ANALISIS KRIPTOGRAFI DAN STEGANOGRAFI AUDIO MENGGUNAKAN *ADVANCED ENCRYPTION STANDARD* DAN *PEMODELAN PSYCHOACOUSTIC*

Nur Shabrina[1)], Bambang Hidayat, DR., Ir.[2)], Rian Febrian Umbara, S.Si, M.Si[3)].
[1,2,3)]Fakultas Teknik Universitas Telkom

Abstrak

Pengamanan data saat pengiriman informasi merupakan hal yang harus diperhatikan dalam teknologi telekomunikasi saat ini. Kemudahan dalam mendapatkan informasi dan bertukar data menyebabkan pengguna jasa telekomunikasi harus lebih berhati hati dan diperlukan suatu teknik untuk mengamankan data yang dikirim, salah satunya dengan teknik steganografi dan kriptografi. Steganografi adalah teknik menulis pesan tersembunyi atau menyembunyikan pesan rahasia agar orang yang tidak berhak tidak menyadari keberadaan pesan tersebut. Sementara kriptografi adalah teknik menulis pesan secara rahasia, salah satu metode yang digunakan adalah enkripsi. Dalam steganografi audio, media tempat untuk menyembunyikan pesan yang disebut dengan *cover* berupa file audio. Namun diperlukan adanya suatu optimalisasi yaitu dengan memilih tempat penyisipan pesan menggunakan pemodelan *Psychoacoustic.*

Pada Tugas Akhir ini dianalisis dan disimulasikan proses enkripsi pesan menggunakan Advanced Encryption Standard (AES), proses penyisipan, dan juga proses pengekstrakan pesan. Untuk proses penyisipannya dilakukan dengan mengganti sinyal cover pada daerah tertentu yang tidak sensitif oleh pendengaran manusia. Daerah tersebut didapat dari pemodelan *Psychoacoustic*.

Hasil yang diperoleh dari Tugas Akhir ini adalah sebuah file audio stego yang telah tersisipi pesan berupa teks yang telah dienkripsi AES yang memenuhi kriteria kriteria steganografi yaitu keberadaan pesan tidak dapat dipersepsi (SNR > 110 dB dan juga MSE < 1 x 10-13), kualitas file stego tidak berbeda jauh dengan file asli (MOS mendekati 5), juga pesan dapat diekstrak kembali. Namun sistem tidak memiliki ketahanan terhadap serangan berupa kompresi MP3, Cropping, Resampling, dan pemberian AWGN. Seluruh pesan yang telah disisipi tidak dapat terkestrak kembali sesuai pesan yang disisipkan

Kata Kunci: Steganografi, Audio, *Cryptography, Psychoacoustic, Advanced Encryption Standard*

Abstract

Data Security during transmission of information is something that must be considered in today's telecommunication technology. The simplicity in getting the information and exchange data causing user of telecommunications services should be more cautious, so we need a technique to secure data sent, one of them with steganography and cryptography techniques. Steganography is a technique of writing hidden messages or hide the secret message, so that, the unauthorized people are not aware of the existence of the message. While cryptography is the technique of writing a message in secret, one of the methods used is encryption. In audio steganography, media place to hide a message is called "a cover" in the form of an audio file. However, it's necessary to have an optimization, in example with choose the place to insert messages using Psychoacoustic modeling.

This final project is analyzed and simulated the message encryption process using Advanced Encryption Standard (AES), the insertion process and also the message extraction processes. The insertion process is done by replacing the cover signal in a certain area that is not sensitive to human hearing. That area obtained from Psychoacoustic modeling.

The results of this final project is an audio file that has text messages that have been encrypted AES that meet the criteria of steganography is the existence of a message can't be perceived (SNR> 110 dB and MSE <1 x 10-13), quality steganography file is not much different from the original file (MOS approaching 5), also the message can be extracted again. However, the system does not have the resilience to attacks such as MP3 compression, cropping, resampling, and the provision of AWGN. The entire message that has inserted can't be returned according to the insertion message

Key words: Steganography, Audio, Cryptography, Psychoacoustic, Advanced Encryption Standard

1. PENDAHULUAN

Pengamanan data saat pengiriman informasi merupakan hal yang harus diperhatikan dalam teknologi telekomunikasi saat ini. Kemudahan dalam mendapatkan informasi dan bertukar data menyebabkan pengguna jasa telekomunikasi harus lebih berhati hati dengan data yang hendak dikirimnya.

Untuk itu diperlukan sebuah teknik untuk mengamankan pesan yang hendak dikirim. Salah satunya steganografi, yaitu teknik menyembunyikan pesan sehingga selain pengirim dan penerima tidak ada yang menyadari keberadaan pesan rahasia.Berbeda dengan kriptografi yang pesan pesan berkodenya tidak disembunyikan dan dapat menimbulkan kecurigaan pihak yang tidak berkepentingan. Steganografi sendiri sudah banyak diaplikasikan di berbagai media, seperti teks, gambar, audio, maupun video. Biasanya informasi yang berupa text dimasukkan ke dalam bit-bit penyusun audio digital. Namun metode ini masih cukup sederhana sehingga keberadaan informasi masih bisa dideteksi oleh pihak lain.

Oleh karena itu, dalam tugas akhir ini dibuatlah sebuah implementasi agar metode steganografi teks pada audio digital menjadi lebih aman. Metode yang digunakan adalah mengenkripsi teks terlebih dahulu dengan algoritma kriptografi AES (*Advanced Encryption Standard*). Dan digunakan sebuah metode yang memanfaatkan daerah dari audio *cover* yang berada dibawah ambang batas pendengaran manusia dengan tujuan agar keberadaan pesan rahasia tidak terdeteksi oleh pihak yang tidak seharusnya, yaitu metode *psychoacoustic*.

2. DASAR TEORI

2.1 Audio Digital

Audio digital mengacu pada suatu teknologi yang merekam, dan memproduksi suara dengan cara mengencode sinyal audio dalam bentuk digital, bukan dalam bentuk sinyal analog. Audio yang berada dalam komputer selalu dalam bentuk digital karena komputer yang biasa digunakan hanya mengenali sinyal dalam bentuk digital. Saat kita merekam suara ke dalam komputer, soundcard akan mengubah sinyal suara manusia yang berbentuk analog ke dalam bentuk digital. Prosesnya disebut dengan digitizing. Sinyal audio terdiri dari telephone quality speech (300 Hz – 3400 Hz), wideband speech (50 Hz – 3000 Hz), dan wideband audio (20 Hz – 20000 Hz).

2.1.1 File WAV

Waveform Audio File Format (WAVE) atau yang lebih dikenal dengan WAV adalah format file standard Microsoft dan IBM untuk menyimpan bitstream audio di komputer. WAV merupakan aplikasi dari metode format bitstream Resource Interchange File Format (RIFF) untuk menyimpan data dalam "chunks". WAV adalah format utama yang digunakan pada sistem Windows untuk audio baku dan biasanya tidak terkompresi.

2.2 Steganografi Audio

Steganografi berasal dari kata steganos yang berarti "tersembunyi" dan graphien yang berarti "menulis". Jadi dapat disimpulkan bahwa steganografi adalah teknik menuliskan pesan secara tersembunyi, sehingga selain pengirim dan penerima tidak ada yang mengetahui atau bahkan menyadari keberadaan pesan rahasia tersebut. Berbeda dengan kriptografi hanya menyamarkan arti dari pesan tapi tidak menyembunyikannya, sehingga pesan tersebut dapat menimbulkan kecurigaan pihak lain.

Sehubungan dengan keamanan sistem informasi, steganografi hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. Steganografi lebih cocok digunakan bersamaan dengan metode lain untuk menciptakan keamanan yang berlapis. Sebagai contoh, steganografi dapat digunakan bersama dengan metode enkripsi.

Properti yang digunakan dalam steganografi yaitu:[1]

a. Embedded message (hidden object): pesan yang disembunyikan.
b. Cover object: pesan yang digunakan untuk menyembunyikan embedded message.
c. Stego object: cover yang sudah berisi pesan embedded message.
d. Stego key: kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stego object.

Ada beberapa kriteria yang seharusnya dimiliki oleh sistem steganografi, yaitu:[1]

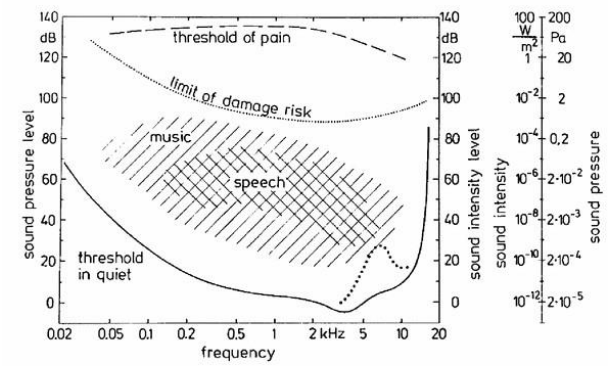
a. Imperceptible
Keberadaan pesan rahasia tidak dapat dipersepsi.
b. Fidelity.
Mutu cover audio tidak jauh berubah akibat embedded.
c. Recovery.
Data yang disembunyikan harus dapat diungkapkan kembali.

Kriteria robustness tidak terlalu penting karena yang utama steganografi bertujuan untuk menghindari kecurigaan (lawan tidak menyadari keberadaan pesan tersembunyi).

Maka, audio steganografi dapat diartikan sebagai cara penyembunyian atau penanaman/penyisipan data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu file audio, tetapi tidak diketahui keberadaannya oleh indera manusia (baik indera penglihatan maupun indera pendengaran), dan tahan terhadap serangan sampai pada tahap tertentu

2.3 *Psychoacoustic Model*[3]

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



Gambar 2.1 *Hearing Area*[3]

Pada kurva di Gambar 2.1 terlihat daerah di bawah kurva *masking* (*global masking threshold curve*) adalah daerah dimana telinga manusia tidak sensitif terhadap suara. Daerah di atas kurva *masking* sampai pada garis batas (*limit of damage risk*) adalah daerah dimana rata-rata telinga manusia dapat mendengar dengan jelas (daerah sensitif), sedangkan daerah di atas *threshold of pain* yaitu daerah dimana jika telinga mendengar sinyal suara yang melewati batas tersebut maka suara akan terdengar menyakitkan (*pain*) sehingga bisa merusak gendang telinga.

Saat ini *Psychoacoustic* diterapkan dalam berbagai bidang dari pengembangan perangkat lunak, di mana pengembang peta pola-pola matematis terbukti dan eksperimental, dalam pemrosesan sinyal digital seperti steganografi dan MP3 menggunakan model *Psychoacoustic* untuk meningkatkan rasio kompresi dan menghemat *bandwidth*.

2.4 AES[5]

Algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES (Data Encryption Standard) yang diadakan oleh NIST (National Institutes of Standards and Technology) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan Advanced Encryption Standard (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya.

AES memiliki ukuran *block* yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Panjang kunci yang digunakan mempengaruhi banyaknya round yang digunakan dalam proses AES, AES-128 membutuhkan 10 round, AES-192 12 round, dan AES-256 menggunakan 14 round. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran *block* yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal.

Blok-blok data masukan dan kunci dari AES dioperasikan dalam bentuk array. Sebelum menghasilkan keluaran chipertext. Setiap anggota array dinamakan dengan state. Setiap state akan mengalami proses yang secara garis besar terdiri dari empat tahap, yaitu:

1. Add Round Key

Pada dasarnya adalah melakukan XOR antara plaintext dengan round key yang di dapat dari proses key expansion. Proses XOR dilakukan per kolom yaitu kolom-1 plaintext di XOR dengan kolom-1 round key dan seterusnya.

- Key Expansion

Pada intinya, key expansion merupakan proses pembentukan round key atau membangkitkan array kunci menjadi 10 buah round key berbeda.

2. Sub-Bytes

Prinsipnya adalah menukar isi matriks/table yang ada dengan matriks lain yang disebut dengan Rijndael S- Box. Tidak seperti pada enkripsi DES di mana tabel S- Box berbeda pada setiap putaran, AES hanya mempunyai satu tabel S-Box untuk semua putaran (round).

3. Shift Rows

Adalah sebuah proses yang melakukan shift atau pergeseran per elemen pada setiap baris blok array.

4. Mix Columns

Pada proses ini, setiap kolom matriks hasil dari ShiftRows dikalikan dengan polinom a(x) mod (x4+1). Setiap kolomnya diperlakukan sebagai polinom 4-suku Galois Field GF (28). Polinom a(x) yang ditetapkan adalah:

a(x) = {03}x3 + {01}x2 + {01}x + {02}

Untuk proses dekripsi dari AES sendiri tidak jauh berbeda dengan proses enkripsinya. Proses dekripsi juga terdiri dari 4 proses utama yaitu:

1. Add Round Key

Proses ini sama dengan add round key pada proses enkripsi yaitu menggunakan operasi XOR. Proses XOR dilakukan antara chipertext dengan round key yang sama dengan round key saat proses enkripsi.

2. Inverse Shift Rows

Merupakan proses kebalikan dari proses Shift Rows yang dilakukan saat proses enkripsi.

2.5 FFT (*Fast Fourier Transform*)

Fast Fourier Transform (FFT) adalah suatu algoritma yang digunakan untuk merepresentasikan sinyal dalam domain diskrit dan domain frekuensi. Algoritma FFT digunakan untuk menghitung DFT (Discrete Fourier Transform) dengan cepat dan lebih efisien. Sebagai perbandingan, bila menggunakan DFT, maka kompleksitas transfomasi sebesar O(N2), sementara bila menggunakan FFT, selain waktu transformasi yang lebih cepat, kompleksitas pun menurun menjadi O(N log(N)). FFT bekerja dengan persamaan seperti yang disebutkan pada Persamaan (2.1).

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{j2\pi kn}{N}}$$; k=0,1,2,..,N-1… (2.1)[2]

Keterangan
Xk = output DFT

N = jumlah sampel yang akan diproses
xn = nilai sampel sinyal
k = variable frekuensi diskrit ; k = N/2

FFT diperoleh dengan memodifikasi DFT, yaitu dengan cara mengelompokkan batas n ganjil dan batas n genap, sehingga N point DFT menjadi (N/2) point, sehingga menghilangkan proses perhitungan kembar dalam DFT.

2.6 Java

Java adalah bahasa pemrograman berorientasi objek murni yang dibuat oleh James Gosling saat masih bergabung di *Sun Microsystem* dan dirilis pada tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sisntaksi model objek yang lebih sederhana. Saat ini java merupakan bahasa pemrograman yang paling populer digunakan, dan secraa luas dimanfaatkan dalam pengembangan berbagai jenis perangkat lunak aplikasi ataupun aplikasi berbasis web.

2.7.1 Pengelompokan Tipe Data dalam Java[16]

Java mendefinisikan delapan buah tipe data sederhana: *byte, short, int, long, char, float, double,* dan *boolean*. Tipe-tipe tersebut kemudian dikelompokkan menjadi beberapa bagian

- Tipe *Integer* (Bilangan bulat)

Kelompok ini terdiri dari tipe *byte, short, int,* dan *long*; yang digunakan untuk merepresentasikan data data yang bertipe bilangan bulat, misalnya -5, 0, 4, 100 dan sebagainya.

- Tipe *Floating-point* (Bilangan riil)

Kelompok ini terdiri dari tipe *float,* dan *double;* yang digunakan untuk merepresentasikan data-data yang bertipe bilangan riil (mengandung pecahan), misalnya -12.34, 0.65, dan sebagainya

- Tipe *Karakter*

Terdiri dari sebuah data yaitu *char*; yang merepresentasikan data dalam bentuk karakter alfanumerik dan simbol, misalnya ‘a’, ‘#’, ’@’, dan sebagainya

- Tipe *Boolean*

Kelompok ini juga terdiri dari sebuah tipe data, yaitu *boolean*; yang digunakan untuk merepresentasikan nilai logika (benar/salah)

2.7.2 Operator *Bitwise* dalam Java[16]

Operator *Bitwise* digunakan untuk melakukan operasi boolean terhadap dua buah *operand* bertipe *integer*. Operasi ini dilakukan bit demi bit. Dalam operasi ini nilai *true* direpresentasikan dengan nilai 1 dan *false* dengan nilai 0.

2.7 Parameter Penlaian pada Steganografi

Berdasarkan dengan kriteria steganografi (Robustness, Capacity, dan Imperceptibility) maka untuk mengetahui kualitas steganografi dapat digunakan beberapa parameter, baik parameter objektif, maupun subjektif

1. SNR (Signal to Noise Ratio)

(dB). Menurut International Federation of the Phonographic Industry (IFPI), SNR sinyal audio steganografi harus lebih besar dari 20 dB. Pada tugas akhir ini sinyal audio yang diukur adalah sinyal audio stego. Perhitungan mencari SNR dilihat pada persamaan (2.2)

$$SNR = 10 \log \frac{P_{signal}}{P_{noise}} \quad \text{…… (2.2)}$$

2. MSE (Mean Square Error)

MSE adalah rata-rata nilai error antara audio cover dengan audio stego. Secara matematis, dapat dirumuskan dalam persamaan (2.3)

$$MSE = \frac{1}{N} \sum_{i=1}^{N-1} \left[I_i - I_i^{'} \right]^2 \quad \text{…….. (2.3)}$$

Keterangan :
I(i) = data cover
I’(i) = data stego
N = panjang data

SNR adalah perbandigan antara sinyal audio dengan noise yang di representasikan dengan satuan decibel

3. CER (Character Error Rate)

Karena data yang disisipkan berupa teks, maka diperlukanlah perhitungan CER yang mencerminkan seberapa banyak karakter yang eror akibat pengolahan sistem. Perhitungan CER dapat dirumuskan dengan persamaan (2.4)

$$CER = \frac{\text{[illegible]}}{\text{[illegible]}} \quad \text{..... (2.4)}$$

4. MOS (Mean Opinion Score)

MOS adalah penilaian subjektif yang didapat dari pengamatan responden terhadap perbandingan kualitas audio hasil steganografi bila dibandingkan dengan audio asli. Penilaian MOS menggunakan skala pada tabel 2.1:

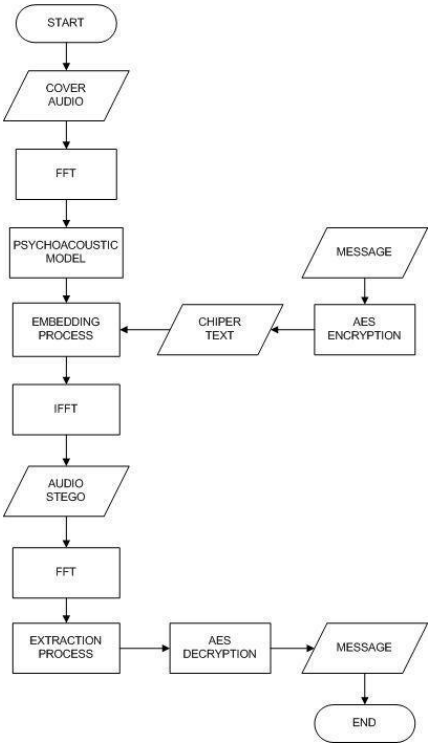
Tabel 2.1 Kriteria Penilaian MOS

MOS	*Quality*	*Impairment*
5	*Exellent*	*Imperceptible*
4	*Good*	*Perceptible but not annoying*
3	*Fair*	*Slightly annoying*
2	*Poor*	*Annoying*
1	*Bad*	*Very annoying*

3. PERANCANGAN DAN IMPLEMENTASI SISTEM

3.1 Model Sistem

Secara keseluruhan, model sistem embedding dan ekstraksi yang dirancang untuk sistem audio steganografi dalam tugas akhir ini, adalah seperti ditunjukkan pada Gambar 3.1



Gambar 3.1 Diagram Alir Proses Penyisipan

Secara umum, sistem terdiri dari 2 proses. Proses pertama adalah penyisipan (Embedding) di pihak pengirim, yaitu suatu proses dimana file cover yang berupa audio akan disisipi pesan berupa teks yang telah di enkripsi terlebih dahulu menggunakan algoritma AES (Advanced Encryption Standard). Hasil dari proses ini adalah sebuah file audio stego yang memiliki nilai SNR yang baik dan memiliki sifat imperceptible. Proses selanjutnya adalah ekstraksi di pihak penerima. Penerima akan mengekstrak file audio stego sehingga akan di dapatkan pesan rahasia tersebut.

Proses penyisipannya sendiri dapat dilakukan dengan menggunakan pemodelan psychoacoustic maupun tanpa menggunakan pemodelan psychoacoustic. Perbedaannya adalah pada tempat penyisipan yang dipilih. Kalau dengan pemodelan psychoacoustic tempat penyisipan dipilih di frekuensi yang tidak sensitif oleh pendengaran manusia (dimodelkan oleh global masking curve). Sedangkan bila tanpa menggunakan pemodelan psychoacoustic, penyisipan pesan dilakukan secara tersebar di seluruh bandwidth cover nya.

3.2 Sistem Penyisipan

3.2.1 AES Encryption

Penjelasan mengenai proses enkripsi dengan algoritma AES, adalah sebagai berikut:

Pesan yang di inputkan user diubah ke dalam bentuk hexadecimal menggunakan tabel ASCII dan kemudian dibagi menjadi blok blok matriks dengan ukuran 4x4

Kunci yang di inputkan juga diubah ke dalam bentuk ASCII dan dimasukkan ke matriks 4x4. Kunci kemudian di proses key expansion untuk mendapatkan round key

Kemudian blok pesan di add round key atau di XOR dengan round key yang didapatkan dari proses key expansion sebelumnya

Selanjutnya dilakukan beberapa proses yang diulang sebanyak 10 kali. Pada perulangan 1-9 dilakukan proses sub bytes, shift rows, mix columns dan add round key. Sedangkan pada perulangan terakhir, hanya dilakukan proses sub bytes, shift rows, dan add round key.

Setelah seluruh proses di atas selesai dilakukan, maka selanjutnya akan dilakukan konversi ulang nilai hexadecimal menjadi nilai biner karena nilai biner inilah yang diperlukan untuk proses penyisipan pesan (embedding).

3.2.2 Normalisasi dan Fast Fourier Transform (FFT)

Sinyal audio *cover* yang disimulasikan pada Tugas Akhir ini merupakan sinyal audio musik. Sinyal audio *cover* kemudian dinormalisasi sehingga didapatkan data dengan rentang -1 sampai 1. Kemudian data tersebut ditransformasi menggunakan *fast fourier transform* (FFT) menggunakan library JTransfroms[14]. Tujuannya adalah untuk mentransformasikan sinyal dari domain waktu ke domain frekuensi. Dilakukan transformasi ke domain frekuensi agar mudah mencari tempat penyisipan, yaitu pada titik dan frekuensi tertentu pesan disisipkan.

3.2.3 Psychoacoustic Model

Model psychoacoustic memanfaatkan keterbatasan indera manusia, terutama indera pendengaran. Dengan model ini dapat diketahui posisi mana yang cocok untuk menyisipkan pesan agar tidak merusak cover-audio sehingga meminimalkan kecurigaan pihak lain karena audio stego yang dihasilkan mirip dengan cover audionya.

Proses penyisipan dilakukan dengan mencari power spectral density yang kurang dari global masking threshold. Prosesnya:

Memodelkan kurva global masking threshold kemudian dilakukan pemilihan titik-titik pada kurva global masking threshold dimana telinga manusia kurang sensitif, yaitu dengan memilih dari sinyal cover yang amplitudonya berada dibawah kurva global masking threshold.

Lalu disingkronkan antara titik terpilih pada kurva global masking threshold dengan titik hasil FFT. Selanjutnya dicari pada frekuensi berapa titik-titik tersebut. Keluaran dari pemodelan ini yaitu, didapatkan titik-titik penyisipan pada domain frekuensi dari audio cover. Setelah didapatkan titik penyisipan maka titik tersebut yang akan dipakai sebagai tempat penyisipan.

3.2.4 Proses Penyisipan Pesan

Proses penyisipan dilakukan pada domain frekuensi setelah audio cover di FFT. Pesan teks pertama di enkripsi dengan algoritma AES. Keluaran dari proses AES adalah chiper dalam bentuk byte heksadesimal. Kemudian byte heksadesimal tersebut diubah ke dalam bentuk bit-bit biner.

Bit-bit pesan tersebut akan disisipkan pada titik yang sudah dipilih sebelumnya. Jika bit 1 maka koefisien FFT akan ditambahkan dengan +0,001, sedangkan pesan dengan bit 0, koefisien FFT dikurangi dengan nilai -0,001. Setelah semua bit pesan tersisipi, kemudian

dilakukan transformasi ke domain waktu menggunakan IFFT.

4. PENGUJIAN SISTEM DAN ANALISIS HASIL

4.4. Analisis Hasil Pengujian

4.4.1 Pengujian Sistem Dengan Menggunakan *Psychoacoustics* Model dan Algoritma AES

Sistem diuji dengan menyisipkan pesan rahasia dengan panjang (100 karakter, 500 karakter, dan 1000 karakter) ke file audio dengan durasi 5 detik, 10 detik, dan 15 detik. Pesan rahasia sebelumnya di enkripsi dengan proses enkripsi algoritma AES-128. Kemudian pesan disisipkan pada file audio yang berada di bawah threshold. Threshold didapat dari pemodelan *psychoacoustic*. Proses penyisipan dilakukan dengan menambahkan atau mengurangkan nilai dari file audio dengan 0.001 bergantung dengan pesan yang disispkan apakah "1" atau "0".

4.4.1.1 Analilis Kriteria *Imperceptibility*

Suatu sistem steganografi yang baik harus memenuhi kriteria *imperceptibility*, yaitu keberadaan pesan tidak dapat dipersepsikan. Kriteria *imperceptibility* dilihat berdasarkan nilai SNR dan MSE dari audio yang telah melalui proses steganografi. Pada Tugas Akhir ini, dapat dilihat dari Gambar 4.1 bahwa nilai SNR sudah baik, yaitu berkisar antara 119 dB – 140 dB. Dari Gambar 4.1 juga dapat terlihat bahwa panjang pesan mempengaruhi nilai SNR. Semakin panjang pesan yang disisipkan, maka nilai SNR menurun walaupun penurunannya tidak terlalu signifikan.

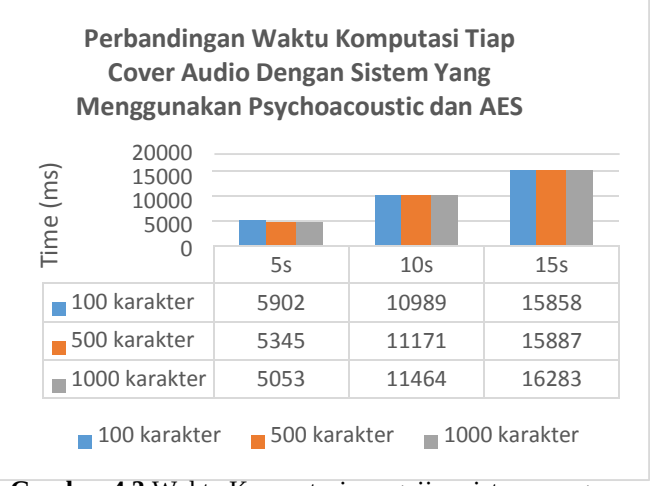
Gambar 4.1 SNR pengujian sistem dengan menggunakan *psychoacoustic* dan AES

Gambar 4.2 MSE pengujian sistem yang menggunakan *psychoacoustic* dan AES

Dari Gambar 4.2 dapat dilihat nilai MSE dari pengujian dengan menggunakan *psychoacoustic* model dan enkripsi AES sudah baik, pada semua durasi audio *cover*, dan dengan semua pengujian panjang pesan didapatkan nilai MSE < $1x10^{-13}$.

Dari kedua parameter yang telah disebutkan (SNR dan MSE) dapat dikatakan bahwa sistem steganografi dengan menggunakan pemodelan *psychoacoustic* ditambah dengan enkripsi dengan algoritma enkripsi AES memenuhi kriteria *imperceptibility* atau keberadaan pesan tidak dapat dipersepi atau kesamaan antara file audio *cover* dengan file audio stego sangat tinggi.

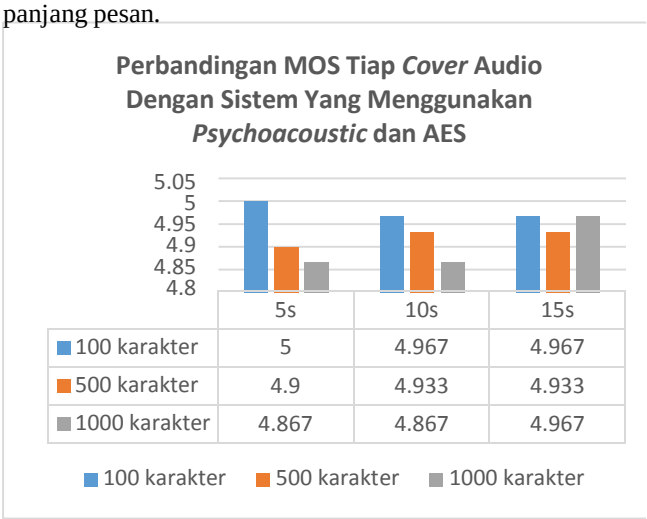
Untuk waktu komputasi, waktu dihitung dari saat sistem membaca file audio *cover* sampai proses ekstraksi dan *decoding* selesai dilakukan. Dapat dilihat pada Gambar 4.3, panjang pesan yang disisipkan tidak mempengaruhi waktu komputasi, tetapi dipengaruhi oleh panjang durasi *cover* audio. Semakin panjang durasinya, maka waktu yang dibutuhkan semakin lama, yaitu mencapai 16 detik. Dari Gambar 4.3 juga terlihat bahwa panjang pesan tidak mempengaruhi waktu komputasi. Waktu dipengaruhi oleh durasi cover audio, semakin lama cover audio, semakin banyak pula sampel yang harus diproses, maka dibutuhkan waktu yang lebih lama.



Gambar 4.3 Waktu Komputasi pengujian sistem yang menggunakan *psychoacoustic* dan AES

4.4.1.2 Analisis Kriteria *Recovery* Kriteria *recovery* pada sistem steganografi terpenuhi apabila pesan yang sudah disisipkan dapat diungkap lagi. Pada sistem dengan menggunakan pemodelan *psychoacoustic* dan algoritma AES, semua pesan, baik yang 100 karakter, 500 karakter, ataupun 1000 karakter, dengan durasi *cover* audio yang berbeda dapat ter- ekstrak dengan baik. Dengan kata lain, nilai CER atau *Character Error Rate* sama dengan 0 karena tidak ada karakter terekstrak yang eror.

4.4.1.3 Analisis Kriteria *Fidelity*
Kriteria *fidelity* terpenuhi apabila kualitas audio tidak jauh berubah setelah proses penyisipan. Oleh karena itu, kriteria *fidelity* dilihat dari MOS atau *Mean Opinion Score* yang diberikan kepada 30 responden. Hasilnya dapat dilihat dari Gambar 4.4. Dari 30 responden, mayoritas memberikan nilai 5 (tidak ada perbedaan sama sekali antara file audio cover dan audio stego) kepada semua kombinasi durasi audio cover dan panjang pesan.



Gambar 4.4 MOS pengujian sistem yang menggunakan *psychoacoustic* dan AES

4.4.2 Pengujian Sistem Dengan Menggunakan *Psychoacoustic* Model Tanpa Menggunakan Algoritma AES

Pengujian sistem hampir sama dengan pengujian sistem dengan pemodelan *psychoacoustic* dan enkripsi AES, namun pengujian ini tidak menggunakan AES sebagai algoritma kriptografinya. Pesan berupa teks, langsung dirubah kedalam bentuk biner dan lalu disisipkan pada file audio yang berada dibawah batas threshold *psychoacoustic*.

4.4.2.1 Analisis Kriteria *Imperceptibility*
Pada pengujian dengan sistem hanya menggunakan pemodelan *psychoacoustic* tanpa menggunakan algoritma AES , dapat dilihat dari Gambar 4.5 bahwa nilai SNR sudah baik, yaitu berkisar antara 119 dB – 141 dB tidak jauh berbeda dengan sistem yang menggunakan pemodelan *psychoacoustic* ditambah dengan algoritma kriptografi AES. Hal tersebut dikarenakan, penggunaan algoritma kriptografi AES hanya bertujuan untuk mengamankan pesan, sehingga tidak berpengaruh terhadap SNR file audio. Dari Gambar 4.1 juga dapat terlihat bahwa panjang pesan sedikit mempengaruhi nilai SNR. Semakin panjang pesan yang disisipkan, maka nilai SNR menurun walaupun penurunannya tidak terlalu signifikan.

Gambar 4.5 SNR pengujian sistem yang hanya menggunakan pemodelan *psychoacoustic*

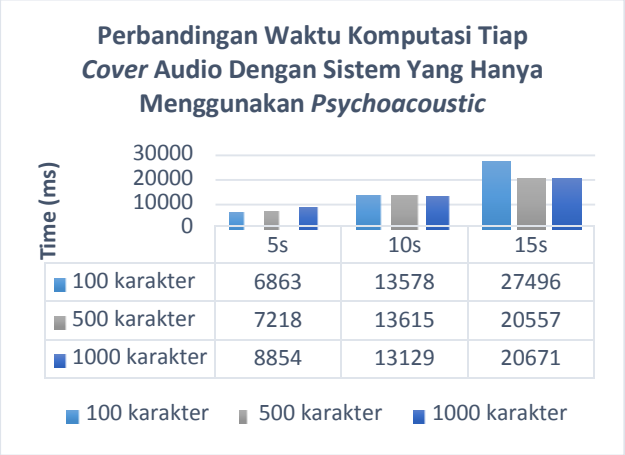
Gambar 4.6 MSE pengujian sistem yang hanya menggunakan pemodelan *psychoacoustic*

Dari Gambar 4.6 dapat dilihat nilai MSE dari pengujian dengan hanya menggunakan pemodelan *psychoacoustic* tanpa terlebih dahulu mengalami proses enkripsi AES sudah baik, pada semua durasi audio *cover*, dan dengan semua pengujian panjang pesan didapatkan nilai MSE < $1x10^{-13}$.

Dari kedua parameter yang telah disebutkan (SNR dan MSE) dapat dikatakan bahwa sistem steganografi dengan hanya menggunakan pemodelan *psychoacoustic* tanpa ditambahkan proses enkripsi dengan algoritma enkripsi AES memenuhi kriteria *imperceptibility* atau keberadaan pesan tidak dapat dipersepi atau kesamaan antara file audio *cover* dengan file audio stego sangat tinggi.

Untuk waktu komputasi, waktu dihitung dari saat sistem membaca file audio *cover* sampai proses ekstraksi dan *decoding* selesai dilakukan. Dapat dilihat pada Gambar 4.7, panjang pesan yang disisipkan tidak mempengaruhi waktu komputasi, tetapi dipengaruhi oleh panjang durasi *cover* audio. Semakin panjang durasinya, maka waktu yang dibutuhkan semakin lama, yaitu mencapai 27 detik, cenderung memiliki waktu komputasi yang lebih lama dibandingkan dengan sistem yang menggunakan pemodelan *psychoacoustic* ditambah algoritma AES, hal tersebut dikarenakan, saat tidak menggunakan AES, teks dirubah ke dalam bit biner dan sebaliknya secara manual, sehingga prosesnya cenderung lebih lama. Dari Gambar 4.7 juga terlihat

bahwa panjang pesan tidak mempengaruhi waktu komputasi. Waktu dipengaruhi oleh durasi cover audio, semakin lama cover audio, semakin banyak pula sampel yang harus diproses, maka dibutuhkan waktu yang lebih lama.

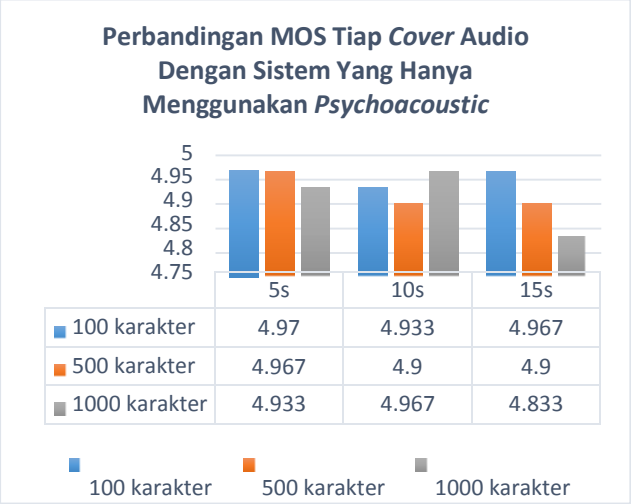


Gambar 4.7 Waktu Komputasi sistem yang hanya menggunakan pemodelan *psychoacoustic*

4.4.2.2 Analisis Kriteria *Recovery* Kriteria *recovery* pada sistem steganografi terpenuhi apabila pesan yang sudah disisipkan dapat diungkap lagi. Pada sistem dengan menggunakan pemodelan *psychoacoustic* tetapi tidak menggunakan algoritma AES sebagai algoritma kriptografinya, semua pesan, baik yang 100 karakter, 500 karakter, ataupun 1000 karakter, dengan durasi *cover* audio yang berbeda dapat ter-ekstrak dengan baik. Dengan kata lain, nilai CER atau *Character Error Rate* sama dengan 0 karena tidak ada karakter terekstrak yang error.

4.4.2.3 Analisis Kriteria *Fidelity*

Kriteria *fidelity* terpenuhi apabila kualitas audio tidak jauh berubah setelah proses penyisipan. Oleh karena itu, kriteria *fidelity* dilihat dari MOS atau *Mean Opinion Score* yang diberikan kepada 30 responden. Hasilnya, sangat baik, mayoritas dari 30 responden memberikan nilai 5 ke audio stego yang hanya menggunakan pemodelan *psychoacoustic* tanpa menggunakan kriptografi AES.



Gambar 4.8 MOS sistem yang hanya menggunakan pemodelan *psychoacoustic*

4.4.3 Pengujian Sistem Tanpa Menggunakan *Psychoacoustics* Model Tetapi Menggunakan Algoritma AES

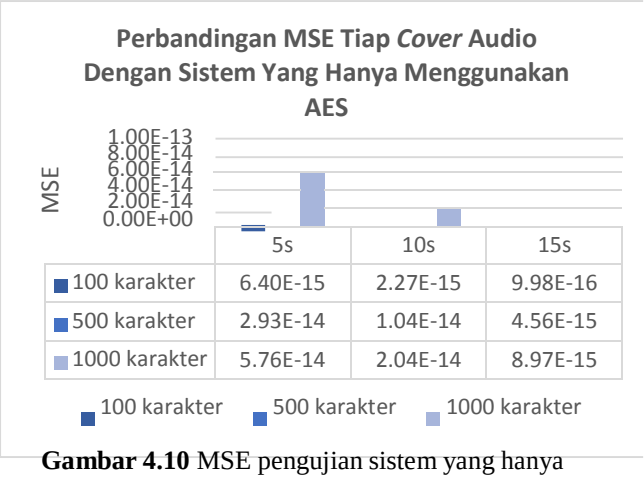
Pengujian sistem kali ini, sistem tidak menggunakan pemodelan *psychoacoustic* untuk mendapatkan threshold, namun pesan yang telah di enkripsi dengan algoritma AES, langsung disisipkan diseluruh koefisien FFT dengan cara penyisipan pesan yang sama dengan sistem yang menggunakan pemodelan *psychoacoustic*, yaitu menambah koefisien FFT dengan ±0,001 sesuai dengan bit pesan yang disisipkan, apakah bit "0" atau bit "1".

4.4.3.1 Analisis Kriteria *Imperceptibility*

Pada pengujian dengan sistem hanya menggunakan algoritma AES tanpa menggunakan pemodelan *psychoacoustic*, didapatkan hasil yang sama dengan penyisipan dengan menggunakan pemodelan *psychoacoustic* ditambah dengan algoritma AES dapat dilihat dari Gambar 4.9 bahwa nilai SNR sama dengan nilai SNR pada Gambar 4.1, hal ini dikarenakan, pemodelan *psychoacoustic* hanya digunakan untuk memilih tempat menyisipkan pesan, baik menggunakan pemodelan *psychoacoustic* maupun tidak, penyisipan dilakukan dengan cara yang sama yaitu menambah atau mengurangkan nilai FFT pada tempat penyisipan terpilih dengan 0,001. Sehingga sistem yang berbeda dengan audio cover dan jumlah pesan yang sama dapat menghasilkan SNR yang sama.

Dari Gambar 4.9 juga dapat terlihat bahwa panjang pesan sedikit mempengaruhi nilai SNR. Semakin panjang pesan yang disisipkan, maka nilai SNR menurun walaupun penurunannya tidak terlalu signifikan.

Gambar 4.9 SNR pengujian sistem yang hanya menggunakan AES tanpa pemodelan *psychoacoustic*

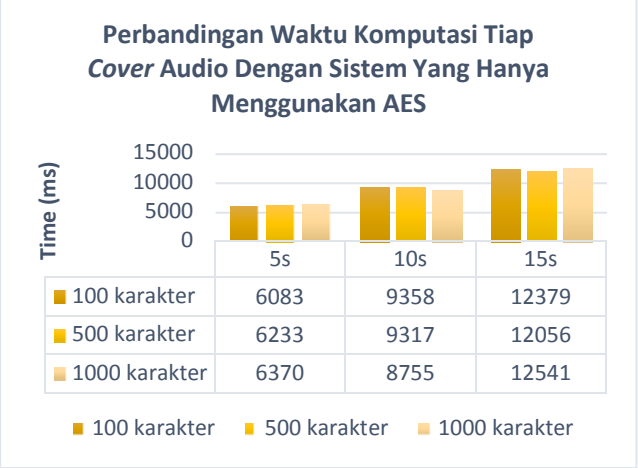


Gambar 4.10 MSE pengujian sistem yang hanya menggunakan AES tanpa pemodelan *psychoacoustic*

Dari Gambar 4.10 dapat dilihat nilai MSE dari pengujian dengan hanya menggunakan kriptografi AES tanpa menggunakan pemodelan *psychoacoustic* untuk mencari tempat penyisipan pesan sudah baik, pada semua durasi audio *cover*, dan dengan semua pengujian panjang pesan didapatkan nilai MSE < $1x10^{-13}$.

Dari kedua parameter yang telah disebutkan (SNR dan MSE) dapat dikatakan bahwa sistem steganografi dengan hanya menggunakan kriptografi AES tanpa menggunakan pemodelan *psychoacoustic* memenuhi kriteria *imperceptibility* atau keberadaan pesan tidak dapat dipersepi atau kesamaan antara file audio *cover* dengan file audio stego sangat tinggi.

Untuk waktu komputasi, berbeda dengan sistem yang menggunakan pemodelan *psychoacoustic* ditambah kriptografi AES, sistem yang hanya menggunakan kriptografi AES tanpa menggunakan pemodelan *psychoacoustic* memilik waktu komputasi yang lebih sedikit, maksimal hanya 12 detik, berbeda dengan sistem dengan menggunakan pemodelan *psychoacoustic* dan kriptografi AES yang waktu maksimalnya adalah 16 detik. Dari Gambar 4.11 juga terlihat bahwa panjang pesan tidak mempengaruhi waktu komputasi. Waktu dipengaruhi oleh durasi cover audio, semakin lama cover audio, semakin banyak pula sampel yang harus diproses, maka dibutuhkan waktu yang lebih lama.



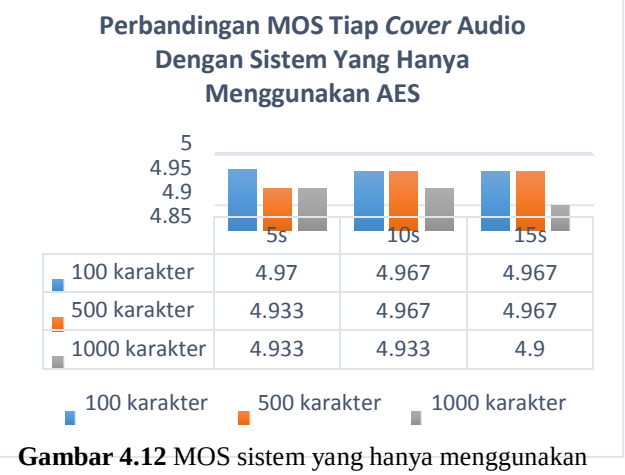
Gambar 4.11 Waktu komputasi sistem yang hanya menggunakan AES tanpa pemodelan *psychoacoustic*

4.4.3.2 Analisis Kriteria *Recovery*

Kriteria *recovery* pada sistem steganografi terpenuhi apabila pesan yang sudah disisipkan dapat diungkap lagi. Pada sistem ini yang tidak menggunakan pemodelan *psychoacoustic* tetapi menggunakan algoritma AES menghasilkan semua pesan, baik yang 100 karakter, 500 karakter, ataupun 1000 karakter, dengan durasi *cover* audio yang berbeda dapat ter-ekstrak dengan baik. Dengan kata lain, nilai CER atau *Character Error Rate* sama dengan 0 karena tidak ada karakter terekstrak yang berbeda dengan karakter yang disisipkan.

4.4.3.3 Analisis Kriteria *Fidelity*

Kriteria *fidelity* terpenuhi apabila kualitas audio tidak jauh berubah setelah proses penyisipan. Oleh karena itu, kriteria *fidelity* dilihat dari MOS atau *Mean Opinion Score* yang diberikan kepada 30 responden. Hasilnya, sangat baik. Dari Gambar 4.12 terlihat bahwa rata rata nilai MOS untuk sistem yang hanya menggunakan AES tanpa menggunakan pemodelan *psychoacoustic* melebihi nilai 4,9. Artinya, sistem yang hanya menggunakan AES tanpa pemodelan *psychoacoustic* memenuhi kriteria *fidelity*.



Gambar 4.12 MOS sistem yang hanya menggunakan AES tanpa pemodelan *psychoacoustic*

4.4.4 Pengujian Sistem Tanpa Menggunakan *Psychoacoustic* Model dan Tanpa Menggunakan Algoritma AES

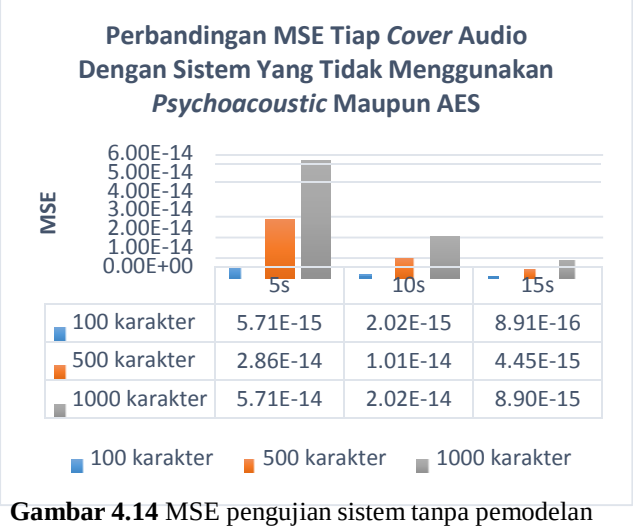
Pengujian sistem kali ini, sistem tidak menggunakan pemodelan *psychoacoustic* untuk mendapatkan threshold, juga tidak menggunakan kriptografi AES untuk mengenkripsi pesan. Jadi pesan langsung diubah ke bit biner lalu disisipkan ke koefisien FFT. Cara penyisispannya sama dengan sistem yang menggunakan pemodelan *psychoacoustic*.

4.4.4.1 Analisis Kriteria *Imperceptibility*

Pada pengujian dengan sistem yang tidak menggunakan pemodelan *psychoacoustic* maupun kriptografi AES, didapatkan hasil yang sama dengan penyisipan dengan sistem yang hanya menggunakan pemodelan *psychoacoustic* tanpa kriptografi AES. dapat dilihat dari Gambar 4.13 bahwa nilai SNR sama dengan nilai SNR pada Gambar 4.5, hal ini dikarenakan, pemodelan *psychoacoustic* hanya digunakan untuk memilih tempat menyisipkan pesan, baik menggunakan pemodelan *psychoacoustic* maupun tidak, penyisipan dilakukan dengan cara yang sama yaitu menambah atau mengurangkan nilai FFT pada tempat penyisipan terpilih dengan 0,001. Sehingga sistem yang berbeda

dengan audio cover dan jumlah pesan yang sama dapat menghasilkan SNR yang sama.
Dari Gambar 4.13 juga dapat terlihat bahwa panjang pesan mempengaruhi nilai SNR. Semakin panjang pesan yang disisipkan, maka nilai SNR menurun walaupun penurunannya tidak terlalu signifikan.

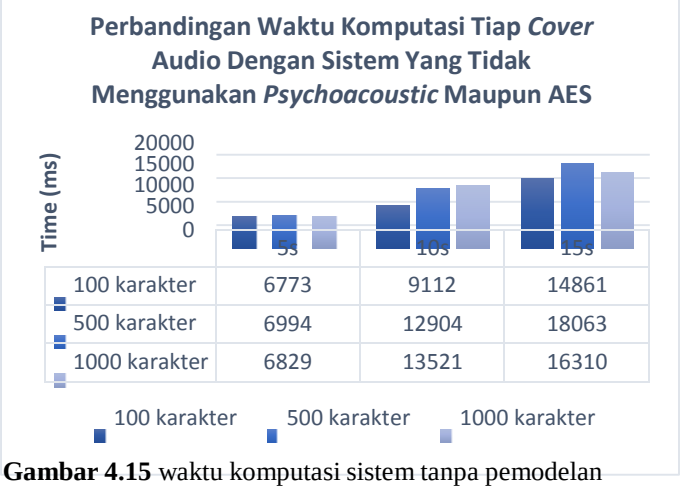
Gambar 4.13 SNR pengujian sistem tanpa pemodelan *psychoacoustic* dan tanpa AES



Gambar 4.14 MSE pengujian sistem tanpa pemodelan *psychoacoustic* dan tanpa AES Dari Gambar 4.14 dapat dilihat nilai MSE dari pengujian sistem tanpa menggunakan pemodelan *psychoacoustic* untuk mencari tempat penyisipan pesan dan tidak menggunakan kriptografo AES sebagai pengaman pesan sudah baik, pada semua durasi audio *cover*, dan dengan semua pengujian panjang pesan didapatkan nilai MSE < $1x10^{-13}$.

Dari kedua parameter yang telah disebutkan (SNR dan MSE) dapat dikatakan bahwa sistem steganografi tanpa menggunakan pemodelan *psychoacoustic* dan tidak menggunakan kriptogrfai AES memenuhi kriteria *imperceptibility* atau keberadaan pesan tidak dapat dipersepi atau kesamaan antara file audio *cover* dengan file audio stego sangat tinggi.

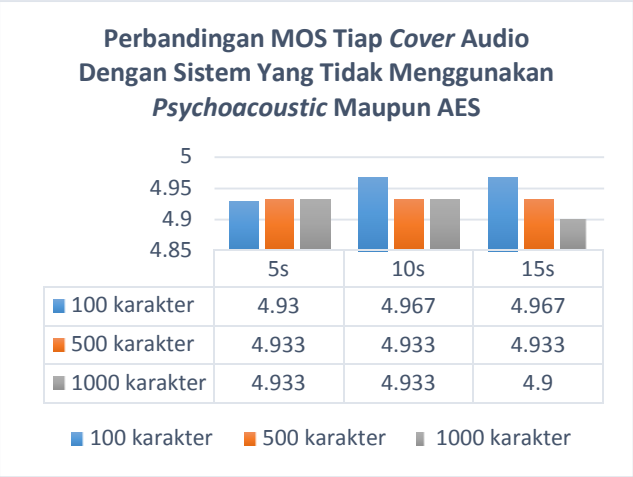
Untuk waktu komputasi, berbeda dengan sistem yang menggunakan pemodelan *psychoacoustic* tanpa kriptografi AES yang waktu komputasinya mencapai maksimal 27 detik (Gambar 4.7), waktu yang dibutuhkan sistem dari membaca file audio sampai mendecode pesan pada sistem yang tidak menggunakan pemodelan *psychoacoustic* juga tidak menggunakan kriptografi AES hanya maksimal 18 detik (Gambar 4.15). Waktu komputasi ini juga berbeda dengan sistem yang hanya menggunakan kriptografi AES tanpa pemodelan *psychoacoustic* yang memiliki waktu komputasi 12 detik (Gambar 4.11). Sistem tanpa menggunakan pemodelan *psychoacoustic* cenderung memiliki waktu komputasi yang lebih cepat dibandingkan dengan yang menggunakan pemodelan *psychoacoustic*. Dan sistem yang tidak menggunakan kriptografi AES cenderung lebih lama waktu komputasinya dibandingkan dengan sistem yang menggunakan AES, karena proses perubahan teks menjadi bit biner dan sebaliknya dilakukan sistem secara manual, jadi membutuhkan waktu yang lebih lama dibanding dengan proses enkripsi dan dekripsi AES.
Dari Gambar 4.15 juga terlihat bahwa panjang pesan tidak mempengaruhi waktu komputasi. Waktu dipengaruhi oleh durasi cover audio, semakin lama cover audio, semakin banyak pula sampel yang harus diproses, maka dibutuhkan waktu yang lebih lama.



Gambar 4.15 waktu komputasi sistem tanpa pemodelan *psychoacoustic* dan tanpa AES

4.4.4.2 Analisis kriteria *Recovery* Kriteria *recovery* pada sistem steganografi terpenuhi apabila pesan yang sudah disisipkan dapat diungkap lagi.
Pada sistem ini yang tidak menggunakan pemodelan *psychoacoustic* dan tidak menggunakan algoritma AES, semua pesan, baik yang 100 karakter, 500 karakter, ataupun 1000 karakter, dengan durasi *cover* audio yang berbeda dapat ter-ekstrak dengan baik. Dengan kata lain, nilai CER atau *Character Error Rate* sama dengan 0 karena tidak ada karakter terekstrak yang salah atau berbeda dengan karakter yang disisipkan.

4.4.4.3 Analisis Kriteria *Fidelity*
Kriteria *fidelity* terpenuhi apabila kualitas audio tidak jauh berubah setelah proses penyisipan. Oleh karena itu, kriteria *fidelity* dilihat dari MOS atau *Mean Opinion Score* yang diberikan kepada 30 responden. Hasilnya, juga baik. Mayoritas responden memberikan nilai 5 ke audio stego yang dihasilkan sistem. Sehingga nilai rata rata MOS melebihi nilai 4,9. Yang artinya sistem juga memenuhi kriteria *fidelity*.



Gambar 4.16 MOS untuk sistem tanpa pemodelan *psychoacoustic* dan tanpa AES

4.4.5 Analisis Kriteria *Robustness*

Kriteria steganografi yang lainnya yaitu *robustness* yang artinya pesan rahasia yang disisipkan relatif tidak rusak jika stego mengalami proses pengolahan sinyal. Kriteria *robustness* tidaklah wajib terpenuhi, karena pada dasarnya, tujuan utama steganografi hanyalah menyembunyikan pesan tanpa menimbulkan kecurigaan pihak yang tidak berkepentingan (pihak lain tidak menyadari keberadaan pesan rahasia)

Untuk mengetahui ketahanan sistem terhadap performansi *robustness* ini maka audio stego diuji dengan berbagai pengolahan sinyal (Kompresi ke bentuk MP3, cropping, resampling, dan menambahkan noise AWGN).

Untuk analisis *robustness*, digunakan file audio 5 detik, 10 detik, dan 15 detik dengan panjang pesan 100 karakter, 500 karakter, dan 1000 karakter, yang sebelumnya telah di sisipkan dengan 4 skenario pengujian yang telah dijelaskan sebelumnya. Jadi pengolahan sinyal dilakukan terhadap 36 file audio stego, dan total file yang digunakan untuk analisis *robustness* ini adalah 144 file

4.4.5.1 *Robustness* Terhadap Kompresi MP3

Hasil pengujian menunjukkan bahwa, sistem steganografi tetap memenuhi kriteria *imperceptibility* yaitu keberadaan pesan tidak dapat dipersepsi, memenuhi kriteria *fidelity* karena kualitas audio steganografi masih baik. Namun, sistem tidak memenuhi kriteria *recovery* atau pesan dapat diekstrak kembali, karena proses kompresi WAV ke MP3 adalah menghilangkan komponen yang tidak sensitif oleh telinga manusia. Disimpulkan bahwa sistem tidak memenuhi kriteria *robustness* terhadap kompresi MP3.

4.4.5.2 *Robustness* Terhadap *Cropping*

Pengujian dilakukan dengan memotong file audio sebesar 1 detik di akhir file menunjukkan bahwa, sistem steganografi tetap memenuhi kriteria *imperceptibility* yaitu keberadaan pesan tidak dapat dipersepsi, memenuhi kriteria *fidelity* karena kualitas audio steganografi masih baik walaupun sudah dipotong di bagian akhir. Namun, sistem tidak memenuhi kriteria *recovery* atau pesan dapat diekstrak kembali, karena setelah di cropping, ukuran sampel antara file audio asli dan file stego yang sudah di cropping berbeda, sehingga tidak bisa dilakukan perbandingan dan pengekstrakan pesan. Disimpulkan bahwa sistem tidak memenuhi kriteria *robustness* terhadap cropping.

4.4.5.3 *Robustness* Terhadap *Resampling*

Audio diuji ketahanannya terhadap proses *down sampling* (*resampling*) dari sample rate asli sebesar 44100 Hz diturunkan menjadi 22050 Hz. Pengujian menunjukkan bahwa, sistem steganografi tetap memenuhi kriteria *imperceptibility* yaitu keberadaan pesan tidak dapat dipersepsi, memenuhi kriteria *fidelity* karena kualitas audio steganografi masih baik walaupun sudah dirubah frekuensi sampling nya. Namun, sistem tidak memenuhi kriteria *recovery* atau pesan tidak dapat diekstrak kembali, karena setelah di resampling, ukuran sampel antara file audio asli dan file stego berbeda, sehingga tidak bisa dilakukan perbandingan dan pengekstrakan pesan. Disimpulkan bahwa sistem tidak memenuhi kriteria *robustness* terhadap cropping.

4.4.5.4 *Robustness* Terhadap Pemberian Noise AWGN

Pada Tugas Akhir ini ketahanan sistem diuji dengan pemberian 3 jenis noise AWGN. Yaitu noise AWGN dengan SNR 50, SNR 30, dan SNR 10. Pengujian dilakukan pada durasi audio 5 detik, 10 detik, 100 detik. Dan dengan panjang pesan 100, 500 dan 1000 karakter. Dan menggunakan semua kombinasi sistem penyisipan. Hasilnya untuk semua file stego tidak jauh berbeda. Ketika diberi AWGN dengan SNR 10, ke 36 file audio stego tetap memenuhi kriteria *imperceptibility* yaitu file audio tidak menimbulkan kecurigaan kalau terdapat pesan rahasia yang tersisip didalamnya. Seluruh file audio yang diberi AWGN dengan SNR 10 tidak memenuhi kriteria *fidelity* karena kualitas file audio stego menurun drastis. Dapat dilihat pada tabel MOS yang terlampir pada lampiran C. mayoritas responden memberikan nilai 1 ke file audio yang diberi AWGN dengan SNR 10. Kriteria *recovery* juga tidak terpenuhi atau pesan tidak dapat terekstrak dengan benar (CER mencapai maksimal). Sistem pengekstrakan yang hanya menghitung selisih antara sampel audio cover dengan sampel audio stego menyebabkan sistem menjadi sangat sensitif terhadap perubahan sampel dari file audio stego, sehingga pesan tidak dapat terekstrak.

Berikutnya, pengujian dengan pemberian AWGN dengan SNR 30. Hasilnya, ke 36 file audio stego yang diujikan, memenuhi kriteria *imperceptibility* karena pada file audio tidak dicurigai terdapat pesan rahasia. Namun seluruh file audio yang diujikan tidak memenuhi kriteria *fidelity* karena kualitas file audio stego menurun. Terlihat dari MOS yang diberikan 30 responden menghasilkan MOS dengan nilai mayoritas 2 – 3. Kriteria *recovery* juga tidak terpenuhi karena pesan tidak terkestrak dengan benar (nilai CER mencapai maksimal).

Selanjutnya pengujian dengan pemberian AWGN dengan SNR 50. Hasilnya, seluruh file audio stego yang diujikan dengan pemberian AWGN dengan SNR 50 memenuhi kriteria *imperceptibility* karena keberadaan pesan rahasia tidak dapat dipersepsi oleh indera manusia. Kriteria *fidelity* juga terpenuhi karena kualitas file stego tidak berubah jauh dari file audio cover asli. Terlihat dari MOS yang rata-ratanya bernilai 4. Namun,

setelah diberi AWGN SNR 50 tetap tidak memenuhi kriteria *recovery* atau pesan tidak dapat terekstrak dengan benar. Pesan yang berupa teks yang rawan terhadap perubahan bit juga menjadi salah satu alasan pesan tidak dapat terekstrak dengan benar.

4.4.6 Analisis Kriptografi

Sampai saat ini, AES merupakan algoritma kriptografi yang paling banyak digunakan dan cukup tinggi tingkat keamanannya. Jika kunci yang digunakan pada proses AES dapat disembunyikan secara aman, maka akan sangat sulit untuk mengambil pesan rahasia yang telah disisipkan. Pengujian AES dapat dilakukan dengan cara *Brute Force Attack*, yaitu dengan mencoba semua kemungkinan kunci yang ada, dimana dalam Tugas Akhir ini menggunakan AES-128 dengan panjang kunci 16 karakter atau 128 bit. Setiap bitnya mempunyai peluang yang sama antara 0 dan 1, sehingga total kemungkinan kuncinya adalah 2^{128} atau jika dituliskan dalam bilangan hexadesimal adalah 16^{32}.

Perhitungan waktu komputasi untuk memecahkan kunci AES dapat dihitung sebagai berikut[5] :

$$\text{[illegible]} = \frac{16^{32}}{2\text{[illegible]}} = \frac{16^{32}}{2.10^{9}\ \text{[illegible]}}$$

$$= 1{,}7014 \times 10^{29}\ \text{[illegible]}$$
$$= 4{,}726 \times 10^{25}\ \text{[illegible]}$$
$$= 1{,}969 \times 10^{24}\ h\text{[illegible]}$$
$$= 6{,}564 \times 10^{22}\ \text{[illegible]}$$
$$= \text{[illegible]}$$

Oleh karena itu, sampai saat ini AES masih menjadi salah satu algoritma kriptografi yang paling aman dan populer digunakan untuk menjaga keamanan data yang bersifat sangat rahasia, baik di bidang pemerintahan, perusahaan maupun pertukaran data personal.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Rancangan sistem audio steganografi yang telah disimulasikan terbukti mampu bekerja dengan baik
2. Proses ekstraksi pesan masih membutuhkan cover asli (blind steganography)
3. Sistem memiliki SNR yang baik yaitu > 110 dB dan MSE < $1x10^{-13}$
4. Ukuran pesan yang akan disisipkan berbanding lurus dengan ukuran cover, jika ingin menyisipkan pesan yang lebih banyak, dibutuhkan audio cover yang lebih besar
5. Proses penyisipan sistem dengan pemodelan psychoacoustic dan enkripsi AES membutuhkan waktu lebih lama daripada tanpa pemodelan psychoacoustic dan tanpa enkripsi AES
6. Jumlah pesan yang dapat disisipkan pada sistem dengan pemodelan psychoacoustic lebih sedikit dibandingkan pada sistem yang tidak menggunakan pemodelan psychoacoustic
7. Sistem tidak cukup baik menangani serangan berupa pengolahan sinyal maupun pemberian noise AWGN, terlihat dari pesan berupa teks yang disisipkan ke file audio yang tidak terekstrak dengan benar
8. Sistem sangat rentan terhadap perubahan bit sehingga performansinya kurang maksimal dan pesan tidak dapat diekstrak dengan benar
9. Metode AES memiliki tingkat keamanan yang tinggi, dengan cara brute force attack dibutuhkan waktu $5.47x10^{21}$ tahun untuk dapat memecahkan kunci AES

5.2 Saran

Adapun saran untuk pengembangan penelitian selanjutnya adalah:

1. Sistem bisa disimulasikan dengan jenis pesan yang lain, misal audio atau gambar
2. Sistem bisa dijalankan secara *real-time*
3. Sistem bisa dibuat kedalam aplikasi android
4. Dicobakan pengujian *robustness* terhadap proses *steganalysis*
5. Menggunakan teknik deteksi dan koreksi eror untuk meminimalkan kesalahan data saat pengestrakan, misal BCH Code
6. Menggunakan algoritma AES-192 atau AES-256 yang mempunyai kunci yang lebih panjang sehingga meningkatkan keamanan pesan

REFERENSI

[1] R. Munir, *Kriptografi*. Penerbit Informatika, 2006.

[2] K. R. Rao, D. N. Kim, and J. J. Hwang, *Fast Fourier Transform - Algorithms and Applications: Algorithms and Applications Signals and Communication Technology*. Springer Science & Business Media, 2011.

[3] H. Fastl and E. Zwicker, *Psychoacoustics: Facts and Models*, 3rd ed. Springer Series in Information Sciences, 2007.

[4] N. R. Wagner, "The Laws of Cryptography with Java Code," 2003.

[5] F. Information, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001.

[6] L. Mutmainnah, "Analisis Pengamanan Data dengan Steganografi Audio Berbasis Teknik Psychoacoustic," 2012.

[7] S. Nurjamillah, "Simulasi dan Analisis Steganografi Audio Dengan Convolutional Code dan Pemodelan Psychoacoustic," 2013

[8] S. Zmudzinski and M. Steinebach, "Psycho-acoustic Model-based Message Authentication Coding for Audio Data," pp. 75–84, 2008.

[9] C. Jin-lun, "Implementation and Optimization of Psychoacoustic Models based on DSP," 2010.

[10] "Microsoft WAVE soundfile format." [Online]. Available: https://ccrma.stanford.edu/courses/422/projects/WaveFormat/. [Accessed: 25-Aug-2014].

[11] "File:ASCII-Table-wide.svg - Wikimedia Commons." [Online]. Available: http://commons.wikimedia.org/wiki/File:ASCII-Table-wide.svg. [Accessed: 25-Aug-2014].

[12] "WavReader.java." [Online]. Available: http://webpages.cs.luc.edu/~pld/courses/346/sum07/java/WavReader.java. [Accessed: 25-Aug-2014].
[13] B. K. Kim, "Ch 8. Analog Interface."
[14] G. L. P. License, "JTransforms." Free Software Foundation, Inc, Boston, 1999.
[15] "Session 2 Lecture Notes for First Course in Java." [Online]. Available: http://www.write-technical.com/126581/session2/session2.htm. [Accessed: 25-Aug-2014].
[16] B. Raharjo, I. Heryanto, and A. Haryono, *Mudah Belajar JAVA*. Bandung: Penerbit Informatika, 2007.