ANALISIS KINERJA IMAGE STEGANOGRAPHY MENGGUNAKAN TRANSFORMASI WAVELET PERFORMANCE ANALYSIS OF IMAGE STEGANOGRAPHY USING WAVELET TRANSFORM

I Dewa Nyoman Wirabuwana[1], -[2]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Steganography merupakan teknik pengamanan data informasi, dimana pengamanan data dilakukan dengan menyembunyikan keberadaan informasi tersebut dalam suatu media pembawa. Dengan demikian diharapkan keberadaannya tidak mengundang kecurigaan dari persepsi pengamatan indera manusia. Dengan memanfaatkan kelemahan dari mata manusia, maka dipilih citra digital sebagai media pembawa selama data yang disisipkan tersebut tidak merusak kualitas citra pembawa.

Penerapan teknik steganography pada citra digital dikatakan memiliki kinerja yang baik apabila citra pembawa tidak mengalami penurunan kualitas. Oleh sebab itu, saat ini telah banyak metoda untuk steganography, seperti metode LSB, HC-RIOT coder dan DCT. Metode–metode ini memiliki beberapa kelebihan dan kekurangan, sehingga pada tugas akhir ini digunakan metode Discrete Wavelet Transform yang diharapkan dapat menangani beberapa kekurangan yang ada pada metode–metode sebelumnya. Citra digital yang digunakan dalam tugas akhir ini adalah citra berwarna 24 Bit dalam format (*.bmp) dengan kriteria low detail, medium detail serta high detail. Data atau informasi yang akan disisipkan adalah file teks dengan format (*.txt). Uji kehandalan dari sistem steganography ini dilakukan dengan memberi gangguan noise, kompresi JPEG, rescaling dan rotasi.

Dari hasil pengujian yang dilakukan disimpulkan bahwa sistem steganography ini tahan terhadap gangguan noise sebesar 21 dB keatas. Hal ini ditunjukkan dengan nilai BER pada saat diberi noise sebesar 21 dB adalah 0.07% dan 0.1% untuk level dekomposisi tingkat 1 dan 2. Sistem ini juga tahan terhadap kompresi JPEG dengan faktor kualitas 85 dan 55 untuk level dekomposisi tingkat 1 dan 2 dengan nilai BER 0.12% dan 0.2%. Namun untuk rescaling BER mencapai 53.1% dan 0.18% serta 0.58% dan 0.29% masing-masing untuk level dekomposisi tingkat 1 dan 2 pada faktor skala 0.5 dan 0.75. Untuk rotasi, diperoleh nilai BER sekitar 40%-50% untuk masing-masing sudut rotasi. Dalam keadaan tanpa gangguan, BER data ekstraksi dapat mencapai 0%. Secara subyektif, diperoleh nilai MOS sebesar 4.4 dan 3 untuk level dekomposisi tingkat 1 dan level dekomposisi tingkat 2. Ini berarti citra hasil steganography memiliki kualitas yang baik.

Kata Kunci :

Abstract
Steganography is a technique to secure information data, where it can be done by hiding the information into a carrier media. Thereby, the existences of the information will not expecting suspicion of human visual perception. By using that weakness, the digital image is chosen as carrier media as long as the data that has been embedded will not destruct carrier media quality. The implementation of steganography technique on digital image has good performance if carrier media quality do not degraded. Therefore, nowadays there are so many methods for steganography, such as LSB, HC-RIOT Coder, and DCT. These methods have advantages and disadvantages so this final project will be used Discrete Wavelet Transform which is expected to handle the weaknesses of the past methods. Digital image that used in this final project is 24 bit colored image in BMP format with low detail, medium detail, and high detail criteria. Data or information that will be embedded in digital image is a text file in (*.txt) format. In order to test the robustness, the proposed scheme of steganography is attacked in several ways with noise, JPEG compression rescaling and rotation.
Based on simulation, it can be concluded that the steganography system is robust to noise at 21 decibel and above. It can be shown by the given BER value at 21 dB is 0.07% and 0.1% for 1st and 2nd decomposition level. The system is also robust to JPEG compression with the quality factor 85 and 55 for the 1st and 2nd decomposition level with 0.12% and 0.2% BER value. But against geometric distortion, rescaling and rotation, BER reaches 53.1% and 0.18% for decomposition level 1, 0.58% and 0.29% for decomposition level 2 with both scaling factor 0.5 and 0.75. Unfortunately, it has 40%-50% BER values for each rotation angle. In a state of without any noise, BER value of extracted data reaches 0%. Subjectively, it has 4.4 and 3 Mean Opinion Score (MOS) value for the 1st and 2nd decomposition level. Its mean that steganography image has good quality.

Keywords :

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi digital dan multimedia yang semakin pesat menjadikan pertukaran informasi jarak jauh semakin mudah. Informasi yang dikirimkan dapat berupa citra digital, audio maupun video. Kemudahan ini memberikan kebebasan pada setiap orang untuk saling bertukar informasi dalam suatu jaringan komputer, baik lokal maupun global. Dengan adanya kebebasan ini, maka dibutuhkan suatu sistem keamanan yang dapat mengamankan suatu informasi dari pihak lain yang tidak berkepentingan. Sehingga privasi seseorang untuk saling bertukar informasi dapat dijaga dengan baik.

Cryptography merupakan salah satu teknik pengamanan data yang sangat populer yang lebih menekankan suatu teknik penyandian. Pada teknik ini informasi yang dikirim disandikan menggunakan suatu algoritma tertentu, sehingga hanya orang yang memiliki algoritma tersebut yang dapat menterjemahkan informasi yang telah disandikan. Namun pada teknik *cryptography*, keberadaan informasi masih dapat diketahui sehingga ada kemungkinan orang lain untuk membuka kode sandi dari informasi tersebut. Oleh karena itu diperlukan suatu teknik yang dapat menyembunyikan keberadaan informasi yang akan dikirimkan. Salah satu teknik penyembunyian data tersebut adalah *Steganography*.

Steganography merupakan suatu ilmu yang mempelajari, meneliti dan mengembangkan teknik menyembunyikan suatu informasi dalam suatu media. *Steganography* berasal dari bahasa yunani yang berarti ”tulisan tersembunyi”. Pada jaman dahulu, teknik ini telah sering dilakukan untuk menyampaikan pesan-pesan rahasia. Tujuan utama *Steganography* adalah untuk menjaga kerahasiaan informasi yang sesungguhnya ingin disampaikan. Steganography juga banyak digunakan sebagai hak cipta (*copyright protection*) yang mencegah terjadinya pembajakan produk–produk digital.

Dalam tugas akhir ini, akan dilakukan teknik *steganography* pada citra digital menggunakan DHWT *(Discrete Haar Wavelet Transform)*. Citra digital dipilih sebagai media pembawa, karena terdapat kelemahan pada indera manusia, seperti mata. Sehingga tidak mengundang kecurigaan dari persepsi pengamatan manusia. Penerapan teknik *steganography* pada citra digital dikatakan baik apabila media pembawa tidak mengalami penurunan kualitas. Saat ini telah banyak metoda untuk teknik *steganography*, seperti teknik penyisipan pada nilai LSB (*Least Significant Bit*), *steganography* menggunakan HC-RIOT *(Homogenous Connected-Region Interested Ordered Transmission) Coder* dan DCT *(Discrete Cosine Transform)*. Metoda-metoda ini memiliki beberapa kelebihan ataupun kekurangan, sehingga pada tugas akhir ini digunakan transformasi wavelet untuk mengatasi beberapa kekurangan yang ada pada metode sebelumnya.

Pengujian yang akan dilakukan pada tugas akhir ini adalah dengan memberikan gangguan noise (*uniform noise*), kompresi JPEG *(JPEG Compression)*, *Rescalling*, dan rotasi terhadap data yang disisipkan serta citra hasil *steganography*. Dengan pengujian ini diharapkan transformasi wavelet dapat memberikan ketahanan data (*robustness*) yang baik dan memberikan kualitas citra hasil *steganography* yang baik pula.

1.2 Rumusan Masalah

Permasalahan yang dibahas dalam tugas akhir ini meliputi :

1. Menerapkan teknik *steganography* pada citra digital menggunakan DHWT *(Discrete Haar Wavelet Transform).*
2. Membandingkan *stego-image* (citra yang telah disisipkan informasi) dengan *real-image* (citra asli).
3. Melakukan pengujian terhadap *stego-image* (citra yang telah disisipkan data) dengan memberikan gangguan noise (*Uniform Noise*) dan melakukan kompresi JPEG *(JPEG Compression)* serta memberikan distorsi geometris seperti *rescalling* dan rotasi serta menganalisa hasilnya.
4. Mengukur nilai MSE (*Mean Square Error*), SNR (*Signal to Noise Ratio*) dan BER (*Bit Error Rate*) pada *stego-image* setelah dilakukan pengujian.

5. Mengukur nilai MOS (*Mean Opinion Score*) terhadap *stego-image* yang diambil dari 30 orang pengamat.

1.3 Batasan Masalah

Batasan masalah yang digunakan dalam Tugas Akhir ini adalah:

1. Citra digital yang akan digunakan sebagai tempat penumpangan informasi adalah citra berwarna 24 Bit dalam format BMP (*.bmp).
2. Informasi yang akan ditumpangkan adalah file teks dengan format (*.txt).
3. Transformasi yang digunakan adalah DHWT (*Discrete Haar Wavelet Transform*) dengan level dekomposisi yang berbeda, yaitu : level 1 dan level 2.
4. Ketahanan data yang disisipkan akan diuji terhadap ganguan noise *(Uniform Noise*), kompresi JPEG *(JPEG Compression), rescalling* dan rotasi.
5. Parameter yang diukur secara obyektif adalah MSE (*Mean Square Error*), PSNR (*Peak Signal to Noise Ratio*) dan BER (*Bit Error Rate*).
6. Parameter yang diukur secara subyektif adalah MOS (*Mean Opinion Score*) yang diambil dari 30 orang pengamat.

1.4 Tujuan dan Kegunaan

1.4.1 Tujuan

Tujuan dari tugas akhir ini adalah sebagai berikut :

1. Merancang teknik *steganography* pada citra digital menggunakan DHWT *(Discrete Haar Wavelet Transform)*.
2. Membandingkan kualitas *stego-image* (citra yang telah disisipkan data) dengan *cover-image* (citra penampung).
3. Menguji ketahanan data yang disisipkan terhadap hilangnya informasi pada *stego-image* akibat proses kompresi JPEG, gangguan noise, *rescalling* dan rotasi yang dilakukan.
4. Menguji kualitas *stego-image* terhadap proses kompresi JPEG, gangguan noise, *rescalling* dan rotasi yang dilakukan.

1.4.2 Kegunaan

Pelaksanaan Tugas Akhir ini bertujuan untuk memperkenalkan salah satu aplikasi dari *Discrete Wavelet Transform* (DWT) dan metode partisi blok yaitu pada sistem *steganography* selain aplikasi lainnya. Untuk selanjutnya, Tugas Akhir ini diharapkan dapat digunakan sebagai referensi untuk merekomendasikan penggunaan metode partisi blok dan *Discrete Waveler Transform* untuk keperluan praktis *steganography* pada masalah *data security* (keamanan data) atau *copyright protection*, seperti watermarking.

1.5 Metodologi Penelitian

Penelitian ini dilakukan dengan beberapa metode, yaitu :

1. Melakukan studi literature dengan mempelajari permasalahan yang berkaitan
   dengan representasi citra digital, teknik *steganography* dan transformasi Wavelet.
2. Proses pembelajaran materi penelitian melalui pustaka-pustaka yang berkaitan dengan penelitian, baik berupa buku maupun jurnal ilmiah.
3. Pengumpulan data-data penunjang diperoleh dari hasil simulasi yang dilakukan dan data-data yang diperoleh dari *paper* yang tersebutkan pada daftar pustaka.
4. Penelitian dilakukan dengan bentuk perancangan dan pemodelan sistem yang disimulasikan menggunakan *software* Matlab 6.5 untuk mendapatkan data-data yang diperlukan pada proses analisa.

1.6 Sistematika Penulisan

Tugas akhir yang akan disusun ini terdiri dari lima bab ditambah dengan lampiran-lampiran yang diperlukan.

Berikut ini rincian dari bab-bab tersebut:

BAB I PENDAHULUAN

Merupakan uraian mengenai latar belakang masalah, tujuan penelitian, perumusan masalah, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi penjelasan tentang representasi citra digital, dekomposisi dan rekontsruksi dengan transformasi wavelet, proses penyisipan data, proses ekstraksi data dan kriteria pengujian yang akan dilakukan.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM IMAGE *STEGANOGRAPHY*

Bab ini berisi perumusan matematis dan pembentukan algoritma – algoritma yang akan digunakan dalam perancangan sistem *steganography* pada citra digital menggunakan DHWT *(Discrete Haar Wavelet Transform)*. Dalam perancangan tersebut, *software* yang digunakan adalah Matlab 6.5.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini membahas analisa dari hasil pengujian teknik *steganography* berdasarkan ketahanan data yang disisipkan terhadap *uniform noise*, kompresi JPEG, *rescalling*, dan rotasi dengan menghitung nilai MSE, SNR, BER dan MOS.

BAB V PENUTUP

Bab ini memberikan kesimpulan dari keseluruhan hasil analisa dalam tugas akhir ini dan beberapa saran untuk pengembangan teknik *steganography* lebih lanjut.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisa pengukuran baik secara obyektif maupun subyektif yang menunjukkan kinerja dari teknik *image steganography* menggunakan transformasi wavelet, maka diperoleh kesimpulan sebagai berikut :

1. Level dekomposisi wavelet mempengaruhi jumlah bit informasi maksimum yang dapat disisipkan dalam sistem *image steganography*. Level dekomposisi tingkat 1 dapat menampung sebanyak 4096 bit sedangkan level dekomposisi tingkat 2 hanya dapat menampung 1024 bit informasi saja.
2. Kapasitas informasi yang disisipkan mempengaruhi kualitas citra hasil *steganography* (*stego-image*). Semakin besar kapasitas informasi yang disisipkan, *stego-image* akan mengalami degradasi visual yang semakin besar pula. Hal ini dapat dilihat dari nilai PSNR untuk kapasitas 4096 bit adalah 31 dB sedangkan untuk kapasitas 1024 bit adalah 36 dB.
3. Kriteria citra yang digunakan mempengaruhi kualitas citra hasil *steganography* (*stego-image*). Citra *low detail*, *medium detail* dan *high detail* dengan kapasitas informasi maksimum (4096 bit) masing-masing memberikan nilai PSNR sebesar 32 dB, 29 dB dan 26 dB. Hal tersebut menunjukkan bahwa citra dengan kriteria *low detail* lebih cocok digunakan sebagai citra penampung.
4. Sistem steganography dengan level dekomposisi tingkat 1 dan tingkat 2 memiliki sifat cukup *robust* terhadap noise, kompresi JPEG, dan *rescalling*. BER data ekstraksi yang dihasilkan untuk masing-masing level dekomposisi adalah 0,07% dan 0,1% pada saat gangguan noise 21 dB, 0,12% dan 0,2% pada saat kompresi JPEG dengan faktor kualitas 85 dan 55, serta 0,317% dan 0,59% pada saat rescalling dengan skala ¾ dan ½. Namun BER yang dihasilkan setelah dilakukan rotasi sangat buruk, yaitu sekitar 40%-55%.

5. Semakin besar nilai *robustness* yang diberikan maka semakin *robust* pula informasi yang disisipkan, namun citra hasil *steganography* (*stego-image*) akan mengalami degradasi visual yang semakin besar pula. BER yang dihasilkan untuk nilai *robustness* 10 dan 50 adalah 21.77% dan 0% (pada tabel 4.8), sedangkan PSNR yang dihasilkan untuk nilai *robustness* 10 dan 50 adalah 42dB dan 35dB (gambar 4.9a).
6. Dari analisa citra secara subyektif, diperoleh nilai MOS sebesar 4,4 untuk citra *low detail* (file tulip.bmp) pada level dekomposisi tingkat 1 dan nilai MOS sebesar 3 untuk citra *low detail* (file tulip.bmp) pada level dekompisisi tingkat 2 walaupun disisipkan data sebesar kapasitas maksimal. Ini berati perbedaan kualitas *stego-image* dengan citra sebelum disisipkan data tidak begitu besar.

5.2 Saran

Untuk perkembangan selanjutnya yang dapat dilakukan pada sistem citra *watermarking* ini adalah :

1. Informasi yang akan disembunyikan sebaiknya dienkripsi terlebih dahulu sebelum disisipkan kedalam citra penampung, sehingga hal ini akan menambah keamanan informasi tersebut.
2. Mengembangkan kembali sistem *steganography* ini agar lebih *hidden* dan *robust* bahkan terhadap distorsi geometris, khususnya rotasi. Misalnya: dengan menambahkan spread spectrum, atau membuat suatu algoritma agar pembentukan blok bisa dinamis, dll.
3. Mengembangkan sistem *steganography* ini agar dapat diimplementasikan lebih lanjut. Misalnya, diimplementasikan untuk sistem MMS *(multimedia messaging service)* pada *Handphone* menggunakan J2ME.

DAFTAR PUSTAKA

[1] **Burrus, C. Sidney.** 1998. *Introduction to Wavelets and Wavelet Transforms.* Prentice Hall.

[2] **Cahyono, Sigit**. 2001. *Implementasi Dekoder Image Steganography Menggunakan Metode Spread Spectrum*. Jurusan Teknik Elektro. STT Telkom

[3] **Dharma, Eddy Muntina.** 2004. *Teknik Steganography Pada Citra Digital Dengan Transformasi Wavelet.* Institut Teknologi Bandung.

[4] **Gonzales, Rafael C.** 1993. *Digital Image Processing*. Addison-Wesley Publishing Company, Inc.

[5] **Haryadi, Ferdi.** 2003. *Perancangan dan Impelementasi Teknik Steganography pada Citra Digital dengan Metoda DCT*. Jurusan Teknik Informatika. STT Telkom bandung.

[6] **Jordan, Ramiro and Roberto Lotufo.** 1997. *Wavelet Concepts*. KRI, ISTEC. http://www.leca.ufrn.br/cursos/dip/dipcourse/

[7] **Meylani, Linda.** 2002. Implementasi *Image Steganography Menggunakan HC-RIOT Coder*. Jurusan Teknik Elektro. STT Telkom Bandung.

[8] **Munir, Rinaldi.** 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik.* Informatika Bandung.

[9] **Matlab,** Wavelet Toolbox. 2001. The MathWorks, Inc.

[10] **Polikar, Roby.** 1996. *The Wavelet Tutorial*, Iowa State University, Ames, USA, www.wavelets.com

[11] **Rahardjo, Jangkung, Ir, MT.** 2004. *Diktat kuliah Pemrosesan Sinyal Multimedia*. Jurusan Teknik Elektro. STT Telkom Bandung.

[12] **Ramadhaniati, Elva**. 2005. *Studi Penentuan Koefisien Pencampur Optimal Pada Proses Watermarking Dengan Metode ICA-Wavelet Pada Citra Digital.* Jurusan Teknik Elektro. STT Telkom

[13] **Satriadi, IGB.** 2002. *Analisis Perbandingan Aplikasi Transformasi Fourier dan Transformasi Wavelet Pada Proses Kompresi Citra Digital.* Jurusan Teknik Informatika. STT Telkom Bandung.

[14] **Usman, Koerdianto., et Al.** 2004. *A Study of Sub-band Frequency Combination to Improve The Performance of ICA-Wavelet Watermarking Scheme For Medical Images in Telemedicine Application*. Bandung.