STEGANALISIS CITRA DIGITAL BERBASIS *DISCRETE COSINE TRANSFORM* DENGAN MENGGUNAKAN METODE *K-NEAREST NEIGHBOR*

Sheira Banu Nasution [1)], Bambang Hidayat [2)], I Nyoman Apraz Ramatryana [3)]

[1),2),3)] Teknik Telekomunikasi, Universitas Telkom
Jl. Telekomunikasi No.1 Bandung
Email : sheirabnst@students.telkomuniversity.ac.id

Abstrak. *Di era yang semakin maju, berbagai macam cara komunikasi dapat dilakukan, salah satunya dengan menyembunyikan pesan ke dalam suatu objek lain. Hal ini disebut dengan steganografi. Untuk mengontrol kemungkinan adanya dampak buruk dari steganografi, maka diperlukan adanya steganalisis. Objek dari Steganalisis adalah untuk mendeteksi pesan tersembunyi pada suatu cover citra, seperti citra dijital. Pada paper ini, kami menyajikan sebuah metode steganalisis yang dapat mendeteksi pesan tersembunyi pada citra dijital dengan menggunakan metode DCT (Discrete Cosine Transform) dan digunakan PCA (Principal component Analysis) untuk mereduksi citra dijital. K-Nearest Neighboor untuk klasifikasi. Hasil pengujian yang didapatkan adalah 64,5% untuk citra ukuran 128, 64% untuk citra ukuran 256, 58,5% untuk citra dijital ukuran 512. Untuk pengujian pengaruh layer terhadap performansi akurasi didapatkan hasil akurasi terbaik sebesar 66% untuk citra ukuran 256 pada layer merah, 64% untuk citra ukuran 256 pada layer hijau, dan 78% untuk citra ukuran 128 pada layer biru. Selain itu, untuk pengujian panjang pesan terhadap performansi akurasi didapatkan hasil akurasi terbaik sebesar 72,5% denagn penyisipan sebesar 1KB, 2KB, dan 3KB, serta sebesar 70% pada penyisipan secara keseluruhan.*

***Katakunci**: Steganalisis, DCT. K-Nearest Neighboor, PCA*

1. Pendahuluan

1.1 Latar Belakang

Pada zaman sekarang, teknologi berkembang dengan pesat, sehingga dapat mempermudah kita untuk melakukan komunikasi. Berbagai jenis cara untuk berkomunikasi dapat dilakukan, salah satunya dengan menyembunyikan pesan ke dalam suatu objek lain. Hal ini dapat disebut dengan steganografi. Steganografi merupakan ilmu untuk menyembunyikan pesan ke dalam suatu objek lain, sehingga keberadaan pesan tersebut tidak diketahui. Dengan cara seperti ini dapat memudahkan kita untuk saling bertukar pesan dengan konten, baik yang menguntungkan maupun yang merugikan. Penyalahgunaan steganografi sering terjadi belakangan ini, salah satunya digunakan untuk menyisipkan suatu pesan tertentu atas dasar kriminalitas. Maka dari itu, diperlukan adanya steganalisis untuk mengontrol akan adanya penyalahgunaan steganografi.

Sebuah permasalahan yang menarik adalah bagaimana cara mendeteksi keberadaan pesan rahasia dalam sebuah media penampung tanpa mengetahui bagaimana cara pesan tersebut disisipkan ke dalam media penampung. Oleh karena itu, dalam penelitian ini disimulasikan sebuah skema *blind steganalysis* pada citra digital dengan menggunakan DCT *(Discrete Cosine Transform)* sebagai metode identifikasi ekstraksi ciri dan menggunakan metode K-NN (*K-Nearest Neighbor*) sebagai klasifikasi untuk membedakan citra stego dan citra non-stego yang kemudian dilakukan perhitungan nilai akurasi dari setiap pengujian yang digunakan. Setelah itu dibuat persentase hasil dari perhitungan terhadap akurasinya sehingga dapat dilihat performansi dari sistem yang telah dibuat pada penelitian ini.

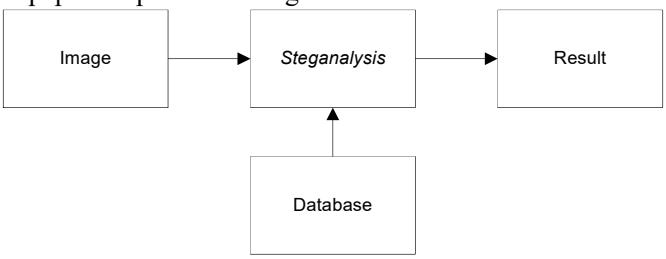
Steganalisis didefinisikan sebagai teknik dan seni mendeteksi keberadaan pesan rahasia dalam sebuah media penampung. Keberadaan pesan rahasia dideteksi berdasarkan analisis terhadap media penampung secara visual, spasial, statistic dan lain-lain[4]. Tujuan dari steganalisis ini adalah untuk mengidentifikasi adanya keberadaan pesan tersembunyi dalam suatu media digital, dan jika memungkikan adanya keberadaan pesan rahasia tersebut, maka akan diekstraksi data tersembunyi tersebut.

Ada banyak teknik steganalisis. Masing -masing teknik memiliki karakteristik yang unik dan menerapkan algoritma yang berbeda-beda. Walaupun demikian, secara garis besar teknik-teknik

steganalisis dapat dikategorikan menjadi dua macam[4], yaitu *specific steganalysis* dan *blind steganalysis*.
Sejauh ini beberapa penelitian menunjukkan bahwa *specific steganalysis* memiliki tingkat akurasi yang lebih baik dibanding *blind steganalysis*. Fenomena ini memang wajar, sebab dengan mengetahui bagaimana sebuah pesan rahasia disisipkan maka relatif lebih mudah untuk mendeteksi keberadaan dan bahkan mengekstrak isi pesan rahasia tersebut.
Namun pada kenyataannya, warden cenderung tidak mengetahui algoritma steganografi yang digunakan. Di sisi lain, tanpa berbekal informasi tentang teknik steganografi yang digunakan, *blind steganaysis* dapat mendeteksi keberadaan pesan rahasia. Jika keberadaan pesan rahasia telah terdeteksi, maka mengetahui isi pesan tersebut tidak menjadi suatu keharusan. Dengan mendeteksi keberadaan dan melumpuhkan transmisi pesan rahasia saja sudah dianggap menggagalkan steganografi[5]. Oleh karena itu maka *blind steganalysis* dianggap lebih dapat diaplikasikan secara luas untuk kasus-kasus real world[6].
DCT merupakan salah satu metode ekstraksi ciri yang sering digunakan pada *blind steganalysis.* Beberapa teknik steganalisis dengan menggunakan DCT menunjukkan tingkat akurasi yang tinggi, diantaranya adalah [7] and [8] yang mencapai tingkat akurasi masing-masing 93.75& dan 88.97%.

2. Pembahasan

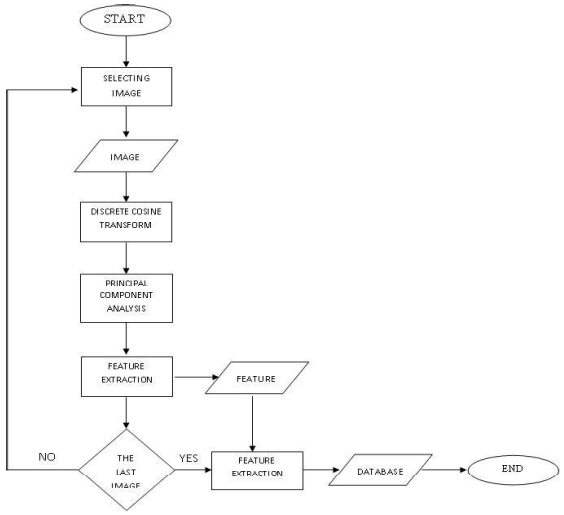
Sistem steganalisis yang dirancang menggunakan metode *Discrete Cosine Transform* (DCT) bertujuan untuk mentransformasikan sinyal tersebut dari domain waktu ke domain frekuensi. Karena proses ekstraksi akan lebih mudah jika dilakukan dalam domain frekuensi. Proses ini hanya dapat mengubah satu layer citra.
Deskripsi sistem dimulai dengan memilih citra yang akan dideteksi apakah ada pesan atau tidak. Sistem steganalisis yang dirancang akan mengolah citra tersebut dan memberikan hasil apakah citra tersebut termasuk kelas asli atau tersisipi. Sebuah citra diproses dalam steganalisis 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 1. Blok Diagram Steganalisis

2.1 Perancangan Sistem

Pada sistem ini, teknik steganografi yang digunakan adalah *Discrete Wavelet Transform* (DWT). Sistem steganalisis yang dirancang terdiri dari dua bagian yaitu: proses pengambilan ciri acuan dan pengujian. Proses pengambilan ciri acuan adalah proses untuk mengambil ciri yang menjadi acuan dari K-NN untuk menentukan kelas pada proses pengujian. Ciri acuan didapat dari dua kelompok kelas citra yaitu kelas asli dan kelas tersisipi dari citra acuan. Dimana citra acuan tersebut akan diproses dengan transformasi DCT mentransformasikan sinyal tersebut dari domain waktu ke domain frekuensi. Karena proses ekstraksi akan lebih mudah jika dilakukan dalam domain frekuensi. Setelah itu, dilakukan ekstraksi ciri dan diakhir dikumpulkan semua ciri dari masing-masing citra untuk menjadi data ciri acuan atau data latih dan target acuan (*group*).
Penjelasan proses pengambilan ciri acuan dipaparkan pada diagram alir berikut.



Gambar 2. Diagram Alir *Database*

Proses pada Gambar 2. adalah:

a. Tahapan pertama yaitu pemilihan citra yang akan diproses untuk didapatkan cirinya dimana citra dibagi menjadi dua kelas yaitu citra asli dan citra yang mengandung pesan rahasia

b. Setelah dilakukan pemilihan citra, tahapan selanjutnya yaitu melakukan proses transformasi ke domain frekuensi dengan menggunakan DCT. Berikut persamaannya [1]:

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{m\,n} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (1)$$

Dengan $0 \le p \le M-1$; $0 \le q \le N-1$

Dimana $a_{p=}$ $\begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}$ (2)

$a_{q=}$ $\begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}$ (3)

Proses ini hanya dapat mengubah satu layer citra.

a. Lalu, dilakukan reduksi terhadap matriks citra dengan ,menggunakan PCA.

b. Hasil transformasi *cosine* diskrit direduksi dengan menggunakan *Principal Component Analysis* (PCA). Hasil tersebut dikumpulkan dan kemudian akan diurutkan berdasarkan perhitungan *mean* dan deviasi standar nya dengan menggunakan rumus berikut [2] : (4)

Mean: $E(x) = \frac{1}{n}\sum_{k=1}^{n} x_k$

Deviasi Standar: $Var(x) = \frac{1}{n}\sum_{i=1}^{n}(x_k - E(x))^2$ (5)

dimana: *n* = banyak nya data

c. Selanjutnya dilakukan perhitungan jarak antara data latih dengan data uji menggunakan perhitungan jarak *Euclidian Distance* dengan rumus berikut [3] :

$$L_2(X,Y) = \sqrt{\sum_{i=1}^{d}(X_i - Y_i)^2} \quad (6)$$

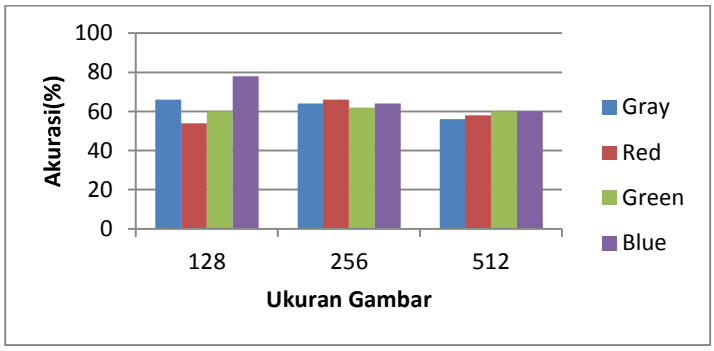
3. Analisis dan Hasil Simulasi

Pengujian pada penelitian ini menggunakan kombinasi dari 10 buah citra utama berformat .jpg. Selain itu, tiap – tiap citra akan dilakukan penyisipan pesan dengan kapasitas 1 KB, 2 KB, 3KB dan full. Sehingga jumlah total citra pengujian 50 citra dengan pesan sisipan dan 10 citra tanpa ada sisipan.

Skenario pengujian yang diterapkan pada sistem steganalisis berdasarkan ukuran pesan, ukuran gambar, dan layer gambar.
Berdasarkan skenario pengujian yang telah ditetapkan sebelumnya, maka dilakukan analisis sebagai berikut:

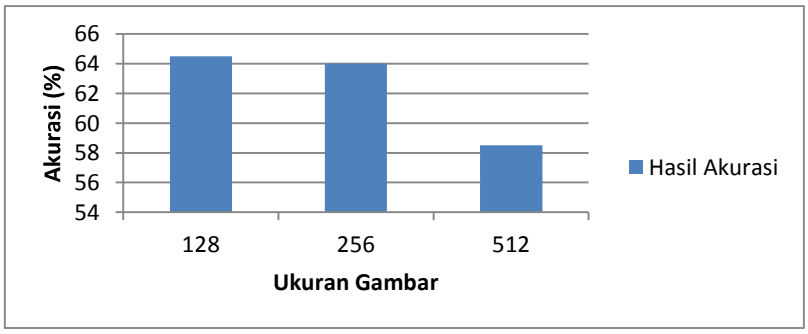
2.1 Analisis Pengaruh Ukuran Gambar Terhadap Akurasi

Pada proses pendeteksian ini, ukuran citra yang digunakan ada 3 yaitu 128 x 128, 256 x 256, dan 512 x 512. Tiap – tiap citra dengan ukuran tersebut akan dilihat presentasi akurasi yang diperoleh dari masing-masing ukuran citra tersebut.



Gambar 3. Grafik Skenario Ukuran Gambar

Berdasarkan gambar pengujian diatas didapatkan nilai akurasi berbeda-beda pada penggunaan ukuran gambar setiap *layer* nya. Pada penggunaan ukuran gambar, pada *layer red* menghasilkan akurasi 54% pada ukuran 128, 66% pada ukuran 256, dan pada ukuran gambar 512 sebesar 58%. Pada *layer green* 60% pada ukuran 128, 64% pada ukuran 256, dan pada ukuran 512 sebesar 60%. Pada *layer blue* 78% pada ukuran 128, 62% pada ukuran 256, dan 60% pada ukuran 512. Pada *layer gray* 66% pada ukuran 128, 64% pada ukuran 256, dan 56% pada ukuran 512. Selanjutnya pada Gambar 4., dijelaskan perhitungan rata-rata nilai akurasi.

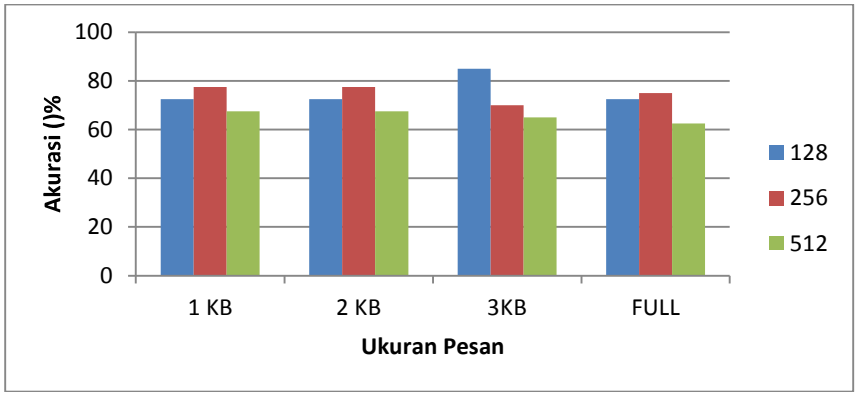


Gambar 4. Grafik Akurasi Ukuran Gambar

Pada grafik Gambar 3. ditunjukkan skenario ukuran gambar. Dimana akurasi terbaik pada penggunaan ukuran gambar 128 dengan nilai akurasi rata-rata 64,5%, ukuran gambar 256 menghasilkan akurasi sebesar 64%, dan akurasi terendah pada penggunaan ukuran gambar 512 sebesar 58,5%. Pada pengujian ukuran gambar terhadap akurasi terjadinya penurunan nilai dari ukuran gambar 128 ke ukuran gambar 256 yaitu sebesar 0.5% tetapi terdapat penurunan dari ukuran gambar 256 ke 512 yaitu sebesar 5,5%. Hal tersebut disebabkan karena pada saat penggunaan ukuran gambar 128 ciri yang didapat lebih baik dibanding pada ukuran gambar 256 dan 512.

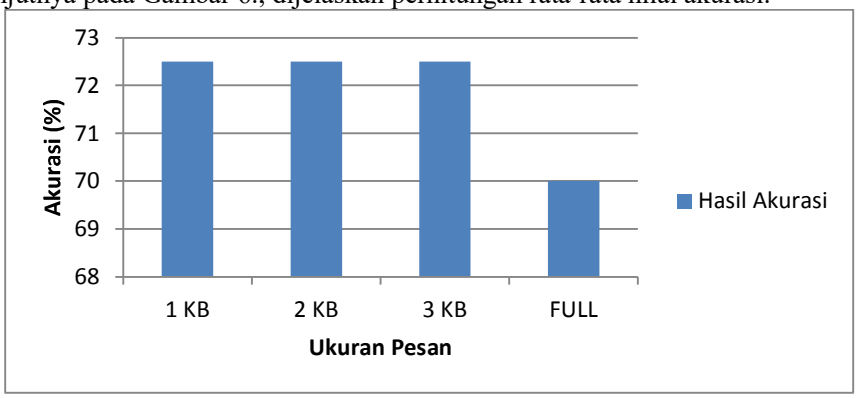
2.2 Analisis Pengaruh Ukuran Pesan Terhadap Akurasi

Pada pengujian kali ini yang akan diujikan adalah pengaruh ukuran pesan pada citra *grayscale* dan citra RGB.Ukuran pesan yang disisipi yaitu 1KB, 3KB, 5KB, dan dengan kapasitas penuh.



Gambar 5. Grafik Skenario Ukuran Pesan

Berdasarkan gambar pengujian diatas didapatkan akurasi dari pengujian ukuran gambar terhadap ukuran pesan yang disisipi nya. Dimana nilai akurasi terbaik pada ukuran gambar 128 dengan menggunakan ukuran penyisipan 3 KB sebesar 85% dan akurasi terendah pada penyisipan 1 KB, 2 KB, dan secara menyeluruh sebesar 72,5 %. Pada ukuran gambar 256 didapatkan akurasi terbaik pada ukuran penyisipan 1 KB dan 2 KB sebesar 77.5% dan akurasi terendah pada penyisipan ukuran pesan 3KB sebesar 70%. Pada ukuran gambar 512 didapatkan akurasi terbaik pada ukuran penyisipan 1 KB dan 2 KB sebesar 67,5% dan akurasi terendah pada penyisipan secara keseluruhan yaitu sebesar 62,5%. Selanjutnya pada Gambar 6., dijelaskan perhitungan rata-rata nilai akurasi.



Gambar 6. Grafik Akurasi Skenario Ukuran Pesan

Pada grafik Gambar 6. dijelaskan skenario pengujian ukuran pesan terhadap akurasi. Didapatkan akurasi pada penyisipan ukuran pesan 1KB, 2 KB dan 3 KB yaitu sebesar 72,5%. Terjadi penurunan nilai akurasi untuk penyisipan pesan secara keseluruhan yaitu sebesar 2,5%.

3. Simpulan

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 program steganografi dalam domain *Discrete Wavelet Transform* (DWT)
2. Ukuran citra uji mempengaruhi performansi sistem dengan rincian yaitu citra dengan ukuran 128 menghasilkan akurasi sebesar 64,5 %, ukuran 256 menghasilkan akurasi 64%, dan untuk ukuran citra 512 sebesar 58,5%
3. Ukuran penyisipan pesan terhadap citra mempengaruhi performansi dimana disaat dilakukan penyisipan 1KB, 2KB, 3 KB sebesar 72,5%, dan penyisipan pesan secara penuh sebesar 70%.

DaftarPustaka

[1]. Khayam, S.A. 2003. *The Discrete Cosine Transform (DCT): Theory and Application*.

[2]. Handoko, Ronny. 2014. *Steganalisis Citra Digital Menggunakan Metode Discrete Wavelet Transform dan K-Nearest Neighbor.* Bandung : Jurusan Teknik Telekomunikasi Universitas Telkom.
[3]. Fadhillah, Armanda, Nur., Novamizanti, Ledya. Ssi., MT., dan Atmaja, Ratri Dwi, ST., MT. 2015. *Analisis dan Implementasi Klasifikasi K-Nearest Neighbor (K-NN) pada Sistem Identifikasi Biomterik Telapak Kaki Manusia*. Bandung : Jurusan Teknik Telekomunikasi Universitas Telkom.
[4]. YunQShi."DigitalImageBlindSteganalysis"Internet:www.cs.surrey.ac.uk/FMS/wmms/downloads/YunShi2007-08-08.pdf, Aug.8,2007 [May. 25, 2009].
[5]. I. Avcibas, N. Memon and B. Sankur. "Steganalysis Using Image Quality Metrics." IEEE Transactions on Image Processing, vol. 12, pp. 221-229, Feb. 2003.
[6]. Xiangyang Luo, D. Wang, Wei Hu and F. Liu. "Blind Detection For Image Steganography: A System Framework and Implementation." The International Journal of Innovative Computing, Information and Control, vol. 5, pp. 443-442, Feb. 2009.
[7]. Xiang Li and Jianhua Li. "A New Blind Steganalysis Method for JPEG Images" in Proc. International Conference on Computer Science and Software Engineering, 2008, pp. 939-942.
[8]. J. Ba rbier, E. Filiol and K. Mayoura. "Universal Detection of JPEG Ste ganography." Journal of Multimedia, vol. 2, pp. 1-9, Apr. 2007.