IMPLEMENTASI *WATERMARKING* PADA GAMBAR MENGGUNAKAN METODA *DISCRETE WAVELET TRANSFORM*

Torkis Nasution[1], Adyanata Lubis[2]
Program Studi Teknik Informatika
[1]STMIK Amik Riau, [2]Universitas Pair Pengaraian
e-mail: torkisnasution@stmik-amik-riau.ac.id, adyanata@gmail.com

Abstrak : *Setiap gambar perlu diberikan tanda watermarking pada gambar. Adapun permasalahan yang ada pada saat ini adalah belum ada tanda yang dibubuhkan pada gambar milik kampus, sampai saat ini belum ada gambar yang di veriefied oleh manajemen, sehingga tidak diketahui gambar versi resmi dan yang tidak resmi. Gambar milik kampus potensial di salah gunakan untuk kepentingan pribadi, begitu juga rekayasa gambar sangat mudah dilakukan, sehingga dapat di manipulasi sesuai dengan keinginan pembuat. Permasalah tersebut perlu diberikan solusi, urgensi dari pemecahan masalah adalah dapat dijadikan sebagai media pengontrolan atas rekayasa gambar milik kampus, serta dapat dijadikan sebagai media promosi masif dan terstruktur. Permasalahan ini di ajukan untuk diselesaikan menggunakan watermark, yakni memberikan tanda air dan terlihat pada gambar dengan metoda Discrete Wavelet Tranformation. Adapun tahapan pemecahan masalah adalah gambar milik kampus di kumpulkan, selanjutnya dilakukan verifikasi gambar, dengan ruang lingkup internal kampus, selanjutnya gambar yang masuk dalam kategori branding image, dikumpulkan untuk diberi penandateks dengan tulisan STMIK Amik Riau kemudian nama asli gambar dan nama perubahan di rekam ke dalam database, sampai disini gambar sudah diberikan penanda. Setiap gambar yang beredar dapat dibedakan berdasarkan tanda air dengan status resmi atau tidak resmi.*

Kata Kunci: *citra digital, DWT, pengamana, watermark.*

PENDAHULUAN

Perkembangan teknologi dewasa ini membuat manusia ingi meningkatkan efektifitas dan efisiensi dengan teknologi digital. Sebagai contoh, dahulu mayoritas manusia apabila ingin mengambil gambar suatu objek masih menggunakan kamera analog, akan tetapi sekarang dapat menggunakan kamera digital, hasil pemoteratan dapat diolah, disimpan dan dikirim secara elektronik. Komputer mempunyai peran yang sangat besar dalam pengolahan data karena memiliki kemampuan komputasi tinggi, sehingga data yang diolah menjadi sebuah informasi. Dalam tatanan praktis gambar sering di jadikan objek manipulasi untuk kebutuhan tertentu. Hal ini sudah banyak terjadi dan kenyataan yang baru saja terjadi adalah foto Ketua Komisi Pemberantasan Korupsi [06] dibuat bermesraan dengan seorang wanita dengan hanya menggunakan pengolah gambar sederhan, dan ilmu pengetahuan yang tidak mesti harus seorang memiliki pendidikan tinggi. Dari fakta tersebut tergambar dengan jelas, diperlukan upaya perlindungan atas gambar yang dihasilkan baik dari kamera handphone, kamera statis, maupun video yang dinyatakan sebagai milik kampus STMIKAmik Riau.

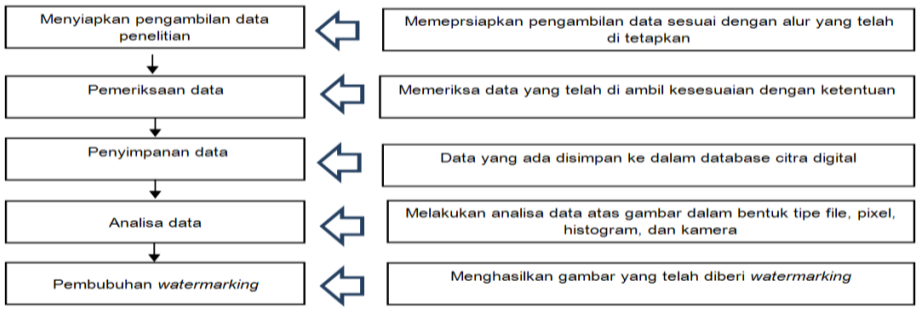
Upaya perlindungan terhadap hak cipta pada gambar perlu untuk di lakukan sebagai perlindungan institusi terhadap hak milik. Perlindungan tersebut dapat dilkaukan mulai dari menyimpan foto pada tempat yang aman, atau mengumpulkan seluruh foto untuk di seleksi manasaja yang dapat diberikan kepada masyarakat. Seluruh upaya tersebut pasti ada resiko dan keuntungan pada masing-masing pilihan. Namun demikian perlu dipikirkan suatu upaya yang tidak membatasi, namun memberikan dampak yang positip dalam posisi kampus yang akan tumbuh dan berkembang diantara pesaing.

Dari uraian diatas perlu di rumuskan suatu penyelesaian berupa bagaimana membuat aplikasi yang mampu memberikan pengamanan atas hak cipta pada gambar menggunakan watermarking dengan metoda *Discrete Wevelet Transform*. Bilamana rumusan tersebut di jawab melalui penelitian, maka akan diperoleh suatu aplikasi yang benar-benar memiliki kemapuan

untuk melindungi hak cipta pada gambar. STMIK Amik Riau dapat menggunakan sebagai media promosi atau mengenalkan kampus kepada khalayak ramai melalui tulisan yang terbuat pada gambar dalam bentuk *visible mark.*

PROSEDUR PENELITIAN

Tahapan penelitian yang dilakukan dapat dilihat pada gambar 2 dibawah ini. Penelitian didahului dengan menyiapkan data, pemeriksaan data, penyimpanan data, analisa data, dan menyimpulkan luas objek.

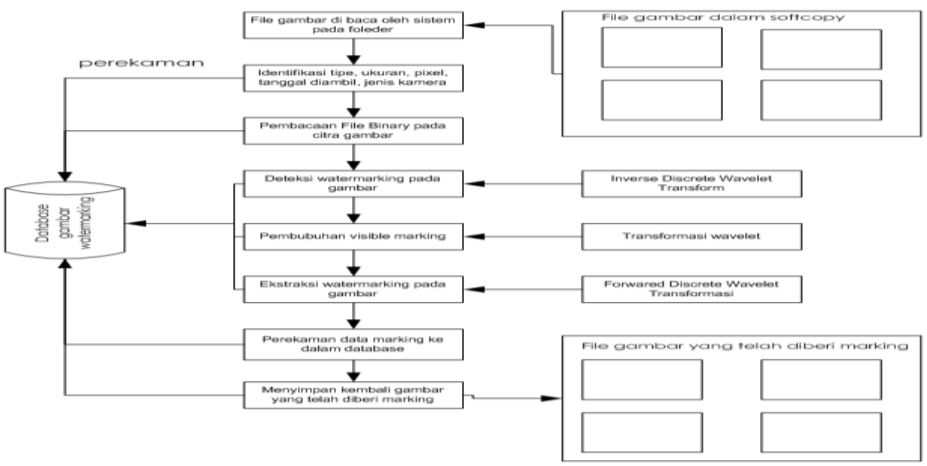


Gambar 1. Tahapan Penelitian

Penelitian ini konsentrasi pada pembuatan tanda air pada citra digital dengan cara memahami pixel untuk di hitung dan di sesuaikan dengan satuan centimeter. Berikut ini prosedur dalam rancangan penelitian :

1. Gambar yang di tangkap melalui kamera di kumpulkan pada media penyimpanan dalam bentuk soft file
2. Berdasarkan aturan yang berlaku, melakukan klasifikasi file, sekaligus menentukan teks yang akan di bubuhi dalam bentuk tanda air pada gambar
3. Sistem membaca atribut file gambar (tipe, ukuran, jenis file, histogram, tanggal pengambilan, jam, media yang digunakan)
4. Membaca file binary gambar, sebagai langkah awal untuk memberikan tanda air
5. Memeriksa, apakah file sudah pernah dibubuhi tanda air atau belum
6. Memberikan tanda air sesuai dengan teks yang telah ditentukan dan posisi yang tetapkan
7. Menguji file yang telah diberi tanda air, melalui ekstraksi tulisan yang terbubuhi pada file gambar tersebut.
8. Merekam tulisan yang dibubuhi pada file gambar pada database
9. Menyimpan kembali file yang telah diberi tanda air dengan nama file dan folder baru.

Semua hasil pada setiap tahapan di rekam pada database *watermarking*, sehingga dapat di sajikan informasi yang lengkap untuk setiap langkah untuk setiap percobaan. Setiap tahapan yang telah di jelaskan di atas dapat dilihat pada gambar di bawah ini.



Gambar 2. Bagan Alir Penelitian Penelitian

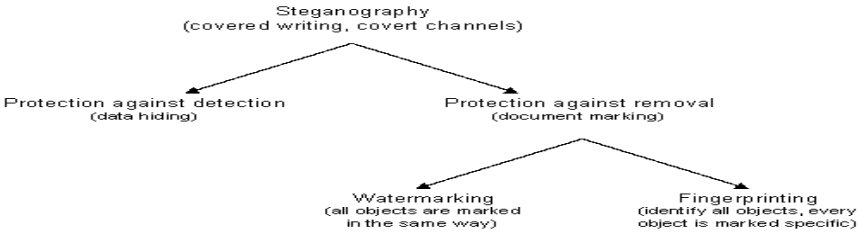
Hak Cipta

Hak cipta (lambang internasional: ©, Unicode: U+00A9) merupakan [03] kekayaan intelektual di bidang ilmu pengetahuan, seni, dan sastra yang mempunyai peranan strategis dalam mendukung pembangunan bangsa dan memajukan kesejahteraan sebagaimana diamanatkan oleh Undang-Undang Dasar Negara Republik Indonesia Tahun 945. Pemegang Hak Cipta untuk mengatur penggunaan hasil penuangan gagasan atau informasi tertentu. Pada dasarnya, hak cipta merupakan hak untuk menyalin suatu ciptaan. Hak cipta dapat juga memungkinkan pemegang hak tersebut untuk membatasi penggandaan tidak sah atas suatu ciptaan. Secara umum, hak cipta memiliki masa berlaku tertentu yang terbatas.

Berdasarkan Presiden Republik Indonesia, Undang-Undang Republik Indonesia Nomor 28 Tahun 2014 Tentang Hak Cipta, Hak cipta berlaku pada berbagai jenis karya seni atau karya cipta atau ciptaan. Ciptaan tersebut dapat mencakup puisi, drama, serta karya tulis lainnya, film, karya-karya koreografis (tari, balet, dan sebagainya), komposisi musik, rekaman suara, lukisan, gambar, patung, foto, perangkat lunak komputer, siaran radio dan televisi, dan (dalam yurisdiksi tertentu) desain industri. Hak cipta merupakan salah satu jenis hak kekayaan intelektual, namun hak cipta berbeda secara mencolok dari hak kekayaan intelektual lainnya (seperti paten, yang memberikan hak monopoli atas penggunaan invensi), karena hak cipta bukan merupakan hak monopoli untuk melakukan sesuatu, melainkan hak untuk mencegah orang lain yang melakukannya. Hukum yang mengatur hak cipta biasanya hanya mencakup ciptaan yang berupa perwujudan suatu gagasan tertentu dan tidak mencakup gagasan umum, konsep, fakta, gaya, atau teknik yang mungkin terwujud atau terwakili di dalam ciptaan tersebut. Sebagai contoh, hak cipta yang berkaitan dengan tokoh kartun Miki Tikus melarang pihak yang tidak berhak menyebarkan salinan kartun tersebut atau menciptakan karya yang meniru tokoh tikus tertentu ciptaan Walt Disney tersebut, namun tidak melarang penciptaan atau karya seni lain mengenai tokoh tikus secara umum.

Watermarking Citra Digital

Secara hierarkis, *watermarking* merupakan suatu proses yang berakar pada konsep ilmu *steganography*. *Steganography* sendiri sudah dikenal sejak jaman Mesir kuno. Menurut Cachin dalam [3], *steganography* diartikan sebagai suatu seni dan ilmu untuk menyembunyikan pesan yang sebenarnya sehingga orang awam tidak dapat mendeteksinya. Menurut Popa dalam [19], *steganography* dapat dibagi menjadi 2 (dua) bagian yaitu *protection against detection* (*data hiding*) dan *protection against removal* (*document marking*). *Watermarking* merupakan salah satu jenis dari *document marking*. Pembagian *steganography* dapat dilihat dalam gambar dibawah ini.



Gambar 2. Pembagian Steganograpi

Watermarking terhadap gambar (*image*) paling banyak dilakukan untuk melindungi gambar seperti foto. Saat ini cukup banyak teknik maupun algoritma *watermarking* terhadap gambar yang ditawarkan. Beberapa diantaranya sebagai berikut:

a. *Simple Watermarking*, Teknik ini merupakan teknik yang paling sederhana dimana *watermarking* dilakukan dengan menambahkan gambar atau teks tertentu pada gambar asli. Dan untuk mendapatkan gambar asli kembali, *watermark* yang ditambahkan dapat dibuang dengan teknik, tool dan keahlian tertentu. Gambar berikut ini merupakan contoh *watermarking* sederhana.

b. *Least Significant Bit Hiding (Image Hiding),* merupakan salah satu metode *watermarking* yang bekerja dalam mode warna *RGB (Red, Green, Blue)*. Metode ini bekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiap elemen *RGB*. Perubahan bit paling kanan hanya menimbulkan perubahan nilai *RGB* sebesar 1 dari 256 warna yang ada. Perubahan tersebut tidak dapat dideteksi dengan mata telanjang. Namun dengan komputer, misalnya menggunakan metode *Enhanced LSB*, dapat dideteksi dengan mudah apakah gambar mengandung *watermark* atau tidak. Metode *LSB* mudah untuk dideteksi karena penyisipan informasi dilakukan secara langsung dalam bit-bit dokumen tanpa melalui proses pengacakan.
c. *Hue Saturation Lightness (HSL),* Metode*watermarking* dengan HSL pada dasarnya mirip dengan metode *LSB*. Metode *HSL* bekerja pada mode warna *HSL* sedangkan metode *LSB* bekerja pada mode *RGB*. Evan dalam [10] mencoba memanfaatkan metode *HSL* ini untuk melakukan *watermarking* pada citra *bitmap*. Hasilnya metode *HSL* lebih baik dibanding metode *LSB*.
d. *Discrete Cosine Transformation (DCT),* sebelum dilakukan *encoding*, gambar asli dibagi terlebih dahulu menjadi beberapa bagian, misalnya matriks 8 x 8. Algoritma dalam teknik *DCT* ini selain digunakan untuk menyembunyikan informasi, juga digunakan untuk melakukan kompresi terhadap gambar, terutama yang bertipe *JPEG*. Menurut [14], teknik *DCT* memiliki kelebihan dalam optimasi dan kecepatannya.
e. *Discrete Wavelet Transformation (DWT),* teknik ini merupakan teknik yang lebih efektif dibanding *DCT*, dimana memiliki tingkat kompresi yang lebih tinggi.
f. *Independent Component Analysis (ICA),* prinsip dasar *independent component analysis (ICA)* dan penerapannya dalam *signal processing*. Saat ini ICA juga diterapkan dalam teknik *watermarking*, misalnya dalam [22], algoritma ICA diterapkan dalam blok dari *host image* dan *watermark image*. Di dalam [18] didiskusikan mengenai penerapan *blind content based watermarking* dengan memanfaatkan konsep ICA dan DCT. Hasilnya jauh lebih baik dan akurat dibanding teknik tanpa ICA, akan tetapi memiliki kelemahan dalam hal kecepatannya.
g. *Singular Value Decomposition (SVD),* pemanfaatan teknik *SVD* dalam *watermarking* dijelaskan dalam [4]. Teknik ini dapat digunakan untuk melakukan autentifikasi citra berdasarkan nilai korelasi *watermark* yang di-ekstrak. Teknik ini cukup *robust* terhadap beberapa pengolahan citra.
h. *Spread Spectrum Watermarking*, metode *spread spectrum watermarking* melakukan penyisipan dan pendeteksian *watermark* dalam ranah transform [20]. Mula-mula citra ditransformasikan ke dalam ranah frekuensi, lalu bit *watermark* disisipkan pada koefisien transformasi (misalnya koefisien *DCT*, *FFT*, *DWT*). Metode ini lebih *robust* terhadap gangguan atau serangan seperti kompresi, *cropping* dan *low pass filtering*.

Citra ditigalmerupakan suatu cara untuk menanamkan data *watermark* pada suatu gambar *host*. Gambar *host* dimodifikasi bersama-sama dengan citra *watermark* untuk menghasilkan gambar *stego*. Dalam proses ini, gambar *stego* akan mengalami *error* atau distorsi. Untuk meyakinkan sifat transparansi data *watermark* yang telah ditanam, jumlah distorsi citra yang terjadi pada proses *embedding* harus seminimal mungkin. Gambar *stego* kemudian didistribusikan dan mungkin disirkulasikan dari konsumen legal ke konsumen yang ilegal. Dengan demikian, akan terjadi bermacam-macam distorsi pada gambar. Distorsi gambar kemungkinan dihasilkan oleh proses kompresi gambar *lossy*, *re-sampling* atau serangan khusus pada data *watermark* yang telah ditanamkan.

Proses ekstraksi *watermark*, tergantung dari aplikasinya, memerlukan referensi gambar *host* untuk mengestimasikan data *watermark* pada gambar yang diterima. Citra *watermark* diperoleh dari gambar *stego*. Dalam proses ini dapat terjadi perbedaan antara citra *watermark* yang diuraikan dengan citra *watermark* asli. Proses *watermarking* yang baik akan meminimumkan perbedaan/*error* antara citra *watermark* yang diuraikan dengan citra *watermark* asli.

Karakteristik *Watermarking*

Ada beberapa karakteristik sistem *watermarking* seperti *robustness*, *tamper resistance*, *fidelity*, dan *computational cost*. Dimana setiap karakteristik tersebut terdapat *trade-off* diantaranya. Evaluasi terhadap karakteristik sistem *watermarking* tidak sama untuk semua aplikasi, sehingga pemilihan *trade-off* yang sesuai harus benar-benar dipertimbangkan berdasarkan aplikasi *watermarking*.

1. *Rebustness*, *watermark*harus *robust* artinya *watermark* di dalam data *host* harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti penkonversian dari digital ke analog dan dari analog ke digital, dan kompresi terutama kompresi *lossy*. Kadang-kadang sebuah *watermark* hanya tahan terhadap sebuah proses tetapi rentan terhadap proses yang lain. Tetapi untungnya dalam banyak aplikasi, ketahanan *watermark* terhadap semua proses yang mungkin tidak diperlukan dan dianggap terlalu berlebihan. Biasanya *watermark* harus tahan terhadap pemrosesan sinyal yang terjadi hanya antara proses *embedding* (penyembunyian *watermarking* dalam data) dan deteksi. Ukuran *robustness* terhadap proses tertentu yang diperlukan untuk aplikasi tertentu mungkin tidak diperlukan dalam aplikasi yang lain. Untuk menentukan ukuran *robustness* harus terlebih dahulu dipikirkan aplikasi apa yang akan menggunakan sistem *watermarking*.
2. *Tamper Resistance*, yaituketahanan sistem *watermarking* terhadap kemungkinan adanya serangan (*attack*) atau usaha untuk menghilangkan, merubah bahkan untuk memberikan *watermark* palsu terhadap suatu data *host*. Ada beberapa jenis serangan (*attack*) terhadap sistem *watermarking* :
   a. *Active attacks*. Merupakan serangan dimana seseorang berusaha untuk menghilangkan *watermark* yang terdapat di dalam data *host*.
   b. *Passive attacks*. Berbeda dengan *active attacks*, yang serangannya hanya ditujukan untuk mengetahui apa isi *watermark* tersebut, jika memang ada di dalam data *host*.
   c. *Collusion attacks*. Serangan ini merupakan usaha seseorang untuk menghasilkan sebuah *copy* dari data *host* yang tidak memiliki *watermark* dengan memanfaatkan beberapa data *host* yang memiliki berbagai *watermark*, seperti pada aplikasi *fingerprinting*. Serangan ini merupakan serangan khusus yang termasuk dalam *active attacks*.
   d. *Forgery attacks.* Serangan ini tidak hanya bertujuan untuk membaca atau menghilangkan *watermark* yang ada, tetapi juga menanamkan suatu *watermark* yang baru (tentunya yang valid) ke dalam suatu data *host*. Serangan ini cukup menjadi perhatian yang serius terutama untuk aplikasi bukti kepemilikan (*proof of ownership*)
3. *Fidelity*, salah satu*trade-off* antara karakteristik *watermarking* yang sangat kelihatan adalah antara *robustness* dengan *fidelity*. Dalam beberapa literatur *fidelity* kadang disebut dengan *invisibility* untuk jenis data citra dan video atau *inaudible* untuk data jenis suara. Yang dimaksud dengan *fidelity* di sini adalah derajat degradasi data *host* sesudah diberikan *watermark* dibandingkan dengan sebelum diberikan *watermark*. Biasanya bila *robustness* dari *watermark* tinggi maka memiliki *fidelity* yang rendah, sebaliknya *robustness* yang rendah dapat membuat *fidelity* yang tinggi. Jadi sebaiknya dipilih *trade-off* yang sesuai, sehingga keduanya dapat tercapai sesuai dengan tujuan aplikasi. Untuk data *host* yang berkualitas tinggi maka *fidelity* dituntut setinggi mungkin sehingga tidak merusak data aslinya, sedangkan data *host* yang memiliki *noise* (kualitas kurang) maka *fidelity*-nya bisa rendah seperti pada suara pada siaran radio, suara pada telepon ataupun *broadcast* acara televisi.
4. *Computational Cost*, ada beberapa aplikasi yang menuntut proses *watermarking* baik *embedding* maupun *extracting* bekerja secara *real time*, ada juga yang mengharapkan salah satu baik *extracting* atau *embedding* saja yang *real time* ataupun duanya boleh tidak *real time*. Contohnya untuk aplikasi *owner identification* atau *proof of ownership*, proses *watermarking* baik *embedding* maupun *extracting* tidak perlu *real time*, sedangkan untuk aplikasi *fingerprinting* pada service *video on demand*, maka proses *embedding watermark* harus dilakukan secara *real time*.

Transformasi *Wavelet* Diskrit

Transformasi Wavelet merupakan sebuah fungsi variabel riil t yang digunakan untuk melokalisasi suatu fungsi dalam ruang dan skala *L2(R)*, diberi notasi *ψ(t) sebagai mother wavelet*. *Doughter wavelet* $\psi_{a,b}(t)$ dihasilkan oleh parameter dilatasi a dan translasi/kontraksi b, yang dinyatakan dalam persamaan :

$$\psi_{a,b}(t) = a^{-1/2}\psi\left(\frac{t-b}{a}\right);\ a>0,\ b \in R$$

dengan :
a = parameter dilatasi atau kontraksi,
b = parameter translasi
R = mengkondisikan nilai a dan b dalam nilai *integer*

selanjutnya $W_{\psi}(f)(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} f(t)\ \psi\left(\frac{t-b}{a}\right) \mathrm{dt}$

dan formula *Calderon* memberikan:

$$f(t) = C_{\psi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \langle f, \psi_{a,b} \rangle\ \psi_{a,b}(t) a^{-2}\, dadb$$

Wavelet yang sering digunakan didefinisikan dengan fungsi *Haar* :

$$\psi(t) = \begin{cases} 1, & 0 \le t \le \frac{1}{2} \\ -1, & \frac{1}{2} \le t \le 1 \\ 0 & otherwise \end{cases}$$ dan

$$\psi_{j,k}(t) = a^{j/2}\psi\left(2^j t - k\right);\ j,k \in Z$$

dengan: j *integernonnegative*, $0 \le k \le 2^{j-1}$, 2^j = parameter dilatasi (parameter frekuensi atau skala), k = parameter waktu atau lokasi ruang dan Z = mengkondisikan nilai j dan k dalam nilai integer. Fungsi -fungsi diatas harus memenuhi kondisi $\int_{-\infty}^{\infty} \psi(t)\, dt = 0$, yang menjamin terpenuhinya sifat ortogonalitas vektor [01]. Pada dasarnya, transformasi *wavelet* dapat dibedakan menjadi dua tipe berdasarkan nilai parameter translasi dan dilatasinya, yaitu *Continue Wavelet Transform (CWT)* dan *Discrete Wavelet Transform (DWT)*. Transformasi *wavelet* kontinu ditentukan oleh nilai parameter dilatasi *(a)* dan translasi *(b)* yang bervariasi secara kontinu, dimana $a,b \in R$ dan $a \neq 0$. *Continue Wavelet Transform* (CWT) menganalisis sinyal dengan perubahan skala pada *window* yang dianalisis, pergeseran *window* dalam waktu dan perkalian sinyal serta mengintegral semuanya sepanjang waktu. Secara matematis dirumuskan sebagai :

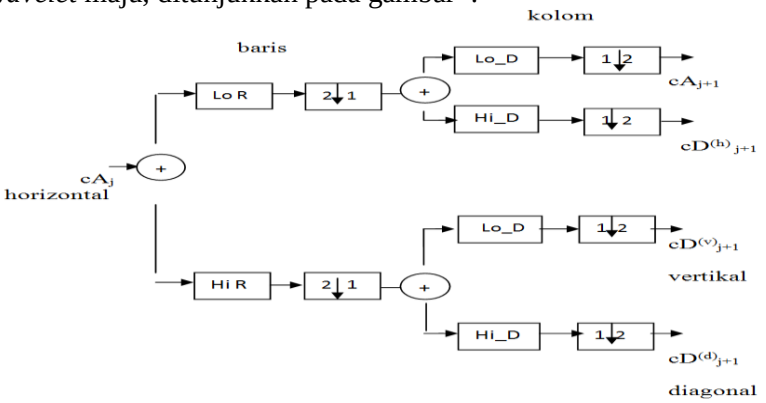
$$CWT(a,b) = \int f(t)\psi^{*}_{a,b}(t)dt$$

Transformasi *wavelet* diskrit bertujuan untuk mengurangi redundansi yang terjadi pada transformasi *wavelet* kontinu dengan cara mengambil nilai diskrit dari parameter *a* dan *b*. Transformasi *wavelet* diskrit menganalisa suatu sinyal dengan skala yang berbeda dan merepresentasikannya ke dalam skala waktu dengan menggunakan teknik *filtering* dimana sinyal dalam domain waktu dilewatkan ke dalam *High Pass Filter* dan *Low Pass Filter* untuk memisahkan komponen frekuensi tinggi dan frekuensi rendah, yakni menggunakan *filter* yang berbeda frekuensi *cut-off*-nya.

Transformasi *Wavelet* Diskrit Maju

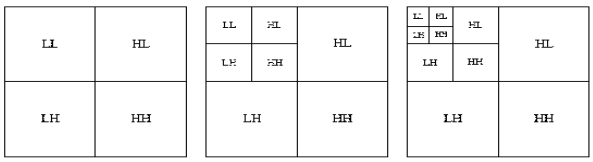
Discrete Wavelet Transform (DWT) dikelompokkan menjadi dua yaitu *DWT* maju dan *DWT* balik. Pada tahap *DWT* maju dilakukan proses dekomposisi data citra, yang dimulai dengan melakukan dekomposisi terhadap baris dari data citra yang diikuti dengan operasi

dekomposisi terhadap kolom pada koefisien citra keluaran dari tahap pertama. Cara kerja dari transformasi *wavelet* maju, ditunjukkan pada gambar :



Gambar 3. Gambar *Forward DWT* Dua Dimensi Skala Satu

Citra masukan diinterpretasikan sebagai sinyal, didekomposisi menggunakan *Lo_D* (*Low Pass Filter Decomposition*) dan *Hi_D(High Pass Filter Decomposition)* kemudian dilakukan *downsampling* dua. Keluaran berupa sinyal frekuensi rendah dan frekuensi tinggi. Kedua proses tersebut dilakukan sebanyak dua kali, terhadap baris dan terhadap kolom sehingga diperoleh empat subband keluaran yang berisi informasi frekuensi rendah dan informasi frekuensi tinggi. Koefisien aproksimasi mengandung informasi *background* danKoefisien detail, yaitu : detail horizontal, detail vertikal, dan detail diagonal yang mengandung informasi tepian. Dekomposisi transfomasi *wavelet*, ditunjukkan pada gambar :



a. Transformasi wavelet level 1, b. Transformasi wavelet level 2 dan c. Transformasi wavelet level 3

Gambar 4. Transformasi Wavelet

Transformasi *wavelet* level 2 didapatkan dengan membagi kembali *subband* residu pelolos rendah dari transformasi *wavelet* level 1 menjadi *subband-subband* yang lebih kecil dan seterusnya.

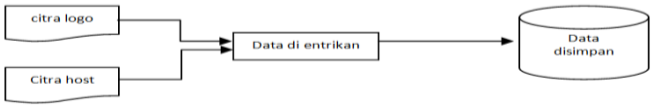
Transformasi *Wavelet* Diskrit Balik

DWT balik merupakan kebalikan dari *DWT* maju. Pada tahap ini dilakukan proses rekonstruksi dengan arah yang berlawanan dari proses sebelumnya, yaitu dengan proses *up-sampling* dan pem-*filter*-an dengan koefisien-koefisien filter balik. Proses *up-sampling* dilakukan dengan mengembalikan dan menggabungkan sinyal seperti semula. Proses ini dilakukan dengan menyisipkan sebuah kolom berharga nol di antara setiap kolom dan melakukan konvolusi pada setiap baris dengan *filter* satu dimensi. Hal yang sama dilakukan dengan menyisipkan sebuah baris nol di antara setiap baris dan melakukan konvolusi pada setiap kolom dengan *filter* yang lainnya. *Filter* yang digunakan pada transformasi balik (rekonstruksi) ini adalah *filter* yang mempunyai hubungan khusus terhadap *filter* pada sisi dekomposisi yaitu *filter Lo_R* (*Low Pass Filter Reconstruction*) dan *Hi_R (High Pass Filter Reconstruction)*.

Spesifikasi dan Alat

Penelitian ini membangun suatu program aplikasi yang digunakan untuk memberikan *watermark* pada suatu media citra digital, menguji *watermark* yang telah disisipkan, juga

memberikan perlakuan yang tidak normal kepada citra digital yang telah disisipi *watermark*. Aplikasi ini dapat membantu user untuk memberikan suatu label *watermark* terhadap gambar yang akan diproteksi, sekaligus memungkinkan user untuk menguraikan *watermark* yang telah disisipkan. Data dimasukkan oleh user adalah: citra host, citra logo. Berikut ini adalah proses yang terjadi bila digambarkan dalam sebuah diagram



Gambar 5. Data di entrikan oleh user

Pada aplikasi ini, terdapat seorang user yang dapat menggunakan sistem ini. User akan berinteraksi dengan sistem untuk melakukan proses *embedding watermarking*, memproses, dan memberikan serangan terhadap citra digital yang telah disisipi *watermark*

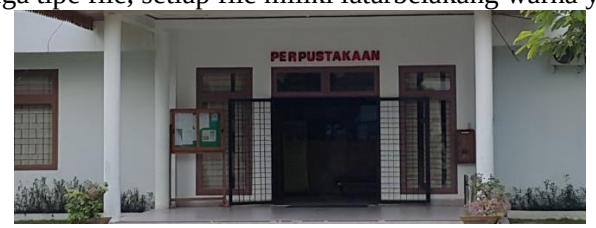
Spesifikasi Citra

Dalam pengujian program *watermarking* berkas citra digital dengan metode alihragam *Discrete Wavelet Transform* (*DWT*) digunakan berkas citra digital kedalaman piksel 24 bit, dan 8 bit warna.

Tabel 2. Daftar Ragam Citra *Host*

Nama File	Tipe File	Besar	Warna
Gambar-1-jpg	JPEG	254000	24 bit
Gambar-2-gif	GIF	867000	8 bit

Citra host terdiri atas tiga tipe file, setiap file miliki latarbelakang warna yang sama, yaitu putih.



Gambar 6. Citra *Host* yang digunakan

Citra logo yang digunakan adalah logo kampus STMIK Amik Riau, tiga tipe file dengan latar belakang file berwarna putih

Tabel 3. Daftar Ragam Citra Logo

Nama File	Tipe File	Besar	Warna
Logo-1-jpg	JPEG	254000	24 bit
Logo-2-gif	GIF	867000	8 bit
Logo-4-png	PNG	3366000	32 bit

Sementara itu, citra logo yang digunakan terdiri atas tiga tipe file, setiap file miliki latarbelakang warna yang sama, yaitu putih.

Gambar 7. Citra Logo

Pengujian

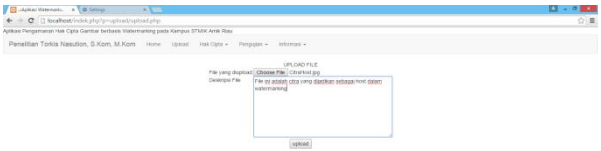
Pada penelitian ini menggunakan algoritma *watermarking* dalam kawasan *Discrete Wavelet Transform* (DWT). Algoritma *watermarking* harus dapat bertahan (*robust*) terhadap serangan-serangan yang berusaha membuang atau menghilangkan *watermark* dari citra watermark.

Antarmuka Aplikasi

Aplikasi di bangun menggunakan bahasa pemerograman PHP, dengan file pendukung *Javascript*, *Command Style Sheet* (*CSS*), dan *HTML*. Pada saat pertama aplikasi dijalankan terlihat tampilan sebagai berikut :

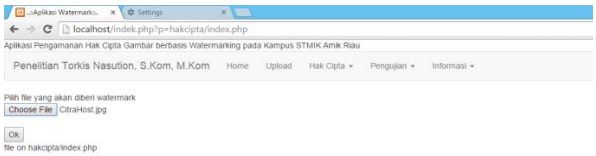
Gambar 8. Tampilan awal aplikasi

File yang akan dijadikan citra *host*, terlebih dahulu di *upload* selanjutnya file ini akan di baca pada saat pembubuhan *watermark.*



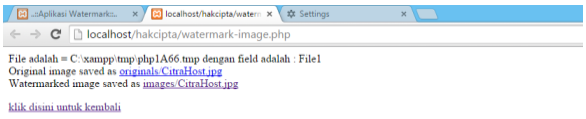
Gambar 9. *Upload* file citra *host*

Pada saat akan dibubuhi *watermark*, sistem memberikan pilihan untuk mencari kembali pada direktori yang berbeda. Selanjutnya, sistem akan memberikan watermark



Gambar 10. File Citra *Host* di *Upload*

Bila proses memberikan watermark pada citra host berhasil, maka akan terlihat tampilan berikut :



Gambar 11. Proses Menghasilkan Citra Watermarking

Untuk melihat hasil citra yang telah di bubuhi *watermark*, dapat di klik pada link images/ CitraHost.jpg

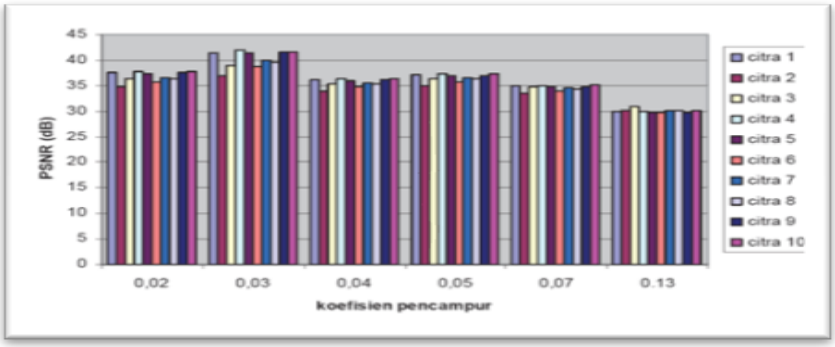
Gambar 12. Citra Watermarking pada sudut kanan bawah

Pada saat buat *histogram* maka terlihat gambar berikut

Gambar 13. *Histogram* citra *watermarking*

Pengaruh Koefisien Pencampur

Berikut ini merupakan hasil pengujian performansi system *Blind imagewatermarking* yang diujikan terhadap 10 buah citra dengan berbagai kategori. Untuk data *host* dan data digunakan ukuran 512 x 512 *pixel* sedangkan untuk jenis citra digunakan jenis citra (b).

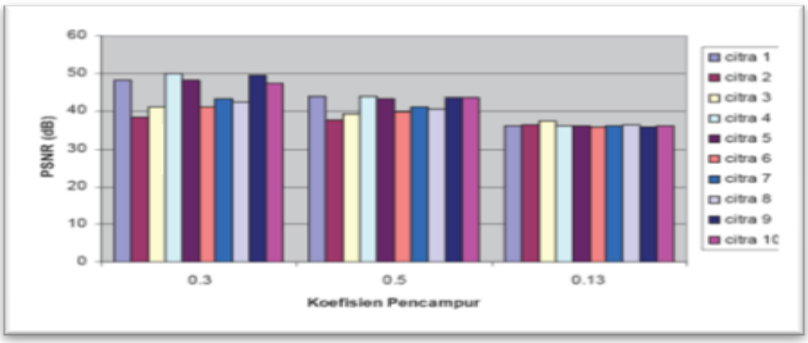


Gambar 14.Pengaruh koefisien pencampur terhadap PSNR

Berdasarkan gambar 16 diatas dapat diketahui bahwa performansi kualitas citra hasil *watermarking* dipengaruhi oleh koefisien pencampur yang diberikan. Terlihat penurunan nilai koefisien pencampur rata rata menaikkan kualitas dari citra watermark begitu juga menaikkan nilai koefisien akan menyebabkan turunnya kualitas citra *watermarking*. Untuk koefisien 0.03 yang menunjukkan performansi yang terbaik belum tentu dijadikan sebagai koefisien yang optimal karena harus diujikan terhadap ketahanan (*robustness*) watermark terhadap *attack* yang mungkin terjadi pada saat pengiriman sinyal.

Pengaruh Dimensi Citra Logo Terhadap Kualitas Citra *Watermarking*

Dalam simulasi ini proses pemberian watermarking hanya dapat dilakukan jika ukuran citra data memiliki ukuran maksimal sebesar dimensi dari citra *host*. Berikut ini merupakan hasil pengujian performansi watermarking untuk citra logo berukuran 256 x 256 *pixel*.



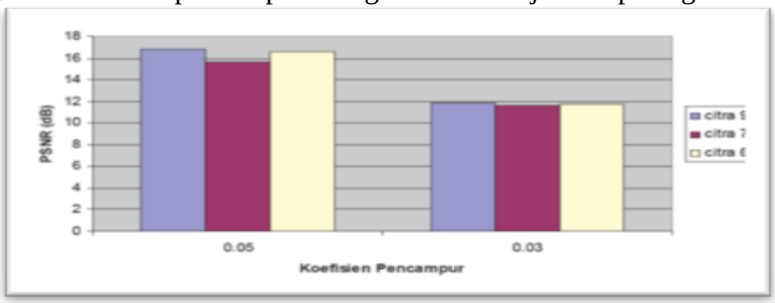
Gambar 15. Pengaruh ukuran citra terhadap kualitas citra hasil *watermarking*

Dapat dibandingkan dengan gambar 17 yang merupakan penanaman citra logo berukuran 512 x 512 *pixel*, pada gambar 17 terlihat peningkatan PSNR yang cukup signifikan dengan rata

rata peningkatan bisa mencapai 11.49 dB. Untuk koefisien 0.02 terjadi peningkatan rata-rata sebesar 13.21 dB, untuk koefisien 0.02 terjadi peningkatan rata-rata sebesar 10.06 dB dan untuk koefisien 0.13 terjadi peningkatan rata-rata sebesar 11.194. Namun penurunan dimensi citra data akan memiliki dampak pada ketahanan citra untuk bisa mendapatkan hasil ekstraksi yang baik.

Kinerja Sistem *Blind Image Watermarking* pada kompresi JPEG

Pengujian pertama kinerja sistem *Blind image watermarking* dilakukan dengan menggunakan proses kompresi JPEG yang memiliki sifat mengurangi sinyal pada *frekuensi high* pada citra *digital*. Berikut ini merupakan hasil pengujian obyektif terhadap tiga buah citra pada dua koefisien pencampur, dimana salah satunya memiliki nilai PSNR tertinggi dalam pengujian pengaruh koefisien pencampur sebagaimana ditunjukkan pada gambar 16

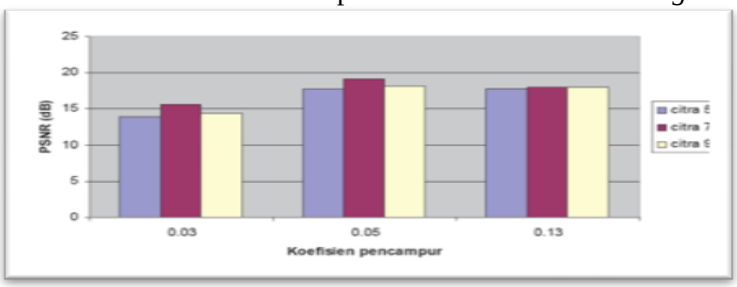


Gambar 16. Pengaruh kompresi 70% JPEG terhadap PSNR logo *watermark* dari tiga buah citra

Berdasarkan gambar 18 diatas dapat dilihat kemampuan *watermarking* untuk kofisien 0.05 lebih baik daripada koefisien 0.03 berdasarkan ketahanan dalam kompresi sinyal *JPEG*. Pengujian terhadap kualitas citra terhadap ketahanan dari kompresi JPEG juga akan dilakukan pada citra *watermarking* dengan citra logo yang sama namun format *file*-nya berbeda. Seperti pada kualitas citra hasil *watermarking*, citra ekstraksi pun tidak dipengaruhi oleh format citra logo yang ditanamkan. Meski sudah mengalami kompresi JPEG sebesar 70% kualitas citra ekstraksi untuk setiap format memiliki nilai PSNR (dB) yang mendekati serupa.

Kinerja Sistem *Blind Image Watermarking* Pada Gaussian *Noise*

Berikut ini merupakan pengaruh koefisien pencampur terhadap ketahanan citra logo setelah dikenakan derau. Pemberian derau dilakukan pada citra hasil *watermarking*.



Gambar 17. Pengaruh Koefisien Terhadap hasil Ekstraksi Citra Watermarking

Berdasarkan gambar 19 diatas dapat diketahui untuk ketahanan dalam *noise* koefisien 0.05 memiliki ketahanan yang paling baik pada ekstraksi citra setelah terkena *noise* uniform. Koefisien 0.05 memiliki keunggulan PSNR rata-rata 1.325 dibanding koefisien 0.13.

Pengujian Subyektif

Analisa subyektif dilakukan dengan menghitung nilai *MOS* (*Mean Opinion Score*) yaitu nilai yang menunjukkan tingkat penerimaan responden terhadap kualitas *image watermarking* serta kemampuan manusia untuk mengidentifikasi citra hasil ekstraksi. Dalam pengujian menggunakan responden sebanyak 2 orang dengan kriteria penilaian *MOS* untuk kualitas hasil *watermarking* adalah sebagai berikut :

a. Excelent : 5
b. Fine : 4
c. Passable : 3
d. Marginal : 2
e. Unuseable : 1

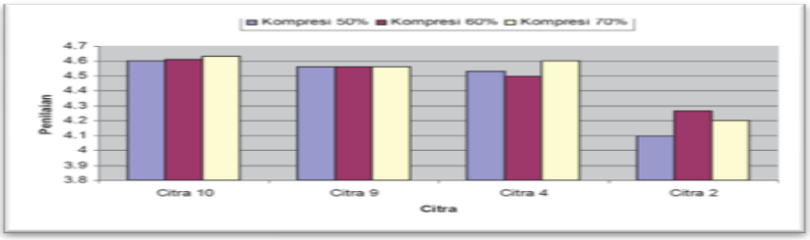
Sedangkan untuk kriteria penilaian *MOS* untuk authentifikasi dari citra ekstraksi adalah sebagai berikut :

a. Terbaca dengan jelas : 5
b. Terbaca dengan kurang jelas : 4
c. Terbaca tetapi tidak jelas : 3
d. Terlihat tetapi tidak terbaca : 2
e. Tidak terlihat dan tidak terbaca : 1

Penilaian subyektif terhadap kualitas citra *watermarking* adalah penilaian suatu citra berdasarkan penglihatan. Penilaian ini sangat tergantung pada persepsi penglihatan dari tiap responden. Untuk penilaian subyektif dilakukan untuk koefisien dengan nilai 0.05 Hal ini dilakukan berdasarkan hasil obyektif menunjukkan performansi yang paling baik.

Citra Hasil Ektraksi untuk Ketahanan Kompresi JPEG dalam Authentifikasi

Penilaian yang dilakukan adalah dengan melihat hasil kualitas citra hasil ektraksi. Besarnya nilai penilaian adalah dengan terbaca atau tidaknya citra huruf hasil ekstraksi. Grafik performansi *watermarking* setelah mengalami kompresi 50%, 60%, dan 70% ditunjukkan pada gambar berikut.

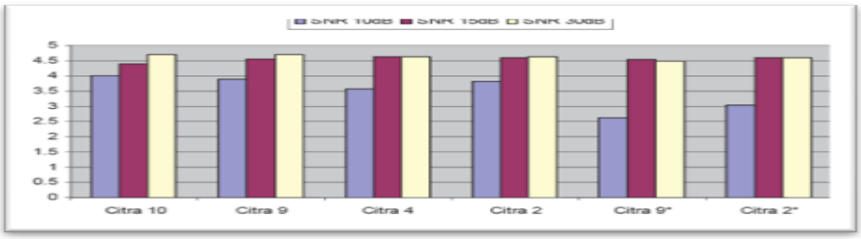


Gambar 18. Citra Hasil Ektraksi dalam Ketahanan Kompresi JPEG pada Authentifikasi

Seperti terlihat pada gambar 20 Citra Huruf pada citra hasil ekstraksi masih terbaca oleh responden meski dengan kurang jelas dan kualitas citranya tidak sempurna seperti sebelum ditanamkan dan mengalami kompresi. Hal ini masih bisa diterima untuk fungsi authentifikasi.

Citra Hasil Ektraksi setelah Penambahan Gaussian *Noise*

Pengujian selanjutnya dalam simulasi adalah melakukan penambahan *noise* yang mungkin diperoleh citra dalam perpindahan data. *Noise* yang diberikan disini adalah *Gaussiannoise* sehingga mempengaruhi semua frekuensi dalam sinyal. Pada Gambar 4.17 terlihat ketahanan citra watermarking meski SNR-nya mencapai 10 dB. Dengan rata-rata penilaian 3.85 menunjukkan untuk SNR 10 dB rata-rata responden masih dapat membaca rangkaian huruf pada citra meski tidak jelas. Namun untuk citra data yang memiliki ukuran lebih kecil dari citra data responden , citra hasil ekstraksi sudah mulai sulit terbaca. Untuk SNR lebih tinggi citra hasil ekstraksi tidak memiliki masalah untuk authentifikasi.



Gambar 19. Penilaian Citra Hasil Ektraksi Dalam Ketahanan Terhadap *Noise* Untuk Authentifikasi

Simpulan dan Saran

Setelah dilakukan pengujian program dalam bentuk training atas data, maka dapat di tarik kesimpulan Perbedaan warna latar belakang dari citra logo terhadap citra host yang sama memiliki pengaruh yang cukup besar terhadap performansi citra *watermarking*. Citra watermark yang memiliki warna yang sama dengan latar belakang citra host akan menghasilkan warna yang sangat baik dari segi persepsi manusia. Sementara warna yang berbeda antara citra host dengan citra watermark akan menimbulkan warna yang kacau. Ukuran citra logo yang akan ditanamkan pada citra asli memiliki ukuran dimensi maksimum sama dengan citra asli. Sehingga tidak dapat memberikan citra *watermak* dengan ukuran yang melebihi citra host. Dalam pengujian membuktikan bahwa perbedaan format file citra logo tidak memiliki pengaruh yang berarti terhadap peformansi watermarking karena citra watermarking sehingga secara sembarang citra watermark yang dijadikan watermark pada citra host akan mengikuti tipe file gambar pada citra *host*. Metode *Blind Watermarking* dengan menggunakan *Wavelet* tidak terlalu baik untuk serangan sinyal yang bersifat geometris, seperti *resize image* dan *rotasi image*. *Disamping itu juga d*alam upaya pemanfaatan gambar terhadap media promosi tidak begitu baik untuk digunakan. Pengujian juga membuktikan bahwa Penambahan *watermark* ke dalam citra ter-*watermarking* akan penyebabkan penurunan kualitas citra *watermarking*. Hal ini dapat dilihat pada saat pengujian dengan latar belakang warna yang berbeda antara citra *watermark* dengan citra *host* dengan menghasilkan gambar citra *watermarking*. Penilaian secara subyektif, skema *watermarking* ini menunjukkan kualitas *fine* yaitu citra memiliki kualitas yang tinggi, enak dilihat tanpa adanya gangguan-gangguan yang berarti. Disamping itu, Untuk metode *blind watermarking* pada simulasi ini diperoleh nilai 0.05 sebagai koefisien pencampur yang paling optimal, karena meski tidak memberikan hasil citra hasil *watermarking* yang terbaik, namun memiliki ketahanan terhadap *attack* paling baik untuk fungsi authentifikasi hak cipta. Dengan metode *blind watermarking* PSNR rata-rata untuk citra hasil *watermarking* mencapai 40.01267 dB untuk citra logo dengan ukuran setengah dari citra *decoy*, dan 35.2255 dB untuk citra logo yang memiliki ukuran sama dengan citra *decoy*.

Beberapa hal yang disarankan untuk dilakukan penelitian di masa mendatang, peningkatan Kinerja sistem *blind image watermarking* wavelet dapat ditingkatkan dengan dukungan terhadap ekstraksi terhadap citra logo dengan citra *host*. Sehingga gambar yang asli (citra *host*) dan citra *watermark* dapat di peroleh tanpa mengurangi nilai keaslian masing-masing. Untuk mendapatkan perlindungan yang terbaik setiap citra logo, citra *host*, maupun citra *watermarking* seluruh atribut disimpan dalam database, hal ini diperlukan untuk menghindari terjadi upaya pembajakan dengan menggunakan *software* aplikatif, dengan tersimpannya data dalam database memungkinkan untuk dilakukan kalibrasi. Disamping itu, penelitian tentang audio dan video *watermarking* menggunakan teknik *blind* untuk ektraksinya.

DAFTAR PUSTAKA

[1] Bhupendra Ram, Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform, International Journal of Advancements in Research & Technology, ISSN 2278-7763, Volume 2, Issue4, April-2013

[2] Kuntadi Widiyoko1, Iwan Setyawan, Perbandingan Penggunaan Mean Lokal, Median Lokal dan Invarians Statistik Koefisien DCT dalam Perancangan *Image Hashing* Techné Jurnal Ilmiah Elektroteknika Vol. 13 No. 2 Oktober 2014 Hal 205 – 212

[3] Merlin Felyana, Watermarking Video Menggunakan Transformasi Wavelet Diskrit, Jurnal Generic, Vol. 8, No. 1, pp. 198~208, ISSN: 1907-4093 (Print), 2087-9814 (online), Maret 2013

[4] Pallavi Patil, D.S. Bormane, DWT Based Invisible Watermarking Technique for Digital Images, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[5] Timmy Gupta, Image Watermarking Usingdiscrete Wavelet Transform, International Journal of Data & Network Security, www.ijdnsonline.com ISSN 2319-1236, Volume 1 No.2, October, 2012

[6] Reena Anju, Vandana, Modified Algorithm for Digital Image Watermarking Using Combined DCT and DWT, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 7 (2013), pp. 691-700, 2013

[7] Rinaldi Munir, Image Watermarking untuk Citra Berwarna dengan Metode Berbasis Korelasi dalam Ranah DCT, Program Studi Teknik Informatika ITB Sekolah Teknik Elektro dan Informatika ITB, JURNAL PETIR VOL. 3 NO. 1 JANUARI 2010

[8] Vijaya K. Ahire, Vivek Kshirsagar, Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011

[9] Abdul Kadir, Dasar Pengolahan Citra dengan Delphi, Andi Offset, Yogyakarta, 2013

[10] Presiden Republik Indonesia, Undang-Undang Republik Indonesia Nomor 28 Tahun 2014 Tentang Hak Cipta

[11] Presiden Republik Indonesia, Peraturan perundang - undangan, Undang Undang Republik Indonesia No.19 Tahun 2002 Tentang Hak Cipta.