ANALISIS DAN SIMULASI STEGANOGRAFI VIDEO MENGGUNAKAN METODE *WAVELET* PADA *FRAME* YANG DIPILIH BERDASARKAN DETEKSI FASA

Analysis And Simulation Of Video Steganography Using Wavelet Method In Selected Frame Based On Phase Detection

Amelia Shaffira Arifin[1], Bambang Hidayat[2], I Nyoman Apraz Ramatryana[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]ameliashaffira@students.telkomuniversity.ac.id, [2]bhidayat@telkomuniversity.ac.id,
[3]ramatryana@gmail.com

Abstrak

Dalam tugas akhir ini, dibuat sistem steganografi untuk menyisipkan pesan rahasia (.txt) pada video (.avi) . Metode yang digunakan untuk menyisipkan pesan adalah Discrete Wavelet Transform (DWT), dilakukan dengan cara mengganti nilai koefisien yang dibawah nilai threshold dengan pesan rahasia. Penyisipan pesan dilakukan pada gambar saat terdeteksi fasa yang terpilih dengan menggunakan proses Fast Fourier Transform (FFT) yang merupakan realisasi dari proses DFT.

Parameter yang digunakan sebagai pengujian Video Steganografi seperti: Waktu Komputasi, BER, CER, MSE, PSNR dan MOS. Hasil yang diperoleh adalah sistem steganografi dengan waktu komputasi tercepat 2,9450 detik pada saat penyisipan dan 0,1782 detik pada saat ekstraksi. Untuk nilai MSE 0,0309 dan nilai PSNR mencapai 63,2293 dB dengan BER dan CER yang sama yaitu 0 saat tidak ada serangan noise Gaussian. Sistem steganografi yang dibuat tahan terhadap serangan noise Gaussian pada citra dengan nilai mean=0 hingga variansi 1x10-4, saat diberikan variansi 1x10-2 BER nya menjadi 0,4695. Hasil MOS yang didapatkan dari survey terhadap 30 koresponden memiliki nilai rata-rata total 3,62 yang berarti kualitas video yang tersisipi adalah cukup baik.
Kata kunci: Steganografi, DWT, Fasa, DFT

Abstract

In this final task, created a system of steganography to insert messages (.txt) on the video (.avi) . The method used to embeed messages is a Discrete Wavelet Transform (DWT), replacing the value of coefficient below threshold value with a secret message. Insertion of message is performed on image when the selected phase was detected by using the process of Fast Fourrier Transform (FFT) which is realization of DFT.

The parameters used as testing Video Steganography such as : Time computing, BER, CER, PSNR, MSE and MOS. The result of Steganography system with fastest computing time of 2.9450 seconds when embedding and 0.1782 seconds when extracting. MSE values for 0.0309 and the PSNR value reach 63.2293 dB, with BER and CER the same vakue is 0 when there is no attack noise Gaussian. A steganography system is resistant to attacks on the image with a Gaussian noise mean = 0 until variansi 1x10-4, when the system attack with variance 1x10-2 the value of BER is 0.4695. The results obtained from surveys of the MOS against 30 correspondents have the average value of the total 3.62 which means the stego video quality is pretty good.
Keywords: Steganography, DWT, Phase, DFT

1. Pendahuluan

Seiring berkembangnya pertukaran informasi melalui media digital, keamanan dan kerahasiaan data merupakan hal yang sangat penting. Dalam beberapa kasus pertukaran informasi, pihak yang berkirim pesan menginginkan pesan tersebut terjamin kerahasiannya sampai pada pihak penerima, walaupun mereka mamanfaatkan internet. Perlindungan keamanan dan kerahasiaan data digital diperlukan suatu teknik untuk mengamankan data tersebut, salah satunya dengan steganografi. Metode ini diharapkan dapat mengurangi terjadinya pencurian dan penyalahgunaan data sehingga data yang dikirimkan dapat sampai kepada penerima dengan aman. Pada tugas akhir ini, dibuat sistem steganografi untuk menyisipkan pesan rahasia (.txt) pada video (.avi) . Metode yang digunakan untuk menyisipkan pesan adalah Discrete Wavelet Transform (DWT), dilakukan dengan cara mengganti nilai koefisien yang dibawah nilai threshold dengan pesan rahasia. Penyisipan pesan

dilakukan pada gambar saat terdeteksi fasa yang terpilih dengan menggunakan proses Fast Fourier Transform (FFT) yang merupakan realisasi dari proses DFT.

2. Landasan Teori

A. Steganografi

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyaari bahwa ada suatu pesan rahasia. Kata steganografi berasal dari bahasa Yunani "*steganos*" yang artinya tersembunyi atau terselebung, dan "*graphein"* yang artinya menulis. [1]. Pada umumnya terdapat dua proses di dalam steganografi, yaitu proses penyisipan pesan rahasia dan proses ekstraksi untuk mendapatlan kembali pesan rahasi tersebut.

B. Video [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.

C. Discrete Wavelet Transform (DWT) [3]

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).

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.

(a) (b)

Gambar 1 (a) DWT Level 1 [3] **(b) DWT Level 2** [3]

D. Discrete Fourrier Transform (DFT) [4]

Pada proses ini dilakukan proses Fast Fourier Transform (FFT) yang merupakan realisasi dari proses DFT yaitu mentransformasikan sinyal dari domain waktu ke domain frekuensi untuk mempermudah perhitungan. Berikut rumus untuk menghitung FFT:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-\frac{j2\pi kn}{N}}$$

k = 1,2,3,….N-1

N =jumlah titik FFT

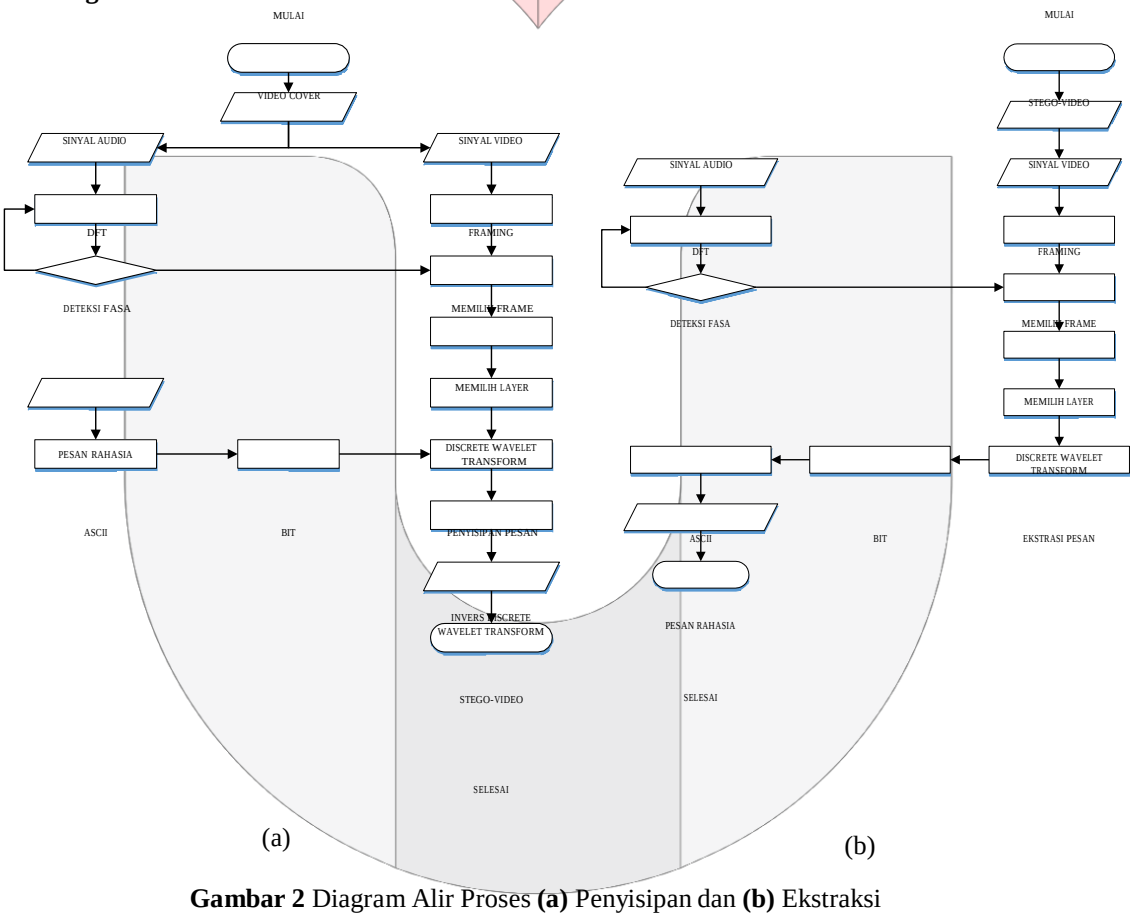
E. Parameter Pengujian [2]

1. *Mean Square Error* (MSE)

Mean Square Error adalah parameter yang digunakan untuk menganalisi 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.

2. *Peak Signal to Noise Ratio* (PSNR)
   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.
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.
4. *Character Error Rate* (CER)
   Character Error Rate (CER) adalah perbandingan jumlah karakter yang *error* dengan total karakter. CER merupakan parameter pengujian yang digunakan untuk melihat kualitas pesan yang disisipkan.
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)
   Pengujian ini dilakukan dengan membandingkan kualitas 2 video, video asli dengan yang sudah disisipi pesan. Nilai yang digunakan pada MOS adalah dari 1 yang paling rendah dan 5 yang paling tinggi.

3. Perancangan Sistem



Gambar 2 Diagram Alir Proses **(a)** Penyisipan dan **(b)** Ekstraksi

Berdasarkan gambar 2 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 video berformat .avi dengan metode *Discrete Wavelet Transform*. Penyisipan dilakukan pada frame yang terdeteksi fasa menggunakan *Discrete Fourrier Transform*. Keluaran dari proses penyisipan ini berupa video-stego dimana terdapat pesan rahasia yang telah disispkan. Kemudian video-stego dikirim ke penerima. Di sisi penerima dilakukan proses ekstraksi dengan bantuan stego-*key* untuk mengembalikan pesan rahasia berupa file teks dengan format .txt.

4. Pembahasan

Pengujian sistem steganografi yang dirancang pada Tugas Akhir ini dilakukan dengan menggunakan 4 buah video sebagai cover dengan format .avi dan 5 pesan yang berbentuk teks dengan format .txt .

Pada tabel 2 (a) merupakan spesifikasi video sebagai cover dan pada tabel 2 (b) merupakan spesifikasi pesan rahasia yang akan digunakan pada percobaan kali ini.

Tabel 1 (a) Video *Cover* dan (b) Pesan

No.	Cover Video	Durasi Video	Resolusi Video	Jumlah Frame
1	kartun_1.avi	00:00:10	320x240	301
2	kartun_2.avi	00:00:10	640x480	301
3	surat_1.avi	00:00:10	320x240	301
4	surat_2.avi	00:00:10	640x480	301

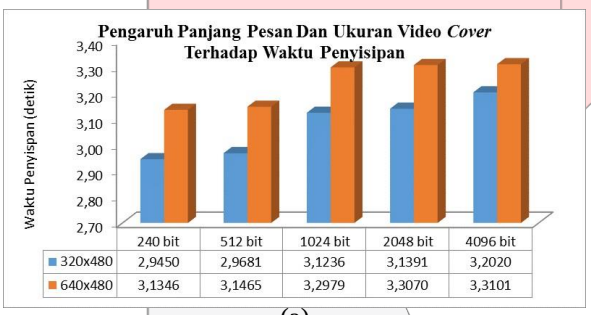
(a)

No.	Nama File	Ukuran (bit)
1	1.txt	240
2	2.txt	512
3	3.txt	1024
4	4.txt	2048
5	5.txt	4096

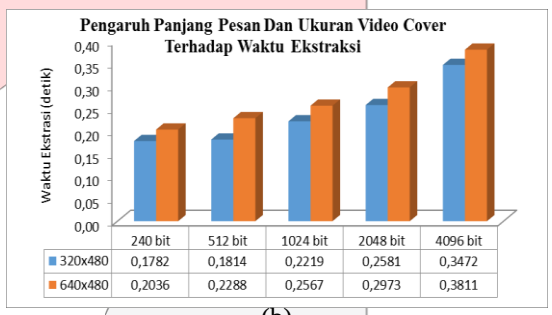
(b)

A. Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap Waktu Komputasi

Pengujian ini dilakukan dengan menyisipkan pesan sepanjang 240 bit, 512 bit, 1024 bit, 2048 bit dan 4096 bit pada video cover. Video cover yang digunakan adalah kartun_1.avi dan kartun_2.avi .



(a)



(b)

Gambar 3 (a) Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap Waktu Penyisipan (b) Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap Waktu Ekstraksi

Grafik diatas menunjukkan pada cover video 640x480, penyisipan 4096 bit membutuhkan waktu komputasi hingga 3,3101 detik untuk proses penyisipan dan 0,3811 detik untuk ekstraksi. Sementara untuk panjang pesan 184 bit waktu penyisipan yang dibutuhkan hanya 3,1346 detik dan 0,2036 untuk ekstraksi. Dari hasil pengujian tersebut dapat dilihat bahwa semakin besar data yang disisipkan, maka semakin lama waktu komputasinya ketika penyisipan dan ekstraksi. Hal ini disebabkan semakin panjang pesan maka semakin banyak bit yang akan disisipkan, sehingga sistem membutuhkan waktu yang lebih lama untuk melakukan proses tersebut. Selain itu, semakin besar ukuran video cover maka semakin lama juga waktu komputasi yang diperlukan. Pesan dengan panjang 1024 bit disisipkan pada video dengan ukuran 320 x 240 membutuhkan waktu 3,1236 detik untuk penyisipan dan 0,2219 detik untuk ekstraksi. Sementara itu video dengan ukuran 640 x 480 membutuhkan waktu yang lebih lama yaitu 3,2979 detik untuk penyisipan dan 0,2567 detik untuk ekstraksi.

B. Pengaruh Jenis Video *Cover* Terhadap Daya Tampung Penyisipan

Pada pengujian ini dilakukan penyisipan pada 2 jenis video cover yang berbeda, kartun dan surat dengan panjang yang sama yaitu 10 detik dan jumlah frame total adalah 301.

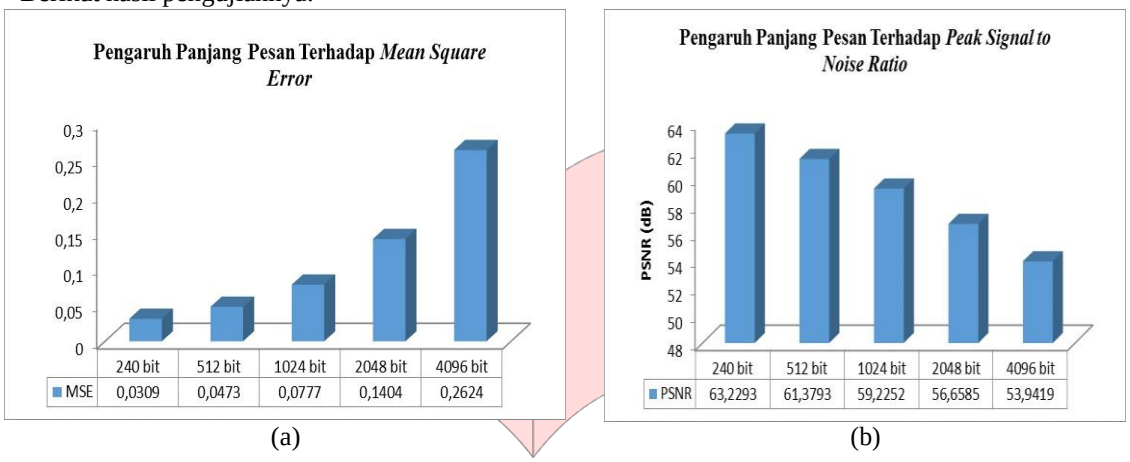
Tabel 2 Jenis Video Cover Terhadap Daya Tampung Penyisipan

No.	Jenis Video	Jumlah Frame	Selected Frame
1	kartun	301	199
2	surat	301	237

Berdasarkan tabel diatas , apat diketahui bahwa jenis video mempengaruhi jumlah daya tampung penyisipan pesan karena masing-masing video *cover* memiliki daya tampung yang berbeda tergantung dari seberapa banyak terdapat fasa 0 derajat yang terdeteksi dengan menggunakan DFT.

C. Pengaruh Panjang Pesan Terhadap MSE dan PSNR

Pengujian kali ini,menggunakan video kartun dengan ukuran 640 x 480, dan juga dengan menyisipkan pesan rahasia sepanjang sepanjang 240 bit, 512 bit, 1024 bit, 2048 bit dan 4096 bit pada video cover. Berikut hasil pengujiannya:



(a) (b)

Gambar 4 (a) Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap MSE (b) Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap PSNR

Berdasarkan Gambar 4 (a) diatas, pesan yang disisipkan dan ukuran video dapat mempengaruhi nilai MSE. Semakin panjang pesan yang disisipkan maka semakin besar nilai MSE dan semakin besar ukuran video *cover* semakin besar pula nilai MSE yang didapat. Hal itu menunjukkan bahwa tingkat kemiripan video *cover* video stego semakin kecil dan tingkat kesalahan yang terjadi pada video *stego* meningkat. Sementara itu Gambar 4 (b) menunjukkan bahwa semakin panjang pesan yang disisipkan maka semakin kecil nilai PSNR. Nilai MSE berbanding balik dengan nilai PSNR. Semakin besar nilai MSE, maka semakin kecil nilai PSNR yang diperoleh, begitu pula sebaliknya. Semakin kecil nilai MSE maka semakin besar nilai PSNR yang diperoleh.

D. Pengaruh Panjang Pesan dan Ukuran Video *Cover* Terhadap Akurasi Pesan Terekstraksi

Pada pengujian ini dilakukan pada semua jenis video *cover* dengan menyisipkan pesan rahasia sepanjang 240 bit, 512 bit, 1024 bit, 2048 bit dan 4096 bit pada masing-masing video.

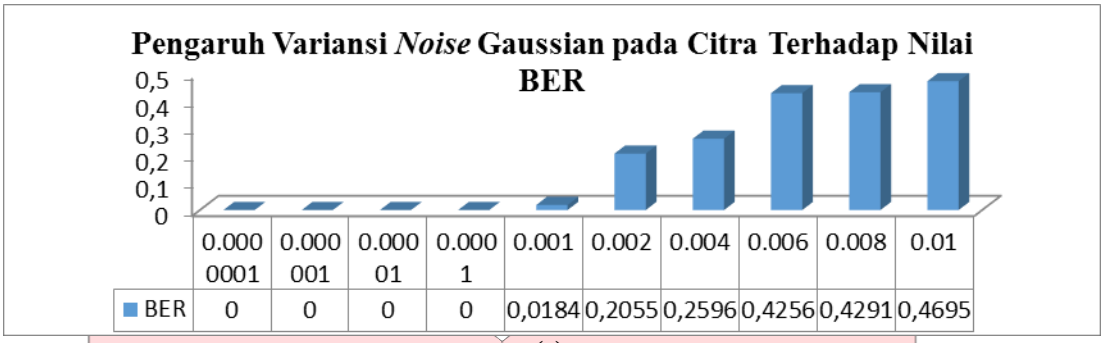
Nilai akurasi pesan terekstraksi pada sistem tetap 100% walaupun ukuran video *cover* dan panjang pesan berbeda-beda. Semakin besar ukuran video *cover* semakin banyak pula pesan yang dapat disisipkan, tetapi hal tersebut tidak mempengaruhi tingkat akurasi pesan terekstraksi.

E. Hasil Pengujian Terhadap Nilai BER dan CER

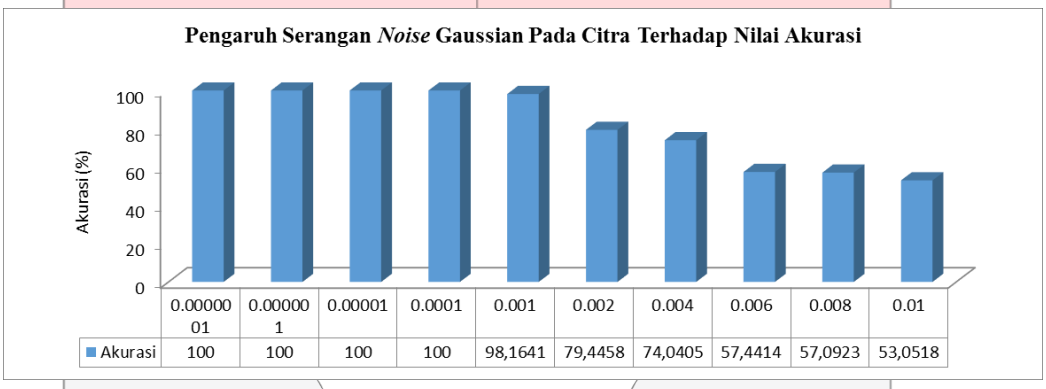
Setelah melakukan beberapa pengujian tanpa serangan *noise*, didapatkan nilai BER=0 dan CER=0. Hal ini menunjukkan bahwa tidak ada perbedaan nilai antara pesan asli sebelum disisipkan dengan pesan yang telah didapat saat proses ekstraksi.

F. Pengaruh Serangan *Noise* Gaussian Terhadap Nilai BER dan Akurasi

Pada pengujian ini ditambahkan noise Gaussian pada citra yang dilakukan pada saat mean=0 dengan variansi 1x10-7 sampai 1x10-1 pada video cover kartin_2.avi ukuran 640x480 yang telah disipi pesan seanjang 4096 bit. Hasil yang diperoleh adalah seperti pada tabel berikut ini :



(a)



(b)

Gambar 5 (a) Pengaruh *Noise* Gaussian pada Citra Terhadap BER (b) Pengaruh *Noise* Gaussian pada Citra Terhadap Akurasi

Pengujian dilakukan dengan menyisipkan pesan dengan panjang 4096 bit pada video *cover* ukuran 640x480. Pada Gambar 5 (a) terlihat bahwa sistem dengan serangan *noise* Gaussian tahan hingga variansi $1x10^{-4}$ dengan nilai BER yang tidak sama dengan nol. Semakin besar nilai variansi *noise* Gaussian yang diberikan, maka kualitas video akan semakin buruk karena semakin banyak piksel yang berubah. Hal ini disebabkan karena jangkauan *noise* Gaussian yang semakin lebar. Hal tersebut juga ditunjukkan pada Gambar 4 (b) yaitu akurasi 100% hanya sampai pada variansi $1x10^{-4}$.

G. Uji Parameter MOS

Pengujian parameter MOS yang dilakukan bertujuan untuk melihat kualitas vide-stego jika diberi sisipan pesan dengan panjang yang berbeda. Panjang pesan yang disisipkan yaitu sepanjang 240 bit, 512 bit, 1024 bit, 2048 bit dan 4096 bit. Video *cover* yang digunakan memiliki ukuran 320 x 240 dan 640 x 480.

Setelah melalukan survey terhadap 30 koresponden, didapatkan nilai rata-rata MOS sebagai berikut.

Tabel 3 Nilai Rata-rata MOS Terhadap Video Cover

Ukuran Video	320x240					640x480				
Panjang Pesan (bit)	240	1840	4472	6776	8064	240	1840	4472	6776	8064
Rata - Rata Nilai MOS	4,3333	3,8333	3,3667	3,1	3,0333	4,4	3,9333	3,6333	3,4	3,1667

Berdasarkan Tabel 3 diatas, diperoleh nilai rata-rata MOS video keseluruhan sebesar 3,62. Dari survey yang dilakukan dapat dilihat bahwa sistem steganografi yang dirancang memiliki kualitas cukup baik.

5. Kesimpulan

Dari hasil analisis pada pengujian didapatkan bahwa sistem yang dibuat mampu melakukan proses steganografi video menggunakan DWT dengan pemilihan frame berdasarkan deteksi fasa dengan baik. Berdasarkan tabel diatas, Panjang pesan dan ukuran video *cover* mempengaruhi waktu komputasi pada saat proses penyisipan dan ekstraksi pesan. Semakin panjang pesan yang disisipkan dan semakin besar ukuran video *cover*

yang digunakan maka semakin lama waktu komputasi yang dibutuhkan untuk melakukan proses penyisipan dan ekstraksi pesan. Hasil yang diperoleh adalah sistem steganografi dengan waktu komputasi tercepat 2,9450 detik pada saat penyisipan dan 0,1782 detik pada saat ekstraksi. Untuk nilai MSE 0,0309 dan nilai PSNR mencapai 63,2293 dB dengan BER dan CER yang sama yaitu 0 saat tidak ada serangan noise Gaussian. Sistem steganografi yang dibuat tahan terhadap serangan noise Gaussian pada citra dengan nilai mean=0 hingga variansi $1x10^{-4}$. Hasil MOS yang didapatkan dari survey terhadap 30 koresponden memiliki nilai rata-rata total 3,62 yang berarti kualitas video yang tersisipi adalah cukup baik.

Daftar Pustaka:

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

[4] J. W. Cooley dan J. W. Tukey. "Analgorithm for the machine calculation of complex Fourier series". Mathematics of Computation, 19:297-301, 1965