SIMULASI DAN ANALISIS STEGANALISIS CITRA DOMAIN *DISCRETE MULTIWAVELET TRANSFORM* (DMWT) MENGGUNAKAN METODE *K-NEAREST NEIGHBOR* (K-NN)

SIMULATION AND ANALYSIS IMAGE STEGANALYSIS DISCRETE MULTIWAVELET TRANSFORM (DMWT) DOMAIN USING K-NEAREST NEIGHBOR (K-NN) METHOD

Diati Levi Putri [1], Dr. Ir. Bambang Hidayat, DEA.[2], I Nyoman Apraz Ramatryana, ST., MT.[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom

diatileviptr@gmail.com, [1] bbhtelkom@gmail.com, [2] ramatryana@gmail.com [3]

Abstrak

Pada era ini teknologi sudah berkembang sangat pesat. Terlebih lagi dibidang telekomunikasi baik pertukaran informasi suara maupun data. Semakin berkembang teknologi maka ruang pribadi semakin menipis. Makadari itu lahirlah *steganography* yang merupakan suatu teknik untuk menyisipkan suatu informasi tersembunyi kedalam suatu media baik suara, video maupun data yang dapat mengirimkan suatu informasi tanpa diketahui oleh pihak lain. Disisi lain *steganography* memiliki efek negatif dimana terdapat beberapa pihak yang menyalahgunakan penggunaan *steganography* untuk mengirimkan suatu pesan atas dasar kriminalitas. Maka dari itu lahirlah *steganalysis* yang keberadaannya untuk menyerang *steganography* dengan mengetahui ada atau tidaknya pesan tersisipi dalam suatu media. Pada penelitian *steganalysis* kali ini merupakan *steganalysis* dalam *Domain Discrete Multiwavelet Transform* (DMWT) dengan metode klasifikasi K-NN pada citra. Dari hasil pengujian berdasarkan penggunaan level DMWT dihasilkan akurasi 56,12% pada penggunaan DMWT Level 1, 54,58% untuk DMWT level 2, 53,16% untuk DMWT level 3, 51,58% untuk DMWT level 4, dan 51,24% untuk DMWT level 5. Setelah itu pengaruh ukuran gambar pada akurasi performansi citra yaitu ukuran 128 sebesar 49,83%, 256 sebesar 60,41%, dan 512 sebesar 56%. Pengaruh pengujian nilai K pada K-NN terhadap performansi akurasi yaitu nilai K=1 sebesar 83,75%, K=3 sebesar 82,5%, K=7 sebesar 86,25%, dan K=9 sebesar 81,25%. Pengaruh penggunaan jenis K-NN terhadap akurasi performansi yaitu, akurasi K-NN jenis *Euclidean* sebesar 78%, *Cityblock* sebesar 86%, *Cosine* sebesar 74%, dan *Correlation* sebesar 96%. Pengaruh ukuran pesan terhadap akurasi performansi yaitu, penyisipan ukuran pesan 1KB sebesar 63,33%, penyisipan ukuran pesan 3KB sebesar 61,66%, penyisipan ukuran pesan 5KB sebesar 70%, dan penyisipan pesan secara sepenuhnya atau *full* sebesar 73,33%.

Kata Kunci : *Steganalysis, Discrete Multi Wavelet Transform* (DMWT), *K-Nearest Neighbor* (K-NN)

Abstract

In this era, technology has grown rapidly especially in telecommunication field to exchange information in form of voice or data. The more technology grow, the smaller private space. That is why steganography, a technique to insert hidden information into a media including voice, video, or data that can send information without being known by anyone else appears. In the other side, steganography has a negative impact in which some people misuse it to send information in purpose of criminality. Based on that reason, steganalysis appears to attack steganography by knowing whether hidden message does exist or not in a media. In this research, the steganalysis is in Domain Discrete Multiwavelet Transform (DMWT) with K-NN classification method on image. From the test result based on DMWT level usage, the accuracy result is 56,12% for level 1 DMWT, 54,58% for level 2 DMWT, 53,16% for level 3 DMWT , 51,58% for level 4 DMWT, 51,24% for level 5 DMWT. While the effect of image size to the image performance accuracy is 49,83% for 128, 60, 41% for 256, 56% for 512. The effect of K value used in K-NN to the accuracy is 83,75% for K=1, 82,5% for K=3, 86,25% for K=7, 81,25% for K=9. The effect of sort of K-NN used to the performance accuracy is 78% for Euclidean K-NN, 86% for Cityblock K-NN, 74% for Cosine K-NN, and 96% for Correlation. The effect of image size to performance accuracy is 63,33% for 1KB message insertion, 61,66% for 3KB message insertion, 70% for 5KB message insertion, and 73,33% for full message.

Keyword : Steganalysis, Discrete Multiwavelet Transform (DMWT), K-Nearest Neighbor (K-NN)

1. Pendahuluan

Seiring dengan perkembangan era globalisasi semakin meningkat pula kebutuhan akan teknologi informasi. Semakin banyak tuntukan atau permintaan akan kebutuhan teknologi mengakibatkan menipisnya ruang *privacy* seseorang. Oleh karna itu, terciptalah *steganography* yang merupakan teknik atau cara penyisipan suatu pesan rahasia kedalam teks, gambar maupun video untuk menyembunyikan kode atau pesan rahasia dari orang tertentu.

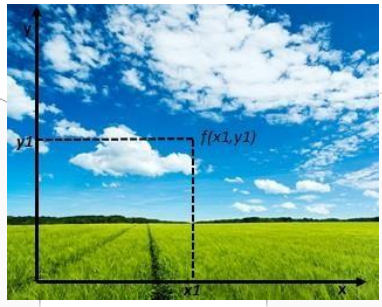
Belakangan ini sudang sering terjadi penyalahgunaan dalam penggunaan *steganography* diantaranya digunakan untuk menyisipkan suatu pesan atau kode tertentu atas dasar kriminalitas. Oleh karena itu, lahirnya *steganalysis* yang merupakan salah satu cara untuk menganalisis *steganography* dengan mengidentifikasi apakah suatu media pernah disisipi suatu pesan rahasia atau tidak.

Berdasarkan pada penelitian sebelumnya, dalam tugas akhir ini telah disimulasikan sebuah skema *steganalysis* citra digital dengan menggunakan *multiwavelet* sebagai metode identifikasi ekstraksi ciri dan menggunakan metode K-NN(*K-Nearest Neighbor*) sebagai klasifikasi yang akan dilakukan perhitungan nilai akurasi dari setiap pengujian yang digunakan. Setelah itu dibuat persentase hasil dari perhitungan terhadap akurasi nya sehingga dapat dilihat performansi dari sistem yang telah dibuat pada tugas akhir ini.

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, hal tersebut diilustrasikan pada Gambar 2.1.[1]

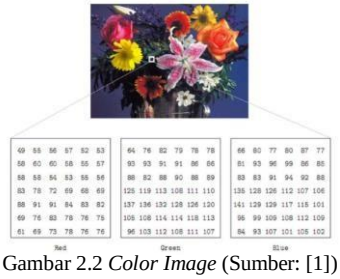


Gambar 2.1 Koordinat spasial citra

Pengolahan citra digital merupakan teknik atau tata cara mengolah citra. Terdapat beberapa aplikasi dalam pengolahan citra digital, diantaranya *color image*, *grayscale*, dan *binary image*.

2.1.1 *Color Image* atau RGB (*Red, Green, and Blue*)

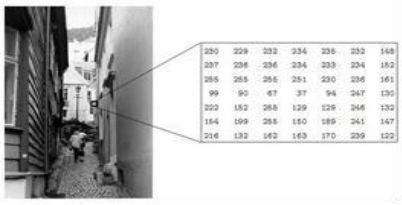
Terdapat beberapa warna tertentu pada color image diantaranya merah (*Red*), hijau (*Green*), dan biru (*Blue*) dimana setiap warna memiliki nilai piksel tersendiri. RGB ini terdiri dari tiga matriks yang mewakili nilai-nilai merah, hijau dan biru untuk setiap pikselnya, seperti yang ditunjukkan Gambar 2.2



Gambar 2.2 *Color Image* (Sumber: [1])

2.1.2 *Grayscale*

Citra digital *grayscale* setiap pikselnya mempunyai warna gradasi mulai dari putih sampai hitam. Rentang warna pada black and white sangat cocok digunakan untuk pengolahan file gambar. Salah satu bentuk fungsinya digunakan dalam kedokteran (*X-ray*).



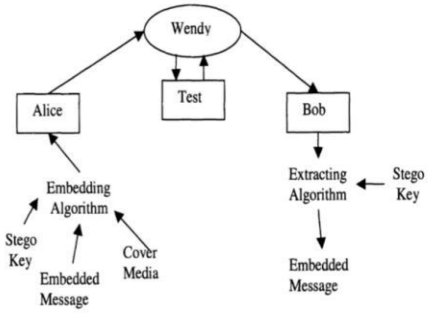
Gambar 2.3 *Grayscale*

2.1.3 Binary Image

Binary Image merupakan hasil pengolahan dari *black and white* dengan menggunakan fungsi.

2.2 *Steganography*

Steganography yang merupakan teknik atau cara penyisipan suatu pesan rahasia kedalam teks, gambar maupun video untuk menyembunyikan kode atau pesan rahasia dari orang tertentu. maka arti secara harfiah berarti menulis tersembunyi. *Steganography* menggunakan teknik untuk menyampaikan informasi dengan cara yang tersembunyi[2]. Gambar 2.4 dibawah ini merupakan salah satu contoh analogi dengan menggunakan *steganography*.



Gambar 2.4 *Framework of Steganography* (Sumber: [3])

Sebuah informasi yang tersembunyi ditandai dengan memiliki tiga aspek yang berbeda, diantaranya *capacity, security*, dan *robustness.*

Gambar 2.5 *Information-hiding system features*

2.3 *Steganalysis*

Steganalysis merupakan suatu teknik atau cara untuk mematahkan *steganography* dimana untuk mengetahui suatu media tersisipi pesan rahasia atau tidak.[4] Citra sangat sering digunakan dalam *steganalysis* sebagai pembawa karna jumlah nya yang banyak dan memiliki resolusi piksel yang tinggi.

2.3.1 Klasifikasi *Steganalysis*

Terdapat dua klasifikasi pada *steganalysis*, diantaranya:[4]

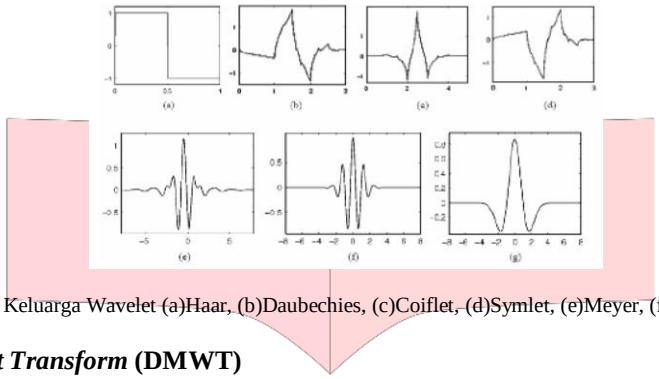
1. *Specific Steganalysis*: merupakan pendekatan secara spesifik yang menggambarkan kelas pada teknik *steganalysis* citra yang bergantung pada algoritma yang digunakan serta memiliki tingkat keberhasilan yang tinggi untuk mendeteksi ada atau tidaknya pesan rahasia
2. *Generic Steganalysis:* disebut dengan *blind steganalysis* yang bekerja dengan baik pada algoritma yang diketahui maupun tidak tapi memiliki akurasi yang akurat dibanding *spesific* steganalysis.

2.4 Transformasi Citra

Terdapat beberapa transformasi yang sering digunakan dalam citra untuk mempermudah dalam pengolahannya. Berikut merupakan contoh penggunaan transformasi citra:

2.4.1 Discrete Wavelet Transform (DWT)

Wavelet merupakan keluarga dari turunan fungsi tunggal yang ditranslasikan dan didilatasikan. Induk wavelet (*mother wavelet*) menghasilkan semua fungsi wavelet melalu translasi dan penskalaan oleh karena itu induk wavelet juga akan menentukan karakteristik dari transformasi wavelet yang dihasilkan. Pada Gambar 2.6 merupakan fungsi-fungsi yang termasuk didalam keluarga wavelet.



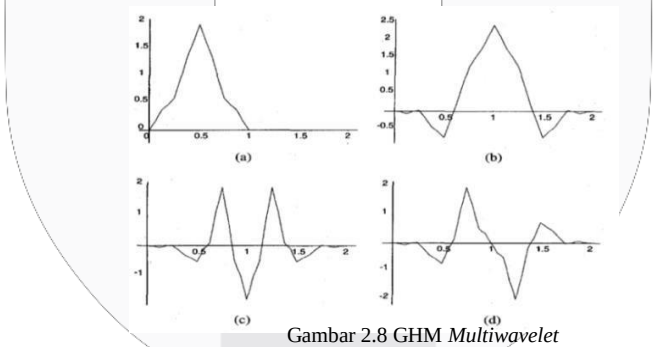
Gambar 2.6 Keluarga Wavelet (a)Haar, (b)Daubechies, (c)Coiflet, (d)Symlet, (e)Meyer, (f)Morlet, (g)Mexican Hat.

2.4.2 *Discrete Multiwavelet Transform* (DMWT)

DMWT merupakan penggunaan lebih dari satu skala wavelet fungsi untuk mewakili sinyal dimana dekomposisi dapat diimplementasikan dengan *filter bank* .[5]

Dimana filter H_k merupakan *low pass filter dan* G_k merupakan *high pass multi wavelet filter banks*. Koefisien filter merupakan nilai matriks pada DMWT yang memberikan nilai yang lebih dibandingkan dengan wavelet skalar.

2.4.2.1 *Geronimo, Hardin, and Massopust Multiwavelet* (GHM Multiwavelet)



Gambar 2.8 GHM *Multiwavelet*
(a) dan (b) merupakan fungsi penskalaan $\phi_1(t)$ dan $\phi_2(t)$
(c) dan (d) merupakan fungsi wavelet $\psi_1(t)$ dan $\psi_2(t)$

Terdapat dua fungsi penskalaan dan fungsi induk yang sesuai dengan wavelet dimana mereka dapat menghasilkan persamaan matriks berikut:[5]

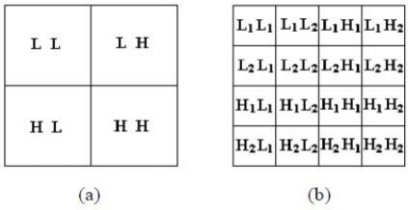
$$\left\{\Phi(t)=\begin{bmatrix}\varphi_1(t)\\ \varphi_2(t)\end{bmatrix}=H_0\Phi(2t)+H_1\Phi(2t-1)+H_2\Phi(2t-2)+H_3\Phi(2t-3)\right\} \quad (2.9)$$

$$\left\{\psi(t)=\begin{bmatrix}\psi_1(t)\\ \psi_2(t)\end{bmatrix}=G_0\phi(2t)+G_1\phi(2t-1)+G_2\phi(2t-2)+G_3\phi(2t-3)\right\} \quad (2.10)$$

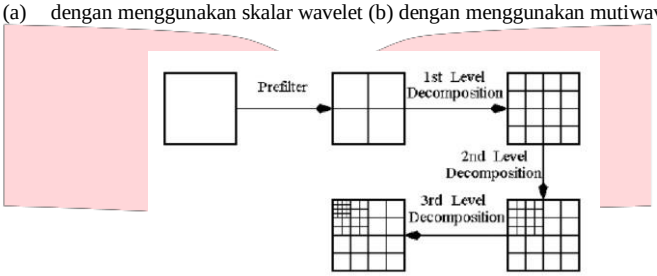
Pada Persamaan (2.9) merupakan fungsi penskalaan $\varphi_1(t)$ dan $\varphi_2(t)$ dengan koefisien LPF dan pada persamaan (2.10) merepresentasikan hubungan fungsi wavelet $\psi_1(t)$ dan $\psi_2(t)$ dengan koefisien HPF.

2.4.2.2 *Multiwavelet Filter Banks*

Penggunaan untuk 1 level dekomposisi akan menghasilkan 16 *subband* yang dihasilkan dari empat subband LPF dan HPF. Ditunjukkan pada Gambar 2.10 dan dekomposisi *multiwavelet* sampai tingkat ketiga ditunjukkan pada Gambar 2.11[5]



Gambar 2.10 *First level of decomposition*
(a) dengan menggunakan skalar wavelet (b) dengan menggunakan mutiwavelet



Gambar 2.11 *Multiwavelet decomposition up to third level*

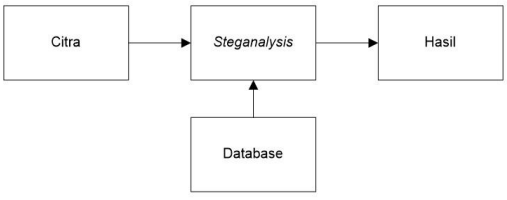
2.5 Metode K-NN

K-NN (*K-Nearest Neighbor*) merupakah salah satu metode klasifikasi pada citra yang berdasarkan ciri-ciri data pembelajaran (data latih) yang paling mendekati objek. Dimana ciri direpresentasikan dengan ukuruan jarak yang akan diolah dalam hitungan matematis. Dalam metode K-NN akan dihitung nilai jarak antara titik yang merepresentasikan data pengujian dangen semua titik yang merepresentasikan data latihnya. Untuk menghitung jarak antar tetangga digunakan beberapa cara, diantaranya: [6] Perhitungan jarak pada K-NN diantaranya: *City Block, Euclidean Distance, Cosine*, dan *Correlation.*

3. Pembahasan

3.1. Deskripsi Sistem

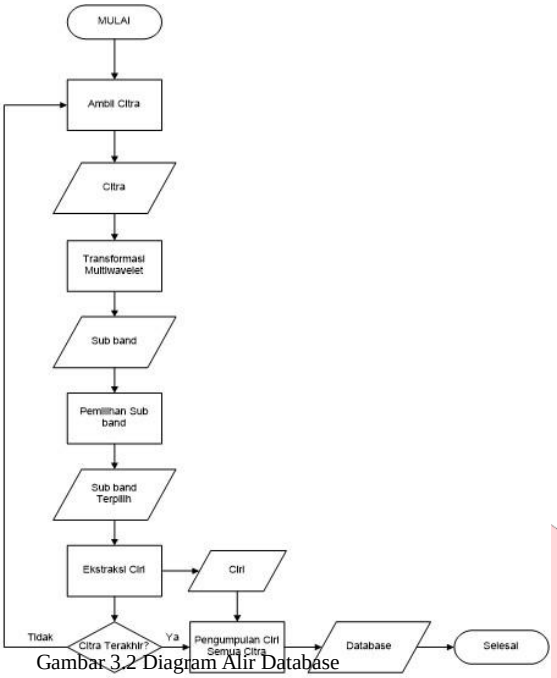
Deskripsi sistem dimulai dengan memilih citra yang akan dideteksi apakah ada pesan atau tidak. Sistem *steganalysis* yang dirancang akan mengolah citra tersebut dan memberikan hasil apakah citra tersebut termasuk kelas asli atau tersisipi. Sebuah citra diproses dalam *steganalysis* berdasarkan database dari K-NN yang akan menghasilkan analisis apakah suatu citra disisipi pesan rahasia atau tidak. Proses tersebut dipaparkan pada blok diagram dibawah ini.



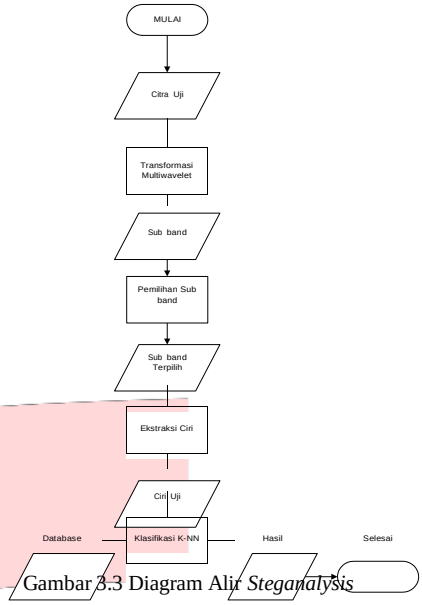
Gambar 3.1 Blok Diagram *steganalysis*

3.2. Perancangan Sistem

Sistem *steganalysis* yang dirancang terdiri dari dua bagian yaitu: proses pengambilan ciri acuan dan pengujian. Penjelasan proses pengambilan ciri acuan dipaparkan pada diagram alir berikut.



Gambar 3.2 Diagram Alir Database



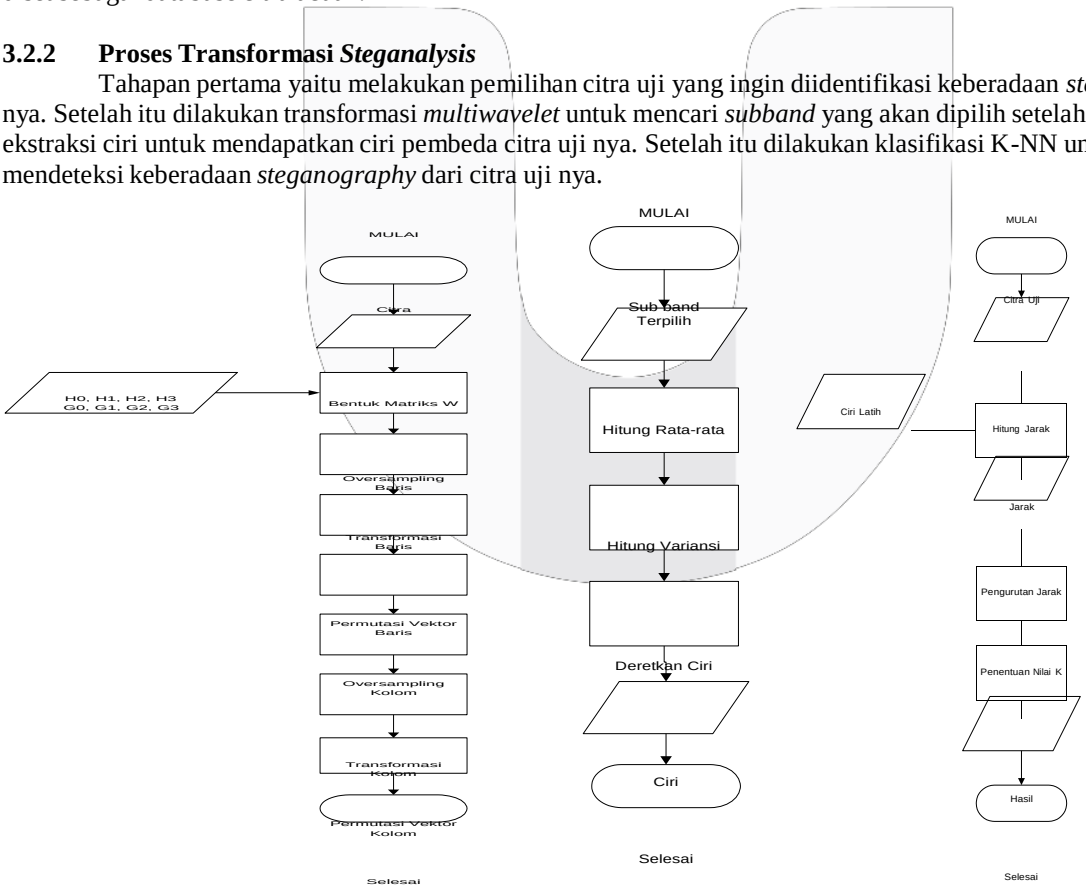
Gambar 3.3 Diagram Alir *Steganalysis*

3.2.1 Proses Transformasi Database

Tahapan pertama yaitu melakukan pemilihan citra setelah itu dilakukan transformasi *multiwavelet* untuk didapatkan nilai *subband* yang diinginkan setelah itu dilakukan pencarian ciri dari citra acuannya. Keluarannya akan diset sebagai database citra acuan.

3.2.2 Proses Transformasi *Steganalysis*

Tahapan pertama yaitu melakukan pemilihan citra uji yang ingin diidentifikasi keberadaan *steganography* nya. Setelah itu dilakukan transformasi *multiwavelet* untuk mencari *subband* yang akan dipilih setelah itu dilakukan ekstraksi ciri untuk mendapatkan ciri pembeda citra uji nya. Setelah itu dilakukan klasifikasi K-NN untuk mendeteksi keberadaan *steganography* dari citra uji nya.



Gambar 3.4 Diagram Alir *Multiwavelet* Gambar 3.5 Diagram Alir Ekstraksi Ciri Gambar 3.6 Diagram Alir K-NN

3.2.3 Proses Transformasi *Multiwavelet*

Tahapan pertama yaitu membentuk matriks W yang diinisialisasi dari koefisien H0, H1, H2, H3, G0, G1, G2, dan G3. Setelah itu dilakukan transformasi baris dengan melakukan *oversampling* baris. Selanjutnya dilakukan transformasi kolom dengan melakukan *oversampling* kolom.

3.2.4 Proses Transformasi Ekstraksi Ciri

Setelah dilakukan transformasi *multiwavelet* yang menghasilkan *subband* setelah itu dilakukan ekstraksi ciri. Ekstraksi ciri statistik yang dilakukan yaitu menghitung nilai rata-rata dan standar deviasi nya. Proses ekstraksi ciri dilakukan dengan mencuplik 3x3 blok citra untuk perhitungan ciri statistik nya. Setelah dilakukan perhitungan ciri selanjutnya ciri rata-rata dan ciri deviasi standar diurutkan.

3.2.5 Proses Transformasi K-NN

Pertama dilakukan pemilihan citra uji yang akan diidentifikasi keberadaan *steganography* nya. Setelah itu menentukan nilai K nya. Setelah itu dilakukan perhitungan jarak dan dilakukan pengurutan jarak. Setelah itu diambil nilai jarak terdekat sejumlah K nya. Pengklasifikasian berdasarkan kelas mayoritas dari jarak terdekatnya.

4. Implementasi dan Analisis

4.1 Lingkup Pengujian

Pengujian pada tugas akhir ini menggunakan kombinasi dari 10 buah citra utama seperti yang terdapat pada tabel 4.1.1 Selain itu, tiap – tiap citra akan dilakukan penyisipan pesan dengan kapasitas 1KB, 3 KB dan 5KB. Sehingga jumlah total citra pengujian 30 citra dengan pesan sisipan dan 10 citra tanpa ada sisipan.

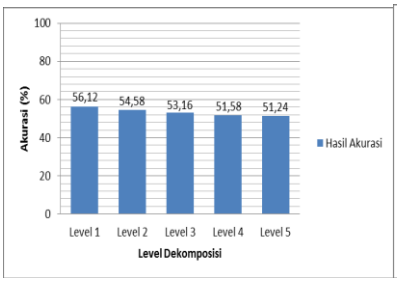
4.2 Skenario Pengujian Sistem

Skenario yang dilakukan untuk melakukan pengujian sistem *steganalysis* yang sudah dirancang

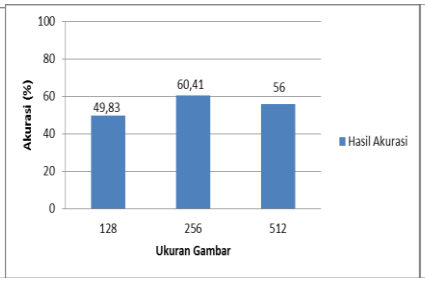
1. Ukuran Gambar
2. Level DMWT
3. Ukuran Pesan

4.3 Hasil Pengujian

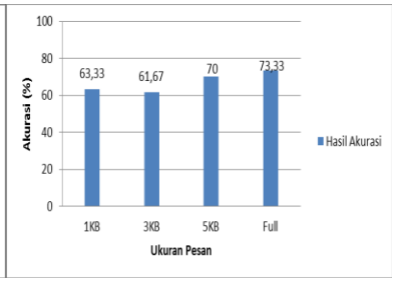
Berdasarkan skenario pengujian yang telah ditetapkan sebelumnya, maka dilakukan analisis sebagai berikut:



Gambar 4.1 Grafik Skenario Level DMWT



Gambar 4.2 Grafik Skenario Ukuran Gambar



Gambar 4.3 Grafik Skenario Ukuran Pesam

4.3.1 Analisis Pengaruh Banyak Level Dekomposisi DMWT Terhadap Akurasi

Akurasi terbaik didapatkan saat penggunaan level 1 DMWT yaitu sebesar 56,12%. Terjadi penurunan akurasi dari level 1 hingga ke level 5. Hal tersebut terjadi karena disaat nilai level semakin besar maka ukuran *subband* DMWT akan semakin kecil sehingga ciri yang didapatkan juga akan semakin sedikit. Dimana saat nilai ciri semakin sedikit didapat maka pembeda antara ciri asli dengan ciri stego juga sedikit. Maka sulit untuk dilakukan pendeteksian dari citra tersebut.

4.3.2 Analisis Pengaruh Ukuran Gambar Terhadap Akurasi

Akurasi terbaik pada penggunaan ukuran gambar 256 dengan nilai akurasi rata-rata 60,42%, ukuran gambar 512 menghasilkan akurasi sebesar 56%, dan akurasi terendah pada penggunaan ukuran gambar 128 sebesar 49,83%. Hal tersebut disebabkan karena pada saat penggunaan ukuran gambar 256 ciri yang didapat lebih baik dibanding pada ukuran gambar 512 dan 128.

4.3.3 Analisis Pengaruh Ukuran Pesan Terhadap Akurasi

Pada grafik Gambar 4.5 dijelaskan skenario pengujian ukuran pesan terhadap akurasi. Didapatkan akurasi pada penyisipan ukuran pesan 1KB yaitu sebesar 63,33%. Penyisipan ukuran pesan 5KB yaitu sebesar 70% dan penyisipan secara penuh yaitu sebesar 73,33%. Hal ini disebabkan karena semakin banyak ukuran pesan yang disisipi maka dibutuhkan lebih banyak bit untuk penyisipannya yang mengakibatkan semakin banyak pula perubahan pada citra yang disisipi. Maka semakin besar kemungkinan pendeteksian citra asli maupun citra stego.

5 Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil pengujian yang dilakukan pada tugas akhir ini, dapat disimpulkan sebagai berikut.

1. Sistem yang dibuat mampu mendeteksi keberadaan pesan rahasia yang disisipkan menggunakan aplikasi steganografi *Silent Eye* dan *QuickStego*
2. Ukuran citra uji mempengaruhi performansi sistem dengan rincian yaitu citra dengan ukuran 128 menghasilkan akurasi sebesar 49,83%, ukuran 256 menghasilkan akurasi 60,41%, dan untuk ukuran citra 512 sebesar 56%
3. Perbedaan jumlah level yang digunakan pada transformasi mempengaruhi akurasi pendeteksian dari sistem dengan rincian yaitu 56,12% pada level 1, 54,58% pada level 2, 53,16% pada level 3, 51,58% pada level 4, dan 51,24% pada level 5.
4. Pemilihan nilai K pada K-NN mempengaruhi akurasi performansi dimana saat penggunaan K=1 akurasi sebesar 83,75%, K=3 sebesar 82,5%, K=5 sebesar 83,73%, K=7 sebesar 86,25%, dan untuk K=9 sebesar 81,25%
5. Pemilihan jenis K-NN mempengaruhi transformasi dimana saat penggunaan jenis *euclidean* akurasi sebesar 78%, jenis *cosine* sebesar 74%, *cityblock* sebesar 86%, dan *correlation* sebesar 96%
6. Ukuran penyisipan pesan terhadap citra mempengaruhi performansi dimana disaat dilakukan penyisipan 1KB menghasilkan akurasi sebesar 63,33%, penyisipan ukuran pesan 3KB sebesar 61,66%, penyisipan ukuran pesan 5KB sebesar 70%, dan penyisipan pesan secara penuh sebesar 73,33%

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah

1. Citra yang digunakan bisa berupa citra 3 dimensi atau citra bergerak (video)
2. Menggunakan format citra yang lain seperti .jpg, .gif, atau .png.
3. Teknik *steganalysis* yang digunakan jangan hanya bersifat pasif, tapi harus bersifat aktif yang dapat memperkirakan jumlah pesan sisipan, letak pesan sisipan serta isi dari pesan yang disisipkan.

Daftar Pustaka

[1] RD. Kusumanto, Pambudi, Wahyu S., Tompunu, Alan N. 2012. *Aplikasi Sensor Vision untuk Deteksi MultiFace dan Menghitung Jumlah Orang*. Palembang : Jurusan Teknik Komputer Politeknik Negri Sriwijaya.

[2] Richer, Pierre. 2003. *Steganalysis*: *Detecting hiding information with computer forensic analysis.* United States : SANS Institue.

[3] Chen, Chen. 2005. *Study Of Steganalysis Method*. New Jersey : New Jersey Institute of Technology.

[4] Chhikara, Rita., Singh, Latika. 2013. *A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted*. India : ITM University.

[5] X. G. Xia, J. S. Geronimo, D. P. Hardin, dan B. W. Suter. 1999. *Design of Prefilters for Discrete Multiwavelet Transform.* United States : IEEETrans *Signal Processing.*

[6] Fadhillah, Nur Armanda, Novamizanti, Ledya., Ssi., MT., dan Atmaja, Ratri Dwi, ST., MT. 2015. *Analisis dan Implementasu Klasifikasi K-Nearest Neighbor (K-NN) pada Sistem Identifikasi Biometrik Telapak Kaki Manusia*. Bandung : Jurusan Teknik Telekomunikasi Universitas Telkom.