STEGANOGRAFI VIDEO DENGAN PENYISIPAN PESAN RAHASIA MENGUNAKAN TEKS PADA FRAME VIDEO BERBASIS SSB-4 DAN DISCRETE COSINE TRANSFORM (DCT)

VIDEO STEGANOGRAPHY WITH SECRET MESSAGES USING TEXT ON SSB-4 AND DISCRETE COSINE TRANSFORM (DCT) BASED ON VIDEO FRAME

Satrio Ardhimasetyo[1], Iwan Iwut Tritoasmoro, S.T.,M.T.[2], Nur Ibrahim, S.T.,M.T.[3]

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
satrioardhimasetyo@student.telkomuniversity.ac.id,

Abstrak

Seiring dengan perkembangan pertukaran informasi yang semakin lama semakin membutuhkan privasi, maka keamanan dan kerahasiaan sebuah pesan informasi sangat perlu diperhatikan. Maka dari itu diperlukan suatu cara untuk menyisipkan pesan yang membawa informasi kedalam media *cover* tertentu contohnya audio dan video, cara tersebut salah satunya menggunakan steganografi. Media yang digunakan pada Tugas Akhir ini video berformat AVI untuk format penyimpanan video setelah dilakukan proses penyisipan dan pesan yang akan disisipkan kedalam video berupa teks.

Pada Tugas Akhir ini menggunakan pesan teks rahasia yang akan di input ke dalam video host yang dilakukan dengan metode SSB-4 dan DCT sebagai penentuan lokasi dimana akan disisipkan pesan tersebut. SSB-4 merupakan metode yang dilakukan dengan mengubah bit ke 4 dari citra *cover* akan digantikan oleh bit pesan dan memodifikasi bit-bit *reminder* (yang ada pada bit ke 1,2,3 dan 5). Metode DCT digunakan energinya sebagai penentuan *frame* terpilih.

Nilai parameter terbaik yaitu pada video berukuran 720p dengan pesan yang disisipkan sebanyak 233 karakter, nilai yang didapatkan setelah dilakukan proses penyisipan pesan dan ekstraksi pesan menghasilkan nilai MSE = 0,048, PSNR = 61,256, BER = 0, dan CER = 0. Metode penyisipan menggunakan SSB-4 dan DCT sebagai penentuan *frame* terpilih terbukti tahan terhadap gangguan *Gaussian Blur* dengan nilai BER = 0 dan CER = 0 saat menggunakan video berukuran 360p dan 720p dengan pesan yang disisipi sebanyak 233 karakter.

Kata Kunci : Steganografi video, PSNR, MSE, BER, CER.

Abstract

Along with the development of information exchange that increasingly requires privacy, the security and confidentiality of an information message are very important. So from that, we need a way to insert messages that bring information into certain media coverings, for example, audio and video one of which uses steganography. The media used in this Final Project is AVI format video for video storage format after the insertion process and the message will be inserted into the video in the form of text.

In this Final Project use secret text messages that will be input into the video host which is done by the SSB-4 and DCT methods as a determination of the location where the message will be inserted. SSB-4 is a method that is done by changing the 4th bit of the cover image to be replaced by the message bit and modifying the reminder bits (which are in bits to 1,2,3 and 5). The DCT method uses its energy to determine the selected frame .

The best parameter value is in 720p video with 233 characters inserted, the value obtained after message insertion and message extraction results in MSE = 0.048, PSNR = 61.256, BER = 0, and CER = 0. Insertion method uses SSB -4 and DCT as the determination of selected frames proved to be resistant to Gaussian Blur interference with BER = 0 and CER = 0 when using 360p and 720p videos with 233 characters inserted messages.

Keywords : Video Steganography, PSNR, MSE, BER, CER.

1. Pendahuluan

Cara untuk melindungi data maupun informasi yang dimiliki oleh seseorang memiliki banyak cara, salah satunya yaitu dengan teknik steganografi. Arti dari steganografi yaitu tindakan komunikasi rahasia, yang berarti bahwa hanya pengirim, dan penerima yang sadar akan komunikasi rahasia. Untuk mencapai semua itu, pesan rahasia disembunyikan di dalam komunikasi yang tidak tampak ,yang dikenal sebagai teks terselubung. Bagi orang lain, jelas bahwa melakukan komunikasi, tetapi gabungan dari teks terselubung dan pesan

tersembunyi membuat pesan tersebut seperti tidak melakukan komunikasi, itulah yang disebut sebagai teks steganografi atau karya steganografi [1].

Banyak metode steganografi video yang dapat digunakan untuk diimplementasikan dalam video, tetapi metode yang digunakan dalam Tugas Akhir ini adalah teknik *System of Steganography using* Bit 4 (SSB-4) dan *Discrete Cosine Transform* (DCT). *System of Steganography using* Bit 4 (SSB-4) merupakan teknik penyembunyian data yang bekerja pada domain spasial [1]. Pada penelitian [2], menggunakan metode SWT dengan teknik LSB-DCT dengan melakukan pengujian pesan beserta cover tanpa menggunakan compressive sensing dan pengujian performansi sistem dengan menggunakan *compressive sensing* [2]. Pada jurnal [3], peneliti tersebut melakukan implementasi dan analisis steganografi pada video berformat AVI dengan menggunakan metode LSB dan SSB-4 dengan melakukan pengujian ketahanan sistem steganografi saat diberikan *rescaling* dan *gaussian blur* [3]. Masalah terbesar pada steganografi ini adalah bagaimana agar video stego yang sudah diberikan gangguan tidak rusak baik dari sisi video maupun dari sisi pesan teks yang terdapat di dalamnya.

Pada penelitian ini akan digunakan metode SSB-4 sebagai proses untuk penyisipan dan proses ekstraksi, kemudian untuk penentuan posisi *frame* mana saja yang akan disisipi pesan teks menggunakan metode DCT dengan menentukan dari audio video. Video yang akan di masukan pesan berukuran 360p dan 720p dengan pesan sebanyak 233 karakter dan 1411 karakter.

Tabel 1. Hasil pengujian 360p dan 233 karakter

Hasil Pengujian 1					
MSE	PSNR	Waktu	CER	BER	Waktu
0,239	54,339 dB	14 s 16 ms	0	0	9 s 42 ms

Tabel 2. Hasil pengujian video 360p 1411 karakter

Hasil Pengujian 2					
MSE	PSNR	Waktu	CER	BER	Waktu
1,365	46,777 dB	48 s78 ms	0	0	70 s 06 ms

Tabel 3. Hasil pengujian 720p dan 233 karakter

Hasil Pengujian 3					
MSE	PSNR	Waktu	CER	BER	Waktu
0,0486	61,2563 dB	38 s 12 ms	0	0	53 s 27 ms

Tabel 4. Hasil pengujian 720p dan 1411 karakter

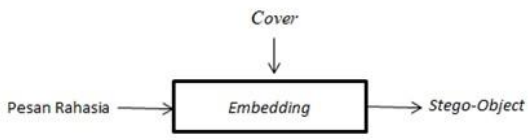
Hasil Pengujian 4					
MSE	PSNR	Waktu	CER	BER	Waktu
0,302	53,317 dB	61 s 11 ms	0	0	80 s 19 ms

Proses penyisipan pada video menggunakan format MPEG-4 pada video yang berukuran 360p dan 720p. Setelah video berhasil di sisipkan pesan, video disimpan kembali kedalam format AVI yang bertujuan agar pesan teks yang terdapat didalam video dapat terbaca sepenuhnya tanpa ada kesalahan. Penelitian ini dibagi menjadi empat bagian utama. Pertama, pengantar, membahas latar belakang masalah video steganografi dan menjelaskan bagian-bagian sederhana dari penelitian ini dan menyampaikan kontribusi yang dihasilkan dari penelitian ini. Kedua, skeanrio pemberian gangguan pada video steganografi, diagram blok sistem steganografi dengan SSB-4 dan pemilihan *frame* dengan metode DCT. Ketiga , hasil dan analisis terkait dengan simulasi yang dilakukan pada program Matlab dan diskusi hasil penelitian. Terakhir, kesimpulan dan saran adalah ringkasan dari hasil penelitian yang telah dilakukan,

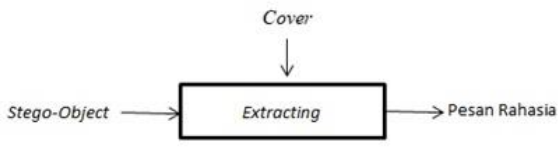
2. Dasar Teori dan Sistem Model

2.1. Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu steganos yang berarti tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga jika digabungkan keduanya artinya adalah menulis tulisan yang tersembunyi atau terselubung [4]. Steganografi secara harfiah berarti ”pesan tertutup” dan melibatkan transmisi pesan rahasia melalui tampaknya file berbahaya. Tujuannya agar tidak hanya melakukan pesan tetap tersembunyi, tetapi juga bahwa pesan tersembunyi bahkan dikirim tidak terdeteksi. Steganografi mendukung menyembunyikan pesan di antara volume besar lalu lintas internet, dalam file media mana. Selain dari pesan tersembunyi sulit untuk mendeteksi dengan mata manusia bahkan jika file tersebut dilihat. Pada steganografi, ada dua proses umum, yaitu proses penyisipan (*embedding*) pesan rahasia dan proses ektraksi ciri (*extracting*) video untuk mendapatkan pesan rahasia tersebut [5].



Gambar 1. Proses *Embedding*



Gambar 2. Proses *Extacting*

Pada 2 gambar diatas merupakan proses umun yang terjadi pada steganografi . Proses penyisipan pesan rahasia ke *cover* dengan menggunakan metode penyisipan pada steganografi. *Cover* yang telah disisipkan pada proses embedding akan menjadi stego-object. Stego-object adalah *cover* yang sudah tersisipkan oleh pesan rahasia. Bentuk stego-object menyesuaikan dengan *cover* dan metode penyisipan yang dilakukan. Kemudian untuk mendapatkan pesan rahasia itu kembali digunakan proses *extracting*. Metode proses *extracting* menyesuaikan dengan metode proses *embedding* yang digunakan. proses *extracting* digunakan untuk mengekstraksi pesan rahasia dari stego object. Dan didapatkan pesan rahasia sesuai dengan format yang digunakan [5].

2.2. *System Of Steganography Using* Bit 4

Teknik SSB-4 ini dikembangkan oleh J.M.Rodrigues, J.R.Rios dan W.Puech. Dalam *image* RGB 24bit, variasi-variasi kecil dalam nilai *channel color* tidak nampak oleh mata manusia. Metode yang diajukan dapat diaplikasikan pada citra yang disimpan dalam setiap tipe format file yang ada, selama menggunakan 8 bit per color dan menggunakan kompresi *lossless*. Bit ke 4 dari citra *cover* akan digantikan oleh bit pesan dan memodifikasi bit-bit *reminder* (1,2,3 dan 5). Ukuran citra pesan harus lebih kecil dari citra *cover*-nya. Pada Tabel 5 merupakan tabel bit citra pesan dan matriksnya dan pada Tabel 6 pixel citra *cover* dan matriks B 11 sebagai contoh metode SSB-4 dengan menggunakan citra pesan berupa citra biner dan citra *cover* berupa *grayscale*. Contoh: Citra pesan adalah matriks A dengan ukuran 4 x 4 [3].

Tabel 5. Bit Citra Pesan

x/y	0	1	2	3
0	1	0	0	1
1	0	0	1	0
2	1	1	1	0
3	0	1	0	0

Tabel 6. Bit Citra Cover

x\y	0	1	2	3	4	5
0	150	112	0	112	45	50
1	100	45	56	12	34	67
2	69	160	255	230	45	12
3	9	56	78	100	200	115
4	100	70	80	90	0	55
5	255	67	45	78	12	40

Pesan tersebut akan disisipkan kedalam citra *cover* dengan metode SSB-4. Metode penyisipan ada dua macam, yaitu sisipan merata dan sisipan kiri atas. Untuk contoh ini menggunakan sisipan kiri atas. Jadi pesan disisipkan sesuai dengan posisi x dan y citra *cover*. Pada Tabel 6 dijelaskan nilai biner modifikasi bit ke-4 [5]. Untuk pixel B(0,0) dengan nilai 150 akan disisipkan bit A(0,0) yaitu bit 1. Berikut tabel perubahan bit-bit (0,0). Dengan merubah bit ke-3 dan ke-2, maka nilai desimalnya menjadi 152 dengan selisihnya adalah 2. Ini adalah nilai yang paling mendekati dengan nilai aslinya yaitu 150. Jadi hasil akhirnya dari proses modifikasinya adalah 152. Jika bit ke-4 dari piksel yang akan disisipkan pesan nilainya sama, maka nilai piksel tesebut tidak berubah. Sebaliknya jika bit ke-4 piksel tidak sama dengan bit pesan, maka nilai piksel akan berubah sesuai pergantian bit pesan dan modifikasi bit-bit remindernya. Begitu seterusnya bit-bit pesan akan menggantikan bit ke-4 sampai seluruh pesan berhasil disisipkan ke citra *cover* [3].

Tabel 7. Nilai Biner Modifikasi Bit ke 4

	Nilai Biner							
	Desimal	8	7	6	5	4	3	2	1
Nilai desimal asli	150	1	0	0	1	0	1	1	0
Nilai desimal yang telah di modifikasi	158	1	0	0	1	1	1	1	0

Tabel 8. Nilai Biner modifikasi Bit *Reminder*

	Nilai Biner							
	Desimal	8	7	6	5	4	3	2	1
Nilai desimal asli	150	1	0	0	1	0	1	1	0
Nilai desimal yang telah di modifikasi	152	1	0	0	1	1	0	0	0

Pada nilai desimal yang dimodifikasi telah mengalami perubahan yaitu penggantian bit pada bit ke-4 menjadi 158. Perubahan dari nilai aslinya adalah 8. Namun nilai tersebut dapat dirubah lagi supaya selisihnya dengan desimal asli sekecil mungkin. Jadi kita akan mencari nilai yang mendekati nilai asli pikselnya. Kita dapat merubah nilai pada bit remindernya yaitu bit 5,3,2 dan 1. Pada tabel 8 merupakan nilai biner modifikasi bit reminder. Dengan merubah bit ke-3 dan ke-2, maka nilai desimalnya menjadi 152 dengan selisihnya adalah 2. Ini adalah nilai yang paling mendekati dengan nilai aslinya yaitu 150. Jadi hasil akhirnya dari proses modifikasinya adalah 152. Jika bit ke-4 dari piksel yang akan disisipkan pesan nilainya sama, maka nilai piksel tesebut tidak berubah. Sebaliknya jika bit ke-4 piksel tidak sama dengan bit pesan, maka nilai piksel akan berubah sesuai pergantian bit pesan dan modifikasi bit-bit *reminder* nya. Begitu seterusnya bit-bit pesan akan menggantikan bit ke-4 sampai seluruh pesan berhasil disisipkan ke citra *cover* [3].

2.1. *Discrete Cosine Transform* (DCT)

DCT adalah fungsi transform yang sangat populer digunakan dalam pemrosesan sinyal. DCT mengubah sinyal dari domain waktu ke domain frekuensi, dan mampu menunjukkan fragmen sinyal audio dalam ringkasan fungsi kosinus di frekuensi yang berbeda. Tujuan dari DCT untuk mengkonversi data ke dalam penjumlahan serangkaian gelombang kosinus *tray* pada frekuensi yang berbeda. DCT didefinisikan

sebagai berikut:

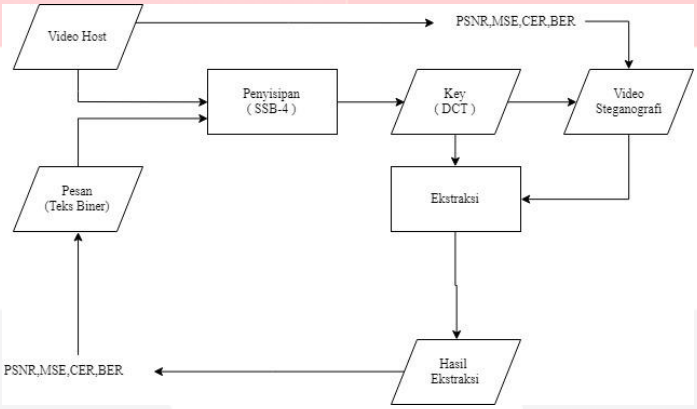
$$x(k) = \sum_{n=1}^{N} x(n) \cos\left\{\frac{\pi}{2N}(2n-1)(k-1)\right\} \; K = 1,2 \ldots N \quad (1),$$

$$w(k) = \frac{1}{\sqrt{N}}, K = 1 \quad (2),$$

$$w(k) = \sqrt{\frac{2}{N}}, 2 \leq k \leq N \quad (3)$$

Dimana, $x(n)$ merupakan sinyal audio asli dan N adalah jumlah sampel. Salah satu fitur yang paling penting bahwa DCT mengubah adalah energi buffer di beberapa sampel. Fitur ini dapat digunakan untuk mengurangi distorsi sinyal asli dalam proses audio watermarking, karena DCT memiliki fitur yang memiliki penyangga energi pada beberapa sinyal sampel [6].

2.1. Desain Sistem



Gambar 2. Digram Blok Proses Steganografi

Gambar 2 merupakan gambaran diagram blok proses steganografi yang mana akan dilakukan pengujian nilai PSNR dan MSE pada video yang telah disisipkan pesan. Nilai parameter CER dan BER akan dihitung pada proses ekstraksi yang mengeluarkan *output* pesan teks. Untuk rumus penghitungan PSNR,MSE,BER, dan CER adalah seperti berikut :

$$\text{MSE} = \frac{\sum[f(i,j) - F(i,j)]^2}{M \times N} \quad (4),$$

Dimana:
MSE = Nilai error frame video yang telah disisipi.
f(i,j) = Pixel luminance frame video asal.
F(I,j) = Pixel luminance frame video yang telah disisipi. .
M = Panjang frame video.
N = Lebar frame video.

$$\text{PSNR} = 10 \times \log_{10}\left[\frac{MAXi^2}{MSE}\right] db \quad (5),$$

Dimana:
PSNR = Tingkat noise frame setelah disisipi.
MAXi = Nilai maksimum dari pixel frame video yang digunakan.
MSE = Nilai Error frame video yang telah disisipi.

Niai yang didapatkan dari CER jika semakin hasilnya maka semakin baik karena semakin sedikit nilai karakter yang *error* pada pesan teks yang disisipi.

$$CER = \frac{Jumlah\ Karakter\ Error}{Jumlah\ Karakter\ Keseluruhan} \quad (6),$$

Nilai BER yang masih dapat ditoleransi adalah 30%. Jika lebih dari 30%, citra pesan sudah terlalu rusak untuk dapat dikenali lagi.

$$BER = \frac{Jumlah\ bit\ error}{Jumlah\ total\ bit} \quad (7)$$

Gambar 4. *Frame* Video 360p

Spesifikasi Video dan Audio						
Video						
Format	**Ukuran**	***Bit Rate***	***Width***	***Height***	**Durasi**	**Jumlah Frame**
MPEG-4	1,09 Mb	512 Kbps	640 piksel	360 piksel	14s 96ms	449
Audio						
Channel Count			***Mode Extention***			***Bit Rate***
2			*Stereo*			96 Kbps

Tabel 9. Spesifikasi Video 360p

Gambar 4 dan tabel 9 merupalan spesifikasi dari video sample yang memiliki ukuran 360p dan potongan frame gambar dari video tersebut. Pada video sample ini mengunakan 2 kanal audio yang berfungsi untuk penentuan frame yang akan disisipkan pesan dengan menggunakan metode DCT

Gambar 5. *Frame* Video 720p

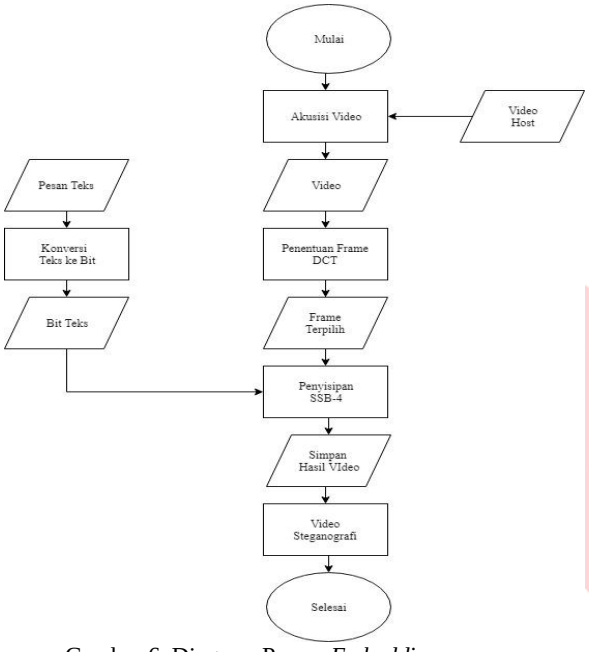
Spesifikasi Video dan Audio						
Video						
Format	**Ukuran**	***Bit Rate***	***Width***	***Height***	**Durasi**	**Jumlah Frame**
MPEG-4	2,99 Mb	1474 Kbps	1280 piksel	720 piksel	15s 22ms	450
Audio						
Channel Count			***Mode Extention***			***Bit Rate***
2			*Stereo*			192 Kbps

Tabel 10. Spesifikasi Video 720p

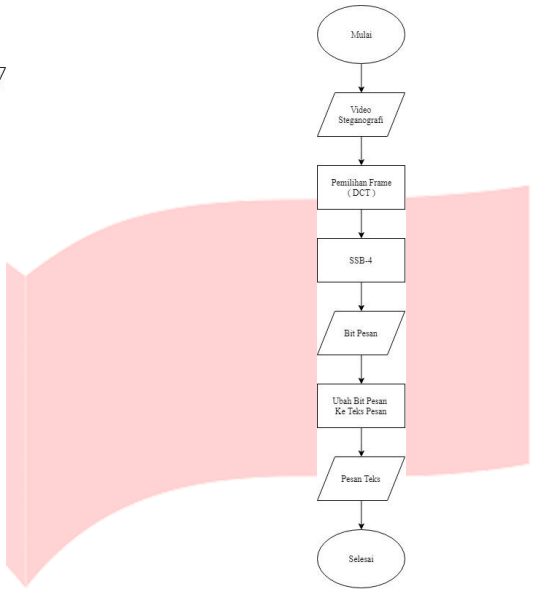
Gambar 5 dan tabel 10 merupalan spesifikasi dari video sample yang memiliki ukuran 720p dan potongan frame gambar dari video tersebut. Pada video juga digunakan 3 kanal audio yang akan digunakan dalam proses penentuan frame mana yang akan disisipi oleh pesan teks.

2.3. *Embedding* dan Ekstraksi

Proses *embedding* (penyisipan) dilakukan dengan cara pesan rahasia yang dimasukan dalam bentuk teks yang di ubah dalam bentuk biner, kemudian setelah menjadi biner diubah kembali menjadi bentuk bit. Frame gambar yang telah terpilih dari video akan dilakukan proses *embedding* dengan cara menyisipkan nilai biner dari teks yang telah diubah dari teks biner.Penentuan frame dilakukan dengan proses audio diana akan diambil frame dengan frekuensi yang tinggi sebagai frame terpilih. Proses *embedding* dilakukan pada frame terpilih yang nantinya akan disimpan sebagai video steganografi. Dalam proses penyisipan menggunakan DCT sebagai penentuan lokasi bit dan menggunakan metode SSB-4 untuk proses penyisipannya.



Gambar 6. Diagram Proses *Embedding*



Gambar 7. Diagram Proses *Extracting*

Dalam proses ekstraksi langkah pertama video yang telah disisipi pesan rahasiadi input sebagai video host. Setelah di masukan di video steganografi langkah selanjutnya yaitu dilakukannya proses extracting menggunakan metode SSB-4, sama dengan metode yang dilakukan pada saat proses embedding. Kemudian video yang sudah selesai proses extracting di dapatkan bit pesan rahasia. Setelah didapatkan bit teks pada video steganografi dilakukan pengubahan dari bit teks ke pesan teks.

3. Analisis

3.1. Data Asli

Pada proses steganografi dilakukan terhadap video berukuran 360p dan 720p dengan pesan yang disisipkan sebanyak 233 karakter dan 1411 karakter.Pada bagian ini, video stego belum diberikan gangguan apapun hanya disisipkan oleh pesan teks Pada tabel dibawah ini menjelaskan nilai dari masing masing parameter pengujian.

Tabel 11. Hasil Pengujian Data Asli

Hasil Pengujian				
Spesifikasi	360p 233 Karakter	360p 1411Karakter	720p 233 Karakter	720p 1411 Karakter
MSE	0,2394	1,3657	0,0486	0,3029
PSNR	54,339 dB	46,7772 dB	61,2563 dB	53,3176 dB
Waktu	14s 16ms	48s 77ms	38s 12ms	61s 11ms
BER	0	0	0	0
CER	0	0	0	0
Waktu	9s 42ms	70s 06ms	53s 27ms	80s 19ms

3.2. Data Asli Diberi Gangguan

Pada bagian ini akan menunjukan hasil dari video stego yang telah diberikan 3 jenis gangguan yang berbeda dengan koefisien ganggun 0,1 dan 0,5. Berikut ada nilai dari parameter pengujian:

a. Rescalling

Pada jenis gangguan ini mengubah video menjadi piksel piksel yang tidak beraturan, semakin besar koefisien diberikan maka semakin besar juga mengecilkan piksel piksel yang terdapat dalam video.

Tabel 12. Hasil Pengujian Gangguan *Rescalling*

Hasil Pengujian dengan Gangguan *Rescalling*								
Spesifikasi	360p 233 Karakter		360p 1411 Karakter		720 p 233 Karakter		720p 1411 Karakter	
Koef	0,1	0,5	0,1	0,5	0,1	0,5	0,1	0,5
MSE	3,9778	1,1695	3,977	1,169	2,559	0,5259	2,559	0,525
PSNR (dB)	42,1343	47,4508	42,134	47,45	44,049	50,921	44,049	50,921

Waktu	34,26	22,57	9,36	7,48	144,11	1133,47	117,98	373,69
BER	0,503	0,454	0,505	0,535	0,445	0,428	0,508	0,5239
CER	1	1	1	1	1	1	1	1
Waktu(s)	19,26	9,39	9,58	9,22	14,44	32,47	13,85	21,52

b. Noise Salt and Pepper

Noise salt and pepper merupakan gangguan yang diberikan terhadap image yang terdiri dari titik-titik hitam dan titik-titik putih . Pada Matlab akan dimasukan noise salt and pepper dengan nilai koefisien 0,1 dan 0,5 dengan semakin besarnya koefisien gangguan diberikan maka akan semakin banyak titik hitam dan titik putihnya.

Tabel 13. Hasil Pengujian Gangguan *Salt and Pepper*

Hasil Pengujian dengan Gangguan *Salt and Pepper*								
Spesifikasi	360p 233 Karakter		360p 1411 Karakter		720 p 233 Karakter		720p 1411 Karakter	
Koef	0,1	0,5	0,1	0,5	0,1	0,5	0,1	0,5
MSE	6,194	30,9711	6,19	30,96	8,654	43,274	8,656	43,276
PSNR	33,22	40,21	40,211	33,23	38,758	31,768	38,7573	31,768
Waktu	46,42	58,51	28,94	43,08	803,36	469,7	1029,57	397,39
BER	0,046	0,242	0,337	0,417	0,509	0,237	0,346	0,424
CER	0,296	0,896	0.931	0,987	0,339	0,909	0,939	0,987
Waktu	99,85	10,65	8,88	9,06	29,77	17,63	17,68	14,46

c. Gaussian Blur

Merupakan gangguan yang diberikan terhadap video stego yang membuat video menjadi tampak buram. Sama seperti rescaling dan salt and pepper, semakin besar koefisien yang diberikan maka semakin buram video stego tersebut.

Tabel 14. Hasil Pengujian Gangguan *Gaussian Blur*

Hasil Pengujian dengan Gangguan Gaussian Blur								
Spesifikasi	360p 233 Karakter		360p 1411 Karakter		720 p 233 Karakter		720p 1411 Karakter	
Koef	0,1	0,5	0,1	0,5	0,1	0,5	0,1	0,5
MSE	0	0,2238	0	0,2239	0	0,1167	0	0,116
PSNR	~	54,631	~	54,63	~	0,1167	~	57,458
Waktu	34,82	7,492	8,1	8,63	343,67	727,74	135,18	357,32
BER	0	0,192	0,328	0,388	0	0,189	0,328	0,434
CER	0	0,716	0,918	0,961	0	0,832	0,918	0,995
Waktu	9,95	8,91	8,87	9,47	14,64	21,13	17,08	14,12

4. Kesimpulan dan Saran

4.1. Kesimpulan

Dalam penilitian ini dilakukan evaluasi hasil dari video stego yang diberikan 3 jenis gangguan yaitu *Rescalling, Noise Salt and Pepper,* dan *Noise Gaussian Blur.* Berdasarkan hasil dari simulasi yang dilakukan pada sistem steganografi, dapat disimpulkan secara umum bahwa sistem yang dirancang dapat bekerja dengan baik. Pesan yang disisipkan pada seluruh video dapat disisipkan dengan sangat baik, tanpa ada perbedaan dengan video asli. Pada proses ekstraksi pun memilikihasil yang memuaskan, pesan yang disisipkan tidak berubah setelah dilakukan penyisipan .

Pesan teks yang terdapat di dalam video tidak berubah jika diberikan serangan *noise gaussian blur* dengan koefisien 0,1. Untuk nilai MSE, PSNR, BER dan CER terbaik terdapat pada video yang memiliki ukuran 720p dengan pesan yang disisipi sebanyak 233 karakter MSE= 0,048, PSNR= 61,256 dB, BER= 0, dan CER= 0.

4.2. Saran

Untuk melanjutkan penelitian ini , terdapat beberapa hal yang dapat dikembangkan yaitu dengan menggunakan metode transformasi *Wavelet Dual Tree Complex* untuk penentuan pemilihan *frame* mana yang akan disisipkan pesan dan menggabungkan metode steganografi menggunakan SSB-4 dan LSB. Menggunakan durasi video yang lebih panjang dan ukuran video yang lebih besar

Daftar Pustaka

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan kaufmann, 2007.

[2] R. D. A. M. F. Pamungkas and I. Safitri, eProceedings of Engineering, vol. 1, no. 1, 2019.

[3] I. B. H. F. Q. Rekamasanti and I. N. A. Ramatryana, eProceedings of Engineering, vol. 2, no. 2, 2015.

[4] D. Kahn, "The history of steganography," in International Workshop on Information Hiding. Springer, 1996, pp. 1–5.

[5] R. Anggara, G. Budiman, and L. Novamizanti, "Perancangan dan analisis steganografi video dengan menyisipkan teks menggunakan metode dct," eProceedings of Engineering, vol. 2, no. 2, 2015.

[6] G. Budiman *et al.*, "Kinerja Teknik LWT-DCT-SVD Pada Audio Watermarking Stereo Dengan Sinkronisasi dan Compressive Sampling Performance LWT-DCT-SVD Technique On Audio Watermarking."