JSI (Jurnal Sistem Informasi) Universitas Dirgantara Marsekal Suryadarma
p-ISSN: 2355-9675
e-ISSN: 2541-3228

Data hiding pada video digital menggunakan metode discrete cosine transform

Fajrul Malik A. Napitupulu[1,*]
[1]Jurusan Ilmu Komputer, Institut Modern Arsitektur dan Teknologi
fajrulmalik@imat.ac.id

Article Info

Article history:
Received October 2, 2025
Accepted December 6, 2025
Published January 2, 2026

Kata Kunci:

Steganografi
Discrete Cosine Transform
Video digital
Character Error Rate
Data Hiding

ABSTRAK

Pertukaran data digital memerlukan mekanisme keamanan yang tidak hanya menjaga kerahasiaan, tetapi juga menyamarkan keberadaan pesan. Penelitian ini mengembangkan teknik steganografi pada video digital menggunakan Discrete Cosine Transform (DCT) yang diterapkan pada blok 8×8 koefisien luminance dalam format MJPEG. Penyisipan pesan dilakukan dengan memodifikasi bit least significant (LSB) pada koefisien kuantisasi DCT. Evaluasi menggunakan parameter Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), dan Character Error Rate (CER) untuk mengukur fidelity, robustness, dan recovery. Hasil eksperimen menunjukkan stego-video memiliki kualitas visual tinggi dengan PSNR rata-rata 42,51 dB. Namun, metode ini hanya robust terhadap penambahan kontras, dan gagal pada manipulasi rotasi atau konversi grayscale dengan CER mencapai 100%. Nilai CER rata-rata pada kondisi normal adalah 0,29%, mengindikasikan keberhasilan ekstraksi pesan selama tidak terjadi distorsi struktural. Disimpulkan bahwa teknik DCT layak untuk penyembunyian pesan pada video MJPEG, tetapi memerlukan peningkatan ketahanan terhadap manipulasi video.

Corresponding Author:

Fajrul Malik A. Napitupulu,
Jurusan Ilmu Komputer ,
Institut Modern Arsitektur dan Teknologi,
Email: *fajrulmalik@imat.ac.id

1. PENDAHULUAN

Pertukaran data digital semakin meningkat seiring kemajuan teknologi komunikasi modern. Berbagai informasi personal, dokumen industri, hingga data pemerintahan kini berpindah secara daring dan rentan terhadap akses ilegal. Kasus kebocoran data oleh kelompok peretas seperti “Bjorka” pada 2022 memperlihatkan bahwa informasi yang bersifat rahasia dapat terekspos apabila tidak dilindungi dengan mekanisme keamanan memadai (Kompas, 2022). Kondisi ini menekankan pentingnya pengembangan metode perlindungan data yang tidak hanya menjaga kerahasiaan, tetapi juga menyamarkan keberadaan informasi tersebut (Awaludin et al., 2024). Salah satu pendekatan yang banyak dikaji dalam keamanan data adalah steganografi, yaitu teknik menyembunyikan pesan ke dalam media penampung sehingga tidak terdeteksi secara visual (Johnson & Jajodia, 1998). Media yang digunakan dapat berupa dokumen, citra, audio, maupun video, dengan video menjadi pilihan menarik karena sifatnya yang dinamis dan memiliki kapasitas data besar (Jadeja, A., Shah, K., & Jhaveri, M., 2023). Dalam praktiknya, steganografi memungkinkan pertukaran berkas secara normal tanpa memunculkan kecurigaan karena perbedaan antara media asli dan media berisi pesan sangat kecil (Awaludin & Amelia, 2022).

Pada ranah video digital, salah satu transformasi yang banyak digunakan adalah Discrete Cosine

Transform (DCT). Transformasi ini mengubah data spasial menjadi domain frekuensi sehingga penyisipan pesan dapat dilakukan pada koefisien tertentu tanpa mengganggu kualitas visual secara signifikan (Ahmed et al., 1974; Rao & Yip, 2014). Teknik DCT juga cocok untuk kodek seperti Motion JPEG (MJPEG) yang berbasis kompresi blok frekuensi. Selain itu, video berformat AVI, MPEG, dan MKV umum digunakan sebagai media penampung dalam berbagai penelitian steganografi (Faruqi, A. A., & Rozi, I. F., 2015).

Penelitian terkini menunjukkan bahwa metode berbasis DCT mampu menghasilkan nilai Peak Signal-to-Noise Ratio (PSNR) tinggi dan Bit Error Rate rendah, sehingga kualitas media tetap baik dan pesan dapat diekstraksi secara akurat (Tutuncu, K., & Hacimurtazaoglu, M., 2021; Garno, G., Rizal, A., Solehudin, A., & Ekstanza, R., 2022). Studi lain juga menemukan bahwa penggunaan tanda (sign) dari koefisien DCT dapat meningkatkan ketahanan pesan terhadap kompresi JPEG, terutama ketika dikombinasikan dengan teknik koreksi kesalahan (Zhang, J., He, X., & Cao, Y., 2024). Temuan tersebut mengindikasikan bahwa pendekatan DCT masih relevan untuk pengembangan metode steganografi yang lebih efisien (Awaludin, 2023). Meskipun demikian, tantangan besar tetap ada terutama terkait robustness terhadap manipulasi seperti kompresi ulang, rotasi, penajaman, perubahan kontras, atau pemotongan. Berbagai laporan menunjukkan bahwa metode berbasis DCT masih rentan terhadap distorsi tertentu, terutama pada sistem video dengan proses kompresi berulang (Huang, Y., Liu, Z., Wu, Q., & Liu, X., 2024; Zhang, J., Wu, M., Wang, Z., & Liu, Y., 2024). Hal ini mendorong kebutuhan penelitian lanjutan untuk meningkatkan daya tahan metode terhadap serangan atau modifikasi media penampung.

Berdasarkan perkembangan tersebut, penelitian ini berfokus pada implementasi teknik DCT pada video digital menggunakan kodek MJPEG untuk mengevaluasi tiga aspek utama: fidelity, robustness, dan recovery. Parameter seperti Mean Squared Error (MSE), PSNR, dan Character Error Rate (CER) digunakan untuk menilai kualitas citra dan keberhasilan ekstraksi pesan (Yunus, M., & Harjoko, A., 2014). Melalui evaluasi ini, penelitian diharapkan dapat memberikan kontribusi terhadap pengembangan metode steganografi video yang lebih aman, stabil, dan layak diterapkan pada sistem pertukaran data modern.

2. METODE

Tabel State of the Art Steganografi Video Berbasis DCT (2023–2024)

No.	Nama Peneliti (Tahun)	Pembahasan	Hasil
1.	Jadeja, A., Shah, K., & Jhaveri, M. (2023)	**Masalah:** Perlunya teknik steganografi video yang lebih dinamis dan memiliki kapasitas tinggi tanpa mengganggu kualitas visual. **Solusi:** Tinjauan analitis terhadap berbagai teknik steganografi video, termasuk DCT, dengan fokus pada kestabilan dan kapasitas penyisipan.	Hasil tinjauan menunjukkan bahwa video cocok sebagai media steganografi karena sifatnya yang dinamis dan kapasitas besar, namun masih diperlukan optimasi robustness terhadap manipulasi.
2.	Huang, Y., Liu, Z., Wu, Q., & Liu, X. (2024)	**Masalah:** Metode DCT rentan terhadap distorsi akibat kompresi JPEG dan manipulasi citra. **Solusi:** Mengusulkan modulasi	Teknik yang diusulkan menunjukkan peningkatan robustness terhadap kompresi JPEG dengan nilai PSNR tetap

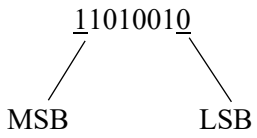
No.	Nama Peneliti (Tahun)	Pembahasan	Hasil
		residu DCT untuk meningkatkan ketahanan terhadap kompresi JPEG pada steganografi citra, yang dapat diadaptasi untuk video.	tinggi, namun belum diuji secara spesifik pada video.
3.	Zhang, J., He, X., & Cao, Y. (2024)	**Masalah:** Steganografi berbasis DCT masih rentan terhadap kesalahan ekstraksi pesan setelah kompresi. **Solusi:** Menggunakan kode polar steganografi untuk mencapai robust errorless pada steganografi JPEG berbasis DCT.	Metode berhasil mencapai **errorless recovery** pada kondisi kompresi tertentu, dengan CER mendekati 0% pada uji citra diam.
4.	Zhang, J., Wu, M., Wang, Z., & Liu, Y. (2024)	**Masalah:** Ketahanan terhadap kompresi JPEG masih lemah pada metode DCT konvensional. **Solusi:** Mengembangkan teknik modulasi residu DCT untuk meningkatkan robustness terhadap kompresi JPEG pada steganografi citra.	Hasil simulasi menunjukkan peningkatan signifikan dalam hal ketahanan terhadap kompresi, dengan nilai PSNR > 40 dB dan MSE rendah pada kondisi kompresi te

Steganografi

Steganografi merupakan teknik penyembunyian informasi ke dalam media digital dengan tujuan menjaga kerahasiaan pesan tanpa menimbulkan perubahan yang mencolok secara visual. Konsep dasar ini menempatkan pesan pada elemen-elemen tertentu dari media sehingga tidak terdeteksi oleh pengamat biasa (Petitcolas, Anderson, & Kuhn, 1999). Pada penelitian ini, media penampung (cover-file) berupa video digital digunakan untuk menyisipkan pesan rahasia yang telah dikonversi ke dalam bentuk biner.

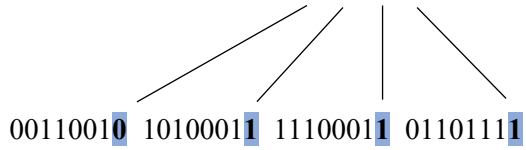
1) Teknik Penyembunyian Data

Penyembunyian data dilakukan dengan memodifikasi bit-bit tertentu pada komponen citra menggunakan metode *Least Significant Bit* (LSB). Pendekatan ini dipilih karena perubahan pada bit paling rendah memiliki dampak minimal terhadap kualitas visual media, serta terbukti efisien dalam kapasitas penyisipan pada berbagai jenis media digital (Provos & Honeyman, 2003). Perhatikan contoh sebuah susunan bit pada sebuah byte:



Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil. Misalkan segmen data citra sebelum perubahan:

00110011 10100010 11100010 01101111
Segmen data citra setelah '0 1 1 1' disembunyikan:



2) Ukuran Data yang Disembunyikan

Ukuran data yang akan disembunyikan bergantung pada ukuran berkas penampung. Pada citra 24-bit yang berukuran 256 × 256 piksel terdapat 65536 piksel, setiap piksel berukuran 3 byte (komponen *Red Green Blue*/RGB), berarti seluruhnya ada 65536 × 3 = 196608 byte. Karena setiap byte hanya bisa menyembunyikan satu bit di LSB-nya, maka ukuran data yang akan disembunyikan di dalam citra maksimum 196608/8 = 24576 byte. Ukuran data ini harus dikurangi dengan panjang nama berkas, karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama berkasnya.

3) Teknik Ekstraksi Data

Data yang disembunyikan di dalam berkas media dapat dibaca kembali dengan cara ekstraksi (*extraction*). Posisi byte yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan. Bilangan acak yang dihasilkan harus sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam *cover-file* dapat dikumpulkan kembali.

Discrete Cosine Transform (DCT)

Transformasi DCT mengubah blok citra 8×8 dari domain spasial ke domain frekuensi untuk memisahkan komponen frekuensi rendah, menengah, dan tinggi. Karena mata manusia lebih peka terhadap perubahan global daripada detail frekuensi tinggi, penyisipan pesan dapat dilakukan pada koefisien tertentu tanpa menurunkan kualitas visual secara signifikan. Oleh sebab itu, DCT banyak digunakan pada kompresi dan steganografi untuk mempertahankan kualitas citra (Gonzalez & Woods, 2018). Persamaan DCT dapat didefinisikan sebagai persamaan 1 berikut:

$$F(u,v) = \frac{1}{\sqrt{2N}} C(u)C(v) \sum_{x=1}^{N} \sum_{y=1}^{N} f(x,y) \cos\left(\frac{(2x+1)u\pi}{2N}\right) cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (1)$$

$u = 1,2, \dots 8$ dan $v = 1,2, \dots 8$ di mana N = 8 dan besar $C(k)$ adalah:

$$C(k) = \begin{cases} 1/\sqrt{2} & untuk\ k = 0 \\ 1 & untuk\ lainnya \end{cases}$$

Sedangkan untuk menghitung nilai inversi DCT dilakukan dengan menggunakan persamaan 2 sebagai berikut:

$$f(x,y) = \frac{1}{\sqrt{2N}} \sum_{x=1}^{N} \sum_{y=1}^{N} C(u)C(v)F(u,v) \cos\left(\frac{(2x+1)u\pi}{2N}\right) cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (2)$$

$u = 1,2, \dots 8$ dan $v = 1,2, \dots 8$ di mana N = 8.

1) Perhitungan DCT

Citra berukuran MxN dipecah menjadi blok 8x8 piksel, kemudian dilakukan transformasi 2 dimensi (2-D) diskrit kosinus pada setiap blok. Nilai DCT dikalkulasi menggunakan persamaan 1 dan 2. Pada blok DCT, bagian atas kiri merupakan koefisien frekuensi rendah sedangkan bagian bawah kanan merupakan koefisien frekuensi tinggi. Nilai koefisien frekuensi rendah lebih tinggi dibanding nilai koefisien frekuensi tinggi.

2) Kuantisasi

Kuantisasi dilakukan setelah koefisien DCT dari setiap blok DCT dikalkulasi. Tujuan dilakukannya kuantisasi agar memperoleh citra dengan ukuran kecil. Nilai kuantisasi diperoleh dengan membagi setiap elemen blok DCT dengan nilai yang sesuai pada tabel matriks kuantisasi dan hasilnya dibulatkan ke angka integer terdekat. Oleh karena mata manusia sulit membedakan perbedaan pada komponen frekuensi tinggi, maka nilai frekuensi tinggi dapat dikompres lebih lanjut. Komponen bagian bawah kanan matriks kuantisasi nilainya tinggi, sehingga setelah dilakukan kuantisasi komponen frekuensi tinggi menjadi nol. Nilai koefisien blok kuantisasi "P" dapat dihitung menggunakan persamaan 3 berikut:

$$P(u,v) = F(u,v)/Q(u,v) \qquad (3)$$

Di mana F = Koefisien DCT dan Q = Matriks kuantisasi.

3) Penyisipan Data

Bit data pada pesan rahasia disisipkan ke dalam komponen koefisien kuantisasi dengan cara mengubah nilai LSB-nya.

Jika bit data "0", maka buat koefisien kuantisasinya genap
Jika bit data "1", maka buat koefisien kuantisasinya ganjil

Jika terdapat sebuah matriks citra P sebagai berikut:

MATRIKS 8X8 CITRA P

Indeks	1	2	3	4	5	6	7	8
1	10	4	2	5	1	0	0	0
2	3	9	1	2	1	0	0	0
3	-7	-5	1	-2	-1	0	0	0
4	-3	-5	0	-1	0	0	0	0
5	-2	1	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Ketika semua data sudah disisipkan ke dalam matriks P, maka susunannya akan berubah menjadi matriks P' sebagai berikut:

MATRIKS 8X8 CITRA P'

Indeks	1	2	3	4	5	6	7	8
1	10	**3**	2	5	**2**	0	0	0
2	3	9	**2**	2	1	0	0	0
3	-7	-5	1	-2	-1	0	0	0
4	-3	-5	0	-1	0	0	0	0
5	-2	1	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

4) Inversi Kuantisasi

Setelah pesan rahasia berhasil disisipkan, langkah selanjutnya yaitu melakukan proses inversi kuantisasi. Proses ini dilakukan dengan menggunakan persamaan 4 berikut:

$$F'(u,v) = P'(u,v).Q(u,v) \qquad (4)$$

Di mana F' = Koefisien inversi kuantisasi dan P' = Matriks kuantisasi yang telah disisipkan pesan rahasia.

5) Inversi Transformasi Diskrit Kosinus

Setelah mendapatkan nilai koefisien inversi kuantisasi, dilakukan proses inversi transformasi diskrit kosinus. Proses ini dikalkulasi menggunakan persamaan 2.

Pengujian Kualitas Steganografi

Ada dua cara pengukuran kualitas steganografi, yaitu pengukuran subjektif dan pengukuran objektif. Pengukuran objektif merupakan pengukuran secara matematis pada steganografi yang sedang diukur kualitasnya dan dapat dikerjakan secara otomatis oleh komputer. Berdasarkan ada tidaknya berkas referensi, pengukuran objektif dikelompokkan ke dalam tiga jenis, yaitu: (1) Jika berkas referensi tersedia secara penuh (*full reference*), (2) Jika hanya sebagian berkas referensi yang tersedia (*reduced reference*), dan (3) Jika berkas referensi tidak tersedia sama sekali (*no reference*).

1) *Mean Square Error*

Mean Square Error (MSE) merupakan parameter yang menunjukkan tingkat kesalahan piksel-piksel citra hasil pemrosesan signal, terhadap citra asli. Nilai dari pada parameter MSE ini dinyatakan dalam satuan *desibel* (dB). Untuk menghitung nilai MSE digunakan persamaan 5 sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{X=1}^{M} \sum_{y=1}^{N} \left|\left(f(x,y) - g(x,y)\right)^2\right| \qquad (5)$$

2) *Peak Signal to Noise Ratio*

Peak Signal to Noise Ratio (PSNR) merupakan besaran parameter yang menunjukkan rasio tingkat toleransi desau tertentu terhadap banyaknya desau pada suatu piksel citra. Desau yang dimaksudkan di sini adalah kerusakan piksel pada bagian tertentu dalam sebuah citra sehingga mempengaruhi kualitas piksel tersebut. Dengan kata lain PSNR menunjukkan nilai kualitas suatu piksel citra. Untuk menghitung nilai komponen PSNR dari sebuah citra dapat dilakukan melalui persamaan 6 sebagai berikut:

$$PSNR = {}^{20}\log 10\left(\frac{255}{\sqrt{MSE}}\right) \qquad (6)$$

PSNR yang lebih tinggi menunjukkan bahwa kualitas citra hasil keluaran lebih baik atau dapat dikatakan menyerupai citra aslinya. Nilai parameter PSNR ini dinyatakan dalam satuan *desibel* (dB). Nilai PSNR yang baik untuk citra adalah lebih besar dari 30 dB.

3) CER

CER adalah suatu perhitungan yang berkaitan dengan banyaknya jumlah karakter pesan rahasia yang rusak pada *stego-file*. Rumusan CER dapat dilihat pada persamaan 7 berikut:

$$CER = \frac{Jumlah\ karakter\ error}{Jumlah\ total\ karakter} \qquad (7)$$

Algoritma Penyisipan Pesan (Embed)

Langkah-langkah yang dilakukan pada proses *encode* pada saat menyisipkan pesan adalah sebagai berikut:

1) Baca pesan yang ingin disisipkan.
2) Ubah pesan menjadi rangkaian biner.

3) Baca *cover-file* yang telah dipilih.
4) Ekstrak semua rangkaian frame pada *cover-file*.
5) Ubah rangkaian frame yang akan disisipkan pesan/data rahasia menjadi nilai komponen YCbCr.
6) Ambil komponen *luminance* pada frame kemudian bagi menjadi blok-blok 8x8 piksel.
7) DCT diterapkan pada setiap blok untuk mendapatkan nilai koefisien DC dan AC.
8) Kuantisasi koefisien DCT pada setiap blok.
9) Ganti nilai LSB hasil kuantisasi di koordinat (4,4) dengan bit dari pesan/data rahasia secara sinambung pada setiap blok.
10) Terapkan kebalikan (inversi) kuantisasi pada setiap blok 8x8.
11) Terpakan inversi DCT pada setiap blok 8x8.
12) Buat frame baru (*stego-frame*) dari nilai komponen YCbCr.
13) Simpan *stego-frame* menjadi berkas *stego-video*.

Proses Pengungkapan Pesan (Extract)

Proses untuk mengekstraksi pesan secara garis besar hampir sama dengan proses penyisipan pesan namun menggunakan urutan proses yang berbeda dimana proses dilakukan secara terbalik. Untuk mengembalikan data ke dalam bentuk semula maka dilakukan proses sebagai berikut:

1) Baca berkas *stego-video*.
2) Ekstrak semua rangkaian frame pada *stego-video*.
3) Setiap rangkaian frame dipecah menjadi 8x8 blok piksel.
4) DCT diterapkan untuk setiap blok untuk mendapat nilai koefisien DCT.
5) Kuantisasi koefisien DCT pada setiap blok.
6) Hitung LSB dari koefisien DC secara sinambung.
7) Lakukan konversi LSB koefisien DC menjadi data/rangkaian biner.
8) Konversi data/rangkaian biner menjadi pesan/data rahasia.

3. HASIL DAN PEMBAHASAN

Uji Faktor Fidelity

Eksperimen pada uji kualitas *stego-video* dan *cover-file* menghasilkan perhitungan untuk mengukur tingkat desau. Hasil eksperimen uji kualitas video menggunakan persamaan 5 dan 6 disertakan pada Tabel 1 berikut ini:

Tabel 1 Hasil Implementasi Steganografi pada Video Digital

No.	Media Penampung	Keterangan	Hasil *Stego-Video*
1.	 Siang.avi	MSE : 9,50 PSNR : 39,58 dB	 Siang_Stego.avi
2.	 Rumah.avi	MSE : 7,44 PSNR : 40,27 dB	 Glass_stego.avi
3.	 Malam.avi	MSE : 1,97 PSNR : 45,56 dB	 Malam_Stego.avi
4.	 Indoor.avi	MSE : 3,47 PSNR : 43,06 dB	 Indoor_Stego.avi

5.	 Ayam.avi	MSE : 2,57 PSNR : 44,08 dB	 Ayam_Stego.avi

Hasil penyisipan pada tabel 1 menghasilkan *stego-video* yang sama persis dengan video aslinya. Durasi dan gambar pada tiap frame tidak berubah yaitu 300 frame. Perubahan hanya terjadi pada ukuran berkas video, dikarenakan telah terjadi perubahan susunan bit pada tiap frame video.

Faktor Robustness

Hasil uji kualitas faktor *robustness* dengan cara mengekstrak pesan pada *stego-video* yang telah dilakukan dengan cara manipulasi penajaman kontras, rotasi, ataupun *grayscale.* Hasilnya ditampilkan pada Tabel 2 berikut ini:

Tabel 2 Hasil uji *stego-file* terhadap manipulasi citra

No.	Jenis Manipulasi	Pesan yang Diungkap	Keterangan
1.	Penambahan Kontras	Tidak Ada	Aplikasi tidak dapat mendeteksi adanya pesan rahasia pada *stego-video*
2.	Rotasi 180^0	Tidak Ada	Aplikasi tidak dapat mendeteksi adanya pesan rahasia pada *stego-video*
3.	Pembesaran	Tidak Ada	Aplikasi tidak dapat mendeteksi adanya pesan rahasia pada *stego-video*
4.	Pengurangan Jumlah Frame	Sebagian	Aplikasi mendeteksi adanya pesan rahasia pada *stego-video*. Pesan yang diungkap hanya yang terkandung di dalam frame utuh
5.	Perubahan Rasio Frame	Semua	Aplikasi dapat mendeteksi adanya pesan rahasia pada *stego-video*
6.	Grayscale	Tidak Ada	Aplikasi tidak dapat mendeteksi adanya pesan rahasia pada *stego-video*

Hasil pada Tabel 2 menunjukkan bahwa penyisipan pesan pada video MJPEG berjalan dengan baik, namun proses ekstraksi gagal ketika video mengalami manipulasi rotasi dan *grayscale*. Kondisi ini terjadi karena teknik penyisipan pada domain DCT bersifat linier dan sensitif terhadap pergeseran nilai, sehingga perubahan struktural pada frame dapat merusak bit pesan. Meskipun demikian, metode DCT tetap terbukti sesuai untuk video MJPEG selama media tidak mengalami distorsi yang signifikan.

Tabel 3 Hasil Implementasi Steganografi berdasarkan panjang pesan yang disisipkan

No.	*Stego-Video*	Panjang Pesan				
		5%	**25%**	**50%**	**75%**	**105%**
1.	Siang_Stego.avi	Gagal	Berhasil	Berhasil	Berhasil	Gagal
2.	Rumah_Stego.avi	Gagal	Berhasil	Berhasil	Berhasil	Gagal
3.	Malam_Stego.avi	Gagal	Berhasil	Berhasil	Berhasil	Gagal
4.	Indoor_Stego.avi	Gagal	Berhasil	Berhasil	Berhasil	Gagal

5.	Ayam_Stego.avi	Gagal	Berhasil	Berhasil	Berhasil	Gagal

Berdasarkan Tabel 3, dapat dilihat bahwa ketika panjang pesan yang disisipkan ke dalam *cover-video* sangat pendek atau sangat banyak, maka pesan rahasia tersebut tidak bisa diungkap kembali. Pesan rahasia hanya bisa diungkap kembali ketika panjang pesan yang disisipkan pendek, menengah, atau panjang.

Dari pemaparan di atas dapat dikatakan bahwa penggunaan teknik DCT cocok untuk media penampung berupa video berkodek MJPEG.

***Faktor* Recovery**

Hasil eksperimen pada proses ekstraksi menggunakan *stego-video* dengan kodek MJPEG. Proses ekstraksi ini menghasilkan pesan rahasia berupa teks yang sama atau mendekati sama dengan pesan teks sisipan dari pengirim. Untuk menghitung berapa banyak karakter yang rusak akibat proses penyisipan dan ekstraksi aplikasi, maka digunakan CER sesuai dengan Persamaan 7. Semakin kecil nilai CER, maka proses penyisipan dan ekstraksi semakin baik. Hasil eksperimen proses ekstraksi disertakan pada Tabel berikut:

Tabel 4 Hasil Uji faktor *recovery*

No.	***Stego-Video***	**Nilai CER**			
		Normal	**Kontras +50%**	**Rotasi 90ºCW**	***Grayscale***
1.	Siang_Stego.avi	0,32%	0,32%	100%	100%
2.	Rumah_Stego.avi	0,64%	0,64%	100%	100%
3.	Malam_Stego.avi	0,11%	0,11%	100%	100%
4.	Indoor_Stego.avi	0%	0%	100%	100%
5.	Ayam_Stego.avi	0,37%	0,37%	100%	100%

Berdasarkan Tabel 4, diperoleh data bahwa proses ekstraksi pesan rahasia berupa teks dapat diimplementasikan pada *stego-video*. Ekstraksi tersebut menghasilkan pesan teks rahasia yang mirip dengan pesan teks rahasia yang asli. Pada eksperimen di atas, nilai CER rata-rata yang dihasilkan adalah 0,29%. Nilai CER tersebut memiliki makna bahwa proses penyisipan dan ekstraksi dilakukan dengan sempurna.

4. KESIMPULAN

Berdasarkan penelitian, pengujian, dan analisis yang dilakukan, maka didapatkan simpulan sebagai berikut:

1) Data rahasia pada berkas video digital telah berhasil diamankan dengan cara menyisipkan bit pesan ke dalam LSB koefisien dct pada setiap *frame* video, sehingga pengguna dapat melakukan pertukaran data secara aman.
2) Proses mengamankan data rahasia pada berkas video digital menggunakan teknik DCT intinya adalah dengan melakukan penyisipan dan ekstraksi pesan melalui aplikasi yang telah dibuat. Kebutuhan fungsional dari program, seperti proses penyisipan dan ekstraksi pesan rahasia dapat dilakukan dengan benar.
3) Proses penyisipan dan ekstraksi data rahasia telah berhasil dengan terpenuhinya syarat-syarat sebagai berikut:
   a) *Fidelity*
      Hasil pengujian terhadap lima data uji menunjukkan bahwa seluruh stego-video memiliki PSNR di atas 30 dB dengan rata-rata mencapai 42,51 dB, sehingga metode DCT dapat dikatakan memberikan fidelity yang baik pada video berkodek MJPEG. Meski demikian, kualitas stego-video cenderung menurun ketika panjang pesan yang disisipkan semakin besar, karena lebih banyak koefisien DCT yang harus dimodifikasi selama proses embedding.
   b) *Robustness*
      Berdasarkan pengujian faktor *robustness*, teknik DCT pada video berkodek MJPEG *robust* terhadap manipulasi penajaman kontras, namun tidak *robust* terhadap manipulasi data yang lain.
   c) *Recovery*

Rata-rata tingkat *recovery* hanya bisa dilakukan pada salah satu dari 3 jenis manipulasi yaitu penambahan kontras, sehingga metode ini rentan terjadi kerusakan terhadap operasi manipulasi.

DAFTAR PUSTAKA

Ahmed, N., Natarajan, T., & Rao, K. R. (1974). Discrete cosine transform. *IEEE Transactions on Computers, 100(1)*, 90–93. https://doi.org/10.1109/T-C.1974.223784

Awaludin, M. (2023). Perancangan Sistem Informasi Cuti Karyawan Berdasarkan Siklus Hidup Pengembangan Sistem Di Universitas Dirgantara Marsekal Suryadarma. *Jurnal Sistem Informasi Universitas Suryadarma*, *10*(2), 139–146. https://doi.org/10.35968/jsi.v10i2.1083

Awaludin, M., & Amelia, L. V. (2022). Penerapan Structural Equation Modeling (Sem) Dengan Lisrel Terhadap Perbedaan Tarif Penerbangan Pada Penumpang Domestik Di Bandara Halim Perdanakusuma. *Jurnal Sistem Informasi Universitas Suryadarma*, *9*(1). https://doi.org/10.35968/jsi.v9i1.855

Awaludin, M., Nuryadi, H., & Pribadi, G. N. (2024). *Sistem Otomatisasi Laporan untuk Optimalisasi Pelaporan Data Penelitian dan Pengabdian kepada Masyarakat di Universitas Dirgantara Marsekal Suryadarma*. *9675*, 1–7.

Faruqi, A. A., & Rozi, I. F. (2015). Implementasi Steganography Menggunakan Algoritma Discrete Cosine Transform. Jurnal Informatika Polinema, 2(1). https://doi.org/10.33795/jip.v2i1.52

Garno, G., Rizal, A., Solehudin, A., & Ekstanza, R. (2022). Comparison of Steganography Using the Discrete Cosine Transform Method on Image Based Bilinear, Nearest Neighbor and Spline Interpolation. JUITA: Jurnal Informatika, 9(1). https://doi.org/10.30595/juita.v9i1.7302

Gonzalez, R. C., & Woods, R. E. (2018). *Digital image processing* (4th ed.). Pearson.

Huang, Y., Liu, Z., Wu, Q., & Liu, X. (2024). Robust image steganography against JPEG compression based on DCT residual modulation. Signal Processing, 219, 109431. https://doi.org/10.1016/j.sigpro.2024.109431

Jadeja, A., Shah, K., & Jhaveri, M. (2023). Analytical review on video steganography techniques. GIS Science Journal, 10(4). https://doi.org/10.2139/ssrn.4428447

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26–34. https://doi.org/10.1109/MC.1998.4655281

Kompas. (2022). Dugaan kebocoran data oleh peretas Bjorka. *Kompas.com*.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). *Information hiding—a survey*. Proceedings of the IEEE, 87(7), 1062–1078. https://doi.org/10.1109/5.771065

Provos, N., & Honeyman, P. (2003). *Hide and seek: An introduction to steganography*. IEEE Security & Privacy, 1(3), 32–44. https://doi.org/10.1109/MSECP.2003.1203220

Rao, K. R., & Yip, P. (2014). *Discrete cosine transform: Algorithms, advantages, applications*. Academic Press.

Tutuncu, K., & Hacimurtazaoglu, M. (2021). KBM Based Variable Size DCT Block Approaches for Video Steganography. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 220–231. https://doi.org/10.18201/ijisae.2021473643

Yunus, M., & Harjoko, A. (2014). Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT. Indonesian Journal of Computing and Cybernetics Systems. https://doi.org/10.22146/ijccs.3498

Zhang, J., He, X., & Cao, Y. (2024). Errorless robust JPEG steganography using steganographic polar codes. EURASIP Journal on Information Security, 2024(22), Article 22. https://doi.org/10.1186/s13635-024-00173-4

Zhang, J., Wu, M., Wang, Z., & Liu, Y. (2024). Robust image steganography against JPEG compression based on DCT residual modulation. Signal Processing, 219, 109431. https://doi.org/10.1016/j.sigpro.2024.109431