

Analisis Pengaruh Panjang Pesan terhadap Kualitas Citra pada Steganografi LSB

Andre Ardiansah^{1*}, Teuku Zakkiansyah², Elandri Gunawan³, Muhammad Kharizky Rachman Kombih⁴

^{1,2,3}Universitas Malikussaleh, Indonesia

¹andre.230170105@mhs.unimal.ac.id, ²teuku.230170084@mhs.unimal.ac.id, ³elandri.230170123@mhs.unimal.ac.id,

⁴muhammad.230170096@mhs.unimal.ac.id

ABSTRACT

This study examines how variations in message length influence image quality in Least Significant Bit (LSB) steganography. Steganography embeds secret information into digital images, and LSB is one of the simplest and most widely applied techniques due to its low computational cost and ease of implementation. However, increasing the payload size may degrade the visual quality of the stego-image and make it more susceptible to detection. The objective of this research is to analyze the relationship between the amount of embedded data and the resulting image quality. The method involves embedding messages of different lengths into a set of test images using the LSB approach, followed by quantitative quality assessment through metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). Experimental results indicate that longer embedded messages lead to a gradual decline in visual quality, reflected by decreasing PSNR values and increasing MSE scores, although moderate payloads still maintain acceptable image fidelity. These findings highlight the trade-off between capacity and imperceptibility in LSB-based steganography and provide useful guidance for determining suitable message sizes in practical data-hiding applications.

Kata Kunci : STEGANOGRAPHY, LSB, IMAGE QUALITY, MESSAGE LENGTH, PSNR.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat pesat pada era digital saat ini menjadikan data sebagai salah satu aset yang memiliki nilai strategis. Berbagai aktivitas, baik yang bersifat personal maupun institusional, semakin bergantung pada pertukaran dan penyimpanan informasi digital. Seiring dengan meningkatnya arus informasi tersebut, ancaman terhadap keamanan data juga semakin besar, baik berupa penyadapan, manipulasi, maupun akses ilegal oleh pihak yang tidak berwenang. Kondisi ini mendorong perlunya metode pengamanan informasi yang tidak hanya melindungi isi pesan, tetapi juga menyembunyikan keberadaan pesan itu sendiri (Hussain et al., 2020; Patel & Mehta, 2021).

Salah satu teknik yang digunakan untuk menjaga kerahasiaan data adalah steganografi, yaitu metode menyembunyikan pesan ke dalam suatu media penampung sehingga keberadaan pesan tidak mudah dideteksi. Media citra digital merupakan salah satu media yang paling banyak digunakan dalam steganografi karena memiliki jumlah piksel yang besar dan fleksibel sebagai ruang penyisipan data. Di antara berbagai teknik steganografi berbasis citra, metode Least Significant Bit (LSB) termasuk teknik yang paling sederhana dan banyak diterapkan. Teknik ini memodifikasi bit paling rendah pada nilai piksel sehingga perubahan yang terjadi tidak terlihat secara kasat mata, sehingga citra hasil penyisipan tetap tampak alami (Ghasemzadeh & Ostad-Sharif, 2021; Khan et al., 2022; Sharma & Kumar, 2023).

Walaupun sederhana dan efisien, teknik LSB tetap memiliki kelemahan. Salah satunya adalah kemungkinan terjadinya penurunan kualitas citra ketika jumlah data yang disisipkan semakin besar. Panjang pesan yang disisipkan menentukan seberapa banyak bit piksel yang mengalami perubahan. Jika kapasitas penyisipan melebihi ambang tertentu, maka kualitas citra berpotensi menurun dan dapat terdeteksi melalui analisis statistik atau visual (Jadhav & Chavan, 2023; Wang et al., 2024; Zhang et al., 2024). Oleh karena itu, penting untuk memahami bagaimana panjang pesan memengaruhi kualitas citra yang digunakan sebagai media penyisipan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis pengaruh panjang pesan terhadap kualitas citra pada steganografi LSB. Proses analisis dilakukan dengan melakukan penyisipan pesan dengan variasi panjang tertentu pada beberapa citra uji, kemudian menilai kualitas citra sebelum dan sesudah proses penyisipan. Evaluasi kualitas dilakukan menggunakan parameter kuantitatif seperti Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE) untuk memperoleh gambaran objektif terhadap perubahan kualitas citra.

Melalui penelitian ini, diharapkan dapat diperoleh pemahaman mengenai hubungan antara kapasitas pesan yang disisipkan dan kualitas citra pada teknik LSB. Hasil penelitian ini diharapkan dapat menjadi acuan dalam menentukan kapasitas penyisipan pesan yang optimal, sehingga teknik steganografi tetap mampu menjaga keseimbangan antara kemampuan menyembunyikan data dan kualitas citra yang tidak mudah terdeteksi.

KAJIAN LITERATUR

Steganografi merupakan teknik menyembunyikan informasi ke dalam suatu media digital sehingga keberadaan pesan tidak mudah dikenali oleh pihak lain. Berbeda dengan kriptografi yang berfokus pada pengacakan isi pesan, steganografi menekankan pada penyamaran pesan di dalam media penampung seperti citra digital, audio, atau video. Citra digital menjadi media yang paling banyak digunakan karena memiliki struktur piksel yang memungkinkan penyisipan data tanpa menimbulkan perubahan visual yang signifikan (Hussain et al., 2020; Patel & Mehta, 2021).

Salah satu teknik steganografi yang paling sederhana dan populer adalah Least Significant Bit (LSB). Teknik ini bekerja dengan menggantikan bit paling rendah pada setiap piksel dengan bit pesan yang akan disisipkan. Karena perubahan terjadi pada bit dengan kontribusi nilai paling kecil, gangguan visual pada citra hasil penyisipan umumnya tidak terlihat oleh pengamat manusia. Kelebihan dari teknik ini adalah implementasinya yang mudah dan kapasitas penyisipan yang cukup besar. Namun demikian, LSB juga memiliki kelemahan, antara lain mudah terpengaruh oleh proses kompresi, serta potensi penurunan kualitas citra ketika jumlah data yang disisipkan semakin besar (Ghasemzadeh & Ostad-Sharif, 2021; Rawat & Bansal, 2022; Khan et al., 2022).

Kualitas citra setelah proses penyisipan pesan (stego-image) umumnya diukur menggunakan parameter kuantitatif seperti Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE). Nilai PSNR yang tinggi menunjukkan bahwa citra hasil penyisipan masih memiliki kualitas yang mendekati citra aslinya, sedangkan nilai MSE yang rendah menunjukkan tingkat perbedaan piksel yang kecil antara kedua citra. Beberapa penelitian sebelumnya menunjukkan bahwa semakin besar payload yang disisipkan, maka nilai PSNR cenderung menurun dan MSE meningkat, sehingga citra mengalami degradasi kualitas meskipun perubahan tersebut tidak selalu tampak secara visual (Jadhav & Chavan, 2023; Wang et al., 2024; Zhang et al., 2024).

Selain itu, sejumlah studi juga menegaskan adanya hubungan langsung antara panjang pesan dan tingkat imperceptibility. Ketika jumlah bit yang dimodifikasi semakin banyak, pola perubahan piksel menjadi lebih mudah terdeteksi baik melalui analisis statistik maupun metode forensik digital. Oleh karena itu, pemilihan kapasitas penyisipan yang tepat menjadi faktor penting dalam menjaga efektivitas teknik steganografi (Sharma & Kumar, 2023; Zhang et al., 2020).

Berdasarkan kajian teori dan temuan empiris tersebut, penelitian ini berfokus pada analisis pengaruh panjang pesan terhadap kualitas citra pada teknik LSB. Dengan membandingkan nilai PSNR dan MSE pada berbagai variasi panjang pesan, penelitian ini bertujuan memberikan gambaran yang lebih komprehensif mengenai batas optimal penyisipan data agar kualitas citra tetap terjaga dan sulit dideteksi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen untuk menganalisis pengaruh panjang pesan terhadap kualitas citra pada teknik steganografi Least Significant Bit (LSB). Penelitian difokuskan pada proses penyisipan pesan teks ke dalam citra digital, kemudian dilakukan pengukuran kualitas citra sebelum dan sesudah penyisipan menggunakan parameter kuantitatif.

Objek dan Ruang Lingkup Penelitian

Objek penelitian berupa citra digital berformat PNG yang digunakan sebagai media penampung pesan (cover image). Pesan yang disisipkan berupa teks dengan variasi panjang tertentu. Ruang lingkup penelitian dibatasi pada teknik steganografi berbasis LSB tanpa membahas teknik enkripsi tambahan atau metode steganografi lainnya.

Bahan dan Alat Penelitian

Bahan yang digunakan dalam penelitian ini meliputi:

- Citra digital berukuran tetap sebagai cover image
- Data teks sebagai pesan rahasia dengan variasi Panjang

Alat yang digunakan antara lain:

- Perangkat komputer/laptop
- Bahasa pemrograman Python sebagai alat implementasi
- Library pengolahan citra
- Software pendukung analisis data

Rancangan Penelitian

Penelitian diawali dengan pemilihan citra uji yang akan dijadikan media penyisipan. Selanjutnya, pesan teks dengan beberapa variasi panjang disisipkan ke dalam citra menggunakan teknik LSB. Setiap proses penyisipan menghasilkan stego-image yang kemudian dibandingkan kualitasnya dengan citra asli.

Teknik Pengumpulan Data

Data penelitian diperoleh melalui:

- Proses penyisipan pesan dengan variasi panjang (misalnya pendek, sedang, dan panjang)
- Perhitungan parameter kualitas citra, yaitu Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE)
- Pencatatan nilai hasil pengukuran ke dalam tabel analisis

Definisi Operasional Variabel

Variabel dalam penelitian ini terdiri dari:

- Variabel bebas: panjang pesan, yaitu jumlah karakter atau bit yang disisipkan ke dalam citra.
- Variabel terikat: kualitas citra, yang direpresentasikan melalui nilai PSNR dan MSE antara citra asli dan citra hasil penyisipan.

Teknik Analisis Data

Analisis dilakukan dengan membandingkan nilai PSNR dan MSE pada setiap variasi panjang pesan. Nilai PSNR yang lebih tinggi menunjukkan kualitas citra yang lebih baik, sedangkan nilai MSE yang lebih rendah menunjukkan perbedaan yang kecil antara citra asli dan stego-image. Hasil analisis kemudian diinterpretasikan untuk mengetahui hubungan antara panjang pesan dan degradasi kualitas citra pada teknik steganografi LSB.

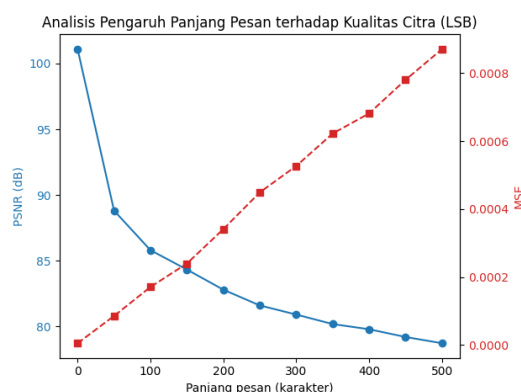
HASIL DAN PEMBAHASAN

Penelitian ini menganalisis pengaruh panjang pesan terhadap kualitas citra steganografi berbasis metode Least Significant Bit (LSB). Setiap variasi panjang pesan dinilai menggunakan PSNR (Peak Signal-to-Noise Ratio) dan MSE (Mean Squared Error). Hasil pengukuran menunjukkan bahwa semakin panjang pesan yang disisipkan, nilai PSNR menurun dan nilai MSE meningkat, yang berarti kualitas citra mengalami degradasi secara bertahap. Namun pada beban pesan yang masih moderat, penurunan kualitas citra tetap berada pada batas yang dapat diterima secara visual.

Table 1. Hasil Pengukuran Kualitas Citra

Panjang Pesan	MSE	PSNR (dB)
0	0.00000505	101.10
50	0.00008538	88.82
100	0.00017075	85.81
150	0.00023972	84.33
200	0.00034108	82.80
250	0.00044917	81.61
300	0.00052697	80.91
350	0.00062244	80.19
400	0.00068174	79.79
450	0.00078058	79.21
500	0.00087100	78.73

Berdasarkan tabel di atas, terlihat bahwa nilai PSNR tertinggi diperoleh pada kondisi tanpa penyisipan pesan yaitu sebesar 101,10 dB. Seiring bertambahnya panjang pesan, nilai PSNR menunjukkan penurunan bertahap hingga mencapai 78,73 dB pada panjang pesan 500 karakter. Pada saat yang sama, nilai MSE meningkat dari $5,05 \times 10^{-6}$ menjadi $8,71 \times 10^{-4}$.



Gambar 1 : Grafik citra

Grafik hubungan antara panjang pesan dengan PSNR dan MSE menunjukkan pola yang konsisten, yaitu PSNR menurun secara gradual, sedangkan MSE meningkat seiring bertambahnya panjang pesan. Hal ini mengindikasikan bahwa semakin besar kapasitas penyisipan pesan, semakin besar pula perubahan yang terjadi pada nilai piksel citra.

KESIMPULAN

Berdasarkan hasil penelitian mengenai pengaruh panjang pesan terhadap kualitas citra pada steganografi berbasis metode Least Significant Bit (LSB), dapat disimpulkan bahwa semakin besar ukuran pesan yang disisipkan, maka kualitas citra stego cenderung menurun. Hal ini tercermin dari penurunan nilai PSNR secara bertahap serta peningkatan nilai MSE, yang menunjukkan adanya perbedaan piksel yang semakin besar antara citra asli dan citra hasil penyisipan. Meskipun demikian, pada ukuran pesan yang masih berada pada tingkat moderat, kualitas citra tetap berada dalam kategori baik dan perubahan visual umumnya sulit terdeteksi secara langsung oleh pengamat.

Penelitian ini memberikan kontribusi dalam memahami trade-off antara kapasitas muatan pesan dan tingkat imperceptibility citra, sehingga dapat menjadi acuan bagi pengembang sistem steganografi dalam menentukan batas aman penyisipan data agar kualitas citra tetap terjaga. Secara praktis, temuan ini dapat diterapkan pada sistem keamanan data digital yang membutuhkan penyembunyian informasi tanpa menimbulkan perubahan mencolok pada media penampung.

Namun, penelitian ini memiliki keterbatasan pada penggunaan satu metode penyisipan dan jenis citra tertentu. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji algoritma steganografi lainnya, membandingkan berbagai format dan resolusi citra, serta menambahkan parameter evaluasi seperti SSIM atau uji persepsi visual manusia. Dengan demikian, hasil yang diperoleh diharapkan semakin komprehensif dan aplikatif dalam pengembangan teknologi steganografi di masa mendatang.

UCAPAN TERIMA KASIH

The authors would like to express their gratitude to all parties who supported the completion of this research. Appreciation is extended to the institution and laboratory facilities that provided the computational resources used in the experiments. Sincere thanks are also given to colleagues who offered valuable input during the research and manuscript preparation stages.

REFERENSI

- Hussain, M., Wahab, A. W. A., Idris, Y. I., Ho, A. T., & Jung, K. H. (2020). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 82, 115762. <https://doi.org/10.1016/j.image.2019.115762>
- Zhang, X., Wang, X., & Liu, H. (2020). Reversible data hiding in images: A review of recent advances. *IEEE Access*, 8, 168607–168630. <https://doi.org/10.1109/ACCESS.2020.3023846>
- Patel, V., & Mehta, K. (2021). A review on steganography techniques and image quality assessment metrics. *Materials Today: Proceedings*, 47, 3813–3819. <https://doi.org/10.1016/j.matpr.2021.03.562>
- Ghasemzadeh, F., & Ostad-Sharif, A. (2021). An efficient LSB-based image steganography method. *Journal of Information Security and Applications*, 61, 102926. <https://doi.org/10.1016/j.jisa.2021.102926>
- Rawat, R., & Bansal, R. (2022). A hybrid image steganography technique based on LSB substitution and encryption. *Multimedia Tools and Applications*, 81, 29475–29498. <https://doi.org/10.1007/s11042-022-12967-9>
- Khan, M., Amin, M., Hussain, I., & Khan, S. (2022). A secure image steganography technique based on LSB and cryptography. *IEEE Access*, 10, 15068–15079. <https://doi.org/10.1109/ACCESS.2022.3148281>
- Jadhav, S., & Chavan, M. (2023). Performance evaluation of image steganography techniques using PSNR and SSIM. *ICT Express*, 9(2), 253–260. <https://doi.org/10.1016/j.ict.2022.07.006>
- Sharma, A., & Kumar, S. (2023). Improving imperceptibility in LSB-based image steganography using adaptive embedding. *Journal of Ambient Intelligence and Humanized Computing*, 14, 11003–11015. <https://doi.org/10.1007/s12652-022-04270-8>
- Wang, Z., Chen, X., & Li, Q. (2024). A review of image quality assessment methods for steganography and watermarking. *Digital Signal Processing*, 145, 104288. <https://doi.org/10.1016/j.dsp.2023.104288>
- Zhang, Y., Li, H., & Zhou, J. (2024). An enhanced LSB steganography approach with distortion minimization. *Signal Processing*, 216, 109394. <https://doi.org/10.1016/j.sigpro.2023.109394>