Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT

Alfiro Siowanta Pratama[1], I Made Suartana[2]

[1,2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]alfiropratama16051204010@mhs.unesa.ac.id
[2]madesuartana@unesa.ac.id

***Abstrak*— Peran media digital saat ini merupakan dampak dari pencapaian teknologi terkini. Tidak dapat dipungkiri bahwa internet merupakan sarana akses data dan komunikasi yang paling sering digunakan. Namun, internet juga menjadi sarang bagi para penyerang untuk mengakses informasi penting dan berharga dari pengguna atau negara lain. Steganografi menjadi salah satu teknik yang digunakan dalam konteks komunikasi yang aman dengan menyembunyikan informasi rahasia. Tujuan utama steganografi adalah untuk menghapus kecurigaan pihak ketiga atas informasi rahasia yang dikirimkan. Terdapat tiga syarat fundamental dari teknik steganografi yang efektif, yaitu kapasitas embedding, imperceptibility, dan robustness. Steganografi digital dapat diimplementasikan pada file multimedia seperti audio, video, teks atau gambar. Steganografi video relatif kurang diteliti karena struktur file yang kompleks yang membuatnya lebih kuat. Selain itu, ukuran video relatif lebih besar daripada file audio dan gambar yang dapat mencapai kapasitas penyematan tinggi. Melalui penelitian ini, kualitas video hasil stego-video menggunakan teknik transformasi kombinasi antara DCT (discrete cosine transform) dan DWT pada file video dengan format file Audio Video Interleaved (AVI) yang merupakan hasil kerja dari Microsoft Corporation akan diamati. Proses steganografi diawali dengan membaca frame dari video yang telah dipilih, kemudian dilakukan transformasi DWT dan DCT tiap frame yang berhasil dibaca, menyisipkan bit-bit pesan ke dalam frame pada high frekuensi band hingga semua bit pesan masuk seluruhnya. Pengukuran kualitas video ini berdasarkan nilai Mean Square Error dan Peak Signal to Noise Ratio dari video yang telah disisipi pesan rahasia. Hasilnya, dari 4 kali pengujian penyisipan pesan rahasia didapat masing-masing nilai MSE dan PSNR pada pengujian 1 (sebelum disisipkan pesan) sebesar 4607,2607 dan 71,7363, pada pengujian 2 (disisipkan 14.400 karakter) sebesar 4612,0937 dan 71,7318, pada pengujian 3 (disisipkan 28.800 karakter) sebesar 4624,1798 dan 71,7204, serta pada pengujian 4 (disisipkan 32.500 karakter) sebesar 4624,1798 dan 71,7204.**

***Kata Kunci* — AVI, DCT-DWT, Video, Steganografi**

I. PENDAHULUAN

Media digital saat ini telah menjadi bagian penting dalam setiap bidang kehidupan manusia berkat kemajuan teknologi hingga saat ini [1]. Tidak dapat diragukan lagi bahwa media digital telah banyak menggantikan peran media-media konvensional karena alasan efektifitas dan fleksibilitasnya. Media digital dan internet telah berkembang menjadi media komunikasi yang paling dibutuhkan saat ini.

Internet telah digunakan sebagai media komunikasi baik oleh pengguna bisnis maupun pribadi karena memberikan banyak kemudahan yang tidak disajikan oleh media komunikasi lain. Internet mengjangkau semua orang dari seluruh bagian dunia tanpa harus terhalang jarak dan waktu. Diantara banyaknya kemudahan-kemudahan yang diberikan, penggunaan internet sebagai media komunikasi justru memiliki resiko yang tidak dihadirkan oleh penggunaan media konvensional, yaitu terkait keamanan data. Para penyerang dapat dengan mudah mengakses informasi penting dan berharga dari data-data yang ditransmisikan melalui internet [1].

Data-data penting yang dikirimkan melalui media transmisi harus dipastikan keamanannya. Menyembunyikan data merupakan salah satu langkah keamanan yang dapat diambil untuk mengamankan data. Penyembunyian data sangat penting dalam identifikasi, otentikasi, dan perlindungan hak cipta media digital [2]. Kriptografi sering digunakan dalam bentuk komunikasi rahasia, namun teknik ini sering kali menarik perhatian peretas karena *ciphertext* data yang telah diamankan akan terlihat sangat berbeda dengan data asli. Teknik pengamanan lainnya adalah *watermarking,* yang banyak digunakan untuk perlindungan hak cipta. Teknik *watermarking* pada [3] dikombinasikan dengan *Convolutional Neural Network* (CNN) dan *Discrete Wavelett Transform* (DWT) untuk mengamankan citra berwarna. Algortima DWT digunakan untuk menguraikan citra menjadi beberapa *sub-band* yang berbeda. Piksel-piksel pada frekuensi tinggi dan rendah pada tiap sub-band kemudian dijadikan inputan untuk melatih CNN. Citra hasil *watermarking* diuji menggunakan parameter PSNR, NC, dan SSIM, dan didapatkan hasil bahwa metode yang diajukan memiliki keunggulan dari sisi *invisibility* dan *robustness* dibandingkan dengan metode lain.

Steganografi merupakan sebuah metode menyembunyikan data ke dalam media pembawa, media yang dimaksud dapat berupa file digital apapun seperti gambar, audio, teks, dan video. Steganografi menjadi salah satu teknik kemanan informasi yang diperhitungkan dalam dunia digital saat ini. Dalam konteks komunikasi rahasia, teknik ini dinilai lebih aman dibandingkan teknik *watermarking* dan kriptografi, hal ini karena steganografi dapat menyimbunyikan informasi ke dalam media tanpa memberikan tanda bahwa media tersebut telah digunakan untuk menyimbunyikan informasi penting, sehingga antara pengirim dan penerima dapat terjalin komunikasi secara rahasia. Terdapat tiga hal mendasar yang harus dipenuhi dalam teknik steganografi yang baik, yaitu *embedding capacity*, *imperceptibility*, dan *robustness*. [4]

Embedding capacity berhubungan dengan jumlah pesan rahasia yang dapat disematkan dalam objek stego. *Imperceptibility* adalah ketahanan terhadap distorsi visual, sedangkan *robustness* adalah ketahanan terhadap kompresi dan serangan melalui pemrosesan sinyal yang berbeda. Cara paling sederhana untuk membedakan kualitas dari objek-stego adalah

melalui *Human Visual System* (HVS), karena HVS tidak dapat melihat distorsi marjinal sehingga menghindari kecurigaan.

Digital Steganografi dapat dilakukan pada berbagai media, seperti teks, suara, gambar, dan video. Media suara dan video dinilai sebagai media yang baik untuk menyembunyikan informasi karena terdapat banyak redundasi [5]. Teknik steganografi menggunakan sinyal redudansi dari media untuk menyembunyikan pesan rahasia untuk menghasilkan sinyal stego berkualitas tinggi [6]. Penelitian terkait penggunaan suara sebagai media pembawa telah banyak dilakukan. Penelitian [5] berhasil menghasilkan audio hasil stego-audio berkualitas tinggi yang disisipi informasi rahasia berupa text melalui pengukuran PSNR dan MSE. Penelitian [4] menggunakan teknik steganografi pada video dengan kualitas *standart* dan *high definition* untuk menyembunyikan data rahasia berupa gambar. Data rahasia disematkan setelah sebelumnya dilakukan enkripsi pada komponen sub-band frekuensi menengah dari dekomposisi DWT tingkat kedua dari frame. Skenario pengujian diterapkan dengan memberikan serangan *Gaussian* dan *salt and pepper noise*. Melalui pengukuran PSNR, SSIM, dan BER, teknik yang diusulkan terbukti mampu mencapai *imperceptibility* yang tinggi pada video SD maupun HD. Teknik ini juga terbukti tahan terhadap berbagai jenis serangan noise dan kompresi sehingga cocok digunakan pada skema transmisi data yang aman. Penelitian [7] memanfaatkan DWT dan *Arnold Scrambling* untuk *preprocessing* gambar rahasia sebelum disembunyikan kedalam file video. Penyematan gambar rahasia kedalam video dilakukan menggunakan teknik LSB. Melalui penelitian ini, teknik yang diusulkan memiliki tingkat keamanan dan ketahanan yang tinggi karena menggabungkan kriptografi dan steganografi.

Penggunaan koefisien *Discreate Wavelet Transformation* (DWT) yang digabungkan dengan koefisien *Discreate Cosine Transformation* (DCT) pada teknik steganografi telah banyak digunakan pada berbagai media. Penelitian [8] mengusulkan penggunaan koefisien DCT dan DWT untuk meningkatkan keamanan data tersembunyi dan meminimalkan distorsi untuk menjaga kualitas video yang lebih baik. Dalam penelitian tersebut, deteksi scene-changes dilakukan menggunakan koefisien DCT dari urutan video untuk menyembunyikan data. Kemudian, cover-video dan *payload* digabungkan dan dinormalisasi menggunakan koefisien DWT untuk meningkatkan kualitas video. Teknik yang diusulkan menghasilkan nilai PSNR lebih tinggi dengan distorsi yang lebih rendah dibanding dengan metode lain.

Teknik steganografi pada video relatif kurang diteliti karena struktur file dan ukuran yang lebih besar dibanding dengan media lainnya [1]. Pada penelitian ini akan dilakukan penyematan pesan teks rahasia kedalam video menggunakan koefisien DWT dan DCT. Tujuan dari penelitian ini adalah (1) mengetahui kapasitas maksimal pesan yang dapat disisipkan pada tiap frame. (2) Untuk menguji kualitas stego-video setelah proses penyisipan pesan melalui pengukuran parameter *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE).

II. METODOLOGI PENELITIAN

Steganography merupakan salah satu teknik pengamanan data yang diperhitungkan dalam dunia digital saat ini. Penggunaan media video dinilai lebih aman karena terdapat banyak redudansi. Sistem yang dirancang menggunakan bahasa *phyton* pada penelitian ini mampu melakukan teknik stego-video pesan teks menggunakan media *video* bertipe *AVI* dan dapat mengekstrak pesan rahasia yang telah disisipkan tanpa menghilangkan informasi yang telah disisipkan penerima.

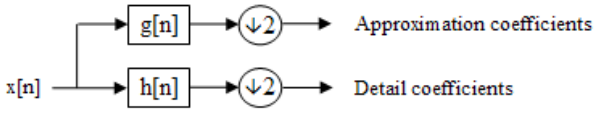
1. *Discreate Cosine Transform*

DCT adalah sebuah skema *lossy compression* dimana NxN blok ditransformasikan dari domain spasial ke domain DCT *[9]*. Pada umumnya, DCT merupakan transformasi *one-to-one mapping* dari suatu array berisi nilai piksel menjadi komponen-komponen yang terbagi berdasarkan frekuensinya. Steganografi menggunakan DCT dilakukan dengan melakukan transformasi video kemudian dilakukan modifikasi terhadap koefisien DCT sesuai dengan bit pesan yang disisipkan. Setelah proses penyisipan selesai dilakukan, *inverse* DCT sebagai finalisasi untuk mengembalikan data citra ke domain spasial sehingga dapat kembali direpresentasikan *[10]*.

2. *Discreate Wavelet Transform*

DWT bekerja dengan membagi frekuensi gambar/frame kedalam beberapa sub-band frekuensi: rendah, menengah, dan tinggi. Dekomposisi 2D-DWT level 1 akan memecah frame menjadi beberapa frekuensi: *Low-low frequency* (LL), *low-high frequency* (LH), *high-low frequency* (HL), dan *high-high frequency* (HH). Dimana LL sub-band adalah aproksimasi frame, LH mendefinisikan frekuensi horizontal, HL mendefinisikan frekuensi vertikal, dan HH memberikan detail informasi frame, seperti nilai diagonal.

Dalam DWT, penggambaran sebuah skala waktu sinyal digital didapatkan dengan menggunakan teknik filterisasi digital [11]. Sinyal DWT (x) diuraikan secara bersamaan menggunakan *high pass (h)* dan *low pass (g) filter*. Penguraian sinyal menggunakan *high pass filter* akan menghasilkan koefisien detail sedangkan penggunaan *low pass filter* akan menghasilkan koefisien aproksimasi. Kedua filter bekerja saling terkait satu sama lain atau disebut dengan filter cermin segi empat. Gbr 1 merupakan diagram keterkaitan antara *filter high* dan *low pass*



Gbr 1 Diagram blok analisis filter

3. Embedding Pesan Rahasia

Embedding adalah proses menyisipkan pesan rahasia kedalam objek stego. *Embedding* pada penelitian ini diawali dengan membaca *frame* dari video yang telah dipilih, kemudian dilakukan transformasi DWT dan DCT tiap *frame* yang berhasil dibaca. Menyisipkan bit-bit pesan ke dalam frame pada high frekuensi band hingga semua bit pesan masuk seluruhnya. Pada penelitian ini, sistem memiliki fungsi untuk dapat menghitung nilai PSNR dan MSE dari video yang telah melalui proses stego-video. Alur proses penyisipan pesan kedalam media menggunakan DCT dan DWT pada penelitian ini dapat dilihat pada Gbr 2

Kualitas objek hasil stego-video dapat diukur dari tingkat perbedaan objek original dengan hasil proses stego-video. Kualitas stego-video dapat diuji secara eksperimental menggunakan metode kuantifikasi PSNR dalam *decibel* (dB) dapat dihitung menggunakan persamaan(1) [4]:

$$PSNR = 10 \log_{10} \frac{{Max_{or}}^2}{MSE} \quad (1)$$

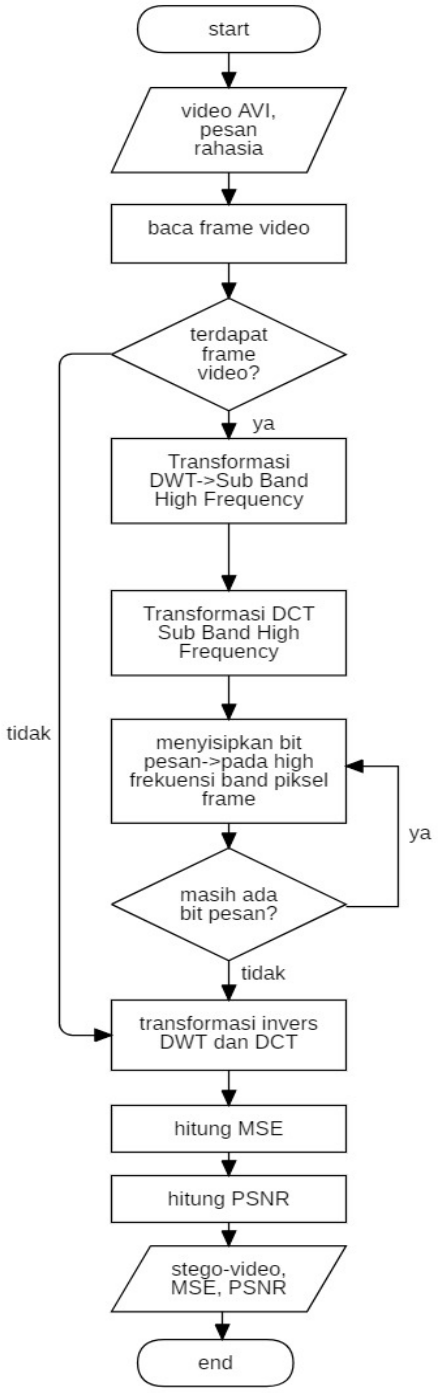
Dengan

$$MSE = \frac{1}{r\ x\ c} \sum_{i=0}^{r-1} \sum_{j=0}^{c-1} (or_{i,j} - st_{i,j}) \quad (2)$$

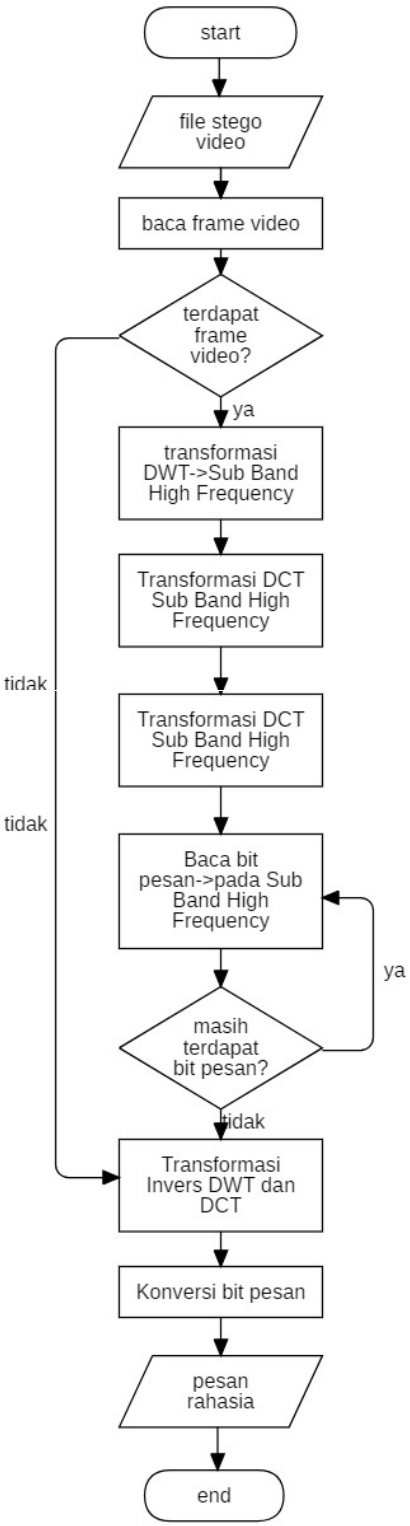
Dimana:
or = original frame
st = stego frame
r, c = resolusi frame
Max_{or} = nilai pixel maksimum dari frame asli

4. Ekstraksi Pesan Rahasia

Proses ektraksi ditujukan untuk mendapatkan pesan rahasia yang berhasil disematkan di dalam sebuah media. Proses ini diperlukan agar sisi penerima dapat mengerti dan mendapatkan pesan yang dikirimkan oleh pengirim. Pesan yang diekstraksi haruslah sama dengan pesan yang dikirimkan tanpa adanya informasi yang hilang. Alur proses ekstraksi pesan menggunakan sistem ini dapat dilihat pada Gbr 3



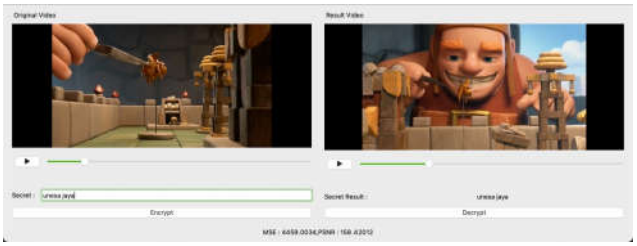
Gbr 2. Proses penyisipan pesan ke dalam media menggunakan DCT dan DWT



Gbr 3. Alur Proses Ekstraksi Pesan dari Video

III. HASIL DAN PEMBAHASAN

Pada penelitian ini pengujian dilakukan dengan melakukan stego-video atau menyembunyikan pesan rahasia kedalam media video menggunakan sistem yang telah dirancang. Gbr 3 merupakan hasil tangkapan layar dari sistem yang telah berhasil menjalankan proses stego-video dan mengekstrak pesan rahasia yang sebelumnya telah disisipkan ke dalam media video.



Gbr 4. Sistem berhasil melakukan proses stego-video dan mengekstrak pesan rahasia

Pada pengujian yang dilakukan, parameter yang diamati adalah nilai *Mean Squared Error* (MSE), dan nilai *Peak Signal to Ratio (PSNR)*. Pengujian dilakukan pada sebuah *file video AVI* dengan detail masing-masing file dapat dilihat pada tabel I

TABEL I
DETAIL INFORMASI FILE UJI STEGO-VIDEO

Video File	Resolusi (pixel)	Durasi (detik)	FPS	Ukuran File
Sample-2s.avi	1280 x 720	2	1/s	162 KB

Video dilakukan 4 tahap pengujian penyisipan pesan rahasia. Pengujian pada sistem menghasilkan masing-masing nilai MSE dan PSNR pada pengujian 1 (sebelum disisipkan pesan) sebesar 4607,2607 dan 71,7363, pada pengujian 2 (disisipkan 14.400 karakter) sebesar 4612,0937 dan 71,7318, pada pengujian 3 (disisipkan 28.800 karakter) sebesar 4624,1798 dan 71,7204, serta pada pengujian 4 (disisipkan 32.500 karakter) sebesar 4624,1798 dan 71,7204 dengan kapasitas maksimal pesan yang dapat disisipkan sebesar 14.400 karakter/frame. Untuk perhitungan nilai kapasitas maksimal pesan pada tiap frame dapat menggunakan rumus sebagai berikut.

$$Max\ char = n_{row}/8 \times n_{col}/8$$

Dimana, n_{row} merupakan jumlah baris/lebar resolusi frame pada video. Sedangkan, n_{col} merupakan jumlah kolom/tinggi resolusi frame pada sebuah video. Untuk pembagian 8 tersebut ialah mengikuti metode dari DCT yang membagi 8 blok pada setiap frame video.

Nilai MSE dan PSNR dari file hasil stego-video dapat dilihat pada table-tabel berikut.

TABEL II
HASIL UJI PARAMETER PSNR STEGO VIDEO SEBELUM PENYISIPAN PESAN

Video File	MSE	PSNR	Ukuran File
Sample-2s.avi	4607,2407	71,7363	162 KB

Pada tabel II merupakan hasil nilai MSE dan PSNR dari stego video sebelum proses penyisipan pesan.

TABEL III
HASIL UJI PARAMETER PSNR STEGO VIDEO DENGAN TEXT 1
(BERJUMLAH 14.400 KARAKTER)

Video File	MSE	PSNR	Ukuran File
Sample-2s.avi	4612,0937	71,7318	546 KB

Pada tabel III merupakan hasil nilai MSE dan PSNR dari stego video yang telah disisipkan pesan sejumlah 14.400 karakter. Dan terlihat terdapat perbedaan nilai dari tahap uji pertama (tabel II), yakni dari nilai MSE, PSNR, dan ukuran file video. Semakin menurunnya nilai PSNR menunjukkan bahwa kualitas stego video semakin menurun setelah dilakukan proses penyisipan pesan rahasia.

TABEL IV
HASIL UJI PARAMETER PSNR STEGO VIDEO DENGAN TEXT 2
(BERJUMLAH 28.800 KARAKTER)

Video File	MSE	PSNR	Ukuran File
Sample-2s.avi	4624,1798	71,7204	550 KB

Pada tabel IV merupakan hasil nilai MSE dan PSNR dari stego video yang telah disisipkan pesan sejumlah 28.800 karakter. Dan terlihat terdapat perbedaan nilai dari tahap uji sebelumnya, yakni dari nilai MSE, PSNR, dan ukuran file video. Semakin menurunnya nilai PSNR menunjukkan bahwa kualitas stego video semakin menurun setelah dilakukan proses penyisipan pesan rahasia.

TABEL V
HASIL UJI PARAMETER PSNR STEGO VIDEO DENGAN TEXT 4
(BERJUMLAH 32.500 KARAKTER)

Video File	MSE	PSNR	Ukuran File
Sample-2s.avi	4624,1798	71,7204	550 KB

Pada tabel V merupakan hasil nilai MSE dan PSNR dari stego video yang telah disisipkan pesan sejumlah 32.500 karakter. Dan terlihat terdapat persamaan nilai dari tahap uji ketiga (tabel IV), yakni dari nilai MSE, PSNR, dan ukuran file video yang menunjukkan nilai yang sama. Hal ini dikarenakan pada tahap keempat ini karakter pesan yang disisipkan telah melebihi kapasitas maksimum yang ada, maka yang terjadi ialah data loss atau dapat diartikan pesan yang melebihi kapasitas maksimum tidak berhasil disisipkan pada frame video yang ada.

IV. KESIMPULAN

Berdasarkan pengukuran parameter *Peak Signal to Ratio (PSNR)* dan *Mean Square Error (MSE)* yang telah dilakukan pada dokumen *video* hasil dari proses stego video menggunakan koefisien DCT dan DWT, dapat disimpulkan beberapa hal sebagai berikut:

1. Sistem yang dirancang berhasil mengetahui kapasitas maksimal pesan *text* yang dapat disisipkan pada tiap frame yang memperoleh nilai maksimal 14.400 karakter/frame.
2. Setelah dilakukan pengujian 4 kali, masing-masing kualitas stego-video mengalami penurunan berdasarkan banyak pesan yang disisipkan, yang dapat dibuktikan dengan menurunnya nilai PSNR dari pengujian sebelumnya.

Proses stego-video untuk menyembunyikan pesan *text* ke dalam file video menghasilkan masing-masing nilai MSE dan PSNR pada pengujian 1 (sebelum disisipkan pesan) sebesar 4607,2607 dan 71,7363, pada pengujian 2 (disisipkan 14.400 karakter) sebesar 4612,0937 dan 71,7318, pada pengujian 3 (disisipkan 28.800 karakter) sebesar 4624,1798 dan 71,7204, serta pada pengujian 4 (disisipkan 32.500 karakter) sebesar 4624,1798 dan 71,7204.

UCAPAN TERIMA KASIH

Ucapan terimakasih yang sangat tulus disampaikan untuk kedua orang tua yang selalu membersamai dan terus memberikan dukungan sehingga penulis memiliki kepercaya dirian untuk menyelesaikan studinya. Tak lupa kepada Tuhan Yang Maha Pemurah, atas restu dan izinnya sehingga penelitian ini dapat terlaksana sesuai yang penulis harapkan. Kepada jajaran dosen dan staff jurusan Teknik Informatika yang tidak hentinya memberikan ilmu selama penulis menjalani masa studi. Kepada teman-teman prodi S1 Teknik Informatika dan seluruh teman-teman jurusan Teknik Informatika yang telah berjuang bersama untuk menyelesaikan tanggungjawabnya.

REFERENSI

[1] M. Dalal dan M. Juneja, "Evaluation of Orthogonal and Biorthogonal Wavelets for Video Steganography," *Information Security Journal: A Global Perspective,* pp. 1-11, 2020.

[2] D. Arraziqi dan E. S. haq, "Optimization of Video Steganography with Additional Compression and Encryption," *TELKOMNIKA,* vol. 17 (3), pp. 1417-1424, 2019.

[3] N. C. Sy, H. H. Kha dan N. M. Hoang, "An Efficient Robust Blind Watermarking Method Based on Convolution Neural Networks in Wavelet Transform Domain," *International Journal of Machine Learning and Computing,* vol. 10 (5), pp. 675-684, 2020.

[4] M. Dalal dan M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," *Multimedia Tools Applications,* vol. 78 (5), pp. 5769-5789, 2019.

[5] A. D. Hendrata dan A. Prihatno, "Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode Least Significant Bit," *Jinacs,* vol. 2 (3), 2021.

[6] M. Baziyad, T. Rabie dan I. Kamel, "Directional Pixogram: A New Approach for Video," dalam *Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, 2020.

[7] H. L. Nuo dan A. W. Oo, "Secure Data Transmission of Video Steganography USing Arnold Scarmbling and DWT," *International Journal Computer Network and Information Security,* vol. 11 (6), pp. 45-53, 2019.

[8] M. Ramalingam dan N. A. M. Isa, "A Data-hiding Technique using Scene-change Detection for Video Steganography," *Computers & Electrical Engineering,* vol. 54, pp. 423-434, 2016.

[9] R. Krasmala, A. B. Purba dan U. T. Lenggana, "Kompresi Citra Dengan Menggabungkan Metode Discrete Cosine Transform (DCT) dan Algoritma Huffman," *JOIN,* vol. 2 (1), pp. 1-9, 2017.

[10] B. A. Wijaya, "Analisis Steganografi Video menggunakan Kombinasi Algoritma Discrete Cosine Transform (DCT-2D) dan Discrete Wavelet Transform (DWT)," Universitas Sumatera Utara, Medan, 2018.

[11] M. Ruswiansari, A. Novianti dan Wirawan, "Implementasi Discreate Wavelet Transform dan SIngular Value Decomposition pada Image Watermarking," *Jurnal Elektro Telekomunikasi Terapan,* pp. 249-259, 2016.

[12] A. KOYUN dan H. B. MACİT, "Generating a Stego-Audio Data Using LSB Technique and Robustness Test," *Journal of Engineering Sciences and Design,* vol. 6 (1), pp. 87-92, 2018.