

DETEKSI POSISI PENYISIPAN DENGAN METODE DISCRETE WAVELET PACKET TRANSFORM PADA FILE VIDEO YANG AUDIONYA TERSISIPI PESAN SECARA PSYCHOACOUSTIC

DETECTION OF INSERTION POSITION WITH DISCRETE WAVELET PACKET TRANSFORM METHOD ON A VIDEO FILES WHICH IS THE AUDIO INSERTED MESSAGES BASED ON PSYCHOACOUSTIC

Muhammad Rizqi Rahmawan¹, Iwan Iwut Tritoasmoro², Nur Ibrahim³,

^{1,2,3}Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom, Bandung

¹rizqirahmawan11@gmail.com, ²iwaniwuttritoasmoro@telkomuniversity.ac.id

³nuribrahim@telkomuniversity.ac.id

Abstrak

Pada era globalisasi ini pertukaran informasi di dunia telekomunikasi bukanlah hal jarang ditemukan. Steganografi adalah seni dan ilmu menulis pesan tersembunyi sehingga hanya pengirim dan penerima saja yang mengetahui ada atau tidaknya pesan tersembunyi tersebut. Dengan semakin berkembangnya teknik steganografi, penyalahgunaan pada ilmu ini pun semakin berkembang. Untuk itu, diperlukannya ilmu yang dapat mendeteksi steganografi, yaitu steganalisis. Steganalisis merupakan ilmu yang mampu mendeteksi informasi tersembunyi. Steganalisis pun telah banyak diterima oleh banyak pihak karena manfaatnya untuk mencegah penyalahgunaan pesan tersembunyi. Judul dari tugas akhir ini adalah Deteksi Posisi Penyisipan Dengan Metode Discrete Wavelet Packet Transform Pada File Video Yang Audionya Tersisipi Pesan Secara Psychoacoustic. Video yang audionya telah tersisipi pesan secara psychoacoustic diuraikan dengan Discrete Wavelet Packet Transform (DWPT) ditinjau dari setiap frame yang terdapat pada file video tersebut. Dalam penelitian ini dibuat suatu perangkat lunak yang mampu mendeteksi keberadaan pesan tersembunyi berupa file video yang audionya tersisipi pesan secara psychoacoustic. Hasil dari steganalisis ini mampu mendeteksi keberadaan dan posisi pesan tersembunyi pada file video yang audionya tersisipi pesan secara psychoacoustic dengan tingkat akurasi sistem sebesar 93% untuk deteksi keberadaan pesan dan 71% untuk deteksi posisi pesan tersembunyi. Penelitian ini dapat dimanfaatkan oleh pihak berkepentingan seperti polisi untuk mendeteksi pesan tersembunyi agar tidak terjadi penyalahgunaan pertukaran informasi..

Kata Kunci : Steganalisis, Discrete Wavelet Packet Transform (DWPT), Psychoacoustic, Video

Abstract

In this era of globalization the exchange of information in the telecommunication world is not rarely found. Steganography is the art and science of writing a hidden message so that only the sender and the recipient alone know the presence or absence of such hidden messages. With the development of steganography techniques, the abuse of this science is growing. For that, need of science that can detect steganography, namely steganalisis. Steganalisis is a science capable of detecting hidden information. Steganalisis has been widely accepted by many parties because of benefits to prevent misuse of hidden messages. The title of this final project is the Detection of Insertion Position With Discrete Wavelet Packet Transform Method On Video Files Which Audion Messages Insert Psychoacoustic. Video inserted audio psychoacoustic described with Discrete Wavelet Packet Transform (DWPT) in terms of each frame contained in the video file. In this study made a software that is able to detect the existence of hidden messages in the form of video files that audio insert psychoacoustic message. The results of this steganalisis are able to detect the presence and position of hidden messages in the audio video file inserted by the message psychoacoustic with a system accuracy of 93 % for detection of the presence of messages and 71 % for the detection of position of hidden messages. This research can be used by interested parties such as the police to detect hidden messages so there is no misuse of information exchange..

Keywords: Steganalisis, Discrete Wavelet Packet Transform (DWPT), Psychoacoustic, Video.

1. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat saat ini membuat komunikasi menjadi semakin luas dan mudah. Untuk itu diperlukannya metode yang menjamin keamanan saat pertukaran informasi, salah satu metode yang populer untuk menjamin kerahasiaan data adalah steganografi. Steganografi berasal dari bahasa Yunani, Steganos artinya tersembunyi dan grapho artinya menulis sehingga steganografi adalah suatu seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan ke dalam suatu *carrier* [1]. Namun, hal ini

memungkinkan terjadinya pertukaran informasi yang ilegal, seperti kegiatan pertukaran informasi tentang peredaran narkoba yang mana banyak sekali menggunakan steganografi dalam hal pengiriman pesan tersembunyi ke pihak tertentu, sehingga dikembangkan suatu ilmu yang dapat mengungkap pesan rahasia tersebut yaitu steganalisis. Steganalisis adalah suatu seni dan ilmu untuk mendeteksi suatu pesan tersembunyi [2]. Teknik ini diharapkan dapat membantu pihak kepolisian dan badan intellegensi untuk mengungkap kejahatan tersebut. Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi [2]. Kebalikan dari steganografi, tujuan steganalisis adalah mendeteksi sebuah berkas yang diyakini berisikan data terselubung. Steganalisis merupakan salah satu solusi yang dapat digunakan untuk dapat mengawasi pendistribusian informasi yang dilakukan secara tersembunyi. Tugas akhir ini berjudul “Deteksi Posisi Penyisipan Dengan Metode Discrete Wavelet Packet Transform Pada File Video yang Audionya Tersisipi Pesan Secara Psychoacoustic”, Pada penelitian ini file yang dianalisa adalah video yang telah tersisipi pesan secara psychoacoustic yang pada dasarnya pesan tersebut sulit dideteksi oleh indra manusia. Dengan menggunakan metode Discrete Wavelet Packet Transform pesan yang tersisipi tersebut dapat terenkripsi dengan baik karena dalam pengimplementasiannya relatif mudah dan sederhana sehingga efisien dalam penggunaannya.

2. Tinjauan Pustaka

A. Steganografi

Steganografi adalah cara dan teknik dalam menyembunyikan pesan. Suatu sistem steganografi mampu menyembunyikan pesan ke dalam suatu *cover* media sehingga tidak akan menimbulkan suatu kecurigaan jika terdapat pesan rahasia di dalamnya. Steganografi yang merupakan teknik untuk menyembunyikan pesan mempunyai beberapa perbedaan jika dibandingkan dengan kriptografi, perbedaannya dapat dilihat dari hasil keluarannya. Pada kriptografi biasanya data keluaran yang dihasilkan biasanya tampak seolah-olah berantakan, tetapi itu bisa dikembalikan seperti pesan semula, sedangkan pada steganografi keluaran yang dihasilkan akan berbeda, yaitu akan sama dengan bentuk asli media atau *cover*. Sehingga dengan menggunakan steganografi ini tidak mudah diketahui jika terdapat pesan di dalamnya.

B. Steganalisis

Steganalisis mengacu pada suatu ilmu dan seni yang digunakan untuk membedakan antara *stego object* dan *cover object* sehingga teknik ini dimanfaatkan dalam mengungkap keberadaan pesan tersembunyi dalam suatu media. Tujuan dari steganalisis untuk mengetahui ada atau tidaknya pesan rahasia dalam suatu media dengan melihat perubahan yang terjadi pada media tersebut (jika ada media asli, dilakukan dengan melihat perubahan):

C. Discrete Wavelet Packet Transform (DWPT)

Prinsip dasar dari Discrete Wavelet Packet Transform (DWPT) yaitu menentukan bagaimana cara mendapatkan representasi waktu dan skala dari sebuah sinyal dengan teknik pemfilteran digital dan operasi sub-sampling [2]. Sinyal informasi dilewatkan pada *high-pass filter* dan *low-pass filter*, kemudian dilakukan proses dekomposisi satu tingkat yaitu dengan mengambil setengah dari masing-masing keluaran perpaket yang nantinya dianggap sebagai *sample* melalui operasi *sub-sampling*. Proses dekomposisi dapat dilihat pada gambar 2.3 Dekomposisi satu tingkat ditulis melalui persamaan berikut [1]:

$$Y_{high}[k] = \sum_{in} x[n]h[2k - n] \quad (2.1)$$

$$Y_{low}[k] = \sum_{in} x[n]g[2k - n] \quad (2.2)$$

D. Psychoacoustic

Psychoacoustic adalah studi ilmiah persepsi suara. Lebih khusus lagi adalah cabang ilmu pengetahuan yang mempelajari tentang respon psikologis dan fisiologis yang berhubungan dengan suara (*speech* dan musik) [4]. Atau bisa diartikan sebagai ilmu yang mempelajari cara otak menerjemahkan suara.

E. K-Nearest Neighbor

KNN merupakan salah satu algoritma pengklasifikasian yang cukup mudah dipahami, karena KNN mencari jumlah kesamaan terbanyak antara data yang diuji dengan data latih (data yang ada pada database). Data uji tersebut akan masuk ke dalam kelas dengan jumlah kesamaan terbanyak. Konsep dasar dari *K-Nearest Neighbor* (KNN) adalah seperti pada algoritma *Nearest Neighbor*, yaitu mencari jarak terdekat dari nilai yang akan dievaluasi (titik query) dengan tetangga terdekatnya dalam suatu data.

Berikut ini adalah langkah-langkah untuk mengklasifikasikan data dengan metode *K-Nearest Neighbor* : [5]

1. Tentukan parameter K = jumlah tetangga terdekat.

2. Hitung jarak antara data yang akan dievaluasi dengan semua data pelatihan. Perhitungan dapat dilakukan dengan beberapa pendekatan. Pendekatan yang digunakan antara lain:

a. Fungsi jarak *Euclidean*, yaitu :

$$d(q, p) = \sqrt{\sum_{i=1}^n (q_i - p_i)^2} \quad (2.4)$$

b. Fungsi jarak *Cosine*, yaitu dari sudut antar titik (diperlakukan sebagai *vector*).

$$\cos(di, dj) = \frac{\sum_{k=1}^n a_{ik}a_{jk}}{\sqrt{\sum_{k=1}^n a_{ik}^2} \sqrt{\sum_{k=1}^n a_{jk}^2}} \quad (2.5)$$

c. Fungsi jarak *Correlation*, yaitu 1-b, dimana b adalah korelasi antara titik-titik sampel (diperlakukan sebagai urutan nilai). Secara umum rumus korelasi yaitu:

$$S_{ij} = \frac{\sum_{k=1}^n (x_{ik} - x_t)(x_{jk} - x_j)}{[\sum_{k=1}^n (x_{ik} - x_t)^2 \sum_{k=1}^n (x_{jk} - x_j)^2]^{1/2}} \quad (2.6)$$

Dimana x_t dan x_j adalah nilai rata-ratanya.

d. Fungsi jarak *Cityblock*, yaitu penjumlahan dari nilai diferensial *absolut*

$$D(x, y) = \sum_{i=1}^n |X_i - Y_i| \quad (2.7)$$

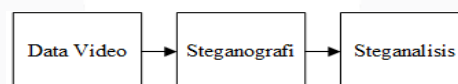
3. Urutkan jarak yang terbentuk (dari yang terdekat sampai yang terjauh) pada masing-masing titik sejumlah K dan tentukan jarak terdekat pada tiap titik-titik tersebut sampai urutan ke-K.

4. Pasangkan kelas yang bersesuaian (jarak paling dekat antara setiap titik dengan sebuah kelas (data latih) adalah kelas yang bersangkutan).

Cari jumlah kelas terbanyak dari tetangga terdekat tersebut, dan tetapkan kelas tersebut sebagai kelas data yang dievaluasi (data uji).

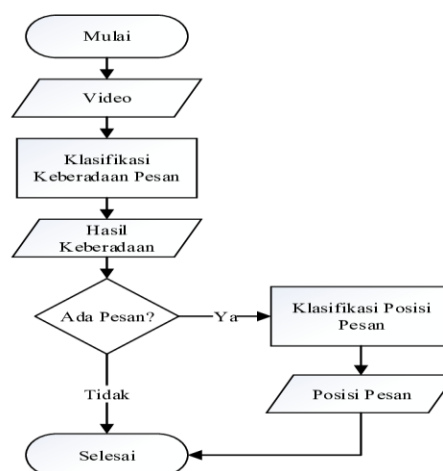
3. Perancangan Sistem

Sistem pada tugas akhir ini dibagi menjadi 3 tahap utama, yaitu data video, steganografi, dan steganalisis. Ketiga tahap tersebut ditunjukkan dalam bentuk diagram blok pada Gambar 3.1. Tahap awal sistem adalah pengumpulan data video .mp4. Data video sebanyak 40 data video asli yang dipisah menjadi 20 data latih dan 20 data uji. Data video terdiri dari data frame dan data video. Data Latih dan data uji selanjutnya disisipi pesan pada proses steganografi menggunakan metode DWPT pada data video dari tiap data video tersebut. Hasil dari proses steganografi adalah video stego yang disisipkan pesan rahasia dengan jumlah karakter yang berbeda, posisi yang berbeda, dan ukuran *frame* yang berbeda. Proses steganalisis menggunakan klasifikasi K-NN dengan ciri statistik dari hasil transformasi DWPT. Klasifikasi melalui dua tahap, yaitu tahap latih dan tahap uji. Tahap latih sebagai pencarian nilai parameter terbaik yang akan menjadi acuan sebagai database program untuk klasifikasi K-NN dan tahap uji sebagai proses yang digunakan dalam tahap pengujian data.



Gambar 1 Diagram Blok Perancangan Sistem

A. Perancangan Sistem Utama

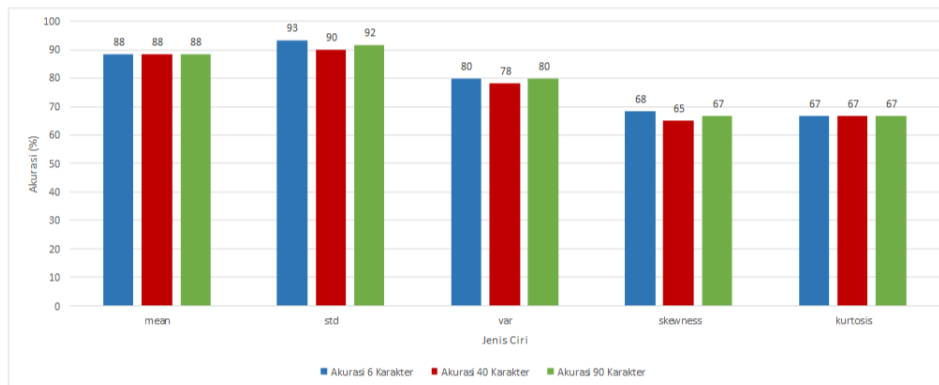


Gambar 2 Diagram Alir Steganalisis

Proses model steganalisis merupakan suatu tahapan analisis ada atau tidaknya pesan suatu data stego pada file host video. Pada gambar diatas menunjukkan proses penyisipan dari perancangan sistem. Model steganalisis yang dirancang terdiri dari dua model klasifikasi. Klasifikasi pertama adalah untuk klasifikasi keberadaan pesan pada video *input*. Klasifikasi kedua adalah klasifikasi posisi pesan apabila video *input* terklasifikasi sebagai video *stego* pada hasil klasifikasi pertama. Model klasifikasi pertama dan kedua secara garis besar sama, hanya berbeda dari segi data latih yang digunakan untuk membangun model klasifikasi tersebut. Model klasifikasi yang digunakan adalah K-NN dengan ekstraksi ciri DWPT.

4. Hasil Analisis

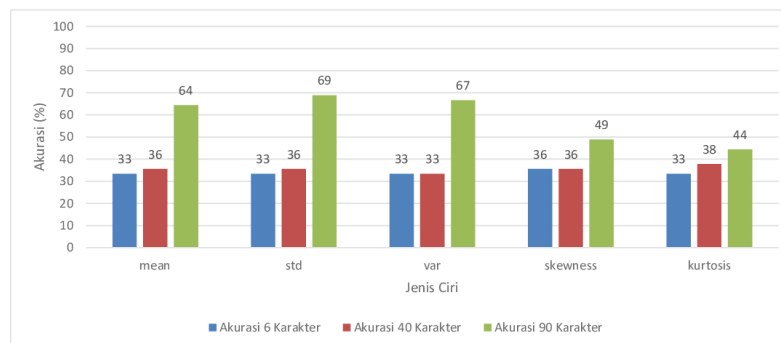
A. Pengujian Pengaruh Jenis Ciri Terhadap Akurasi Keberadaan Pesan



Gambar 3 Akurasi Keberadaan Pesan Pengujian Jenis Ciri

Pada gambar 3 menunjukkan pada ciri *std* menghasilkan akurasi terbesar untuk ketiga kondisi teks. Ciri *std* merupakan ciri yang memberikan informasi perbedaan nilai pada hasil transformasi DWPT dibandingkan ciri *mean* yang merupakan rata-rata nilai ciri hasil transformasi DWPT. Ciri *var* yang merupakan nilai kuadrat dari ciri *std* menghasilkan akurasi yang lebih rendah dibandingkan ciri *std*.

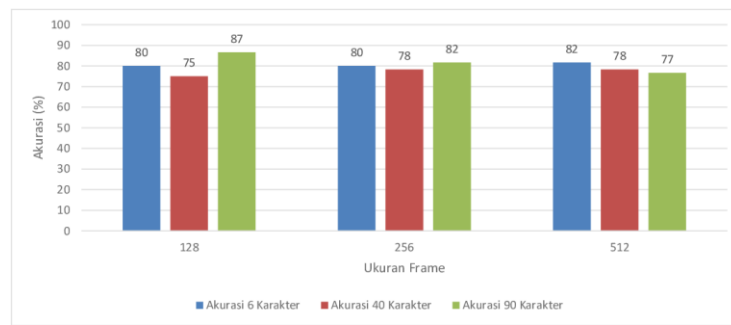
B. Pengujian Pengaruh Jenis Ciri Terhadap Akurasi Posisi Pesan



Gambar 4 Akurasi Posisi Pesan Pengujian Jenis Ciri

Pada gambar 4 menunjukkan hasil bahwa semakin banyak jumlah teks pesan rahasia, menghasilkan akurasi deteksi posisi yang lebih besar.

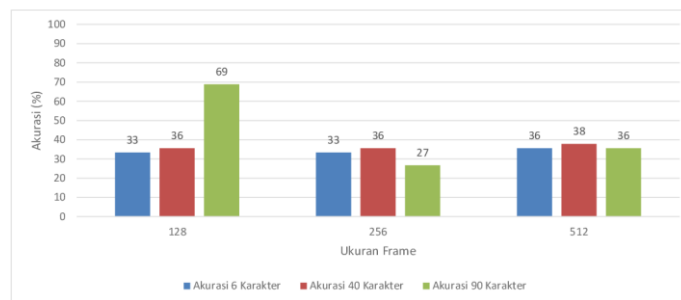
C. Pengujian Pengaruh Ukuran *Frame* Terhadap Akurasi Keberadaan Pesan



Gambar 5 Akurasi Keberadaan Pesan Pengujian Ukuran *Frame*

Pada pengujian diatas didapatkan akurasi terbaik adalah sebesar 87% dengan ukuran *frame* sebesar 128 dan jumlah karakter 90. Hal ini berarti dengan ukuran *frame* yang lebih kecil dan jumlah karakter yang banyak menyebabkan jumlah data semakin sedikit menghasilkan ciri yang lebih baik untuk dilakukan klasifikasi menggunakan K-NN. Ciri hasil DWPT juga lebih detail saat ukuran *frame* lebih kecil.

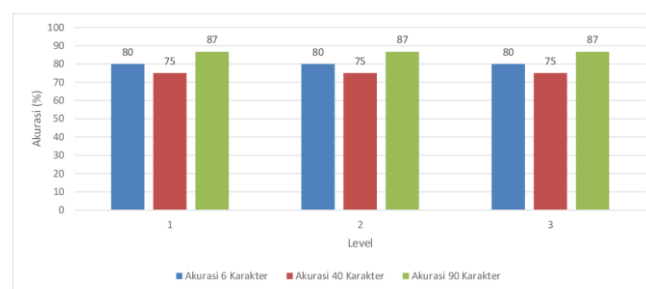
D. Pengujian Pengaruh Ukuran *Frame* Terhadap Akurasi Posisi Pesan



Gambar 6 Akurasi Posisi Pesan Pengujian Ukuran *Frame*

Dari hasil gambar diatas didapatkan nilai akurasi terbaik saat menggunakan ukuran *frame* sebesar 128 pada jumlah teks 90 karakter dengan akurasi 69%. Hal ini berbanding lurus dengan hasil terbaik dari hasil pengujian ukuran pesan terhadap akurasi keberadaan pesan.

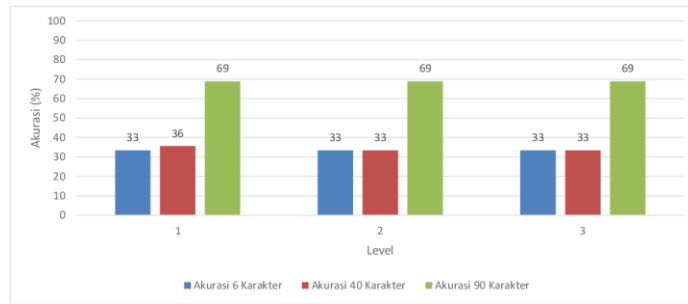
E. Pengujian Pengaruh *Level* DWPT Terhadap Akurasi Keberadaan Pesan



Gambar 7 Akurasi Keberadaan Pesan Pengujian Nilai *Level* DWPT

Hasil akurasi untuk pengujian *level* 1, 2, dan 3 ini menghasilkan akurasi yang sama yaitu 80% pada akurasi 6 karakter, 75% pada akurasi 40 karakter, dan 87% pada akurasi 90 karakter, sehingga nilai *level* DWPT tidak mempengaruhi akurasi deteksi keberadaan pesan.

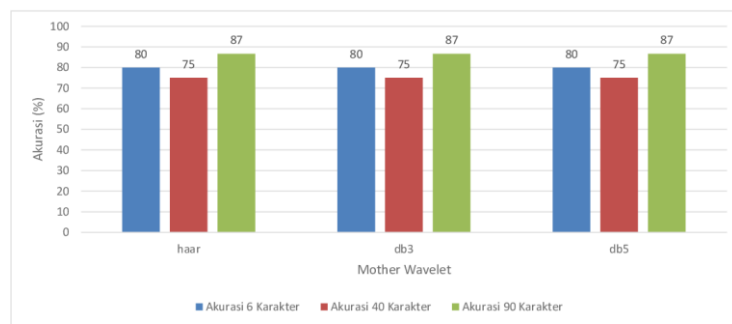
F. Pengujian Pengaruh *Level* DWPT Terhadap Akurasi Posisi Pesan



Gambar 8 Akurasi Posisi Pesan Pengujian Nilai *Level* DWPT

Pada gambar diatas hasil akurasi tidak berubah saat level 1, 2, 3 dan didapatkan analisis bahwa akurasi tertinggi didapat saat jumlah sisipan sebesar 90 karakter yaitu sebesar 69%.

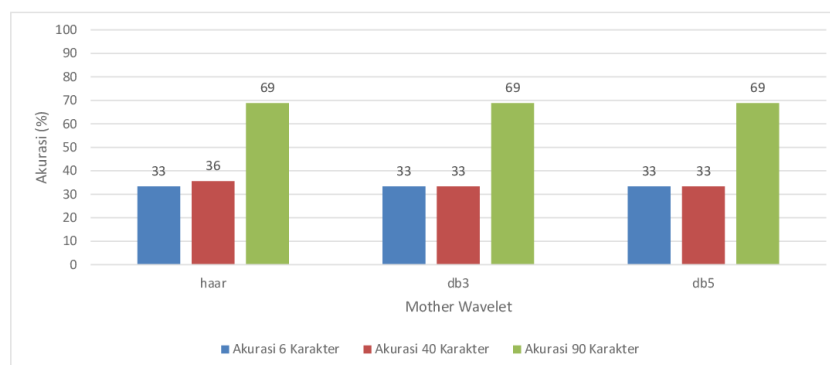
G. Pengujian Pengaruh *Mother* DWPT Terhadap Akurasi Keberadaan Pesan



Gambar 9 Akurasi Keberadaan Pesan Pengujian *Mother* DWPT

Pada pengujian ini didapatkan analisis bahwa jenis *Mother Wavelet* tidak mempengaruhi sistem saat mendeteksi pesan sisipan.

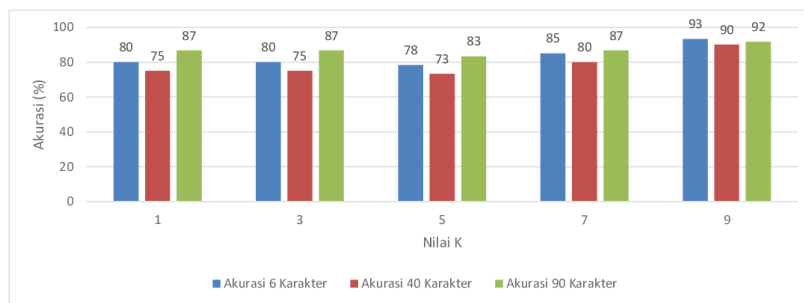
H. Pengujian Pengaruh *Mother* DWPT Terhadap Akurasi Posisi Posisi Pesan



Gambar 10 Akurasi Posisi Pesan Pengujian *Mother* DWPT

Pada pengujian ini hasil akurasi 90 karakter mendapatkan akurasi terbaik sebesar 69% pada setiap jenis *Mother DWPT*. Jenis *Mother Wavelet haar* akan digunakan pada proses selanjutnya.

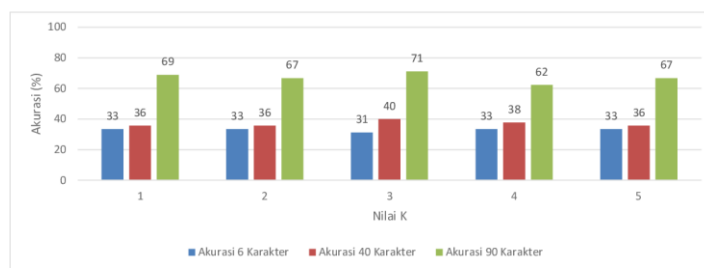
I. Pengujian Pengaruh Nilai K Terhadap Akurasi Keberadaan Pesan



Gambar 11 Akurasi Keberadaan Pesan Pengujian Nilai K

Pada perhitungan diatas didapatkan nilai akurasi terbaik pada saat K=9 dengan rata rata akurasi sebesar 91,67% pada semua karakter pesan sisipan.

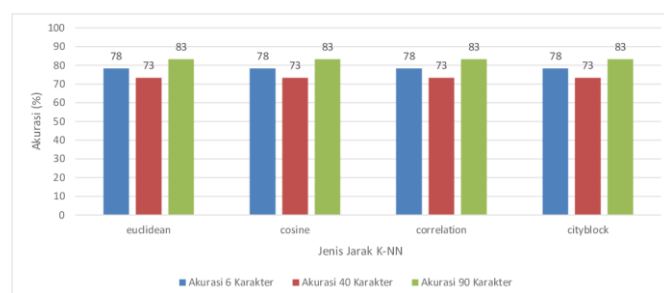
J. Pengujian Pengaruh Nilai K Terhadap Akurasi Posisi Pesan



Gambar 12 Akurasi Posisi Pesan Pengujian Nilai K

Berdasarkan hasil pengujian pengaruh nilai K terhadap akurasi deteksi posisi pesan sisipan didapatkan nilai K=5 memiliki akurasi terbesar saat panjang pesan sisipan 90 karakter yaitu sebesar 71%. Pada pengujian ini juga dapat dilihat bahwa semakin panjang pesan sisipan maka sistem akan lebih baik saat mendeteksi posisi pesan sisipan.

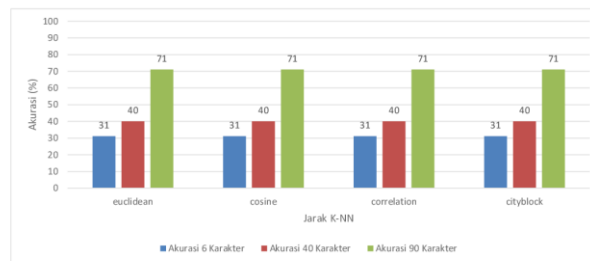
K. Pengujian Pengaruh Jarak K-NN Terhadap Akurasi Keberadaan Pesan



Gambar 13 Akurasi Keberadaan Pesan Pengujian Jenis Jarak K-NN

Pada perhitungan diatas didapatkan analisis bahwa pada saat jenis jarak K-NN diubah ubah tidak akan mempengaruhi akurasi sedangkan semakin panjang pesan sisipan maka sistem yang akan dibangun akan mendeteksi pesan semakin akurat.

L. Pengujian Pengaruh Jarak K-NN Terhadap Akurasi Posisi Pesan



Gambar 14 Akurasi Posisi Pesan Pengujian Jenis Jarak K-NN

Berbanding lurus dengan hasil pengujian deteksi ada tidaknya pesan rahasia skenario ini juga menghasilkan akurasi yang sama dan tidak terjadi perubahan akurasi saat jenis jarak K-NN diubah dan didapatkan analisis bahwa semakin banyak jumlah pesan sisipan, sistem mampu lebih baik mendeteksi posisi pesan rahasia.

5. Kesimpulan

Berdasarkan pengujian dan analisis sistem yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Implementasi sistem steganalisis audio pada file video .mp4 dengan menggunakan metode DWPT dan klasifikasi K-NN mampu menghasilkan performansi yang baik dalam proses deteksi penyisipan pesan dan deteksi posisi.
2. Pada sistem deteksi keberadaan pesan menggunakan parameter fitur statistik Standar deviasi, tipe jarak *euclidean*, ukuran *frame* sebesar 128, *Mother Wavelet* yang digunakan *haar*, *level* sebesar 1, *volume* sisipan 90 karakter dan menggunakan nilai $K=9$ menghasilkan akurasi 93%.
3. Pada sistem deteksi posisi pesan menggunakan parameter fitur statistik Standar deviasi, tipe jarak *euclidean*, ukuran *frame* sebesar 128, *Mother Wavelet* yang digunakan *haar*, *level* sebesar 1, *volume* sisipan 90 karakter dan menggunakan nilai $K=5$ menghasilkan akurasi 71%..

6. Daftar Pustaka

- [1] Nanang Adi Setyawan and Bambang Hidayat, DR., Ir and Sofia Saidah, S.T., M.T., "Steganalisis Audio Digital Dengan Discrete Wavelet Transform Menggunakan Metode Support Vector Machine Classifier" Universitas Telkom, 2013.
- [2] J. Elizabeth, I. Bambanghidayat, And I. N. Apraz, "Simulasi Dan Steganalisis Audio Digital Menggunakan Metode Discrete Wavelet Transform Dan Principal Component Analysis" Universitas Telkom, Pp. 110, 2015.
- [3] D. Thompson Et Al., "Serious Video Games For Health: How Behavioral Science Guided The Development Of A Serious Video Game," Simul. Gaming, Vol. 41, No. 4, Pp. 587606, 2010.
- [4] S. Nurjamillah And S. S. M. S. Umbara, Dr.Ir. Bambang H, Rian Febrian U, "Simulasi Dan Analisis Steganografi Dengan Convolutional Code Dan Pemodelan Psychoacoustic," Universitas Telkom Pp. 18, 2014.
- [5] A. F. Ryamizard, I. B. Hidayat, And S. S. S. T, Menggunakan Metode Mel Frequency Cepstral Coefficient (Mfcc) Dan Klasifikasi K-Nearest Neighbour (Knn) Detection Single Tone Of Bugis Makassar Music Instrument Using Mel Frequency Cepstral (Mfcc) Coefficient And K-Nearest Neighbour Classification (, Pp. 17).