 ISSN:2302-8149
e-ISSN:2540-9719

Peningkatan *Steganografi* DCT pada JPEG menggunakan *Adaptive LSB Matching* untuk Resistensi Deteksi Entropi

Improving DCT-based JPEG Steganography using Adaptive LSB Matching for Resistance to Entropy-based Detection

[1]Intan Utami*, [2]Senie Destya, [3]Miko Kastomo Putro
[1,2,3]Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[1,2,3]Jl. Ring Road Utara Sleman, D.I.Yogyakarta, Indonesia
*e-mail: Intanutami@students.amikom.ac.id

(***received*:** 25 December 2025, ***revised*:** 5 February 2026, ***accepted*:** 6 February 2026)

Abstrak

Keamanan transmisi data menjadi isu krusial di era digital, di mana steganografi berperan penting dalam menyembunyikan informasi rahasia ke dalam media digital. Permasalahan utama pada steganografi berbasis *Discrete Cosine Transform* (DCT) konvensional pada citra JPEG adalah kerentanannya terhadap deteksi statistik melalui analisis entropi dan risiko penurunan kualitas visual yang signifikan. Penelitian ini bertujuan untuk meningkatkan teknik steganografi DCT guna meminimalkan deteksi entropi sekaligus mempertahankan nilai *Peak Signal-to-Noise Ratio* (PSNR) yang optimal. Metode yang diusulkan menggunakan pendekatan *Adaptive LSB Matching* yang menyisipkan pesan pada koefisien frekuensi rendah hingga menengah dengan mekanisme penyesuaian nilai ($x \pm 1$), yang kemudian dibandingkan kinerjanya dengan metode DCT Standar. Hasil eksperimen menunjukkan bahwa metode usulan mampu mempertahankan kualitas visual dengan rata-rata PSNR sebesar 40,41 dB pada beban pesan maksimum dan menekan selisih entropi (ΔH) hingga angka 0,00251. Hal ini membuktikan bahwa teknik yang dikembangkan lebih tangguh terhadap serangan steganalisis statistik dan memiliki fidelitas visual yang lebih baik dibandingkan metode konvensional.

Kata kunci: steganografi citra, discrete cosine transform, analisis entropi, LSB matching, keamanan informasi

Abstract

Data transmission security has become a critical issue in the digital era, where steganography plays an important role in concealing confidential information within digital media. A key limitation of conventional Discrete Cosine Transform (DCT)-based steganography in JPEG images is its vulnerability to statistical detection through entropy analysis, as well as the risk of significant degradation in visual quality. This study aims to enhance DCT-based steganography techniques to minimize entropy-based detection while maintaining an optimal Peak Signal-to-Noise Ratio (PSNR). The proposed method employs an Adaptive LSB Matching approach by embedding messages into low-to-mid frequency coefficients using an adjustment mechanism (x±1). The performance of this method is then compared with the standard DCT approach. Experimental results show that the proposed method is able to preserve visual quality, achieving an average PSNR of 40.41 dB under maximum payload conditions, while reducing the entropy difference (ΔH) to 0.00251. These findings demonstrate that the developed technique is more robust against statistical steganalysis attacks and provides better visual fidelity compared to conventional methods.

Keywords: *image steganography, discrete cosine transform, entropy analysis, LSB matching, information security*

1 Pendahuluan

Seiring dengan pesatnya perkembangan internet dan teknologi komunikasi, insiden keamanan siber seperti pencurian data dan pelanggaran privasi telah menjadi kejadian yang semakin sering dan mengkhawatirkan di seluruh dunia [1]. Kebutuhan untuk melindungi informasi rahasia selama transmisi data menjadi sangat mendesak karena metode komunikasi konvensional sering kali rentan

 ISSN:2302-8149
e-ISSN:2540-9719

terhadap intersepsi oleh pihak yang tidak berwenang [2]. Untuk menjawab tantangan "kejadian" peretasan ini, steganografi digunakan sebagai teknik menyembunyikan keberadaan pesan rahasia di dalam media pembawa sehingga tidak menimbulkan kecurigaan siapa pun [3]. Berbeda dengan kriptografi yang hanya mengacak isi pesan namun tetap terlihat mencurigakan, steganografi bertujuan untuk membuat komunikasi rahasia sama sekali tidak terlihat oleh pengamat [4]. Oleh karena itu, pengembangan metode steganografi yang tangguh menjadi solusi krusial untuk memastikan keamanan pertukaran data di lingkungan digital yang tidak aman [5].

Dalam penelitian ini, format citra JPEG dipilih secara spesifik sebagai media penampung karena karakteristiknya yang sangat efisien dalam menangani foto dengan gradien warna yang kompleks [6]. Berbeda dengan format PNG yang bersifat *lossless* namun cenderung menghasilkan ukuran berkas yang besar, JPEG menggunakan teknik kompresi *lossy* yang memungkinkan ukuran berkas jauh lebih kecil tanpa mengorbankan rentang warna secara signifikan [6]. Efisiensi penyimpanan dan transmisi ini menjadikan JPEG format yang paling dominan dan ideal untuk aplikasi modern, namun karakteristik kompresinya menimbulkan tantangan tersendiri bagi metode steganografi tradisional [6]. Metode domain spasial seperti *Least Significant Bit* (LSB) terbukti tidak cocok untuk JPEG karena data yang disisipkan mudah hilang saat proses kompresi membuang data frekuensi tinggi [7]. Oleh karena itu, teknik steganografi harus beradaptasi dengan bekerja pada domain frekuensi, khususnya menggunakan *Discrete Cosine Transform* (DCT) yang menjadi basis standar JPEG [8].

Meskipun teknik berbasis DCT menawarkan ketahanan yang lebih baik, penyisipan data pada koefisien frekuensi tetap memiliki risiko meninggalkan jejak statistik yang dapat dideteksi [9]. Perubahan pada koefisien DCT dapat mengubah histogram gambar secara tidak wajar, yang kemudian menjadi celah bagi serangan steganalisis statistik seperti analisis *Regular-Singular* (RS) untuk mendeteksi keberadaan pesan [10]. Masalah utama yang sering terjadi adalah metode yang ada saat ini kurang memperhatikan kesamaan konten antar blok DCT, sehingga menyebabkan distorsi yang tidak perlu dan memudahkan deteksi [11]. Selain itu, modifikasi pada koefisien frekuensi juga berpotensi menurunkan kualitas visual citra yang secara langsung mempengaruhi nilai *Peak Signal-to-Noise Ratio* (PSNR) [12]. Menjaga keseimbangan antara kapasitas penyisipan dan ketidaktampakan visual merupakan tantangan teknis yang rumit dalam steganografi domain transformasi [13].

Untuk mengatasi permasalahan deteksi histogram dan penurunan kualitas visual tersebut, penelitian ini mengusulkan pendekatan yang lebih adaptif dalam memodifikasi koefisien DCT [14]. Fokus utama adalah meminimalkan perubahan statistik pada histogram gambar sehingga pesan rahasia dapat bertahan dari serangan analisis statistik modern [1]. Selain itu, teknik ini dirancang untuk memastikan bahwa distorsi yang terjadi tetap berada di bawah ambang batas persepsi manusia, yang dibuktikan dengan nilai PSNR yang tinggi [15]. Penggunaan algoritma optimasi tertentu diharapkan dapat menentukan lokasi penyisipan yang paling aman pada frekuensi menengah untuk menghindari artefak kompresi [7]. Dengan demikian, integritas citra *stego* dapat dipertahankan sekaligus mengamankan data yang disembunyikan [3].

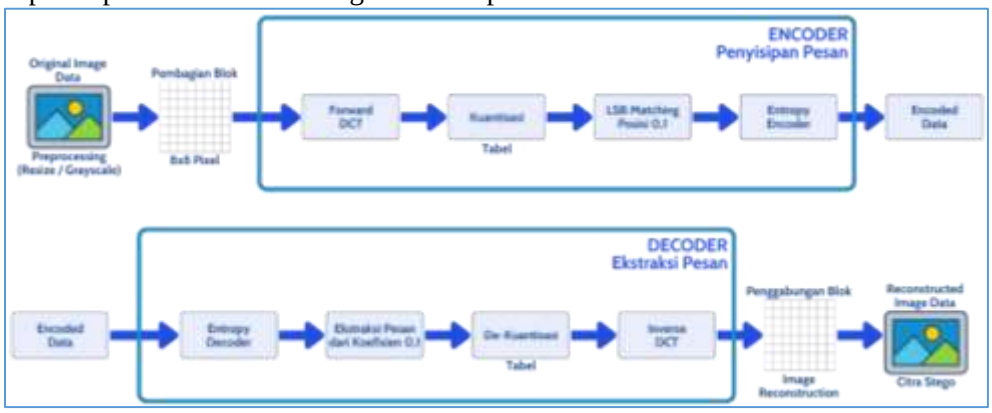
Berdasarkan paparan di atas, penelitian ini bertujuan untuk meningkatkan teknik steganografi DCT pada citra JPEG guna secara signifikan mengurangi risiko deteksi histogram serta mempertahankan nilai PSNR yang optimal. Signifikansi dari penelitian ini terletak pada penyediaan metode komunikasi rahasia yang aman dan efisien, yang mampu memanfaatkan popularitas format JPEG tanpa mengorbankan kualitas visual maupun keamanan data [6]. Penelitian ini diharapkan dapat memberikan kontribusi nyata dalam melawan ancaman steganalisis statistik yang semakin canggih di era pertukaran informasi digital saat ini [10]. Hasil akhirnya adalah sebuah sistem steganografi yang tangguh, di mana informasi rahasia dapat dikirimkan melalui jaringan publik tanpa memicu kecurigaan atau terdeteksi oleh pihak ketiga [8].

2 Tinjauan Literatur

Evolusi teknik steganografi citra digital telah menunjukkan transisi fundamental dari pemrosesan domain spasial menuju domain transformasi, yang dipicu oleh kebutuhan mendesak akan ketahanan data terhadap kompresi dan serangan steganalisis [1]. Literatur terdahulu mengonfirmasi bahwa metode domain spasial seperti *Least Significant Bit* (LSB), walaupun unggul dalam kapasitas, memiliki kelemahan fatal berupa kerentanan terhadap manipulasi sinyal sederhana dan kompresi *lossy* [16]. Sebagai respons terhadap kelemahan tersebut, penelitian terkini memusatkan perhatian pada *Discrete Cosine Transform* (DCT) yang menjadi basis kompresi JPEG, karena kemampuannya

 ISSN:2302-8149
e-ISSN:2540-9719

mendistribusikan energi citra ke dalam koefisien frekuensi yang lebih stabil [6]. Pendekatan ini memungkinkan penyisipan informasi dilakukan pada domain frekuensi terkuantisasi, yang secara teoritis mampu menjaga integritas perseptual citra jauh lebih baik dibandingkan manipulasi piksel langsung [17]. Guna memperjelas mekanisme transformasi data tersebut, kerangka kerja dasar proses penyisipan pesan pada domain DCT digambarkan pada Gambar 1 berikut:



Gambar 1 Diagram kerangka kerja penyisipan pesan pada domain frekuensi DCT

Dalam ranah steganografi berbasis DCT, berbagai strategi optimasi telah diajukan untuk meningkatkan efisiensi penyisipan dan keamanan. Penggunaan kode koreksi seperti *Hamming Code* telah diadopsi untuk meningkatkan efisiensi modifikasi, memungkinkan penyisipan data dengan jumlah perubahan koefisien yang minimal [18]. Selain itu, strategi pemilihan koefisien pada pita frekuensi menengah (*middle frequency*) sering diterapkan untuk menghindari distorsi visual yang nyata pada frekuensi rendah sekaligus mencegah penghapusan data oleh kompresi pada frekuensi tinggi [7]. Meskipun demikian, tantangan utama tetap terletak pada bagaimana menyeimbangkan kapasitas penyisipan dengan ketahanan statistik. Metode konvensional sering kali mengabaikan fakta bahwa perubahan koefisien DCT dapat mengubah karakteristik lokal citra yang dapat dideteksi. Perbandingan kritis antara metode spasial, metode frekuensi standar, dan pendekatan adaptif yang diusulkan dalam penelitian ini dirangkum dalam Tabel 1 berikut:

Tabel 1 Perbandingan metode steganografi

Karakteristik	Domain Spasial (LSB)	Domain Frekuensi (DCT Standar)	DCT Adaptif (Usulan)
Media Penyisipan	Piksel citra langsung (*spatial domain*)	Koefisien DCT terkuantisasi (*frequency domain*)	Koefisien DCT terpilih berdasarkan analisis Entropi
Ketahanan (*Robustness*)	Rendah (rentan kompresi & cropping)	Tinggi (tahan kompresi JPEG)	Tinggi (tahan kompresi & analisis statistik)
Kualitas Visual (PSNR)	Sangat Tinggi	Baik (tergantung *payload*)	Dipertahankan Tinggi (> 40dB)
Keamanan Statistik	Rentan analisis visual	Rentan deteksi perubahan Entropi	Tinggi (Meminimalkan anomali Entropi)

Meskipun metode berbasis DCT menawarkan ketahanan visual yang lebih baik, literatur terbaru menyoroti bahwa teknik penyisipan standar masih rentan terhadap steganalisis statistik yang berbasis pada pengukuran entropi. Entropi, sebagai ukuran ketidakpastian atau kompleksitas informasi dalam citra, menjadi indikator krusial dalam mendeteksi keberadaan pesan tersembunyi [19]. Penelitian menunjukkan bahwa penyisipan data yang tidak memperhatikan karakteristik lokal blok DCT cenderung meningkatkan nilai entropi secara tidak wajar pada area yang seharusnya memiliki entropi rendah (halus), sehingga memicu kecurigaan steganalis [10]. Metode *reversible* yang ada saat ini, meskipun mampu memulihkan citra asli, sering kali gagal mempertahankan profil entropi alami citra *stego* [15]. Kegagalan dalam menjaga karakteristik statistik ini menjadikannya target mudah bagi

 ISSN:2302-8149
e-ISSN:2540-9719

detektor modern [12]. Ketiadaan evaluasi kesamaan konten (*content similarity*) dalam proses penyisipan sering menjadi penyebab utama mengapa anomali entropi ini muncul [11].

Kesenjangan penelitian (*research gap*) yang signifikan teridentifikasi dari tinjauan ini adalah kurangnya mekanisme adaptif pada steganografi JPEG yang secara spesifik menjadikan parameter entropi sebagai panduan utama dalam pemilihan koefisien DCT [13]. Mayoritas penelitian sebelumnya berfokus pada minimalisasi distorsi visual (meningkatkan PSNR) atau kapasitas, namun mengabaikan dampak penyisipan terhadap distribusi entropi lokal. Akibatnya, metode yang ada sering kali mengorbankan keamanan statistik demi mempertahankan nilai PSNR yang tinggi, atau sebaliknya, sehingga citra *stego* tetap rentan terdeteksi oleh sistem keamanan canggih. Belum banyak penelitian yang secara spesifik mengintegrasikan mekanisme pemilihan koefisien adaptif yang dirancang khusus untuk meminimalkan perubahan entropi sekaligus menjaga fidelitas visual dalam satu kerangka kerja DCT [12].

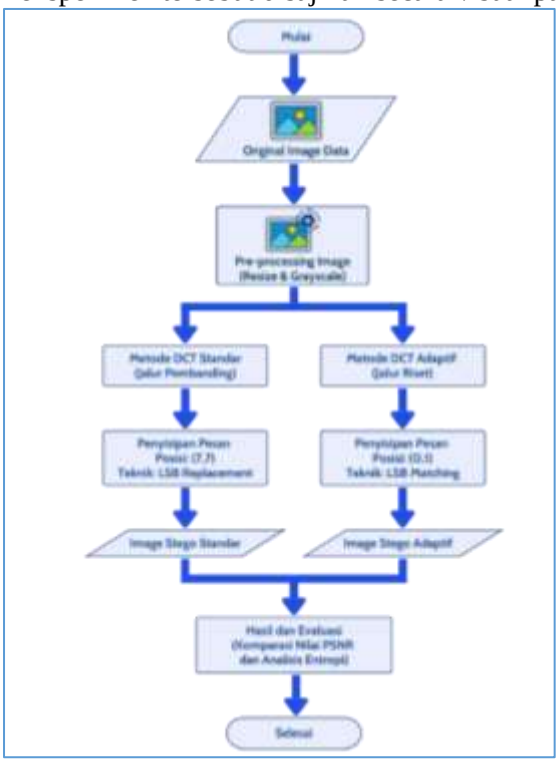
Oleh karena itu, penelitian ini berfokus pada bagian yang belum dikerjakan tersebut, yaitu pengembangan teknik steganografi DCT yang disempurnakan dengan algoritma adaptif untuk secara simultan mengurangi deteksi entropi dan mempertahankan nilai PSNR yang optimal. Pendekatan ini diharapkan dapat mengisi celah dalam literatur terkini dengan menyediakan keseimbangan yang lebih baik antara kapasitas penyisipan, kualitas visual, dan keamanan statistik terhadap serangan steganalysis.

3 Metode Penelitian

Penelitian ini mengimplementasikan dua teknik steganografi pada domain DCT citra JPEG, yaitu metode DCT Standar yang menggunakan *LSB Replacement* pada frekuensi tinggi dan metode DCT Adaptif yang diusulkan dengan menerapkan *LSB Matching* pada frekuensi rendah hingga menengah. Tujuan penelitian ini adalah membandingkan kinerja kedua metode secara komparatif, dengan menitikberatkan pada kemampuan metode usulan dalam menyeimbangkan kualitas visual (*imperceptibility*) dan keamanan statistik terhadap deteksi berbasis entropi.

A. Rancangan dan Alur Penelitian

Rancangan penelitian difokuskan pada evaluasi dua skenario eksperimen penyisipan pesan dalam proses kompresi citra JPEG. Pengumpulan data dilakukan melalui eksperimen penyisipan pesan teks biner ke dalam citra JPEG dengan menerapkan masing-masing metode melalui alur yang berbeda. Tahapan dan alur eksperimen tersebut disajikan secara visual pada Gambar 2:



Gambar 2 Diagram alur penelitian

 ISSN:2302-8149
e-ISSN:2540-9719

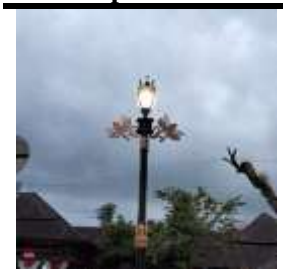
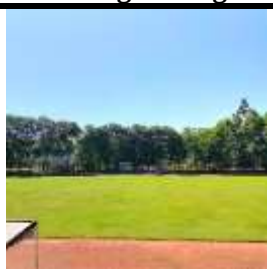
Sesuai dengan alur pada Gambar 2, prosedur pengumpulan data dibagi menjadi dua eksperimen yang berbeda:

1. Metode DCT Standar: Metode ini merepresentasikan pendekatan konvensional. Penyisipan pesan dilakukan pada koefisien frekuensi tinggi (posisi indeks matriks 7,7) dengan menggunakan teknik LSB Replacement. Metode ini dijadikan variabel kontrol untuk mengukur seberapa besar dampak distorsi dan kerentanan data pada metode standar.
2. Metode DCT Adaptif (Usulan): Metode ini merupakan implementasi dari teknik yang diusulkan. Penyisipan pesan difokuskan pada koefisien frekuensi rendah-menengah (posisi indeks matriks 0,1) dengan menggunakan teknik *LSB Matching* ($x \pm 1$). Pemilihan posisi frekuensi (0,1) ini didasarkan pada pertimbangan stabilitas energi; koefisien pada posisi ini memiliki nilai energi yang signifikan sehingga data yang disisipkan memiliki resistensi tinggi (tidak mudah hilang) terhadap tabel kuantisasi JPEG. Meskipun area ini lebih sensitif terhadap persepsi visual, potensi artifak diminimalisir oleh mekanisme adaptif *LSB Matching* yang tidak melakukan penggantian nilai secara kasar, melainkan hanya melakukan penyesuaian minimal (+1 atau -1). Hal ini bertujuan untuk menjaga keseimbangan antara ketahanan data dan minimalisasi jejak statistik entropi.

B. Ruang Lingkup, Data, dan Objek Penelitian

Objek penelitian ini menggunakan citra berformat JPEG yang terdiri dari empat sampel representatif: *Lampu Jalan 1*, *Lampu Jalan 2*, *Langit Siang*, dan *Langit Sore.*

Tabel 2 Daftar citra untuk penelitian

Lampu Jalan 1	Lampu Jalan 2	Langit Siang	Langit Sore
			
Kontras tinggi, objek dominan gelap terang	Banyak detail daun/pohon, tekstur kasar	Area langit luas, gradasi halus	Gradasi awan kompleks, pencahayaan lembut

Sampel citra dipilih secara *purposive* untuk merepresentasikan variasi karakteristik tekstur, mulai dari area *smooth* (langit) hingga area dengan detail frekuensi tinggi (lampu jalan). Variasi ini penting untuk menguji kemampuan adaptif algoritma terhadap kompleksitas visual yang berbeda. Sebagai tahap persiapan, seluruh citra dikonversi ke dalam ruang warna *grayscale* (kanal tunggal) dan dinormalisasi ke dimensi 512x512 piksel. Normalisasi dimensi ini dilakukan guna menjamin konsistensi pembagian blok DCT berukuran 8x8 piksel, sehingga menghasilkan total 4.096 blok per citra sebagai ruang tampung pesan (*payload capacity*)

C. Perangkat Penelitian

Penelitian ini dilaksanakan secara mandiri menggunakan perangkat komputer pribadi untuk menjalankan eksperimen dan analisis data. Spesifikasi perangkat yang digunakan meliputi:

1. Perangkat Keras (*Hardware*): Satu unit laptop ASUS Vivobook dengan spesifikasi prosesor 12th Gen Intel® Core™ i5-1235U, RAM 16.0 GB, dan Windows 11 (64-bit).
2. Perangkat Lunak (*Software*): Algoritma dibangun menggunakan bahasa pemrograman Python dengan dukungan pustaka (*library*) utama sebagai berikut:
   - OpenCV: Digunakan untuk akuisisi citra, konversi format warna, dan normalisasi dimensi (resizing).
   - NumPy: Digunakan untuk operasi aljabar matriks, termasuk manipulasi blok piksel dan perhitungan koefisien.
   - SciPy: Digunakan untuk eksekusi algoritma transformasi sinyal, yaitu Forward DCT dan Inverse DCT (IDCT).

 ISSN:2302-8149
e-ISSN:2540-9719

- Matplotlib: Digunakan untuk visualisasi histogram dan perbandingan citra hasil (stego-image).

D. Teknik Metode Usulan

Berdasarkan serangkaian eksperimen yang telah dilakukan, dirumuskan prosedur metode usulan *Adaptive LSB Matching* dengan tahapan sebagai berikut:

1. Transformasi Domain: Citra cover dibagi menjadi blok-blok berukuran 8x8 piksel yang tidak saling tumpang tindih (*non-overlapping*). Setiap blok kemudian dikonversi dari domain spasial ke domain frekuensi menggunakan fungsi Forward DCT (*FDCT*).
2. Kuantisasi dan Penentuan Target Frekuensi: Koefisien DCT dikuantisasi menggunakan tabel standar JPEG. Pada metode usulan (DCT Adaptif), proses penyisipan difokuskan pada koefisien frekuensi rendah-menengah (indeks matriks 0,1) pada setiap blok secara sekuensial. Pemilihan posisi frekuensi spesifik ini dilakukan untuk memanfaatkan karakteristik citra JPEG, di mana modifikasi pada area ini menghasilkan fluktuasi histogram yang lebih halus dibandingkan frekuensi tinggi, sehingga meminimalkan deteksi anomali entropi tanpa memerlukan pembuangan blok.
3. Penyisipan Pesan (*Embedding*) dengan LSB Matching: Pesan rahasia biner disisipkan ke dalam koefisien terpilih menggunakan teknik LSB Matching. Teknik ini bekerja secara adaptif dengan menyesuaikan nilai koefisien ($x \pm 1$) jika bit pesan tidak cocok dengan LSB koefisien. Jika x perlu diubah, operasi penambahan (x+1) atau pengurangan (x-1) dipilih secara acak atau berdasarkan nilai tetangga untuk memastikan distorsi yang dihasilkan menyerupai noise alami citra, berbeda dengan teknik penggantian (replacement) yang bersifat deterministik kaku.
4. Rekonstruksi Citra: Blok-blok DCT yang telah dimodifikasi dikembalikan ke domain spasial menggunakan Inverse DCT untuk menghasilkan citra stego akhir.

E. Definisi Operasional Variabel

Untuk menghindari ambiguitas dalam pengukuran, variabel penelitian didefinisikan sebagai berikut:

1. Variabel Bebas: Teknik penyisipan pesan, yaitu metode DCT Standar (Replacement di frekuensi tinggi) dan DCT Adaptif (Matching di frekuensi rendah)
2. Variabel Terikat:
   - Kualitas Visual (PSNR): Ukuran fidelitas citra stego terhadap citra asli dalam satuan desibel (dB).
   - Keamanan Statistik (Entropi): Tingkat ketidakpastian informasi dalam citra yang diukur dari distribusi histogram.
3. Variabel Terkendali: Ukuran citra (512x512 piksel), format citra (JPEG), dan panjang pesan rahasia yang disisipkan (*payload*).

F. Teknik Analisis Data

Data hasil simulasi dianalisis secara komparatif kuantitatif menggunakan dua parameter pengukuran:

1. Kualitas Visual (PSNR)

   Peak Signal-to-Noise Ratio (PSNR) digunakan untuk mengukur tingkat imperseptibilitas atau seberapa baik citra stego menyembunyikan pesan tanpa merusak visual. Nilai PSNR dihitung menggunakan persamaan (1).

$$PSNR = 10 \cdot log_{10} \left(\frac{MAX_I^2}{MSE} \right) \qquad (1)$$

   Nilai PSNR dihitung dengan membandingkan citra asli (*cover*) dan citra hasil penyisipan (*stego*). Target penelitian ini adalah mempertahankan nilai PSNR yang tinggi (sedikit distorsi) > 40 dB, yang mengindikasikan bahwa degradasi visual sangat minim dan sulit dibedakan oleh mata Manusia.
2. Keamanan Statistik (Entropi)

   Meskipun proses penyisipan pesan dilakukan pada domain frekuensi (koefisien DCT), pengukuran entropi dalam penelitian ini sengaja dilakukan pada domain spasial (distribusi intensitas piksel) pasca-rekonstruksi (Inverse DCT). Pendekatan ini dipilih untuk memvalidasi bahwa teknik LSB Matching ($x \pm 1$) pada domain frekuensi berhasil meratakan

 ISSN:2302-8149
e-ISSN:2540-9719

distribusi gangguan, sehingga tidak memicu lonjakan histogram yang ekstrem pada citra akhir (stego image) yang akan ditransmisikan. Perhitungan entropi dilakukan berdasarkan probabilitas kemunculan nilai intensitas piksel (k) dalam rentang kedalaman warna 8-bit ($0 - 255$). Perhitungan entropi didefinisikan pada Persamaan (2).

$$H = -\sum_{k=0}^{255} P_k \, log_2(P_k) \qquad (2)$$

Analisis difokuskan pada Selisih Entropi (ΔH) antara citra cover dan citra stego. Dalam implementasi kode, metode dianggap unggul jika menghasilkan ΔH yang mendekati 0. Nilai selisih yang kecil menunjukkan bahwa proses penyisipan tidak mengubah distribusi statistik citra secara signifikan, sehingga citra stego aman dari deteksi berbasis analisis entropi spasial.

4 Hasil dan Pembahasan

Hasil eksperimen perbandingan dua teknik steganografi pada domain DCT citra JPEG, yaitu metode DCT Standar (*LSB Replacement*) dan metode DCT Adaptif (*LSB Matching*) yang diusulkan. Evaluasi dilakukan berdasarkan dua parameter utama, yaitu kualitas visual (*imperceptibility*) yang diukur menggunakan PSNR dan keamanan statistik yang dianalisis melalui nilai entropi. Pengujian dilakukan pada empat citra JPEG sampel (Lampu Jalan 1, Lampu Jalan 2, Langit Siang, dan Langit Sore) dengan tiga variasi beban pesan rahasia (*payload*).

A. Hasil Pengujian Kualitas Visual (PSNR)

Pengujian kualitas visual bertujuan untuk menjawab apakah metode usulan mampu mempertahankan kualitas visual citra di atas ambang batas perseptual manusia (>40 dB). Data perbandingan rata-rata nilai *Peak Signal-to-Noise Ratio* (PSNR) antara kedua metode disajikan dalam Tabel 3.

Tabel 3 Perbandingan nilai PSNR

Citra JPEG	Variasi Pesan	PSNR (Standar)	PSNR (Adaptif)
Lampu Jalan 1	Pendek	40.9535	40.9843
	Sedang	40.9269	40.9839
	Panjang	40.9147	40.9835
Lampu Jalan 2	Pendek	38.2193	38.2353
	Sedang	38.2059	38.2349
	Panjang	38.1979	38.2349
Langit Siang	Pendek	40.4794	40.5071
	Sedang	40.4569	40.5068
	Panjang	40.4447	40.5066
Langit Sore	Pendek	41.8772	41.9142
	Panjang	41.8437	41.9140
	Sedang	41.8290	41.9133

Hasil eksperimen menunjukkan bahwa metode DCT Adaptif memiliki kinerja yang lebih stabil dibandingkan metode DCT Standar dalam mempertahankan kualitas citra. Pada beban pesan maksimum, metode DCT Adaptif menghasilkan nilai PSNR yang lebih tinggi dan cenderung konsisten meskipun panjang pesan meningkat, sementara metode DCT Standar mengalami penurunan kualitas. Temuan ini mengindikasikan bahwa penerapan teknik *LSB Matching* ($x \pm 1$) lebih efektif dalam menekan *Mean Squared Error* (MSE). Seluruh nilai PSNR yang diperoleh berada di atas ambang batas >40 dB, yang menunjukkan bahwa secara visual citra stego tidak dapat dibedakan dari citra aslinya dan memenuhi kriteria *imperceptibility*.

B. Hasil Pengujian Keamanan Statistik (Entropi)

Pengujian ini difokuskan pada nilai Selisih Entropi (ΔH) untuk mengukur jejak statistik yang ditinggalkan oleh proses penyisipan. Semakin kecil nilai ΔH, semakin tinggi tingkat keamanan

 ISSN:2302-8149
e-ISSN:2540-9719

steganografi terhadap deteksi. Hasil perbandingan nilai selisih entropi antara metode DCT Standar dan metode DCT Adaptif pada berbagai citra uji disajikan pada Tabel 4.

Tabel 4 Analisis selisih entropi (ΔH)

Citra JPEG	Variasi Pesan	ΔH (Standar)	ΔH (Adaptif)
Lampu Jalan 1	Pendek	0.00018	0.00039
	Sedang	0.00039	0.00041
	Panjang	0.00035	0.00037
Lampu Jalan 2	Pendek	0.00505	0.00464
	Sedang	0.00508	0.00464
	Panjang	0.00520	0.00463
Langit Siang	Pendek	0.00303	0.00248
	Sedang	0.00315	0.00253
	Panjang	0.00298	0.00251
Langit Sore	Pendek	0.00587	0.00602
	Panjang	0.00587	0.00602
	Sedang	0.00578	0.00603

Hasil analisis selisih entropi (ΔH) menunjukkan bahwa metode DCT Adaptif menghasilkan jejak statistik yang lebih rendah dibandingkan metode DCT Standar. Pada citra JPEG bertekstur halus seperti *Langit Siang*, nilai ΔH sebesar 0,00251 mengindikasikan bahwa distribusi piksel citra stego tetap mendekati citra asli. Temuan ini menegaskan bahwa strategi penempatan pesan pada koefisien frekuensi rendah-menengah dan penerapan teknik *LSB Matching* ($x \pm 1$) efektif dalam menyamarkan perubahan serta menjaga stabilitas statistik meskipun muatan pesan meningkat, sehingga meningkatkan keamanan steganografi berbasis entropi.

C. Kapasitas Penyisipan

Kapasitas maksimum teoretis pada citra uji berukuran 512x512 piksel dengan total 4.096 blok DCT (8x8) adalah signifikan. Namun, penelitian ini memposisikan eksperimen sebagai Proof of Concept (PoC) yang berfokus pada validasi stabilitas statistik (entropi) metode usulan, bukan pada pengujian batas jenuh (saturation point) kapasitas. Oleh karena itu, pengujian pengaruh beban data terhadap integritas citra dilakukan secara bertahap menggunakan tiga kategori payload terkontrol sebagaimana dirinci pada Tabel 5.

Tabel 5 Kapasitas dan payload eksperimen

Kategori	Isi Pesan	Panjang Pesan	Ukuran (Bit)
Pendek	“Rahasia”	7	56 bit
Sedang	“Pesan Rahasia”	13	104 bit
Panjang	“Ini Adalah Pesan 1”	18	144bit

Penetapan pesan "Ini Adalah Pesan 1" (144 bit) sebagai batas atas dalam eksperimen ini bertujuan untuk mengobservasi sensitivitas awal algoritma *Adaptive LSB Matching* terhadap perubahan entropi. Meskipun *payload* eksperimen dibatasi pada 144 bit, ukuran ini merepresentasikan skenario transmisi data krusial seperti pengiriman kunci kriptografi atau tanda tangan digital (*digital signature*) yang membutuhkan keamanan statistik tinggi.

Hasil ini memberikan landasan empiris bahwa metode adaptif mampu menyembunyikan jejak modifikasi koefisien secara sempurna pada fase awal penyisipan. Penelitian ini menjadi dasar validasi konsep sebelum dilakukan penelitian lanjutan untuk menguji batas distorsi pada kapasitas ribuan bit (*high-capacity payload*).

D. Akurasi Ekstraksi Pesan (BER)

 ISSN:2302-8149
e-ISSN:2540-9719

Untuk memvalidasi keandalan sistem, dilakukan pengujian ekstraksi data terhadap 12 eksperimen yang mencakup variasi citra JPEG dan panjang payload. Parameter keberhasilan diukur menggunakan Bit Error Rate (BER), di mana nilai 0.00 menunjukkan integritas data terjaga dengan sempurna. Hasil pengujian dirangkum dalam Tabel 6.

Tabel 6 Hasil uji akurasi ekstraksi pesan (BER)

Citra JPEG	Variasi Pesan	Isi Pesan	Hasil Ekstraksi (Standar dan Adaptif)	BER
Lampu Jalan 1	Pendek	"Rahasia"	SUKSES (Identik)	0.00
	Sedang	"Pesan Rahasia"	SUKSES (Identik)	0.00
	Panjang	"Ini Adalah Pesan 1"	SUKSES (Identik)	0.00
Lampu Jalan 2	Pendek	"Rahasia"	SUKSES (Identik)	0.00
	Sedang	"Pesan Rahasia"	SUKSES (Identik)	0.00
	Panjang	"Ini Adalah Pesan 1"	SUKSES (Identik)	0.00
Langit Siang	Pendek	"Rahasia"	SUKSES (Identik)	0.00
	Sedang	"Pesan Rahasia"	SUKSES (Identik)	0.00
	Panjang	"Ini Adalah Pesan 1"	SUKSES (Identik)	0.00
Langit Sore	Pendek	"Rahasia"	SUKSES (Identik)	0.00
	Sedang	"Pesan Rahasia"	SUKSES (Identik)	0.00
	Panjang	"Ini Adalah Pesan 1"	SUKSES (Identik)	0.00

Hasil pengujian menunjukkan bahwa metode DCT Standar dan DCT Adaptif mampu mengekstrak pesan rahasia dengan akurasi 100%, yang ditunjukkan oleh nilai *Bit Error Rate* (BER) sebesar 0,00 pada seluruh eksperimen. Hal ini menunjukkan bahwa penerapan teknik *LSB Matching* ($x \pm 1$) pada metode DCT Adaptif tetap menjaga presisi data, sehingga pemulihan pesan dapat dilakukan secara andal tanpa kesalahan dan layak untuk penerapan steganografi praktis.

Secara keseluruhan, metode DCT Adaptif menunjukkan keunggulan dibandingkan metode DCT Standar (steganografi konvensional) dengan menjaga stabilitas statistik citra, yang tercermin dari nilai selisih entropi (ΔH) yang rendah meskipun beban pesan meningkat. Pemilihan koefisien DCT pada frekuensi rendah–menengah (0,1) mampu mempertahankan kualitas visual dengan nilai PSNR yang stabil di sekitar 40,5 dB, sehingga memberikan keseimbangan antara keamanan statistik dan *imperceptibility*. Keandalan ekstraksi pesan tanpa ketergantungan pada citra asli semakin menegaskan bahwa metode ini efektif dan aplikatif untuk penerapan steganografi.

5 Kesimpulan

Penelitian ini membuktikan bahwa penerapan metode Adaptive DCT dengan pendekatan *LSB Matching* pada koefisien frekuensi rendah–menengah (0,1) mampu menyeimbangkan kualitas visual dan keamanan statistik pada citra JPEG. Dibandingkan metode DCT Standar, metode usulan secara konsisten mempertahankan kualitas citra dengan rata-rata PSNR sebesar 40,41 dB pada beban pesan maksimum serta menekan selisih entropi (ΔH) hingga 0,00251 pada citra homogen. Stabilitas performa ini menunjukkan bahwa pemilihan koefisien strategis dan mekanisme penyesuaian nilai ($x \pm 1$) efektif menyamarkan jejak penyisipan sebagai variasi luminance alami citra, bukan sebagai noise acak. Meskipun payload dibatasi hingga 144 bit sebagai *Proof of Concept* (PoC) untuk memvalidasi stabilitas entropi, hasil penelitian ini memberikan landasan empiris bahwa metode adaptif mampu mengurangi risiko deteksi histogram tanpa mengorbankan integritas visual secara signifikan, serta layak dikembangkan lebih lanjut untuk pengujian kapasitas yang lebih besar.

Referensi

[1] D. M. Abdullah *et al.*, "*Secure Data Transfer Over Internet using Image Steganography: Review*," *Asian J. Res. Comput. SCI.*, Vol. 10, No. 3, hal. 33–52, Jul 2021, DOI:

 ISSN:2302-8149
e-ISSN:2540-9719

10.9734/ajrcos/2021/v10i330243.
[2] S. Ghoul, R. Sulaiman, dan Z. Shukur, "*A Review on Security Techniques in Image Steganography*," *Int. J. Adv. Comput. SCI. Appl.*, Vol. 14, No. 6, hal. 361–384, Jul 2023.
[3] B. T. Ahmed, "*A Systematic Overview of Secure Image Steganography*," *Int. J. Adv. Appl. SCI.*, Vol. 10, No. 2, hal. 178–187, Jun 2021.
[4] W. Luo *et al.*, "*A Comprehensive Survey of Digital Image Steganography and Steganalysis*," *APSIPA Trans. Signal Inf. Process.*, Vol. 13, No. 1, hal. 1–67, Des 2024, DOI: 10.1561/116.20240038.
[5] J. Subramanian dan R. Khilar, "*Adaptive Invisible Steganography Leveraging Entropy-based Image Encryption with the Mimic Octopus Adaptive Framework (MOAF)*," 8 Mei 2025. DOI: 10.21203/rs.3.rs-6300749/v1.
[6] A. Shukla, "*Efficient and Optimized usage of Various Image Formats (JPEG/JPG vs PNG) in Applications*," *J. Math. Comput. Appl.*, Vol. 2, No. 3, hal. 1–3, Sep 2023.
[7] I. A. J. Al Ali, Z. A. Abdulazeez, dan R. M. Aljubouri, "*JPEG-Resistant DCT Steganography for Secure Communication*," *Fusion Pract. Appl.*, Vol. 21, No. 1, hal. 245–264, 2026, DOI: 10.54216/FPA.210118.
[8] M. Xiao, X. Li, B. Ma, X. Zhang, dan Y. Zhao, "*Efficient Reversible Data Hiding for JPEG Images with Multiple Histograms Modification*," *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 31, No. 7, hal. 2535–2546, Jul 2021.
[9] H. Ragab, H. Shaban, K. Ahmed, dan A.-E. Ali, "*Digital Image Steganography and Reversible Data Hiding: Algorithms, Applications and Recommendations*," *J. Image Graph.*, Vol. 13, No. 1, hal. 90–114, Feb 2025.
[10] R. Apau, M. Asante, F. Twum, J. B. Hayfron-Acquah, dan K. O. Peasah, "*Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A Systematic Literature Review*," *PLoS One*, Vol. 19, No. 9, hal. e0308807, Sep 2024.
[11] Z. Wang, G. Feng, Z. Qian, dan X. Zhang, "*JPEG Steganography with Content Similarity Evaluation*," *IEEE Trans. Cybern.*, Vol. 53, No. 8, hal. 5082–5093, Agu 2023.
[12] F. Şahin, T. Çevik, dan M. Takaoğlu, "*Review of the Literature on the Steganography Concept*," *Int. J. Comput. Appl.*, Vol. 183, No. 2, hal. 38–46, Mei 2021, DOI: 10.5120/ijca2021921298.
[13] S. Rahman *et al.*, "*A Comprehensive Study of Digital Image Steganographic Techniques*," *IEEE Access*, Vol. 11, hal. 6770–6791, 2023, DOI: 10.1109/ACCESS.2023.3237393.
[14] W. I. A. Almazaydeh, "*Image Steganography to Hide Unlimited Secret Text Size*," *Int. J. Comput. SCI. Netw. Secur.*, Vol. 22, No. 4, hal. 73–82, Apr 2022.
[15] S. Roy, N. Varish, S. I. Yaqoob, M. S. H. Ansari, dan A. T. Zamani, "*DCT-based Robust Reversible Watermarking Technique based on Histogram Modification*," *Int. J. Electr. Comput. Eng. Syst.*, Vol. 16, No. 6, hal. 473–484, Jun 2025.
[16] N. V Dharwadkar, "*Unveiling the Hidden Pixels: A Comprehensive Exploration of Digital Image Steganography Schemes*," *J. Inf. Hiding Priv. Prot.*, Vol. 7, No. 1, hal. 60898, 2025.
[17] S. Napitupulu, R. R. Siagian, R. Simanullang, K. D. Manalu, dan C. F. Silalahi, "*Implementation of DCT based Steganography Algorithm to Hide Information in Images*," *J. Majelis Paspama*, Vol. 1, No. 2, hal. 12–21, 2023.
[18] D. H. Zulfikar dan Hermanto, "*Hamming Code in JPEG Image Steganography within the Discrete Cosine Transform Domain*," *J. Appl. Informatics Comput.*, Vol. 9, No. 3, hal. 868–875, Jun 2025.
[19] D. Pandey *et al.*, "*Secret Data Transmission using Advance Steganography and Image Compression*," *Int. J. Nonlinear Anal. Appl.*, Vol. 12, hal. 1243–1257, 2021.