ANALISIS DAN SIMULASI STEGANOGRAFI VIDEO BERBASIS DETEKSI BAND FREKUENSI MENGGUNAKAN METODE DISCRETE WAVELET TRANSFORM

Simulation and Analysis of Steganography Based on Band Frequency Detection Using Discrete Wavelet Transform

Muhamad Luthfi Wahid[1], Dr.Ir. Bambang Hidayat, DEA[2], Nur Andini, S.T., M.T.[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Telkom University
[1]luthfimuh@students.telkomuniversity.ac.id, [2]bhidayat@telkomuniversity.ac.id,
[3]nurandini@telkomuniversity.ac.id

Abstrak

Steganografi merupakan metode yang digunakan untuk menyembunyikan pesan pada media digital. Dengan adanya steganografi diharapkan dapat mencegah terjadinya pencurian dan penyalahgunaan data sehingga informasi sampai kepada penerima dengan aman. Dalam tugas akhir ini, akan dibuat sistem steganografi untuk menyisipkan pesan teks pada video. Sebelum melakukan penyisipan akan dilakukan proses *framing* pada sinyal video dan untuk memilih frame yang akan disisipkan pesan rahasia akan ditentukan berdasarkan level frekuensi sinyal audio yang terdapat pada video. Metode yang digunakan untuk menyisipkan pesan adalah *Discrete Wavelet Transform* (DWT). Penyisipan pesan ini dilakukan dengan cara mengganti nilai koefisien yang dibawah nilai *threshold* dengan pesan rahasia. Hasil penelitian tugas akhir ini adalah sebuah sistem yang data menyisipkan pesan teks ke dalam video. Dengan menggunakan metode penyisipan DWT, menguji beberapa ukuran frame video, panjang pesan, dan nilai rentang frekuensi, didapatkan hasil *Peak Signal to Noise Ratio* (PSNR) yang baik. Hasil PSNR terbesar yang didapatkan yaitu 104,6178 dB dan nilai MSE terkecil yang didapatkan sebesar 2,21 x 10^{-6}. Waktu komputasi terbesar yang didapat pada proses penyisipan adalah 14,48626 detik sedangkan pada proses ekstraksi adalah 5,37692 detik. Hasil *Mean Opinion Score* (MOS) yang didapatkan memiliki nilai rata-rata total sebesar 3,9 yang berarti kualitas video tersisipi dengan baik.
Kata kunci : Steganografi, *Discrete Wavelet Transform, Treshold, Fast Fourier Transform, Video*

Abstract

Security and confidentiality of data is very important as the development of the exchange of information through digital media. To ensure the security and confidentiality of data is needed a technique to secure the data, one of them with steganography. Steganography is a method used to hide messages using digital media such as images, audio, and video. With the presence of steganography is expected to prevent data theft and misuse of data so that information can be up to the recipient safely. In this final project, will be made steganographic system to insert the message (.txt) in the video (.avi) uncompressed. Before doing the insertion will be performed on the framing process video signals and to select the frame to be inserted secret message will be determined by the level of frequency of the audio signal contained in the video footage. The method used to insert the message is Discrete Wavelet Transform (DWT). The message insertion is done by replacing the coefficient values below the threshold value with a secret message. Results of this research is a system that inserts the data into a video text messages. By using the method of insertion DWT, testing several video frame size, length of message, and the value of the frequency range, the result Peak Signal to Noise Ratio (PSNR) is good. PSNR results obtained are 104.6178db biggest and smallest MSE value obtained for 2:21 x 10-6. Most computing time obtained in the insertion process is 14.48626 seconds while the extraction process is 5.37692 seconds. Results Mean Opinion Score (MOS) were found to have an average total value of 3.9, which means the quality of the video is inserted properly.
Keywords: *Steganography, Discrete Wavelet Transform, Treshold, Fast Fourier Transform, Video*

1. Pendahuluan

Keamanan dan kerahasiaan data merupakan hal yang sangat penting seiring berkembangnya pertukaran informasi melalui media digital. Perkembangan informasi seharusnya memberikan keuntungan bagi kita ternyata memiliki sisi negatif. Nilai informasi akan menjadi sangat penting jika menyangkut hal-hal yang berhubungan dengan keamanan, keputusan bisnis, ataupun kepentingan umum. Untuk menjamin keamanan dan kerahasiaan data diperlukan suatu teknik untuk mengamankan data tersebut, salah satunya dengan steganografi [4]. Steganografi merupakan metode yang digunakan untuk menyembunyikan pesan dengan menggunakan media digital berupa gambar, audio, maupun video [5]. Sebelumnya sudah banyak dilakukan penelitian tentang steganografi dengan menggunakan metode *Least Significant Bit* (LSB), namun metode LSB rentan terhadap ekstraksi dan rawan terjadinya kesalahan [7]. Pada penelitian di [1] dilakukan steganografi pada video berformat

.avi dengan metode *Least Significant Bit* (LSB). Pada penelitian tersebut dikatakan bahwa metode tersebut dapat diimplementasikan dengan mudah, hanya saja seseorang dapat dengan mudah mencari tahu informasi yang tersembunyi. Pada Tugas Akhir ini akan dilakukan simulasi teknik steganografi pada video dengan format .avi yang tidak terkompresi menggunakan metode *Discrete Wavelet Transform* (DWT). Untuk meningkatkan kualitas steganografi, tempat penyisipan dilaksanakan berdasarkan pita frekuensi pada sinyal audio. Data rahasia yang disembunyikan berupa pesan teks dengan format .txt. Pada proses penyisipan teks, pertama-tama dilakukan pemisahan antara sinyal audio dan video. Kemudian menentukan frekuensi yang diinginkan pada segmen audio sebagai titik acuan untuk melakukan penyisipan pesan rahasia. Setelah itu teks disisipkan pada frame video saat frekuensi tersebut terdeteksi. Performansi system diuji melalui penghitungan *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), *Bit Error Rate* (BER) dan *Mean Opinion Score* (MOS).

2. Landasan Teori

A. Steganografi [3]

Steganografi berasal dari bahasa yunani yaitu *steganós* yang berarti tersembunyi atau menyembunyikan sedangkan *gráphy* berarti tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Teknik steganografi digunakan untuk menyembunyikan pesan rahasia ke dalam pesan lain sehingga pihak ketiga tidak menyadari adanya pesan rahasia di dalam pesan tersebut. 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

Ada empat kriteria yang harus diperhatikan dalam steganografi agar dapat dikatakan *file* stego yang baik, yaitu:

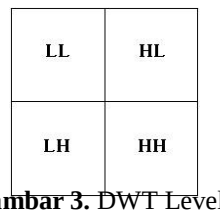
1. *Imperceptible*
   Cover dan *stego-object* harus tidak dapat dibedakan oleh indra manusia agar pesan tidak dapat dipersepsi oleh manusia.
2. *Fidelity*
   Mutu *cover* sebelum dan setelah disisipi pesan rahasia tidak jauh berubah. Sehingga perubahan tersebut tidak dapat dideteksi oleh indra manusia.
3. *Recovery*
   Pesan rahasia yang disembunyikan pada *cover* harus dapat diekstrak kembali agar dapat digunakan oleh penerima.
4. *Robustness*
   Pesan rahasia yang disembunyikan harus tahan terhadap berbagai operasi manipulasi yang dilakukan pada *cover*, seperti pengubahan kontras, penajaman, kompresi, rotasi, pemotongan (*cropping*), enkripsi, dan lain-lain.

B. Video [8]

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 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. Discrete Wavelet Transform [4]

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 3. DWT Level 1

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.

Gambar 4. DWT Level 2

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:

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

$$\sum^{1} \text{[illegible]} = \frac{1}{4} \text{[illegible]}=0 \text{[illegible]}(2\text{[illegible]} + \text{[illegible]}2\text{[illegible]} - \frac{1}{4} \sum^{1} \text{[illegible]}=0 \text{[illegible]}(2\text{[illegible]} + \text{[illegible]}2\text{[illegible]} + 1) \quad (2)$$

$$H\text{[illegible]} = \frac{1}{4} \sum^{1} \text{[illegible]}=0 \text{[illegible]}(2\text{[illegible]}2\text{[illegible]} + \text{[illegible]}) - \frac{1}{4} \sum^{1} \text{[illegible]}=0 \text{[illegible]}(2\text{[illegible]} + 1,2\text{[illegible]} + \text{[illegible]}) \quad (3)$$

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

D. Parameter Pengujian

1. *Mean Square Error* (MSE) [8]

MSE 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 :

$$\text{[illegible]} = \frac{\sum \text{[illegible]} \sum \text{[illegible]} (I'(\text{[illegible]} - \text{[illegible]}(\text{[illegible]})^2}{\text{[illegible]}=1 \quad \text{[illegible]} 1 \quad \text{[illegible]}} \quad (5)$$

2. *Peak Signal to Noise Ratio* (PSNR) [8]

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 :

$$\text{[illegible]} = 10 \text{[illegible]} \log_{10}[\frac{\text{[illegible]}^2}{\text{[illegible]}E}] \quad (6)$$

3. *Bit Error Rate* (BER) [8]

BER 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 tetap harus tersampaikan ke penerima. Adapun cara penghitungan BER, yaitu :

$$BER = \frac{\sum \text{[illegible]} \text{[illegible]}}{\sum \text{[illegible]} \text{[illegible]}} \quad (7)$$

4. *Character Error Rate* (CER) [8]

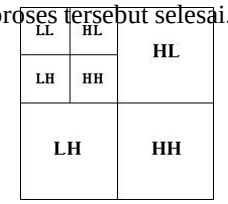
CER (Character Error Rate) adalah perbandingan jumlah karakter yang error dengan total karakter. CER merupakan parameter pengujian yang digunakan untuk melihat kualitas pesan yang disisipkan. Penggunaan parameter BER tidak cukup apabila tidak disertakan dengan pengujian terhadap parameter CER. Hal ini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

$$BER = \frac{\sum \text{[illegible]} \text{[illegible]}}{\text{[illegible]}}$$

5. Waktu Komputasi [8]

(8)

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) [6]

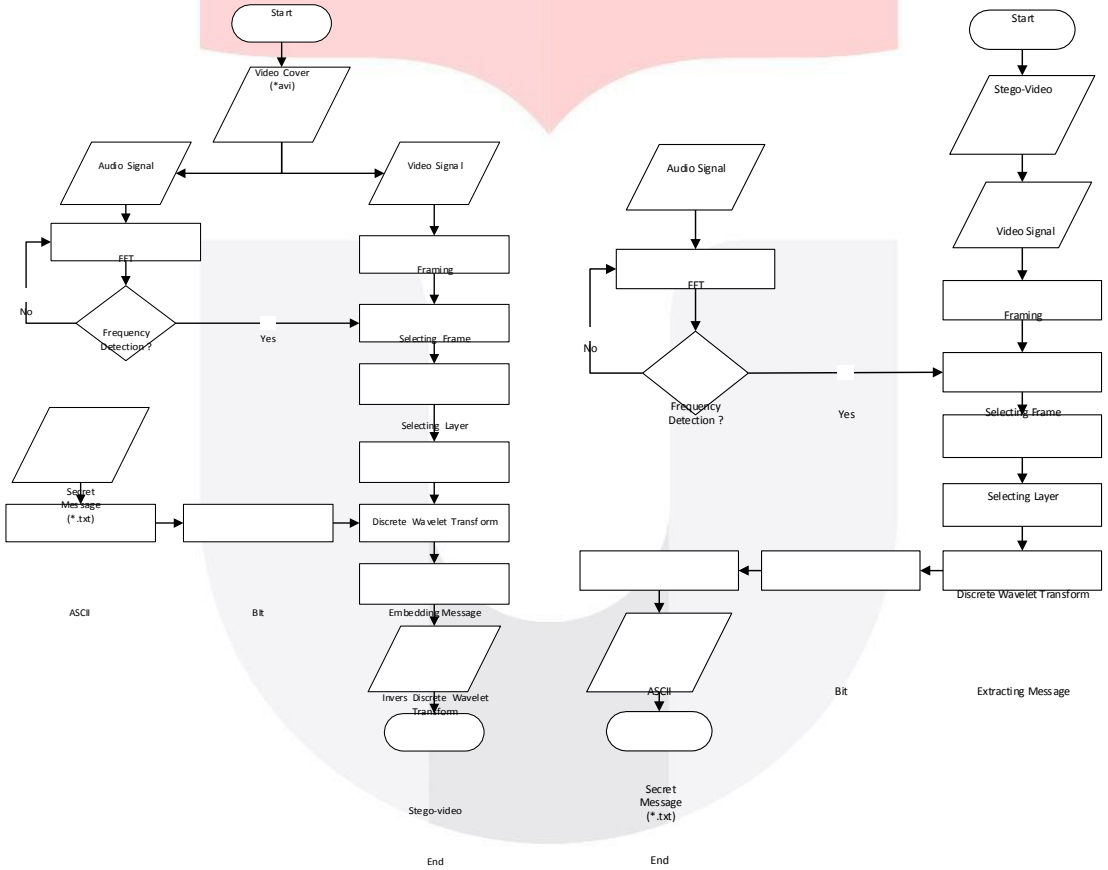
Berdasarkan standar ITU-R BT.500., MOS *(Mean Opinion Score*) merupakan metode penilaian subjektif oleh responden pada data digital baik berupa data audio maupun image/video. Pada Tabel 1 penilaian MOS diekspresikan dengan sebuah nilai pada skala satu sampai dengan lima. Dikarenakan penilaian ini berdasarkan dari pengamatan mata manusia, maka hasilnya akan sangat subjektif karena baik buruknya citra hasil rekonstruksi ini bergantung pada penilaian masing-masing koresponden.

Tabel 1. Penilaian MOS [6]

Skala Penilaian	Kualitas	Persepsi Citra
5	Sempurna	Citra tervisualisasi sangat baik
4	Baik	Citra tervisualisasi baik dan tidak ada kerusakan
3	Cukup	Citra masih dapat dikenali, terdapat kerusakan sedikit menganggu interpretasi
2	Kurang	Citra kurang dapat dikenali, kerusakan yang ada menganggu interpretasi
1	Buruk	Citra tidak dapat dikenali

3. Blok Diagram Sistem

Pada Gambar 5 digambarkan langkah – langkah yang dilakukan sistem untuk menyisipkan dan mengekstraksi pesan.



(a) (b)

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 nilai rentang frekuensi pada sinyal audio 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 sistem steganografi yang dirancang pada tugas akhir ini dilakukan dengan menggunakan pesan rahasia dan *video cover*. Pesan rahasia yang akan digunakan pada sistem steganografi ini berupa teks dengan format .txt dengan ukuran panjang pesan 128 bit, 256 bit, 512 bit, 768 bit, dan 1024 bit. *Cover* yang digunakan pada penyisipan steganografi ini berupa video tanpa kompresi dengan format .avi. Video yang digunakan sebagai *cover* pada penelitian ini adalah sebagai berikut :

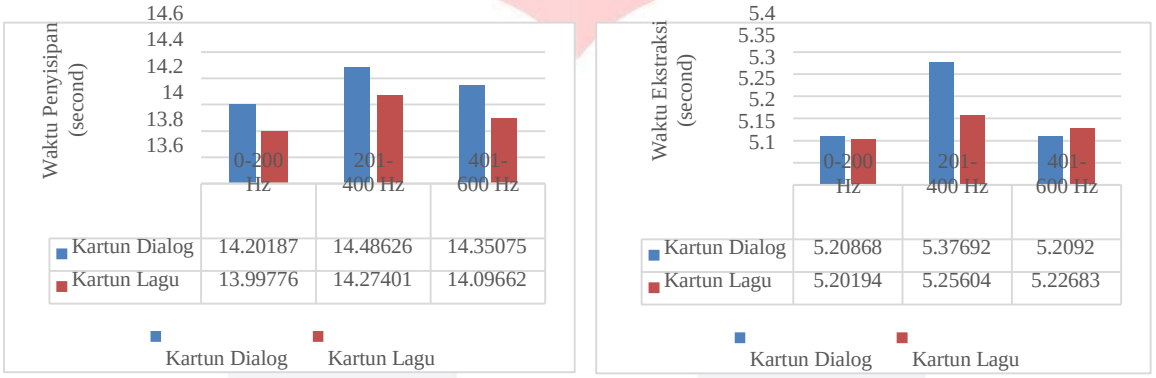
Tabel 2 Video Cover

Vipmen 160x120	Visionface 640x480	Kartun Lagu 720x480	Kartun Dialog 720x480
Length : 00:00:09 *Frame Width* : 160 *Frame Height* : 120	*Length* : 00:00:09 *Frame Width* : 640 *Frame Height* : 480	*Length* : 00:00:09 *Frame Width* : 720 *Frame Height* : 480	*Length* : 00:00:09 *Frame Width* : 720 *Frame Height* : 480

A. Pengaruh Rentang Nilai Band Frekuensi Terhadap Waktu Komputasi

a. Sistematika Pengukuran
Pengukuran waktu komputasi akan dilakukan dengan menggunakan rentang nilai band frekuensi sebesar 0-200 Hz, 201-400 Hz, dan 401-600 Hz. Frame video yang digunakan pada pengujian ini berukuran 720x480 dan pesan yang disisipkan sepanjang 1024 bit dengan *threshold* 0.5.

b. Hasil Pengukuran



(a) (b)

Gambar 6 (a) Pengaruh rentang nilai *band* frekuensi terhadap waktu penyisipan (b) Tabel pengaruh rentang nilai *band* frekuensi terhadap waktu ekstraksi

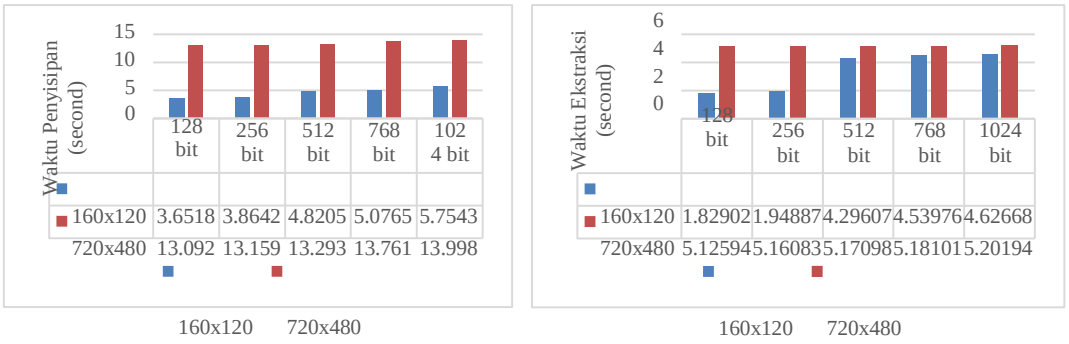
c. Analisis Hasil Pengukuran

Berdasarkan hasil penelitian diatas rentang band frekuensi dapat mempengaruhi waktu komputasi saat penyisipan maupun saat proses ekstraksi. Pemilihan rentang *band* frekuensi mempengaruhi waktu komputasi dikarenakan masing-masing frame video memiliki nilai frekuensi yang berbeda-beda pada sinyal audio sehingga memiliki waktu komputasi yang berbeda. Pada hasil penelitian diatas menunjukkan bahwa pada video berjudul 'Kartun Lagu.avi' waktu komputasi tercepat pada frekuensi 0-200 dengan waktu penyisipan 13.99776 detik dan waktu ekstrak 5.20194 detik. Sedangkan video berjudul 'Kartun Dialog.avi' waktu komputasi untuk proses penyisipan membutuhkan 14.20197 detik dan waktu ekstraksi 5.20194 detik. Proses pada frekuensi tersebut memiliki waktu komputasi yang lebih cepat karena penyisipan dilakukan di frame awal pada video.

B. Pengaruh Panjang Pesan dan Ukuran Cover Terhadap Waktu Komputasi

a. Sistematika Pengukuran
Pengujian ini dilakukan menggunakan nilai *threshold* 0.5 dengan menyisipkan pesan sepanjang 128 bit, 256 bit, 512 bit, 768 bit, dan 1024 bit ke dalam frame video berukuran 160x120 dan 720x480.

b. Hasil Pengukuran



(a) (b)

Gambar 7 (a) Pengaruh panjang pesan dan ukuran *cover* terhadap waktu penyisipan (b) Tabel pengaruh panjang pesan dan ukuran *cover* terhadap waktu ekstraksi

c. Analisis Hasil Pengukuran

Berdasarkan tabel diatas, penyisipan 1024 bit pada cover video membutuhkan waktu komputasi dengan 5.75431 detik untuk proses penyisipan dan 4.62668 detik untuk ekstraksi. Sementara untuk panjang pesan 128 bit waktu penyisipan yang dibutuhkan hanya 3.6518 detik dan 1.82902 detik. Dari hasil pengujian tersebut dapat diketahui bahwa semakin besar data yang disipkan pada *cover*, maka semakin lama waktu komputasi. Hal ini dikarenakan semakin besar pesan rahasia maka semakin banyak pesan yang akan disipkan, sehingga sistem membutuhkan waktu yang lebih lama untuk melakukan proses steganografi. Selain itu, semakin besar ukuran frame cover maka semakin lama juga waktu komputasi yang dibutuhkan. Pesan yang disispkan sepanjanng 512 bit pada ukuran frame 160x120 hanya membutuhkan waktu 4.8205 detik untuk penyisipan dan 4.29607 detik untuk ekstraksi. Sementara itu pada ukuran frame 720x480 dibutuhkan waktu 13.293 detik untuk penyisipan dan 5.17098 detik untuk ekstraksi.

C. Pengaruh Panjang Pesan dan Ukuran Cover Terhadap Nilai MSE dan PSNR

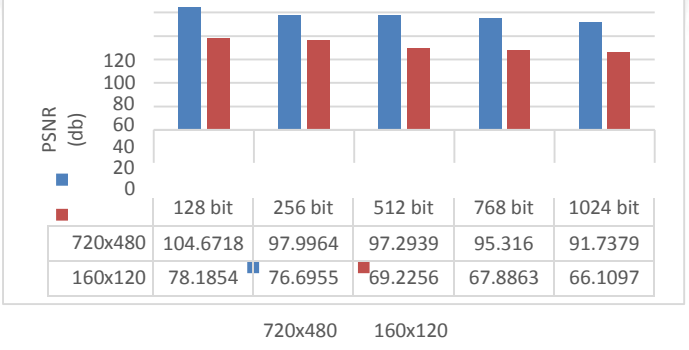
a. Sistematika Pengukuran

Pengujian ini dilakukan menggunakan nilai *threshold* 0.5 dengan menyisipkan pesan sepanjang 128 bit, 256 bit, 512 bit, 768 bit, dan 1024 bit ke dalam frame video berukuran 160x120 dan 720x480.

b. Hasil Pengukuran

Tabel 3 Performansi Panjang Pesan dan Ukuran Cover Terhadap MSE

	128 bit	256 bit	512 bit	768 bit	1024 bit
720x480	2.2177×10^{-6}	0.000010314	0.000012125	0.00001912	0.00004358
160x120	0.0009875	0.0014	0.0078	0.0106	0.0159



Gambar 8 Performansi Panjang Pesan dan Ukuran Cover Terhadap MSE

c. Analisis Hasil Pengukuran

Berdasarkan grafik di atas diketahui bahwa ukuran pesan rahasia yang disisipkan berbeda-beda. Peningkatan jumlah pesan rahasia yang akan disisipkan dapat mempengaruhi nilai MSE. Hal ini menyebabkan tingkat kemiripan *cover video* dan *stego video* semakin kecil dan tingkat kesalahan yang terjadi pada *stego video* meningkat sehingga nilai MSE semakin besar. Sedangkan semakin besar ukuran frame video maka semakin kecil tingkat kesalahan pada *stego-video* yang menyebabkan nilai MSE semakin kecil. Selain itu, semakin panjang pesan yang disisipkan maka semakin kecil nilai PSNR dan semakin besar ukuran frame video maka semakin besar pula nilai PSNR. Hal ini dikarenakan video berukuran '720x480' memiliki ukuran frame dan kapasitas penyisipan yang lebih besar dibandingkan video berukuran '160x120'. Nilai PSNR berbanding terbalik dengan nilai MSE. Semakin besar nilai MSE maka semakin kecil nilai PSNR yang diperoleh. Semakin kecil nilai MSE maka akan semakin besar nilai PSNR yang diperoleh.

D. Pengaruh Nilai Threshold Terhadap MSE, PSNR, BER dan CER

a. Sistematika Pengukuran
Pengujian ini dilakukan dengan menyisipkan pesan rahasia sepanjang 1024 bit ke dalam *cover* dengan ukuran frame 720x480. Nilai *threshold* yang diuji adalah 0.3, 0.4, 0.5, dan 0.6.

b. Hasil Pengukuran

Tabel 3 Pengaruh Nilai Treshold Terhadap MSE, PSNR, BER, dan CER

Treshold	0.3	0.4	0.5	0.6
MSE	0.00096	0.00121	0.00138	0.00152
PSNR	80.609	82.295	81.225	79.673
BER	2.05%	0.16%	0	0.03%
CER	4.17%	1.04%	0	0.26%

c. Analisis Hasil Pengukuran

Dari grafik diatas dapat diketahui, saat digunakan nilai *threshold* sebesar 0.4 didapatkan nilai MSE yang rendah dan nilai PSNR yang tinggi. Hal ini disebabkan karena pada saat nilai *threshold* digunakan tingkat kemiripan dengan *video cover* semakin besar dan tingkat kesalahan yang terjadi pada *stego video* menurun. Tetapi nilai *treshold* 0.5 sangat baik digunakan, karena memiliki nilai BER dan CER = 0 sehingga tidak adanya kesalahan bit ataupun karakter dan pesan yang dikirimkan sama persis antara pesan yang dikirim dengan pesan yang diterima.

E. Pengaruh Serangan Noise

a. Sistematika Pengukuran
Pada sistem ini video cover ukuran 160x120 akan diserang oleh *Gaussian Noise* dan *Salt and Pepper Noise.*

b. Hasil Pengukuran

Tabel 4 Pengaruh Nilai Treshold Terhadap MSE, PSNR, BER, dan CER

	Tanpa Noise	10 dB	20 dB	30 db	40 dB	50 dB
MSE	0.0159	107.0542	81.4084	28.459	3.4186	0.5629
PSNR	66.1097	27.8348	29.0241	33.5886	42.7923	50.6263

Tabel 5 Pengaruh Nilai Treshold Terhadap MSE, PSNR, BER, dan CER

	Video Stego	50%	40%	30%	20%	10%
MSE	0.0159	59.8257	47.8564	35.9841	24.0874	12.1152
PSNR	66.1097	30.3619	31.3314	32.5697	34.3129	37.2975

c. Analisis Hasil Pengukuran

Berdasarkan hasil pengujian MSE dan PSNR pada tabel diatas, dapat diketahui bahwa nilai MSE *stego-video* sebelum diberikan *Gaussian noise* sebesar 0.0159 dan PSNR 66.1097 dB. Setelah diberikan serangan *Gaussian noise* sebesar 10db, 20db, 30db, 40 db, dan 50db, semakin besar serangan yang diberikan maka nilai MSE semakin kecil sedangkan nilai PSNR semakin besar. Berdasarkan hasil pengujian MSE dan PSNR pada tabel diatas, dapat diketahui bahwa nilai MSE *stego-video* sebelum diberikan *salt and pepper noise* sebesar 0.0159 dan PSNR 66.1097 dB. Setelah diberikan serangan *salt and pepper noise* sebesar 10%, 20%, 30%, 40%, dan 50%, semakin besar serangan yang diberikan maka nilai MSE semakin besar sedangkan nilai PSNR semakin kecil.

F. 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, 768 bit, dan 1024 bit. Video yang digunakan sebagai cover video memiliki ukuran frame 160 x 120, 640 x 480, dan 720 x 480. Dari hasil survey MOS, didapatkan nilai rata-rata MOS untuk video pertama sebesar 3.81, untuk video kedua sebesar 3.97, dan untuk video ketiga sebesar 4.21. Berdasarkan nilai yang didapatkan dapat disimpulkan bahwa kualitas *stego video* adalah baik.

Tabel 6 Pengaruh Nilai Treshold Terhadap MSE, PSNR, BER, dan CER

Ukuran Cover Video	Nilai Rata-Rata MOS
160x120	3,81
640x480	3.97
720x480	4,21

5. Kesimpulan

Dari hasil analisis pada pengujian sistema, perancangan simulasi sistem steganografi video berbasi deteksi *band* frekuensi dengan metode *discrete wavelet transform* mampu bekerja dengan baik. Berdasarkan tabel diatas, penyisipan 1024 bit membutuhkan waktu 5,75431 detik, 768 bit membutuhkan 5,07648, 512 bit membutuhkan 4,82051 detik, 256 bit membutuhkan waktu 3,86424 detik, 128 bit membutuhkan waktu 3,65175 detik. Untuk proses penyisipan pada cover video berukuran 160x120 membutuhkan waktu 5,75431 sementara cover berukuran 720x480 membutuhkan waktu 13,99776 detik. Semakin besar ukuran panjang pesan dan semakin besar ukuran *frame* video, maka semakin lama waktu komputasi yang dibutuhkan untuk melakukan proses penyisipan dan ekstraksi pesan. Dari hasil pengujian stego video memiliki kualitas yang baik dan didapatkan PSNR 66,1097 dB – 104,6718 dB. Nilai *threshold* yang digunakan baik untuk sistem ini adalah 0.5. Karena dengan nilai *threshold* tersebut tidak ada kesalahan diantara pesan yang dikirim dan diterima atau dengan kata lain memiliki nilai BER=0 dan CER=0. Hasil parameter MOS yang didapatkan memiliki nilai rata-rata total sebesar 3,9 yang berarti kualitas video tersisipi dengan baik.

Daftar Pustaka:

[1] Ashish T. Bhole dan Rachna Patel. 2012. "*Steganography over Video File using Random Byte Hiding and LSB Technique*". Departement of Computer Engineering, SSBT's COE & T, Bambhori, Jalgaon, India.

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

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

[4] Fahdiani, Isma. Dkk. 2008. "*Implementasi Steganografi pada Video Jenis AVI dengan Menggunakan Transformasi Wavelet Diskrit*". Jurusan Teknik Elektro, Institut Teknologi Telkom, Bandung

[5] 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

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

[7] Klimis S . Ntalianis, Nikolaos D. Doulamis, Anastasios D. Doulamis, and Stefanos D. Kollias. 2002. "*An Automatic Video-Object Based Steganographic System for Multi-Use Message Hiding Using Wavelet Transform*". Electrical & Computer Engineering, National Technical University.

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