STEGANOGRAFI VIDEO MENGGUNAKAN METODE *DISCRETE WAVELET TRANSFORM* PADA FRAME YANG TERPILIH BERDASARKAN DETEKSI SILENCE DENGAN METODE *ZERO CROSSING RATE*

Video Steganography Using Discrete Wavelet Transform on Selected Frame with Silence Detection Based on Zero Crossing Rate

Alifia Fathur Rizkiyah [1], Dr.Ir.Bambang Hidayat,DEA[2], I Nyoman Apraz Ramatryana, S.T,M.T [3]
Prodi Teknik Telekomunikasi, Fakultas Teknik Elektro,Universitas Telkom
alifiafr@gmail.com[1], bhidayat@telkomuniversity.ac.id[2], ramatryana@gmail.com[3]

Abstrak

Penggunaan media internet untuk melakukan pertukaran informasi yang telah berkembang menyebabkan kekhawatiran terkait keamanan dan kerahasiaan data digital yang dikirimkan. Untuk mengamankan data yang dikirimkan melalui media internet, diperlukan suatu teknik agar keamanan dan kerahasiaan informasi tersebut terjamin, salah satunya yaitu Steganografi. Pada penelitian ini, dirancang sebuah sistem steganografi dimana pesan yang disisipkan berupa file teks berformat *.*txt* dan video dengan format *.avi sebagai cover. Pesan informasi disisipkan pada *frame* video berdasarkan deteksi *silence* menggunakan Zero Crossing Rate, dengan mengukur parameter seperti: PSNR, MSE, BER, dan MOS. Dengan menggunakan metode penyisipan *Discrete Wavelet Transform* didapatkan hasil *Peak Signal to Noise Ratio* (PSNR) yang baik. Hasil PSNR terbesar yaitu 64.2775 dB dan nilai MSE terkecil sebesar 0,0243. Waktu komputasi terbesar yang didapat pada proses penyisipan adalah 1.68994 detik, sedangkan pada proses ekstraksi adalah 0,42312 detik. Hasil *Mean Opinion Score* (MOS) yang didapatkan memiliki nilai rata-rata total sebesar 3.8 yang berarti kualitas video tersisipi dengan baik. BER terbesar yang dihasilkan yaitu sebesar 44.2842 saat *mean* = 0.01 dan variansi = 0.0006.

Kata kunci : Steganografi Video, *Zero Crossing Rate*, Deteksi *Silence*, *Discrete Wavelet Transform*

Abstract

*Usage of internet to exchange information that have been developed cause worries about security and privacy of digital data being transmitted. To secure the data sent via internet, a technique to guarantee the security and privacy is needed. One of the method is called Steganography. In this final assignment, a Steganography system is designed to embed *.txt formatted file text to *.avi formatted video. The file text is secret message, while the video is used as cover. The secret message is embedded by DWT method to video frames based on silence detection with ZCR method. The success rate of Video Steganography carried out by measuring several paramaeters, such as: PSNR, MSE, BER, and MOS. PSNR biggest result obtained is 64.2775 dB and MSE lowest result is 0,0243. Longest computational time in embedding process is 1.68994 second, while longest computational time in extraction process is 0.42312 second. MOS result have an average of 3.8, meaning that the quality of the video after embedded with image is good. The resulting BER is equal to 44.2842 when the mean = 0.01 and variance = 0.0006.*

Keywords : Video Steganography, Zero Crossing Rate, Silence Detection, Discrete Wavelet Transform

1. Pendahuluan

Seiring dengan kemajuan teknologi, pertukaran informasi melalui media digital semakin sering dilakukan, dan menjadi aktivitas kebanyakan orang sehari-hari. Namun, tidak dapat dipungkiri bahwa kemajuan teknologi dan informasi selain memiliki banyak keuntungan, juga terdapat sisi negatif, misalnya seperti pencurian konten atau data digital yang dikirim melalui internet dapat disalahgunakan oleh orang yang tidak bertanggung jawab[9]. Penggunaan media internet untuk melakukan pertukaran informasi yang telah berkembang menyebabkan kekhawatiran terkait keamanan dan kerahasiaan data digital tersebut. Sehingga diperlukan suatu teknik untuk dapat bertukar informasi tanpa ada orang lain yang mengetahui kecuali orang yang bersangkutan. Teknik ini dinamakan Steganografi. Pada Tugas Akhir ini, dilakukan analisis dan simulasi teknik steganografi pada video, karena video merupakan gambar berjalan yang terdiri dari beberapa *frame* yang mampu menampung kapasitas yang lebih besar daripada gambar. Video menggunakan format **.avi* yang tidak terkompresi dengan penyisipannya menggunakan metode *DWT*. Serta dilakukan dengan pemilihan *frame* pada video berdasarkan deteksi *silence* berbasis *ZCR*. Data rahasia yang akan disisipkan pada video berupa teks dengan format *.txt.* Pada proses penyisipan teks, dilakukan dengan menentukan daerah *silence* pada sinyal audio, yang merupakan titik acuan dalam melakukan penyisipan pesan rahasia pada *frame* video. Kemudian teks disisipkan pada *frame* video saat daerah *silence* terdeteksi. Performansi sistem diuji berdasarkan perhitungan *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), *Bit Error Rate* (BER) dan *Mean Opinion Score* (MOS). Disamping itu, tingkat ketahanan stego-video ini diuji dengan *Gaussian Noise.*

2. Dasar Teori

A. Steganografi [1]

Steganografi berasal dari bahasa yunani yaitu *steganos* yang berarti tersembunyi atau menyembunyikan, sedangkan *graphy* berarti tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Teknik steganografi digunakan untuk menyembunyikan pesan rahasia ke dalam pesan lain. Pada umumnya terdapat dua proses di dalam steganografi, yaitu proses penyisipan pesan rahasia dan proses ekstraksi pesan untuk mendapatkan pesan rahasia dari dalam pesan tersebut.

Steganografi digital menggunakan *file-file* multimedia sebagai *cover*, misalnya citra, suara, teks, dan video. *Secret message* yang disembunyikan juga dapat berupa citra, suara, teks, atau video. *Stego Object* adalah *cover* yang telah disisipkan pesan rahasia[6].

B. Audio/Video Interleave (AVI) [2]

Audio Video Interleave (AVI) adalah format file penyimpan data- data multimedia. AVI diperkenalkan pertama kali oleh Microsoft pada bulan November 1992 sebagai bagian dari teknlogi video dalam platform Microsoft Windows. Format AVI merupakan salah satu format video tertua yang diperkenalkan Microsoft sejak dilirisnya Windows 3.1. Format file AVI dapat menyimpan data video dan audio dalam satu file yang memungkinkan memainkan kedua jenis data secara bersamaan. Dalam Tugas Akhir ini memakai avi jenis AVI *uncompressed* atau disebut juga AVI *full frames*. Suatu file multimedia dengan format AVI *uncompressed* memiliki informasi frame-frame gambar yang disimpan dengan menggunakan format Bitmap tiga *layer* warna 8 bit, jadi untuk satu *pixel* data *bitmap* akan disimpan dalam wadah berukuran 24 bit.

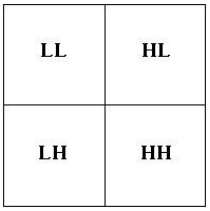
C. Teks Format (.txt) [3]

Format data teks merupakan format teks yang digunakan untuk menyimpan huruf, angka, karakter kontrol (tabulasi, pindah baris, dan sebagainya) atau simbol-simbol lain yang biasa digunakan dalam tulisan seperti titik, koma, tanda petik, dan sebagainya. Satu huruf, angka, karakter kontrol atau simbol pada arsip teks memakan tempat satu *byte*. Berbeda dengan jenis teks terformat yang satu huruf saja dapat memakan tempat beberapa *byte* untuk menyimpan format dari huruf tersebut seperti font, ukuran, tebal atau tidak dan sebagainya. Kelebihan dari format data teks ini adalah ukuran datanya yang kecil karena tidak adanya fitur untuk memformat tampilan teks. Saat ini perangkat lunak yang paling banyak digunakan untuk memanipulasi format data ini adalah Notepad.

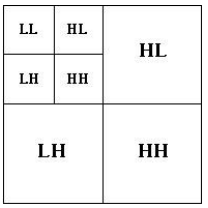
D. Discrete Wavelet Transform (DWT) [5]

Prinsip dasar dari DWT adalah bagaimana mendapatkan representasi waktu dan skala dari sebuah sinyal menggunakan teknik pemfilteran digital dan operasi subsampling. Implementasi DWT dapat dilakukan dengan cara melewatkan sinyal frekuensi rendah dan frekuensi tinggi.

Proses dekomposisi pada sebuah citra akan menghasilkan empat subbidang citra dari citra asli, dimana keempat subbidang citra tersebut berada dalam kawasan wavelet. Keempat subbidang citra tersebut adalah *Low-Low (LL), Low-High (LH), High-Low (HL)* dan *High-High (HH).*



Gambar 1. DWT Level 1 [6]



Gambar 2. DWT Level 2

Sebagian besar informasi citra pada subband LL, sehingga untuk melakukan dekomposisi tingkat dua akan dilakukan pada subband tersebut. Pada dekomposisi tingkat dua akan dihasilkan empat subband baru untuk menggantikan subband LL. Empat subband yang dihasilkan adalah LL2, HL2, LH2, dan HH2.

Bila citra asli *f* dengan M x N pixel didekomposisi menjadi empat subband LL, HL, LH, dan HH. Dengan transformasi wavelet menggunakan filter Haar (Daubechies orde 1), secara matematis dihasilkan dengan persamaan berikut:

$$\text{[illegible]} = \frac{1}{4}\sum^{1} \text{[illegible]}(2\text{[illegible]} + \text{[illegible]}2\text{[illegible]} + \text{[illegible]} \quad (1)$$

$$\text{[illegible]} = \frac{1}{4} \text{[illegible]}(2\text{[illegible]} + \text{[illegible]}2\text{[illegible]} - \frac{1}{4}\sum^{1} \text{[illegible]}(2\text{[illegible]} + \text{[illegible]}2\text{[illegible]} + 1) \quad (2)$$

$$H\text{[illegible]} = \frac{1}{4}\sum^{1} \text{[illegible]}(2\text{[illegible]}2\text{[illegible]} + \text{[illegible]}) - \frac{1}{4}\sum^{1} \text{[illegible]}(2\text{[illegible]} + 1,2\text{[illegible]} + \text{[illegible]}) \quad (3)$$

$$H\text{[illegible]} = \frac{1}{4}\{\text{[illegible]}(2\text{[illegible]}2\text{[illegible]} + \text{[illegible]}(2\text{[illegible]} + 1,2\text{[illegible]} + 1) - \text{[illegible]}(2\text{[illegible]} + 1,2\text{[illegible]} - \text{[illegible]}(2\text{[illegible]}2\text{[illegible]} + \text{[illegible]})\} \quad (4)$$

E. Zero Crossing Rate (ZCR) [4]

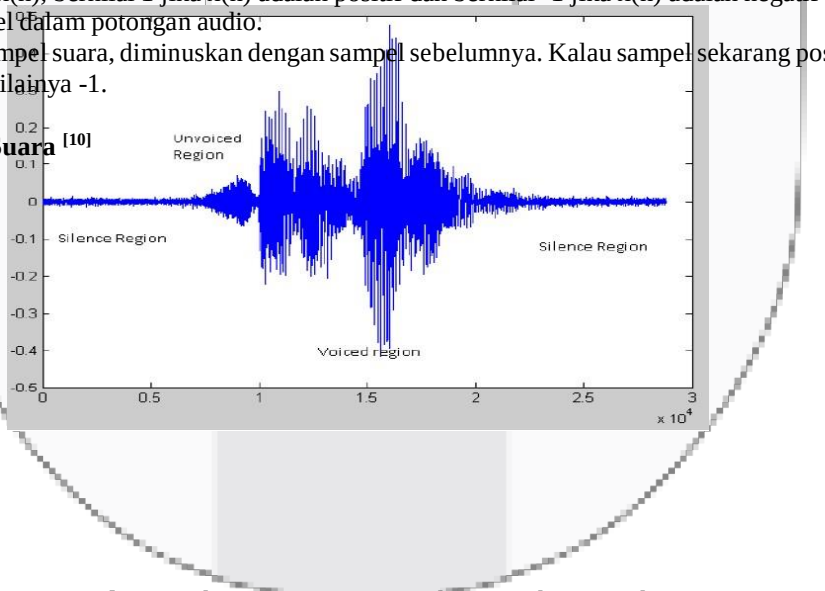
Zero Crossing Rate (ZCR) mengindikasikan frekuensi dengan tanda pada saat berganti signal amplitudo. Jumlah dari ini mutlak dari tanda sampel yang ke-n dikurangi tanda sampel yang ke (n-1) di bagi dengan 2 kali banyaknya sampel, di mana tanda sampel yang ke n, akan bernilai 1, jika sampelnya positif. Minus 1, jika sampelnya negatif.

$$Z\text{[illegible]} = \frac{\sum \text{[illegible]}=1 \left|\text{[illegible]}(\text{[illegible]}) - \text{[illegible]}(\text{[illegible]}-1)\right|}{2\text{[illegible]}} \quad (5)$$

Sgn x(n) = Tanda dari x(n), bernilai 1 jika x(n) adalah positif dan bernilai -1 jika x(n) adalah negatif
N = Jumlah total sampel dalam potongan audio.

Untuk melihat 1 sampel suara, diminuskan dengan sampel sebelumnya. Kalau sampel sekarang positif, nilainya 1, sedangkan negatif, nilainya -1.

E. Klasifikasi Sinyal Suara [10]



Gambar 3. *S*ilence region, unvoiced region, dan voiced region

Pengklasifikasikan bagian-bagian atau komponen sinyal ucapan secara sederhana dibagi menjadi tiga kondisi yang berbeda, yaitu:

1. ***Silence*** : sinyal pada saat tidak terjadi proses produksi suara ucapan, dan sinyal yang diterima oleh pendengar dianggap sebagai bising latar belakang.
2. ***Unvoiced***, keadaan pada saat *vocal cord* tidak melakukan vibrasi, sehingga suara yang dihasilkan bersifat tidak periodik atau bersifat random;
3. ***Voiced***, keadaan pada saat terjadinya vibrasi pada *vocal cord*, sehingga menghasilkan suara yang bersifat kuasi periodik.

F. Parameter Pengujian

1. ***Mean Square Error*** **(MSE)**

Mean Square Error adalah parameter yang digunakan untuk menganalisis performansi sistem dengan melihat hasil kualitas *stego-video*. Dalam metode MSE ini dilakukan dengan cara mencari rata-rata nilai *error* antara citra *cover* dengan citra *stego*. Semakin besar nilai MSE yang didapat maka kualitas *stego-video* semakin buruk. Persamaan matematis yang digunakan adalah sebagai berikut :

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[I(x,y) - I'(x,y)]^2}{MN} \quad (6)$$

dimana : MSE = Mean Square Error(dB) I(x,y) = Nilai piksel dari citra cover
M = Panjang citra stego (dalam piksel) I'(x,y) = Nilai piksel dari citra stego
N = Lebar citra stego (dalam piksel)

2. *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio (PSNR) merupakan tinjauan kualitas video secara objektif. PSNR adalah nilai tertinggi dari perbandingan daya sinyal dengan noise. Kualitas *stego-image* dapat dikatakan baik jika nilai PSNR-nya besar. Berikut ini formula PSNR :

$$PSNR = 10 \log_{10}\left[\frac{MAXi^2}{MSE}\right] \quad (7)$$

dimana :
PSNR = Peak Signal To Noise Ratio (dB)
MAXi = 255, nilai intensitas maksimum dari pixel citra yang digunakan.

Semakin besar nilai PSNR yang didapatkan maka kualitas *stego-video* yang dihasilkan semakin bagus atau dengan kata lain semakin kecil nilai MSE maka kualitas *stego-video* yang dihasilkan semakin bagus.

3. *Bit Error Rate* (BER)

BER (*Bit Error Rate*) merupakan parameter pengujian dimana bagus tidaknya sistem steganografi dan ekstraksi yang telah dibuat didasarkan pada benar atau tidaknya sistem dalam mengekstraksi bit-bit pesan yang telah dikirimkan. Parameter BER ini sangat menentukan bagus tidaknya sistem steganografi yang telah dibuat karena mengingat dari tujuan steganografi itu sendiri adalah menyampaikan pesan. Sehingga walaupun penyampaian pesan secara rahasia atau sembunyi-sembunyi, pesan tetap harus tersampaikan ke penerima. Tersampaikannya pesan ke penerima merupakan salah satu kriteria steganografi, yakni *recovery*. Adapun cara penghitungan BER, yaitu :

$$BER = \frac{\sum Bit\ error}{\sum Bit\ pesan} \quad (8)$$

4. *Character Error Rate* (CER)

CER (Character Error Rate) adalah perbandingan jumlah karakter yang *error* dengan total karakter. CER merupakan parameter pengujian yang digunakan untuk melihat kualitas pesan yang disisipkan. Penggunaan parameter BER tidak cukup apabila tidak disertakan dengan pengujian terhadap parameter CER. Hal ini dikarenakan, nilai BER yang rendah belum berarti menghasilkan nilai CER yang rendah juga. Berikut ini rumus untuk menghitung CER.

$$CER = \frac{\sum Karakter\ error}{\sum Karakter\ pesan} \quad (9)$$

5. Waktu komputasi

Waktu Komputasi adalah waktu yang dibutuhkan sistem untuk melakukan suatu proses. Waktu komputasi sistem dihitung dari mulainya proses hingga proses tersebut selesai.

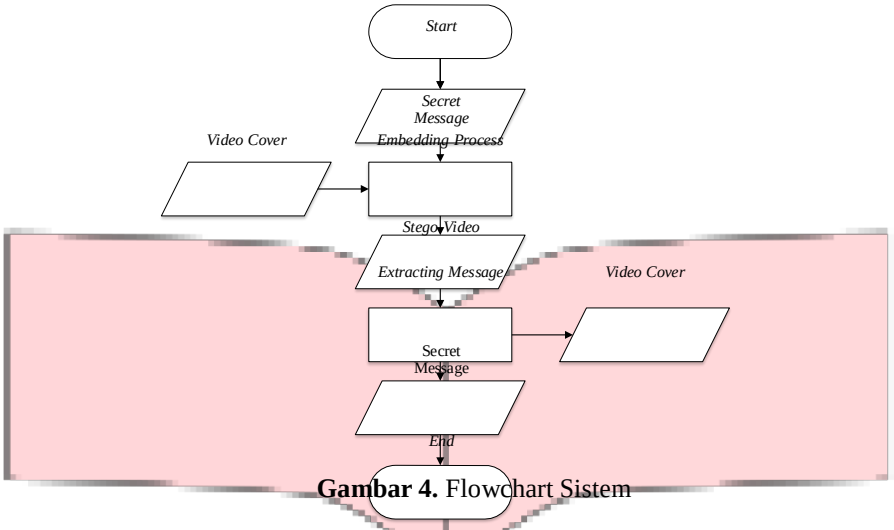
6. ***Mean Opinion Score* (MOS)**

Mean Opinion Score merupakan rekomendasi ITU P.800 yang digunakan untuk mengukur kinerja dari suatu komunikasi multimedia melalui jaringan berdasarkan pandangan dari responden. responden akan memberikan penilaian dengan range angka 1-5 dimana, angka 1 berarti kualitas yang amat buruk dan angka 5 adalah kualitas yang sangat baik.

Tabel 1. Kriteria Pengujian MOS

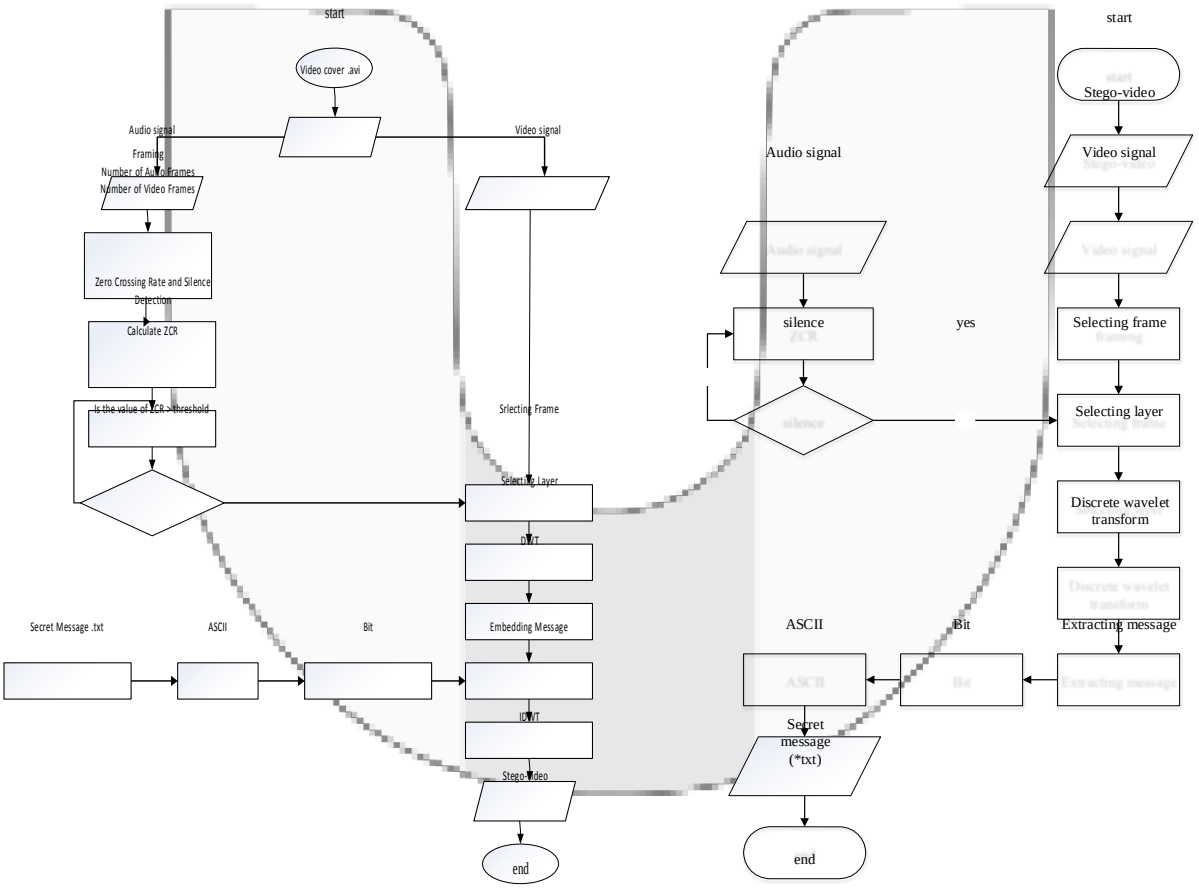
Indeks	Kategori	Keterangan
5	Sangat baik (*excellent*)	Video yang diamati mempunyai kualitas sangat baik, hampir serupa dengan video aslinya
4	Baik (*good*)	Video yang diamati mempunyai kualitas yang cukup baik, tanpa gangguan-gangguan yang cukup berarti
3	Cukup (*fair*)	Video yang diamati mempunyai kualitas yang cukup baik dengan gangguan-gangguan atau perubahan yang berarti
2	Buruk (*bad*)	Video yang diamati mempunyai kualitas sangat buruk tetapi masih dapat terlihat dengan gangguan yang sangat jelas
1	Sangat buruk (*worst*)	Video yang diamati sangat buruk sekali sehingga tidak dapat diamati lagi

3. Blok Diagram Sistem .



Gambar 4. Flowchart Sistem

Sistem yang dirancang pada tugas akhir ini adalah sistem steganografi dengan video sebagai *cover*. Penyisipan dilakukan di sisi pengirim dengan menyisipkan pesan rahasia berupa file teks dengan format **.txt* ke dalam sebuah *cover* yang berupa *file* video dengan format **.avi.* Keluaran dari proses penyisipan ini yaitu berupa *video steganography* dimana terdapat video yang telah disisipi pesan rahasia. Lalu *video steganography* dikirimkan ke penerima. Kemudian disisi penerima dilakukan proses ekstraksi, untuk mengembalikan pesan rahasia berupa *file* teks dengan format **.txt*.



Gambar 5. Diagram Alir Proses Penyisipan (a) dan Ekstraksi (b)

Berdasarkan Gambar 5 sistem yang dirancang pada tugas akhir ini adalah sistem steganografi dengan video sebagai *cover*. Penyisipan dilakukan di sisi penerima dengan menyisipkan pesan rahasia berupa file teks dengan format *.txt* ke dalam sebuah cover berupa file video berformat *.avi* dengan metode *Discrete Wavelet Transform*. Penyisipan dilakukan berdasarkan deteksi *silence* pada sinyal audio dengan metode ZCR untuk memilih frame yang akan disisipkan pesan rahasia. Layer yang disisipkan adalah layer dominan dari frame pada video *cover*. Keluaran dari proses penyisipan berupa *stego-video* dimana terdapat pesan video yang telah disisipi pesan rahasia. Kemudian *stego-video* dikirimkan kepada penerima. Di sisi penerima dilakukan proses ekstraksi, untuk mengembalikan pesan rahasia berupa file teks dengan format .txt..

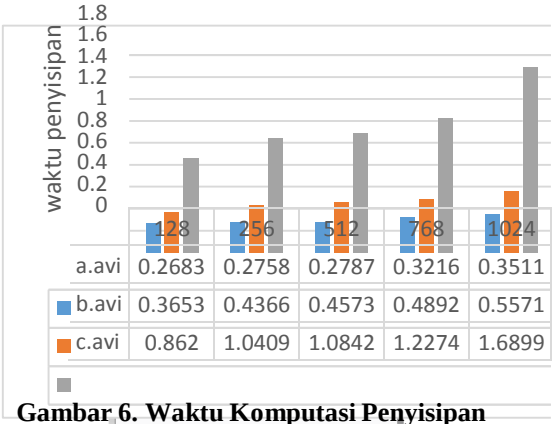
4. Pembahasan

Pengujian pada sistem steganografi ini menggunakan video sebagai cover, serta pesan rahasia (teks) dengan ukuran panjang pesan 64 bit, 128 bit, 256 bit, 512 bit dan 1024 bit. Video cover yang digunakan adalah video yang memiliki panjang maksimum 10 detik dengan format *.avi. Berikut adalah video cover yang digunakan:

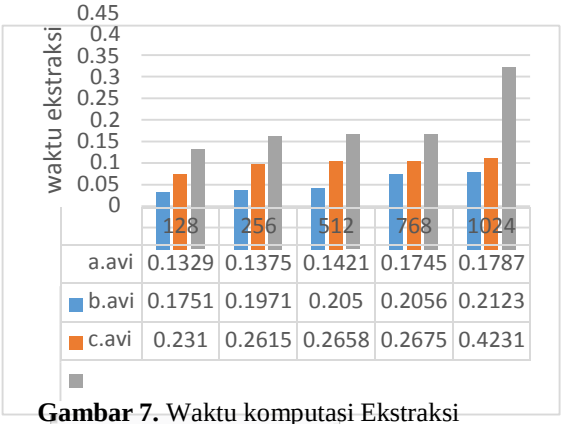
Tabel 2. *Video Cover*

a.avi	b.avi	c.avi
Length: 10 second	Length: 10 second	Length: 10 second
Frame width: 180	Frame width: 320	Frame width: 640
Frame height: 150	Frame height:240	Frame height: 480

A. Pengaruh Panjang Pesan dan Ukuran Video Cover terhadap Waktu Komputasi



Gambar 6. Waktu Komputasi Penyisipan

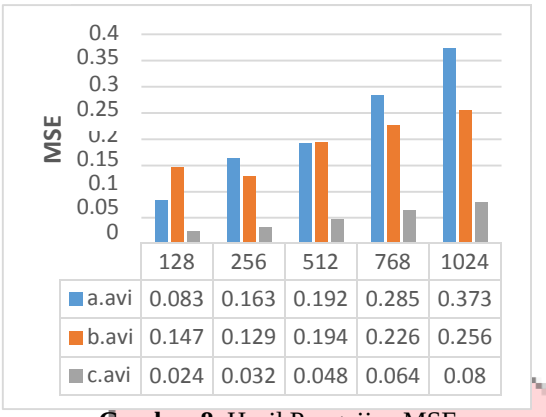


Gambar 7. Waktu komputasi Ekstraksi

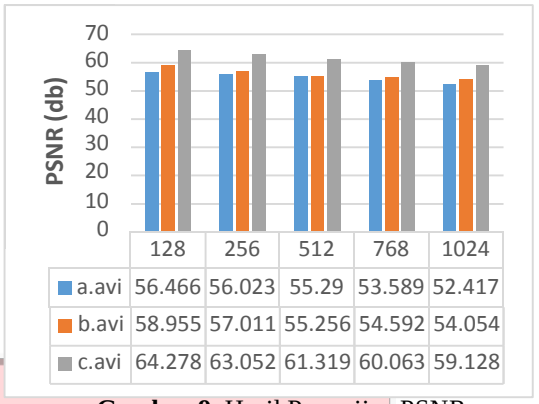
Pada kedua grafik di atas merupakan waktu komputasi rata-rata yang diperlukan dalam proses penyisipan dan ekstraksi. Dalam sistem steganografi, penyisipan pesan sepanjang 1024 bit ke video cover membutuhkan waktu terlama yaitu 1.6899 detik pada video berukuran 640x480 (c.avi) dan untuk ekstraksi membutuhkan waktu komputasi 0.4231 detik.

Dari pengujian yang telah dilakukan, dapat dilihat bahwa semakin besar ukuran panjang pesan yang disisipkan dan semakin besar ukuran video cover, maka semakin lama pula waktu komputasi yang diperlukan. Begitu pula disisi penerima. Hal ini terjadi dikarenakan dalam proses penyisipan pesan maupun ekstraksi pesan pada proses steganografi dengan ukuran yang semakin besar membuat bit-bit pesan yang akan diproses semakin banyak..

B. Pengaruh Panjang Pesan dan Ukuran Video Cover terhadap MSE dan PSNR



Gambar 8. Hasil Pengujian MSE



Gambar 9. Hasil Pengujian PSNR

Berdasarkan **Gambar 8** diketahui bahwa ukuran pesan rahasia yang disisipkan memiliki panjang bit yang berbeda-beda . Semakin panjang bit atau banyak pesan yang akan disispkan hal ini juga akan berpengaruh terhadap nilai MSE. Hal ini akan menyebabkan nilai MSE yang di dapat semakin besar itu artinya tingkat kemiripan antara *video cover* dengan *video stego* semakin kecil. Selain itu ukuran *cover* juga mempengaruhi nilai MSE yang di dapat semakin besar ukuran *frame* video akan mendapatkan nilai MSE semakin kecil begitupun sebaliknya apabila semakin kecil ukuran *frame* videonya maka akan di dapatkan nilai MSE yang semakin besar.

Berdasarkan hasil yang diperoleh pada **Gambar 9.** Maka ukuran pesan berpengaruh juga terhadap nilai PSNR yang di dapat. Semakin panjang atau banyak bit pesan yang disisipkan maka akan menghasilkan nilai PSNR yang semakin kecil. Berbeda dengan nilai MSE pada MSE semakin kecil hasil yang diperoleh maka akan semakin baik tetapi pada PSNR semakin kecil hasil yang diperoleh itu artinya kualitas dari *video* yang dilakukan penyisipan atau *video stego* kurang baik. PSNR erat kaitannya dengan MSE apabila MSE nya kecil maka akan berpengaruh terhadap PSNR ,yaitu mendapatkan nilai PSNR yang besar. Minimal nilai PSNR yang harus diperoleh untuk menandakan baiknya hasil setelah dilakukan steganografi yaitu harus lebih besar dari 20 dB. Berdasarkan hasil yang diperoleh maka nilai PSNR yang di dapat masih baik karena memiliki nilai lebih besar dari 20 dB.

C. Ketahanan Sistem Terhadap Serangan Noise

Ketahanan sistem steganografi pada video yang telah dibuat dapat diketahui dan diuji dengan memberikan serangan berupa *noise* pada video . Noise yang diberikan yaitu berupa *Gaussian Noise* dengan variansi $1x10^{-4}$ sampai $6x10^{-4}$.Pengujian akan dilakukan pada saat mean 0 dan 0.001.Video yang akan digunakan yaitu video yang memiliki ukuran 180x150 dan akan disisipkan pesan sepanjang 1024 bit. Berikut adalah hasil pengujian sistem yang telah diberikan *noise* :

Table 3. Pengaruh Mean dan Variansi Gaussian Noise Terhadap BER

Variansi	Mean		
	0	0.001	0.01
0.0001	0	0	0
0.0002	0	0	0
0.0003	0	0	0.0977
0.0004	0	0	0.1953
0.0005	0	0.0977	7.5195
0.0006	0.1953	0.3906	44.2842

Berdasarkan **Tabel 3,** sistem hanya mampu bertahan dengan kesalahan bit sama dengan nol saat *mean* = 0 pada variansi $1x10^{-4}$ hingga $5x10^{-4}$, *mean* = 0,001 pada variansi $1x10^{-4}$ hingga $4x10^{-4}$, dan *mean* = 0.01 pada variansi $1x10^{-4}$ hingga $2x10^{-4}$. Semakin besar nilai *mean* dan variansi, maka semakin besar pula tingkat kesalahan bit yang dihasilkan. Hal ini disebabkan karena nilai piksel-piksel pada frame video berubah sesuai dengan penyebaran besar kecilnya serangan *gaussian* yang diberikan. Sehingga pesan hasil ekstraksi menjadi rusak.

C. Mean Opinion Score (MOS)

Pengujian parameter MOS yang dilakukan bertujuan untuk melihat kualitas *stego video* jika diberi input pesan dengan panjang yang berbeda-beda. Panjang pesan yang diinputkan sepanjang 128 bit, 256 bit, 512 bit, 768bit, dan 1024 bit. Video yang digunakan sebagai cover video memiliki ukuran frame 180 x 150, 320 x 240, dan 640 x 480. Dari hasil survey MOS, didapatkan nilai rata-rata MOS untuk video pertama sebesar 3.5, untuk video kedua sebesar 3.7, dan untuk video ketiga sebesar 4.2. Berdasarkan nilai yang didapatkan dapat disimpulkan bahwa kualitas *stego video* adalah baik.

5. Kesimpulan

Dari hasil analisis pengujian sistem steganografi pada *frame* yang terdeteksi *silence* yang telah dilakukan, didapatkan hasil bahwa Panjang pesan dan Ukuran Video Cover sangat berpengaruh terhadap waktu komputasi. Dari penelitian yang telah dilakukan, waktu komputasi penyisipan terbesar yaitu 1.68994 dan waktu komputasi ekstraksi terbesar yaitu 0.42312. dari video cover c.avi (640x480) dengan panjang pesan yang disisipkan sebesar 1024 bit. Dari hasil pengujian stego video memiliki kualitas yang baik dan didapatkan nilai PSNR terbesar 64.2775 dan nilai MSE terendah 0.0243. Sistem yang telah dibuat masih sangat lemah terhadap serangan *noise*. Hal ini dapat dilihat dari hasil pengujian saat diberikan serangan *Gaussian Noise.*Dari hasil pengujian dengan MOS yang telah dilakukan, empat ukuran *cover* video yang berbeda mendapatkan nilai MOS rata-rata total sebesar 3,8 yang mengindikasikan sistem memiliki kualitas yang baik..

5.2 Saran

Untuk penelitian yang lebih lanjut diharapkan dapat memperbaiki segala bentuk kekurangan dan dapat mengembangkan segala sesuatu yang telah dilakukan pada penelitian ini. Oleh karena itu dapat dilakukan hal-hal sebagai berikut :

1. Proses steganografi dapat disimulasikan lebih lanjut pada Bahasa pemrograman yang lainnya, seperti Bahasa java, C, dan sebagainya.
2. Sistem dapat disimulasikan dengan bentuk pesan rahasia yang berbeda seperti video atau gambar.
3. Sistem dapat disimulasikan dengan jenis data *cover* yang lainnya, seperti image, video, dan audio.
4. Terdapat analisis mengenai ketahanan sistem dari berbagai jenis serangan, seperti *cropping*, *resize*, *rotate* dan lainnya.
5. Dapat dikombinasikan dengan metode yang lainnya, seperti MFCC, DCT, MLSB, dan lainnya.

DAFTAR REFERENSI

[1] Berg G, Davidson, Ming-Yuan Dual, Paul G. 2003. “Searching For Hidden Message: Automatic Detection of Steganography”. Washington: Computer Science Departement, University at Albany.

[2] Oktaviany, Arina Rizky. Dkk. 2008. “Implementasi dan Analisis Steganografi Video Berbasis Wavelet”. Jurusan Teknik Elektro, Institut Teknologi Telkom, Bandung.

[3] Sitorus, Eunike Johana. 2013. “Studi Perbandingan Kompresi Menggunakan Metode Shannon Fano Dan Unary Coding Pada File Teks”. Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara.

[4] Lu, Guojun, 1999, *Multimedia Database Management Systems*, Artech House Inc., London, hal. 107-115.

[5] Burrus, C Sidney, Gopinath, Ramesh A., Guo, Haitao. 1998. “*Introduction to Wavelet and Wavelet Transform*”. Prentiice-Hall,Inc .

[6] Fauzi, Rizki. Dkk. 2014. “*Simulasi dan Analisis Steganografi Ganda Pada Video Menggunakan Metode Duat Tree Complex Wavelet Transform dan Discrete Wavelet Transform*”. Fakultas Teknik, Departemen Elektro dan Komunikasi, Universitas Telkom.

[7] Feryando, Dara Aulia. 2015. “*Steganografi Citra pada Karakter Khusus Aksara Jawa Menggunakan Metode Discrete Cosine Transform*”. Fakultas Teknik Elektro, Universitas Telkom.

[8] Wahid, Muhammad Luthfi. 2015. “*Analisis dan Simulasi Steganografi Video Berbasis Deteksi Band Frekuensi Menggunakan Metode Discrete Wavelet Transform*”. Fakultas Teknik Elektro, Universitas Telkom.

[9] ITU-R BT.500-11 , *Methodology for The Subjective Assessment of The Quality of Television Pictures*., 2002.

[10] Arry Akhmad Arman. “*Proses Pembentukan dan Karakteristik Sinyal Ucapan*”.Departemen Teknik Elektro,ITB. Bandung.

[11] Moch Soleh, Ridwan. 2008. “*Denoising Rekaman Sinyal Elektrokardiogram (EKG) Menggunakan Algoritma Iterative Threshold Pada Subband Wavelet*”. Skripsi Sarjana Institut Teknologi Telkom Bandung : tidak diterbitkan