



Analisis Performa Steganografi Hybrid DCT–DWT dengan Enkripsi AES-GCM dan Kompresi Zlib

Mokhamad Yusron Rafi*, Agung Budi Susanto, Makhsun

Program Pascasarjana, Prodi Magister Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia

Email: ^{1,*} mokhamadyusronrafi23@gmail.com, ² dosen02680@unpam.ac.id, ³ makhsun_toha@yahoo.com

Email Penulis Korespondensi: mokhamadyusronrafi23@gmail.com

Abstrak—Pertukaran data digital yang semakin intensif menuntut metode keamanan informasi yang tidak hanya melindungi isi pesan, tetapi juga menyamarkan keberadaannya. Penelitian ini menganalisis performa steganografi citra digital berbasis *Hybrid Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT) yang dikombinasikan dengan enkripsi *Advanced Encryption Standard-Galois/Counter Mode* (AES-GCM) serta kompresi zlib pada citra ruang warna RGB. Metode penelitian menggunakan eksperimen kuantitatif dengan membandingkan tiga skenario penyisipan, yaitu DCT, DWT, dan Hybrid DCT-DWT. Data uji berupa citra RGB beresolusi 256×256, 512×512, dan 1024×1024 piksel, sedangkan payload berupa dokumen digital berformat DOCX dan PDF dengan ukuran berbeda. Payload dikompresi menggunakan zlib, dienkripsi menggunakan AES-GCM, kemudian disisipkan ke dalam koefisien transformasi citra. Evaluasi dilakukan menggunakan *Peak Signal-to-Noise Ratio* (PSNR), *Mean Square Error* (MSE), keberhasilan ekstraksi, kapasitas payload, histogram, dan ketahanan terhadap manipulasi citra. Hasil pengujian menunjukkan bahwa ketiga metode berhasil melakukan penyisipan dan ekstraksi payload pada skenario normal. Pada payload kecil, nilai PSNR berada pada kategori tinggi, misalnya 48,66 dB pada citra 256×256 dan 60,73 dB pada citra 1024×1024. Peningkatan ukuran payload menurunkan PSNR dan menaikkan MSE. Hybrid DCT-DWT menunjukkan performa visual yang relatif sebanding dengan DCT dan DWT, serta unggul dari sisi fleksibilitas karena menggabungkan dua domain transformasi.

Kata Kunci: Steganografi; Hybrid DCT-DWT; AES-GCM; Kompresi Zlib; PSNR; MSE

Abstract—The increasing exchange of digital data requires information security methods that not only protect message content but also conceal its existence. This study analyzes the performance of digital image steganography based on Hybrid Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) combined with Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) encryption and zlib compression in RGB color images. The research employed a quantitative experimental method by comparing three embedding scenarios: DCT, DWT, and Hybrid DCT-DWT. The test data consisted of RGB images with resolutions of 256×256, 512×512, and 1024×1024 pixels, while the payload consisted of DOCX and PDF documents with different sizes. The payload was compressed using zlib, encrypted using AES-GCM, and embedded into image transform coefficients. The evaluation was conducted using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), extraction success, payload capacity, histogram analysis, and robustness against image manipulation. The results show that all methods successfully embedded and extracted payloads under normal scenarios. For small payloads, the PSNR values were in the high-quality category, such as 48.66 dB for 256×256 images and 60.73 dB for 1024×1024 images. Increasing payload size reduced PSNR and increased MSE. Hybrid DCT-DWT produced visual quality relatively comparable to DCT and DWT, while offering greater flexibility by combining two transform domains.

Keywords: Image Steganography; Hybrid DCT-DWT; AES-GCM; Zlib Compression; PSNR; MSE

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah meningkatkan intensitas pertukaran data digital melalui jaringan publik. Dokumen internal, dokumen bisnis, data penelitian, dan informasi pribadi sering dikirimkan dalam bentuk digital sehingga membutuhkan mekanisme perlindungan yang mampu menjaga kerahasiaan, integritas, dan ketersediaan informasi. Kriptografi dapat mengubah pesan menjadi bentuk yang tidak dapat dibaca, tetapi keberadaan ciphertext tetap dapat menimbulkan kecurigaan. Sebaliknya, steganografi berupaya menyembunyikan pesan rahasia ke dalam media digital sehingga keberadaan pesan tidak mudah diketahui oleh pihak ketiga. Dalam konteks citra digital, pesan disisipkan ke dalam cover image dan menghasilkan stego image yang secara visual diharapkan tetap mirip dengan citra asli.

Steganografi citra digital dapat diterapkan pada domain spasial maupun domain transformasi. Domain spasial seperti *Least Significant Bit* relatif sederhana dan memiliki kapasitas yang baik, namun lebih sensitif terhadap manipulasi citra karena perubahan langsung dilakukan pada nilai piksel. Domain transformasi, seperti *Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT), menyisipkan pesan pada koefisien frekuensi sehingga lebih sesuai untuk menjaga keseimbangan antara kualitas visual dan keamanan penyisipan. DCT dikenal efisien dalam representasi frekuensi dan banyak digunakan dalam kompresi citra, sedangkan DWT memiliki kemampuan multiresolusi karena membagi citra ke dalam sub-band LL, LH, HL, dan HH. Kedua metode tersebut memiliki karakteristik yang berbeda sehingga kombinasi keduanya berpotensi menjadi pendekatan yang lebih fleksibel.

Penelitian sebelumnya menunjukkan bahwa metode berbasis DWT mampu menghasilkan kualitas visual yang tinggi pada invisible watermarking, tetapi belum selalu mengintegrasikan kriptografi modern untuk melindungi isi payload (Syahdilan & Prawira, 2024). Kombinasi DCT-DWT juga telah digunakan pada media video dan mampu mempertahankan kualitas visual, namun kenaikan *payload* tetap menyebabkan penurunan kualitas *stego-video* (Pratama & Suartana, 2021). Pada citra RGB, integrasi AES dengan DWT menunjukkan nilai PSNR yang baik, namun pendekatan tersebut masih menggunakan satu domain transformasi sehingga belum mengeksplorasi pembagian karakteristik DCT dan DWT secara terpadu (Umam & Muslih, 2023). Penelitian lain menegaskan bahwa steganografi



DCT dapat menjaga kualitas citra digital, tetapi beberapa studi belum menyertakan evaluasi kuantitatif PSNR dan MSE secara lengkap (Imam Budi Setiawan, Latif Fajar Pramukti, 2023) (Saifuddin, Agus Rakhmadi Mido, 2020).

Integrasi steganografi dengan kriptografi menjadi penting karena pesan yang berhasil diekstraksi oleh pihak tidak berwenang tetap harus sulit dibaca tanpa kunci. AES-GCM relevan digunakan karena menyediakan authenticated encryption, yaitu enkripsi sekaligus autentikasi integritas data. (Susanti et al., 2024). menunjukkan bahwa algoritma kriptografi modern seperti AES-GCM memiliki keunggulan pada aspek keamanan dan efisiensi. Selain itu, kompresi lossless zlib digunakan untuk memperkecil ukuran payload sebelum dienkripsi dan disisipkan, sehingga rasio payload terhadap kapasitas cover image dapat ditekan. Pendekatan berlapis ini sejalan dengan penelitian cryptosteganography yang menggabungkan penyembunyian pesan dan perlindungan isi pesan (Mulyono et al., 2023) (Alanzy et al., 2023).

Permasalahan utama dalam penelitian ini adalah bagaimana metode *Hybrid DCT-DWT* dibandingkan dengan metode transformasi tunggal DCT dan DWT dalam menjaga kualitas citra stego pada ruang warna RGB. Kualitas tersebut dianalisis menggunakan parameter *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Square Error* (MSE). Nilai PSNR yang lebih tinggi menunjukkan kualitas rekonstruksi yang lebih baik, sedangkan nilai MSE yang lebih kecil menunjukkan distorsi piksel yang lebih rendah. Selain itu, penelitian juga menilai kapasitas payload, keberhasilan proses ekstraksi, perubahan histogram, dan ketahanan citra stego terhadap manipulasi dasar seperti cropping, rotate, resize, dan convert.

Kontribusi penelitian ini terletak pada analisis eksperimental terhadap tiga pendekatan steganografi, yaitu DCT, DWT, dan *Hybrid DCT-DWT*, dengan alur pengamanan *payload* yang sama berupa kompresi zlib dan enkripsi AES-GCM. Dengan demikian, perbandingan tidak hanya berfokus pada keberhasilan penyisipan, tetapi juga pada hubungan antara ukuran *payload*, resolusi citra, kapasitas penyisipan, dan kualitas visual citra stego. Hasil penelitian diharapkan dapat menjadi acuan dalam pemilihan metode steganografi transformasi untuk pengamanan dokumen digital berbasis citra RGB.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif. Eksperimen dilakukan untuk membandingkan performa tiga metode steganografi citra digital, yaitu DCT, DWT, dan *Hybrid DCT-DWT*. Pendekatan kuantitatif digunakan karena performa metode diukur melalui nilai numerik PSNR, MSE, kapasitas payload, dan status keberhasilan ekstraksi. Objek penelitian berupa citra digital RGB sebagai media penampung dan dokumen digital sebagai payload rahasia. Setiap skenario diuji menggunakan alur keamanan yang sama, yaitu payload dikompresi dengan zlib, dienkripsi menggunakan AES-GCM, kemudian disisipkan ke dalam citra melalui metode transformasi.

Variabel bebas dalam penelitian ini adalah metode steganografi, resolusi citra cover, ukuran payload, dan bit mode penyisipan. Variabel terikatnya adalah kualitas citra stego yang dinilai dari PSNR dan MSE, kapasitas maksimum payload, serta keberhasilan ekstraksi. Hipotesis kerja yang digunakan adalah bahwa metode *Hybrid DCT-DWT* mampu memberikan kualitas citra stego yang kompetitif dibandingkan metode DCT dan DWT karena menggabungkan kelebihan domain wavelet dan domain kosinus. Namun, kualitas akhir tetap dipengaruhi oleh rasio payload terhadap kapasitas citra dan jumlah bit yang dimodifikasi.

2.2 Tahapan Penelitian

Tahapan penelitian dimulai dari pengumpulan citra cover dan payload, analisis kebutuhan sistem, perancangan proses embedding dan extraction, implementasi metode, pengujian kualitas citra, pengujian kapasitas, pengujian ketahanan, serta analisis hasil. Citra cover yang digunakan memiliki resolusi 256×256, 512×512, dan 1024×1024 piksel. Payload berupa dokumen DOCX dan PDF dengan ukuran beragam, mulai dari puluhan kilobyte hingga lebih dari satu megabyte. Penggunaan variasi ukuran payload bertujuan untuk mengetahui perubahan PSNR dan MSE ketika beban penyisipan meningkat.

Pada tahap pra-pemrosesan, payload dikompresi menggunakan zlib untuk mengurangi redundansi data. Setelah itu payload dienkripsi menggunakan AES-GCM agar isi pesan terlindungi serta memiliki authentication tag. Hasil enkripsi dikonversi ke bentuk bitstream dan disisipkan ke dalam citra. Pada metode DCT, citra diproses dalam blok 8×8 dan bit payload dimasukkan pada koefisien non-DC menggunakan pendekatan kuantisasi. Pada metode DWT, citra didekomposisi menggunakan wavelet Haar satu level dan penyisipan dilakukan pada sub-band detail. Pada metode *Hybrid DCT-DWT*, payload dibagi menjadi dua bagian; bagian pertama disisipkan melalui DWT pada kanal Blue, sedangkan bagian berikutnya disisipkan melalui DCT pada kanal Green. Setelah proses embedding selesai, citra direkonstruksi menjadi stego image dan dievaluasi.

Tabel 1. Dataset Citra dan *Payload* Pengujian

Komponen	Jenis Data	Keterangan
Cover image	Pohon dan Kucing	RGB 256×256 piksel, format JPG
Cover image	Pesawat dan Lena	RGB 512×512 piksel, format JPG
Cover image	Pantai dan Gunung Bromo	RGB 1024×1024 piksel, format JPG



Komponen	Jenis Data	Keterangan
Payload	D1-D17	Dokumen DOCX dan PDF dengan ukuran 17,7 KB hingga 1,930 KB
Output	Stego image	Citra hasil penyisipan yang dievaluasi dengan PSNR, MSE, histogram, dan ekstraksi

2.3 Model Penyisipan dan Ekstraksi

2.3.1 Model Discrete Cosine Transform (DCT)

Model penyisipan pada DCT dilakukan dengan membagi kanal citra ke dalam blok 8×8 piksel (Alvin & Pahlevi, 2025). Setiap blok ditransformasi ke domain frekuensi menggunakan DCT (Setiadikarunia & Setiawan, 2025). Koefisien DC pada posisi awal dihindari karena membawa informasi utama citra, sedangkan koefisien non-DC digunakan untuk menyisipkan bit payload. Setelah koefisien dimodifikasi, inverse DCT diterapkan untuk menghasilkan kembali citra pada domain spasial. Model ini memanfaatkan karakteristik DCT yang relatif efisien dalam menjaga perubahan visual pada komponen frekuensi tertentu.

2.3.2 Model Discrete Wavelet Transform (DWT)

Pada model DWT, kanal citra didekomposisi menjadi sub-band cA, cH, cV, dan cD menggunakan wavelet Haar (Alvin & Pahlevi, 2025). Penyisipan dilakukan pada sub-band detail terlebih dahulu karena perubahan pada area detail lebih sulit diamati secara langsung oleh mata manusia. Jika payload membutuhkan ruang lebih besar, penyisipan dapat dilanjutkan pada sub-band lain sesuai kapasitas yang tersedia. Proses ekstraksi dilakukan dengan urutan yang sama seperti proses penyisipan agar bitstream payload dapat dibaca kembali secara tepat.

2.3.3 Model Hybrid DCT-DWT

Pada model Hybrid DCT-DWT, payload tidak dipaksa masuk ke satu domain transformasi saja. Payload dibagi berdasarkan kapasitas DWT, kemudian sisanya diproses dengan DCT. Pembagian ini memberikan fleksibilitas karena DWT dapat menjaga imperceptibility pada sub-band tertentu, sementara DCT dapat memanfaatkan struktur blok untuk penyisipan lanjutan. Setelah payload diekstraksi, bitstream hasil DWT dan DCT digabungkan kembali, didekripsi dengan AES-GCM, dan didekompresi menggunakan zlib untuk memperoleh dokumen asli.

Tabel 2. Skenario Pengujian Metode Steganografi

Metode	Media Penyisipan	Proses Utama	Parameter Evaluasi
DCT	Koefisien non-DC pada blok 8×8	Kompresi zlib, enkripsi AES-GCM, embedding DCT, IDCT	PSNR, MSE, ekstraksi, histogram
DWT	Sub-band wavelet pada kanal citra	Kompresi zlib, enkripsi AES-GCM, DWT Haar, embedding, IDWT	PSNR, MSE, ekstraksi, histogram
Hybrid DCT-DWT	DWT kanal Blue dan DCT kanal Green	Payload split, embedding DWT, embedding DCT, rekonstruksi citra	PSNR, MSE, ekstraksi, kapasitas, robustness

2.4 Parameter Evaluasi

Kualitas citra stego dievaluasi menggunakan MSE dan PSNR (Ashillah et al., 2025). MSE mengukur rata-rata kuadrat selisih antara piksel citra cover dan stego. Semakin kecil MSE, semakin rendah distorsi yang dihasilkan (Fauzi & Khairani, 2025). PSNR menghitung rasio antara nilai piksel maksimum dan derau akibat perubahan citra. Pada citra 8-bit RGB, nilai maksimum piksel adalah 255 (Ilham & Kirana, 2026). Nilai PSNR di atas 40 dB umumnya menunjukkan kualitas visual yang baik karena perubahan citra sulit diamati secara kasat mata.

2.4.1 MSE (Mean Square Error)

Mean Square Error adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi; MSE adalah nilai error kuadrat rata-rata antara citra asli (*cover-image*) dengan citra hasil penyisipan (*stego-image*) (Fauzi & Khairani, 2025) (Fitriyani & Fachri, 2026).

$$MSE = \frac{1}{M \times N \times C} \sum (I_{cover} - I_{stego})^2 \quad (1)$$

Dalam perhitungan tersebut, I_{cover} merupakan nilai piksel pada *cover image* atau citra asli sebelum proses penyisipan, sedangkan I_{stego} merupakan nilai piksel pada *stego image*, yaitu citra yang telah mengalami proses penyisipan. M menunjukkan dimensi tinggi citra, sementara N menunjukkan dimensi lebar citra. Selanjutnya, C merepresentasikan jumlah *channel* warna yang terdapat pada citra. Khusus pada citra RGB, nilai C = 3 karena terdiri atas tiga *channel*, yaitu merah (Red), hijau (Green), dan biru (Blue).

2.4.2 PSNR (Peak Signal to Noise Ratio)

Peak Signal to Noise Ratio merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan *decibel* (dB). PSNR digunakan untuk mengetahui perbandingan kualitas citra cover (asli) sebelum dan sesudah disisipkan pesan (Humayrah et al., 2023).

Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE (*Mean Square Error*).

$$PSNR = 10 \log_{10} \left(\frac{C_{max}^2}{MSE} \right) \quad (2)$$

Dalam perhitungan evaluasi citra, C_{max} merupakan nilai piksel terbesar yang terdapat pada keseluruhan citra, sedangkan MSE (*Mean Squared Error*) merupakan nilai yang diperoleh dari hasil perhitungan tingkat kesalahan antara citra yang dibandingkan. Kedua parameter tersebut digunakan untuk mendukung proses analisis dan evaluasi kualitas citra.

Selain PSNR dan MSE, penelitian ini mengevaluasi kapasitas payload dan ketahanan citra stego. Kapasitas menunjukkan jumlah data maksimum yang dapat disisipkan pada citra cover berdasarkan resolusi dan bit mode. Ketahanan diuji melalui cropping, rotate, resize, dan convert format. Pengujian ketahanan penting untuk mengetahui apakah payload masih dapat diekstraksi ketika citra mengalami perubahan struktur piksel atau kompresi ulang.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi Sistem

Implementasi sistem menghasilkan aplikasi steganografi yang mampu menjalankan proses encode dan decode pada metode DCT, DWT, dan Hybrid DCT-DWT. Pada proses encode, sistem membaca cover image dan payload, melakukan kompresi zlib, mengenkripsi payload dengan AES-GCM, menyisipkan bitstream ke dalam citra, kemudian menghasilkan stego image. Pada proses decode, sistem membaca stego image, mengambil header dan bit payload, melakukan dekripsi, serta mengembalikan payload ke format dokumen asal. Pengujian fungsional menunjukkan bahwa seluruh metode mampu mengekstraksi payload pada skenario tanpa manipulasi citra. Hal ini menunjukkan bahwa mekanisme header, urutan embedding, dan proses ekstraksi telah berjalan konsisten.

3.2 Hasil Analisis Pengujian

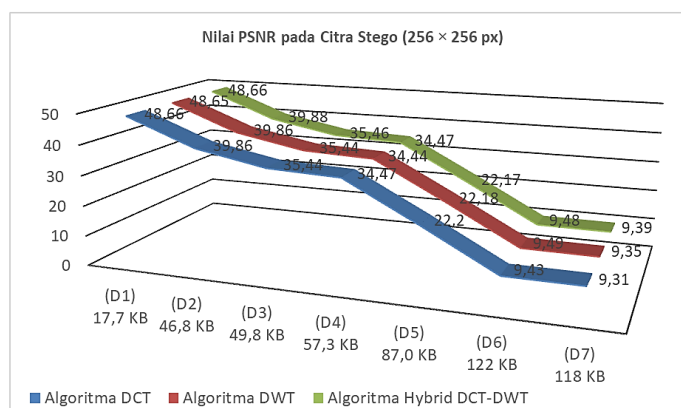
3.2.1 Analisis Pengujian Kualitas Citra (*Imperceptibility*)

Pengujian kualitas citra steganografi dapat ditentukan dengan beberapa metode, salah satu metode yang paling banyak digunakan adalah dengan mengukur nilai MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*).

a. Hasil Nilai PSNR dan MSE pada Citra Stego (256×256 px)

Tabel 3. Hasil Nilai PSNR pada Citra Stego (256×256 px)

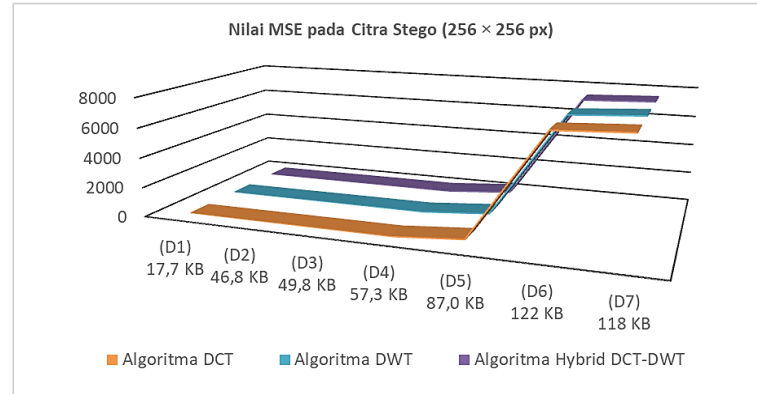
	Nilai PSNR pada Citra Stego Pohon.jpg 256×256 px (57,7 KB)						
	(D1) 17,7 KB	(D2) 46,8 KB	(D3) 49,8 KB	(D4) 57,3 KB	(D5) 87,0 KB	(D6) 122 KB	(D7) 118 KB
DCT	48.66	39.86	35.44	34.47	22.20	9.43	9.31
DWT	48.65	39.86	35.44	34.44	22.18	9.49	9.35
Hybrid	48.66	39.88	35.46	34.47	22.17	9.48	9.38



Gambar 1. Grafik Perbandingan Kualitas Citra Nilai PSNR pada Citra Stego (256×256 px)

Tabel 4. Hasil Nilai MSE pada Citra Stego (256×256 px)

	Nilai MSE pada Citra Stego Pohon.jpg 256×256 px (57,7 KB)						
	(D1) 17,7 KB	(D2) 46,8 KB	(D3) 49,8 KB	(D4) 57,3 KB	(D5) 87,0 KB	(D6) 122 KB	(D7) 118 KB
DCT	0.8856	6.7110	18.5857	23.2121	392.0971	7411.5815	7615.9155
DWT	0.8882	6.7207	18.5980	23.3996	394.0120	7306.6743	7552.5620
Hybrid	0.8858	6.6915	18.5049	23.2327	394.7007	7336.6802	7506.2910

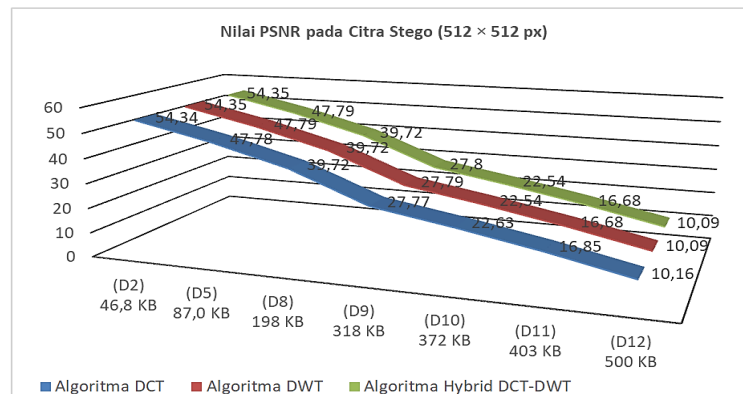


Gambar 2. Grafik Perbandingan Kualitas Citra Nilai MSE pada Citra Stego (256 × 256 px)

b. Hasil Nilai PSNR dan MSE pada Citra Stego (512 × 512 px)

Tabel 5. Hasil Nilai PSNR pada Citra Stego (512 × 512 px)

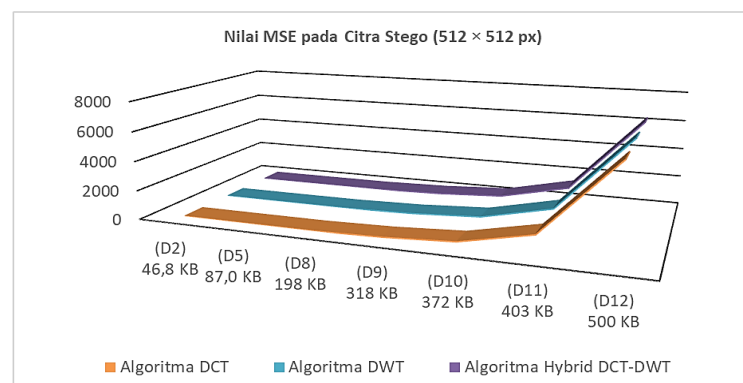
Nilai PSNR pada Citra Stego Pesawat.jpg 512 × 512 px (78,2 KB)							
	(D2) 46,8 KB	(D5) 87,0 KB	(D8) 198 KB	(D9) 318 KB	(D10) 372 KB	(D11) 403 KB	(D12) 500 KB
DCT	54.34	47.78	39.72	27.77	22.63	16.85	10.16
DWT	54.35	47.79	39.72	27.79	22.54	16.68	10.09
Hybrid	54.35	47.79	39.72	27.80	22.54	16.68	10.09



Gambar 3. Grafik Perbandingan Kualitas Citra Nilai PSNR pada Citra Stego (512 × 512 px)

Tabel 6. Hasil Nilai MSE pada Citra Stego (512 × 512 px)

Nilai MSE pada Citra Stego Pesawat.jpg 512 × 512 px (78,2 KB)							
	(D2) 46,8 KB	(D5) 87,0 KB	(D8) 198 KB	(D9) 318 KB	(D10) 372 KB	(D11) 403 KB	(D12) 500 KB
DCT	0.2396	1.0836	6.9334	108.5582	354.6708	1341.8967	6266.7852
DWT	0.2386	1.0825	6.9307	108.2580	362.2775	1396.5973	6375.2212
Hybrid	0.2389	1.0804	6.9309	107.9160	362.1286	1397.8192	6375.9663

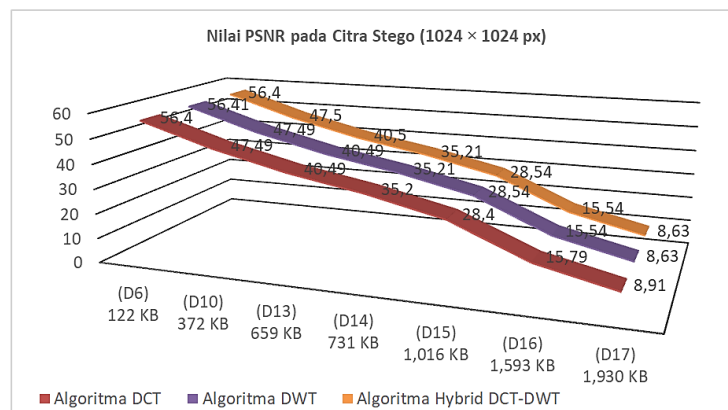


Gambar 4. Grafik Perbandingan Kualitas Citra Nilai MSE pada Citra Stego (512× 512 px)

c. Hasil Nilai PSNR dan MSE pada Citra Stego (1024×1024 px)

Tabel 7. Hasil Nilai PSNR pada Citra Stego (1024×1024 px)

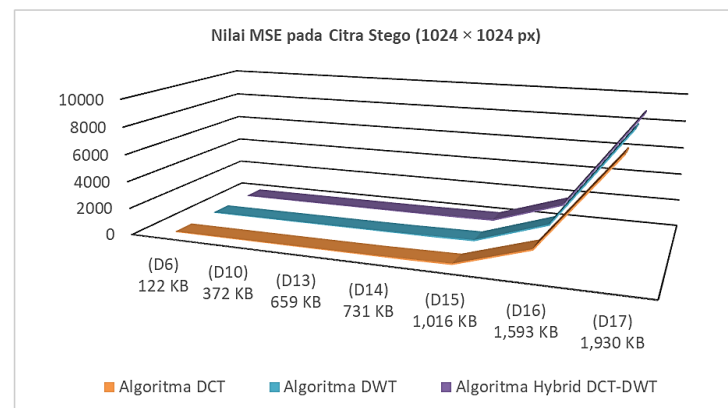
Nilai PSNR pada Citra Stego Pantai.jpg 1024×1024 px (469 KB)							
	(D6) 122 KB	(D10) 372 KB	(D13) 659 KB	(D14) 731 KB	(D15) 1,016 KB	(D16) 1,593 KB	(D17) 1,930 KB
DCT	56.40	47.49	40.49	35.20	28.40	15.79	8.91
DWT	56.41	47.49	40.49	35.21	28.54	15.54	8.63
Hybrid	56.40	47.50	40.50	35.21	28.54	15.54	8.63



Gambar 5. Grafik Perbandingan Kualitas Citra Nilai PSNR pada Citra Stego (1024×1024 px)

Tabel 8. Hasil Nilai MSE pada Citra Stego (1024×1024 px)

Nilai MSE pada Citra Stego Pantai.jpg 1024×1024 px (469 KB)							
	(D6) 122 KB	(D10) 372 KB	(D13) 659 KB	(D14) 731 KB	(D15) 1,016 KB	(D16) 1,593 KB	(D17) 1,930 KB
DCT	0.1490	1.1592	5.8150	19.6299	94.0194	1714.7157	8348.0195
DWT	0.1485	1.1592	5.8079	19.5705	91.0697	1816.9537	8914.6650
Hybrid	0.1489	1.1561	5.8011	19.5761	90.9463	1816.1846	8915.8350



Gambar 6. Grafik Perbandingan Kualitas Citra Nilai MSE pada Citra Stego (1024×1024 px)

Berdasarkan pengujian pada citra stego 256×256 px, 512×512 px, dan 1024×1024 px, kualitas citra yang dihasilkan oleh DCT, DWT, dan Hybrid DCT-DWT relatif sebanding. Namun, secara rata-rata keseluruhan, DCT sedikit lebih unggul, meskipun selisihnya sangat kecil.

Tabel 9. Algoritma dengan Kualitas Terbaik Berdasarkan Resolusi

Resolusi Citra	Algoritma Terbaik	Dasar Penilaian
256×256 px	Hybrid DCT-DWT	PSNR sedikit lebih tinggi dan MSE sedikit lebih rendah
512×512 px	DCT	MSE lebih rendah dan PSNR sedikit lebih stabil
1024×1024 px	DCT	MSE lebih rendah pada payload besar
Keseluruhan	DCT sedikit lebih unggul secara total	Rata-rata PSNR dan MSE lebih stabil, tetapi selisih antarmetode kecil



Pada Tabel 9 memperlihatkan bahwa metode terbaik dapat berubah sesuai resolusi dan ukuran payload. Pada resolusi 256×256, Hybrid DCT-DWT sedikit lebih baik karena pembagian payload dapat mengurangi konsentrasi perubahan pada satu domain. Pada resolusi 512×512 dan 1024×1024, DCT terlihat sedikit lebih stabil pada skenario tertentu. Akan tetapi, selisih numerik yang kecil memperlihatkan bahwa kualitas visual ketiga metode relatif sebanding. Oleh karena itu, pemilihan metode sebaiknya tidak hanya didasarkan pada satu nilai PSNR atau MSE, tetapi juga mempertimbangkan kebutuhan sistem, kompleksitas implementasi, kapasitas payload, serta skenario penggunaan.

Analisis histogram mendukung hasil numerik PSNR dan MSE. Pada payload kecil, histogram cover image dan stego image cenderung memiliki pola distribusi yang mirip, sehingga perubahan visual sulit diamati. Pada payload besar, distribusi histogram mulai menunjukkan perbedaan karena lebih banyak piksel atau koefisien yang dimodifikasi. Namun, perubahan histogram pada skenario yang masih memiliki PSNR di atas 40 dB tetap relatif terkendali. Hal ini memperkuat kesimpulan bahwa kualitas citra stego sangat bergantung pada kecukupan kapasitas cover image terhadap ukuran payload yang disisipkan.

3.2.2 Analisis Pengujian Pengaruh Besarnya Citra Cover

Hasil analisis kualitas citra menunjukkan bahwa ukuran payload merupakan faktor paling dominan terhadap perubahan PSNR dan MSE. Pada citra berukuran 256×256 piksel, payload kecil masih menghasilkan PSNR tinggi, tetapi payload besar menyebabkan penurunan kualitas secara drastis. Kondisi ini terjadi karena jumlah piksel dan koefisien yang tersedia relatif terbatas, sehingga payload besar memaksa lebih banyak koefisien mengalami modifikasi. Pada citra 512×512 piksel, kualitas masih baik untuk payload kecil dan menengah, tetapi payload 500 KB menyebabkan PSNR turun hingga sekitar 10 dB. Pada citra 1024×1024 piksel, sistem mampu mempertahankan kualitas yang lebih baik pada payload yang lebih besar, misalnya payload 659 KB masih menghasilkan PSNR sekitar 40,49-40,50 dB, yang berada pada batas kategori baik.

Tabel 10. Ringkasan Nilai PSNR dan MSE pada Payload Kecil dan Besar

Resolusi/Citra	Payload	DCT PSNR/MSE	DWT PSNR/MSE	Hybrid PSNR/MSE
256×256 Pohon	D1 17,7 KB	48,66 / 0,8856	48,65 / 0,8882	48,66 / 0,8858
256×256 Pohon	D7 118-122 KB	9,31 / 7615,9155	9,35 / 7552,5620	9,38 / 7506,2910
512×512 Pesawat	D1 17,7 KB	54,77 / 0,2167	54,78 / 0,2162	54,76 / 0,2175
512×512 Pesawat	D12 500 KB	10,16 / 6266,7852	10,09 / 6375,2212	10,09 / 6375,9663
1024×1024 Pantai	D1 17,7 KB	60,68 / 0,0556	60,71 / 0,0553	60,73 / 0,0550
1024×1024 Pantai	D17 1,930 KB	8,91 / 8348,0195	8,63 / 8914,6650	8,63 / 8915,8350

Berdasarkan Tabel 10, perbedaan performa DCT, DWT, dan Hybrid DCT-DWT pada payload kecil relatif sangat kecil. Pada citra 1024×1024 dengan payload D1, Hybrid DCT-DWT memperoleh PSNR 60,73 dB dan MSE 0,0550, sedikit lebih baik dibandingkan DCT dan DWT. Perbedaan kecil ini menunjukkan bahwa perubahan koefisien akibat penyisipan masih sangat rendah. Pada payload besar, seluruh metode mengalami penurunan kualitas. Fenomena ini mengonfirmasi hubungan berbanding terbalik antara PSNR dan MSE: ketika payload meningkat, perubahan piksel bertambah, MSE naik, dan PSNR menurun.

Pada resolusi 256×256, payload di atas kapasitas ideal menyebabkan nilai PSNR turun di bawah 20 dB. Nilai ini menunjukkan bahwa distorsi sudah tinggi dan kualitas citra tidak lagi layak untuk skenario steganografi yang mengutamakan imperceptibility. Hal serupa terjadi pada resolusi 512×512 ketika payload mencapai 500 KB. Namun, pada resolusi 1024×1024, payload 659 KB masih menghasilkan PSNR sekitar 40,50 dB pada Hybrid DCT-DWT dan MSE 5,8011. Hasil ini menunjukkan bahwa peningkatan resolusi memperbesar ruang penyisipan sehingga sistem lebih mampu menjaga kualitas citra, terutama ketika rasio payload terhadap kapasitas belum terlalu tinggi.

Perbandingan antaralgoritma menunjukkan bahwa DCT, DWT, dan Hybrid DCT-DWT memiliki nilai yang berdekatan pada sebagian besar skenario. DCT sedikit lebih stabil pada beberapa payload besar, sedangkan Hybrid DCT-DWT menunjukkan keunggulan pada skenario tertentu, terutama dari sisi fleksibilitas penyisipan karena payload dapat dibagi ke dalam dua domain transformasi. Dengan demikian, klaim utama penelitian bukan bahwa Hybrid DCT-DWT selalu paling unggul secara numerik pada seluruh skenario, melainkan bahwa metode tersebut mampu memberikan kualitas visual yang sebanding sambil menyediakan desain penyisipan yang lebih fleksibel. Pernyataan ini penting agar interpretasi hasil tetap objektif dan tidak melebihi-lebihkan peningkatan performa.

3.2.3 Analisis Pengujian Kapasitas Pesan

Kapasitas payload meningkat seiring kenaikan resolusi dan bit mode. Citra 256×256 memiliki kapasitas 16 KB pada 1-bit dan 128 KB pada 8-bit. Citra 512×512 memiliki kapasitas 64 KB pada 1-bit dan 512 KB pada 8-bit. Citra 1024×1024 memiliki kapasitas 256 KB pada 1-bit dan 2048 KB pada 8-bit. Meskipun bit mode tinggi meningkatkan kapasitas, kualitas visual dapat menurun karena lebih banyak bit koefisien yang dimodifikasi. Oleh karena itu, bit mode perlu dipilih secara proporsional terhadap ukuran payload dan target kualitas citra.

Tabel 11. Estimasi Kapasitas *Payload File* Berdasarkan Resolusi dan Bit Mode

Dimensi <i>Citra Cover</i>	Bit Mode	Estimasi Kapasitas <i>Payload File</i>
Pohon.jpg	1-bit	16,00 KB



Dimensi <i>Citra Cover</i>	Bit Mode	Estimasi Kapasitas <i>Payload File</i>
256 x 256 px (57,7 KB)	2-bit	32,00 KB
	3-bit	48,00 KB
	4-bit	64,00 KB
	5-bit	80,00 KB
	6-bit	96,00 KB
	7-bit	112,00 KB
	8-bit	128,00 KB
	1-bit	64,00 KB
Pesawat.jpg 512 x 512 px (78,2 KB)	2-bit	128,00 KB
	3-bit	192,00 KB
	4-bit	256,00 KB
	5-bit	320,00 KB
	6-bit	384,00 KB
	7-bit	448,00 KB
	8-bit	512,00 KB
	1-bit	256,00 KB
Pantai.jpg 1024 x 1024 px (469 KB)	2-bit	512,00 KB
	3-bit	768,00 KB
	4-bit	1024,00 KB
	5-bit	1280,00 KB
	6-bit	1536,00 KB
	7-bit	1792,00 KB
	8-bit	2048,00 KB

Pada Tabel 11 menunjukkan hubungan linear antara resolusi, bit mode, dan kapasitas penyisipan. Citra yang lebih besar menyediakan jumlah piksel dan koefisien lebih banyak sehingga dapat menampung payload lebih besar. Akan tetapi, kapasitas maksimum tidak selalu berarti konfigurasi terbaik. Pada penelitian ini, penggunaan payload yang mendekati batas kapasitas menyebabkan nilai MSE meningkat signifikan. Dengan kata lain, sistem perlu menggunakan validasi kapasitas otomatis agar pengguna tidak memilih payload yang terlalu besar untuk citra tertentu. Validasi ini penting untuk menjaga agar *stego image* tetap berada pada kategori kualitas visual yang dapat diterima.

Tabel 12. Pengaruh Bit Mode terhadap Kualitas Citra Stego

Bit Mode	Kapasitas Payload	PSNR	MSE	Kualitas Citra
1-bit	Sangat kecil	Sangat tinggi	Sangat rendah	Sangat baik
2-bit	Kecil	Tinggi	Rendah	Baik
3-bit	Sedang	Cukup tinggi	Sedang	Baik
4-bit	Sedang-besar	Menurun	Meningkat	Masih baik
5-6 bit	Besar	Rendah	Tinggi	Mulai menurun
7-8 bit	Sangat besar/maksimum	Sangat rendah	Sangat tinggi	Kurang baik

Pengujian bit mode memperlihatkan trade-off klasik pada steganografi, yaitu kapasitas berbanding terbalik dengan imperceptibility. Bit mode rendah menghasilkan kualitas visual yang lebih baik, tetapi kapasitas payload terbatas. Bit mode tinggi meningkatkan kapasitas, namun lebih berisiko menurunkan PSNR dan menaikkan MSE. Pada sistem yang ditujukan untuk dokumen rahasia, konfigurasi 1-bit hingga 3-bit lebih aman untuk menjaga kualitas visual, sedangkan 4-bit ke atas perlu digunakan secara selektif pada citra dengan resolusi besar. Hal ini sejalan dengan prinsip bahwa steganografi yang baik harus mempertahankan *fidelity* dan *imperceptibility* tanpa mengorbankan *recoverability payload*.

3.2.4 Analisis Pengujian Ketahanan Citra Stego Image

Keberhasilan ekstraksi pada skenario normal menunjukkan bahwa penggunaan zlib dan AES-GCM tidak mengganggu proses pengembalian *payload* selama struktur citra stego tidak berubah. Kompresi zlib membantu mengurangi ukuran *payload*, sedangkan AES-GCM memastikan *payload* yang disisipkan tidak dapat dibaca tanpa *password* yang sesuai. Namun, keamanan kriptografis ini tidak otomatis membuat *citra stego* tahan terhadap perubahan piksel. Jika citra mengalami manipulasi, struktur bit yang membawa *payload* dapat berubah sehingga proses ekstraksi gagal.

Tabel 13. Ringkasan Pengujian Ketahanan Citra Stego Image

Manipulasi	Dampak terhadap Citra	Hasil Ekstraksi	Interpretasi
<i>Cropping</i>	Sebagian area citra hilang	Gagal	Payload ikut terpotong atau posisi bit berubah
<i>Rotate</i>	Susunan piksel berubah	Gagal	Urutan koefisien tidak sama dengan proses



Manipulasi	Dampak terhadap Citra	Hasil Ekstraksi	Interpretasi
			embedding
<i>Resize</i>	Dimensi dan interpolasi piksel berubah	Gagal	Bit payload berubah akibat resampling
<i>Convert PNG ke JPG</i>	Terjadi kompresi lossy	Gagal	Perubahan nilai piksel merusak bit tersembunyi

Pada Tabel 13 menunjukkan bahwa citra stego masih sensitif terhadap manipulasi dasar. Semua skenario menyebabkan kegagalan ekstraksi. Hasil ini menunjukkan bahwa metode yang dikembangkan lebih sesuai untuk skenario penyimpanan atau pengiriman citra stego tanpa perubahan format dan tanpa proses pengeditan ulang. Dalam konteks praktis, *stego image* perlu disimpan dalam format lossless dan tidak boleh dikompresi ulang sebelum proses ekstraksi. Untuk kebutuhan sistem yang harus tahan terhadap serangan citra, metode ini masih perlu ditingkatkan dengan strategi embedding adaptif, redundansi payload, koreksi kesalahan, atau pemilihan koefisien yang lebih robust.

Dibandingkan penelitian sejenis, hasil penelitian ini memiliki posisi yang realistis. Beberapa studi berbasis LSB dan enkripsi dapat menghasilkan PSNR sangat tinggi pada payload tertentu, tetapi metode spasial cenderung sensitif terhadap kompresi dan manipulasi piksel (Hidayat & Andono, 2025), (Jatmoko et al., 2025). Studi berbasis DWT dan alpha blending juga menunjukkan PSNR tinggi pada skenario tertentu (Tevaramani & Ravi, 2022), sedangkan pendekatan DCT-DWT dengan optimasi atau teknik tambahan dapat meningkatkan imperceptibility namun sering menambah kompleksitas sistem (Anna Baita, Rohmatullah Batik Firmansyah, 2025). Dalam penelitian ini, kontribusi utama terletak pada integrasi kompresi zlib, AES-GCM, dan perbandingan tiga metode transformasi pada ruang RGB dengan payload dokumen nyata. Dengan demikian, penelitian memberikan gambaran praktis tentang batas kualitas citra ketika ukuran payload meningkat.

Secara umum, penelitian ini memperlihatkan bahwa *Hybrid DCT-DWT* layak digunakan sebagai alternatif steganografi citra RGB karena mampu menjalankan penyisipan dan ekstraksi payload secara konsisten pada skenario normal. Meskipun secara rata-rata DCT sedikit lebih unggul pada beberapa skenario numerik, *Hybrid DCT-DWT* tetap memiliki nilai akademik dan praktis karena desainnya memungkinkan distribusi payload ke dua domain transformasi. Model ini dapat menjadi dasar untuk penelitian lanjutan yang menambahkan optimasi pemilihan kanal warna, pemilihan sub-band, pemilihan koefisien DCT, serta strategi adaptif berdasarkan tekstur citra. Dengan pengembangan tersebut, *Hybrid DCT-DWT* berpotensi memberikan keseimbangan yang lebih baik antara kapasitas, *imperceptibility*, *security*, dan *robustness*.

3.3 Pembahasan

Pembahasan hasil menunjukkan bahwa hipotesis penelitian hanya terpenuhi secara parsial. *Hybrid DCT-DWT* tidak selalu menghasilkan PSNR tertinggi dan MSE terendah pada seluruh skenario, tetapi mampu memberikan kualitas yang relatif setara dengan DCT dan DWT serta menyediakan fleksibilitas arsitektural yang lebih baik. Pada payload kecil, ketiga metode menghasilkan perubahan visual yang sangat rendah. Pada payload besar, kualitas turun pada semua metode, sehingga faktor rasio *payload* terhadap kapasitas lebih dominan dibandingkan pilihan algoritma. Hasil ini penting karena menunjukkan bahwa optimasi steganografi tidak cukup dilakukan hanya dengan memilih metode transformasi, tetapi juga harus mengatur kapasitas, bit mode, kanal warna, dan format keluaran citra.

Temuan ini konsisten dengan literatur yang menyatakan bahwa kenaikan payload akan meningkatkan distorsi media penampung. Studi (Umam & Muslih, 2023) menunjukkan bahwa DWT dan AES mampu mempertahankan PSNR pada rentang baik untuk pesan tertentu, namun peningkatan ukuran pesan tetap berpengaruh terhadap kualitas. Penelitian (Mulyono et al., 2023) juga menegaskan bahwa kombinasi kriptografi dan steganografi dapat menjaga keamanan data, tetapi aspek visual tetap perlu diukur secara objektif. Hasil penelitian ini memperluas pembahasan tersebut dengan menunjukkan bahwa integrasi AES-GCM dan zlib dapat diterapkan pada payload dokumen sebelum proses transformasi tanpa menghambat ekstraksi normal. Dengan demikian, pendekatan keamanan berlapis dapat diterapkan, tetapi tetap membutuhkan kontrol kualitas citra.

Keterbatasan utama penelitian ini terletak pada robustness. Seluruh manipulasi citra yang diuji menyebabkan kegagalan ekstraksi, terutama karena perubahan struktur piksel dan koefisien tidak dapat dikompensasi oleh metode ekstraksi. Keterbatasan ini menunjukkan bahwa metode lebih tepat disebut sebagai *secure image embedding* untuk skenario lossless, bukan robust watermarking untuk citra yang akan diedit atau dikompresi ulang. Penelitian lanjutan dapat mengintegrasikan error correction code, embedding berulang, pemilihan koefisien berbasis tekstur, atau pendekatan optimasi berbasis kecerdasan buatan untuk meningkatkan ketahanan tanpa mengorbankan PSNR secara signifikan.

4. KESIMPULAN

Penelitian ini berhasil menerapkan dan membandingkan steganografi citra digital RGB menggunakan metode DCT, DWT, dan *Hybrid DCT-DWT* yang dipadukan dengan kompresi zlib dan enkripsi AES-GCM. Hasil pengujian menunjukkan bahwa ketiga metode mampu menjalankan proses penyisipan dan ekstraksi payload pada skenario normal, serta



menghasilkan citra stego dengan kualitas visual yang baik ketika ukuran payload masih proporsional terhadap kapasitas citra. Nilai PSNR cenderung tinggi dan MSE rendah pada payload kecil, misalnya lebih dari 48 dB pada citra 256×256 dan lebih dari 60 dB pada citra 1024×1024. Namun, peningkatan ukuran payload menyebabkan penurunan PSNR dan peningkatan MSE pada seluruh metode. Hybrid DCT-DWT belum menunjukkan dominasi numerik pada semua skenario, tetapi memiliki keunggulan dari sisi fleksibilitas karena menggabungkan domain DWT dan DCT dalam satu alur penyisipan. Dengan demikian, metode hybrid dapat menjadi alternatif yang efektif untuk pengamanan dokumen digital berbasis citra, terutama pada skenario penyimpanan atau pengiriman tanpa manipulasi citra. Keterbatasan penelitian ini adalah rendahnya ketahanan terhadap cropping, rotate, resize, dan convert format, karena seluruh manipulasi tersebut menyebabkan kegagalan ekstraksi. Penelitian selanjutnya disarankan mengoptimalkan pemilihan kanal RGB, sub-band DWT, koefisien DCT, bit mode, serta menambahkan parameter evaluasi seperti SSIM, BER, NCC, histogram correlation, error correction, dan analisis steganalysis agar kualitas, kapasitas, keamanan, dan robustness dapat ditingkatkan secara lebih komprehensif.

REFERENCES

- Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. *Mdpi: Applied Sciences*, 13(21), 1–20. <https://doi.org/10.3390/app132111771>
- Alvin, F., & Pahlevi, S. S. (2025). Analisis Komparatif Kinerja DCT, DWT, dan PCA pada Teknik Kompresi Citra Lossy. *Jurnal Aplikasi Teknologi Dan Komputasi*, 1(2), 74–82. <https://journals.arc.es.org/jatekom/article/view/49>
- Anna Baita, Rohmatullah Batik Firmansyah, S. D. A. (2025). Optimasi Nilai Imperceptibility pada Watermarking Citra Warna Berbasis DCT-DWT. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, 10(1), 622–629. <https://doi.org/10.29100/jipi.v10i1.6878>
- Ashillah, S., Gulo, S. A., Rahmi, Y., & Niska, D. Y. (2025). Implementasi algoritma pengolahan citra digital untuk perbaikan kualitas gambar. *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, 8(3), 274–280. <https://doi.org/10.47970/siskom-kb.v8i3.823>
- Fauzi, I., & Khairani, M. (2025). Analisis Perbandingan Kapasitas Penyisipan Data dan Kualitas Citra Dalam Teknik Steganografi LSB dan MSB Menggunakan Peak to Signal to Noise Ratio dan Mean Squared Error. *Jurnal Ilmu Komputer Dan Sistem Informasi*, 4(3), 344–355. <https://doi.org/10.70340/jirsi.v4i3.236>
- Fitriyani, L. A., & Fachri, F. (2026). Penerapan Teknik Steganografi dalam Gambar pada Aplikasi Telegram Menggunakan Metode Least Significant Bit (LSB). *Jurnal Teknologi Informasi Dan Multimedia*, 8(2), 357–368. <https://doi.org/10.35746/jtim.v8i2.1021>
- Hidayat, S., & Andono, P. N. (2025). Analisis Keamanan Steganografi Multi-Layer dengan Enkripsi Vigenère dan Caesar Cipher pada Citra Digital. *Jurnal Pendidikan Dan Teknologi Indonesia (JPTI)*, 5(3), 869–880. <https://doi.org/10.52436/1.jpti.786>
- Humayrah, R., Elhanafi, A. M., & Batubara, M. T. (2023). Analisa Histogram dan PSNR Pada Citra True Color Dalam Pengamanan Teks Menggunakan Spread Spectrum dan LSB. *Jurnal Ilmu Komputer Dan Sistem Informasi*, 2(1), 72–84. <https://doi.org/10.70340/jirsi.v2i1.48>
- Ilham, M., & Kirana, C. (2026). Perbandingan Kualitas Citra Grayscale Steganografi Metode LSB dan DCT Berdasarkan PSNR dan SSIM. *Journal of Information System Management (JOISM)*, 7(2), 330–337. <https://doi.org/10.24076/joism.2026v7i2.2492>
- Imam Budi Setiawan, Latif Fajar Pramukti, A. T. H. (2023). Algoritma Discrete Cosine Transform (DCT) untuk Pengamanan Citra Digital Dengan OTP Berbasis Web. (*JUKOMTEK*): *Jurnal Komputer Dan Teknologi*, 2(1), 18–26. <https://doi.org/10.58290/jukomtek.v1i2.52>
- Jatmoko, C., Sinaga, D., Lestiawan, H., Astuti, E. Z., Sari, C. A., & Fajar, G. (2025). Optimized Visualization of Digital Image Steganography using LSB and AES for Secret Key Encryption. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 10(3), 377–386. <https://doi.org/10.22219/kinetik.v10i3.2252>
- Mulyono, I. U. W., Kusumawati, Y., & Ningrum, N. K. (2023). Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher. *Jurnal Masyarakat Informatika*, 14(1), 16–28. <https://doi.org/10.14710/jmasif.14.1.51484>
- Pratama, A. S., & Suartana, I. M. (2021). Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT. *JIEET: (Journal Information Engineering and Educational Technology)*, 5(1), 13–18. <https://doi.org/10.26740/jieet.v5n1.p13-18>
- Saifuddin, Agus Rakhmadi Mido, E. I. H. U. (2020). Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android. *Progresif: Jurnal Ilmiah Komputer*, 16(1), 25–36. <https://doi.org/10.35889/progresif.v16i1.425>
- Setiadikarunia, D., & Setiawan, A. (2025). Analisis Watermarking Citra Digital Berbasis Contourlet Transform dan DCT dalam Ruang Warna RGB, YCbCr, dan YIQ. *Jurnal Telematika*, 20(2), 74–84. <https://doi.org/10.61769/telematika.v20i2.741>
- Susanti, A., Prasetya, B. A., Pangesti, O. D., Suryawati, L. D., & Saputro, I. A. (2024). Perbandingan Kinerja dan Keamanan Algoritma Kriptografi Modern AES-GCM dengan CHACHA20-POLY1305. *Infomatek*, 26(2), 253–264. <https://doi.org/10.23969/infomatek.v26i2.19255>



- Syاهدیلان, A., & Prawira, M. A. (2024). Implementasi Algoritma Discrete Wavelet Transform untuk Menambahkan Invisible Watermarking Pada Citra Digital. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(6), 12205–12217. <https://doi.org/10.36040/jati.v8i6.11711>
- Tevaramani, S. S., & Ravi, J. (2022). Image Steganography Performance Analysis Using Discrete Wavelet Transform and Alpha Blending for Secure Communication. *Global Transitions Proceedings*, 3(1), 208–214. <https://doi.org/10.1016/j.gltp.2022.03.024>
- Umam, C., & Muslih, M. (2023). Enkripsi Data Teks Dengan AES dan Steganografi DWT. *InComTech : Jurnal Telekomunikasi Dan Komputer*, 13(1), 28. <https://doi.org/10.22441/incomtech.v13i1.15059>