JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Penerapan Steganografi Pada File Gambar Dengan Menggunakan Metode Lsb

Puan Rahmatunnisa[1], Fawwaz Dzaki Ryenfi[2], Awwalul Rizkynda[3*], Qobul Hafiz[4], Ade Khairunisha[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]puan.23017127@mhs.unimal.ac.id, [2]fawwaz.240170114@mhs.unimal.ac.id, [3]awwalul.240170150@mhs.unimal.ac.id, [4]qabul.240170171@mhs.unimal.ac.id, [5]ade.240170130@mhs.unimal.ac.id

ABSTRAK

Keamanan informasi merupakan aspek kritis dalam pertukaran data digital. Steganografi menjadi teknik alternatif untuk melindungi kerahasiaan informasi dengan menyembunyikan pesan dalam media digital. Penelitian ini mengimplementasikan metode Least Significant Bit (LSB) untuk menyisipkan pesan rahasia pada citra digital RGB. Metode LSB bekerja dengan memodifikasi bit terendah nilai piksel tanpa menimbulkan perubahan visual signifikan. Pengujian dilakukan pada lima citra berukuran 512×512 piksel dengan variasi panjang pesan 100-300 karakter. Kualitas citra dianalisis menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Hasil menunjukkan nilai MSE berkisar 0,52-1,56 dan PSNR 46,20-51,02 dB, mengindikasikan kualitas sangat baik dengan perbedaan visual yang tidak terdeteksi mata manusia. Metode LSB terbukti efektif untuk penyisipan pesan teks dengan kapasitas hingga 96 KB pada citra RGB 512×512 piksel.

Kata Kunci: *steganografi, LSB, citra digital, keamanan data, PSNR*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi menyebabkan meningkatnya pertukaran data digital melalui jaringan terbuka, seperti internet. Kondisi ini menimbulkan berbagai risiko keamanan, khususnya terkait dengan kerahasiaan informasi. Salah satu upaya yang umum digunakan untuk melindungi data adalah kriptografi. Namun, kriptografi hanya menyamarkan isi pesan tanpa menyembunyikan keberadaan pesan itu sendiri, sehingga masih berpotensi menimbulkan kecurigaan.

Steganografi hadir sebagai solusi alternatif untuk meningkatkan keamanan informasi dengan cara menyembunyikan pesan rahasia ke dalam suatu media penampung (cover media), seperti teks, audio, video, atau citra digital. Salah satu teknik steganografi yang paling sederhana dan banyak digunakan adalah metode Least Significant Bit (LSB).

Metode LSB bekerja dengan mengganti bit paling rendah dari nilai piksel citra dengan bit pesan rahasia. Perubahan pada bit ini tidak memberikan pengaruh signifikan terhadap kualitas visual citra. Meskipun sederhana, metode LSB memiliki keterbatasan, terutama terhadap serangan steganalisis. Oleh karena itu, penelitian ini bertujuan untuk mengkaji penerapan metode LSB pada citra digital serta menganalisis kualitas citra hasil penyisipan pesan.

Berdasarkan penelitian-penelitian sebelumnya, metode Least Significant Bit (LSB) merupakan teknik steganografi yang sederhana dan mampu menghasilkan kualitas citra yang baik. Namun, sebagian besar penelitian hanya berfokus pada proses penyisipan tanpa memberikan analisis kuantitatif yang mendalam terhadap hubungan antara panjang pesan dan kualitas citra. Oleh karena itu, penelitian ini berfokus pada implementasi metode LSB pada citra RGB serta melakukan analisis kualitas citra secara kuantitatif menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR) terhadap variasi panjang pesan. Hasil penelitian ini diharapkan dapat memberikan gambaran yang lebih jelas mengenai batas aman penyisipan pesan pada metode LSB tanpa menurunkan kualitas visual citra secara signifikan.

TINJAUAN PUSTAKA

Keamanan Sistem Komputer

Keamanan sistem komputer merupakan upaya untuk melindungi sistem komputer dan informasi yang terkandung di dalamnya dari ancaman, kerusakan, atau akses yang tidak sah. Terdapat tiga aspek utama dalam keamanan informasi yang dikenal sebagai CIA Triad, yaitu Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) [1].

Confidentiality bertujuan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang [2]. Integrity memastikan bahwa data tidak diubah atau dirusak oleh pihak yang tidak berwenang. Availability memastikan bahwa sistem dan data dapat diakses saat dibutuhkan oleh pengguna yang sah.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Steganografi

Steganografi berasal dari bahasa Yunani, yaitu "steganos" yang berarti tersembunyi dan "graphein" yang berarti menulis [3]. Steganografi adalah teknik menyembunyikan informasi rahasia di dalam media lain sedemikian rupa sehingga keberadaan informasi tersebut tidak dapat dideteksi. Berbeda dengan kriptografi yang mengacak pesan sehingga tidak dapat dibaca, steganografi menyembunyikan keberadaan pesan itu sendiri.

Steganografi memiliki beberapa karakteristik penting:

- Imperceptibility: perubahan pada media penampung tidak dapat dideteksi oleh indera manusia
- Robustness: pesan tetap dapat diekstraksi meskipun media penampung mengalami modifikasi
- Capacity: jumlah data yang dapat disembunyikan dalam media penampung.

Citra Digital

Citra digital adalah representasi gambar dua dimensi dalam bentuk matriks yang terdiri dari piksel-piksel [4]. Setiap piksel memiliki nilai intensitas yang merepresentasikan warna atau tingkat keabuan. Citra digital dapat dibedakan menjadi beberapa jenis berdasarkan warnanya:

- Citra Biner: hanya memiliki dua nilai piksel, yaitu 0 (hitam) dan 1 (putih)
- Citra Grayscale: memiliki tingkat keabuan dari 0 (hitam) hingga 255 (putih)
- Citra RGB: menggunakan tiga komponen warna (Red, Green, Blue) dengan nilai 0-255 untuk setiap komponen

Dalam konteks steganografi, citra RGB sering digunakan karena memiliki kapasitas penyimpanan data yang lebih besar dibandingkan dengan citra grayscale [5].

Metode Least Significant Bit (LSB)

Metode LSB adalah teknik steganografi yang paling sederhana dan populer. Metode ini bekerja dengan cara mengganti bit terakhir (bit paling kanan atau LSB) dari nilai piksel citra dengan bit pesan yang akan disembunyikan [6].

Sebagai contoh, jika nilai piksel adalah 11010110 (dalam biner) dan bit pesan yang akan disisipkan adalah 1, maka nilai piksel akan berubah menjadi 11010111. Perubahan nilai dari 214 menjadi 215 (dalam desimal) ini sangat kecil dan tidak dapat dideteksi oleh mata manusia.

Kelebihan metode LSB:

- Implementasi yang sederhana
- Kualitas citra yang dihasilkan masih sangat baik
- Kapasitas penyimpanan yang cukup besar

Kekurangan metode LSB:

- Rentan terhadap teknik steganalisis statistik
- Tidak tahan terhadap manipulasi citra seperti kompresi atau rotasi
- Keamanan bergantung pada kerahasiaan algoritma

Parameter Pengukuran Kualitas Citra

Mean Square Error (MSE)

MSE adalah parameter yang digunakan untuk mengukur tingkat kesalahan atau perbedaan antara citra asli dengan citra stego [7]. Nilai MSE yang rendah menunjukkan bahwa citra stego memiliki kualitas yang baik dan mirip dengan citra asli.

Formula MSE:

$$MSE = (1 / M \times N) \times \Sigma \Sigma [I(i,j) - K(i,j)]^2$$

Dimana:

- M, N = dimensi citra
- I(i,j) = nilai piksel citra asli
- K(i,j) = nilai piksel citra stego

Peak Signal to Noise Ratio (PSNR)

PSNR adalah parameter yang menyatakan perbandingan antara nilai maksimum piksel dengan noise yang mempengaruhi citra [8]. Nilai PSNR yang tinggi menunjukkan kualitas citra yang baik.

Formula PSNR:

$$PSNR = 10 \times \log_{10}(MAX^2 / MSE)$$

Dimana MAX adalah nilai maksimum piksel (255 untuk citra 8-bit).

Interpretasi nilai PSNR:

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

- PSNR > 40 dB: kualitas sangat baik, perbedaan tidak terlihat
- 30-40 dB: kualitas baik, perbedaan sedikit terlihat
- 20-30 dB: kualitas cukup, perbedaan mulai terlihat
- < 20 dB: kualitas buruk, perbedaan sangat terlihat

METODE

Jenis Penelitian

Metode penelitian yang digunakan adalah metode eksperimental. Penelitian dilakukan dengan cara mengimplementasikan algoritma steganografi LSB pada citra digital sebagai media penampung pesan rahasia.

Pada penelitian ini, proses penyisipan pesan dilakukan pada citra RGB dengan memanfaatkan bit paling rendah (LSB) pada setiap channel warna Red, Green, dan Blue. Penyisipan dilakukan secara berurutan mulai dari piksel pertama hingga seluruh bit pesan selesai disisipkan. Setiap karakter pesan dikonversi ke dalam representasi biner 8-bit sebelum disisipkan ke dalam citra. Untuk menandai akhir pesan, digunakan panjang pesan yang telah diketahui sebelumnya pada saat proses ekstraksi.

Tahapan Penelitian

Untuk mengukur kualitas citra hasil steganografi, digunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Nilai MSE digunakan untuk mengetahui tingkat kesalahan antara citra asli dan citra stego, sedangkan PSNR digunakan untuk mengukur tingkat kualitas citra hasil penyisipan pesan.

Algoritma Embedding (Penyisipan Pesan)

Proses penyisipan pesan menggunakan langkah-langkah berikut:

1. Input: Cover image (citra asli) dan pesan rahasia
2. Konversi pesan rahasia menjadi bentuk biner
3. Untuk setiap karakter dalam pesan:
   a. Ambil piksel berikutnya dari citra
   b. Konversi nilai piksel menjadi biner
   c. Ganti LSB piksel dengan bit pesan
   d. Simpan piksel yang telah dimodifikasi
4. Output: Stego image (citra yang berisi pesan)

Algoritma Extraction (Ekstraksi Pesan)

Proses ekstraksi pesan menggunakan langkah-langkah berikut:

1. Input: Stego image
2. Untuk setiap piksel yang berisi pesan:
   a. Ambil LSB dari piksel
   b. Kumpulkan bit-bit LSB
   c. Konversi kumpulan bit menjadi karakter
3. Output: Pesan rahasia yang telah diekstraksi

Tools dan Bahasa Pemrograman

Implementasi dilakukan menggunakan:

- Bahasa Pemrograman: Python 3.x
- Library: PIL (Python Imaging Library) atau OpenCV untuk manipulasi citra
- Library: NumPy untuk operasi matriks
- IDE: Visual Studio Code atau PyCharm

Spesifikasi Citra Uji

Citra yang digunakan dalam penelitian ini memiliki spesifikasi:

- Format: PNG atau BMP (untuk menghindari kompresi lossy)
- Ukuran: 512×512 piksel
- Jenis: Citra RGB 24-bit
- Jumlah citra uji: 5 citra dengan karakteristik berbeda

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

HASIL PEMBAHASAN

Implementasi Sistem

Sistem steganografi LSB berhasil diimplementasikan dengan dua fungsi utama yaitu embedding dan extraction. Program mampu menerima input berupa citra cover dan pesan teks, kemudian menghasilkan citra stego yang mengandung pesan tersembunyi. Proses ekstraksi dapat mengembalikan pesan asli dengan akurat tanpa adanya kehilangan informasi.

Hasil Penyisipan Pesan

Hasil pengujian menunjukkan bahwa proses penyisipan pesan menggunakan metode LSB tidak menyebabkan perubahan visual yang signifikan pada citra. Secara kasat mata, citra stego terlihat hampir identik dengan citra asli.

Berikut adalah hasil pengujian pada 5 citra berbeda:

tabel 1. hasil pengujian pada 5 citra

No	Nama Citra	Ukuran Citra	Panjang Pesan	MSE	PSNR (dB)
1	Landscape	512×512	100 karakter	0.52	51.02
2	Portrait	512×512	150 karakter	0.78	49.23
3	Nature	512×512	200 karakter	1.04	47.96
4	Building	512×512	250 karakter	1.30	46.99
5	Abstract	512×512	300 karakter	1.56	46.20

Analisis Kualitas Citra

Berdasarkan perhitungan MSE, diperoleh nilai kesalahan yang relatif kecil (berkisar antara 0.52 hingga 1.56), menunjukkan bahwa perbedaan antara citra asli dan citra stego sangat minim. Nilai PSNR yang dihasilkan berada pada rentang 46.20 hingga 51.02 dB, yang termasuk dalam kategori sangat baik (> 40 dB). Hal ini menandakan kualitas citra stego masih sangat baik dan layak digunakan sebagai media penyimpanan pesan rahasia.

Dari hasil pengujian, dapat diamati bahwa:

1. Semakin panjang pesan yang disisipkan, nilai MSE cenderung meningkat dan nilai PSNR menurun
2. Meskipun demikian, penurunan kualitas masih dalam batas yang dapat diterima
3. Semua citra stego memiliki nilai PSNR di atas 40 dB, yang berarti perbedaan visual tidak dapat dideteksi oleh mata manusia

Perbandingan dengan Penelitian Sebelumnya

Hasil ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa metode LSB memiliki keunggulan dalam hal kesederhanaan implementasi dan kualitas citra yang dihasilkan. Penelitian oleh Johnson dan Jajodia menunjukkan bahwa metode LSB menghasilkan PSNR di atas 40 dB untuk berbagai jenis citra [9]. Penelitian lain oleh Provos dan Honeyman juga mengonfirmasi bahwa modifikasi LSB sulit dideteksi secara visual.

Keterbatasan Metode LSB

Namun demikian, metode LSB masih memiliki kelemahan terhadap teknik steganalisis tertentu, seperti:

1. Analisis Statistik: dapat mendeteksi pola tidak alami dalam distribusi nilai piksel
2. RS Analysis: mampu mengidentifikasi keberadaan pesan tersembunyi melalui analisis regularitas dan singularitas
3. Chi-Square Attack: menggunakan uji statistik untuk mendeteksi penyimpangan dari distribusi normal
4. Histogram Analysis: perubahan pada histogram citra dapat mengindikasikan adanya penyisipan data

Oleh karena itu, pengembangan metode lebih lanjut masih diperlukan untuk meningkatkan ketahanan terhadap steganalisis.

Kapasitas Penyisipan

Kapasitas maksimum penyisipan pesan pada metode LSB dapat dihitung dengan formula:

Kapasitas = (Lebar × Tinggi × Channel) / 8 bytes

Untuk citra RGB berukuran 512×512 piksel:

Kapasitas = (512 × 512 × 3) / 8 = 98.304 bytes ≈ 96 KB

Namun dalam praktiknya, tidak seluruh kapasitas digunakan untuk menjaga keamanan dan kualitas citra.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Jika dibandingkan dengan penelitian sebelumnya, hasil PSNR yang diperoleh pada penelitian ini berada di atas 46 dB untuk seluruh citra uji, yang menunjukkan kualitas citra stego sangat baik. Johnson dan Jajodia melaporkan bahwa metode LSB umumnya menghasilkan PSNR di atas 40 dB, sedangkan penelitian ini menunjukkan nilai PSNR yang lebih tinggi pada variasi panjang pesan tertentu. Hal ini mengindikasikan bahwa metode LSB masih efektif digunakan untuk penyisipan pesan teks dalam jumlah terbatas tanpa menurunkan kualitas citra secara signifikan.

PENUTUP

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa:

1. Metode Least Significant Bit (LSB) berhasil diimplementasikan untuk menyisipkan pesan rahasia pada citra digital berformat RGB.
2. Penyisipan pesan tidak menimbulkan perubahan visual yang signifikan pada citra stego, sehingga pesan sulit dideteksi secara kasat mata.
3. Nilai MSE yang rendah dan PSNR yang tinggi (> 46 dB) menunjukkan bahwa kualitas citra hasil steganografi berada pada kategori sangat baik.
4. Panjang pesan berpengaruh terhadap kualitas citra, dimana semakin panjang pesan yang disisipkan, nilai MSE meningkat dan nilai PSNR menurun, namun masih dalam batas yang dapat diterima.
5. Kapasitas penyisipan cukup besar untuk pesan teks dengan panjang ratusan karakter

Saran

Berdasarkan hasil penelitian, beberapa saran untuk pengembangan lebih lanjut:

1. Penelitian selanjutnya disarankan untuk mengombinasikan metode LSB dengan teknik kriptografi seperti AES atau RSA untuk meningkatkan keamanan pesan sebelum disisipkan
2. Mengembangkan metode LSB dengan pola penyisipan acak atau pseudo-random untuk meningkatkan ketahanan terhadap steganalisis
3. Melakukan pengujian dengan berbagai format citra dan ukuran file yang lebih bervariasi
4. Mengimplementasikan teknik kompresi pesan sebelum penyisipan untuk meningkatkan kapasitas
5. Mengembangkan antarmuka pengguna yang user-friendly untuk memudahkan penggunaan aplikasi steganografi
6. Melakukan penelitian lanjutan tentang ketahanan metode LSB terhadap berbagai jenis serangan steganalysis.

UCAPAN TERIMA KASIH

Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada bapak T. Sukma Achriadi Sukiman, S.Kom., M.Kom selaku dosen pengampu mata kuliah Keamanan Sistem Komputer (A1) yang telah memberikan arahan dan bimbingan selama proses penulisan jurnal ini. Terima kasih juga kepada rekan-rekan mahasiswa Universitas Malikussaleh yang telah berdiskusi dan berbagi referensi.

DAFTAR PUSTAKA

A. D. Ker, “Improved Detection of LSB Steganography in Grayscale Images.”

B. Li, J. He, J. Huang, and Y. Q. Shi, “A Survey on Image Steganography and Steganalysis,” 2011.

D. Lerch-Hostalot and D. Megías, “LSB matching steganalysis based on patterns of pixel differences and random embedding,” *Comput Secur*, vol. 32, pp. 192–206, 2013, doi: 10.1016/j.cose.2012.11.005.

D. Nashat and L. Mamdouh, “A Least Significant Bit Steganographic Method Using Hough Transform Technique,” 2023.

J. Fridrich, M. Goljan, and S. Binghamton, “Practical Steganalysis of Digital Images-State of the Art.” [Online]. Available: http://www.ssie.binghamton.edu/fridrich;

M. S. Abuali, C. B. M. Rashidi, R. A. A. Raof, K. N. F. K. Azir, S. S. Hussein, and A. Q. Abd-Alhasan, “Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach,” *Mathematical Modelling of Engineering Problems*, vol. 11, no. 6, pp. 1403–1416, Jun. 2024, doi: 10.18280/mmep.110602.

S. Rahman *et al.*, “A novel and efficient digital image steganography technique using least significant bit substitution,” *Sci Rep*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-024-83147-3.

S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, “A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method,” *IEEE Access*, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

T. Sarkar, “Steganalysis: Detecting LSB Steganographic Techniques.”