APLIKASI *WATEMARKING* UNTUK PERLINDUNGAN HAKI PADA CITRA DIGITAL DALAM DOMAIN FREKUENSI MENGGUNAKAN *FAST FOURIER TRANSFORM* (FFT)

Kartika Firdausy, Anton Yudhana, Eka Rahmat. B
Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
Kampus III UAD Jl. Prof. Dr. Soepomo, Janturan, Umbulharjo, Yogyakarta
Telp. (0274) 379418-381523 psw 101/220, Fax 0274-381523
e-mail: kartikaf@indosat.net.id, anton@uad.ac.id, ka2_proletar@yahoo.com

Abstrak

Watermarking adalah suatu metode untuk menyebunyikan data pada data digital tanpa diketahui oleh indera penglihatan atau pendengaran. Dalam paper ini watermarking di aplikasikan untuk perlindungan HaKI pada citra digital khususnya citra diam (gambar). Metode watermarking yang digunakan dengan memanfaatkan transformasi matematis Fast Fourier Transform (FFT) yang berfungsi untuk mentransformasikan dari domain spasial ke domain frekuensi, karena citra label yang tertanam di dalam citra host lebih kuat terhadap serangan setelah melaluai transformasi terlebih dahulu. Ada dua program utama dari aplikasi watermarking yaitu program proses inserting (penyisipan) yang berfungsi untuk menyisipkan citra label atau label kepemilikan kedalam citra yang dilindungi dan program proses extracting (pendeteksian) sebagai pendeteksi label yang tertanam di dalam citra tersebut. Hasil watermarking yang dicapai dalam paper ini adalah informasi atau label yang tertanam dalam citra digital, invisible (tidak nampak oleh kasat mata) dan robust (tahan) terhadap penghapusan secara langsung atau dari beberapa proses pengolahan citra digital.

Kata kunci : *Watermarking,* PSNR, HaKI, FFT.

1. PENDAHULUAN

Perkembangan teknologi digital serta Internet saat ini telah memberi kemudahan untuk melakukan akses serta mendistribusikan berbagai informasi dalam format digital. Apa saja yang dibutuhkan yang berhubungan dengan teknologi ini dengan mudah didapatkan dan hak ciptapun mulai terancam karena banyaknya pihak yang tidak bertanggung jawab mengambil hak cipta orang lain untuk memenuhi kebutuhannya. Setiap orang mulai khawatir tentang hukum yang mengatur proteksi terhadap hak cipta untuk data digital seperti gambar (*image*), film (*movie*) dan suara (*audio*). Keterbatasan pengetahuan tentang bagaimana menjaga keamanan hasil karya dari berbagai sifat yang merusak hasil karya, membuat orang berpikir kreatif, bagaimana caranya menjaga hasil karya itu dengan kemampuan dan fasilitas yang ada.

Seiring dengan perkembangan teknologi informasi yang semakin pesat, maka metode-metode baru dalam bidang keamanan semakin dikembangkan. Untuk melindungi data atau informasi digital hasil karya tersebut yang berhubungan dengan HaKI atau disebut juga Intellectual Propertyright.

Watermark (tanda air) berbeda dengan tanda air pada uang kertas. Ide awalnya muncul pada tahun 1990. Pada tahun 1993 A.Z. Tirkel, dkk[1] mulai menggunakan kata 'watermark' dalam papernya, namun baru pada tahun 1995/1996 topik ini menjadi perhatian dan mulai menjadi salah satu fokus riset. *Watermark* merupakan suatu bentuk dari *Steganography* yang mempelajari teknik-teknik bagaimana menyimpan suatu data digital ke dalam data *host* atau data digital lain. Istilah "*Steganography*" berasal dari bahasa Yunani, yang berarti *covered-writing* atau tulisan tersembunyi. Teknik ini memanfaatkan keterbatasan indra manusia khususnya indera penglihatan dan pendengaran, sehingga *watermark* yang disisipkan pada dokumen tidak akan disadari kehadirannya oleh manusia.

2. METODE PENELITIAN

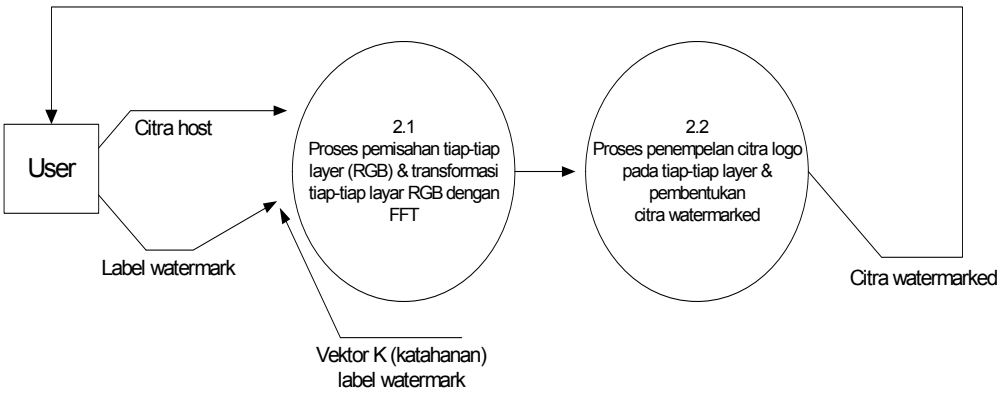
Watermarking atau tanda air dapat diartikan sebagai suatu teknik penyembunyian data atau informasi "rahasia" ke dalam suatu data lainya untuk "ditumpangi"[2]. Jadi kalau dilihat secara kasat mata data atau informasi yang disisipkan kedalam citra digital tidak terlihat dan tahan terhadap serangan berupa pengolahan citra digital serta tidak menghambat pendistribusian. Jadi *watermark* harus:

a. *Invisible* : tidak terlihat oleh indera penglihatan dan pendengaran
b. *Robust* : tahan terhadap serangan berupa pengolahan citra digital atau penghapusan secara langsung.
c. *Trackabel* : tidak menghambat proses penduplikasian tetapi penyebaran data dapat dikendalikan.

Ada dua proses yang harus dilakukan pada proses *watermarking*, yaitu:

a. Proses *inserting* atau proses penyisipan

Proses yang terjadi pada proses penyisipan melibatkan aliran informasi berupa citra *host* dan citra label yang kemudian diproses dengan menggunakan algoritma yang telah ditentukan sebelumnya, dengan memasukan ketahanan yang berfungsi sebagai ketahanan atau untuk mempertahankan label ketika dikenakan pengolahan citra atau serangan lainya, vektor ketahanan sangat berpengaruh terhadap citra label yang disisipkan pada citra *host,* semakin besar nilai ketahanannya semakin kuat terhadap serangan tetapi label semakin terlihat hal ini menyebabkan kualitas citra menurun sebaliknya nilai ketahanan semakin kecil label kepemilikan semakin tidak tampak kualitas citra bagus tetapi ketahanan labelnya berkurang, selanjutnya proses pembentukan citra *watermarked*.



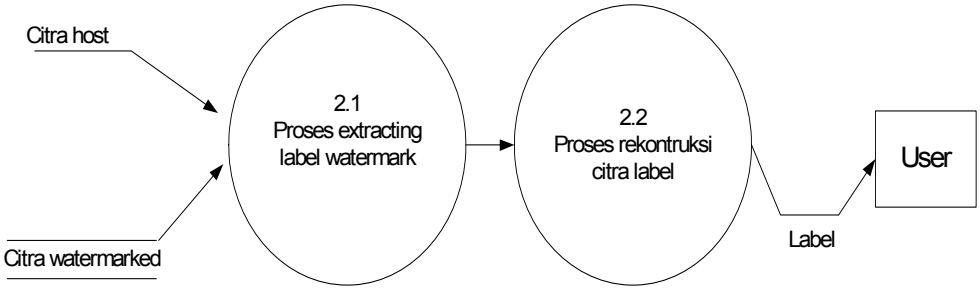
Gambar 1. Proses *inserting* pada teknik *watermarking*

Berdasarkan Gambar 1, ada beberapa langkah yang harus dilakukan untuk proses *inserting* yaitu sebagai berikut :

1). Baca citra *host* dan pisahkan tiap-tiap layer pada citra *host* karena tiap-tiap layer akan ditempelkan label kepemilikan (citra label).
2). Baca Citra label dan konversikan kedalam bentuk biner dan ditambahkan ketahanan (*Robust*), hal tersebut untuk menjaga keutuhan citra *watermark* ketika ada proses serangan dan pengekstraksian.
3). Sesuaikan bentuk matrik citra label sesuai dengan ukuran citra *host*. Karena citra label tidak boleh lebih besar dari citra *host*, untuk menjaga kualitas citra yang akan didistribusikan.
4). Transformasikan tiap-tiap layer citra *host* dan citra label menggunkan FFT, kemudian citra label ditempelkan ke dalam masing-masing layer citra *host* yang telah ditransformasikan dan menetapkan *invers* (IFFT) pada masing-masing layer yang telah disisipi citra label untuk mengembalikan kembali ke domain spasial agar citra bisa dibaca kembali.
5). Proses terakhir. Pembentukan citra *watermarked* dengan cara menggabungkan kembali semua layer yang telah ditempeli label kepemilikan.

b. Proses *extracting* atau proses pendeteksian

Proses ini melibatkan aliran informasi berupa citra *host* dan citra *watermarked*, yang diambil dari tempat penyimpanan yang telah disediakan dari proses sebelumnya (proses *inserting*). Citra *host* dan citra *watermarked* disertakan sebagai input dalam proses *extracting* atau proses pendeteksian label dari citra *watermarked*, kemudian kedua citra tersebut diproses dan hasil dari proses tersebut adalah citra label (label kepemilikan), kemudian hasilnya dikembalikan ke *user*.



Gambar 2. Proses *extracting* pada teknik *watermarking*

Berdasarkan Gambar 2, ada beberapa langkah yang harus dilakukan untuk proses *extracting* yaitu sebagai berikut:

1). Pada setiap layer (RGB) citra *host* dan citra *watermarked* dipisahkan untuk memudahkan ketika proses *extracting* dilakukan, karena ditiap-tiap layer disisipi citra label.
2). Sesuaikan ukuran citra watermarked dengan ukuran citra host.
3). Ekstrak layer dari kedua citra yang telah dipisahkan tiap-tiap layernya citra watermarked dikurangi citra host.
4). Bentuk citra label. Dalam pembentukannya tiap-tiap label yang berada pada tiap-tiap layer yang telah di ekstrak dekalikan 255 untuk membentuk kembali citra label.

3. HASIL DAN PEMBAHASAN

Pada tahap pengujian ini bermaksud untuk menguji ketahanan citra digital dari hasil proses *watermarking* (citra *watermarked*), citra hasil akan dikenai beberapa jenis serangan (pengolahan citra digital) serangan akan dilakukan dengan persepsi bahwa citra yang telah diserang masih bisa digunakan atau didistribusikan oleh pihak lain, baik pihak yang mengetahui bahwa citra tersebut telah ditempeli sebuah pesan atau informasi maupun pihak yang belum mengetahui sama sekali.

Sistem ujicoba pada 4 citra yang sama dengan format *true color*, tipe .*BMP, ketahanan yang digunakan 1-5 dengan serangan berupa beberapa pengolahan citra dan hasilnya ditunjukkan pada Tabel 1 dan 2.

Table 1. Hasil *watermarking* sebelum terkena serangan

Ketahanan	Nilai PSNR pada citra *watermarked* (dB)
1	48.8569
2	42.8363
3	39.3145
4	36.8157
5	34.8775

Dari hasil perhitungan yang tertampil pada Tabel 1 dan 2, pengujian menggunakan citra dengan ukuran 269x334x24b dengan indeks pengujian 100 kecuali pada *noise* 1x. Hasil dari

nilai-nilai yang didapat dalam table-tabel tersebut berdasarkan dari perhitungan PSNR (*Peak Signal to Noise Ratio*) dengan cara untuk Tabel 1 membandingkan citra *host* (asli) dengan citra yang *watermarked* dan pada Tabel 2 perbandingan antara citra *watermarked* sebelum terkena pengolahan citra dengan citra *watermarked* sesudah terkena pengolahan citra.

Table 2. Hasil *watermarking* setelah terkena serangan berupa beberapa pengolahan citra digital

Ketahanan	Nilai PSNR (dB)			
	Kompresi *Lossy* JPG 100	**Blurring 100**	**Sharpening 100**	**Noise 1x**
1	42.0471	34.9226	31.5264	21.3821
2	42.0256	34.8376	31.4385	21.3560
3	42.0131	34.6932	31.2883	21.3060
4	42.0333	34.4884	31.0775	21.2463
5	42.0288	34.2412	30.8237	21.1842

Hasil dari perhitungan tersebut memperlihatkan kualitas citra masih dalam keadaan relative cukup baik sesuai dengan criteria table PSNR yaitu dengan kualitas *Poor* dengan nilai 30 dB dan *Good* dengan nilai 40 dB di bawah nilai 30 dB kualitas citra buruk dan akan berpengaruh pada citra label yang tertanam di dalamnya, citra label akan rusak atau tidak dapat dilihat dengan jelas, seperti pada proses noise dengan 1x.

4. SIMPULAN

Keberadaan label masih dapat dipertahankan dan kualitas citra *watermarked*-nya pun masih dalam keadaan relatif cukup baik. Hal ini berarti citra label yang disisipkan sebagai label kepemilikan masih dapat diperoleh kembali dan dikenali oleh si pemiliknya, namun label tidak dapat direkonstruksi ulang atau dibentuk kembali apabila terkena proses yang lebih ekstrim seperti *noise*, karena serangan tersebut sangat berpengaruh banyak terhadap intensitas atau bit-bit yang bersangkutan, sehingga mengakibatkan citra label tidak bisa direkonstruksi secara baik oleh algoritma yang telah dibangun. Pada pengembangan lebih lanjut tentang teknik *watermarking* perlu dititikberatkan pada pembuatan algoritma yang bisa mempertahankan label kepemilikan dari berbagai serangan berupa pengolahan citra digital tanpa harus mengurangi kualitas citra pembawanya atau citra yang ditumpanginya, sehingga citra dapat terjaga kualitasnya dan tahan terhadap berbagai serangan berupa pengolahan citra digital seperti: *Cropping,Rotating, Resize* dan *Noise.*

DAFTAR PUSTAKA

[1] Agung, P, W., **"Digital Watermarking Teknologi Pelindung HaKI Multimedia"**, Elektro Indonesia, No 35, Tahun VI, Februari, Jakarta, 2000.

[2] Firdausy, F., Hawariyanta, I., dan Murinto, **"Implementasi *Watermarking* untuk Penyembunyian Data pada Citra dalam Domain Frekuensi Menggunakan *Discrete Cosine Transform*"**, Jurnal Telkomnika, Vol 4, No. 1, 2006.

[3] Purbaningsih, E, SN., Mardi, S., dan Suprapto, K, Y., **"Proteksi Watermarking pada Citra Diam dengan Metode RSPPMC"**, Reseach GrouP on Intelegent Technology for Non Linier System, Sekolah Tinggi Informatika & Komputer Indonesia, Politeknik Elektro Negeri Surabaya, ITS, Surabaya, 2004.