

# Perlindungan Hak Cipta Gambar dengan *Watermarking* menggunakan Metoda *Discrete Wavelet Transform*

Torkis Nasution

Program Studi Teknik Informatika, STMIK Amik Riau

torkisnasution@stmik-amik-riau.ac.id

## 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 (pimpinan), 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 Transformation*. 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 penanda teks 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, pengamanan, watermark

## 1. Pendahuluan

Perkembangan teknologi dewasa ini membuat manusia ingin 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 pemotretan 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 sederhana, 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 STMIK Amik Riau.

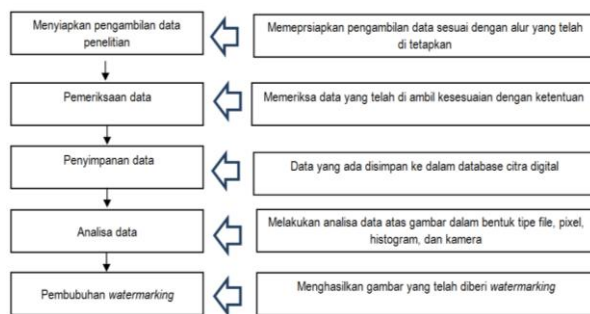
Upaya perlindungan terhadap hak cipta pada gambar perlu untuk di lakukan sebagai perlindungan institusi terhadap hak milik. Perlindungan tersebut dapat dilkauan mulai dari menyimpan foto pada tempat yang aman, atau mengumpulkan seluruh foto untuk di seleksi manasaja yang dapat diberikan kepada masyarakat. 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 positif 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 kemampuan 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*.

## 2. 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.

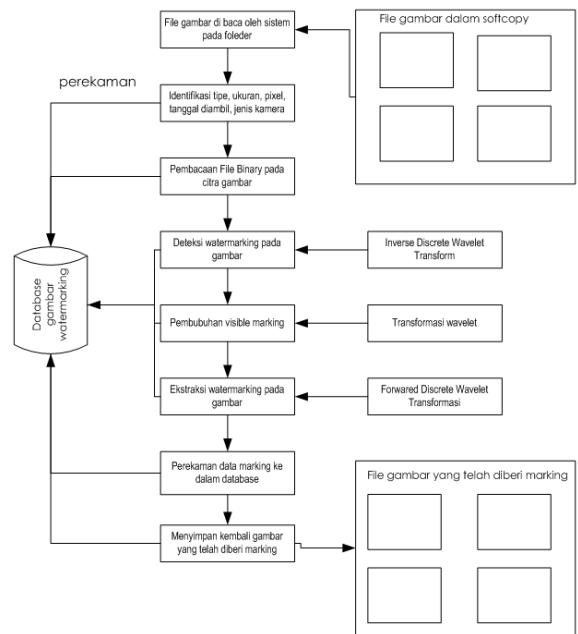


**Gambar 1. Tahapan penelitian**

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 ditetapkan
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**

### 3. Penelitian sebelumnya

Beberapa penelitian yang pernah dilakukan terkait dengan perlindungan hak cipta menggunakan watermark menggunakan metoda *Discrete Wavelet Transform*, diantaranya dilakukan oleh Merlin Felyana [03], yang meneliti tentang watermark dengan judul *Watermarking Video Menggunakan Transformasi Wavelet Diskrit*, pelayanan citra watermark di sisipkan ke dalam video. Tujuan dari penyisipan ini adalah untuk memberikan tanda ke aslian sehingga dapat meminimalkan upaya pembajakan atas kepemilikan. Disamping peneliti tersebut, juga Pallavi Patil, D.S. Bormane [04] melakukan penelitian watermarking menggunakan DWT dengan judul *DWT Based Invisible Watermarking Technique for Digital Images*. Penelitian ini fokus pada sistem steganografi membahas dua hal, yaitu kualitas *stego-image* dan kapasitas yang dapat ditampung oleh citra host. Penyisipan data dengan cara *lossles* di representasikan pada besaran koefisien discrete wavelet transform dalam pesan yang disembunyikan. Dengan menggunakan konsep DWT, akan di masukkan pesan ke dalam citra host dengan tidak menggunakan nilai koefisien pada setiap konstruksi untuk 3-level 2-D. dalam penelitian ini juga membahas bagaimana memasukkan pesan dan meng-ekstrak dari citra host. Gambar asli dapat di peroleh setelah pesan di ekstrak kembali.

Sementara penelitian *watermarking* yang telah dilakukan Timmy Gupta [05] menyimpulkan bahwa penerapan empat tipe algoritma spasial, DCT, DWT, dan spektrum dapat menghasilkan citra *watermarking* yang tahan atas kompresi dan *noise*, disamping itu juga dapat meng-ekstraksi kembali citra *watermark*. Reena Anju, Vandana [06] menyatakan *watermark* pada citra *host* mengidentifikasi informasi yang termuat dalam sebuah citra, dalam beberapa algoritma sangat sulit untuk di buang. Dalam pembahasan ini, *wavelet transform* telah memiliki kemampuan untuk mengenali lebih baik citra *watermarking*. Jika karakter ini di kombinasikan dengan DWT akan dapat transpransi citra *digital watermark*. Dalam penelitian ini akan menggunakan pendekatan algoritma DCT dan DWT sebagai algoritma. Pada algoritma ini, informasi citra *watermark* yang telah melewati algoritma DCT di letakkan pada frekwensi tinggi pada citra *host*. Citra *watermarking* di evaluasi menggunakan PSNR, *normalized correlation* dan waktu perhitungan. Hasil evaluasi menampilkan hasil kombinasi dua transform bekerja dengan baik dan efisien. Penyisipan teks berada pada tingkat bit, sebagaimana disampaikan Merlin Felyana [03] bahwa *watermarking* video bertujuan membantu untuk menentukan hak otentikasi terhadap suatu video. *Watermarking* dilakukan dengan penyisipan citra biner terhadap suatu video dengan format MPEG1 kemudian melakukan ekstraksi terhadap *watermark* video. *Transformasi wavelet diskrit* (TWD) digunakan sebagai proses penyisipan citra terhadap suatu video dan proses ekstraksi terhadap *watermark* video. Analisis kualitas *watermark* video dapat diketahui dengan melakukan perhitungan *peak signal to noise ratio* (PSNR). Hasil eksperimen menunjukkan bahwa 100% *watermark* video tidak mengalami perubahan dari video asli, serta citra biner memiliki hasil terbaik untuk digunakan sebagai citra sisipan dibandingkan dengan citra berwarna.

Gambar yang telah disisipi pesan dapat di ekstrak kembali sebagaimana disampaikan Reena Anju, Vandana [04] pada sistem steganografi membahas dua hal, yaitu kualitas *stego-image* dan kapasitas yang dapat ditampung oleh citra *host*. Penyisipan data dengan cara *lossles* di representasikan pada besaran koefisien *discrete wavelet transform* dalam pesan yang disembunyikan. Dengan menggunakan konsep DWT, akan di masukkan pesan ke dalam citra *host* dengan tidak menggunakan nilai koefisien pada setiap konstruksi untuk 3-level 2-D. dalam penelitian ini juga membahas bagaimana memasukkan pesan dan meng-ekstrak dari citra *host*. Gambar asli dapat di peroleh setelah pesan di ekstrak kembali.

*Watermarking digital* merupakan solusi terbaik dalam melindungi *content digital* sebagaimana di sampaikan Bhupendra Ram [01] menyatakan informasi yang dimuat di dalam *watermark* adalah pemilik, pembuat, distributor, dan waktu. Dalam penelitian ini

di perkenalkan teknik baru untuk menambahkan *watermark* ke citra *host*. Metoda ini mengoperasikan frekwensi domain pesan melalui *pseudo-random* bilangan *real* untuk memilih koefisien DCT. *Watermark* akan memilih nilai koefisien dan menyisipkan pada citra *host* dengan memilih nilai memiliki warna kuat. Cara ini menjamin *watermark* tidak dapat di hapus. Dalam penelitian Kuntadi Widiyoko<sup>1</sup>, Iwan Setyawan [05] menyatakan bahwa *watermarking* dapat digunakan untuk melindungi hak cipta secara hukum. Untuk membuktikan kepemilikan dan melindunginya, diperlukan menyisipkan informasi secara aman dari upaya fake sehingga harus di cari lokasi secara tidak sama di dalam citra *host*. *Watermarking* dapat digunakan pada objek multimedia untuk mendeteksi dan meng-ekstrak informasi. dalam informasi dapat memuat identitas pembeli, pembuat, waktu, dan lain Untuk itu, dapat di sisip informasi visible dan invisible. Ada empat tipe dalam algoritma *watermarking*, yaitu : spasial, DCT, DWT, dan spektrum. Dalam penelitian menggunakan teknik *wavelet transform*.

Penggunaan hashing dalam *watermark* meningkatkan ketahanan gambar, sebagaimana di sampaikan Kuntadi Widiyoko, Iwan Setyawan [02] menyatakan sistem *image hashing* dengan berbagai tipe. Tipe 1 merupakan sistem *image hashing* yang cara kerjanya membandingkan nilai *mean* citra dengan *mean* tiap blok dalam citra tersebut. Tipe 2 adalah sistem *image hashing* yang membandingkan nilai median citra dengan median tiap blok. Tipe 3 merupakan sistem *image hashing* yang membandingkan nilai *mean* sebuah blok dengan blok selanjutnya dalam 1 citra. Tipe 4 adalah pengembangan tipe 3, yaitu dengan terlebih dahulu mengacak blok-blok citra. Tipe 5 adalah *image hashing* yang membandingkan nilai-nilai koefisien DCT tiap blok. Kinerja kelima tipe tersebut diuji dari sisi ketahanannya dalam menghadapi gangguan seperti kompresi JPEG, *sharpening*, *histogram equalization* dan *low pass filtering*.

Penggabungan dua metoda akan meningkatkan keamanan data yang dilindungi sebagaimana disampaikan Vijaya K. Ahire, Vivek Kshirsagar [08], menyatakan citra *host* di urai pada tiga level menggunakan DWT. DCT menyeleksi blok koefisien sub band DWT pada masing-masing sub band yang dipilih. Untuk menyisipkan informasi (dalam bentuk bit) menyesuaikan dengan angka random yang akan di tambah ke dalam frekwensi koefisien tengah pada blok DCT. Untuk mengekstrak *watermarking* menggunakan prosedur yang sama. Hubungan antara koefisien *mid-band* dan angka random adalah menghitung bit informasi yang disisip. Implementasi algoritma ini mudah dan tahan terhadap serangan.

Teknologi *watermarking* dapat menjaga keaslian gambar, masyarakat akan memperoleh gambar yang

merupakan versi resmi dari institusi. Citra *watermark* yang *visible* dapat dilihat secara langsung, akan mendorong tekat dari masyarakat untuk lebih selektif terhadap sumber dan gambar yang di terima. Dampak lebih jauh yang bisa didapatkan selain informasi yang benar dan sumber yang tepat, juga dapat meningkatkan citra institusi di masyarakat. Secara umum penelitian berbasis *watermarking* dengan metoada DWT menyimpulkan :

1. Melindungi hak cipta atas gambar sehingga masyarakat memperoleh gambar yang asli juga dari sumber yang benar.
2. Penggunaan metoda secara serial akan lebih bagus terhadap ketahanan gambar terhadap kompresi dan noise.
3. Selain gambar dapat juga di implementasikan terhadap *audio*, *video*, dan teks

Dari beberapa penelitian diatas belum ada yang melaksanakan penelitian tentang aplikasi watermark dalam penggunaan untuk gambar pada organisasi, penelitian bidang *watermark* masih dalam tatanan konsep, algoritma, dan teknik. Sementara dalam penelitian aplikatif masih bersifat normatif dan teoritis, belum di ujikan secara nyata. Hal ini dibuktikan dengan belum adanya data yang disajikan atas tingkat efisiensi dan efektifitas. Oleh karena itu penelitian ini akan meneliti tentang Aplikasi Pengamanan Hak Cipta Gambar dengan *Watermarking* menggunakan Metoda *Discrete Wavelet Transform* pada Kampus STMIK Amik Riau

#### 4. Hak Cipta

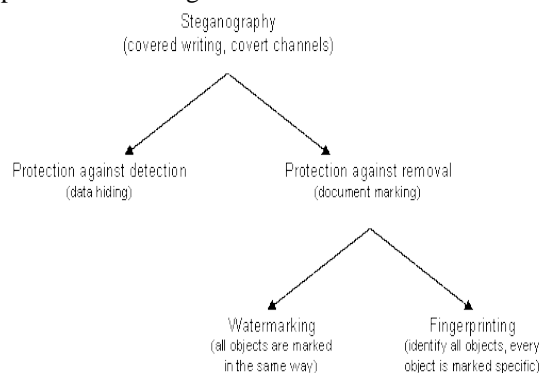
Hak cipta (lambang internasional: ©, Unicode: U+00A9) merupakan [03] kekayaan intelektual di bidang ilmu pengetahuan, seni, dan sastra yang mempunyai peranan strategis dalam mendukung pembangunan bangsa dan memajukan kesejahteraan sebagaimana diamanatkan oleh Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pemegang Hak Cipta untuk mengatur penggunaan hasil penguasaan gagasan atau informasi tertentu. Pada dasarnya, hak cipta merupakan hak untuk menyalin suatu ciptaan. Hak cipta dapat juga memungkinkan pemegang hak tersebut untuk membatasi penggunaan 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.

#### 5. 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 Steganografi**

*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 digital merupakan 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 mengestimasi 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.

Tabel 1. Istilah proses watermarking citra digital

Istilah	Keterangan
Gambar host	Gambar asli yang akan disisipi pesan hak cipta/signature
Citra watermark	Citra yang berupa pesan hak cipta/signature
Gambar stego	Gambar host yang telah disisipi dengan pesan hak cipta/signature
Embedding	Proses penyisipan citra watermark dalam citra host
Ekstraksi	Proses penguraian citra watermark atas citra stego

Watermarking dapat diklasifikasikan berdasarkan beberapa hal. Berdasarkan media penyembunyian data, watermarking dapat diklasifikasikan menjadi image, audio, video, text. Berdasarkan bisa atau tidaknya

dirasakan oleh indra manusia, *watermarking* dapat diklasifikasikan menjadi (1) *Visible Watermarking*: *watermarking* dapat dirasakan oleh indra manusia; (2) *Invisible Watermarking*: *watermarking* tidak dapat dirasakan oleh indra manusia. Berdasarkan kebutuhan terhadap data asal pada saat verifikasi, *watermarking* dapat diklasifikasikan menjadi (1) *Blind Watermarking*: proses verifikasi tidak membutuhkan data asal; (2) *Nonblind Watermarking*: proses verifikasi membutuhkan data asal.

Berdasarkan bisa atau tidaknya dirasakan oleh indra manusia, *watermarking* dapat diklasifikasikan menjadi (1) *Visible Watermarking*: *watermarking* dapat dirasakan oleh indra manusia; (2) *Invisible Watermarking*: *watermarking* tidak dapat dirasakan oleh indra manusia. Berdasarkan kebutuhan terhadap data asal pada saat verifikasi, *watermarking* dapat diklasifikasikan menjadi (1) *Blind Watermarking*: proses verifikasi tidak membutuhkan data asal; (2) *Nonblind Watermarking*: proses verifikasi membutuhkan data asal. Berdasarkan metode yang digunakan, *watermarking video* dapat diklasifikasikan menjadi:

1. *Spatial Domain Method*: Metode ini bekerja pada kawasan spasial. Secara umum metode ini rentan terhadap proses kompresi, transmisi dan *encoding*. Beberapa teknik algoritma yang termasuk ke dalam metode ini adalah: *Least Significant Bit Modification*, *Correlation-based Techniques*, *m-frame*, *spread spectrum*.
2. *Frequency Domain Method*: Metode ini bekerja pada domain frekuensi. Beberapa teknik algoritma yang termasuk ke dalam metode ini adalah: *Discrete Cosine Transform (DCT)*, *Discrete Wavelet Transform (DWT)*, *Discrete Fourier Transform (DFT)*, *Radon Transform*.
3. *MPEG Coding Structured Based Method*: Beberapa teknik algoritma yang termasuk ke dalam metode ini adalah: *MPEG-4 object-based*, *MPEG-2 blocked-based*.

Berdasarkan kegunaannya, *watermarking* dapat diklasifikasikan menjadi:

1. *Watermarking untuk Broadcast Monitoring*: *Watermarking* yang digunakan dalam *broadcast monitoring* dengan menambahkan *watermark* yang unik kedalam tiap video ataupun suara sebelum ditayangkan oleh stasiun televisi atau disiarkan oleh stasiun radio.
2. *Watermarking untuk Copy Control*: *Watermarking* yang disertai dengan *watermarking detector*, yang berfungsi untuk mendeteksi ada tidaknya data *watermark* di dalam file, jika ada maka beberapa proses yang akan dilakukan untuk *hardware* tersebut akan di-*disable*.
3. *Watermarking untuk Owner Identification*: *Watermarking* yang disisipkan ke dalam data *host* dan merupakan bagian dari data *host* tersebut.

Sehingga usaha untuk menghilangkan *watermark* tersebut akan mengurangi kualitas dari data *host*.

4. *Watermarking untuk Proof of Ownership*: *Watermarking* yang berfungsi sebagai pembuktian kepemilikan.
5. *Watermarking untuk Authentication*: *Watermarking* di mana data *watermark* digabungkan dengan data *host*, sehingga kemanapun data tersebut, baik di-*cropping*, diubah ke dalam format digital lain, dan sebagainya, *watermark*-nya tetap akan ada bersama dengan data *host*.
6. *Watermarking untuk Fingerprinting*: *Watermarking* dengan menyembunyikan informasi *watermark* yang berbeda-beda kepada tiap data digital yang didistribusikan.

*Watermarking untuk Covert Communication*: *Watermarking* yang digunakan sebagai media untuk mengirimkan pesan-pesan rahasia. Aplikasi *watermarking* ini juga disebut *data hiding*.

## 6. Transformasi Wavelet Diskrit

*Transformasi Wavelet* merupakan sebuah fungsi variabel riil  $t$  yang digunakan untuk melokalisasi suatu fungsi dalam ruang dan skala  $L_2(R)$ , diberi notasi  $\psi(t)$  sebagai *mother wavelet*. *Daughter 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

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

dan formula *Calderon* memberikan:

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

*Wavelet* yang sering digunakan didefinisikan dengan fungsi *Haar* :

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

$$\Psi_{j,k}(t) = a^{j/2} \Psi(2^j t - k); j, k \in Z$$

dengan:  $j$  integer nonnegative,  $0 \leq k \leq 2^j - 1$ ,  $2^j$  = 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 mengintegrasikan 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.

## 8. 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

### 8.1. 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 memiliki 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 memiliki latarbelakang warna yang sama, yaitu putih.



Gambar 7. Citra Logo

### 9. 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.

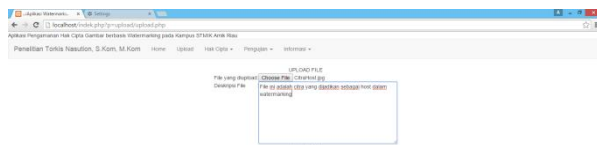
#### 9.1. Antarmuka Aplikasi

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



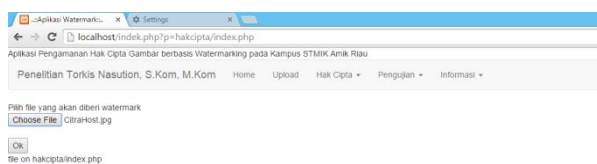
Gambar 8. Tampilan awal aplikasi

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



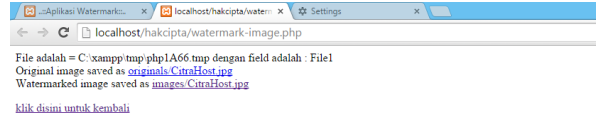
Gambar 9. Upload file citra host

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

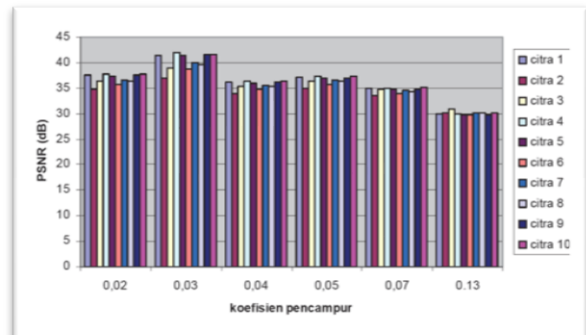
Pada saat buat *histogram* maka terlihat gambar berikut



Gambar 13. Histogram citra watermarking

#### 9.2. Pengaruh Koefisien Pencampur

Berikut ini merupakan hasil pengujian performansi system *Blind image watermarking* 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).



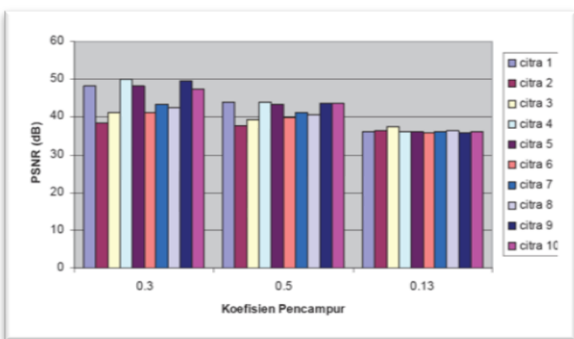
Gambar 14. Pengaruh koefisien pencampur terhadap PSNR



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.

**9.3. 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*.



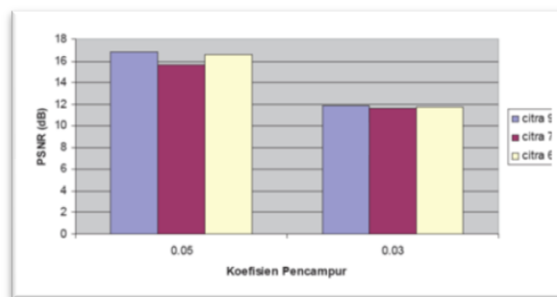
**Gambar 15. Pengaruh ukuran citra terhadap kualitas citra hasil watermarking**

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.

**9.4. 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

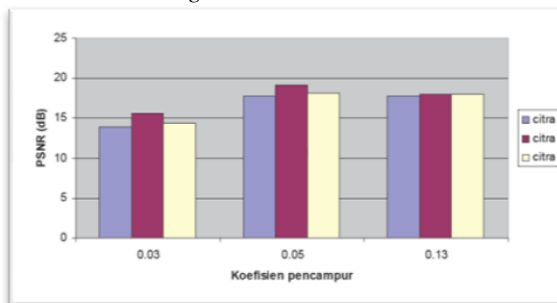


**Gambar 16. Pengaruh kompresi 70% JPEG terhadap PSNR logo watermark dari tiga buah citra**

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.

**9.5. 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.

## 9.6. 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 :

- Excelent : 5
- Fine : 4
- Passable : 3
- Marginal : 2
- Unuseable : 1

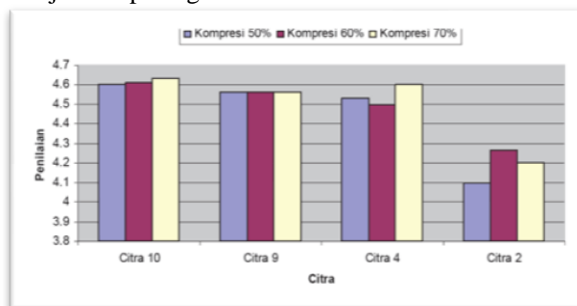
Sedangkan untuk kriteria penilaian *MOS* untuk autentifikasi dari citra ekstraksi adalah sebagai berikut :

- Terbaca dengan jelas : 5
- Terbaca dengan kurang jelas : 4
- Terbaca tetapi tidak jelas : 3
- Terlihat tetapi tidak terbaca : 2
- 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.

## 9.7. Citra Hasil Ekstraksi untuk Ketahanan Kompresi JPEG dalam Autentifikasi

Penilaian yang dilakukan adalah dengan melihat hasil kualitas citra hasil ekstraksi. 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.

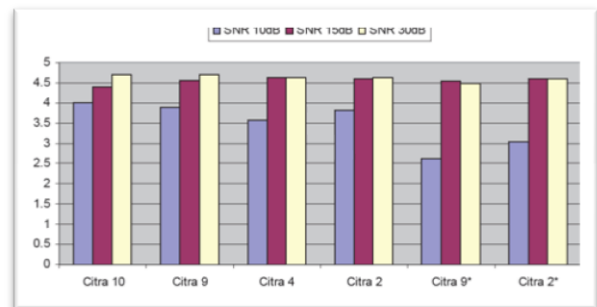


Gambar 18. Citra Hasil Ekstraksi dalam Ketahanan Kompresi JPEG pada Autentifikasi

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 autentifikasi.

## 9.8. Citra Hasil Ekstraksi setelah Penambahan Gaussian Noise

Pengujian selanjutnya dalam simulasi adalah melakukan penambahan *noise* yang mungkin diperoleh citra dalam perpindahan data. *Noise* yang diberikan disini adalah *Gaussian noise* 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 autentifikasi.



Gambar 19. Penilaian Citra Hasil Ekstraksi Dalam Ketahanan Terhadap Noise Untuk Autentifikasi

## 10. Kesimpulan

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 *watermark* dengan ukuran yang melebihi citra host. Dalam pengujian membuktikan bahwa perbedaan format file citra logo tidak memiliki pengaruh yang berarti terhadap performansi *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 dalam upaya pemanfaatan gambar terhadap media promosi tidak begitu baik untuk digunakan. Pengujian juga membuktikan bahwa Penambahan *watermark* ke dalam citra *watermarking* akan menyebabkan 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 autentifikasi 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 ekstraksinya.

## Referensi

- [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 Using discrete 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