

IMPLEMENTASI BLIND WATERMARKING PADA CITRA DIGITAL DENGAN TRANSFORMASI WAVELET HAAR

I Putu Hendra Wiguna

Jurusan Matematika, Fakultas MIPA, Universitas Udayana, Denpasar - Bali
hendra_wiguna@yahoo.com

ABSTRACT

The development of computer technology, to provide convenience in the field of multimedia digital data than conventional, especially in the process of distribution, namely the Internet network and can be made the exact same copy of the original.

With the ease in copying and distribution of digital data can then cause a negative impact of this is related to the ease in making copies and distribute digital data illegally. This is a violation of intellectual property rights of legitimate owners digital data. One solution in this problem is with digital watermarking. Digital watermarking is the inculcation of a Watermark to a digital data carrier or the main / host. Digital Watermark is a digital signal that is inserted into the data such as text, image, sound or video for various purposes. Signal is inserted in such a way so that her nose is not observed by human vision or hearing. Blind watermarking is a process in which the watermarking extraction process does not require the original data.

At the end of the task blind watermarking techniques are implemented on a digital image of the Haar wavelet transformation. Then compare how the image quality of the results with the original image after the form is inserted Watermark image, using the MSE (Mean Square Error) and PSNR (Peak Signal To Noise Ratio) of the parameters and how the resilience of the Watermark noise, JPEG compression, resize and rotation.

Keyword : Digital Image, Wavelet, Watermarking, Blind Watermarking

ABSTRAK

Perkembangan teknologi komputer memberikan kemudahan dalam bidang multimedia digital dibandingkan dengan data konvensional, terutama dalam proses penyebarannya, yaitu dengan jaringan internet dan dapat dibuat salinan yang sama persis dengan aslinya.

Dengan kemudahan dalam penyebaran dan penyalinan data digital maka dapat menimbulkan dampak negatif hal ini berkaitan dengan kemudahan dalam membuat dan menyebarkan salinan data digital secara ilegal. Ini merupakan pelanggaran hak kekayaan intelektual dari pemilik sah data digital tersebut. Salah satu solusi dalam masalah ini adalah dengan *digital watermarking*. *Digital watermarking* merupakan penanaman suatu *watermark* digital ke data utama atau *carrier/host*. *Digital watermark* merupakan sinyal digital yang disisipkan ke dalam data seperti teks, citra, video atau suara untuk berbagai keperluan. Sinyal tersebut disisipkan sedemikian rupa sehingga keberadaannya tidak teramati oleh indera penglihatan atau pendengaran manusia. *Blind watermarking* merupakan proses watermarking dimana dalam proses ekstraksi tidak memerlukan data asli.

Pada tugas akhir akan diimplementasikan teknik *blind watermarking* pada citra digital dengan transformasi *wavelet haar*. Kemudian membandingkan bagaimana kualitas citra hasil dengan citra asli setelah disisipkan watermark berupa citra, dengan menggunakan parameter MSE (*Mean Square Error*) dan PSNR (*Peak Signal To Noise Ratio*) dan bagaimana ketahanan watermark terhadap *noise*, kompresi JPEG, *resize* dan rotasi.

Kata kunci : Citra Digital, Wavelet, Watermarking, Blind Watermarking

PENDAHULUAN

Perkembangan komputer memberikan banyak kemudahan di bidang multimedia digital yang terbukti lebih unggul dibandingkan dengan multimedia konvensional. Kemudahan ini diantaranya adalah kualitas tidak berubah selama arsip multimedia yang bersangkutan tidak mengalami perubahan. Hal ini berbeda dengan multimedia konvensional yang kualitasnya cenderung menurun seiring dengan berlalunya waktu.

Data multimedia digital dapat disebarkan dengan mudah melalui jaringan komputer, misalnya internet. Serta data dapat dibuat salinan yang sama persis dari sebuah data digital. Pada data multimedia analog, pembuatan salinan dapat menyebabkan penurunan kualitas. Kemudahan dalam penyebaran dan penyalinan data digital seperti yang telah disebutkan di atas dapat pula memberikan dampak negatif. Hal ini berkaitan dengan kemudahan untuk membuat dan menyebarkan salinan secara ilegal dari sebuah data digital. Ini merupakan pelanggaran terhadap hak kekayaan intelektual dari pemilik sah data digital tersebut.

Karena itu, perlu ada usaha untuk melindungi hak pemilik data digital yang sah. Salah satu cara yang dapat menjadi solusi dalam permasalahan ini adalah pemberian watermark digital. Watermark digital adalah sinyal yang disisipkan secara permanen pada data digital (audio, citra, video, dan teks) yang dapat dideteksi kembali dengan menggunakan operasi komputasi dengan tujuan untuk membuktikan kepemilikan data yang bersangkutan (Suhail, Mohamed Abdulla, 2005).

Watermarking merupakan suatu bentuk dari Steganography (teknik untuk menyembunyikan suatu informasi pada suatu media tanpa perubahan yang berarti pada media tersebut) (Munir, Rinaldi, 2004). Teknik watermarking akan menyisipkan informasi digital yang disebut watermark ke dalam suatu data digital yang disebut carrier. Watermark yang disisipkan dapat berupa teks biasa, audio, citra maupun video tergantung dari kemampuan media yang ditumpanginya. Penambahan watermark ke dalam suatu materi multimedia tanpa mempengaruhi kualitasnya dapat digunakan sebagai bukti otentik kepemilikan suatu data.

Selama ini hidden watermarking memiliki robust yang rendah, dengan kata lain tidak tahan terhadap derau. Dan sebaliknya, robust watermarking memiliki hidden yang

rendah karena citra logo tampak pada citra asli. Dengan menggunakan channel luminance diharapkan memiliki hidden yang tinggi dan citra watermarking lebih mirip dengan citra asli, dimana channel luminance digunakan untuk mendapatkan rasio penyebaran dari nilai perubahan pada subband. Alasan mengapa didistribusikan dengan menggunakan rasio penyebaran, karena perubahan dalam area luminance rendah lebih jelas dari pada dalam area dengan luminance tinggi. Watermark digital disertakan pada data penampung sedemikian rupa sehingga menjadi bagian yang tidak terpisahkan dari data tersebut dan dapat bertahan terhadap berbagai operasi terhadap data penampung. Dengan watermarking, data multimedia digital dapat diakses seperti biasa tetapi sudah ditandai secara permanen.

Watermark berupa citra dan suara lebih disukai karena kesalahan pada beberapa bit watermark tidak menghasilkan perubahan yang berarti pada waktu verifikasi. Hasil ekstraksi watermark masih dapat dipersepsi secara visual (pada watermark berupa citra) maupun pendengaran (pada watermark berupa suara).

LANDASAN TEORI

Representasi Citra Digital

Citra dapat didefinisikan sebagai fungsi kontinu intensitas cahaya dua dimensi $f(x,y)$, dengan x dan y menyatakan koordinat spasial dan harga f pada sembarang titik (x,y) sebanding dengan skala keabuan (*brightness*) dari citra pada titik tersebut (Gonzales, Rafael C., Woods Richard E. 1987). Dalam bidang pengolahan citra, citra yang diolah adalah citra digital, yaitu citra kontinu yang telah diubah ke dalam bentuk diskrit, baik koordinat ruang maupun intensitas cahayanya.

Citra digital $f(x,y)$ direpresentasikan sebagai sebuah matriks yang indeks baris dan kolomnya mengidentifikasi sebuah titik pada citra dan nilai dari elemen matriks yang bersangkutan merupakan tingkat warna pada titik tersebut. Elemen tersebut disebut elemen citra, elemen gambar (*picture elements*), *pixels*, atau *pels* (Munir, Rinaldi, 2006). Picture elements atau pixel dapat didefinisikan sebagai elemen terkecil dari sebuah citra digital yang menentukan resolusi citra tersebut. Semakin tinggi resolusi yang dihasilkan, semakin kecil ukurannya yang berarti bahwa citra yang dihasilkan semakin halus.

Citra digital yang berupa matriks dengan ukuran $M \times N$ dapat digambarkan sebagai berikut :

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,M-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix}$$

Gambar 1. Representasi Matriks Citra Digital

Pada Tugas Akhir ini, citra yang digunakan adalah citra dengan format Bitmap (*Bmp). Pada representasi bitmap, sebuah citra dibagi menjadi kotak-kotak yang berukuran kecil dimana setiap kotaknya menyimpan intensitas warna yang disebut sebagai *pixel*.

Watermarking Citra Digital

Watermarking merupakan suatu bentuk dari *steganography*. *Steganography* adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia (Munir, Rinaldi, 2004). *Steganography* berbeda dengan *cryptography*, letak perbedaannya adalah hasil keluarannya (Supangkat, dkk, 2000). Hasil dari *cryptography* biasanya berupa bentuk data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan (tetapi dapat dikembalikan ke bentuk semula) sedangkan hasil keluaran dari *steganography* ini memiliki bentuk yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolahan digital lainnya.

Watermarking ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Jadi *watermarking* merupakan suatu cara untuk menyembunyikan atau menanamkan data / informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indra penglihatan atau pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital sampai pada tahap tertentu (Supangkat, dkk, 2000).

Watermarking digital merupakan penanaman suatu *watermark* digital ke data utama atau *carrier/host*. *Digital watermark* merupakan sinyal digital yang disisipkan ke dalam data seperti teks, citra, video atau suara untuk berbagai keperluan. Sinyal

tersebut disisipkan sedemikian rupa sehingga keberadaannya tidak teramati oleh indera penglihatan atau pendengaran manusia. Tidak teramati karena pada dasarnya indera manusia sangat sulit membedakan antara data yang disisipi *watermark* dan data yang belum. Walaupun demikian komputer dapat mendeteksi keberadaan *watermark* dengan mudah, tentunya dengan algoritma tertentu. Sinyal *watermark* tersebut biasanya mempresentasikan informasi tertentu misalnya label pengenalan, sehingga dengan *watermark* ini kepemilikan sebuah informasi dapat ditentukan dengan jelas.

Watermarking citra digital adalah proses penyisipan suatu *watermark* digital ke dalam media citra digital. Secara visual, *watermark* dibedakan menjadi dua macam, yaitu *robust watermarking* dan *hidden watermarking*. Pada *robust watermarking*, *watermark* digital tampak pada citra asli sedangkan pada *hidden watermarking*, *watermark* digital tidak tampak pada citra asli.

Karakteristik Digital Watermark

Ada beberapa karakteristik atau sifat khusus tertentu yang dimiliki oleh sebuah *watermark*. Sifat-sifat tersebut sangat bergantung pada aplikasi *watermarking* yang akan dibuat. Meskipun demikian ada beberapa sifat yang secara umum dipunyai aplikasi *watermarking*. Sifat-sifat tersebut diantaranya adalah sebagai berikut (Swanson et al, 1998) dan (Langelaar et al, 2000) : 1. *Perceptual transparency*, 2. *Robustness*, 3. *Security* dan 4. *Public vs Private Watermarking*.

Wavelet

Transformasi Wavelet mulai diperkenalkan pada tahun 1980-an oleh Morlet dan Grossman sebagai fungsi matematis untuk merepresentasikan data atau fungsi sebagai alternatif transformasi-transformasi matematika yang lahir sebelumnya untuk menangani masalah resolusi (Polikar, Roby, 1996).

ANALISA DAN PERANCANGAN SISTEM

Studi Literatur

Metode yang digunakan yaitu terlebih dahulu melakukan studi literatur mengenai bagaimana menggunakan transformasi *wavelet haar* dalam penerapan *watermarking* citra digital pada beberapa buku, makalah dan situs internet.

Perancangan Sistem

Pada tahapan ini penulis melakukan perancangan sistem *Blind Watermarking* Pada Citra Digital Dengan Transformasi *Wavelet Haar* dan implementasinya dengan menggunakan bahasa pemrograman Matlab 7.0. Secara garis besar langkah yang dilakukan antara lain :

Proses penyisipan *watermark (Embedding)* adapun langkah-langkah secara garis besarnya antara lain : (a) Menginput citra asli. (b) Melakukan proses pemisahan layer RGB citra asli. (c) Melakukan transformasi *wavelet* dengan filter *haar* kemudian citra asli di dekomposisi ke dalam empat *subband*. (d) Pengambilan *subband HH* yang akan digunakan sebagai tempat penyisipan *watermark*.

Proses ekstraksi *watermark* (a) Proses pemisahan layer RGB citra *watermarking*. (b) Proses transformasi *wavelet*. (c) Proses pengambilan *subband HH*. (d) Proses ekstraksi.

Pengujian Sistem Beserta Implementasi dan Analisis Sistem

Pada tahapan ini penulis melakukan pengujian dengan menjalankan sebuah contoh kasus dengan skenario misalnya bagaimana menyisipkan *watermark* ke dalam sebuah citra yang telah ditentukan dan membandingkan hasil citra yang asli dengan citra yang ter*watermark*, kemudian melakukan ekstraksi untuk melihat ada atau tidak *watermark* dalam citra tersebut, kemudian melakukan analisis pengukuran secara obyektif dengan menggunakan parameter-parameter.

IMPLEMENTASI DAN EVALUASI

Perancangan Sistem

Pada perancangan sistem tugas akhir ini disimulasikan sistem *Blind Digital Image Watermarking* dengan menggunakan DH-WT. Aplikasi sistem watermarking ini terdiri atas bagian penyisipan *watermark (embedding)* dan bagian ekstraksi *watermark*.

Pengujian dan Implementasi Sistem

Pada tugas akhir ini implementasi sistem *blind digital image watermarking* disimulasikan dengan bahasa pemrograman matlab 7.0. dan tahapan ini menjelaskan cara kerja program.

Lingkungan Uji Coba

Pada tahap ini digunakan citra yang digunakan sebagai pengujian yaitu citra

berwarna RGB 24 bit berukuran 512x512 piksel dengan format *Bitmap (*.bmp)* karena sesuai dengan batasan masalah yang diberikan.

Pelaksanaan Uji Coba

Pelaksanaan uji coba dilakukan dengan menjalankan aplikasi yang dibuat. Adapun langkah-langkah yang dilakukan dari jalannya program adalah sebagai berikut :

Buka Citra Pengujian dan Melakukan Transformasi *Wavelet*

Citra yang akan digunakan dalam pengujian sistem ini adalah citra berwarna citra RGB 24 bit dengan format *Bitmap*. Berikut citra-citra yang akan diuji :

No	Nama	Ukuran
1	Bunga.bmp	512x12
2	Peppers.bmp	512x12
3	Burung.bmp	512x12
4	Lena.bmp	512x12
5	Kupu-kupu.bmp	512x12
6	Selancar.bmp	512x12
7	Ruang.bmp	512x12
8	Pesawat.bmp	512x12
9	Perahu.bmp	512x12
10	Mobil.bmp	512x12

Tabel 1. Citra Pengujian

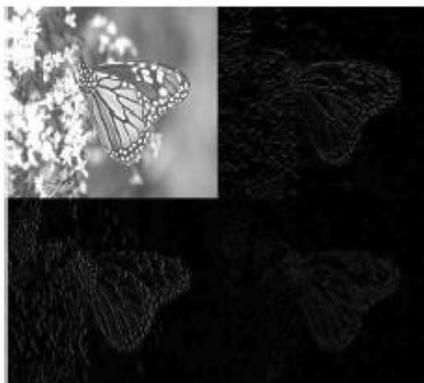
Pertama yang dilakukan adalah membuka citra yang akan digunakan sebagai pengujian dimana digunakan 10 citra pengujian yang terdapat dalam Tabel 1 dan melakukan transformasi *wavelet* seperti yang ditampilkan dibawah ini :



(1) Layer R

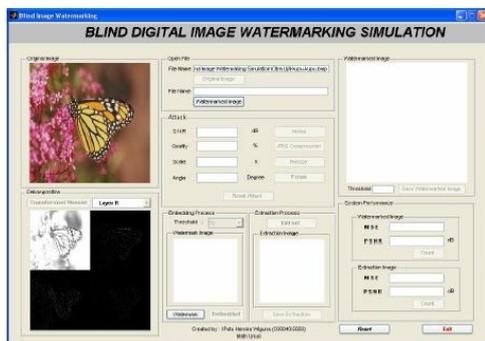


(2) Layer G



(3) Layer B

Gambar 1. Proses Transformasi Wavelet Menghasilkan Empat Subband. (1) Layer R (2) Layer G (3) Layer B



Gambar 2. Proses Transformasi Wavelet

Buka Citra Watermark dan Melakukan Proses *Embedded* (Penyisipan)

Setelah dilakukan transformasi wavelet proses selanjutnya membuka citra *watermark* atau logo kemudian melakukan proses *embedded* dimana dalam proses ini akan melibatkan suatu nilai *threshold* dimana disediakan nilai *threshold* dari 10, 20, 30, 40 dan 50.

Berikut adalah citra *watermark* (logo) yang digunakan dalam tugas akhir ini sebagai pengujian :



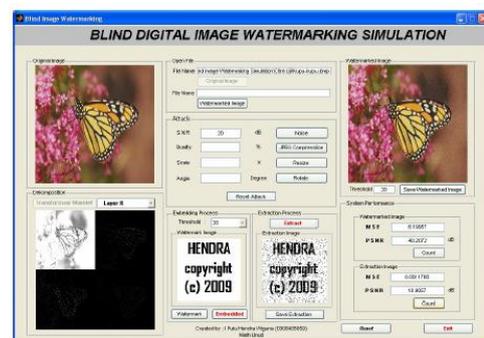
Gambar 3. Citra Watermark (logo) Pengujian



Gambar 4. Proses *Embedded*

Proses Ekstraksi

Dalam proses ekstraksi citra *watermarking* mengalami gangguan atau *attack* kemudian mengukur kualitas citra asli dengan citra *watermarking* dan kualitas citra *watermark* dengan citra hasil ekstraksi dari citra watermarking yang telah mengalami gangguan atau *attack*. Pengukuran ini menggunakan nilai MSE dan PSNR. Contoh dibawah adalah citra *watermarking* yang telah mengalami gangguan berupa penambahan *noise* dan hasil ekstraksinya :



Gambar 5. Proses Ekstraksi

Dari perancangan dan uji coba sistem maka akan disimulasikan sistem blind digital image *watermarking* dengan transformasi wavelet. Dengan aplikasi ini dilakukan pengujian serta analisis beberapa citra uji sebagai citra asli untuk:

Mengetahui kualitas citra watermarking setelah disisipkan *watermark* pada citra asli. Mengetahui ketahanan (*robust*) citra *watermark* yang disisipkan pada citra asli terhadap hilangnya informasi karena *attack* yang diberikan pada citra watermarking.

Mengetahui *sensitivitas* citra *watermark* (logo) yang disisipkan pada citra asli terhadap hilangnya informasi akibat *attack* yang diberikan pada citra *watermarking*. Bila citra watermarking diberikan *attack* tidak terlalu besar maka citra *watermark* hasil ekstraksi mengalami perubahan.

SIMPULAN

Dari hasil pengujian dan analisis pada yang menunjukkan kinerja dari teknik *blind digital image watermarking* dengan transformasi wavelet haar, maka dapat ditarik beberapa kesimpulan sebagai berikut :

Transformasi wavelet haar diskrit menunjukkan kinerja yang bagus terhadap *blind image watermarking*, dimana citra yang disisipkan *watermark* (citra watermarking) memiliki PSNR rata-rata 40 dB keatas, semakin kecil nilai *threshold* yang dimasukkan maka kualitas citra *watermarking* semakin bagus tetapi semakin tidak tahan terhadap serangan (*attack*). Dengan metode ini semakin kecil nilai *threshold* yang digunakan maka semakin besar tingkat *sensitivitas watermark* sedangkan ketahanan *watermark* akan semakin besar jika digunakan nilai *threshold* yang semakin besar.

Metode ini membuat *watermark* tertanam secara permanen atau tidak bisa dihapus sehingga dapat digunakan sebagai fungsi *otentifikasi*. *Watermark* yang disisipkan pada citra memiliki *sensitivitas* yang cukup tinggi pada *gaussian noise* pada saat menggunakan nilai *threshold* 10, sedangkan untuk ketahanan *watermark* (*robustness*) menunjukkan performansi yang baik pada saat nilai *threshold* 50.

Watermark sangat sensitive terhadap kompresi JPEG dengan nilai *threshold* 10 dan dengan menggunakan nilai *threshold* 10 dan dengan menggunakan nilai *threshold* 50 watermark mulai tahan pada saat diberikan faktor kualitas kompresi 75%. *Sensitivitas watermark* ekstraksi pada *resize/rescaling* dengan skala < 1 jika diberikan nilai *threshold* 10. Dengan nilai *threshold* 50 *watermark* ekstraksi mulai tahan dengan skala ≥ 0.75 . Dengan proses rotasi disini menunjukkan *watermark* sangat sensitif dan tidak tahan terhadap rotasi meskipun hanya

diberikan sudut 1 derajat, hasil ekstraksi mengalami kerusakan yang sangat parah hal ini disebabkan karena perubahan posisi dari tiap piksel pada citra *watermarking* yang mengakibatkan nilai tiap piksel ikut mengalami perubahan. Sehingga tidak dapat diekstrak dengan bagus.

DAFTAR PUSTAKA

- [1] Dharma, Eddy Mutina. 2004. **Teknik Steganography Pada Citra Digital Dengan Transformasi Wavelet**. Bandung : Institut Teknologi Bandung.
- [2] Gonzales, Rafael C., Woods Richard E. 1987. *Digital Image Processing Second Edition*. Prentice-Hall, Inc.
- [3] Joachim J. Eggers., Jonathan K. Su. 2000. **Robustness of A Blind Image Watermarking Scheme**. Nuremberg : Telecommunications Laboratory University of Erlangen.
- [4] Matlab. 2001. **Wavelet Toolbox**. The Math Works, Inc.
- [5] Munir, Rinaldi. 2006. **Kriptografi**. Bandung : Informatika.
- [6] Polikar, Roby. 1996. **The Wavelet Tutorial**. Ames USA : Iowa State University.
- [7] Supangkat, Suhono H., Kuspriyanto dan Juanda. 2000. **Watermarking Sebagai Teknik Penyembunyian Label Hak Cipta Pada Data Digital**. Bandung: Institut Teknologi Bandung.
- [8] Suhail, Mohamed Abdulla 2005, **Digital Watermarking for Protection of Intellectual Property**. Multimedia Security, Steganography and Digital Watermarking Techniques For Protection of Intellectual Property. Idea Group Publishing.
- [9] Swanson, M. D. Kobayashi., dan Tewfik, A. H., Juni 1998, **Multimedia Data Embedding and Watermarking Technologies**, Proceedings of the IEEE, Vol 86, No 6.
- [10] Taskovski, Dimitar. 2005. **Blind Low Frequency Watermarking Method**. International Journal of Signal Processing. Volume 2. Number 3.
- [11] Wirabuana, I Dewa Nyoman. 2005. **Analisis Kinerja Image Steganography Menggunakan Transformasi Wavelet**. Bandung : STT Telkom.