

VIDEO STEGANOGRAFI MENGGUNAKAN METODE *ENHANCED LEAST SIGNIFICANT BIT* PADA *FRAME* YANG DIPILIH BERDASARKAN DETEKSI ENERGI PITA FREKUENSI DENGAN *DISCRETE WAVELET PACKET TRANSFORM*

VIDEO STEGANOGRAPHY USING *ENHANCED LEAST SIGNIFICANT BIT* ON *SELECTED FRAME* WITH ENERGY OF BAND FREQUENCY DETECTION BASED ON *DISCRETE WAVELET PACKET TRANSFORM*

Bella Yunita Kusuma¹, Dr.Ir.Bambang Hidayat,DEA², I Nyoman Apraz Ramatryana ST.,MT³

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

¹bellayunita@students.telkomuniversity.ac.id, ²bhidayat@telkomuniversity.ac.id,

³ramatryana@telkomuniversity.ac.id

Abstrak

Perkembangan di dunia teknologi dan informasi saat ini sudah memasuki *era digital*. Dimana pertukaran informasi saat ini dilakukan melalui internet. Namun pertukaran informasi yang dilakukan melalui internet menimbulkan kekhawatiran jatuhnya informasi kepada pihak yang tidak berkepentingan karena sifat internet yang dapat diakses oleh siapapun, kapanpun dan dimanapun. Oleh karena itu perlunya sistem untuk menjaga keamanan suatu data yaitu dengan steganografi. Steganografi adalah teknik menyembunyikan informasi ke dalam file multimedia. Dalam tugas akhir ini akan dibuat steganografi yang dapat menyembunyikan pesan teks ke dalam video. Proses penyisipan pesan akan dilakukan dengan menggunakan metode *Enhanced Least Significant Bit*. Untuk lebih menjaga keamanannya pemilihan tempat penyisipan *frame* pada video akan ditentukan berdasarkan deteksi *Energy Band Frequency* pada audio, dengan menggunakan metode *Discrete Wavelet Packet Transform*. Kemudian steganografi yang dibuat dilakukan pengujian berdasarkan MSE, PSNR dan MOS. Hasil yang didapatkan cukup baik dimana mendapatkan nilai PSNR sebesar 71.0221 dan nilai MSE terkecil yaitu 0.0051 serta hasil rata-rata MOS yaitu 3.99778

Kata Kunci : Steganografi, Discrete Wavelet Packet Transform, Enhanced Least Significant Bit, Video.

Abstract

Developments in the world of technology and information is now entering the digital era. Where the exchange of information is currently done through internet. However, the exchange of information is done through the internet raises concerns fall of information to unauthorized parties because character of the internet that can be accessed by anyone, anytime and anywhere. Hence the need for the system to maintain the security of the data that is with steganography. Stegnaografi is the technique of hiding information into multimedia files. in this final task will be made steganography to hide text message into a video. The process of inserting a message will be performed using *Enhanced Least Significant Bit*. Selection of the insertion point in the video frame will be determined based on the detection of *Frequency Band Energy* in audio, by using methods of *Discrete Wavelet Packet Transform*. Then steganography made testing based on the MSE, PSNR and MOS. The results obtained are quite good that acquiring the PSNR value of 71.0221 and the smallest MSE value is 0.0051, and the average of MOS is 3.99778

Keyword: Steganography, Discrete Wavelet Packet Transform, Enhanced Least Significant Bit, Video

1. Pendahuluan

Perkembangan di dunia teknologi, informasi dan komunikasi saat ini semakin canggih dan modern, dimana saat ini sudah memasuki era digital. Seperti halnya dalam hal pertukaran informasi yang dilakukan melalui internet. Internet memang memberikan kemudahan dalam pertukaran dan mendapatkan informasi, Namun pertukaran informasi yang dilakukan melalui internet menimbulkan kekhawatiran akan sampainya atau terjadinya penyalahgunaan informasi oleh pihak yang tidak berkepentingan karena sifat internet yang publik yang dapat diakses oleh siapa saja, kapan saja dan dimana saja. Untuk dapat menjaga keamanan informasi yang dikirimkan dapat dilakukan salah satunya dengan steganografi. Steganografi merupakan teknik menyembunyikan informasi ke dalam file multimedia. Salah satu metode yang paling mudah digunakan adalah dengan metode *Least Significant Bit*. Namun metode ini memiliki kelemahan dapat dengan mudah diketahui

karena penyisipan dilakukan pada bit terakhir[1]. Pada tugas akhir ini akan dilakukan steganografi dengan menyisipkan pesan teks ke dalam sebuah video berformat avi. Proses penyisipan akan dilakukan menggunakan metode *Enhanced Least Significant Bit* dimana metode ini merupakan modifikasi dari metode LSB, penyisipan pesan dilakukan dengan mengacak nomor bit dari *file host* untuk *embedding* pesan rahasia dan dengan cara mengacak *sample host* yang mengandung bit pesan rahasia berikutnya[2]. Untuk lebih menjaga keamanan dari video steganografi ini tempat penyisipan pada *frame* video ditentukan berdasarkan deteksi energi band frequency pada audio. Pendeteksian energi dilakukan dengan menggunakan metode *Discrete Wavelet Packet Transform*. Kemudian nantinya steganografi video yang dibuat akan dilakukan pengujian secara objektif dan subjektif. Pengujian secara objektif dilakukan dengan parameter MSE, PSNR, BER dan CER. Sementara pengujian secara subjektif dilakukan dengan parameter MOS.

2. Dasar Teori

A. Steganografi[4]

Kata *steganografi* berasal dari bahasa Yunani *steganos* yang berarti “tertutup atau tersamar” dan *graphy* yang berarti “tulisan atau gambar”. Jadi secara etimologis steganografi berarti “tulisan yang tersamar”. Steganografi adalah teknik dan seni menyembunyikan pesan rahasia pada suatu medium dengan cara tertentu sehingga keberadaan pesan rahasia pada medium tersebut diharapkan tidak menimbulkan kecurigaan.

Ada empat kriteria yang harus diperhatikan dalam steganografi agar dapat dikatakan *file stego* yang baik, yaitu[4]:

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 di deteksi oleh indra manusia.
3. *Recovery* : Pesan rahasia yang disembunyikan pada *cover* harus dapat di ekstrak kembali agar dapat digunakan oleh penerima.
4. *Robustness* : Pesan rahasia yang disembunyikan harus tahan terhadap berbagai operasi manipulasi yang dilakukan pada *cover*, seperti perubahan *contrast*, penajaman, kompresi, rotasi, pemotongan dan lain-lain..

B. Audio Video Interleave (AVI)[3]

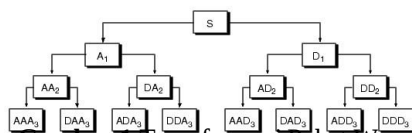
Audio/Video Interleave atau biasa disingkat AVI, adalah salah satu format video multimedia yang diperkenalkan oleh Microsoft pada tahun 1992. Sama seperti pada jenis video lainnya, AVI berisikan frame gambar dan suara yang bisa dijalankan secara bersamaan dan simultan sehingga jadi suatu film.. Suatu 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. Wavelet[5]

Wavelet pertama kali diperkenalkan oleh Morlet dan Grossman pada tahun 1983 sebagai fungsi yang memenuhi persyaratan matematika tertentu dan digunakan dalam merepresentasikan data atau fungsi lain. Sinyal sinusoidal adalah sinyal besar. Berbeda dengan sinyal sinusoidal, wavelet adalah sinyal kecil/singkat yang energinya terkonsentrasi pada suatu selang waktu.

D. Transformasi Paket Wavelet[5]

Metode Transformasi Paket Wavelet adalah suatu generalisasi dari dekomposisi wavelet yang menawarkan kemungkinan analisa sinyal yang lebih luas. Di dalam analisa wavelet, suatu sinyal dipecah atau didekomposisi menjadi koefisien aproksimasi dan koefisien detail. Selanjutnya koefisien aproksimasi tersebut didekomposisi kembali menjadi koefisien aproksimasi dan detail untuk level selanjutnya. Pada analisa Paket Wavelet koefisien aproksimasi dan detail sama-sama didekomposisikan kembali pada level selanjutnya sehingga pada n level dekomposisi akan menghasilkan 2^n koefisien yang berbeda. Namun, karena proses *downsampling* jumlah keseluruhan koefisien masih sama dan tidak ada redundancy terhadap jumlah koefisiennya. Ilustrasi dapat dilihat pada Gambar.



Gambar 1 Transformasi Paket Wavelet

Pada level satu akan menghasilkan A_1 dan D_1 dimana A_1 adalah koefisien aproksimasi dan D_1 adalah koefisien detail. Lalu untuk level dua, koefisien aproksimasi dan koefisien detail di level satu akan dipecah kembali,

koefisien aproksimasi dipecah menjadi koefisien aproksimasi (AA_2) dan koefisien detail (DA_2) koefisien detail juga dipecah menjadi koefisien aproksimasi AD_2 dan koefisien detail (DD_2). Jadi untuk level 2 koefisien yang dihasilkan adalah (AA_2) (DA_2) (DD_2). Demikian seterusnya sampai level ke-n yang diinginkan.

Nilai dari koefisien WPD dapat didefinisikan sebagai berikut. Energi WPD didefinisikan sebagai berikut.

$$E_B(r) = \sum_{r=2,3 \dots, 32, \dots} \quad (1)$$

Dan Energi Rata-ratanya sebagai berikut.

$$E_B(r) = \frac{1}{C} \sum_{r=2,3 \dots, 32, \dots} n_c \quad (2)$$

Keterangan :

r : subband

n_c : nilai koefisien WPD untuk setiap bagian atau subband

C : nilai koefisien WPD

E. Enhanced Least Significant Bit [2]

Pada metode ELSB terdapat dua proses untuk dilakukannya penyisipan yaitu dengan melihat skema pemilihan letak bit *message* dan skema pemilihan sample.

Tabel 1 Skema Pemilihan letak bit message

MSB I	MSB II	Letak bit
0	0	LSB 3
0	1	LSB 2
1	0	LSB 1
1	1	LSB 1

Tabel 2 Skema Pemilihan Sample

MSB I	MSBII	MSBIII	Sample bit
0	0	0	i + 1
0	0	1	i + 2
0	1	0	i + 3
1	0	0	i + 4
0	1	1	i + 5
1	1	0	i + 6
1	0	1	i + 7
1	1	1	i + 8

F. Parameter Pengujian [1]

1. MSE (Mean Square Error)

MSE adalah parameter yang digunakan untuk menganalisis performansi sistem dengan melihat hasil kualitas *stego-video*. Dalam metode ini yaitu mencari nilai rata-rata *error* antara citra cover dengan citra stego.

$$MSE = \frac{1}{N} \sum_{i=1}^N (I_i - S_i)^2 \quad (3)$$

2. 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 rumus PSNR:

$$PSNR = 10 \times \log_{10} \left[\frac{255^2}{MSE} \right] \quad (4)$$

3. BER (Bit Error Rate)

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.

$$BER = \frac{\sum \text{bit error}}{\sum \text{total bit}} \quad (5)$$

4. CER (Character Error Rate)

CER merupakan parameter pengujian untuk melihat kualitas pesan yang disisipkan. Berikut rumus CER :

$$CER = \frac{\sum \text{character error}}{\sum \text{total character}} \quad (6)$$

5. Waktu komputasi

Adalah waktu yang dibutuhkan sistem untuk melakukan suatu proses. Dihitung dari mulainya proses hingga proses tersebut selesai.

6. MOS (Mean Opinion Score)

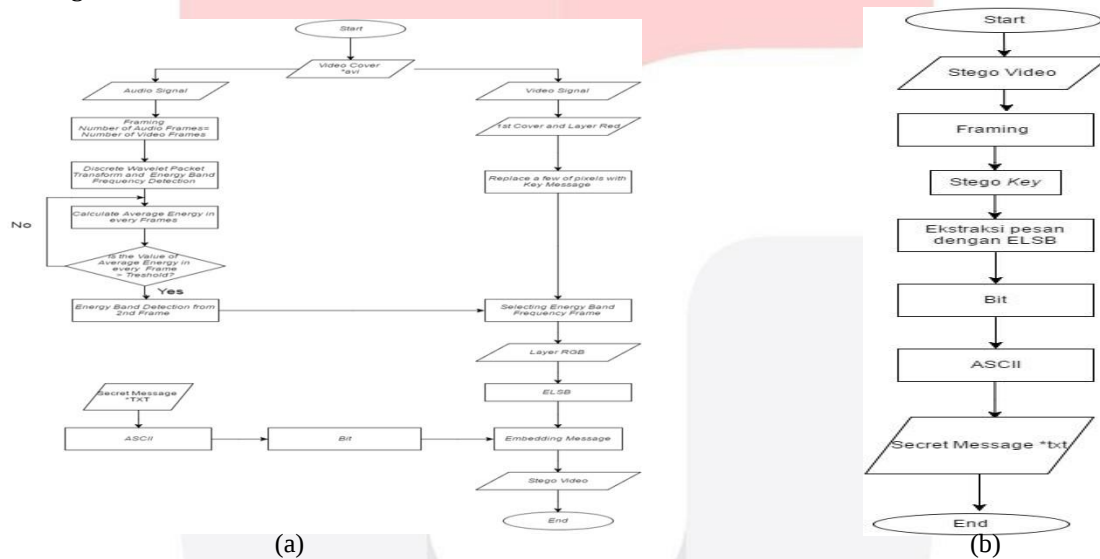
Berdasarkan standar ITU-R BT .500 MOS merupakan penilaian subjektif oleh responden pada digital baik berupa audio, image/video. Pada tabel 3 penilaian MOS di ekspresikan dengan suatu nilai pada skala satu

sampai dengan lima .Dikarenakan penilain ini berdasarkan pada mata manusia,maka hasilnya akan sangat subjektif berdasarkan penilaian masing-masing koresponden.

Tabel 3 Penilaian MOS

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

3. Blok Diagram Sistem



Gambar 2 Blok Diagram Steganografi

Berdasarkan **Gambar 2a** sistem yang dirancang pada tugas akhir ini adalah sistem steganografi menggunakan video sebagai *covernya*. Pada proses *Embedding Message* dilakukan dua proses sebelum video stego dikirimkan, yaitu proses pada audio untuk pemilihan tempat penyisipan frame dan proses pada video dimana pesan disisipkan. Proses pada audio dilakukan sebagai berikut:

1. Pada audio sebelum dilakukan proses dekomposisi wavelet dilakukan proses segmentasi terlebih dahulu. Hal ini bertujuan untuk membagi panjang sinyal yang awalnya sangat panjang menjadi sinyal yang memiliki panjang lebih pendek sehingga mudah untuk dilakukan proses analisis. Segmentasi dilakukan dengan cara membagi jumlah frekuensi sampling pada audio dengan *frame per second* pada video.
2. Setelah dilakukan proses segmentasi kemudian dilakukan proses *Discrete Wavelet Packet Transform* dengan menggunakan *mother wavelet haar* pada setiap *frame* di audio. Dimana sinyal di dekomposisikan menjadi beberapa level. Semakin banyak level maka akan menghasilkan subband semakin banyak. Masing-masing subband pada level yang lebih tinggi akan di dekomposisikan menjadi subband baru sehingga menghasilkan range frekuensi yang lebih kecil. Pada penelitian ini dilakukan dekomposisi hingga level ke enam dikarenakan range frekuensi yang akan dianalisis yaitu dari 300s/d 3400 hz.
3. Setelah itu dilakukan perhitungan energi pada setiap subband pada range frekuensi tersebut, kemudian mencari nilai rata-rata energi setiap frame dari subband terpilih. Setelah itu membandingkan nilai energi rata-rata pada setiap frame dengan *thresholding* yang telah ditentukan. *Thresholding* yang digunakan adalah 0.5 dari energi maksimum. Maka apabila frame yang memiliki nilai energi rata-rata lebih besar dari *thresholding* yang ditentukan maka frame tersebut terpilih. Selanjutnya frame terpilih pada audio akan disesuaikan pada video.

Selanjutnya proses yang dilakukan pada video yaitu menyisipkan pesan rahasia sesuai frame yang terpilih pada audio, pesan disisipkan dengan menggunakan metode *Enhanced Least Significant Bit*. Sebelum disisipkan pesan diubah kedalam bentuk ASCII yang mewakili nilai desimal kemudian diubah menjadi bentuk bit-

bit, Setelah itu baru dilakukan proses ELSB. Sebelum pesan dikirimkan dilakukan penyisipan kunci pada frame pertama yang berisi panjang pesan dan frame yang tersisipi pesan rahasianya. Tujuan disisipkan kunci adalah agar pihak penerima dapat langsung mengetahui pada frame mana pesan disisipkan tanpa harus melakukan pendeteksian pada audio.

Kemudian pada penerima berdasarkan **Gambar 2.b**, proses yang terjadi di pihak penerima agar dapat mengekstrak isi pesan tersebut yaitu, pada pihak penerima melakukan ekstraksi pesan hanya tinggal melihat informasi kunci pada frame pertama tanpa perlu melakukan pendeteksian pada bagian audio. Setelah itu pihak penerima mengekstraksi pesan dengan menggunakan ELSB. Setelah di dapat informasi bit pesan kemudian diubah ke dalam bentuk desimal yang mewakili nilai ASCII. Maka di dapatkan isi pesan rahasia yang telah disembunyikan.

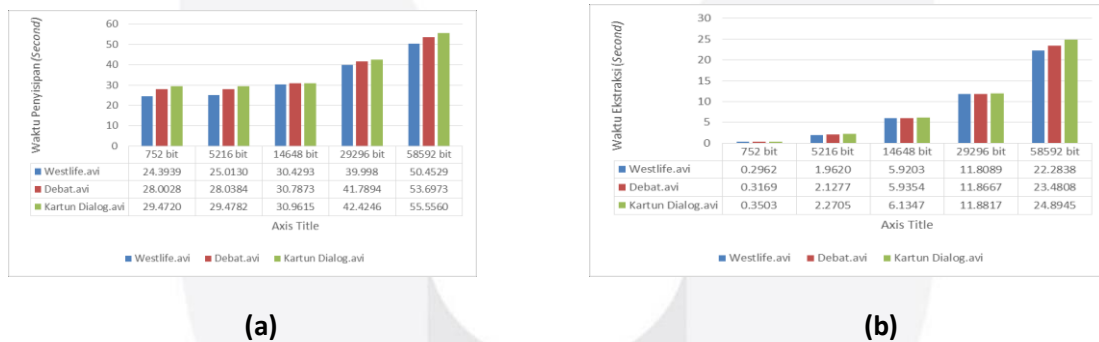
.4. Pembahasan

Pengujian yang akan dilakukan pada sistem steganografi yang dirancang pada tugas akhir ini yaitu menggunakan video sebagai cover dan pesan rahasia (teks) dengan ukuran panjang pesan 752 bit, 5216 bit, 14648 bit, 29296 bit dan 58592 bit. Video cover yang akan digunakan (180x150), (320x240), (400x340)

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

A. Sistematika Pengukuran

Panjang pesan yang akan disisipkan dan ukuran cover pada video sangat berpengaruh terhadap waktu komputasi. Pengujian dilakukan dengan rentang frekuensi 300-3400 Hz dan dipilih nilai threshold sebesar 0.5 dari energi maksimum dengan menyisipkan pesan yaitu 752 bit, 5216 bit, 14648 bit, 29296 bit dan 58592 bit. Berikut grafik waktu komputasi yang di dapat dari proses penyisipan dan ekstraksi dengan panjang pesan dan ukuran cover berbeda dari setiap cover video. Hasil Pengukuran:



Gambar 4 (a) Pengaruh panjang pesan terhadap waktu penyisipan (b) Tabel pengaruh panjang pesan terhadap waktu ekstraksi.

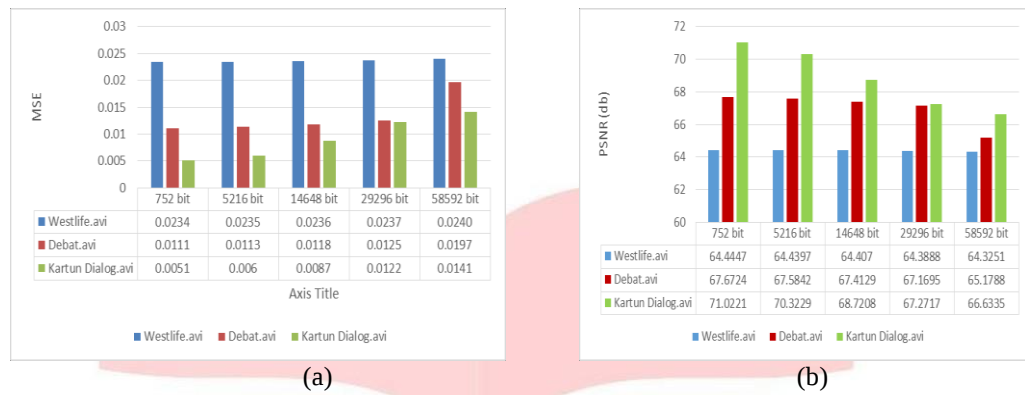
B. Analisis Hasil Pengukuran

Berdasarkan data yang di dapat pada **Gambar 4a** dan **Gambar 4b** ukuran panjang pesan sangat mempengaruhi berapa lama waktu komputasi yang dibutuhkan sistem untuk melakukan proses dari awal sampai dengan selesai. Semakin panjang ukuran pesan yang disisipkan maka akan semakin lama waktu yang di butuhkan dalam proses penyisipan dan ekstraksi. Selain itu juga ukuran cover mempengaruhi waktu komputasi dalam penyisipan dan ekstraksi. Semakin besar ukuran cover maka membutuhkan waktu yang semakin lama juga.

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

A. Sistematika Pengukuran

Selanjutnya setelah dilakukan pengujian waktu komputasi berdasarkan pengaruh panjang pesan dan ukuran cover, maka dilakukan pengujian pengaruh perbedaan pesan dan ukuran cover terhadap MSE dan PSNR. Pada pengujian ini akan dilakukan perbandingan dari tiga video, video pertama memiliki ukuran (180x150), video kedua (320x240), video ketiga (400x340). Berikut Hasil Pengukuran :



Gambar 5a Hasil Pengukuran MSE dan **5b** Hasil Pengukuran PSNR

B. Analisis Hasil Pengukuran

Berdasarkan **Gambar 5a** dan **Gambar 5b** ukuran pesan yang akan disisipkan memiliki panjang yang berbeda. Semakin panjang pesan yang akan disisipkan, maka akan berpengaruh terhadap nilai MSE nya yaitu nilai yang di dapat akan semakin besar, selain itu semakin besar ukuran *frame* video maka semakin kecil tingkat kesalahan yang didapatkan sehingga menghasilkan nilai MSE yang semakin kecil. Sementara apabila nilai MSE yang di dapat semakin kecil maka akan menghasilkan nilai PSNR yang semakin besar tetapi jika nilai MSE nya semakin besar maka didapatkan nilai PSNR yang semakin kecil.

C. Pengaruh Panjang Pesan dan Ukuran Cover terhadap BER dan CER

Setelah dilakukan beberapa pengujian tanpa *noise*, di dapatkan nilai CER dan BER sama dengan 0. Hal ini menunjukkan bahwa tidak ada perbedaan nilai atau hasil antara pesan asli sebelum dilakukan penyisipan dengan pesan setelah dilakukan ekstraksi.

Tabel 4a Hasil Pengujian terhadap nilai BER

Nama File Video	Ukuran Pesan	BER	CER
Westlife.avi	752 bit	0	0
	5216 bit	0	0
	14648 bit	0	0
	29296 bit	0	0
	58592 bit	0	0
Debat .avi	752 bit	0	0
	5216 bit	0	0
	14648 bit	0	0
	29296 bit	0	0
	58592 bit	0	0
Kartun Dialog.avi	752 bit	0	0
	5216 bit	0	0
	14648 bit	0	0
	29296 bit	0	0
	58592 bit	0	0

D.Menguji Ketahanan Sistem terhadap Serangan Noise

A.Sistematika Pengukuran

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 1×10^{-7} sampai 8×10^{-7} . 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 752 bit . Berikut adalah hasil pengukuran yang telah diberikan noise .

Tabel 4b Pengaruh Noise Gaussian saat diberikan mean=0

Mean = 0	Variansi Noise Gaussian	MSE	PSNR	BER	CER
	0.0000001	0.00513896	71.0221	0	0
	0.0000002	0.00514909	71.0135	0	0
	0.0000003	0.00542861	70.7839	0	0
	0.0000004	0.0067756	69.8213	0	0
	0.0000005	0.00984832	68.1972	0.00132979	0.010638
	0.0000006	0.014805	66.4267	0.00265957	0.021277
	0.0000007	0.0213851	64.8297	0.00930851	0.074468
	0.0000008	0.0292673	63.467	0.00664894	0.053191

Tabel 4c Pengaruh Noise Gaussian saat diberikan mean=0.001

Mean = 0.001	Variansi Noise Gaussian	MSE	PSNR	BER	CER
	0.0000001	0.00631771	70.1252	0	0
	0.0000002	0.0209385	64.9213	0.00265957	0.021277
	0.0000003	0.044672	61.6304	0.0159574	0.12766
	0.0000004	0.0691731	59.7314	0.0279255	0.21277
	0.0000005	0.0919664	58.4945	0.272606	0.93617
	0.0000006	0.112216	57.6303	0.0465426	0.29787
	0.0000007	0.130169	56.9857	0.0345745	0.26596
	0.0000008	0.146352	56.4768	0.0531915	0.39362

B Analisis Hasil Pengukuran

Berdasarkan **Tabel 4b** dan **Tabel 4c** besarnya variansi akan mempengaruhi besarnya jangkauan noise tersebut. Dari Tabel di atas terlihat semakin besar nilai variansi maka akan menghasilkan nilai PSNR yang semakin kecil. Hal ini disebabkan karena semakin besar jangkauan noise Gaussian yang diberikan maka piksel yang berubah semakin banyak sehingga mengakibatkan nilai PSNR semakin menurun . Pada pengujian ketahanan sistem ini yaitu diujikan dengan dua nilai mean yaitu ketika *mean* nya sama dengan 0 dan ketika *mean*nya sama dengan 0.001. *Mean* dapat diartikan sebagai power atau kekuatan dari *noise* tersebut . Semakin besar nilai *mean* nya semakin kuat juga noise menyerang. Pada data table terlihat semakin besar nilai *mean*nya maka ketahanan sistem terhadap suatu noise berkurang. Saat *mean* nya sama dengan 0 sistem dapat tahan terhadap noise hingga variansi 4×10^{-7} . Pada data table terlihat semakin besar nilai *mean*nya maka ketahanan sistem terhadap suatu noise berkurang. Saat *mean* nya sama dengan 0 sistem dapat tahan terhadap noise hingga variansi 4×10^{-7} . Sedangkan saat nilai *mean* diubah menjadi 0.001 sistem hanya tahan pada variansi 1×10^{-7}

E.Mean Opinion Score (MOS)

Pengujian selanjutnya dilakukan dengan menggunakan parameter MOS, pengujian ini dilakukan untuk mengetahui kualitas *video stego* jika diberikan input panjang pesan rahasia yang berbeda yaitu 752 bit, 5216 bit,

14648 bit, 29296bit dan 58592 bit. Pengujian ini bersifat subjektif didasarkan pada pengamatn visual manusia. Dari hasil survet MOS didapatkan hasil sebagai berikut:

Tabel 4d Hasil Pengujian Nilai rata-rata MOS

File Video	752 bit	5216 bit	14648 bit	29296 bit	58592 bit
Westlife.avi	4.2	4.1667	3.9667	3.9	3.8333
Debat.avi	4.1333	4.06667	4	3.8667	3.66667
Kartun Dialog.avi	4.2667	4.1667	4.1667	3.8667	3.7

Berdasarkan data **Tabel 4d** maka dapat disimpulkan nilai yang didapatkan adalah baik ,itu artinya sistem yang dirancang memiliki kualitas baik. Karena diperoleh nilai rata-rata MOS 3.99778

5. Kesimpulan

Berdasarkan pengujian yang telah dilakukan ,dapat disimpulkan bahwa, ukuran panjang pesan mempengaruhi waktu komputasi pada saat proses penyisipan dan ekstraksi .Dari hasil penelitian didapatkan untuk menyisipkan pesan 752 bit,5216 bit,14648 bit,29296 bit,58592 bit ke dalam *frame* ukuran 180x150. Waktu komputasi tercepat yang dibutuhkan 24.3939 detik untuk proses penyisipan pesan dan 0.2962 untuk proses ekstraksi. Keberhasilan sistem saat menghasilkan *stego video* memiliki nilai PSNR yang baik dipengaruhi oleh ukuran panjang pesan yang disisipkan pada *video cover*. Semakin sedikit pesan yang disisipkan maka nilai PSNR akan semakin besar. Selain itu nilai PSNR juga dipengaruhi oleh *video cover* , semakin besar ukuran *cover video* maka akan semakin besar nilai PSNR nya. PSNR tertinggi dalam penelitian ini adalah 71.0221. Nilai MSE juga akan bertambah besar jika pesan yang disisipkan bertambah panjang. Semakin besar nilai MSE itu artinya semakin buruk karena terlihat perbedaan antara video asli dengan video yang sudah di steganokan. MSE terendah pada penelitian ini adalah 0.0051. Sistem yang telah dibuat masih sangat lemah terhadap serangan *noise* . Hal tersebut dapat dilihat dari hasil pengujian saat diserang dengan *Gaussian Noise* didapatkan nilai MSE yang besar dan nilai PSNR yang kecil. Karena sistem hanya tahan pada variansi 4×10^{-7} saat *mean* sama dengan 0 dan hanya 1×10^{-7} saat *mean* 0.001 dengan nilai MSE terendah yaitu 0.00513896 dan PSNR tertinggi yaitu 71.0221.

Daftar Pustaka

- [1] Wahid, Muhammad Luthfi.2015."Analisis dan Simulasi Steganografi Video Berbasis Deteksi Band Frekuensi Menggunakan Metode Discrete Wavelet Transfor".Fakultas Teknik Elektro ,Universitas Telkom
- [2] Illiadi,Neng Anggi .2015."Steganografi Enhanced Least Significant Bit Pada Karakter Khusus Citra Tulisan Arab".Fakultas Teknik Elektro ,Universitas Telkom.
- [3] Malik,Afwan Levianto.2007."Steganografi Video pada File Berformat Audio Video Interleave Menggunakan Metode Transformasi Wavelet Diskrit".Jurusan Teknik Informatika ,Sekolah Tinggi Teknologi Telkom,Bandung.
- [4] Munir.Rinaldi.2006.Kriptografi.Bandung :Penerbit Informatika
- [5] Saputra,Nanang .2010."Perancangan Sistem Pengenalan Pembicara pada Text Dependent menggunakan Overlapping Dekomposisi Wavelet Packet Transform dan Jaringan Syaraf Tiruan Propagasi Balik".Departemen Teknik Informatika ,Institut Teknologi Telkom .