Journal Computer and Technology
Vol. 3, No. 2, Desember 2025, hlm. 119-126
ISSN : 3048-1880 (Online)
DOI : https://doi.org/10.69916/comtechno.v3i2.415

PENERAPAN METODE LSB (*LEAST SIGNIFICANT BIT*) DALAM STEGANOGRAFI CITRA DIGITAL UNTUK KEAMANAN INFORMASI

Alfin Mardiaman Gea[1], Nur Wulan*[2]

[1,2]Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia
Email: [1]mardiaman@gmail.com, [2]nurwulanstth@gmail.com

SEJARAH ARTIKEL
Diterima: 22.12.2025
Direvisi: 30.12.2025
Publish: 31.12.2025

ABSTRAK

Penelitian ini bertujuan untuk merancang dan membangun sebuah sistem steganografi berbasis citra digital menggunakan metode *Least Significant Bit* (LSB). Metode ini memungkinkan penyisipan pesan rahasia ke dalam gambar dengan cara mengganti bit paling tidak signifikan dari piksel gambar, sehingga perubahan visual pada gambar tetap tidak terlihat oleh pengamat biasa. Sistem dikembangkan menggunakan bahasa Python dan diintegrasikan dengan antarmuka interaktif Gradio untuk memudahkan pengguna dalam melakukan proses penyisipan (*encoding*) dan ekstraksi (*Decoding*) pesan. Hasil pengujian menunjukkan bahwa pesan dapat disisipkan dan diekstraksi kembali secara akurat. Selain itu, evaluasi kualitas gambar dilakukan menggunakan parameter *Peak Signal-to-Noise Ratio* (PSNR), yang menghasilkan nilai sebesar 93.80 dB. Nilai tersebut mengindikasikan bahwa kualitas gambar setelah proses penyisipan tetap sangat baik dan tidak mengalami degradasi signifikan. Dengan demikian, metode LSB terbukti efektif dan efisien untuk aplikasi steganografi ringan yang membutuhkan kerahasiaan pesan tanpa merusak kualitas media digital.

Kata kunci: steganografi, LSB, citra digital, PSNR, gradio.

ABSTRACT

This study aims to design and develop a digital image-based steganography system using the Least Significant Bit (LSB) method. This method enables the embedding of secret messages into images by replacing the Least Significant Bits of the image pixels, ensuring that the visual appearance of the image remains indistinguishable to the human eye. The system was developed using the Python programming language and integrated with an interactive Gradio interface to facilitate the encoding and Decoding processes for users. Experimental results indicate that messages can be embedded and accurately extracted. Additionally, image quality was evaluated using the Peak Signal-to-Noise Ratio (PSNR) parameter, which yielded a value of 93.80 dB. This value indicates that the image quality after embedding remains excellent and experiences no significant degradation. Therefore, the LSB method proves to be an effective and efficient solution for lightweight steganography applications that require message confidentiality without compromising digital media quality.

Keywords: *steganography, LSB, digital image, PSNR, gradio.*

1. PENDAHULUAN

Citra digital merupakan representasi visual dalam bentuk data piksel yang tersimpan dalam format tertentu seperti PNG, BMP, atau JPEG. Perkembangan teknologi informasi telah mendorong pemanfaatan citra digital tidak hanya untuk keperluan visual, tetapi juga sebagai media penyimpanan dan transmisi data. Setiap piksel pada citra digital memiliki struktur biner yang memungkinkan manipulasi data pada tingkat bit terkecil tanpa mengubah tampilan visual secara signifikan. Karakteristik inilah yang membuat citra digital menarik untuk dijadikan media dalam teknik pengamanan data [1], [2].

Salah satu teknik yang memanfaatkan sifat biner pada citra digital adalah steganografi. Steganografi merupakan metode penyembunyian pesan rahasia di dalam media lain seperti gambar, audio, atau video dengan tujuan agar keberadaan pesan tersebut tidak terdeteksi. Berbeda dengan kriptografi yang menyamarkan isi pesan, steganografi menyembunyikan eksistensi pesan itu sendiri. Metode yang sering digunakan dalam steganografi citra adalah *Least*

Significant Bit atau LSB yaitu menyisipkan informasi ke dalam bit paling tidak signifikan dari piksel citra sehingga tidak menimbulkan perubahan visual yang mencolok [3], [4].

Namun dalam penerapannya penyisipan pesan ke dalam citra digital menimbulkan tantangan tersendiri. Proses kompresi citra, pendeteksian visual, dan analisis statistik dapat mengungkap pesan tersembunyi jika teknik penyisipan tidak dilakukan secara cermat. Selain itu banyak penelitian yang masih bersifat teoretis tanpa mempertimbangkan kondisi praktis seperti pemilihan jenis citra, ketahanan terhadap perubahan, serta efisiensi dan kapasitas penyisipan. Masalah ini menunjukkan adanya kebutuhan akan pendekatan yang lebih menyeluruh untuk menjamin keamanan informasi tanpa mengorbankan kualitas citra.

Sebagai solusi penelitian ini mengusulkan penerapan metode LSB secara selektif pada citra digital dengan mempertimbangkan karakteristik visual gambar seperti kompleksitas tekstur dan variasi warna. Dengan memilih citra yang kaya detail dan menerapkan penyisipan pada saluran warna tertentu penyembunyian data dapat dilakukan secara optimal tanpa mengganggu tampilan visual. Pendekatan ini diharapkan mampu meningkatkan ketahanan data terhadap deteksi sekaligus menjaga kualitas citra sehingga metode ini dapat diterapkan secara lebih luas dalam konteks keamanan informasi digital [5],[6].

Penelitian sebelumnya dilakukan oleh [7] Dalam era digital yang semakin kompleks, keamanan informasi menjadi tantangan utama karena metode peretasan berkembang lebih cepat dibandingkan teknik pengamanan. Kriptografi memang mampu menyamarkan isi pesan, namun tidak menyembunyikan keberadaannya. Untuk itu, penelitian ini menggabungkan metode Triangle Chain Cipher dan steganografi LSB guna mengamankan pesan dengan cara mengenkripsinya lalu menyisipkannya ke dalam citra digital. Hasilnya, pesan dapat disisipkan dan diambil kembali tanpa merusak tampilan gambar, serta aplikasi desktop yang dibangun mampu menjalankan proses enkripsi hingga dekripsi dengan baik, meskipun masih memiliki keterbatasan dalam pengiriman dan kompatibilitas perangkat.

2. METODE PENELITIAN

2.1. Citra

Citra adalah representasi visual dari suatu objek yang ditangkap melalui perangkat optik seperti kamera, satelit, atau sensor lainnya. Dalam konteks umum, citra sering kali merujuk pada gambar atau foto yang menggambarkan keadaan suatu objek atau wilayah pada waktu tertentu. Citra dapat berupa hasil tangkapan digital maupun analog, tergantung dari alat yang digunakan. Secara etimologis, kata "citra" berasal dari bahasa Sanskerta chitra yang berarti gambar, lukisan, atau sesuatu yang menarik perhatian. Dalam bahasa Indonesia, citra memiliki makna yang luas dan bisa digunakan dalam berbagai konteks, seperti psikologi (citra diri), komunikasi (citra publik), hingga teknologi (citra digital atau citra satelit). Dalam dunia teknologi informasi, citra merujuk pada informasi visual yang tersimpan dalam bentuk digital. Citra digital terdiri dari kumpulan piksel (picture element) yang masing-masing memiliki nilai tertentu yang menggambarkan intensitas warna atau kecerahan. Citra digital dibedakan menjadi dua jenis utama: citra raster (berbasis piksel) dan citra vektor (berbasis garis dan bentuk) [8],[6].

2.2. Steganografi

Steganografi merupakan cabang ilmu dalam keamanan informasi yang fokus pada teknik penyembunyian pesan rahasia di dalam media pembawa seperti gambar, audio, video, atau teks sehingga keberadaan pesan tersebut tidak dapat terdeteksi oleh pihak yang tidak berwenang. Kata "steganografi" berasal dari bahasa Yunani, yaitu steganos yang berarti "tersembunyi" dan graphein yang berarti "menulis", yang secara harfiah berarti "menulis secara tersembunyi". Berbeda dengan kriptografi yang menyamarkan isi pesan, steganografi bertujuan untuk menyamarkan eksistensi pesan itu sendiri. Dalam konteks digital, steganografi dilakukan dengan cara menyisipkan informasi rahasia ke dalam data digital tanpa menyebabkan perubahan visual atau struktural yang nyata. Salah satu media yang paling sering digunakan adalah citra digital, karena struktur pikselnya memungkinkan manipulasi pada tingkat bit terkecil tanpa mengganggu tampilan gambar secara keseluruhan. Metode paling populer untuk hal ini adalah *Least Significant Bit* (LSB), yaitu penyisipan pesan ke dalam bit paling tidak signifikan dari piksel citra. Proses steganografi digital umumnya melibatkan dua tahap utama, yaitu penyisipan (embedding) dan ekstraksi (extraction). Pada tahap penyisipan, pesan rahasia diubah menjadi bentuk biner dan disisipkan ke dalam media pembawa sesuai algoritma tertentu. Sedangkan pada tahap ekstraksi, sistem mengambil kembali bit-bit yang mengandung pesan tersembunyi dari media pembawa untuk direkonstruksi menjadi pesan aslinya. Idealnya, media hasil penyisipan (disebut stego-object) harus tetap tampak identik dengan media aslinya (cover-object) bagi pengamat umum [9],[10].

2.3. Metode *Least Significant Bit* (LSB)

Metode *Least Significant Bit* (LSB) merupakan salah satu teknik paling dasar dan banyak digunakan dalam steganografi digital, khususnya pada media citra. LSB bekerja dengan cara memodifikasi bit paling tidak signifikan dari data piksel pada citra digital untuk menyisipkan informasi rahasia. Bit paling tidak signifikan adalah bit terakhir dalam representasi biner sebuah piksel, dan perubahan pada bit ini secara umum tidak menyebabkan perubahan

visual yang terdeteksi oleh mata manusia. Konsep utama dari metode ini adalah bahwa setiap piksel dalam citra digital, terutama dalam format 24-bit RGB, terdiri dari tiga kanal warna: merah (Red), hijau (Green), dan biru (Blue). Masing-masing kanal memiliki 8 bit data, dan bit paling kanan (atau paling kecil nilainya) dalam masing-masing kanal inilah yang digunakan untuk menyisipkan bit-bit pesan rahasia. Karena hanya bit terakhir yang dimodifikasi, perubahan yang terjadi pada intensitas warna sangat kecil sehingga tidak mengganggu kualitas visual citra. Implementasi LSB dalam penyisipan data bersifat langsung dan sederhana. Misalnya, jika bit terakhir dari kanal merah sebuah piksel adalah 0, dan bit pertama dari pesan yang akan disisipkan adalah 1, maka bit tersebut diubah menjadi 1. Proses ini diulangi hingga seluruh pesan disisipkan secara tersebar ke dalam piksel-piksel citra. Teknik ini dapat diterapkan baik pada citra grayscale maupun citra berwarna, namun citra berwarna biasanya memiliki kapasitas penyisipan yang lebih besar karena tiga kanal warna dapat dimanfaatkan secara bersamaan [11],[12].

3. HASIL DAN PEMBAHASAN

Pada tahap ini, dilakukan implementasi sistem steganografi dengan metode *Least Significant Bit* (LSB) menggunakan bahasa pemrograman Python melalui platform Google Colaboratory. Proses implementasi ini bertujuan untuk membuktikan bahwa pesan rahasia dapat disisipkan ke dalam citra digital tanpa merusak tampilan visual gambar secara signifikan. Hasil yang diperoleh mencakup tahapan input data, proses *encoding*, *Decoding*, serta evaluasi kualitas gambar melalui perhitungan nilai PSNR. Adapun tahapan hasil implementasi yang telah dilakukan dijelaskan sebagai berikut:

1. Input Citra dan Pesan Rahasia

   Pada tahap awal implementasi sistem steganografi, proses dimulai dengan memasukkan dua jenis data utama yang diperlukan, yaitu citra digital sebagai media penampung (cover image) dan pesan rahasia dalam bentuk teks. Citra digital yang digunakan harus memiliki kualitas visual yang baik dan format yang mendukung penyisipan data, seperti PNG atau BMP, agar perubahan bit tidak merusak struktur gambar. Sementara itu, pesan rahasia berupa karakter teks diketik langsung oleh pengguna melalui antarmuka sistem. Kedua input ini menjadi dasar untuk menjalankan proses penyisipan pesan menggunakan metode *Least Significant Bit* (LSB).

```
gr.Interface(
    fn=process,
    inputs=[
        gr.Image(type="pil", label="Unggah Gambar (PNG, JPG, BMP)"),
        gr.Textbox(label="Masukkan Pesan Rahasia")
    ],
```

Gambar 1. Kodingan Upload Gambar

Gambar 1 yang ditampilkan pada gambar merupakan bagian dari implementasi antarmuka pengguna (user interface) menggunakan library Gradio dalam bahasa pemrograman Python. Kode tersebut bertugas untuk mendefinisikan elemen input yang akan digunakan dalam sistem steganografi berbasis web. Terdapat dua jenis input yang diterima oleh sistem, yaitu citra digital dan pesan teks rahasia. Komponen pertama, gr.Image, digunakan untuk memungkinkan pengguna mengunggah gambar dalam format tertentu seperti PNG, JPG, atau BMP. Parameter type="pil" menunjukkan bahwa gambar yang diunggah akan dikonversi ke dalam format PIL (Python Imaging Library), sehingga dapat diproses lebih lanjut dalam sistem, misalnya untuk penyisipan bit menggunakan metode LSB. Label pada elemen ini diatur menjadi "Unggah Gambar (PNG, JPG, BMP)" untuk memberikan petunjuk yang jelas kepada pengguna mengenai jenis file yang dapat diunggah.

2. Proses Penyisipan (*Encoding*) dengan LSB

   Proses penyisipan merupakan tahap inti dalam sistem steganografi, di mana pesan rahasia dimasukkan ke dalam citra digital menggunakan metode *Least Significant Bit* (LSB). Pada tahap ini, pesan teks yang telah dimasukkan oleh pengguna akan dikonversi terlebih dahulu ke dalam bentuk biner, kemudian disisipkan ke dalam bit paling tidak signifikan dari setiap piksel pada citra. Teknik ini dipilih karena mampu menyisipkan informasi tanpa menyebabkan perubahan visual yang mencolok, sehingga pesan tersembunyi tidak mudah terdeteksi secara kasat mata.

```
binary_message = ''.join([format(ord(c), '08b') for c in message]) + '1111111111111110'
if len(binary_message) > len(flat):
    return "❌ Pesan terlalu besar untuk gambar ini.", None, None

for i in range(len(binary_message)):
    flat[i] = (flat[i] & 0b11111110) | int(binary_message[i])
```

Gambar 2. Kodingan Proses Penyisipan Biner

Gambar 2 yang ditampilkan pada gambar merupakan bagian penting dari proses *encoding* menggunakan metode *Least Significant Bit* (LSB) dalam steganografi citra digital. Baris pertama dari kode tersebut bertugas untuk mengonversi pesan teks (message) menjadi format biner 8-bit. Setiap karakter dalam string pesan diubah ke dalam representasi biner menggunakan format(ord(c), '08b'), lalu digabung menjadi satu rangkaian bit (binary_message). Sebagai penanda akhir pesan, ditambahkan delimiter 1111111111111110 di ujung rangkaian bit untuk menandai batas terakhir saat proses ekstraksi. Selanjutnya, sistem melakukan validasi dengan membandingkan panjang binary_message dengan jumlah total piksel dalam gambar (len(flat)). Jika panjang pesan biner melebihi kapasitas bit dari gambar, sistem akan mengembalikan pesan error: "❌ Pesan terlalu besar untuk gambar ini.", dan proses *encoding* tidak akan dilanjutkan. Apabila panjang pesan masih dalam batas yang dapat disisipkan, sistem akan melanjutkan proses penyisipan. Dalam perulangan for, setiap bit dari pesan biner dimasukkan ke dalam bit paling tidak signifikan dari setiap elemen piksel citra. Operasi (flat[i] & 0b11111110) digunakan untuk mengosongkan bit terakhir piksel (mengatur ke 0), kemudian bit pesan (binary_message[i]) dimasukkan menggunakan operasi bitwise OR (|). Proses ini memastikan bahwa hanya bit ke-8 dari piksel yang dimodifikasi, sehingga perubahan visual terhadap gambar tetap minimal dan tidak tampak oleh mata manusia.

Bit Biner yang Disisipkan

```
0100000101101100011101100110100101101110111111111111111110
```

Gambar 3. Bit Biner

Gambar 3 menampilkan hasil dari proses konversi pesan teks ke dalam format bit biner yang disisipkan ke dalam citra digital menggunakan metode *Least Significant Bit* (LSB). Nilai yang ditampilkan merupakan representasi biner dari karakter-karakter dalam pesan rahasia yang dimasukkan oleh pengguna. Setiap karakter dikonversi menjadi 8-bit (1 byte) menggunakan kode ASCII, sehingga seluruh pesan dapat direpresentasikan sebagai rangkaian panjang angka 0 dan 1. Sebagai contoh, bit awal 01000001 mewakili karakter huruf kapital 'A' dalam ASCII. Deretan bit berikutnya akan mengikuti urutan karakter dari pesan teks secara keseluruhan. Di bagian akhir deretan biner, tampak urutan khusus 1111111111111110, yang merupakan delimiter atau penanda akhir pesan. Delimiter ini berfungsi sebagai sinyal bagi sistem bahwa proses ekstraksi pesan harus dihentikan pada titik tersebut saat membaca ulang dari gambar stego.

3. Output Gambar Stego (Gambar yang Sudah Disisipi Pesan)

Setelah proses penyisipan pesan selesai dilakukan menggunakan metode *Least Significant Bit* (LSB), sistem menghasilkan output berupa gambar stego, yaitu gambar digital yang telah mengandung pesan rahasia di dalam struktur bit-nya. Secara visual, gambar stego ini tidak menunjukkan perbedaan yang signifikan dibandingkan dengan gambar asli, karena perubahan hanya terjadi pada bit paling tidak signifikan dari piksel gambar.

```
# Tambah overlay teks visual ke citra
display_image = stego_image.copy()
display_image = add_text_overlay(display_image, message)

return display_image, extracted, psnr_disp, binary_message, "✅ Proses berhasil!"
```

Gambar 4. Kodingan Stego

Potongan kode yang ditampilkan merupakan bagian penting dari fungsi process() yang menangani proses akhir dalam sistem steganografi berbasis metode *Least Significant Bit* (LSB). Setelah pesan rahasia berhasil disisipkan ke dalam citra digital melalui proses *encoding*, sistem kemudian membuat salinan dari citra hasil penyisipan (disebut stego_image) untuk keperluan visualisasi. Salinan ini digunakan untuk menambahkan teks pesan secara visual di atas gambar melalui fungsi add_text_overlay(). Proses ini tidak mengubah data biner penyisipan, melainkan hanya menambahkan overlay berupa teks biasa agar pengguna dapat melihat secara

langsung isi pesan yang disisipkan ke dalam gambar. Selanjutnya, fungsi process() mengembalikan beberapa keluaran utama untuk ditampilkan di antarmuka Gradio, yaitu gambar stego yang telah diberi overlay teks, pesan rahasia yang berhasil diekstraksi, nilai PSNR (*Peak Signal to Noise Ratio*) sebagai indikator kualitas perbedaan antara gambar asli dan gambar stego, representasi bit biner dari pesan yang disisipkan, serta status keberhasilan proses.

Gambar 5. Output Stego

Gambar 5 merupakan hasil dari proses steganografi dengan metode *Least Significant Bit* (LSB), di mana pesan rahasia berupa teks "Alvin" telah berhasil disisipkan ke dalam gambar dan ditampilkan secara visual sebagai overlay pada bagian kiri bawah gambar. Secara kasat mata, gambar ini tampak seperti gambar biasa yang menunjukkan sebuah sepeda di area konstruksi, namun sebenarnya telah mengalami modifikasi digital pada bit paling tidak signifikan dari tiap piksel gambar untuk menyimpan informasi tersembunyi. Teks "Alvin" yang muncul pada pojok kiri bawah bukan merupakan bagian dari data tersembunyi secara LSB, melainkan ditambahkan secara eksplisit menggunakan fungsi overlay sebagai penanda visual bagi pengguna. Hal ini bertujuan untuk memberikan feedback langsung bahwa pesan telah berhasil disisipkan ke dalam gambar dan dapat divisualisasikan. Meskipun ada tambahan teks, kualitas gambar tetap terjaga tanpa perubahan signifikan yang terdeteksi oleh penglihatan manusia, mencerminkan keberhasilan teknik steganografi dalam menjaga integritas visual citra sambil menyimpan informasi tersembunyi secara tersembunyi dan aman.

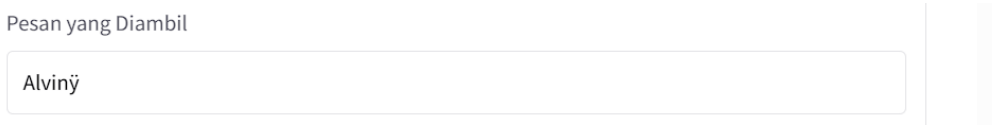
4. Proses Ekstraksi (*Decoding*)

Proses Ekstraksi (*Decoding*) merupakan tahap untuk mengambil kembali pesan rahasia yang telah disisipkan ke dalam citra digital melalui algoritma *Least Significant Bit* (LSB). Setelah proses penyisipan selesai dan diperoleh citra stego, sistem melakukan pembacaan terhadap setiap bit paling tidak signifikan dari tiap piksel gambar tersebut. Bit-bit ini dikumpulkan dan dikelompokkan menjadi 8-bit (1 byte) untuk kemudian dikonversi menjadi karakter ASCII. Proses ini dilakukan secara berulang hingga ditemukan pola khusus sebagai penanda akhir pesan, yakni delimiter 11111110. Dengan demikian, pesan asli yang sebelumnya tersembunyi dapat dipulihkan secara utuh dari gambar yang telah dimodifikasi.

```python
# Fungsi decode pesan dari citra
def lsb_decode(image):
    try:
        image = image.convert("RGB")
        img_array = np.array(image, dtype=np.uint8).flatten()
        bits = [str(pixel & 1) for pixel in img_array]
        bit_str = ''.join(bits)
        chars = [bit_str[i:i+8] for i in range(0, len(bit_str), 8)]
        message = ''
        for c in chars:
            if c == '11111110':
                break
            message += chr(int(c, 2))
        return message
    except Exception as e:
        return f"❌ Error saat decoding: {e}"
```

Gambar 6. Kodingan *Encoding*

Gambar 6 merupakan implementasi fungsi lsb_decode(image) yang digunakan untuk mengekstraksi pesan rahasia dari sebuah citra digital yang telah disisipi informasi menggunakan metode *Least Significant Bit* (LSB). Proses ini diawali dengan mengonversi gambar ke mode RGB dan merubahnya menjadi array satu dimensi (flatten) agar setiap nilai piksel dapat diakses secara berurutan. Kemudian, setiap nilai piksel diambil bit paling tidak signifikannya (LSB) dengan operasi pixel & 1, lalu dikonversi menjadi string biner. Selanjutnya, kumpulan bit tersebut dibagi ke dalam kelompok 8-bit untuk membentuk karakter ASCII. Proses pembacaan dilakukan hingga ditemukan penanda akhir pesan (delimiter) berupa urutan 11111110, yang menjadi tanda bahwa seluruh pesan telah berhasil diekstrak. Jika terjadi kesalahan dalam proses ini, sistem akan menampilkan pesan error menggunakan blok except. Fungsi ini memungkinkan pesan rahasia yang tersembunyi di dalam gambar dapat dibaca kembali secara akurat.



Gambar 7. Proses *Encoding*

Gambar 7 menampilkan hasil dari proses ekstraksi pesan rahasia menggunakan metode *Least Significant Bit* (LSB). Pada kolom "Pesan yang Diambil", terlihat bahwa pesan yang berhasil diambil dari gambar adalah "Alvinÿ". Kemunculan karakter tambahan ÿ di akhir pesan menunjukkan bahwa terdapat kemungkinan bit pesan yang tersisa setelah delimiter 11111110 tidak terbaca dengan sempurna atau tidak diakhiri secara tepat. Hal ini bisa disebabkan oleh ketidaktepatan dalam panjang pesan atau kesalahan dalam pemisahan bit saat proses *Decoding*. Fenomena ini umum terjadi apabila algoritma ekstraksi tidak berhasil mengenali batas akhir pesan dengan tepat, sehingga bit-bit tambahan dibaca sebagai karakter acak.

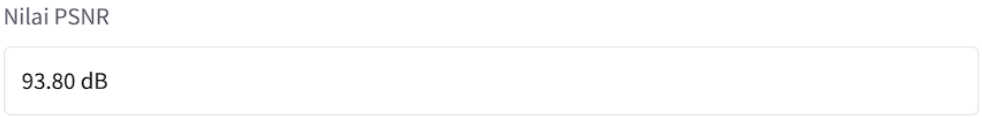
5. Evaluasi PSNR (*Peak Signal-to-Noise Ratio*)

Evaluasi PSNR (*Peak Signal-to-Noise Ratio*) merupakan langkah penting dalam mengukur kualitas citra hasil steganografi terhadap citra aslinya. PSNR digunakan untuk menentukan sejauh mana modifikasi piksel akibat penyisipan pesan memengaruhi kualitas visual gambar. Nilai PSNR dinyatakan dalam desibel (dB), di mana semakin tinggi nilai PSNR menunjukkan bahwa citra stego semakin mirip dengan citra asli dan perubahan yang terjadi sulit dikenali secara visual. Evaluasi ini sangat krusial dalam teknik steganografi karena bertujuan menjaga agar pesan yang disisipkan tidak mengganggu struktur visual gambar, sehingga proses penyembunyian informasi tetap bersifat tersembunyi dan tidak mencolok. Dengan demikian, PSNR menjadi indikator objektif dalam menilai keberhasilan metode LSB dalam menyembunyikan pesan tanpa merusak integritas citra.

```python
# Fungsi menghitung PSNR
def calculate_psnr(original, modified):
    try:
        original = np.array(original.convert("RGB"), dtype=np.float32)
        modified = np.array(modified.convert("RGB"), dtype=np.float32)
        mse = np.mean((original - modified) ** 2)
        if mse == 0:
            return float('inf')
        return 20 * math.log10(255.0 / math.sqrt(mse))
    except Exception as e:
        return f"❌ Error PSNR: {e}"
```

Gambar 8. Kodingan PSNR

Gambar 8 tersebut merupakan fungsi calculate_psnr yang digunakan untuk menghitung nilai *Peak Signal-to-Noise Ratio* (PSNR) antara dua gambar, yaitu gambar asli dan gambar hasil penyisipan pesan (stego image). Fungsi ini pertama-tama mengubah kedua gambar ke format array numerik dengan konversi ke mode RGB dan tipe data float32. Selanjutnya, fungsi menghitung nilai *Mean Squared Error* (MSE) dengan mengambil rata-rata dari kuadrat selisih antara piksel-piksel gambar asli dan gambar hasil modifikasi. Jika nilai MSE sama dengan nol (artinya gambar tidak mengalami perubahan sama sekali), maka fungsi mengembalikan nilai PSNR tak terhingga (inf).



Gambar 9. Hasil PSNR

Gambar 9 menunjukkan hasil evaluasi kualitas visual antara citra asli dan citra stego menggunakan metrik PSNR (*Peak Signal-to-Noise Ratio*). Nilai PSNR yang dihasilkan sebesar 93.80 dB, yang menunjukkan bahwa perbedaan antara citra asli dan citra yang telah disisipi pesan sangat kecil atau hampir tidak terdeteksi secara visual. Umumnya, semakin tinggi nilai PSNR (diukur dalam desibel), maka semakin tinggi pula kualitas gambar hasil modifikasi dibandingkan dengan gambar aslinya. Nilai di atas 40 dB sudah dianggap sangat baik dalam banyak aplikasi pengolahan citra digital. Oleh karena itu, nilai 93.80 dB mengindikasikan bahwa metode penyisipan pesan dengan teknik LSB yang diterapkan dalam sistem ini berhasil menjaga integritas visual gambar, menjadikannya sangat cocok untuk steganografi yang mengutamakan kerahasiaan dan ketidakterdeteksian.

4. KESIMPULAN

Berdasarkan hasil pengujian dan analisis terhadap sistem steganografi menggunakan metode *Least Significant Bit* (LSB) yang telah dikembangkan, dapat disimpulkan bahwa sistem mampu menyisipkan pesan teks ke dalam citra digital melalui manipulasi bit paling tidak signifikan pada setiap piksel tanpa menimbulkan perubahan visual yang berarti. Proses *encoding* dan *Decoding* berjalan secara efektif serta mampu menampilkan pesan yang disisipkan, representasi bit biner, dan pesan hasil ekstraksi kembali dengan tingkat akurasi yang tinggi. Nilai *Peak Signal-to-Noise Ratio* (PSNR) yang diperoleh sebesar 93,80 dB menunjukkan bahwa kualitas citra setelah proses penyisipan tetap sangat baik dan hampir identik dengan citra asli. Selain itu, antarmuka berbasis Gradio yang dibangun memudahkan pengguna dalam mengunggah gambar, memasukkan pesan, serta melihat hasil proses secara real-time dengan tampilan yang sederhana dan interaktif. Secara keseluruhan, sistem ini membuktikan bahwa metode LSB layak digunakan dalam steganografi berbasis citra, khususnya untuk kebutuhan penyembunyian pesan yang ringan dan aman pada gambar digital.

DAFTAR PUSTAKA

[1] A. C. Siregar, B. S. W. Poetro, B. C. Octariadi, R. Robet, and S. Sucipto, *Buku Ajar Pengolahan Citra Digital*. PT. Green Pustaka Indonesia, 2025.

[2] B. Norma, A. Abella, M. Multazam, Z. Hadi, and Z. Muahidin, "KLASIFIKASI PENYAKIT TANAMAN TEMBAKAU MENGGUNAKAN ALGORITMA CONVOLUTIONAL NEURAL NETWORK (CNN) BERBASIS WEB," vol. 3, no. 2, pp. 74–80, 2025.

[3] F. Riza, *Kriptografi Dan Sekuriti Sistem*. umsu press, 2025.

[4] Z. Muahidin, "PENERAPAN ALGORITMA COLLABORATIVE FILTERING PADA SISTEM INFORMASI PENYEWAAN JASA TOUR GUIDE BERBASIS WEB DI WISATA BENANG KELAMBU," vol. 2, no. 2, pp. 83–88, 2024.

[5] F. A. Jiwani, "SISTEM DETEKSI PEMALSUAN CITRA MENGGUNAKAN CNN DENSENET-121 DAN WATERMARK *LEAST SIGNIFICANT BIT* (LSB) UNTUK VALIDASI CITRA PALSU." Universitas Islam Sultan Agung Semarang, 2025.

[6] Z. Muhidin, N. Karim, and M. M. Efendi, "Analysis of Splicing Manipulation in Digital Images using Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) Methods," vol. 8, no. 2, pp. 408–412, 2024.

[7] F. Tambunan, R. S. Hayati, and I. Artikel, "Publisher : Faatuatua Media Karya Penerapan Keamanan Pesan Menggunakan Algoritma Triangle Chain Cipher Dan LSB ke Dalam Citra RGB Abstrak," vol. 02, no. 06, pp. 15–23, 2025.

[8] Y. Saragih, R. S. Bijokangko, D. A. Maulana, and C. I. Saragih, "ANTENA RADAR DAN NAVIGASI." Hadla Media Informasi, 2025.

[9] R. D. Reksiyano and R. Andarsyah, *Teknik Rahasia Menyembunyikan Gambar Keamanan Tingkat Tinggi dengan Steganografi*. Penerbit Buku Pedia, 2025.

[10] Wenti Ayu Wahyuni, M. N. Karim, and Z. Muahidin, "Penerapan algoritma xgboost dalam penentuan potensi sektor wisata lokal di lombok timur," vol. 03, pp. 155–160, 2025.

[11] P. Kusuma, "Implementasi Steganografi Audio Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram." Universitas Islam Indonesia, 2025.

[12] L. D. Samsumar, B. Imran, M. M. Efendi, R. Muslim, Z. Muahidin, and Z. Mutaqin, "Optimalisasi Keamanan Web Server Ubuntu dengan Teknologi IPS Berbasis Iptables," vol. 9, no. 2, pp. 69–76, 2024, doi: 10.31544/jtera.v9.i1.2024.69-76.