PERBANDINGAN KUALITAS CITRA GRAYSCALE STEGANOGRAFI METODE LSB DAN DCT BERDASARKAN PSNR DAN SSIM

Muhammad Ilham[1)] , **Chandra Kirana**[2)]

[1,2)] *Teknik Informatika Institut Sains dan Bisnis Atma Luhur*
email : 2311500021@mahasiswa.atmaluhur [1)], *Chandra.kirana@atmaluhur.ac.id* [2)]

Abstraksi

Penelitian ini membandingkan kualitas citra *grayscale* hasil steganografi menggunakan metode *Least Significant Bit (LSB)* dan *Discrete Cosine Transform (DCT)*. Perbandingan ini penting karena *LSB* dan *DCT* mewakili dua pendekatan utama steganografi, yaitu domain spasial dan domain frekuensi, yang memiliki perbedaan karakteristik dalam kapasitas penyisipan dan kualitas visual citra. Penelitian dilakukan secara eksperimental menggunakan dataset *USC-SIPI* dengan variasi parameter *LSB* (1, 2, dan 4 *bit*) serta *DCT* (*strength* 0.01 dan 0.05). Kualitas citra hasil penyisipan dievaluasi menggunakan *Peak Signal-to-Noise Ratio (PSNR)* dan *Structural Similarity Index Measure (SSIM)*. Hasil penelitian menunjukkan bahwa *DCT-strength* 0.01 menghasilkan kualitas citra terbaik dengan *PSNR* 57.47 *dB* dan *SSIM* 0.9997. Sementara itu, *LSB-1bit* memberikan keseimbangan terbaik antara kualitas citra dan kapasitas penyisipan. Hasil ini menunjukkan adanya *trade-off* antara kualitas dan kapasitas pada kedua metode.

Kata Kunci :
Steganografi, *Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM)*

Abstract

This study compares the quality of grayscale images produced by steganography using the Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) methods. This comparison is important because LSB and DCT represent two main steganographic approaches, namely the spatial domain and the frequency domain, which have different characteristics in terms of embedding capacity and visual image quality. The study was conducted experimentally using the USC-SIPI dataset with variations of LSB parameters (1, 2, and 4 bits) and DCT parameters (strength 0.01 and 0.05). The quality of the stego images was evaluated using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). The results show that DCT with a strength of 0.01 produces the best image quality, achieving a PSNR of 57.47 dB and an SSIM of 0.9997. Meanwhile, LSB with 1-bit embedding provides the best balance between image quality and embedding capacity. These findings indicate a clear trade-off between image quality and capacity for both methods.

Keywords **:**
Steganography, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM)

Pendahuluan

Dalam era digital saat ini, pertukaran informasi melalui citra digital telah menjadi fondasi utama dalam berbagai bidang seperti media sosial, komunikasi, dan keamanan data [1],[2]. Namun, kemudahan akses dan distribusi informasi ini juga meningkatkan risiko penyalahgunaan dan kebocoran data sensitif [3]. Steganografi muncul sebagai solusi penting dalam perlindungan informasi dengan menyembunyikan keberadaan pesan rahasia di dalam media digital seperti citra [4], [5]. Berbeda dengan kriptografi yang hanya mengacak konten pesan, steganografi menyamarkan fakta bahwa terdapat komunikasi rahasia yang terjadi, sehingga menambah lapisan keamanan tambahan [6].

Tantangan utama dalam implementasi steganografi adalah menjaga keseimbangan antara kapasitas penyisipan, ketahanan terhadap manipulasi, dan ketidakterdeteksian [7]. Penyisipan data yang berlebihan dapat menyebabkan degradasi kualitas citra yang dapat dideteksi oleh teknik steganalisis modern [8], [9]. Di antara berbagai metode steganografi yang ada, *Least Significant Bit (LSB)* dan *Discrete Cosine Transform (DCT)* merupakan dua pendekatan fundamental yang banyak digunakan dan diteliti [10], [11].

Tujuan penelitian ini adalah untuk membandingkan kualitas citra grayscale hasil steganografi menggunakan metode *LSB* dan *DCT* berdasarkan parameter *PSNR* dan *SSIM*. Batasan penelitian dibatasi pada evaluasi kuantitatif menggunakan dua metrik tersebut tanpa memperhitungkan aspek keamanan terhadap serangan steganalisis. Metode penelitian yang digunakan adalah eksperimental dengan mengimplementasikan algoritma *LSB* (dengan variasi 1, 2, dan 4 *bit*) dan *DCT* (dengan variasi *strength* 0.01 dan 0.05) pada dataset citra

grayscale dari *USC-SIPI*. Hasil penelitian sebelumnya menunjukkan bahwa metode *DCT* cenderung menghasilkan kualitas citra yang lebih baik meskipun dengan kapasitas yang lebih terbatas [12],[13]. Kontribusi makalah ini adalah memberikan analisis komparatif yang sistematis antara dua metode steganografi populer dengan menggunakan evaluasi kualitas objektif dan perseptual, serta memberikan rekomendasi praktis berdasarkan temuan yang diperoleh.

Tinjauan Pustaka

Perkembangan yang cepat dalam teknologi informasi telah meningkatkan permintaan untuk keamanan data dan perlindungan privasi di dunia maya. Salah satu cara yang sering dipakai untuk menjaga informasi ialah steganografi citra digital, yang merupakan proses menyembunyikan pesan rahasia di dalam gambar sedemikian rupa sehingga tidak dapat ditemukan oleh pihak yang tidak berwenang. Metode yang sangat terkenal di bidang ini ialah *Least Significant Bit (LSB)*, yang berfungsi dengan menyisipkan bit pesan ke dalam *bit* terendah dari setiap pixel gambar. Penelitian [10] menunjukkan bahwa meskipun metode ini memiliki keuntungan dalam hal kesederhanaan dan efisiensi perhitungan, masih ada batasan terkait ketahanan terhadap kompresi serta serangan *steganalysis*.

Metode *LSB* menjadi pilihan banyak peneliti dikarenakan kemudahannya dalam implementasi serta kompatibilitasnya terhadap berbagai format citra digital. Penelitian [4] menunjukkan bahwa penggabungan metode *LSB* dengan algoritma kriptografi mampu meningkatkan aspek keamanan pesan tanpa memberikan dampak signifikan terhadap kualitas visual citra hasil penyisipan. Temuan serupa juga disampaikan dalam Penelitian [8] yang menjelaskan bahwa penerapan kriptografi *RSA* sebelum proses penyisipan dengan *LSB* dapat memperkuat perlindungan pesan terhadap upaya dekripsi yang tidak sah.

Meskipun demikian, karena metode *LSB* beroperasi pada domain spasial, metode ini cenderung rentan terhadap proses pengolahan citra seperti kompresi *JPEG*, rotasi, atau *filtering*. Untuk mengatasi kelemahan tersebut, beberapa penelitian mulai beralih ke teknik penyisipan berbasis domain frekuensi, salah satunya adalah *Discrete Cosine Transform (DCT)*. Penelitian [3] membandingkan performa kedua metode tersebut dan menemukan bahwa pendekatan berbasis *DCT* memiliki ketahanan yang lebih baik terhadap kompresi dan modifikasi citra, meskipun membutuhkan waktu komputasi yang lebih lama dibandingkan *LSB*.

Penelitian [9] memperkenalkan kombinasi antara algoritma enkripsi *hybrid* dengan metode *LSB* dan *DCT* untuk meningkatkan keamanan serta mempertahankan kualitas visual citra. Pengujian yang dilakukan menunjukkan bahwa metode ini dapat menghasilkan nilai *PSNR* lebih dari 40 *dB* dan *SSIM* di atas 0,90, yang menunjukkan bahwa perbedaan antara gambar asli dan gambar yang telah disisipkan hampir tidak bisa dilihat oleh mata manusia.

Kualitas visual dan ketahanan hasil steganografi umumnya dinilai menggunakan dua parameter utama, yakni *Peak Signal-to-Noise Ratio (PSNR)* dan *Structural Similarity Index Measure (SSIM)*. Penelitian [7] menjelaskan bahwa nilai *PSNR* di atas 40 *dB* menunjukkan kualitas citra hasil penyisipan yang sangat baik, sementara nilai *SSIM* di atas 0,9 mengindikasikan tingkat kemiripan struktural yang tinggi antara citra asli dan hasil steganografi. Kedua parameter ini menjadi indikator penting dalam mengevaluasi tingkat imperseptibilitas serta ketahanan citra terhadap deteksi *steganalysis*.

Penelitian [6] menegaskan pentingnya penggunaan kombinasi antara *PSNR* dan *SSIM* untuk memberikan evaluasi yang lebih komprehensif terhadap kualitas citra. *PSNR* hanya mengukur tingkat perbedaan intensitas pixel, sedangkan *SSIM* memperhitungkan kesamaan struktur, luminansi, dan kontras citra.

Penelitian terbaru [3] turut memperkuat temuan sebelumnya dengan menyatakan bahwa meskipun metode *LSB* lebih efisien dari sisi waktu pemrosesan, metode *DCT* lebih unggul dalam mempertahankan kualitas visual citra setelah proses penyisipan pesan. Selain itu, Penelitian [13] menambahkan bahwa penerapan *error-correcting code* seperti *Hamming Code* pada domain *DCT* dapat meningkatkan ketahanan pesan terhadap kerusakan data yang diakibatkan oleh kompresi *JPEG*.

Pada penelitian ini, peneliti menganalisis citra digital dengan menggunakan metode *Least Significant Bit (LSB)* dan *Discrete Cosine Transform (DCT)* pada citra *grayscale*. Pengujian dilakukan dengan menggunakan parameter *Peak Signal-to-Noise Ratio (PSNR)* dan *Structural Similarity Index Measure (SSIM)* untuk menilai kualitas serta ketahanan citra hasil steganografi. Adapun objek yang dijadikan bahan penelitian adalah citra digital yang berperan sebagai media penampung pada proses penyisipan dan ekstraksi pesan. Tujuan dari penelitian ini adalah untuk mengetahui perbandingan performa antara metode *LSB* dan *DCT* dalam menjaga kualitas visual serta tingkat ketahanan citra hasil steganografi.

Metode Penelitian

Rencana Penelitian

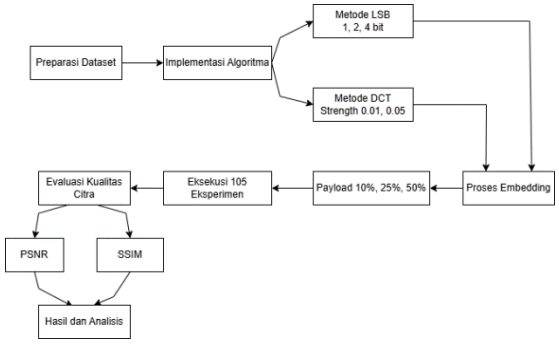
Penelitian ini mengadopsi pendekatan kuantitatif eksperimental dengan rancangan analisis komparatif untuk mengevaluasi kinerja metode steganografi *Least Significant Bit (LSB)* dan *Discrete Cosine Transform (DCT)* pada citra *grayscale* [3][6]. Desain penelitian dirancang untuk membandingkan performa kedua metode berdasarkan parameter kualitas citra *PSNR (Peak Signal-to-Noise Ratio)* dan *SSIM (Structural Similarity Index Measure)*.

Kerangka penelitian disusun melalui lima tahap fundamental yang terintegrasi seperti pada Gambar 1. Tahap pertama meliputi preparasi data dan seleksi dataset dari *USC-SIPI Image Database*. Tahap kedua berupa pemodelan algoritma yang mencakup implementasi metode *LSB* dan *DCT* dengan variasi parameter. Tahap ketiga merupakan eksekusi eksperimen dengan berbagai kombinasi payload. Tahap keempat melibatkan evaluasi kualitas menggunakan metrik objektif dan persepsi visual, sedangkan tahap kelima berupa analisis data dan validasi temuan [10].

Variabel penelitian terdiri dari variabel independen berupa jenis metode steganografi (*LSB* dan *DCT*) dan ukuran *payload* (10%, 25%, 50%), serta variabel dependen berupa nilai *PSNR* dan *SSIM* sebagai indikator kualitas citra. Kontrol ketat diterapkan pada semua parameter eksperimen untuk memastikan reliabilitas hasil [6].

Ukuran *payload* 10%, 25%, dan 50% ditentukan sebagai persentase dari kapasitas maksimum *embedding* pada masing-masing metode dan citra. Pada metode *LSB*, kapasitas maksimum bergantung pada jumlah pixel dan jumlah *bit LSB* yang dimodifikasi, sedangkan pada metode *DCT* kapasitas maksimum ditentukan oleh jumlah blok transformasi *DCT* yang digunakan untuk penyisipan pesan. Payload merepresentasikan rasio antara panjang pesan yang disisipkan terhadap kapasitas maksimum citra.

Analisis komparatif kinerja antara metode *LSB* dan *DCT* akan mengikuti kerangka evaluasi dari studi-studi komparatif steganografi terkini [6],[14] dengan mempertimbangkan *trade-off* antara kapasitas, *imperceptibility*, dan kompleksitas komputasi [1][12].



Gambar 1. Kerangka Penelitian Steganografi *LSB* dan *DCT*

Dataset Citra

Pada penelitian ini menggunakan citra *grayscale* dari *USC-SIPI Image Database* sebagai objek penelitian untuk mengetahui perbandingan kinerja metode steganografi *LSB* dan *DCT* berdasarkan parameter kualitas *PSNR* dan *SSIM*. Standar pengujian untuk mengukur kualitas citra yang telah dimodifikasi melalui proses *embedding* diperlukan untuk mengevaluasi tingkat *imperceptibility* metode steganografi. Citra yang sudah disisipi pesan rahasia diharapkan memiliki kemiripan visual yang tinggi dengan citra asli agar kualitas citra tetap terjaga [10].

Penelitian ini menggunakan 7 citra *grayscale* dari *USC-SIPI Image Database* yang terdiri dari variasi karakteristik tekstur, kompleksitas, dan kontras. Keseluruhan citra digunakan dalam format asli dengan dimensi yang bervariasi untuk memastikan representasi yang komprehensif dalam evaluasi performa algoritma steganografi.

Gambar 2. *Dataset* Citra

Pemilihan ketujuh citra tersebut didasarkan pada pertimbangan variasi karakteristik visual yang dapat mempengaruhi performa algoritma steganografi. Citra dengan tekstur kompleks Gambar 2 (5.1.09.*tiff*) memberikan lingkungan *embedding* yang kaya, sedangkan citra dengan area homogen Gambar 2 (5.1.10.tiff) memungkinkan evaluasi sensitivitas metode terhadap *noise* pada *region* yang seragam [10]. Gambar 2 (7.1.01.*tiff*, 7.1.02.*tiff*) mewakili kategori *object* dengan *edge* yang kuat dan struktur yang jelas.

Setiap citra melalui proses validasi format untuk memastikan konsistensi sebagai *grayscale* 8-*bit* dengan rentang intensitas 0-255. Konversi dan normalisasi dilakukan apabila diperlukan untuk menjaga uniformitas input pada seluruh eksperimen [2]. Seluruh citra diperlakukan secara seragam sebelum proses *embedding* dilakukan. Setiap citra digunakan dalam format *grayscale* 8-*bit* tanpa dilakukan preprocessing tambahan seperti *resizing*, *filtering*, dan *enhancement* sehingga karakteristik asli citra tetap dipertahankan. Parameter *embedding* dan *payload* diterapkan secara identik pada seluruh citra untuk memastikan konsistensi dan keadilan dalam evaluasi kinerja metode.

Implementasi Algoritma *Steganografi*

Metode *Least Significant Bit (LSB)*

Algoritma *LSB* diimplementasikan berdasarkan model *spatial* domain dengan pendekatan manipulasi pixel langsung, mengikuti metodologi yang telah teruji dalam berbagai penelitian steganografi [4][9][11]. Metode ini beroperasi pada domain spasial

dengan memodifikasi *bit-bit* paling tidak signifikan dari nilai intensitas pixel citra. yang telah terbukti efektif untuk penyembunyian data pada citra *grayscale* [8].

Algoritma Embedding LSB

```
Input: original_image, secret_message, num_bits
Output: stego_image
capacity ← (height × width × num_bits) / 8
If length(secret_message) > capacity Then
    Throw Error "Message too large"
End If
binary_message ←
ConvertToBinary(secret_message)
For each pixel in original_image Do
    For bit_pos from 1 to num_bits Do
        If message_index < length(binary_message)
Then
            bit ← binary_message[message_index]
            pixel ← (pixel & mask) | (bit << (num_bits -
bit_pos))
            message_index ← message_index + 1
        End If
    End For
End For
Return stego_image
```

Variasi parameter *LSB* dikembangkan dengan tiga tingkat modifikasi untuk mengevaluasi pengaruhnya terhadap kualitas citra. *LSB-1bit* menggunakan mask 11111110_2 (254) yang memodifikasi *1bit* terakhir, menghasilkan perubahan paling halus dengan kapasitas terbatas. *LSB-2bit* menggunakan *mask* 11111100_2 (252) yang memodifikasi 2bit terakhir, menawarkan keseimbangan antara kapasitas dan kualitas citra. *LSB-4bit* menggunakan *mask* 11110000_2 (240) yang memodifikasi *4bit* terakhir, memberikan kapasitas *embedding* maksimal namun berpotensi menurunkan kualitas citra secara signifikan [4][9][11]. Pemilihan variasi parameter ini memungkinkan analisis mendalam mengenai trade-off antara kapasitas embedding dan kualitas citra, sebagaimana dieksplorasi dalam penelitian serupa [6][15]

Metode *Discrete Cosine Transform (DCT)*

Algoritma *DCT* mengadopsi model frequency domain dengan transformasi berbasis blok, mengimplementasikan pendekatan yang sukses digunakan dalam steganografi domain frekuensi [3][13]. Berbeda dengan *LSB* yang beroperasi langsung pada nilai pixel, metode *DCT* melakukan transformasi citra ke domain frekuensi sebelum proses embedding dilakukan. Pendekatan ini memberikan keunggulan dalam hal ketahanan terhadap kompresi dan analisis statistik.

Algoritma Embedding DCT

```
Input: original_image, secret_message, strength
Output: stego_image
blocks ← DivideIntoBlocks(original_image, 8 ×8)
binary_message ←
ConvertToBinary(secret_message)
message_index ← 0
For each block in blocks Do
    dct_block ← DCT(block)
    If message_index < length(binary_message) Then
        bit ← binary_message[message_index]
        If bit = 1 Then
            dct_block[4,4] ← |dct_block[4,4]| +
(strength × 100)
        Else
            dct_block[4,4] ← |dct_block[4,4]| -
(strength × 100)
        End If
        message_index ← message_index + 1
    End If
    idct_block ← InverseDCT(dct_block)
    ReconstructBlock(stego_image, idct_block)
End For
Return stego_image
```

Variasi parameter *DCT* diterapkan melalui dua tingkat kekuatan modifikasi pada koefisien frekuensi menengah. *DCT-strength* 0.01 menggunakan faktor kekuatan 0.01 yang menghasilkan modifikasi halus dengan dampak minimal terhadap kualitas visual citra. *DCT-strength* 0.05 menggunakan faktor kekuatan 0.05 yang menghasilkan modifikasi lebih signifikan, berpotensi meningkatkan ketahanan terhadap kompresi namun dapat mempengaruhi kualitas citra [3][13]. Variasi parameter ini memungkinkan evaluasi pengaruh tingkat modifikasi terhadap kualitas citra dan ketahanan metode, mengikuti pendekatan eksperimen yang digunakan dalam penelitian sejenis [6][16].

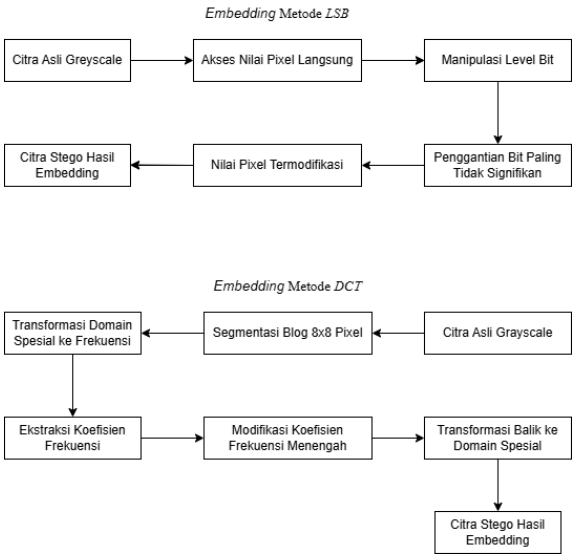
Secara konseptual, proses ekstraksi pesan dilakukan dengan membalik mekanisme embedding sesuai dengan metode yang digunakan. Pada metode *LSB*, ekstraksi dilakukan dengan membaca kembali bit-bit paling tidak signifikan dari setiap pixel citra, sedangkan pada metode *DCT* ekstraksi dilakukan dengan menganalisis perubahan pada koefisien frekuensi yang telah dimodifikasi. Karena fokus penelitian ini adalah evaluasi kualitas citra hasil *embedding*, proses ekstraksi tidak dijabarkan secara algoritmik.

Komparasi Konseptual Metode *LSB* dan *DCT*

Perbedaan fundamental antara pendekatan *LSB* dan *DCT* dalam steganografi diilustrasikan pada Gambar 3. Diagram komparatif ini secara visual merepresentasikan perbedaan filosofis, domain operasi, karakteristik teknis, dan implikasi praktis dari kedua metode yang secara signifikan mempengaruhi performa dan aplikasinya dalam berbagai skenario steganografi.

Berdasarkan analisis mendalam terhadap mekanisme kerja kedua metode, dapat diidentifikasi bahwa *LSB* mengadopsi pendekatan spatial-domain embedding

yang bersifat langsung dan sederhana, sedangkan *DCT* menerapkan pendekatan *frequency-domain embedding* yang lebih kompleks namun *robust*. Perbedaan paradigma ini menghasilkan *trade-off* yang jelas antara kemudahan implementasi dan tingkat keamanan yang ditawarkan oleh masing-masing teknik.



Gambar 3. Perbandingan Konsep *Embedding* Metode *LSB* [4][9] dan *DCT* [4][9]

Metrik Evaluasi Kualitas

Evaluasi Parameter *Peak Signal-to-Noise Ratio (PSNR)*

PSNR merupakan metrik evaluasi yang *widely adopted* dalam pengolahan citra digital untuk mengukur tingkat distorsi [7][11]. Meskipun memiliki keterbatasan dalam korelasi dengan persepsi visual manusia, *PSNR* tetap menjadi *baseline* yang penting dan banyak digunakan dalam studi-studi komparatif steganografi terkini [17][18]. Metrik ini menghitung rasio antara kekuatan sinyal maksimum yang mungkin dan kekuatan *noise* yang mempengaruhi kualitas representasi sinyal tersebut.

$$PSNR = 20 \cdot log_{10}(MAX_i / \sqrt{MSE}) \quad (1)$$

Dengan MAX_i adalah nilai maksimum intensitas pixel (255 untuk citra 8-*bit*) dan *MSE* adalah *Mean Square Error* antara citra asli dan citra stego. Nilai *PSNR* diinterpretasikan berdasarkan standar yang berlaku dalam evaluasi kualitas citra steganografi [17],[18], dimana nilai *PSNR* > 30 *dB* menunjukkan degradasi kualitas yang tidak signifikan secara visual, sedangkan nilai *PSNR* < 20 *dB* mengindikasikan degradasi yang cukup nyata.

Evaluasi Parameter *Structural Similarity Index Measure (SSIM)*

SSIM dikembangkan untuk mengatasi keterbatasan metrik tradisional seperti *PSNR* dengan mempertimbangkan persepsi visual manusia [12]. Studi komparatif metrik kualitas citra menunjukkan bahwa *SSIM* memberikan korelasi yang lebih baik dengan penilaian kualitas subjektif dibandingkan *PSNR*, terutama dalam mendeteksi degradasi pada tekstur dan struktur citra [17]. Metrik ini mengevaluasi kemiripan antara dua citra dengan mempertimbangkan tiga komponen fundamental persepsi visual: luminansi, kontras, dan struktur.

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot s[(x,y)]^{Y} \quad (2)$$

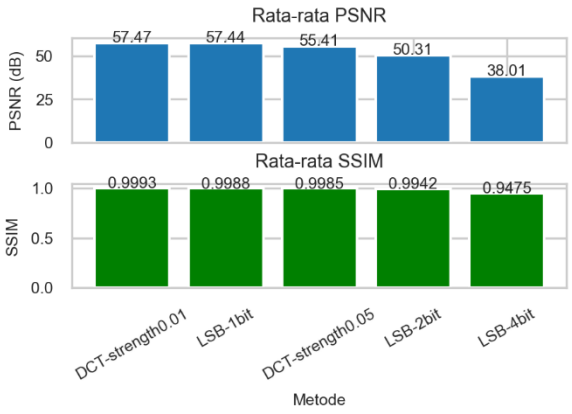
Nilai *SSIM* berkisar antara -1 hingga 1, dimana nilai 1 menunjukkan kesempurnaan identitas struktural. Interpretasi nilai *SSIM* mengikuti standar yang digunakan dalam evaluasi metode *full-reference* [18], dengan nilai *SSIM* > 0.9 menunjukkan kemiripan struktural yang sangat tinggi, dan nilai *SSIM* < 0.7 mengindikasikan perbedaan struktural yang signifikan.

Hasil dan Pembahasan

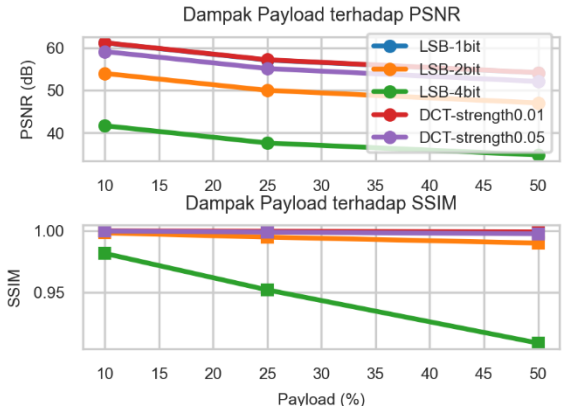
Penelitian ini melakukan analisis komprehensif terhadap 105 eksperimen steganografi menggunakan 7 citra *greyscale* dengan 5 variasi metode dan 3 tingkat *payload*. Hasil pengukuran kuantitatif disajikan dalam Tabel 1, sementara analisis visual divisualisasikan melalui Gambar 1 hingga 3.

Tabel 1. Hasil Pengukuran *PSNR* dan *SSIM* Metode *LSB* dan *DCT*

Metode	Payload 10%	Payload 25%	Payload 50 %	Rata-rata	Kapasitas Maksimal
PSNR (dB)					
LSB-1bit	61.12	57.16	54.13	57.47	8.192 bytes
LSB-2bit	54.22	50.30	47.31	50.61	16.384 bytes
LSB-4bit	42.26	38.32	35.32	38.63	32.768 bytes
DCT-0.01	61.14	57.15	54.13	57.47	640 bytes
DCT-0.05	59.07	55.03	52.00	55.37	640 bytes
SSIM					
LSB-1bit	0.9998	0.9994	0.9988	0.9993	8.192 bytes
LSB-2bit	0.9989	0.9971	0.9942	0.9967	16.384 bytes
LSB-4bit	0.9871	0.9640	0.9304	0.9605	32.768 bytes
DCT-0.01	0.9999	0.9997	0.9994	0.9997	640 bytes
DCT-0.05	0.9997	0.9993	0.9986	0.9992	640 bytes



Gambar 4. Perbandingan Rata-rata *PSNR* dan *SSIM* Antar Metode Steganografi



Gambar 5. Dampak Ukuran Payload terhadap Kualitas Citra

Berdasarkan analisis Tabel 1 dan Gambar 4, teridentifikasi bahwa metode *DCT-strength* 0.01 menghasilkan kualitas terbaik dengan nilai *PSNR* 57.47 *dB* dan *SSIM* 0.9997. Hasil ini mengindikasikan keunggulan pendekatan transformasi frekuensi dalam mempertahankan kualitas citra, dimana nilai *SSIM* mendekati 1.0 menunjukkan kemiripan struktural yang hampir sempurna antara citra asli dan *stego-image* [10]. Secara signifikan, *LSB-1bit* menunjukkan kinerja sangat kompetitif dengan *PSNR* 57.47 *dB* dan *SSIM* 0.9993, mengkonfirmasi efektivitas modifikasi bit terakhir dalam meminimalisir dampak visual [3][9].

Perbandingan nilai kapasitas pada Tabel 1 juga menunjukkan adanya *trade-off inheren* antara kapasitas penyisipan dan kualitas citra. Metode *LSB-4 bit* menawarkan kapasitas penyisipan yang tinggi, namun diikuti oleh penurunan kualitas citra yang signifikan dengan nilai *PNSR* sebesar 38.63 *dB*. Sebaliknya, metode berbasis *DCT* memiliki kapasitas penyisipan yang lebih terbatas, tetapi mampu mempertahankan kualitas citra yang sangat baik. Pola *trade-off* ini sesuai dengan penelitian mengenai keterbatasan praktis dalam steganografi *robust* [6] dan memperkuat temuan tentang spesialisasi domain spatial untuk kapasitas tinggi versus domain frekuensi untuk kualitas optimal [10][12].

Berdasarkan Gambar 5, teramati pola penurunan kualitas gradual pada semua metode seiring peningkatan ukuran *payload*. *LSB-4bit* menunjukkan sensitivitas tertinggi dengan penurunan *PSNR* sebesar 6.94 *dB* dari *payload* 10% ke 50%, sementara *DCT-strength* 0.01 paling *robust* dengan penurunan hanya 7.01 *dB* [6][7]. Karakteristik ini konsisten dengan ketahanan teknik steganografi terhadap analisis statistik [7] dan didukung oleh mekanisme distribusi energi pada koefisien frekuensi *DCT* yang meminimalisir dampak persepsi visual [11][13].

Kelebihan sistem yang teridentifikasi meliputi implementasi sederhana dan komputasi cepat *LSB-1bit* [3][9], kualitas visual superior *DCT-strength* 0.01 dengan distorsi natural [10][13], skalabilitas konsisten *across* berbagai ukuran citra [6][17], serta kontrol *granular* parameter yang memungkinkan *fine-tuning* sesuai kebutuhan aplikasi [1][10]. Namun, kelemahan sistem mencakup kapasitas *DCT* yang terbatas untuk pesan berukuran besar [6][11], kompleksitas komputasi *DCT* yang lebih tinggi [3][10], sensitivitas *LSB-4bit* pada *payload* tinggi [7][9], dan ketergantungan kinerja pada karakteristik citra dasar [8][17].

Temuan penelitian ini memberikan implikasi praktis penting untuk pemilihan metode steganografi. Untuk aplikasi forensik dan keamanan, direkomendasikan *DCT-strength* 0.01 guna optimalisasi kualitas dan keamanan [10][12]. Aplikasi umum dan *real-time* disarankan menggunakan *LSB-1bit* untuk *balance* optimal antara kompleksitas dan kinerja [3][9], sementara aplikasi kapasitas tinggi dapat mempertimbangkan *LSB-4bit* dengan toleransi penurunan kualitas [7][8]. Optimasi lanjutan diperlukan untuk pengembangan algoritma *DCT* dengan peningkatan kapasitas tanpa mengorbankan kualitas [1][11], membuka peluang penelitian *hybrid method* yang memanfaatkan kelebihan kedua pendekatan [1][15].

Evaluasi komprehensif menggunakan metrik *PSNR* dan *SSIM* mendukung validitas hasil yang diperoleh [17][18], sekaligus mengkonfirmasi konsistensi temuan dengan standar assessment kualitas citra terkini. Penelitian ini berkontribusi dalam penyediaan *framework* seleksi metode steganografi berbasis karakteristik aplikasi spesifik, menjawab kebutuhan praktis dalam implementasi sistem penyembunyian data yang robust dan efisien.

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa metode *DCT-strength* 0.01 menghasilkan nilai *PSNR* tertinggi (57.47 *dB*) dan *SSIM* tertinggi (0.9997) dibandingkan metode lainnya, menunjukkan keunggulan dalam mempertahankan kualitas citra hasil steganografi. Metode *LSB-1bit* menghasilkan

nilai *PSNR* (57.47 *dB*) dan *SSIM* (0.9993) yang sangat kompetitif dengan *DCT-strength* 0.01, namun memiliki kapasitas penyimpanan yang lebih besar (8.192 *bytes* vs 640 *bytes*). Di sisi lain, *metode LSB-4bit* menghasilkan nilai *PSNR* terendah (38.63 *dB*) dan *SSIM* terendah (0.9605) meskipun memiliki kapasitas penyimpanan terbesar (32.768 *bytes*). Semua metode mengalami penurunan kualitas citra seiring peningkatan ukuran *payload*, dengan tingkat degradasi paling signifikan terjadi pada metode *LSB-4bit*. Pemilihan metode terbaik bergantung pada prioritas aplikasi: *DCT-strength* 0.01 untuk kualitas optimal, *LSB-1bit* untuk *balance* kualitas dan kapasitas, serta *LSB-4bit* untuk kapasitas maksimal dengan toleransi penurunan kualitas.

Saran

Berdasarkan kesimpulan penelitian dan identifikasi kelemahan yang ditemukan, disarankan untuk penelitian selanjutnya mengembangkan algoritma *DCT* dengan peningkatan kapasitas mengingat keterbatasan kapasitas hanya 640 *bytes* pada penelitian ini, sehingga dapat digunakan untuk aplikasi dengan pesan yang lebih panjang. Perlu juga dilakukan penelitian tentang metode *hybrid LSB-DCT* untuk mengkombinasikan keunggulan kapasitas *LSB* dan kualitas *DCT* dalam satu *framework* terintegrasi. Pengujian ketahanan metode terhadap serangan *steganalysis* juga diperlukan, mengingat penelitian ini hanya fokus pada aspek kualitas tanpa menguji aspek keamanan terhadap deteksi. Disarankan pula penelitian dengan dataset yang lebih variatif mencakup berbagai jenis citra medis, satelit, atau tekstur kompleks lainnya untuk validasi generalisasi metode. Eksplorasi teknik *preprocessing* citra sebelum proses *embedding* dapat dioptimalkan untuk karakteristik citra sebagai media penyembunyian pesan. Penelitian tentang optimasi parameter embedding otomatis berbasis karakteristik citra menggunakan pendekatan *machine learning* atau *deep learning* juga menjadi saran penting. Perlu dilakukan penelitian komparatif dengan metode steganografi terkini seperti berbasis *deep learning* atau generative *models* untuk mengetahui posisi metode *LSB* dan *DCT* dalam perkembangan terbaru. Terakhir, disarankan penelitian tentang metrik kualitas alternatif di luar *PSNR* dan *SSIM* yang lebih sesuai dengan persepsi visual manusia untuk assessment yang lebih komprehensif.

Daftar Pustaka

[1] N. Min-Allah *et al.*, "Quantum Image Steganography Schemes for Data Hiding: A Survey," *Appl. Sci.*, vol. 12, no. 20, 2022, doi: 10.3390/app122010294.

[2] M. Farhan Syakir and P. Studi Sistem dan Teknologi Informasi, "Analisis Penerapan dan Penentuan Teknik Terbaik untuk Steganographic Watermark Beserta Digial Signature Pada Video," 2024.

[3] R. Fahmi, N. Imanudin, I. Kustiawan, and S. Elvyanti, "Steganografi Citra Digital Menggunakan Pendekatan Least Significant Bit dan Discrete Cosine Transform," *Semin. Nas. Tek. …*, no. 207, pp. 1–5, 2023, [Online]. Available: https://snte.fortei.org/list/index.php/snte/article/view/48%0Ahttps://snte.fortei.org/list/index.php/snte/article/download/48/50

[4] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[5] A. Kumar, P. Singla, and A. Yadav, "StegaVision: Enhancing Steganography with Attention Mechanism," pp. 1–2, 2024, [Online]. Available: http://arxiv.org/abs/2411.05838

[6] T. Qiao *et al.*, "Robust steganography in practical communication: a comparative study," *Eurasip J. Image Video Process.*, vol. 2023, no. 1, 2023, doi: 10.1186/s13640-023-00615-y.

[7] R. Apau, M. Asante, F. Twum, J. Ben Hayfron-Acquah, and K. O. Peasah, *Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review*, vol. 19, no. 9 September. 2024. doi: 10.1371/journal.pone.0308807.

[8] D. A. N. S. Lsb and L. S. B. Steganography, "Analysis Of Image Effect On The Combination Of RSA Cryptography And LSB Steganography," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.

[9] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Appl. Sci.*, vol. 13, no. 21, 2023, doi: 10.3390/app132111771.

[10] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[11] A. D. A. N. Dct, "Steganografi Metode Inverted Lsb Menggunakan Pola," vol. 7, no. 2, pp. 218–230, 2024.

[12] M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, "Image Steganography Approaches and Their Detection Strategies: A Survey," *ACM Comput. Surv.*, vol. 57, no. 2, 2024, doi: 10.1145/3694965.

[13] D. Zulfikar and H. Hermanto, "Hamming Code in JPEG Image Steganography within the Discrete Cosine Transform Domain," *J. Appl. Informatics Comput.*, vol. 9, no. 3, pp. 868–875, 2025, doi: 10.30871/jaic.v9i3.9387.

[14] Z. Zhou *et al.*, "Secret-to-Image Reversible Transformation for Generative Steganography," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 5, pp. 4118–4134, 2023, doi: 10.1109/TDSC.2022.3217661.

[15] W. Rehman, "A Novel Approach to Image Steganography Using Generative Adversarial Networks," pp. 1–17, 2024, [Online]. Available: http://arxiv.org/abs/2412.00094

[16] V. Himthani, V. S. Dhaka, M. Kaur, G. Rani, M. Oza, and H. N. Lee, "Comparative performance assessment of deep learning based image steganography techniques," *Sci. Rep.*, vol. 12, no. 1, pp. 1–16, 2022, doi: 10.1038/s41598-022-17362-1.

[17] Y. Al Najjar, "Comparative Analysis of Image Quality Assessment Metrics: MSE, PSNR, SSIM and FSIM," *Int. J. Sci. Res.*, vol. 13, no. 3, pp. 110–114, 2024, doi: 10.21275/sr24302013533.

[18] K. Ohashi *et al.*, "Applicability Evaluation of Full-Reference Image Quality Assessment Methods for Computed Tomography Images," *J. Digit. Imaging*, vol. 36, no. 6, pp. 2623–2634, 2023, doi: 10.1007/s10278-023-00875-0.