

Perbandingan Penggunaan Bit Steganografi Metode Least Significant Bit (LSB) M-Bit Pada Citra Digital

Safrina Amini^{1*}, Mardi Hardjianto², Dewi Kusumaningsih³

^{1,2}Teknik Informatika, Universitas Budi Luhur, Jakarta

Email: ^{1*}safrina.amini@budiluhur.ac.id, ²mardi.hardjianto@budiluhur.ac.id, ³dewi.kusumaningsih@budiluhur.ac.id

(*: coresponding author)

Abstrak - Steganografi merupakan teknik penyembunyian informasi yang bertujuan untuk menjaga kerahasiaan dengan menyisipkan informasi rahasia ke dalam media penampung digital, seperti citra, audio, atau video, tanpa mengungkapkan eksistensi pesan tersebut. Salah satu metode steganografi yang banyak digunakan adalah Least Significant Bit (LSB). Keterbatasan metode ini adalah jumlah pesan yang dapat disembunyikan sangat sedikit. Hal ini dikarenakan jika pesan terlalu besar, media yang memuatnya akan berubah secara jelas. Hal ini dapat menimbulkan kecurigaan orang. Metode LSB memiliki beberapa varian, salah satunya adalah LSB m-bit. Nilai m menunjukkan jumlah bit yang dapat digunakan untuk menyimpan informasi dalam satu byte media penampung. Pada penelitian ini, kami mencari berapa nilai m maksimal yang dapat digunakan agar citra yang telah disisipi informasi (stego image) masih memiliki kualitas yang baik. Hasil pengujian diperoleh nilai PSNR untuk m dari satu sampai tiga adalah 46,36, 39,87, dan 33,31. Hasil ini menunjukkan citra masih memiliki kualitas yang baik. Pengujian dengan m bernilai 4, menghasilkan nilai PSNR sebesar 23,23, yang berarti citra memiliki kualitas cukup baik. Kualitas citra akan terlihat buruk jika menggunakan nilai m adalah 5 dan 6. PSNR yang dihasilkan 21,17 dan 15,46.

Kata Kunci - Steganografi, m-bit, domain spasial, LSB, PSNR

Abstract - Steganography is an information hiding technique that aims to maintain confidentiality by inserting secret information into digital media, such as images, audio, or video, without revealing the existence of the message. One of the widely used steganography methods is Least Significant Bit (LSB). The limitation of this method is that the number of messages that can be hidden is very small. This is because if the message is too large, the media containing it will change clearly. This can arouse people's suspicion. The LSB method has several variants, one of which is the m-bit LSB. The value of m indicates the number of bits that can be used to store information in one byte of storage media. In this research, we look for the maximum m value that can be used so that the image that has been inserted with information (stego image) still has good quality. The test results obtained PSNR values for m from one to three are 46.36, 39.87, and 33.31. These results indicate that the image still has good quality. Testing with an m value of 4, produced a PSNR value of 23.23, which means the image has quite good quality. The image quality will look bad if using m values of 5 and 6. The resulting PSNR are 21.17 and 15.46.

Keywords - Steganography, m-bit, domain spatial, LSB, PSNR

I. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi saat ini berkembang dengan pesat. Salah satu terlihat pada perkembangan teknologi informasi, khususnya kemajuan

internet. Kemajuan internet pada zaman ini sudah menjadi kebutuhan sehari-hari bagi masyarakat. Dampak kemajuan internet, seseorang dapat mengakses, memperoleh informasi dengan mudah dan cepat, serta dapat juga digunakan untuk pengiriman informasi oleh semua orang [1]. Lalu lintas pengiriman informasi saat ini semakin pesat pada akhir-akhir ini.

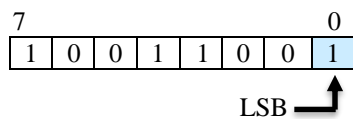
Seiring perkembangan teknologi informasi, teknik kejahatan semakin berkembang juga. Pengiriman informasi dari suatu tempat ke tempat lain memiliki kendala dalam hal keamanan data. Berbagai cara dilakukan untuk memperoleh informasi yang bukan miliknya secara ilegal. Bila informasi yang dikirim bersifat rahasia, maka tidak sembarang orang boleh membacanya. Informasi rahasia yang tersebar luar karena kebocoran akan menimbulkan kerugian bagi pemilik informasi tersebut.

Pentingnya kerahasiaan dan keamanan data semakin meningkat. Mekanisme keamanan yang baik diperlukan untuk mencegah informasi diakses oleh pihak yang tidak berwenang [2]. Berbagai macam cara digunakan untuk mengamankan data penting, diantaranya adalah kriptografi. Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan [3]. Walaupun penggunaan kriptografi sudah cukup aman, namun informasi yang terenkripsi masih dapat dilihat [4]. Selain kriptografi, terdapat metode lain untuk mengamankan data, yaitu steganografi. Steganografi adalah seni menyembunyikan informasi rahasia sedemikian rupa sehingga hanya pengirim dan penerima yang mengetahui keberadaan informasi tersebut. Informasi ini disembunyikan ke dalam suatu media atau wadah dan akan sulit terdeteksi [5] [7]. Wadah yang digunakan untuk menyembunyikan informasi dapat berupa file audio, image atau citra dan video. Untuk meningkatkan keamanan informasi sering kali metode steganografi digabung dengan Kriptografi [7] [9].

Steganografi secara umum diklasifikasikan ke dalam dua kategori berdasarkan ranah tempat data disimpan, yaitu ranah spasial dan ranah frekuensi [10]. Pada ranah spasial, data disisipkan langsung pada piksel gambar atau sampel audio, sedangkan ranah frekuensi, data gambar atau audio diubah ke ranah frekuensi melalui transformasi matematis, lalu data disisipkan di sana. Contoh metode steganografi yang menggunakan ranah spasial seperti LSB, *Masking and Filtering*, sedangkan ranah frekuensi seperti *Discrete Cosine Transform*, *Discrete Wavelet Transform*, *Discrete Fourier Transform*, dll. Banyak penelitian yang menggunakan metode

Least Significant Bit (LSB) seperti yang dilakukan para peneliti ini [4]–[6], [11], [12]. Ada juga yang menggunakan metode Masking and Filtering seperti dilakukan oleh [13]. Selain kedua metode tersebut, ada pula yang menggunakan Transform Domain Techniques seperti yang dilakukan oleh Sharma dan Kumar [14].

Banyak penelitian steganografi metode LSB terdahulu dalam menyembunyikan informasi hanya menggunakan 1-bit data dari setiap satu byte wadah. Hal ini mengakibatkan sedikitnya informasi yang dapat disembunyikan, yaitu hanya 1/8 dari ukuran wadah. Sebagai contoh bila wadah berukuran 80.000 byte, maka informasi yang dapat disembunyikan maksimal hanya 10.000 byte. Bit LSB, yaitu bit paling tidak signifikan yang terletak paling kanan atau bit ke-0 dari byte. Lokasi bit LSB seperti ditunjukkan pada Gambar 1.



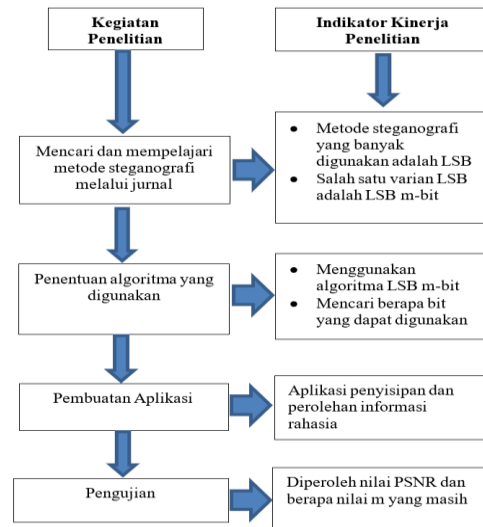
Gambar 1. Lokasi Least Significant Bit

Pada penelitian ini, penyembunyian informasi yang kami lakukan menggunakan steganografi metode Least Significant Bit (LSB) dengan varian m-bit. Wadah yang digunakan untuk menyembunyikan informasi adalah citra yang memiliki bit-depth 24-bit. Penggunaan metode LSB untuk menyembunyikan pesan sangat sederhana, namun yang digunakan pada penelitian ini adalah varian LSB, yaitu LSB m-bit. Metode LSB m-bit memanfaatkan lebih dari 1 bit data per byte dari wadah. Jika LSB biasa hanya menggunakan 1 bit terakhir, maka LSB m-bit menggunakan m-bit terakhir. Misalnya LSB 4-bit, artinya menyisipkan 4 bit per byte (bit ke-0 sampai ke-3). Penggunaan lebih dari satu bit akan menambah daya tampung wadah dalam menyembunyikan informasi, namun kualitas citra yang berkurang. Tujuan penelitian ini adalah untuk mencari tahu seberapa banyak bit yang dapat digunakan untuk menyembunyikan informasi rahasia dengan kualitas citra yang masih baik agar daya tampung wadah dapat dimanfaatkan semaksimal mungkin. Kualitas citra yang telah disisipi informasi rahasia masih dinyatakan baik bila nilai Peak Signal-to-Noise Ratio (PSNR) di atas 30dB [15].

II. METODE PENELITIAN

Langkah penelitian yang digunakan untuk menggambarkan urutan proses kegiatan secara umum ditunjukkan pada Gambar 2. Pada langkah awal penelitian, kami mencari dan mempelajari metode steganografi melalui jurnal-jurnal dari peneliti sebelumnya. Banyak peneliti yang menggunakan metode LSB untuk menyisipkan informasi rahasia karena metode ini cukup mudah diimplementasi. Wadah yang digunakan sebagian besar adalah citra atau image. Secara umum proses steganografi menggunakan wadah citra ditunjukkan pada Gambar 3. Pesan atau informasi disisipkan ke dalam Cover Image sehingga menjadi Stego Image. Proses ini disebut encoding. Proses untuk perolehan kembali informasi rahasia disebut decoding, yaitu dari Stego Image

diperoleh informasi rahasia yang disembunyikan.



Gambar 2. Langkah Penelitian



Gambar 3. Proses Steganografi

Pada metode LSB yang klasik, penyisipan informasi rahasia hanya menggunakan 1 bit dari Cover Object, yaitu bit yang paling kanan. Metode LSB memiliki banyak varian, seperti LSB m-bit. Pada LSB m-bit, penyisipan data informasi rahasia dapat menggunakan 1 atau lebih bit pada Cover Object. Keuntungan dari hal ini adalah dapat menyimpan informasi yang lebih banyak lagi. Sayangnya, makin banyak bit yang digunakan untuk menyimpan informasi rahasia, gambar citra menjadi sangat berubah. Tentu saja hal ini akan menimbulkan kecurigaan bagi steganalis. Pada penelitian ini kami mencari berapa jumlah bit yang dapat digunakan agar kualitas citra masih terlihat baik. Kualitas citra dapat dikatakan masih baik bila nilai Peak Signal-to-Noise Ratio lebih dari 30dB. Perhitungan mencari PSNR menggunakan rumus:

$$PSNR = 10 \cdot \text{Log}_{10} \left(\frac{MAX^2}{MSE} \right) \quad (1)$$

Di mana

PSNR = Nilai Peak Signal-to-Noise Ration (dalam satuan dB)

MAX = Nilai piksel maksimum (255 untuk citra 8-bit)

SE = Mean Squared Error

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (I(i, j) - K(i, j))^2 \quad (2)$$

Di mana

MSE = Mean Squared Error

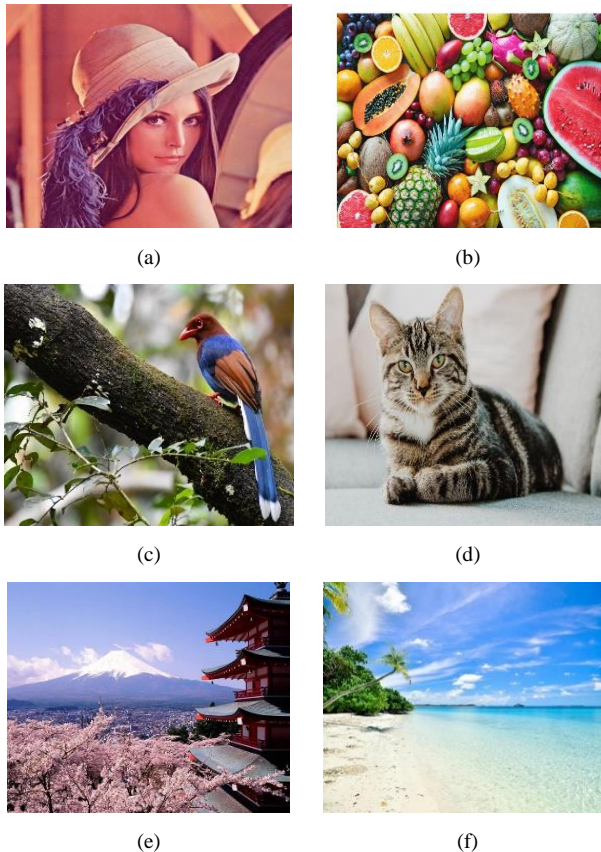
I(i, j) = Nilai piksel pada citra asli (cover image)

K(i, j) = Nilai piksel pada citra yang sudah disisipi (stego image)

m, n = dimensi citra

A. Cover Object

Cover object adalah media atau wadah asli yang digunakan sebagai tempat penyimpanan informasi rahasia dalam proses steganografi. Pada penelitian ini, cover object yang digunakan berbentuk image atau citra. Cover object yang digunakan dalam penelitian ini terdiri dari enam file citra dengan jenis PNG dan BMP masing-masing berukuran 800 x 800 piksel. Keenam data cover object ditunjukkan pada Gambar 4.

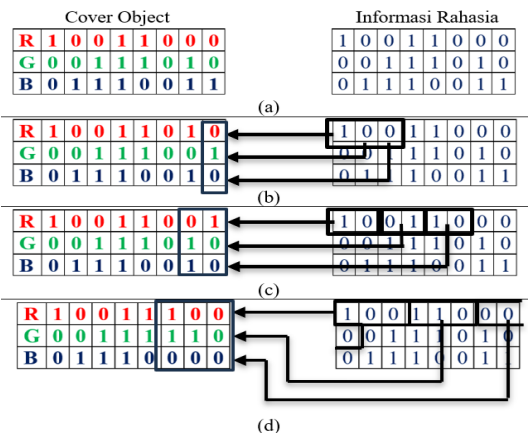


Gambar 4. Sampel Cover Object (a) (b) (c) (d)

B. Proses Penyisipan

Proses penyisipan informasi rahasia ke Cover Object dilakukan mulai dari 1-bit hingga 6-bit. Hal ini untuk mengetahui sampai m ke berapa kualitas citra masih dianggap bagus. 7 dan 8-bit tidak dilakukan karena diperkirakan kualitas citra sudah tidak bagus. Model penyisipan LSB m-bit ditunjukkan pada Gambar 5. Pada Gambar 5 **Error! Reference source not found.** (a) terdapat dua gambar, keadaan awal Cover Object dan informasi rahasia yang akan disisipkan ke Cover Object. Gambar 5(b) menunjukkan proses penyisipan menggunakan 1-bit (m=1). Setiap tiga bit dari informasi rahasia disisipkan ke Cover Object masing-masing ke R, G dan B. Tiga bit berikutnya disisipkan ke RGB berikutnya, dst. Pada Gambar 5(c) penyisipan dilakukan per dua bit dari informasi rahasia. Dua bit pertama disisipkan ke R, dua bit berikutnya disisipkan ke G dan dua bit berikutnya disisipkan ke B. Gambar 5(d) penyisipan menggunakan LSB 3-bit, artinya tiga bit pertama dari informasi rahasia disisipkan ke R, tiga bit berikutnya disisipkan ke G dan tiga bit berikutnya disisipkan ke B.

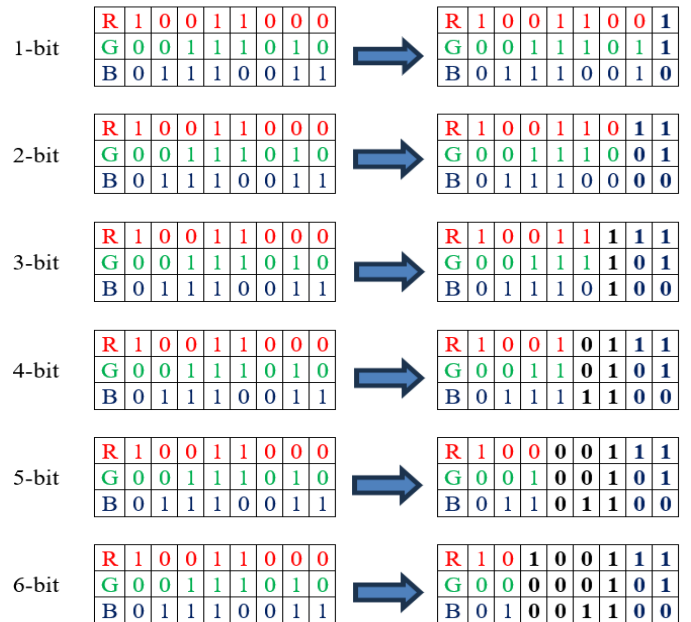
Demikian seterusnya untuk nilai m=4,5 dan 6.



Gambar 5. Penyisipan Informasi Rahasia ke Cover Object

C. Pengujian

Dalam penelitian ini dilakukan pengujian sebanyak dua kali. Pengujian pertama dilakukan pada keenam cover object yang digunakan. Keenam cover object ini akan dilakukan perubahan bit dari bit 0 ke bit 1 dan dari bit 1 ke bit 0. Perubahan ini dilakukan pada m yang bernilai 1, 2, 3, 4, 5 dan 6 saja. Pada m=1, maka bit paling kanan yang diubah. Pada m=2, maka dua bit paling kanan yang diubah dan seterusnya sampai m=6. Pengujian ini dilakukan untuk mengetahui berapa bit yang dapat digunakan dalam kondisi terburuk yaitu proses penyisipan mengubah semua bit yang digunakan. Contoh perubahan ditunjukkan pada Gambar 6 berikut:



Gambar 6. Perubahan Bit Pada m=1, 2, 3, 4, 5 dan 6

Pengujian kedua dilakukan menggunakan beberapa file yang memiliki ukuran berbeda-beda sebagai informasi rahasia. File yang digunakan untuk pengujian kedua ditunjukkan pada Tabel I. Masing-masing file ini akan disisipkan ke enam cover object yang digunakan. File Dokumen1.txt akan disisipkan dengan cover object menggunakan m=1. Dokumen2.txt

menggunakan m=2, Dokumen3.txt menggunakan m=3, dan seterusnya. Tujuan pada pengujian kedua adalah untuk mengetahui berapa m yang dapat digunakan agar stego object-nya masih memiliki kualitas yang baik bila menggunakan file sesungguhnya.

TABEL I
SPESIFIKASI FILE UNTUK PENGUJIAN


No.	Nama File	Ukuran File (Byte)
1.	Dokumen1.txt	240.000
2.	Dokumen2.txt	480.000
3.	Dokumen3.txt	720.000
4.	Dokumen4.txt	960.000
5.	Dokumen5.txt	1.200.000
6.	Dokumen6.txt	1.440.000




III. HASIL DAN PEMBAHASAN

A. Pengujian Pertama

Pada pengujian pertama kami melakukan perubahan nilai bit dari 1-bit hingga 6-bit semua cover object, lalu menghitung nilai PSNR-nya. Keenam cover object yang digunakan, menghasilkan nilai PSNR yang sama. Hasil pengujian ditunjukkan pada Tabel II.

TABEL II
HASIL PENGUJIAN PERTAMA

m	Citra	PSNR (dB)
1-bit		43,36
2-bit		36,37
3-bit		30,14

4-bit		23,88
5-bit		17,74
6-bit		11,99

Dari hasil pengujian ini terlihat bahwa kualitas citra terlihat baik pada m bernilai 1, 2 dan 3. Pada m=4, kualitas citra mulai menurun, namun masih terlihat cukup baik, sedangkan pada m=5 dan 6 kualitas citra sudah tidak baik.

B. Pengujian Kedua

Pada pengujian kedua, digunakan file teks yang berukuran sesuai dengan daya tampung dari cover object. Cover object yang digunakan berukuran 800x800 piksel berjenis RGB 24-bit, sehingga ukuran citranya 800 x 800 x 3 byte (1 piksel berukuran 3 byte) = 1.920.000 byte. Daya tampung citra dapat dihitung dengan rumus:

$$\text{Daya tampung} = \text{Ukuran} * m / 8$$

Di mana:

Daya tampung = Ukuran pesan yang dapat disisipkan (dalam satuan byte)

Ukuran Citra = Ukuran cover object

m = jumlah bit yang digunakan

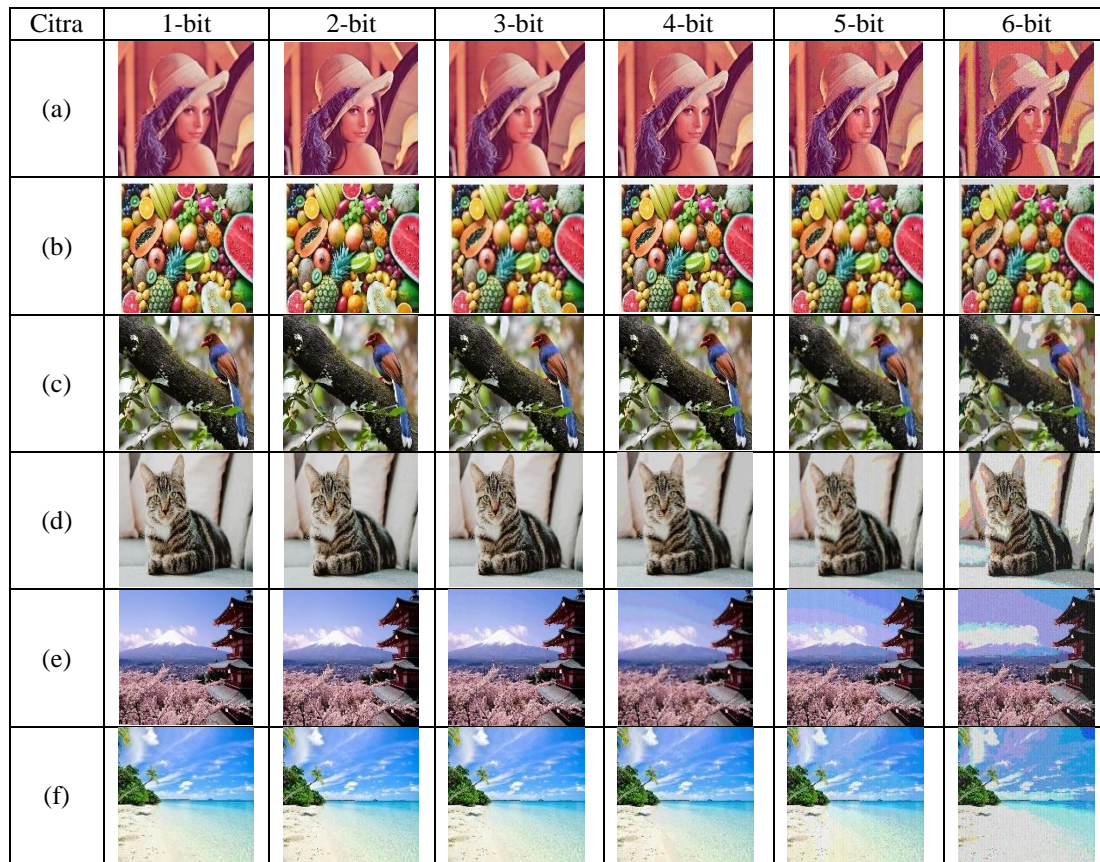
Daya tampung pesan yang dapat disisipkan dengan m bernilai satu hingga enam ditunjukkan pada Tabel III

TABEL III
DAYA TAMPUNG PESAN PADA COVER OBJECT

m	Daya Tampung
1	$1.920.000 * 1 / 8 = 240.000$ Byte
2	$1.920.000 * 2 / 8 = 480.000$ Byte
3	$1.920.000 * 3 / 8 = 720.000$ Byte
4	$1.920.000 * 4 / 8 = 960.000$ Byte
5	$1.920.000 * 5 / 8 = 1.200.000$ Byte
6	$1.920.000 * 6 / 8 = 1.440.000$ Byte

Hasil stego image yang dihasilkan setelah dilakukan penyisipan ditunjukkan pada Tabel IV.

TABEL IV
HASIL CITRA SETELAH DISISIPKAN INFORMASI



Dari stego image yang dihasilkan, dihitung nilai PSNR tiap-tiap citra. Nilai PSNR ditunjukkan pada Tabel 1. Dari nilai PSNR yang dihasilkan, pemakaian bit sampai dengan tiga ($m=3$), kualitas stego image masih baik. Bila menggunakan empat bit, kualitas sudah mulai berkurang namun masih terlihat cukup baik. Penggunaan 5 dan 6 bit terlihat kualitas stego image menjadi buruk.

Tabel 1. Nilai PSNR dari Stego Image

m-bit	PSNR					
	1-bit	2-bit	3-bit	4-bit	5-bit	6-bit
(a)	46,37	39,91	33,33	27,30	21,04	15,56
(b)	46,34	39,73	33,07	27,10	21,01	15,53
(c)	46,38	39,89	33,29	27,44	21,27	15,62
(d)	46,37	39,89	33,39	27,52	21,36	15,42
(e)	46,36	39,91	33,36	27,37	21,54	15,52
(f)	46,37	39,91	33,44	27,36	20,79	15,14
Rerata	46,36	39,87	33,31	23,23	21,17	15,46

IV. KESIMPULAN

Dari hasil pengujian yang dilakukan, maka dapat disimpulkan bahwa metode LSB m-bit dapat digunakan dengan baik sampai m bernilai tiga. Penggunaan nilai m dari satu

hingga tiga menghasilkan nilai rata-rata PSNR sebesar 46,36, 39,87 dan 33,31 artinya kualitas stego image masih terlihat baik. Kualitas stego image akan berkurang bila menggunakan m dari empat hingga tujuh. Penggunaan nilai m sampai dengan tiga, akan dapat meningkatkan daya tampung informasi yang disisipkan hingga tiga kali dan kualitas stego image masih baik.

Saran untuk penelitian selanjutnya agar daya tampung dapat ditingkatkan lagi adalah perlunya dilakukan eksperimen dengan melakukan proses kompresi pada informasi yang disisipkan. Dengan melakukan kompresi, diharapkan ukuran informasi akan menjadi lebih kecil sehingga dapat menyisipkan lebih banyak lagi.

REFERENSI

- [1] N. S. Lubis and M. I. P. Nasution, "Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat," *KOHESI J. Multidisiplin Saintek*, vol. 1, no. 12, pp. 41–50, 2023, doi: <https://doi.org/10.3785/kohesi.v1i12.1311>.
- [2] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia," *Skatika*, vol. 4, no. 1, pp. 66–71, 2021, doi: 10.36080/skatika.v4i1.2044.
- [3] D. Agustina Akmal *et al.*, "Kombinasi Kriptografi Modern Dalam Keamanan Pesan Teks," *Saturnus J. Teknol. dan Sist. Inf.*, vol. 2, no. 4, pp. 11–17, 2024, doi:

- <https://doi.org/10.61132/saturnus.v2i3.204>.
- [4] A. Aryasanti, R. Ujiandari, M. Hardjianto, and R. Kusumawardani, "Implementasi Keamanan File Menggunakan Metode Kriptografi Base-64 dan Steganografi Least Significant Bit (LSB) Random 2-Bit Berbasis Web," *J. Ticom*, vol. 11, pp. 113–118, 2023, doi: <https://doi.org/10.70309/ticom.v11i2.78>.
- [5] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital," *Voteteknika (Vocational Tek. Elektron. dan Inform.,* vol. 11, no. 1, pp. 63-70, 2023, doi: [10.24036/voteteknika.v11i1.121968](https://doi.org/10.24036/voteteknika.v11i1.121968).
- [6] V. Veriarinal, and R. Wanandi, "Implementasi Sistem Steganografi Citra Dengan Metode Substitusi LSB (Least Significant Bit)," *J. Multidisiplin Saintek*, vol. 2, no. 11, pp. 5–24, 2024, <https://doi.org/10.3785/koehi.v2i11.2674>.
- [7] A. R. Mido, E. Iman, and H. Ujianto, "Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan Steganografi LSB," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, pp. 279–286, 2022, doi: [10.25126/jtiik.202294852](https://doi.org/10.25126/jtiik.202294852).
- [8] S. Hidayat, P. N. Andono, T. Informatika, and U. D. Nuswantoro, "Analisis Keamanan Steganografi Multi-Layer dengan Enkripsi Vigenère dan Caesar Cipher pada Citra Digital Security Analysis of Multi-Layer Steganography with Vigenère Encryption and Caesar Cipher on Digital Images," vol. 5, no. 3, pp. 869–880, 2025, doi: <http://dx.doi.org/10.52436/1.jpti.786>.
- [9] N. Ratama and M. Munawaroh, "Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1272, 2022, doi: [10.30865/mib.v6i2.3902](https://doi.org/10.30865/mib.v6i2.3902).
- [10] I. Haverkamp and D. K. Sarmah, "Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis," *International Journal. Information Security.*, vol. 23, no. 4, pp. 2607–2635, 2024, doi: <http://dx.doi.org/10.21203/rs.3.rs-3167378/v1>.
- [11] E M. L. Aksani, L. Azhari, and F. E. Nugroho, "Studi Dan Implementasi Steganografi Pada Citra PNG Dengan Metode Least-Significant Bit (LSB) Menggunakan Java," vol. 14, no. 01, pp. 39–44, 2025, doi: <http://dx.doi.org/10.31000/jt.v14i1.13643>.
- [12] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 36–47, 2020, doi: <https://doi.org/10.32493/informatika.v5i1.4646>.
- [13] P. Kusuma and Y. Prayudi, "Implementasi Steganografi Dengan Menggunakan Metode Masking and Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram Audio," *Ajie - Asian Journal Innovation Entrepreneurship*, vol. 9, no. 1, pp. 1–15, 2025, doi: <http://dx.doi.org/10.20885/ajie.vol9.iss1.art1>.
- [14] M. B. Ulum, S. Sandfreni, and A. H. Azizah, "Perbandingan Teknik Steganografi Domain Spasial Dengan Domain Transformasi Pada Audio," *Sebatik*, vol. 25, no. 2, pp. 661–666, 2021, doi: [10.46984/sebatik.v25i2.1642](https://doi.org/10.46984/sebatik.v25i2.1642).
- [15] R. Humayrah, A. M. Elhanafi, and M. T. Batubara, "Analisa Histogram dan PSNR Pada Citra True Color Dalam Pengamanan Teks Menggunakan Spread Spectrum dan LSB," *JIRSI: Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 2, no. 1, pp. 72-84, 2023, doi: <https://doi.org/10.70340/jirsi.v2i1.48>.