlah biner "1" sama dengan jumlah biner "0". Kemudian salah satu subset ditambah dengan faktor $k \in \{\text{bulat positif}\}$. Faktor k diperoleh dengan menghitung variansi dari kedua subset. Verifikasi dilakukan dengan menghitung perbedaan rata-rata antara kedua subset. Nilai yang diharapkan adalah sebesar k bila ada *watermark* pada citra. Metoda ini cukup tahan terhadap kompresi JPEG (sekitar 90%).

4.1.4 Caroni

Beliau mengusulkan suatu teknik untuk menyembunyikan sejumlah bit label pada komponen intensitas dari citra dengan membagi atas blok-blok, kemudian intensitas dari setiap pixel dalam satu blok akan dinaikan dengan faktor tertentu bila ingin menambahkan *watermark* berisi kode biner bit '1', sedangkan jika ingin mengisi dengan kode biner bit '0' maka nilai intensitas tidak diubah.. Untuk memperoleh *watermark* kembali, maka *brightness* citra yang sudah diberi tanda akan dikurangkan dengan citra asli. Jika rata-rata dari satu blok pixel melewati suatu nilai (*threshold*) tertentu, maka akan dinyatakan sebagai bit '1', bila tidak maka dinyatakan sebagai bit '0'. Cara ini tidak tahan terhadap kompresi JPEG (faktor kualitas hanya sebesar 30%).

4.1.5 Cox

Watermark terdiri dari *zero mean Gaussian sequence* dan ditambahkan ke koefisien DCT terbesar. Karena koefisien terbesar dari DCT akan merepresentasikan karakteristik yang menonjol dari citra, maka untuk mengurangi degradasi setelah penambahan *watermark*, variansi dari *watermark* haruslah kecil. Contohnya watermark memiliki variansi $\sigma^2 = 1$ dan ditambahkan ke 1024 koefisien DCT yang terbesar. Teknik ini merupakan contoh dari *watemarking* generasi kedua.

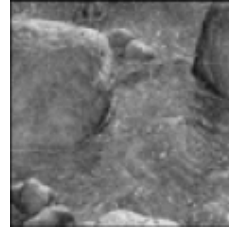
Teknik ini tahan terhadap *additive Gaussian noise* dengan $\mu = 30$ dan $\sigma^2 = 64$, bahkan setelah dikompresi dengan JPEG pada factor kualitas $Q = 60$ (Gambar 5.a menunjukkan citra asli, 5.b menunjukkan hasil citra yang sudah diberi gangguan, kompresi, dan pemotongan).

Namun sayangnya, teknik ini sangat rentan terhadap proses rotasi, bahkan untuk rotasi yang kecil sekalipun dapat menghapus *watermark* di dalamnya. Selain

itu, citra dengan daerah latar belakang yang cukup luas akan meninggalkan tanda yang cukup jelas. Jika variansi diperkecil maka tanda akan menjadi kurang jelas, namun keandalannya akan berkurang pula. (Gambar 5. c menunjukkan citra asli, 5.d menunjukkan citra yang sudah diberi *watermark*).



(a)



(b)



(c)



(d)

Gambar 6 a dan b menunjukkan keandalan metoda Cox, sedangkan c dan d menunjukkan kelemahan dari Metoda Cox

4.1.6 Randomly Sequenced Pulse Position Modulated Code (RSPPMC)

Teknik ini diusulkan oleh Koch dan Zhao [22], juga menggunakan DCT seperti metoda Cox. Namun perbedaannya adalah metoda ini didasarkan pada prinsip format JPEG. Suatu citra *digital* dibagi menjadi blok-blok berukuran 8x8 dan kemudian ditransformasi dengan DCT. Selanjutnya, dengan menggunakan prinsip

spread spectrum (metoda *frequency hopped*) dan RSPPMC (*Randomly Sequenced Pulse Position Modulated Code*), koefisien-koefisien DCT tersebut diubah sedemikian rupa sehingga mengandung informasi 1 bit dari *watermark*. Misalnya untuk menambahkan *watermark* dengan kode biner bit '1' ke dalam suatu blok koefisien DCT 8x8, maka koefisien ketiga dari tiga koefisien yang dipilih harus diubah hingga lebih kecil jika dibandingkan dengan kedua koefisien lainnya.

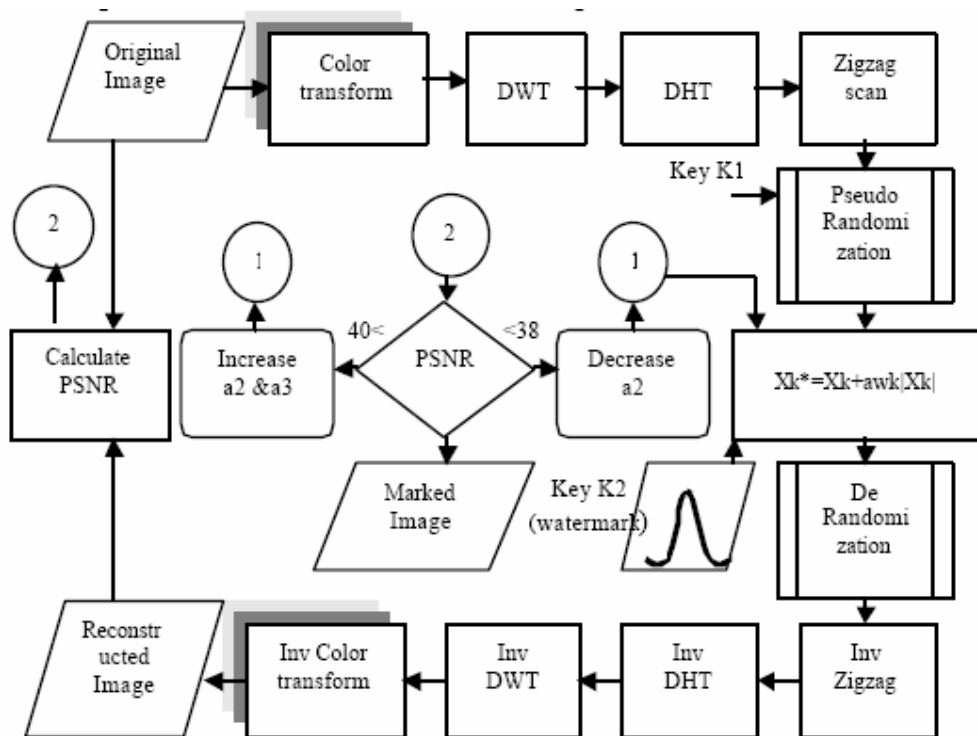
4.2 Perubahan Warna vs. Perubahan Intensitas

Yu dan teman-temannya [12] telah menemukan teknik baru untuk deteksi. Dalam melakukan percobaannya, mereka menggunakan perubahan terhadap Algoritma Kutters. Kutter [13] memanfaatkan kekurangan dari penglihatan manusia dan ketidakmampuannya untuk mendeteksi perubahan kecil pada warna gambar. Algoritma ini berhasil untuk berbagai tipe serangan tetapi proses deteksinya cukup rumit.

Untuk meningkatkan keberhasilan proses deteksi, Yu dan teman-temannya memutuskan untuk menggunakan jaringan saraf tiruan (*Artificial Neural Network*). Untuk melatih jaringan saraf tiruan ini, digunakan banyak citra yang telah diberi *watermark*, kemudian diberikan serangan (pemotongan sebagian, penyaringan dengan *low pass filter*, *median filter*, dan sebagainya, dikompresi) dengan berbagai teknik. Dengan demikian, bila jaringan saraf tiruan ini telah melalui proses belajar hingga tercapai tingkat *error* minimum yang diinginkan, maka citra baru yang belum pernah dihadapi sebelumnya akan dapat dideteksi oleh jaringan ini, yang tentunya akan gagal jika dilakukan oleh detektor *watermark* biasa. Percobaan yang dilakukan mereka telah membuktikan hasil yang baik dan proses deteksi hampir empat kali lebih baik dibandingkan detector biasa untuk jenis serangan yang umum terjadi.

4.3 Perubahan Warna dengan Transformasi IHS, L^*a^*b , YIQ, atau YUV

Dari hasil studi berbagai literatur, hasil yang paling baik untuk teknik *watermarking* yang memanfaatkan perubahan warna adalah transformasi IHS, L^*a^*b , YIQ atau YUV, yang diperkenalkan oleh Gilani dan teman-temannya [21].

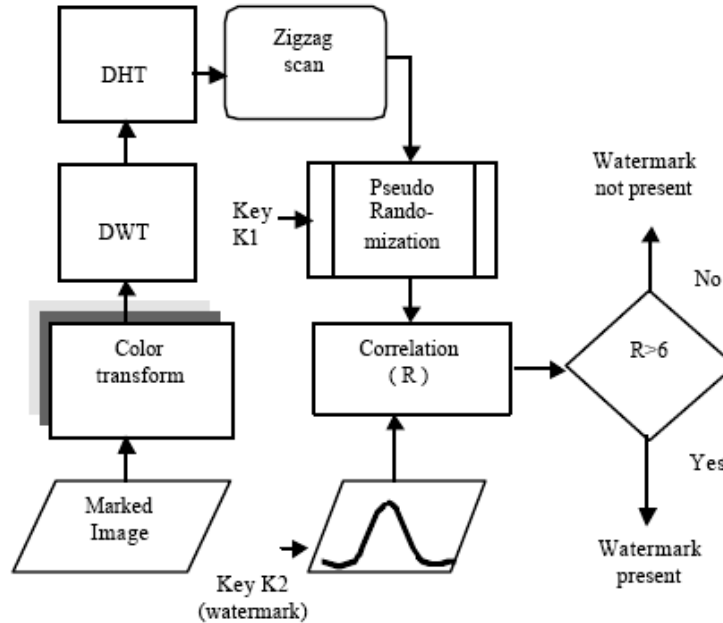


Gambar 7 Algoritma Gilani untuk penambahan *watermark* ke dalam citra berwarna

Keterangan gambar :

- DHT : Discrete Handamard Transform
- DWT : Discrete Wavelet Transform
- PSNR : Peak Signal to Noise Ratio

Teknik pendefinisian warna dengan RGB akan menyebabkan terjadinya korelasi satu sama lain dan sangat tidak sesuai dalam teknik *watemarking*. Algoritma *watemarking* ditunjukkan pada Gambar 7. Pertama-tama citra berwarna akan ditransformasi dengan salah satu transformasi warna, misalnya IHS, L^*a^*b , YIQ atau YUV, sehingga mengurangi korelasi dalam satu saluran (*channel*). Tiap *channel* akan dianggap sebagai citra yang independen, yang akan ditambahkan *watermark*.



Gambar 8 Algoritma Gilani untuk pendeteksian watermark

Peak Signal to Noise Ratio (PSNR) digunakan untuk mengevaluasi kualitas dari citra. Nilai PSNR dikontrol dengan mengatur nilai a . Citra yang diuji akan dibandingkan dengan citra aslinya. Jika hasil perhitungan nilai PSNR berada di antara 38-40 dB, maka proses akan dihentikan. Jika tidak, maka nilai a dinaikkan atau diturunkan hingga kondisi PSNR terpenuhi. Dengan menggunakan kemampuan adaptasi ini maka citra akan ditambahkan watermark hingga diperoleh level maksimum dari *trade-off* antara *invisibility* (tidak terlihat, atau beberapa literatur menyebutnya sebagai *fidelity*) dan keandalan (*robustness*) yaitu parameter a .

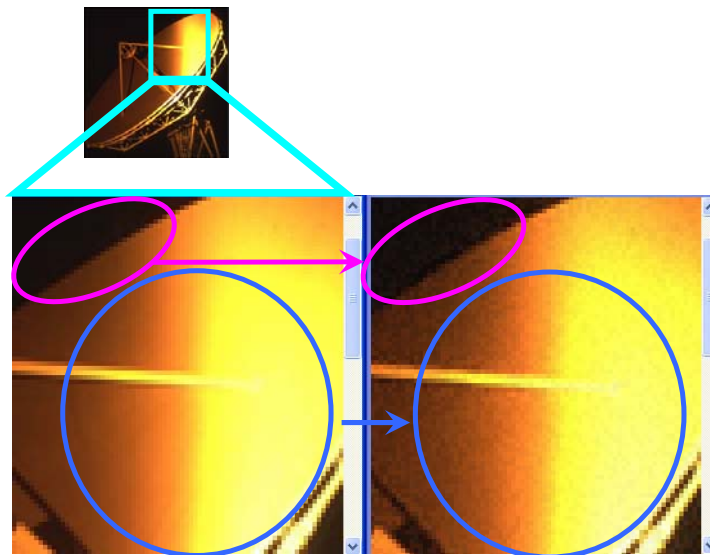


Gambar 9 Implementasi algoritma Gilani pada citra; citra asli (kiri), citra yang telah diberi tanda (kanan)

Implementasi penggabungan dari algoritma segmentasi dan *watemarking* dengan teknik di atas belum dilakukan penulis. Pengembangan yang dilakukan masih berupa pemikiran ide baru dari konsep yang sudah ada sebelumnya.

4.4 Percobaan Menggunakan *Software Digimarc*

Di bawah ini memperlihatkan contoh penambahan *watermark* pada suatu citra dengan menggunakan *tool* berupa *Digimarc Demo Version*. Gambar di sebelah kiri adalah citra asli dan yang di sebelah kanan adalah citra yang sudah dibubuhi oleh *watermark*.



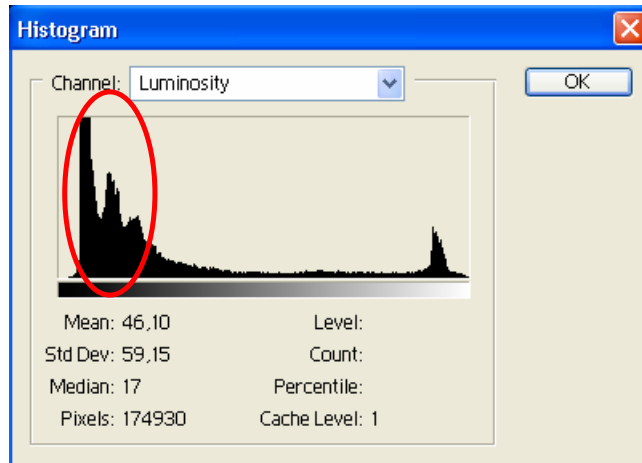
Gambar 10 Contoh *watemarking*: antena parabola; citra asli (kiri) dan hasil *embedding watermark* (kanan)

Gambar di atas memperlihatkan hasil pemberian *watermark* pada suatu citra. Dengan perbesaran 400% maka dapat dilihat bahwa pada sebagian daerah yang memiliki intensitas rendah (ditandai oleh kurva berwarna ungu), hasil *watemarking* dapat dikatakan hampir tidak dapat dibedakan dengan gambar aslinya. Sedangkan pada daerah berintensitas yang lebih tinggi (ditandai oleh kurva berwarna biru), *watermark* menimbulkan degradasi terhadap citra aslinya.

4.5 Usulan Teknik Baru untuk *Watermarking*

Sampai saat ini, *watemarking* dilakukan pada seluruh bagian dari citra *digital*. Dari contoh gambar antena parabola di atas, dapat dilihat bahwa daerah yang

memiliki intensitas rendah setelah diberi *watermark*, akan memiliki *fidelity* yang jauh lebih baik (degradasi dari citra asli jauh lebih kecil) bila dibandingkan dengan daerah yang berintensitas tinggi.



Gambar 11 Histogram dari gambar antenna parabola

Gambar 11 menunjukkan histogram dari gambar antenna parabola. Daerah yang memiliki intensitas sangat rendah jumlahnya cukup banyak (ditandai oleh kurva merah). Di daerah inilah jika ditambahkan *watermark* pada citra, maka hasil degradasinya tidak akan kentara oleh penglihatan manusia. Untuk melakukan hal ini, tentunya citra harus dipotong-potong (segmentasi) terlebih dahulu untuk mendapatkan daerah yang memiliki intensitas rendah.

Algoritma untuk segmentasi dari citra *digital* sebelum dilakukan *watermarking*, telah diperkenalkan oleh Nikolaos dan teman-temannya [20]. Daerah hasil segmentasi diperoleh dengan cara mengumpulkan pixel-pixel dengan intensitas yang tidak jauh berbeda, sedangkan yang berbeda jauh akan dikumpulkan lagi menjadi daerah (segmen) yang lain.

Dasar pemikiran dari Nikolaos adalah rata-rata dari sekumpulan pixel yang berada dalam satu daerah (segmen) tidak akan mengalami perubahan jauh setelah ditambahkan *watermark*, sehingga objek yang sama akan diekstrak dalam proses deteksi.



Gambar 12 Proses segmentasi pada gambar mobil

Penulis mengusulkan bagaimana jika hasil daerah segmentasi dari citra dibandingkan lagi satu sama lain, kemudian diambil daerah (segmen) yang memiliki rata-rata intensitas paling rendah, baru kemudian diterapkan algoritma untuk menambahkan *watermark*, dengan teknik YUV oleh Gilani yang telah dijelaskan pada sub bab 4.2.

4.6 *Watermarking* pada WWW

4.5.1 Keamanan di WWW dengan Enkripsi

Dalam upaya untuk menyediakan tingkat keamanan yang lebih tinggi, dapat didesain sedemikian rupa, sehingga setiap *user* memiliki kunci dekripsi masing-masing, kemudian dikirim ke *server* HTTP (*Hyper Text Transfer Protocol*) melalui CGI (*Common Gateway Interface*) pada *server* [11].

Permintaan untuk informasi yang tidak rahasia ke *server* akan diproses secara normal melalui mekanisme HTTP biasa, sedangkan permintaan untuk halaman web yang mengandung dokumen terenkripsi akan melalui prosedur khusus yang akan dijelaskan berikut ini. Gambar 13 menunjukkan source code HTML dengan menyertakan suatu citra yang telah dienkrpsi. Halaman web ini disimpan sebagai *plaintext* di *server*.

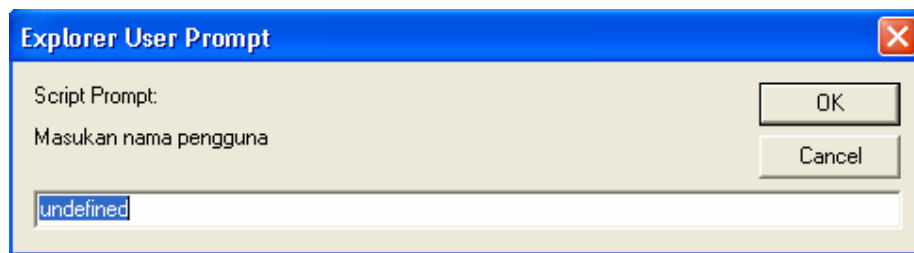
```

<HTML>
  <HEAD>
    <TITLE>Crypter</TITLE>
  </HEAD>
  <BODY>
    <script Language="JavaScript">
      document.writeln("<h1> Contoh dokumen dengan komponen dienkrpsi </h1>");
      document.writeln("Citra berikut ini harus didekripsi");
      document.writeln("<hr>");
      document.writeln("<applet archive='\"Decoder.jar\"' code='\"Decoder.class\"' width=200 height=100>");
      document.writeln("<param name=image value='\"encrypted.gif\">");
      document.writeln("<param name=userid value='\"' + prompt(\"Masukan nama pengguna\") + '\">");
      document.writeln("<param name=decoder value='\"' + prompt(\"Masukan kunci dekripsi\") + '\">");
      document.writeln("</applet>");
      document.writeln("<hr>");
    </script>
  </body>
</html>

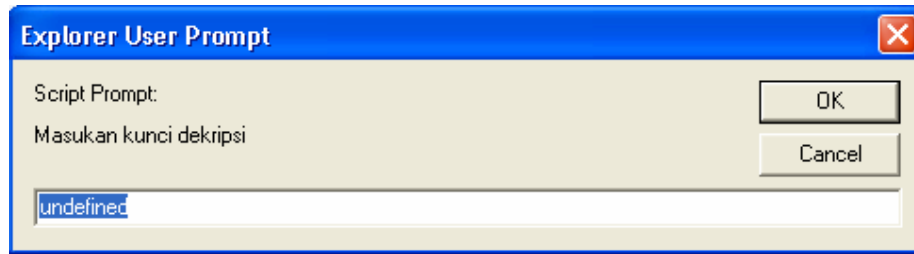
```

Gambar 13 Contoh dokumen HTML menggunakan *Java Script*

Browser akan memperoleh halaman web melalui mekanisme HTTP secara normal, kemudian akan diminta untuk memasukkan *user* ID dan kunci dekripsinya. Tentunya hal ini akan sedikit memperlambat pengguna untuk mengakses suatu web, karena diharuskan memasukkan identitas pengguna dan kunci dekripsinya.



Gambar 14 Tampilan *User Prompt* untuk meminta *user* ID ketika *file* HTML dijalankan



Gambar 15 Tampilan *User Prompt* untuk meminta kunci dekripsi ketika *file HTML* dijalankan

Permintaan *user ID* dan kunci dekripsi ini dikodekan dengan *Script* berbahasa pemrograman *Java* yang terletak pada *source HTML*-nya. Dalam contoh yang diperlihatkan pada gambar di atas, *user* diminta (secara paksa) untuk memberikan informasi ini pada saat menjalankannya, tetapi metoda untuk menyimpan informasi pada komputer *client* ini cukup sulit karena adanya mekanisme seperti *Cookies*, yang dapat dicuri oleh orang lain.

Halaman yang dihasilkan akan mengandung *Java applet* yang akan melewati parameter *user ID* dan kunci dekripsi. Setelah itu, *Decoder applet* akan diberikan informasi yang cukup sehingga dapat melayani permintaan HTTP untuk dokumen terenkripsi yang diminta. Permintaan ini seperti layaknya permintaan CGI ke *server*. Program CGI kemudian akan menerima informasi identifikasi *user* untuk mengenkripsi dokumen beserta nama dokumen yang diminta. Aplikasi CGI akan melakukan pengecekan atas nama *user* dan menentukan kunci enkripsi *user*. Dokumen yang diminta kemudian dienkripsi menggunakan kunci *user* tersebut dan kemudian dikirim melalui *Java applet*. Akhirnya, dokumen akan didekripsi dan ditampilkan menggunakan *Java applet* sesuai metoda di atas.

4.5.2 Watermark Berupa Informasi Dekoder yang Digunakan untuk Dekripsi Dokumen HTML

Sekalipun sistem dirancang sedemikian rupa agar dicapai tingkat keamanan maksimum yang mungkin diwujudkan, tetap saja selalu ada kemungkinan data dapat diperoleh dengan cara curang. Dalam upaya untuk membantu dalam menentukan di mana tempat terjadinya penerobosan sekuriti, maka hal penting yang harus dilakukan adalah dokumen yang sudah dienkripsi diberi tanda *watermark* dengan informasi

yang mengidentifikasi dekoder untuk dekripsinya. Dengan demikian, maka akan dapat ditelusuri kembali jejaknya bila jatuh ke tangan yang tidak berwenang. *Watermark* yang ditandai pada dokumen sebaiknya mencakup informasi tentang mekanisme dekripsi, termasuk tanggal melakukan dekripsi.

Oleh karena setiap pengguna (*user*) memiliki kunci dekripsi yang unik, dan *Java applet* memiliki kontrol untuk proses dekripsi serta menerjemahkannya, maka teknik ini secara langsung akan memiliki tanda *applet* sehingga hasil terjemahan akan secara unik mengidentifikasi pengguna yang mendekripsi dokumen. Jika tanda ini dapat diandalkan dan disembunyikan dengan baik, maka pengguna yang menduplikasi dokumen akan menduplikasi pula informasi yang cukup untuk mengidentifikasi diri mereka sebagai sumber dari penerobosan sekuriti.

Berbagai teknik untuk *watermark* telah dijelaskan pada sub bab sebelum ini. Jika teknik yang telah dijabarkan di atas diintegrasikan ke dalam *Java Script* di HTML, maka akses melalui WWW menjadi lebih aman. Dalam makalah ini tidak dibuat implementasi menggunakan *Java Script*.

Watermarking dapat digabungkan ke dalam sistem enkripsi-dekripsi dalam salah satu dari dua cara berikut [11]:

❖ *Browser-based watermarking*

Metoda ini akan secara langsung menggunakan *Java applet* untuk menerapkan *watermarking* pada citra. Kompleksitas pada pemodelan *Java* ini adalah tidak tersedianya kontrol yang bagus untuk menampilkan warna dengan *applet* yang ada. Oleh karena itu, teknik *watermarking* yang didasarkan pada penggunaan pemetaan warna untuk mengkodekan *watermark* tidak dapat diterapkan.

❖ *CGI-based watermarking*

Mekanisme ini akan menambahkan watermark pada dokumen sebelum dienkripsi dan dikirim ke *browser*. Pada pendekatan berdasarkan CGI, proses *watermarking* dilakukan di *server*, sehingga lebih rumit dan proses komputasi akan lebih berat lagi. *Watermarking* pada level-CGI juga memastikan bahwa proses tidak dapat digagalkan oleh serangan yang disebabkan oleh proses dekripsi berbasis bahasa pemrograman *Java*. Jadi, kekurangan teknik ini hanyalah terletak pada beban komputasi yang cukup besar di sisi *server*.

Bab V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari studi literatur yang dilakukan penulis dan dari hasil percobaan *watemarking* menggunakan *tool Digimarc Demo Version*, teknik *watemarking* yang ada sampai saat ini semuanya menambahkan tanda *watermark* pada **seluruh** bagian citra *digital*.

Keterbatasan manusia pada indera penglihatan dapat dimanfaatkan, terutama pada perubahan warna yang sangat sedikit dan perubahan kecil pada intensitas gambar. Penulis berkesimpulan bahwa dengan memberikan perubahan kecil pada warna di sebagian daerah berintensitas sangat rendah dari suatu citra *digital* (*watemarking parsial*), maka akan diperoleh citra yang sudah diberi tanda yang memiliki *fidelity* yang sangat baik, yaitu tingkat degradasinya tidak dirasakan oleh pengamatan manusia. Bila teknik ini diterapkan dengan menggunakan *Java Script* untuk menyisipkan informasi dekoder untuk menerjemahkan dokumen terenkripsi di WWW, maka tentunya keamanan di internet dapat lebih ditingkatkan lagi.

5.2 Saran

Teknologi *watemarking* dapat dikatakan masih relatif baru dan sampai saat ini masih belum ada standar khusus yang berlaku internasional, sehingga masih membuka peluang riset yang luas. Penelitian mengenai pengembangan teknik *watemarking* sebaiknya tidak hanya dicoba dari tahap awal lagi, tetapi juga dicoba untuk memperbaiki teknik yang sudah ada, sehingga penelitian generasi sebelumnya tidak menjadi sia-sia. Meskipun demikian, tidak tertutup kemungkinan bila ditemukan teknik yang benar-benar baru (bukan berupa pengembangan dari teknik yang telah ada) yang menghasilkan *watemarking* lebih baik lagi daripada hasil telah ada yang sebelumnya.

Bab VI

REFERENSI

- [1] Ir. I. Wiseto P. Agung MSc. *Digital Watermarking : Teknologi Pelindung HAKI Multimedia*. Elektro Indonesia, Nomor 35, Tahun VI, Februari 2001.
- [2] A.Z.Tirkel, G.A.Rankin, R.M. van Schyndel, N.R.A. Mee, C.F. Osborne. *Electronic Water Mark*. DICTA, 1993.
- [3] W. Bender, D. Gruhl, N. Morimoto dan A. Lu. *Techniques for data hiding*. IBM System Journal, Vol. 35, 1996.
- [4] Cox, Ingemar J.; Miller, Matt L.; Bloom dan Jeffrey A. *Watermarking applications and their properties*. Int. Conf. On Information Technology 2000, Las Vegas. 2000.
- [5] L.M. Marnel, C.G Boncelet, Jr dan C.T Retter. *Spread spectrum image steganography*. IEEE Transactions on Image Processing. Agustus 1999. pp 1075-1083.
- [6] Mihai P. Mitrea, Françoise J. Prêteux, dan Adriana Vladl. *Robust Watermarking Method for Colour Still Image Databases*. Juli, 2002.
- [7] *World Wide Web Security*. Diambil 20 Mei 2004 : <http://www.hkcert.org/ish/section5.html>
- [8] *General Information about digital watermarks*. Diambil 20 Mei 2004 : http://www.ewatermark.com/dd_ot_aboutwater.html
- [9] R. Wolfgang dan E. Delp. *A Watermark for Digital Images*. IEEE International Conference on Image Processing, 16-19 September 1996. pp. 219-222.
- [10] Cox, Ingemar J., Miller, Matt L., Bloom and Jeffrey A. *Watermarking applications and their properties*. Int. Conf. On Information Technology 2000, Las Vegas, 2000.
- [11] Patrick Dymond dan Michael Jenkin. *WWW Distribution of Private Information with Watermarking*. Oktober 1998.

- [12] Yu, Tsai, dan Lin. *Digital watermarking based on neural networks for colour images*. Signal Processing (Mar 2001) pp663-671.
- [13] M. Kutter, F. Jordan, dan F.Bossen. *Digital signature of color images using amplitude modulation*. Proc SPIE, Software and Retrieval for Image and Video Databases. Februari 1997. pp 518-526.
- [14] I. J. Cox, J. Kilian, T. Leighton, dan T. Shamoan. *Secure spread spectrum watermarking for multimedia*. Technical report, NEC Research Institute, 1995. Technical Report 95-10.
- [15] G.C. Langelaar, et al. *Copy Protection for Multimedia Data based on Labeling Techniques*. 1996.
- [16] Supangkat, Suhono. H.; Kuspriyanto; Juanda: "Watemarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital", Majalah Ilmiah Teknik Elektro, 2001.
- [17] C.E. Shannon. *Channels with Side Information at the Transmitter*. IBM Journal, Oktober 1958, pp. 289-293.
- [18] F. Petitcolas, R. Anderson, dan M. Kuhn. *Attacks on copyright marking systems*. Proc of the Second workshop on information hiding, David Aucsmith Ed. Lecture Notes - Computer Science Vol. 1525 Portland, USA, 1998.
- [19] G.C. Langelaar, et al. *Copy Protection for MultimediaData based on Labeling Techniques*. 1996.
- [20] Nikolaos V. Boulgouris, Ioannis Kompatsiaris, Vasileios Mezaris, and Michael G. Strintzis. *Content-based Watermarking for Indexing Using Robust Segmentation*. April 2001.
- [21] S.A.M.Gilani, I.Kostopoulos and A.N.Skodras. *Color Image-Adaptive Watermarking*. April 2002.
- [22] E. Koch, J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", Proceedings IEEE Workshop on Non Linier Signal and Image Processing, Neos Marmaras, June, 1995.