DETEKSI POSISI PENYISIPAN PESAN TEXT PADA STEGANOGRAFI AUDIO DENGAN METODE MFCC DAN DECISION TREE

A DETECTION OF THE POSITION MESSAGE TEXT IN AUDIO STEGANOGRAPHY USING MFCC METHOD AND DECISION TREE

Septian Setyo Wicaksono, Rita Magdalena[2], Bambang Hidayat[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**septiansetyow@gmail.com**, [2]**ritamagdalena@telkomuniversity.ac.id**, [3]**bhidayat@telkomuniversity.ac.id**

Abstrak

Data yang diterima dari berbagai sumber sperti google belum tentu sepenuhnya terhindar dari virus. Meskipun antivirus sudah banyak beredar, belum tentu bisa mengetahui apakah ada pesan tersembunyi di balik file yang kita unduh dari mesin pencarian. Steganografi adalah seni dan ilmu menulis pesan tersembunyi sehingga hanya pengirim dan penerima saja yang mengetahui ada atau tidaknya pesan tersembunyi di file yang kita unduh dari mesin pencarian. Untuk mengantisipasi hal tersebut dapat dilakukan dengan menggunakan metode steganalisis. Steganalisis merupakan salah satu solusi yang dapat digunakan untuk mengawasi dan mengidentifikasi pesan yang dicurigai membawa pesan tersembunyi dibalik file tersebut. Dalam penelitian Tugas Akhir ini merancang sebuah arsitektur dari metode bernama MFCC (Mel-Frequency Cepstral Coefficien) dan Decision Tree untuk prses klasifikasi. Dilakukan analisis terhadap nilai-nilai statistik yang dimiliki suatu berkas audio yang memiliki format .wav yang terdeteksi adanya pesan dan posisi pesan berada. Dari nilai yang telah didapat, nilai tersebut digunakan untuk melihat berkas audio yang memiliki format .wav asli dan yang sudah disisipi pesan (file ter-stego) dengan proses penyisipan LSB. Dalam penelitian ini dibuat suatu perangkat lunak yang mampu mendeteksi keberadaan pesan tersembunyi beserta posisi penyisipan dengan menggunakan metode MFCC dengan klasifikasi Decision Tree. Pada penelitian Tugas Akhir ini merancang suatu sistem yang mampu identifikasi pesan rahasia pada file audio berformat .wav dengan metode MFCC dan Decision Tree. Sistem yang dibuat menghasilkan performansi terbaik dengan tingkat akurasi sebesar 67,52% untuk steganalisis. Untuk deteksi posisi didapat akurasi terbaik sebesar 94,73% dari data uji yang teridentifikasi sebagai stego-audio. Sedangkan untuk deteksi terhadap letak posisi didapat akurasi sebesr 56,58%

Kata Kunci: Steganografi, Steganalisis, *Mel-Frequency Cepstral Coefficien* (MFCC), *Decsition Tree*.

Abstract

Data received from various sources such as Google is not necessarily completely protected from viruses. Even though antivirus has been circulating a lot, it is not certain to find out if there are hidden messages behind the files that we download from search engines. Steganography is the art and science of writing hidden messages so that only the sender and recipient are aware of the presence or absence of hidden messages in files that we download from search engines. To anticipate this, it can be done by using the steganalysis method. Steganalysis is one solution that can be used to monitor and identify messages that are suspected of carrying hidden messages behind the file In this Final Project research designed an architecture of a method called MFCC (Mel-Frequency Cepstral Coefficien) and Decision Tree for the classification process. An analysis of the statistical values of an audio file in .wav format detected by the message and where the message is located is performed. From the value obtained, the value is used to view audio files that have the original .wav format and which have been inserted messages (stegoed files) with the LSB insertion process. In this research, a software is made that is able to detect the presence of hidden messages and their insertion positions using the MFCC method with the Decision Tree classification. In this Final Project research designed a system that is able to identify secret messages in audio files with .wav format using MFCC and Decision Tree methods. The system created produces the best performance with an accuracy level of 67.52% for steganalysis. For position detection, the best accuracy is 94.73% from the test data identified as stego-audio. As for the detection of the position position, the accuracy is 56.58%.

Keywords: Steganography, Steganalysis, Mel-Frequency Cepstral Coefficien (MFCC), Decsition Tree.

1. Pendahuluan

Data yang diterima dari berbagai sumber seperti google, bing, ask, dogpile belum tentu sepenuhnya terhindar dari virus. Meskipun antivirus sudah banyak beredar di muka bumi ini belum tentu bisa mengetahui apakah ada pesan tersembunyi di balik file yang kita unduh dari mesin pencarian. Steganografi adalah seni dan ilmu menulis pesan tersembunyi sehingga hanya pengirim dan penerima saja yang mengetahui ada atau tidaknya pesan

tersembunyi difile yang kita unduh dari mesin pencarian [1]. Untuk mengantisipasi hal tersebut dapat dilakukan dengan menggunakan metode steganalisis. Steganalisis merupakan salah satu solusi yang dapat digunakan untuk mengawasi mengidentifikasi pesan yang dicurigai membawa pesan tersembunyi dibalik file tersebut [2].

Dalam penelitian Tugas Akhir ini dilakukan analisis terhadap nilai-nilai statistik yang dimiliki suatu berkas audio yang memiliki format .wav yang terdeteksi adanya pesan dan posisi pesan berada. Dari nilai yang telah didapat, nilai tersbut digunakan untuk melihat berkas audio yang memiliki format .wav asli dan yang sudah disisipi pesan (file ter-stego) dengan proses penyisipan LSB. Dalam penelitian ini dibuat suatu perangkat lunak yang mampu mendeteksi keberadaan pesan tersembunyi beserta posisi penyisiapan dengan menggunakan metode MFCC dengan kasifikasi menggunakan Decision Tree.

Pada penelitian sebelumnya, penulis mengambil referensi dari penelitian-penelitan yang telah dilakukan sebelumnya yang terkait dengan latar belakang masalah pada Tugas Akhir yang penulis susun.

Pada penelitian pertama [3] "Deteksi Posisi Penyisipan Dengan Metode Discrete Fourier Transform Untuk WAV yang Tersisipi Pesan Secara *Psychoacoustics*" dan menghasilkan tingkat akurasi sebesar 100% pada sistem steganalisis dan akurasi sebesar 75,56% pada deteksi posisi dan volume citra tersteganografi.

Lalu dilakukan penelitian kedua [9], telah dilakukan proses steganalisis menggunakan metode statistik Mel-Frequency Cepstral Coefficeint (MFCC) pada berkas audio yang menggunakan klasifikasi Support Vector Machine (SVM). Hasil akurasi yang didapatkan berdasarkan jumlah sisipan yang yang memiliki lebih sedikit pesan "text" yaitu sebesar 43,75%, sedangkan untuk sisipan yang memiliki pesan "text" yang banyak mendapatkan nilai akurasi mecapai 50%.

Namun pada penelitian ini, penulis merancang sistem dengan metode ekstraksi dan metode klasifikasi yang berbeda dari penelitian sebelumnya. Oleh karena itu, dilakukan penelitian Tugas Akhir ini untuk memperbaiki kekurangan pada penelitian sebelumnya yang sudah dilakukan.

2. Konsep Dasar

2.1 Audio Digita

Audio digital merupakan versi digital dari suara analog. Pengubahan suara analog menjadi suara digital membutuhkan suatu alat yang disebut Analog to Digital Converter (ADC). Sedangkan pada proses kebalikannya menggunakan alat yang dikenal Digital to Analog Converter untuk mengubah sinyal digital menjadi sinyal analog. ADC akan mengubah amplitudo gelombang analog menjadi digital yang merupakan proses konversi [4].

2.2 Steganografi

Steganografi adalah seni dan pengetahuan 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. Di masa lalu orang-orang biasa menggunakan tinta tak tampak (invisible ink) untuk berkomunikasi pada steganografi, tetapi dengan teknologi sekarang bisa memberi kemudahan untuk menyembunyikan pesan di suatu media dengan berbagai metode dan cover.

2.3 Steganalisis

Steganalisis merupakan anti-steganografi, dimana memiliki pengertian yaitu suatu teknik yang digunakan untuk mendeteksi dan menganalisa kemungkinan adanya data tersembunyi pada audio tersteganografi. Steganalisis juga merupakan teknik yang digunakan untuk melawan keberadaan steganografi dengan memungkinkan adanya metode deteksi, ekstraksi, destruksi, dan manipulasi dari data tersembunyi yang ada di dalam stego-object. Steganalisis ini bisa dilakukan dengan berbagai macam cara, salah satunya hanya ditujukan untuk mendeteksi keberadaan suatu data yang tersembunyi [5].

2.4 *Mel-Frequency Cepstral Coefficient (MFCC)*

MFCC adalah suatu metode untuk merepresentasikan sinyal suara dalam bentuk vektor. Dalam MFCC terdapat tujuh tahap [6] [7], yaitu:

2.4.1 *Pre-Emphasis*

Pre-emphasis berfungsi untuk meratakan atau menstabilkan nilai magnitude dari sinyal suara.

2.4.2 *Framing*

Framing adalah usaha membagi keseluruhan sinyal suara menjadi beberapa frame dengan panjang tertentu. Panjang tiap frame umumnya sangat singkat sekitar 20 sampai 40 ms.

2.4.3 *Windowing*

Windowing adalah usaha meredam noise yang muncul di kedua ujung *frame*. Teknik yang digunakan dalam windowing ini adalah *Hamming Window*.

2.4.4 *Fast Fourier Transform* (FFT)

FFT adalah penyederhanaan metode Discrete Fourier Transform (DFT) dimana FFT membagi dua perhitungan DFT menjadi komponen ganjil dan genap untuk meringankan komputasi.

2.4.5 *Mel Frequency Filter Bank*

Pada tahap ini, sinyal suara pada domain frekuensi diubah menjadi domain frekuensi mel.

2.4.6 *Discrete Cosine Transform* (DCT)

DCT berfungsi untuk mengembalikan sinyal suara pada domain frekuensi ke domain waktu sehingga didapatkan koefisien cepstrum.

2.4.7 *Ceostral Liftering*

Hasil dari proses MFCC memiliki beberapa kelemahan. Low order dari cepstral coefficients sangat sensitif terhadap spectral slope, sedangkan bagian high order sangat sensitif terhadap noise. Salah satu teknik untuk meminimalisasi sensitifitas adalah menggunakan cepstral liftering.

2.5 *Decision Tree*

Decision tree adalah klasifikasi yang mudah diinterpretasikan terhadap manusia untuk pegenalan pola. Metode ini menggunakan representasi pohon, terdapat node-node yang merepresentasikan atribut, daun yang merepresentasikan kelas, dan cabangnya merepresentasikan nilai dari kelas tersebut. Algoritma decision tree dibentuk dari 3 tipe [8].

2.6 Teknik Penyembunyian Data Berdasarkan Domain

Teknik penyembunyian data pada audio dapat dilkukan dengan dua macam domain, yaitu :

2.6.1 Domain Spasial (domain waktu)

Teknik ini memodifikasi nilai byte dari pesan text. Memiliki hasil yang komputasinya rendah, kapasitas embedding besar, tetapi memiliki kekurangan pasa sisi robustness dan transparency. Salah satu metode yang tergolong dalam domain spasial yaitu metode LSB.

2.6.2 Domain Transform (domain Frekuensi)

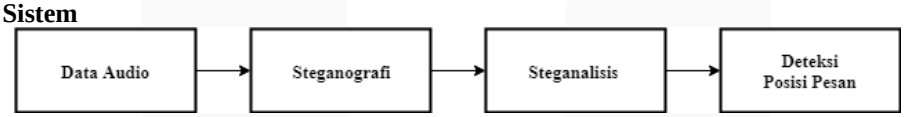
Teknik ini memodifikasi koefisien frekuensi sinyal. Hasil akhirnya memiliki tingkat robustness dan transparency yang lebih baik, tetapi kapasitas embedding lebih sedikit. Transformasi yang biasa digunakan yaitu DWT, DCT dan DFT.

2.7 *Least Significant Bit* (LSB)

Metode LSB merupakan teknik penyembunyian data yang bekerja pada domain waktu atau domain spasial. LSB adalah bit yang mempunyai nilai paling rendah, atau bit yang berada pada posisi paling kanan. Penyisipan dilakukan dengan memodifikasi bit terakhir dalam satu byte data. Metode ini melakukan suatu pendekatan yang sederhana untuk menyisipkan informasi [4]. Untuk menjelaskan metode ini akan menggunakan audio dengan format .wav sebagai covertext. Pada susunan bit dalam sebuah byte (1 byte = 8 bit), dalam bit terdapat MSB yaitu (Most Significant Bit) dan LSB (Least Significant Bit).

3. Perancangan Sistem

3.1 Deskripsi Sistem

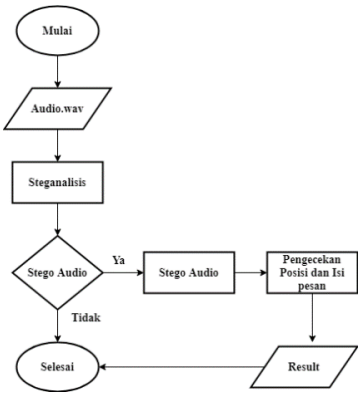


Gambar 1. Blok diagram sistem

Dalam perancangan dan implementasinya sistem pada tugas akhir ini dibagi menjadi 4 tahap utama, yaitu pengumpulan data audio, steganografi untuk mendapatkan data audio stego, steganalisis untuk deteksi keberadaan pesan lalu deteksi posisi pesan tersembunyi. Perancangan sistem ini dibuat untuk medeteksi posisi pesan rahasia pada data audio .wav menggunakan ekstraksi ciri MFCC dan klasifikasi menggunakan Decision Tree. Keempat tahap tersebut ditunjukan dalam bentuk diagram blok pada Gambar 3.1.

3.2 Perancangan Sistem Utama

Sistem steganalisis yang dirancang terdiri dari dua bagian yaitu proses ekstraksi dan proses klasifikasi. Proses ekstraksi ciri yang dilakukan yaitu menggunakan metode Mel-Frequency Ceptstral Coefficients (MFCC) yang memiliki tujuan untuk mendapatkan ciri fitur yang akan dijadikan acuan. Ekstraksi ciri akan terbagi menjadi dua kelas yaitu kelas audio asli dan kelas audio tersisipi pesan text. Metode windowing pada proses steganalisis ini bertujuan untuk mendeteksi posisi pesan pada audio yang tersteganografi. Metode ini juga melakukan iterasi sampai ditemukan letak posisi awal tersisipi pesan tersebut berada di koordinat mana yang tersisipi dan mengetahui isi pesan yang tersembunyi didalam file audio yang tersteganografi.



Gambar 2. Diagram Alir Sistem Utama.

Perancangan sistem seperti pada Gambar 3, adapun prosesnya yaitu sebagai berikut:

A. Tahap awal sistem adalah pengumpulan data audio .wav. data audio sebanyak 40 data, dipisah menjadi 30 data latih dan 10 data uji. Data latih dan data uji selanjutnya disisipi pesan pada proses steganografi menggunakan metode LSB. Hasil dari proses steganografi adalah audio stego yang disisipkan pesan rahasia dengan jumlah karakter yang berbeda, posisi yang berbeda, dan penempatan yang berbeda. Pada data uji, 5 dari data akan tersisipi pesan tersembunyi dan 5 sisanya tidak ada pesan yang tersembunyi.
B. Tahap selanjutnya, file latih sebanyak 40 akan di ekstraksi menggunakan metode MFCC. Pada representasi MFCC di dalamnya terjadi proses transfromasi FFT, diperuntukan mewujudkan perhitungan digital terhadap spektrum-spektrum frekuensi yang dapat dilakukan dengan lebih sederhana dan merubah sinyal dari domain waktu ke domain frekuensi. Pada tahap selanjutnya, hasil dari log mel spektrum harus dikonversikan kembali ke domain waktu dengan invers FFT menggunakan Discrete Cosine Transform (DCT) karena perhitungannya lebih efisien. Hasil akhirnya lah yang disebut sebagai Mel-Frequency Cepstral Coefficient (MFCC). Data ekstraksi tersebut lalu disimpan ke Database untuk dijadikan acuan pembanding pada klasifikasi Decision Tree.
C. Hasil keluaran dari MFCC tersebut sudah berupa koefisien dan data statistik sepekerti mean, variance, skewness, standard deviation, entropy dan kurtosis. Kemudian data-data tersebut akan diklasifikasikan menggunakan metode Decision Tree yang dapat memisahkan dua set data dari dua kelas yang berbeda.
D. Jika hasil klasifikasi telah didapatkan, maka dapat dilakukan perbandingan antara kedua kelas tersebut dan juga pengambilan keputusan apakah ada pesan tersembunyi atau tidak pada berkas audionya.
E. Jika file diidentifikasi adanya pesan tersembunyi, maka langkah selanjutnya adalah mencari pada bagian mana file tersebut disembunyikan pesan rahasia dan apa isi pesan tersembunyi didalam file audio tersebut.
F. Hasil dari steganalisis pada sistem ini dapat mengeluarkan dibagian mana pesan tersebut disembunyikan dan bisa mengetahui isi pesan apa yang tersembunyi. Proses steganalisis dinyatakan selesai.

3.3 Analisis Performansi Sistem

Pada proses pengujian sistem dilakukan untuk mengetahui performa dari sistem yang telah dibuat, dan nantinya bisa diketahui kekurangan maupun kelebihan dari sistem tersebut. Sehingga, dapat dilakukan evaluasi agar analisis yang dilakukan sesuai dengan hasil yang didapatkan. Performa sistem tersebut dapat diukur berdasarkan parameter berikut ini:

3.4.1 Akurasi

Parameter yang pertama yaitu akurasi, dimana parameter ini digunakan untuk mengukur ketepatan atau kebenaran sistem steganalisis yang telah dibuat dengan mengenali sebuah citra masukan, sehingga dapat menghasilkan keluaran yang tepat. Pada penelitian ini, nilai akurasi diberikan arti sebagai ketepatan dalam menentukan terdapat pesan tersembunyi atau tidak, ketepatan dalam menentukan posisi dan volume pada citra tersteganografi. Jika nilai akurasi yang didapat pada sistem semakin tinggi, maka hasil yang didapat menunjukkan bahwa sistem yang dibuat memiliki kinerja yang baik, begitu juga sebaliknya. Parameter ini dapat dirumuskan sebagai berikut:

$$Akurasi = \frac{n\ (Jumlah\ Audio\ Benar)}{N\ (Jumlah\ Audio\ Total)}\ x\ 100\% \qquad (1)$$

3.4.2 Waktu Komputasi

Waktu komputasi dari steganalisis sistem diperlukan untuk melakukan proses dari awal percobaan sampai akhir. Parameter yang dibutuhkan untuk melakukan perhitungan waktu komputasi secara matematis dapat dirumuskan seperti persamaan berikut ini:

$$\text{Waktu Komputasi} = \text{Waktu Akhir} - \text{Waktu Mula}i \quad (2)$$

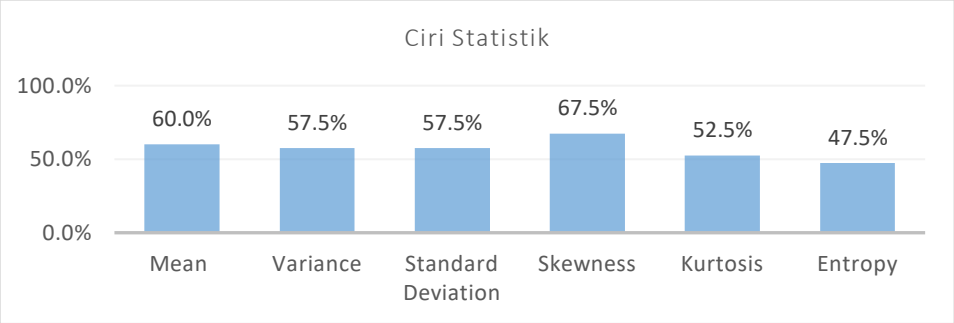
4 Pengujian dan Analisis Sistem

Sistem yang telah dirancang dalam penelitian ini perlu diketahui performansi untuk mengetahui apakah sistem yang telah dirancang mampu melakukan optimasinya dengan baik atau tidak. Untuk itu diperlukan pengujian terhadap sistem dengan mengukur seberapa besar tingkat keberhasilan sistem dan melakukan beberapa analisis terhadap beberapa parameter seperti efisienisi sistem yang telah dirancang.

4.1 Pengujian Sistem Steganalisis

a) Pengujian pengaruh ciri statistik terhadap akurasi sistem

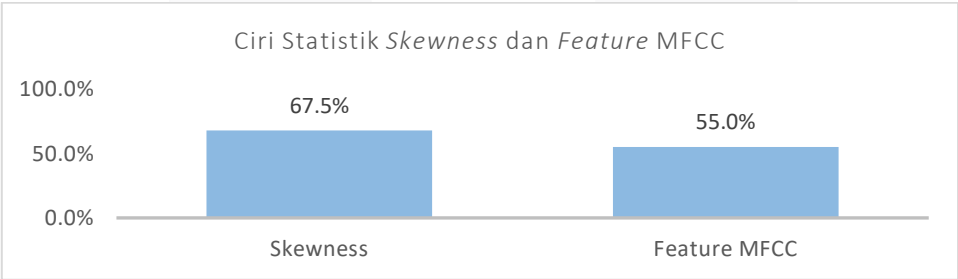
Berdasarkan hasil dari pengujian sistem ciri statistik orde satu, didapatkan ciri dari statistik Mean mengghasilkan akurasi sebesar 60% dengan waktu komputasi 7,27 detik, untuk ciri statistik Variance menghasilkan akurasi sebesar 75% dengan waktu komputasi 7,37 detik, untuk ciri statistik Standard Deviation menghasilkan akurasi sebesar 57,5% dengan waktu komputasi 7,22 detik, untuk ciri statistik Skewness menghasilkan nilai akurasi terbaik sebesar 67,5% dengan waktu komputasi 7,25 detik , pada nilai Kurtosis mendapat nilai akurasi yaitu 67,5% dengan waktu komputasi 7,73 detik, dan yang terakhir adalah Entropy yang mendapatkan nilai akurasi sebesar 47,5% dengan waktu komputasi 7,34 detik.



Gambar 1. *Bar chart* pengujian ciri statistik

b) Pengujian sistem steganalisis tanpa menggunakan ciri statistik

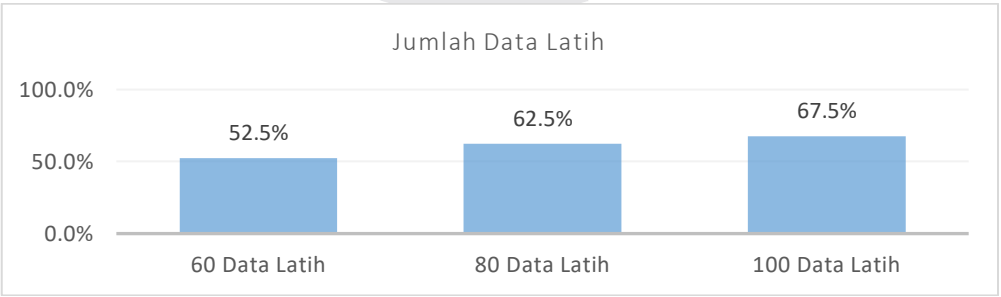
Dari pengujian yang didapat, pengujian dengan menggunakan ciri tebaik yaitu Skewness menghasilkan akurasi sebesar 67,5% dan feature MFCC mendapatkan nilai akurasi sebesar 55%.



Gambar 2. *Bar Chart* perbandingan ciri statistik MFCC

c) Pengujian berdasarkan perbedaan jumlah data latih

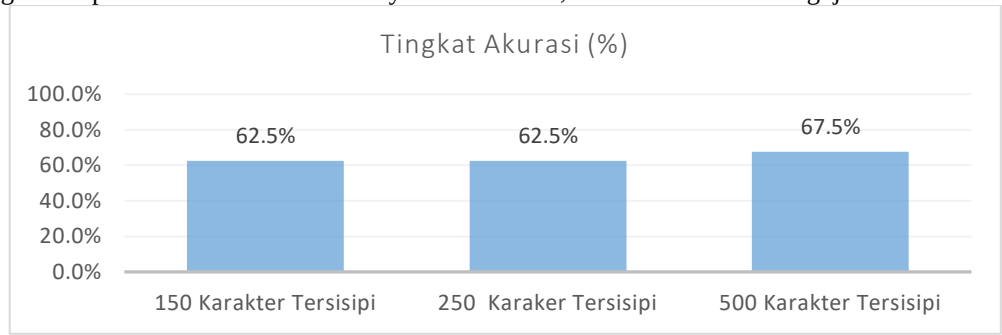
Berdasarkan hasil pengujian, didapatkan tingkat akurasi sebesar 52,5% dari pengujian 60 data latih, lalu pada 80 data latih didapatkan tingkat akurasi sebesar 62,5% dan untuk 100 data latih didapatkan nilai terbaik yaitu sebesar 67,5%.



Gambar 3. *Bar Chart* hasil dari perbedaan jumlah data latih

d) Pengujian pengaruh banyak sedikitnya pesan sisipan

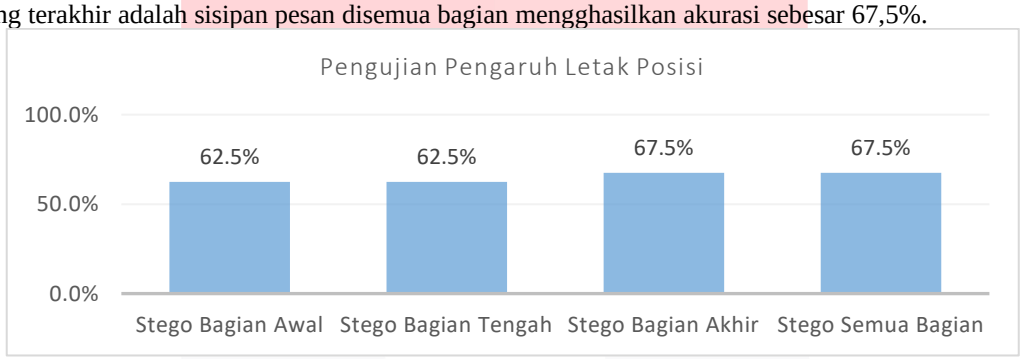
Berdasarkan hasil pengujian yang dilakukan, didapatkan tingkat akurasi sebesar 62,5% dari 150 karakter sisipan, pada 250 karakter sisipan mendapatkan akurasi sebesar yaitu 62,5% dan yang terakhir adalah 500 karakter sisipan yang mendapatkan nilai akurasi terbaik yaitu sebesar 67,5%.Tabel 4. Hasil Pengujian Level DWT.



Gambar 4. *Bar Chart* jumlah karakter sisipan

e) Pengujian pengaruh letak posisi sisipan

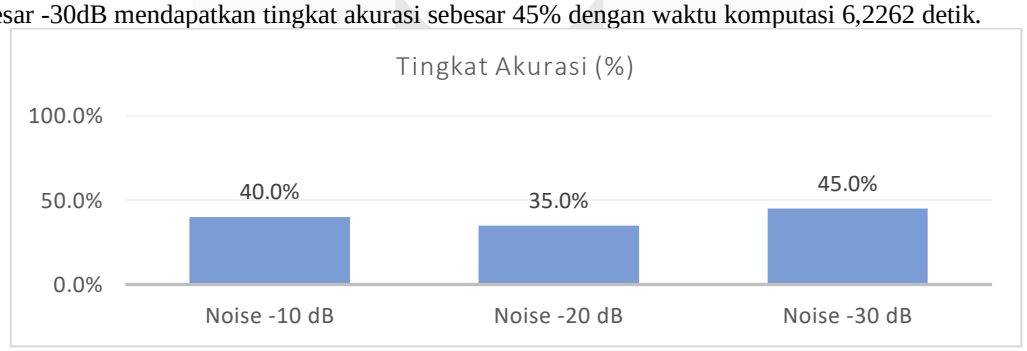
Berdasarkan hasil dari pengujian dari perbedaan letak posisi penyisipan pesan, didapatkan pesan dengan sisipan dibagian awal mengghasilkan akurasi sebesar 62,5%, untuk pesan sisipan dibagian tengah mengghasilkan akurasi sebesar 62,5, untuk pesan sisipan dibagian akhir mengghasilkan akurasi sebesar 67,5, dan untuk pesan sisipan yang terakhir adalah sisipan pesan disemua bagian mengghasilkan akurasi sebesar 67,5%.



Gambar 5. *Bar Chart* hasil dari perbedaan letak posisi

f) Pengujian pengaruh serangan noise terhadap file stego

Berdasarkan hasil dari pengujian dari pebedaan noise yang diinputkan, file yang disisipi noise sebesar -10dB mendapatkan akurasi sebesar 40% dengan waktu komputasi 6,9433 detik, untuk file yang disisipi noise sebesar -20dB mendapatkan nilai akurasi 35% dengan waktu komputasi 6,224 detik, dan yang terakhir file yang disisipi noise sebesar -30dB mendapatkan tingkat akurasi sebesar 45% dengan waktu komputasi 6,2262 detik.



Gambar 6. *Bar Chart* hasil pengujian perbedaan serangan *noise*

4.2 Pengujian Sistem Deteksi Posisi Pesan Sisipan

Pada proses pengujian ini menganalisis bagaimana pengaruh perbedaan posisi penyisipan pesan rahasia, apakah penyisipan tersebut benar disisipkan pada posisi-posisi tertentu, tujuan dari pengujian ini adalah untuk menentukan seberapa akurat sistem ini dalam menentukan posisi penyispian pesan rahasia tersebut.

Tabel 1. Hasil Pengujian Deteksi Posisi Sisiapan

Data ke	Status	Posisi Penyisipan	Status Posisi	Akurasi Posisi

51	Benar	1 2 3 6	Hampir benar	87,5 %
54	Benar	1 4 5 7 9	Hampir benar	61,53 %
56	Benar	1 - 16	Hampir benar	31,25 %
60	Benar	1 2 7 8 9 10 12	Hampir benar	53,84 %
61	Benar	2 6 8 9	Hampir benar	40 %
62	Benar	4 5 7 8 13 15 16 17 18 19	Hampir benar	40 %
63	Benar	2 3 4	Hampir benar	55,56 %
64	Benar	4 8 12	Hampir benar	80 %
65	Benar	4 8 12	Hampir benar	50 %
67	Benar	1 2 5 6	Hampir benar	25 %
69	Benar	2 5 6 9	Hampir benar	30,76 %
70	Benar	1 2 3 4 5 6 7 8 9 10 11 13 14 16 18	Hampir benar	75%
71	Benar	4 7	Hampir benar	44,44 %
72	Benar	5 6 7 8 9 10 11 14	Hampir benar	33,33 %
74	Benar	1 3 4 5	Hampir benar	35,71 %
75	Benar	1 2 5 6	Hampir benar	25 %
77	Benar	2 5 6 9	Hampir benar	46,15 %
80	Benar	5 10 13 16 17	Hampir benar	29,41 %
84	Salah	2 4 5 6 7 8 9 10 13 14 15 16 17 20 22 26 27 28 30 31 32 34	Salah Posisi	40,54 %

Dari pengujian 19 data uji yang diidentifikasikan sebagai audio yang tersisipi pesan rahasia, didapatkan data yang benar dalam mendeteksi posisi pesan sisipannya adalah sebanyak 18 dari 19 data uji yang ada, maka akurasinya adalah sebesar 94,73% dan untuk akurasi letak posisi adalah 46,58%.

4.3 Pengujian Sistem Deteksi Posisi dan Volume Pesan Sisipan

Pada proses pengujian ini menganalisis bagaimana pesan yang teridentifikasi memiliki sisipan pesan rahasia makan akan dilakukan decoding apakah pesan sisipan masih asli atau sudah rusak isi pesannya.

Tabel 2. Hasil Pengujian Deteksi Isi Pesan

Data ke	karakter	Status Volume	Isi Pesan
51	150	Benar	Maju Tak Gentar
54	150	Benar	Maju Tak Gentar
56	150	Benar	Maju Tak Gentar
60	150	Benar	Ibu Kita kartini
61	250	Benar	Ibu Kita kartini
62	250	Benar	Ibu Kita kartini
63	250	Benar	Ibu Kita kartini
64	250	Benar	Ibu Kita kartini
65	250	Benar	Ibu Kita kartini

67	250	Benar	Ibu Kita kartini
69	250	Benar	Indonesia Raya
70	250	Benar	Indonesia Raya
71	500	Benar	Indonesia Raya
72	500	Benar	Indonesia Raya
74	500	Benar	Indonesia Raya
75	500	Benar	Indonesia Raya
77	500	Benar	Indonesia Raya
80	500	Benar	Indonesia Raya
84	500	Benar	Indonesia Raya

Dapat dilihat pada tabel diatas, bahwa hasil akurasi pada deteksi volume sama seperti deteksi posisi pesan sisipan, karena pengujian volume pesan sisipan hasilnya berbanding lurus dengan pengujian pengaruh posisi pesan sisipan, dikarenakan untuk mendapatkan volume pesan sisipan yaitu dengan cara mengurangi posisi terakhir kali penyisipan dengan posisi awal penyisipan, apa bila dalam menentukan posisi didapatkan hasil yang salah, maka dalam menentukan volume juga akan mengalami kesalahan.

4 Kesimpulan

Berdasarkan hasil pengujian penelitian sistem deteksi posisi pada audio tresteganogradi, maka ada beberapa hal yang dapat penulis simpulkan. Metode MFCC dan Decsion Tree dapat diimplementasikan dalam sistem steganalisis dan sistem deteksi posisi audio tersteganografi. Pada pengujian pengaruh ciri statistik didapatkan bahwa ciri statistik Sekwness menjadi ciri statistik terbaik. Pada pengujian sistem steganalisis dihasilkan akurasi terbaik sebesar 67,52%. Untuk akurasi deteksi posisi didapat sebesar 94,73% dan deteksi terhadap letak posisi didapat akurasi sebesar 46,58%

Daftar Pustaka:

[1] Kusuma, I. J. (2017). Analisis Teknik Steganografi Pada Audio MP3 Menggunakan Metode Parity Coding dan Enkripsi Ciphe Transposition. ISSN: 2502-2148, Vol.3 No.2 Juli-Desember 2017.
[2] W. Hidayat, “Mendeteksi Keberadaan Pesan Tersembunyi dalam Citra Digital dengan Blind Steganalysis,” Seniati., Vol.3., no.2, pp. 77–81, 2011.
[3] Asyraf Fakhri, I. I. (2019). DETEKSI POSISI PENYISIPAN DENGAN METODE DISCRETE FOURIER TRANSFORM UNTUK FILE AUDIO WAV YANG TERSISIPI PESAN SECARA PSYCHOACOUSTICS. Tugas Akhir. Jurusan Teknik Telekomunikasi. Universitas Telkom : Bandung, 1-8.
[4] Nur Shabrina and Bambang Hidayat,DR., Ir and S Rian ebrian Umbarra, S.Si, M.Si, “Analisis Kriptografi Dan Steganografi Audio Menggunakan Addvance Enryption Standard Dan Pembodelan Psychoacoustic.” eProceedings of Engineering, 2003.
[5] R. Bohme, “Principles of Modern Steganography and Steganalysis,” pp. 11– 78, 2010.
[6] D. K. Putra, “Simulasi dan Analisis Speaker Recognition Menggunakan Metode Mel Frequency Cepstrum Coefficient (MFCC) dan Gaussian Mixture Model (GMM),” Bandung : Universitas Telkom., 2017.
[7] D. Putra, “Verifikasi Biometrika Suara Menggunakan Metode MFCC dan DTW,” Lontak Komputer Vol.2 No.1 , pp. 11-14, 2011.
[8] Tesy B., Algoritma Klasifikasi Decision Tree, Surabaya: Institut Teknologi Sepuluh, 2009.