PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE LSB DAN DWT

Tugas Akhir

Diajukan oleh:

AGUSTIANTO PURNOMO

71130029

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

YOGYAKARTA

2017

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi, telah membuat banyak perkembangan di dalam kehidupan sehari – hari, seperti berkomunikasi, menyampaikan dan bertukar informasi telah menjadi semakin cepat dan mudah. Tetapi, pertukaran informasi melalui *internet* saat ini masih memiliki banyak celah keamanan sehingga informasi dapat disadap/dicuri oleh pihak ketiga. Celah keamanan tersebut dapat dikurangi dengan beberapa cara, salah satunya dengan menggunakan enkripsi terhadap informasi yang dikirimkan. Salah satu metode enkripsi yang dapat digunakan adalah steganografi.

Steganografi adalah teknik menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Teknik steganografi 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.

Dalam tugas akhir ini, peneliti akan membahas mengenai bagaimana suatu pesan disisipkan kedalam pesan lainnya yaitu citra menggunakan metode *Discrete Wavelet Transform* (DWT), *Least Significant Bit* (LSB), serta melakukan perbandingan pada kualitas citra yang dihasilkan pada setiap metode.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka rumusan masalah penelitian ini adalah:

a. Seberapa besar tingkat keberhasilan citra ketika diproses menggunakan metode DWT dan LSB?

b. Seberapa banyak orang yang dapat membedakan citra asal dan citra hasil steganografi?

1.3 Batasan Masalah

Pada penelitian ini penulis membatasi permasalahan dalam ruang lingkup, sebagai berikut:

a. Penyembunyian pesan dilakukan pada citra digital berformat JPEG, PNG, dan BMP.

b. Algoritma yang digunakan dalam metode DWT dan LSB.

c. Citra digital yang digunakan untuk pengujian adalah *true color*.

d. Aplikasi dibuat pada MATLAB.

e. Parameter pembanding merupakan nilai PSNR dan MSE, serta penambahan ukuran *file* citra setelah disisipi pesan.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan analisa citra steganografi melalui pengujian menggunakan metode DWT dan LSB pada format citra yang berbeda.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini bagi penulis adalah untuk memperluas wawasan dalam menerapkan steganografi pada kasus yang nyata dan juga menyelesaikan tugas akhir perkuliahan.

Manfaat bagi peneliti selanjutnya, diharapkan dengan dilakukannya penilitan ini dapat menjadi bahan acuan untuk penelitian lebih lanjut tentang steganografi. Selain itu hasil perbandingan algoritma yang digunakan penulis juga dapat dijadikan referensi untuk penelitian pada kasus yang sama namun menggunakan algoritma yang berbeda.

1.6 Metodologi Penlitian

Metodologi yang digunakan dalam penelitian adalah sebagai berikut:

1. Studi Literatur

   Pada metode studi literatur, dilakukan pencarian dan pemahaman literatur yang berhubungan dengan penelitian guna dibuatnya aplikasi. Literatur yang digunakan meliputi buku referensi dan dokumentasi internet.

2. Analisis data

   Pada metode ini penulis mempelajari lebih dalam tentang steganografi, dan metode yang digunakan pada penyembunyian pesan beserta teknik ekstraksinya.

3. Perencanaan dan perancangan

   Pada metode ini, dilakukan perencanaan kebutuhan guna proses perancangan aplikasi berdasarkan hasil analisis pada metode sebelumnya mulai dari penggunaan algoritma LSB dan DWT sampai perhitungan nilai PSNR dan MSE sebagai parameter pembanding kualitas citra *cover* sebelum dan sesudah disisipkan pesan rahasia.

4. Implementasi

   Pada metode implementasi ini, aplikasi sudah dibuat secara keseluruhan pada aplikasi pendukung MATLAB mulai dari proses pemilihan citra *cover*, sampai proses penyisipan dan ekstraksi pesan rahasia. Aplikasi pada tahap ini sudah siap untuk dilakukan pengujian.

5. Pengujian

   Pada metode pengujian, aplikasi yang sudah selesai dibuat untuk kemudian diujikan guna mengetahui apakah aplikasi berjalan dengan lancar tanpa ada kekurangan dan kesalahan serta menganalisa hasil uji citra digital dengan acuan data yang diperoleh dan dengan menganalisa lebih dalam mengenai teknik steganografi dan algoritma yang digunakan.

BAB 2
LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam penelitian yang dilakukan oleh Basuki dkk. (2010) dengan judul "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4", menjelaskan bahwa algoritma steganografi LSB bisa digabungkan dengan algoritma kriptografi klasik untuk meningkatkan keamanan data yang disisipi kedalam citra. Kekurangan dari penelitian tersebut adalah program yang dibuat hanya mampu menggunakan 1 jenis format citra saja.

Penelitian lain dilakukan oleh Devi & Jena (2013) dengan judul "A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", menggunakan *pseudo random encoding technique* dimana sebuah *key* digunakan untuk memilih *pixels* secara acak dengan tujuan membuat pola peletakan informasi menjadi lebih sulit diketahui sehingga pesan menjadi lebih aman. Hal ini terbukti dari nilai PSNR milik *pseudo random* lebih tinggi jika dibandingkan dengan nilai PSNR pada LSB tanpa *pseudo random*.

Sedangkan penelitian yang sama tentang steganografi dengan menggunakan metode DWT oleh Bhattacharyya & Sanyal (2012) yang berjudul "A Robust Image Steganography using DWT Difference Modulation (DWTDM)" menggunakan DWT, metode baru dalam teknik mengubah domain citra stenografi DWT *Difference Modulation* (DWTDM) disajikan dimana data rahasia tertanam dalam perbedaan koefisien DWT yang berdekatan. Rentang dinamis dari perbedaan DWT dipertimbangkan, sementara ekstraksi data yang menghasilkan teknik *stegano* yang efisien dan kuat yang dapat menghindari berbagai serangan terhadap *cover-image* dan bekerja dengan baik.

Penelitian lainnya dilakukan oleh Bhattacharya dkk. (2012) dengan judul "A Session based Multiple Image Hiding Technique using DWT and DCT" meneliti

tentang steganografi dengan metode DWT dan DCT yang digabungkan untuk proses stegano, dengan sebelumnya membagi citra menjadi 3 buah citra dengan warna dasar yaitu merah, hijau dan biru (RGB). Setelah citra dibagi menjadi 3 buah warna dasar maka akan dilakukan proses DWT pada masing-masing citra warna dasar, dan proses DCT dilakukan pada *sub band* HH. 3 buah gambar rahasia akan dikonversi menjadi vector 1-D, kemudian frekuensi tertentu dipilih untuk kemudian diproses menggunakan pseudo random 2D. Setelah proses *embedding* dilakukan pada masing-masing citra warna dasar maka akan dilakukan proses *inverse* untuk mendapatkan bentuk spasial, yang selanjutnya 3 buah citra warna dasar tersebut akan digabungkan kembali untuk mendapatkan citra *stegano* yang berwarna. Hasil yang didapat dengan melakukan *embedding* pada frekuensi yang acak adalah semakin sulit untuk mendeteksi adanya sebuah pesan rahasia yang tertanam menggunakan proses steganalysis yang umum digunakan. Dan juga PSNR yang didapat tidak mengecewakan.

2.2 Landasan Teori

2.2.1 Pengolahan Citra Digital

"Pengolahan citra digital adalah proses manipulasi dan modifikasi pada citra untuk mendapatkan hasil tertentu dengan berbagai macam cara" (Kadir, 2013).

2.2.2 Kriptografi

Menurut Kamus Besar Bahasa Indonesia, kriptografi adalah penyelidikan tentang kode rahasia; teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut.

"Kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya" (Rakhmat & Fairuzabadi, 2010).

Dalam kehidupan sehari-hari tidak semua informasi yang akan kita berikan kepada seseorang bersifat umum, oleh karena itu informasi yang bersifat bukan untuk komsumsi umum atau pribadi sebaiknya diamankan dengan menggunakan kriptografi.

2.2.3 Steganografi

Menurut Bhattacharya, Tanmay, Dey (2012), Steganografi adalah proses penyembunyian pesan rahasia didalan sebuah pesan biasa dan melakukan ekstrasi pesan ketika sampai pada tujuannya. Steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang berarti tersembunyi atau terselubung, dan *graphein* yang artinya menulis. Steganografi dapat diartikan tulisan tersembunyi (*covered writing*). Steganografi adalah ilmu dan seni menyembunyikan informasi rahasia di dalam pesan lain sehingga keberadaan informasi rahasia tersebut tidak dapat diketahui.

Steganografi membutuhkan dua properti, yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, *video*, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lain. Proses penyisipan pesan ke dalam media *covertext* dinamakan *encoding*, sedangkan ekstraksi pesan dari *stegotext* dinamakan *decoding*. Kedua proses ini mungkin memerlukan kunci rahasia (yang dinamakan *stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi.

2.2.4 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 *pixel*. Untuk menunjukan tingkat intensitas cahaya suatu *pixel*, seringkali digunakan bilangan bulat 0 untuk warna hitam dan 255 untuk warna putih" (Kadir, 2013). 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).

2.2.4.1 JPEG (*Joint Photographic Experts Group*)

JPEG merupakan skema kompresi citra bitmap. Karena ukuran file yang relatif lebih kecil dan ringan maka format ini digunakan di kalangan fotografer maupun desainer *webpage* karena mudah ditampilkan pada halaman *web*.

Keuntungan lain dari format JPEG adalah dapat diterima pada hampir semua program-program komputer. Sedangkan kelemahan dari format JPEG ini adalah kompresi citra pada format ini mempengaruhi kualitas citra itu sendiri.

2.2.4.2 PNG (*Portable Netwok Graphics*)

Portable Network Graphics atau PNG asal mulanya dikembangkan sebagai pengganti format GIF karena adanya penerapan lisensi GIF. Format ini mendukung pemampatan data tanpa menghilangkan informasi aslinya. Tipe file PNG merupakan kompresi citra yang bagus dengan warna yang lebih banyak. Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (*lossless compression*). Kelebihan file PNG adalah adanya warna transparan dan *alpha*. Warna *alpha* memungkinkan sebuah citra transparan, tetapi citra tersebut masih dapat dilihat mata seperti samar-samar atau bening. Kekurangan dari PNG adalah ukurannya yang besar.

2.2.4.3 BMP

Bitmap merupakan representasi dari citra grafis yang terdiri dari susunan titik (*pixel*) yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu bit data (untuk citra hitam putih) atau lebih (untuk citra berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam citra ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 800×600).

Keuntungan dan kekurangan dari citra *bitmap* tergantung dari resolusinya. Semakin besar resolusi citra akan semakin besar pula ukuran filenya. Resolusi yang semakin tinggi membuat gambar tidak mudah pecah ketika di *zoom*.

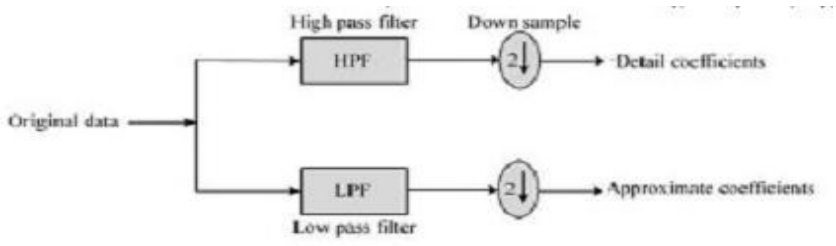
2.2.5 Discrete Wavelet Transform (DWT)

"*Discrete Wavelet Transform* (DWT) merupakan metode yang dapat membagi informasi dari suatu citra menjadi pendekatan dan detail sinyal. Adapun LL *band* meliputi koefisien *low pass* dan pendekatan terhadap suatu citra serta detail sub signal lainnya yang menunjukkan rincian vertikal, horizontal, atau diagonal atau perubahan di dalam suatu citra" (Dinesh, 2012)**.**

Metode DWT merepresentasikan citra sebagai jumlah dari fungsi *wavelet*, yang dikenal sebagai *wavelets*, dengan lokasi dan skala yang berbeda. Metode DWT merepresentasikan data dalam himpunan koefisien *high pass* (detil) dan *low pass* (pendekatan). Data masukan diteruskan melalui himpunan filter *low pass* dan *high pass*. Hasil keluaran filter *high pass* dan *low pass* diperkecil sampelnya menjadi dua. Hasil keluaran filter *low pass* merupakan koefisien pendekatan dan hasil keluaran filter *high pass* merupakan koefisien detil. Adapun mata manusia kurang sensitif terhadap sinyal frekuensi tinggi.

Mata manusia pada umumnya menemukan detil secara lebih baik pada area lebih kecil dan hanya mengingat keseluruhan area yang diperbesar. Prosedur satu dimensi (1-D) ditunjukkan pada gambar 2.1.

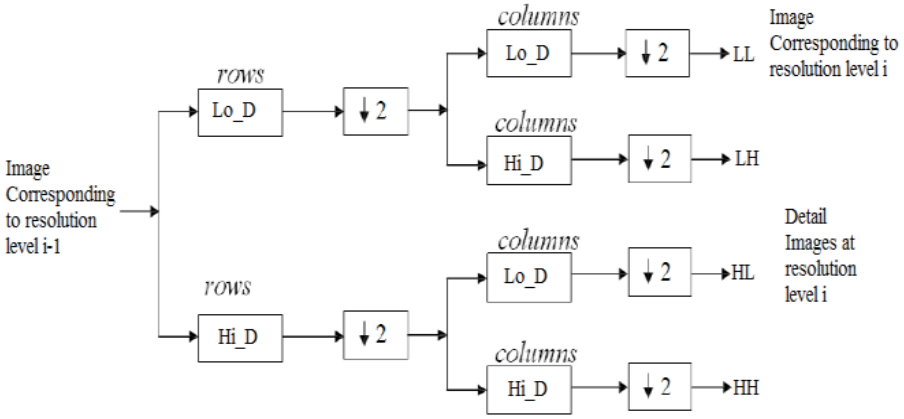
Pada kasus 2-D DWT, data masukan diteruskan melalui himpunan filter *low pass* dan *high pass* pada dua arah, yaitu baris dan kolom. Hasil keluarannya kemudian diperkecil menjadi 2 sampel pada masing-masing arah sebagaimana dalam kasus 1-D DWT.



Gambar 2.1. Blok diagram terusan 1-D DWT

(Archana., et al2013)

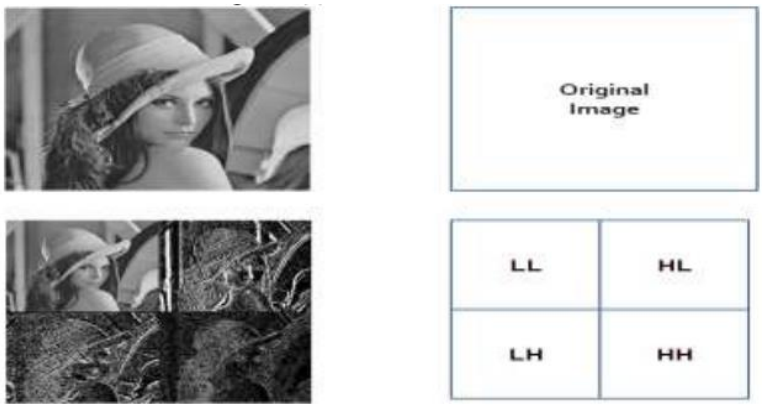
Sebagaimana yang ditunjukkan pada gambar 2.2, hasil keluaran didapatkan dari himpunan 4 koefisien LL, HL, LH, dan HH. Huruf pertama merepresentasikan transformasi pada baris, sedangkan huruf kedua merepresentasikan transformasi pada kolom.



Gambar 2.2. Blok diagram terusan 2-D DWT

(Dinesh, 2012)

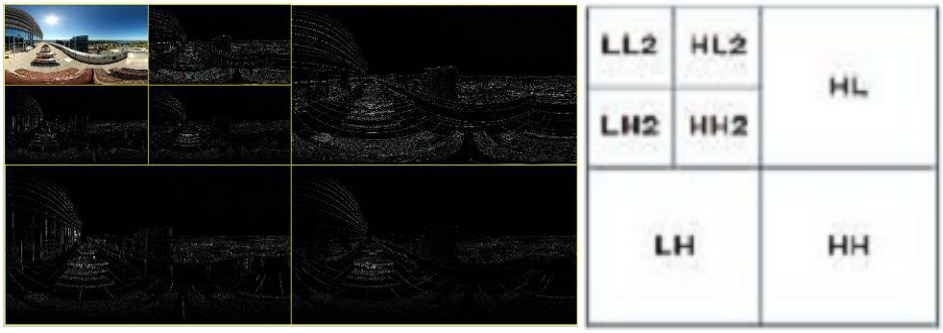
Alfabet L berarti *low pass signal* dan H berarti *high pass signal*. Sinyal LH berarti *low pass signal* pada baris dan *high pass* pada kolom. Oleh karena itu, sinyal LH memuat elemen horisontal. Demikian halnya dengan HL dan HH, dimana masing-masing sinyal tersebut memuat elemen vertikal dan diagonal.



Gambar 2.3. Ilustrasi 1D DWT

(Archana., et al2013)

Gambar ilustrasi hasil keluaran 1D DWT dan 2D DWT ditunjukkan pada gambar 2.3 dan gambar 2.4.



Gambar 2.4. Ilustrasi 2D DWT

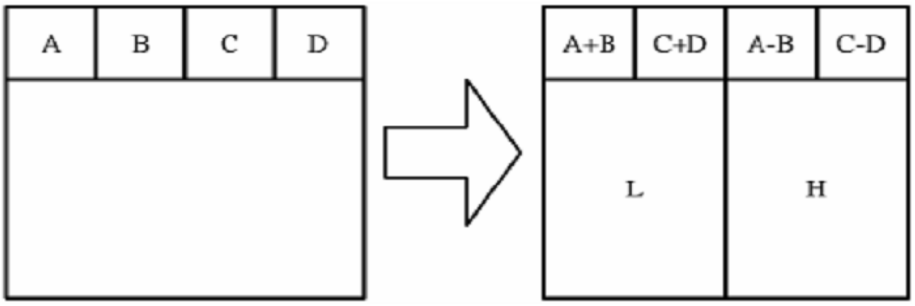
(Dinesh, 2012)

2.2.6 Haar DWT

Berdasarkan penelitian Chen (2006) Transformasi Haar-DWT merupakan bentuk DWT paling sederhana dan terdiri dari dua operasi utama: operasi horisontal serta operasi vertikal. Prosedur detil dari 2D Haar DWT dapat dijabarkan sebagai berikut:

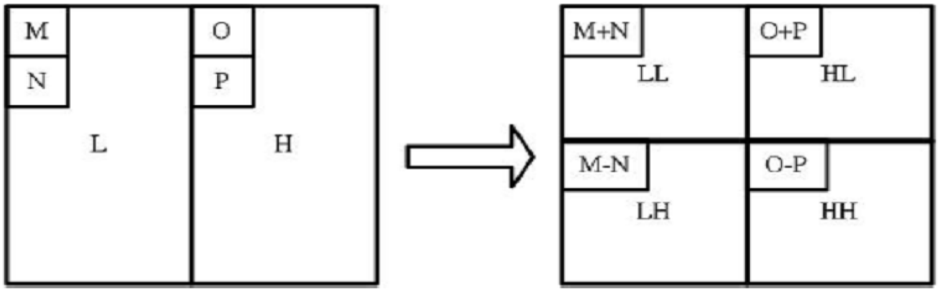
Tahap 1: Pertama, melakukan proses scan terhadap *pixel* dari kiri ke kanan secara horisontal. Kemudian lakukan operasi penjumlahan dan pengurangan pada *pixel* disebelahnya (*neighbouring pixel*). Simpan hasil penjumlahan disebelah kiri dan hasil pengurangan disebelah kanan seperti yang ditunjukkan pada gambar 2.5. Ulangi kembali operasi tersebut hingga seluruh baris berhasil diproses. Hasil penjumlahan *pixel* merepresentasikan bagian berfrekuensi rendah (disimbolkan dengan L) dan hasil pengurangan merepresentasikan bagian berfrekuensi tinggi dari citra asli (disimbolkan dengan H).

Tahap 2: Kedua, lakukan proses *scan pixel* dari atas ke bawah secara vertikal. Kemudian lakukan operasi penjumlahan dan pengurangan pada *pixel* disebelahnya (*neighboouring pixel*) dan simpan hasil penjumlahan pada bagian atas dan hasil pengurangan pada bagian bawah seperti yang ditunjukkan pada gambar 2.6.



Gambar 2.5. Operasi Horisontal pada metode DWT

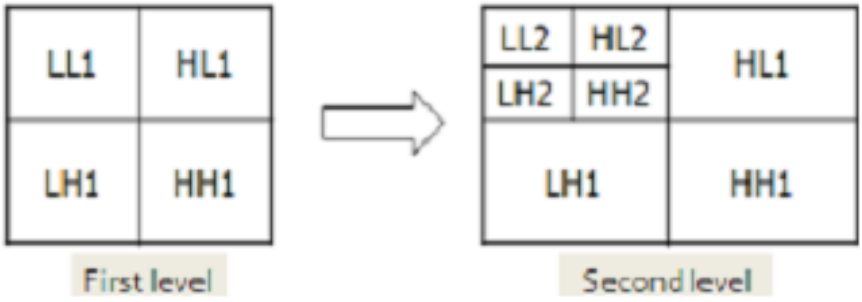
(Archana., et al 2013)



Gambar 2.6. Operasi Vertikal pada metode DWT

(Archana., et al 2013)

Ulangi kembali operasi tersebut hingga seluruh kolom berhasil diproses. Terakhir akan didapatkan 4-sub-himpunan yang disimbolkan dengan LL, HL, LH, dan HH. Adapun sub-himpunan LL merupakan bagian berfrekuensi rendah karena itu memiliki kemiripan dengan citra asli. Keseluruhan prosedur yang dijabarkan diatas tersebut disebut 1D Haar-DWT. Proses 2D DWT dengan mengaplikasikan *Haar-DWT* pada bagian LL. Gambar 2.7 menunjukkan proses 2D DWT.



Gambar 2.7. Proses 2D DWT

(Archana., et al 2013)

2.2.7 Least Significant Bit (LSB)

Menurut Rakhmat & Fairuzabadi (2010) metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext*. Pada susunan bit di dalam sebuah *byte* (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh *byte* 11010010, angka bit 1 (pertama, digaris-bawah) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.

Misalkan segmen *pixel-pixel* citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110

10010110 11001001 11111001 10001000 10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi (digaris-bawah):

00110011 10100011 11100011 10101010 00100110

10010111 11001000 11111001 10001001 10100011

2.2.8 *Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan *decibel* (dB). Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan *Mean Square Error* (MSE). Adapun MSE adalah nilai *error* kuadrat rata-rata antara citra *cover* dengan citra steganografi, secara matematis dapat dirumuskan sebagai berikut:

$$\boldsymbol{MSE = \frac{1}{MN} \sum_{i=1}^{M} \blacksquare \sum_{j=1}^{N} [I(x,y) - K(x,y)]^2} \quad [1]$$

Diketahui:

MSE = Nilai Mean Square Error citra steganografi

M = Panjang citra stego (dalam *pixel*)

N = Lebar citra stego (dalam *pixel*)

I (x,y) = nilai *pixel* dari citra *cover*

K(x,y) = nilai *pixel* pada citra stego

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan sebagai berikut :

$$PSNR = 10.log_{10}\left(\frac{MAX_i^2}{MSE}\right) = 10.log_{10}\left(\frac{MAX_i}{\sqrt{MSE}}\right) \quad [2]$$

Diketahui:

MSE = nilai MSE,

MAX_i = nilai maksimum dari *pixel* citra yang digunakan

Semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi. Nilai acuan PSNR bisa dikatakan baik adalah bernilai ≥ 30.

Daftar pustaka

Archana, Vaidya., Pooja, N., Rita, K., Fegade., Madhuri, A., Bhavsar., dan Raut, P.V. (2013). Image Steganography using DWT and Blowfish Algorithms. IOSR Journal of Computer Engineering. Vol. 8, Issue 6, PP 15-1.

Bhattacharyya, S., & Sanyal, G. (2012). A Robust Image Steganography using DWT Difference Modulation (DWTDM). International Journal of Computer Network and Information Security, 4(7), 27-40.

Bhattacharya, S., Tanmay, Dey, Nilanjan, Chaudhuri, S.R. Bhadra. (2012). A Session based Multiple Image Hiding Technique using DWT and DCT. International Journal of Computer Applications. Vol. 38, No. 5

Chen, P., & Lin, H. (2006). A DWT Based Approach for Image Steganography. International Journal of Applied Science and Engineering, Vol. 4, No. 3, 275-290.

Devi, K. J., & Jena, S. K. (2013). A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique.

Dinesh, Y., dan Ramesh, A.P. (2012). Efficient Capacity Image Steganography by Using Wavelets. International Journal of Engineering Research and Applications (IJERA). Vol. 2, Issue 1, PP 251-259.

Kadir, A., & Susanto. A. (2013). Teori dan Aplikasi Pengolahan Citra. Yogyakarta, Indonesia: Penerbit Andi.

Rakhmat, Basuki, & Fairuzabadi, Muhammad. (2010). Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4. Jurnal Dinamika Informatika. Vol. 5, No.2