`

Key word : Steganography, Haar Discret Wavelet Transform (DWT) method, Baker Map

1. PENDAHULUAN

Salah satu metode yang cukup populer untuk menyembunyikan pesan ke dalam file gambar adalah *Steganografi*. Maka yang menjadi pokok permasalahan adalah bagaimana cara menyisipkan pesan pada sebuah citra bitmap 24 bit tanpa harus mengubah karakteristik citra digital yang berfungsi sebagai *cover image* dan pesan tersebut tidak akan diketahui oleh orang lain.
Untuk memecahkan masalah tersebut maka penulis akan mendesain dan mengimplementasikan sistem steganografi berbasis Haar DWT (*Discret Wavelet Transform*) dengan enkripsi *secret message* menggunakan Baker Map. Algoritma Baker Map adalah mentransformasikan citra dengan cara mengacak koordinasi piksel aslinya.
Setelah proses enkripsi, dilakukan metode DWT. Metode DWT adalah teknik pembagian *subband-subband* berdasarkan frekuensi yang berbeda-beda kedalam beberapa *level* pendekomposisian.

2. DASAR TEORI

2.1. Citra Digital

Citra digital dapat didefinisikan 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. Citra digital dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* - RGB).

2.1.1 Dasar Warna

RGB adalah suatu model warna yang terdiri dari merah, hijau, dan biru, digabungkan dalam membentuk suatu susunan warna yang luas. Setiap warna dasar, misalnya merah, dapat diberi rentang-nilai. Untuk monitor komputer, nilai rentangnya paling kecil = 0 dan paling besar = 255.

2.1.2 Citra Biner

Citra biner diperoleh melalui proses pemisahan piksel-piksel berdasarkan derajat keabuan yang dimilikinya. Piksel yang memiliki derajat keabuan lebih kecil dari nilai batas yang ditentukan akan diberikan nilai 0, sementara piksel yang memiliki derajat keabuan yang lebih besar dari batas akan diubah menjadi bernilai 1.

2.1.3 Citra Bitmap

Citra disimpan di dalam berkas (file) dengan format tertentu . Format citra yang baku di lingkungan system operasi Microsoft Windows dan IBM OS/2 adalah berkas *bitmap* (BMP). Format BMP mempunyai kelebihan dari segi kualitas gambar, yaitu tidak dimampatkan sehingga tidak ada informasi yang hilang.

2.2. Steganografi

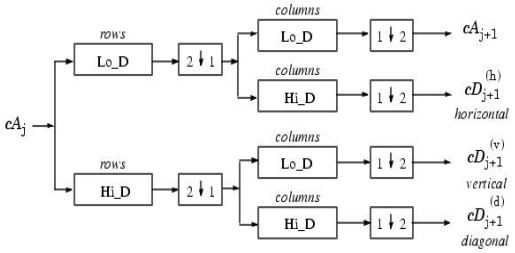
2.2.1. Pengertian Steganografi

Steganografi adalah teknik menyembunyikan data rahasia di dalam media citra digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain. Steganografi membutuhkan empat properti yaitu: wadah penampung (*cover image*) , data rahasia yang akan disembunyikan (*secret message*), kunci penyisipan (*Stego-key*), dan *cover image* yang telah disisipi *secret message (stego image)* . Kriteria dari steganografi adalah sebagai berikut :

- *Fidelity*:Mutu citra penampung tidak jauh berubah setelah penambahan data rahasia.
- *Robustness*:Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra.
- *Recovery*:Data yang disembunyikan harus dapat diungkapkan kembali.

2.3. Metoda DWT

Prinsip dasar dari *DWT* adalah bagaimana cara mendapatkan representasi waktu dan skala dari sebuah sinyal menggunakan teknik pemfilteran digital dan operasi *sub-sampling*. Dimana sinyal pertama kali dilewatkan pada rangkaian *high-pass filter* dan *low-pass filter*, kemudian setengah dari masing-masing keluaran diambil sebagai *sample* melalui operasi *sub-sampling*. Proses ini disebut sebcagai proses dekomposisi.



Gambar 1 *Two-Dimensional* DWT

Dimana:
cA_j = Citra *input*
cA_{j+1} = Koefisien aproksimasi (LL)
$cD^{(h)}_{j+1}$= Koefisien detail horizontal (LH)
$cD^{(v)}_{j+1}$= Koefisien detail vertikal (HL)
$cD^{(d)}_{j+1}$= Koefisien detail diagonal (HH)