



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
FAKULTAS TEKNIK
JURUSAN TEKNIK ELEKTRO
Jalan MT Haryono 167 Telp & Fax. 0341 554166 Malang 65145

KODE
PJ-01

**PENGESAHAN
PUBLIKASI HASIL PENELITIAN SKRIPSI
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK UNIVERSITAS BRAWIJAYA**

NAMA : DZIKRU ROHMATUL IZA
NIM : 0810633046 - 63
PROGRAM STUDI : REKAYASA KOMPUTER
**JUDUL SKRIPSI : STEGANOGRAFI PADA CITRA *DIGITAL* MENGGUNAKAN
METODE *DISCRETE WAVELET TRANSFORM***

TELAH DI-REVIEW DAN DISETUJUI ISINYA OLEH:

Pembimbing 1

Pembimbing 2

Ir. Muhammad Aswin, MT.
NIP. 19640626 199002 1 001

Ali Mustofa, ST., MT.
NIP. 19710601 200003 1 001

**STEGANOGRAFI PADA CITRA *DIGITAL* MENGGUNAKAN
METODE *DISCRETE WAVELET TRANSFORM***

Publikasi Jurnal Skripsi



Disusun Oleh :

DZIKRU ROHMATUL IZA

NIM : 0810633046 - 63

**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
FAKULTAS TEKNIK
MALANG
2013**

STEGANOGRAFI PADA CITRA *DIGITAL* MENGGUNAKAN METODE *DISCRETE WAVELET TRANSFORM*

Dzikru Rohmatul Iza¹, Ir. Muhammad Aswin, MT.², Ali Mustofa, ST., MT.²

¹Mahasiswa Teknik Elektro Univ. Brawijaya, ²Dosen Teknik Elektro Univ. Brawijaya

Jurusan Teknik Elektro Fakultas Teknik Universitas Brawijaya

Jalan MT. Haryono 167, Malang 65145, Indonesia

E-mail: dzikruiza@gmail.com

Abstract—Ease exchange of information through the internet has positive and negative sides. The plus side is the ease to know various information. While the downside if there isn't good security system and the message is confidential, it will be easy for others to know the contents of the message. Steganography is one solution to protect confidential messages via the internet. To do steganography, digital image is good a cover-object, because a lot of exchange of digital imagery through the internet, so as not to invite suspicion of a secret message. Discrete Wavelet Transform (DWT) is one of the methods used in the technique of steganography in the transform domain.

Index Terms—Steganography, Discrete Wavelet Transform, Digital Image.

Abstrak—Kemudahan pertukaran informasi melalui internet memiliki sisi positif dan negatif. Sisi positifnya adalah kemudahan mengetahui berbagai informasi. Sedangkan sisi negatifnya jika tidak ada sistem keamanan yang baik dan pesan yang ingin disampaikan bersifat rahasia, maka akan mudah bagi orang lain mengetahui isi pesan. Steganografi merupakan salah satu solusi untuk melindungi pesan yang bersifat rahasia melalui internet. Untuk melakukan steganografi, citra *digital* merupakan *cover-object* yang baik, karena banyak pertukaran citra *digital* melalui internet, sehingga tidak mengundang kecurigaan akan adanya pesan rahasia yang disisipkan. *Discrete Wavelet Transform (DWT)* merupakan salah satu metode yang digunakan dalam teknik steganografi dalam *domain transform*.

Kata Kunci—Steganografi, *Discrete Wavelet Transform*, Citra *Digital*.

I. PENDAHULUAN

Pesatnya perkembangan teknologi informasi menyebabkan penggunaan media *digital* semakin

banyak digunakan. Penyampaian informasi melalui media *digital* dipilih karena efisiensi waktu pengiriman yang sangat cepat dan penggunaannya yang semakin mudah. Permasalahan muncul ketika seseorang ingin mengirimkan informasi yang bersifat rahasia, namun keamanan pada media internet sangatlah minim, sehingga informasi yang ingin disampaikan rentan sekali terdapat pencurian.

Untuk mengatasi permasalahan keamanan tersebut dapat menggunakan *kriptografi*, yaitu teknik pengenkripsian pesan. Namun teknik ini dapat menimbulkan kecurigaan karena pesan acak tidak memiliki makna secara kasat mata, sehingga mudah dicurigai. Untuk menjawab masalah dari *kriptografi* digunakan teknik penyembunyian pesan yaitu steganografi. Teknik ini menyisipkan pada media lain (*cover object*) yang umum digunakan dalam kehidupan. Pesan yang dikirimkan melalui media yang telah disisipi pesan (*stego-object*) tidak akan mengundang kecurigaan orang lain, karena perbedaannya tidak dapat dilihat secara kasat mata.

Media yang paling mudah dimanfaatkan untuk steganografi adalah berkas multimedia. Berkas yang sering dijumpai adalah citra *digital*. Salah satu jenis citra *digital* yang sering dijumpai di internet berformat *bitmap*. Format ini sangat sering digunakan karena memiliki kualitas yang baik karena dapat menampilkan gambar yang bersifat lebih natural baik dalam bentuk dan warna.

II. TINJAUAN PUSTAKA

A. Citra *Digital*

Citra *digital* adalah suatu matriks yang terdiri dari baris dan kolom dimana setiap pasang indeks baris dan kolom menyatakan suatu titik pada citra. Nilai dari setiap matriks menyatakan nilai kecerahan titik tersebut. Titik-titik tersebut dinamakan sebagai elemen citra atau piksel.

Citra *digital* dapat di definisikan sebagai fungsi dua variabel, $f(x,y)$, dimana x dan y adalah koordinat spasial dan nilai $f(x,y)$ adalah intensitas citra pada koordinat tersebut. Teknologi dasar

untuk menciptakan dan menampilkan warna pada citra *digital* berdasarkan penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* – *RGB*).

B. Warna dan Ruang Warna

Ruang warna atau yang sering juga disebut sebagai model warna merupakan sebuah cara atau metode untuk menentukan, membuat, dan memvisualisasikan warna. Dalam skripsi ini, penulis akan membahas dua ruang warna yang akan digunakan untuk aplikasi steganografi. Dua ruang warna tersebut adalah sebagai berikut [6] :

1. *RGB*, memiliki tiga komponen warna yaitu merah (*red*) R, hijau (*green*) G, dan biru (*blue*) B.
2. *YCbCr* (*Luminance-Chrominance*)
Y merupakan komponen *luminance*, Cb dan Cr adalah komponen *chrominance*.

YCbCr dapat diperoleh dari *RGB* dengan menggunakan persamaan sebagai berikut :

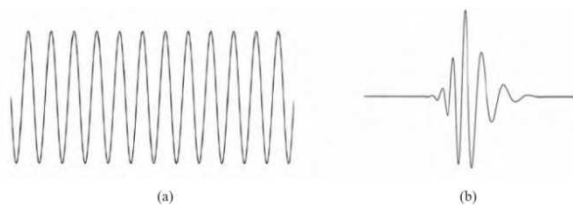
$$Y = 0.229R + 0.587G + 0.114B \quad (1)$$

$$Cb = -0.1687R - 0.3313G + 0.5B + 128 \quad (2)$$

$$Cr = 0.5R - 0.418 - 0.0813B + 128 \quad (3)$$

C. Wavelet

Gelombang (*wave*) adalah sebuah fungsi yang bergerak naik turun ruang dan waktu secara periodik. Sedangkan *wavelet* merupakan gelombang yang dibatasi atau terlokalisasi, atau dapat dikatakan sebagai gelombang pendek. *Wavelet* ini menkonsentrasikan energinya dalam ruang dan waktu sehingga cocok untuk menganalisis sinyal yang sifatnya sementara saja.



Gambar 1. (a) Gelombang (*wave*), (b) *Wavelet*

Wavelet pertama kali digunakan dalam analisis dan pemrosesan sinyal *digital* dari sinyal gempa bumi. Penggunaan *wavelet* pada saat ini sudah semakin berkembang dengan munculnya area sains terpisah yang berhubungan dengan analisis *wavelet* dan teori transformasi *wavelet*. Dengan munculnya area sains ini *wavelet* mulai digunakan secara luas dalam filterisasi dan pemrosesan data, pengenalan citra, sintesis dan pemrosesan berbagai variasi sinyal, kompresi dan pemrosesan citra.

D. Discrete Wavelet Transform

Ide dasar *DWT* sama seperti *continuous wavelet transform* (*CWT*). Di dalam *CWT*, sinyal dianalisis menggunakan seperangkat fungsi dasar yang saling berhubungan dengan penskalaan dan transisi sederhana. Sedangkan di dalam *DWT*, penggambaran sebuah skala waktu sinyal *digital* didapatkan menggunakan teknik filterisasi *digital*. Secara garis besar proses dalam teknik ini adalah melewati sinyal yang akan dianalisis pada *filter* dengan frekuensi dan skala yang berbeda.

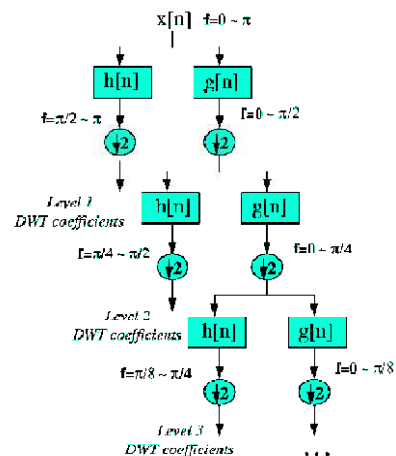
Sebuah sinyal harus dilewatkan dalam dua filterisasi *DWT* yaitu *highpass filter* dan *lowpass filter* agar frekuensi dari sinyal tersebut dapat dianalisis. *Highpass filter* digunakan untuk menganalisis frekuensi tinggi dan *lowpass filter* digunakan untuk menganalisis frekuensi rendah. Analisis terhadap frekuensi dilakukan dengan cara menggunakan resolusi yang dihasilkan setelah sinyal melewati filterisasi. Pembagian sinyal menjadi frekuensi tinggi dan rendah ini disebut dengan dekomposisi. Dekomposisi satu tingkat ditulis dengan persamaan sebagai berikut :

$$y_{tinggi}[k] = \sum_n x[n]h[2k - n] \quad (4)$$

$$y_{rendah}[k] = \sum_n x[n]g[2k - n] \quad (5)$$

$y_{tinggi}[k]$ dan $y_{rendah}[k]$ merupakan hasil dari *highpass filter* dan *lowpass filter* dan sebagai koefisien *DWT* dimana $y_{tinggi}[k]$ adalah detail dari informasi sinyal dan $y_{rendah}[k]$ adalah taksiran dasar dari fungsi penskalaan, $x[n]$ merupakan sinyal asal, $h[n]$ adalah *highpass filter* dan $g[n]$ adalah *lowpass filter*.

Proses dekomposisi dapat dijelaskan seperti gambar berikut :



Gambar 2. Dekomposisi wavelet dengan frekuensi sinyal asal $f=0 \sim \pi$

Proses rekonstruksi diawali dengan menggabungkan koefisien *DWT* dari yang berada pada akhir dekomposisi dengan sebelumnya meng-*upsample* oleh 2 (2) melalui *highpass filter* dan *lowpass filter*. Proses rekonstruksi ini sepenuhnya

merupakan kebalikan dari proses dekomposisi. Sehingga persamaan rekonstruksi pada masing – masing tingkatan dapat ditulis sebagai berikut :

$$x[n] = \sum_k (y_{tinggi} [k] h [-n + 2k]) + (y_{low} [k] g[-n+2k]) \quad (6)$$

Secara umum penyisipan pesan dilakukan dengan cara memodifikasi koefisien pada rentang frekuensi LL, LH, HL, atau HH yang merupakan rentang frekuensi hasil dekomposisi citra menggunakan *wavelet*. Data pesan ini dapat dianggap sebagai rangkaian bilangan w dengan panjang L , yang disisipkan pada koefisien rentang yang dipilih f

Algoritma umum penyisipan pesan pada koefisien adalah :

$$f' = f + \alpha .w(k) , k = 1, \dots, L \quad (7)$$

Dimana α merupakan kekuatan penyisipan yang mengontrol tingkat kekuatan penyisipan pesan dan f' adalah koefisien sinyal asal yang telah dimodifikasi.

E. Steanografi

Steganografi dilihat dari segi bahasa terdiri dari dua kata, yaitu *steganos* dan *graptos* yang diambil dari bahasa Yunani. *Steganos* memiliki arti menyembunyikan, sedangkan *graptos* memiliki arti tulisan. Secara umum steganografi adalah teknik penyisipan pesan ke dalam media.

Ada dua teknik steganografi yang dapat diterapkan pada citra *digital*. Pertama adalah teknik yang bekerja pada *domain spatial*. Teknik pada *domain spatial* sering disebut dengan teknik substitusi. Substitusi dilakukan sedemikian rupa agar indra manusia tidak dapat membedakan adanya pesan yang disisipkan pada media penyisipan pesan. Salah satu metode yang terkenal dalam *domain spatial* adalah metode *Least Significant Byte (LSB)*. Kedua adalah teknik yang bekerja pada *domain transform*. Teknik pada ranah transform memfokuskan penyisipan pesan ke dalam frekuensi dari *cover-file*. Salah satu metode yang bekerja dalam *domain transform* adalah *Discrete Wavelet Transform (DWT)*.

Steganografi memiliki dua buah proses, yaitu penyisipan dan ekstraksi pesan. Proses penyisipan pesan pada steganografi membutuhkan dua buah masukan, yaitu pesan yang ingin disembunyikan dan media penyisipan. Hasil dari proses ini disebut dengan *stego-object*, yaitu suatu media yang mempunyai kemiripan dengan media penyisipan yang telah terdapat pesan tersembunyi di dalamnya.

F. Kriteria Steganografi

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut.

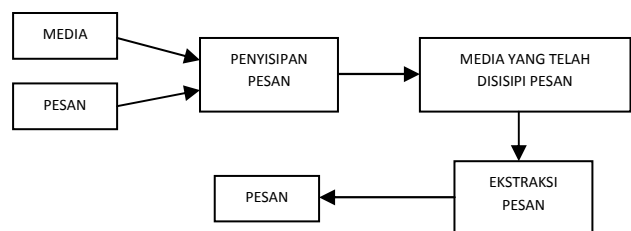
Kriteria yang harus diperhatikan dalam penyembunyian data adalah :

1. *Fidelity*
Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih dapat terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat pesan rahasia.
2. *Robustness*
Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan terhadap citra penampung.
3. *Recovery*
Data yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan dari steganografi adalah penyembunyian data, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

III. PERANCANGAN APLIKASI

A. Blok diagram sistem

Pada sistem steganografi terdiri dari beberapa langkah yang dapat digambarkan menjadi blok diagram dengan model seperti Gambar berikut :



Gambar 3. Diagram Blok Sistem Secara Keseluruhan

Fungsi masing-masing bagian dalam diagram blok ini adalah sebagai berikut :

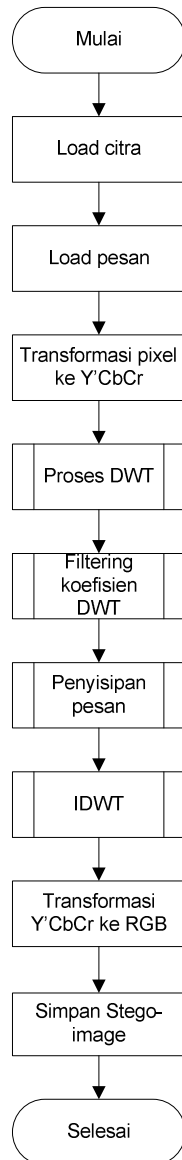
1. Pesan dan media penampung pesan digunakan sebagai *input* sistem.
2. Melakukan *image processing* penyisipan pesan ke dalam media.
3. Proses penyisipan pesan menghasilkan *stego-image*.
4. Melakukan proses ekstraksi pesan dari *stego-image*.

B. Perancangan Perangkat Lunak

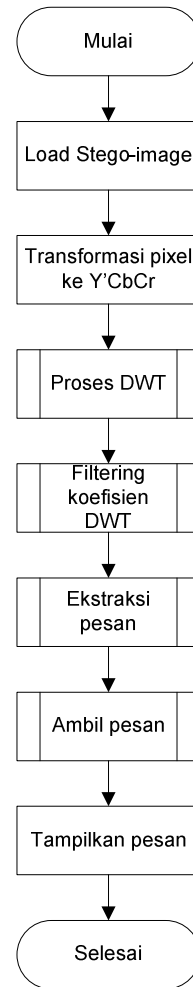
Pada bagian perancangan ini perangkat lunak yang akan dibuat menggunakan bahasa pemrograman *Microsoft Visual Studio C#.NET 2010* dan sistem yang digunakan untuk membangun perangkat lunak ini dirancang dengan spesifikasi mampu melakukan hal-hal berikut :

1. Mengakses data citra yang telah tersimpan di dalam *harddisk* komputer.
2. Mengakses pesan yang akan disisipkan kedalam citra.
3. Melakukan proses transformasi dari pixel ke YCbCr.
4. Melakukan proses DWT.
5. Melakukan proses *filtering* koefisien DWT.
6. Melakukan proses penyisipan pesan.
7. Melakukan proses ekstraksi pesan.

Sedangkan untuk detail desain aplikasi secara umum akan ditunjukkan pada gambar 4 dan 5.



Gambar 4. Detail Desain Aplikasi Penyisipan Pesan.



Gambar 5. Detail Desain Aplikasi Ekstraksi Pesan

C. Cara Kerja Aplikasi

Aplikasi steganografi pada citra digital menggunakan metode *Discrete Wavelet Transform* memiliki cara kerja yang dimulai dari pengambilan citra (*cover-file*) yang akan digunakan sebagai media penyisipan pesan dan pesan rahasia yang ingin disampaikan, kemudian dilakukan proses pengolahan citra penyisipan pesan ke dalam citra sehingga menghasilkan citra yang disisipi pesan (*stego-file*), setelah itu dilakukan proses pengolahan citra mengekstraksi pesan dari *stego-file* sehingga menghasilkan pesan rahasia yang ingin disampaikan

IV. HASIL DAN PEMBAHASAN

A. Pengujian Kualitas Citra Berdasar Nilai PSNR

Tabel 1. Hasil Pengujian Kualitas Citra Pada Gambar KTMRC.

No	Size (px)	Size (kb)	Pesan (karakter)	Size (bytes)	PSNR (dB)
1	586 x 371	637	30	30	99,112

2	586 x 371	637	50	50	98,476
3	586 x 371	637	70	70	95,985
4	586 x 371	637	90	90	91,960
5	586 x 371	637	110	110	91,558

Dari hasil pengujian yang dilakukan pada citra KTMRC yang telah disisipi masing pesan sebesar 30 bytes, 50 bytes, 70 bytes, 90 bytes dan 110 bytes, diperoleh hasil yang nilai PSNR dari masing-masing stego-image berbeda untuk setiap jumlah pesan yang disisipkan.

Dari tabel 1 terlihat bahwa jumlah karakter yang disisipkan pada citra uji berpengaruh terhadap nilai PSNR yang dihasilkan. Semakin banyak karakter yang disisipkan maka semakin berkurang kualitas citra stego-image seiring dengan menurunnya nilai PSNR.

B. Pengujian Tingkat Keberhasilan Ekstraksi Pesan.

Tabel 2. Hasil Pengujian Tingkat Keberhasilan Ekstraksi Pesan.

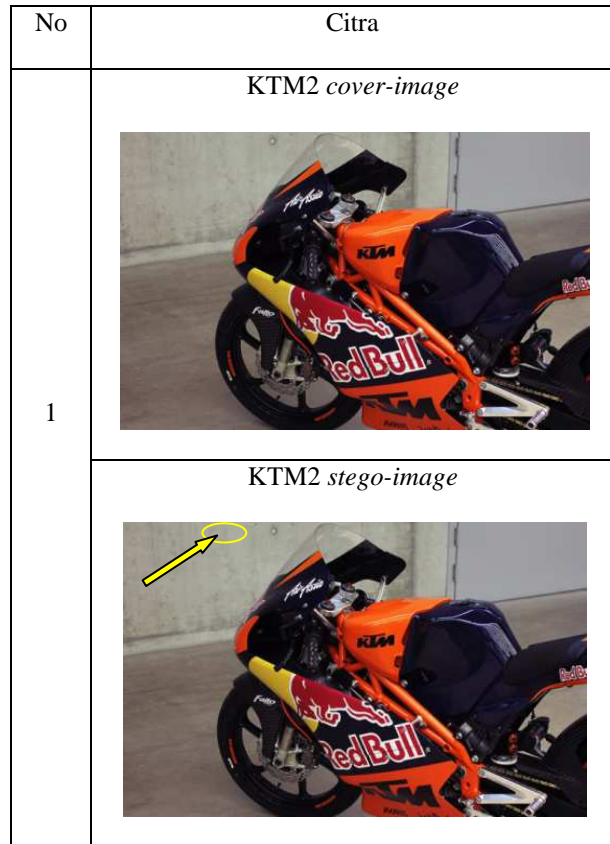
No	Citra	Size (px)	Perubahan secara kasat mata	Status ekstraksi
1	MM99	800 x 450	Tidak	Berhasil
2	Panigale	640 x 426	Tidak	Berhasil
3	KTMRC	586 x 371	Tidak	Berhasil
4	Rossi	480 x 270	Tidak	Berhasil
5	KTM2	586 x 371	Ya	Berhasil
6	Rossi46	480 x 270	Ya	Berhasil

Dari hasil pengujian pada citra percobaan nomor satu sampai dengan empat yang disajikan dalam tabel 2, menunjukkan bahwa citra stego-image tidak mengalami perubahan kualitas citra secara signifikan, perubahan yang tidak nampak dikarenakan ukuran pesan yang disisipkan relatif kecil, yaitu antara 50 bytes sampai dengan 110 bytes.

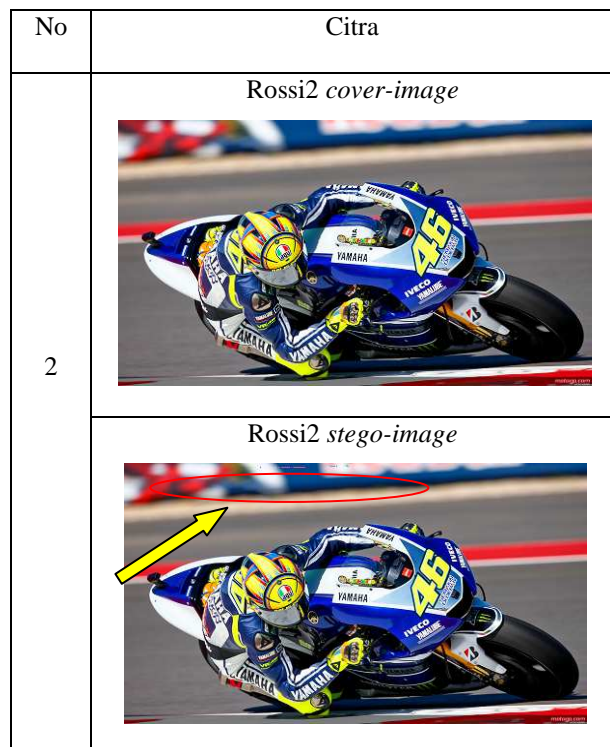
Saat ukuran pesan yang disisipkan berukuran relatif kecil, maka perubahan kualitas citra stego-image tidak dapat terlihat secara kasat mata, sebaliknya saat ukuran pesan yang disisipkan besar maka akan terdapat perubahan kualitas citra yang

dapat diamati secara kasat mata, seperti pada citra nomor lima dan enam yang disajikan pada tabel 2.

C. Pengujian Perubahan Citra Secara Kasat mata.



Gambar 6. Perubahan Citra Secara Kasat Mata (1)



Gambar 7. Perubahan Citra Secara Kasat Mata (2)

Dari hasil pengujian perubahan citra secara kasat mata pada gambar 6 dan 7, terlihat bahwa terjadi perbedaan yang signifikan antara *cover-image* dan *stego-image*. Perbedaan tersebut ditandai dengan panah berwarna kuning. Perbedaan yang terlihat mencolok tersebut disebabkan oleh jumlah pesan yang terlalu besar, sehingga mempengaruhi *pixel image* pada *stego-image* hasil dari proses steganografi.

Selain ukuran pesan yang disisipkan, besarnya resolusi gambar yang digunakan sebagai *cover-image* juga mempengaruhi kualitas citra *stego-image*. Dengan ukuran pesan yang sama, pada gambar 5 dan 6, terlihat bahwa hasil dari perubahan kualitas citra terlihat berbeda, perbedaan perubahan kualitas citra tersebut terjadi dikarenakan ukuran resolusi citra yang dijadikan sebagai *cover-image* berbeda.

V. PENUTUP

A. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, pengujian dan analisis sistem maka dapat diambil kesimpulan sebagai berikut :

1. Resolusi citra yang digunakan sebagai *cover-image* harus ideal dengan ukuran pesan yang akan disisipkan, jika tidak maka akan terlihat perubahan citra *stego-image* yang terlihat secara kasat mata.
2. Terjadinya sedikit perubahan *pixel* yang terlihat secara kasat mata pada *stego-image* tidak menyebabkan terjadinya kerusakan pesan hasil ekstraksi dari *stego-image*.

B. SARAN

Skripsi ini dapat dikembangkan dengan memperbanyak variasi dari format file *cover-image* yang digunakan sebagai media steganografi.

DAFTAR PUSTAKA

- [1] Al-Naima, Fawzi. 2010. *A Modified High Capacity Image Steganography Technique Based on Wavelet Transform*. Iraq: IAJIT.
- [2] Burger, Wilhelm, dkk. 2008. *Digital Image Processing*. New York: Spinger.
- [3] Burrus, C. Sidney, Gopinath, Ramesh A., Guo, Haitao. (1998). *Introduction to Wavelets and Wavelet Transforms: A Primer*. Prentice-Hall, New Jersey.
- [4] Chen Po-Yuech, Lin Hung-Ju. 2006. *A DWT Based Approach for Image Steganography*. Taiwan : IJACE.
- [5] Cole, Eric. 2003. *Hiding in Plainsight : Steganography and the Art of Cover Communication*. Canada: Wiley Publishing.Inc.
- [6] Gonzalez, Rafael C., Woods, R.E., 2002. *Digital Image Processing*. New Jersey : Prentice-Hall, Inc., Upper Saddle River.
- [7] Hayes, Monson H. (1999). *Digital Signal Processing*. McGraw-Hill, New York.
- [8] Munir, Rinaldi. 2006. *Pengolaan Citra Digital*. Bandung: Informatika.
- [9] Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta: Andi.
- [10] Robi Polikar, 'The Story of Wavelets', *In physics and Modern topics in Mechanical and Electrical Engineering*, References Scientific and Eng. Society Press.