

OPTIMASI STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) METODE OPERASI PERGESERAN BIST

Yudhi Darmawan, Nico Fahrul Marinza, Yohanes Dwi Cahyono

Jurusan Telekomunikasi, Politeknik Angkatan Darat

Junrejo, Kota Batu, Jawa Timur-Indonesia 65324

yohanes@poltekad.ac.id

ABSTRAK

Penelitian ini membahas optimasi metode steganografi berbasis Least Significant Bit (LSB) dengan menggunakan operasi pergeseran bit untuk meningkatkan kapasitas penyembunyian pesan dalam gambar digital. Metode ini memodifikasi 8 bit per piksel yang melibatkan warna merah, hijau, biru, dan alpha untuk meningkatkan jumlah karakter yang dapat disisipkan dibandingkan dengan metode sebelumnya yang hanya memodifikasi 3 bit per piksel. Implementasi melibatkan dua tahap utama: operasi masker bit dan injeksi bit dengan logika AND dan OR. Penelitian ini mengevaluasi kualitas gambar steganografi dengan membandingkan nilai Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE) antara gambar penutup dan gambar steganografi. Hasil menunjukkan bahwa meskipun kapasitas penyisipan meningkat, kualitas gambar sedikit menurun dibandingkan metode sebelumnya. Namun, metode yang diusulkan tetap memberikan peningkatan signifikan dalam kapasitas penyembunyian pesan tanpa merusak gambar secara drastis.

Kata kunci : steganografi, LSB, operasi bit, kapasitas penyembunyian, PSNR, MSE.

1. PENDAHULUAN

Steganografi, sebuah teknik untuk menyembunyikan pesan rahasia dalam media yang tampak biasa, seperti gambar, memiliki kepentingan besar dalam konteks keamanan data, privasi komunikasi, dan investigasi kriminal. Keberadaan pesan rahasia dalam gambar memungkinkan komunikasi yang aman tanpa menarik perhatian pihak lain (Jain, 2020). Dalam penelitian ini, fokus utama adalah pada teknik steganografi berbasis Least Significant Bit (LSB) dan varian-varian pendekatannya.

Penelitian-penelitian terkait telah mencoba berbagai teknik, salah satunya menggunakan teknik manipulasi bit, seperti LSB. Meskipun teknik ini menghasilkan gambar steganografi dengan kualitas hampir sama seperti gambar aslinya, daya tampung karakter terbatas (Putra, 2018). Beberapa pendekatan sederhana, seperti Pixel Value Differencing (PVD) dan Modulus Function (MF), berhasil meningkatkan penyisipan pesan rahasia tanpa signifikan merusak kualitas gambar (Darwis, 2020).

Namun, peningkatan kapasitas penyembunyian perlu diperhatikan. Sebagai contoh, varian metode PVD MF 1 dan PVD MF 2 berhasil meningkatkan kapasitas penyembunyian, meskipun dengan trade-off antara PSNR dan HC (Sahu, 2019). Perbaikan lebih lanjut dapat dicapai dengan mengkorelasikan saluran RGB yang berwarna untuk meningkatkan kapasitas penyembunyian. Selain itu, belum dibahas bagaimana teknik penyembunyian pesan dapat dikombinasikan dengan lapisan keamanan tambahan.

Berdasarkan rangkuman penelitian-penelitian sebelumnya, permasalahan penelitian yang muncul melibatkan daya tampung karakter pada gambar steganografi, khususnya pada teknik steganografi LSB dan pendekatannya. Dua masalah penelitian teridentifikasi yang pertama daya tampung karakter

terbatas pada teknik steganografi LSB, dan yang kedua jumlah bit yang dapat ditampung terbatas pada pendekatan PVD MF.

Dari masalah tersebut, terbentuk dua pertanyaan penelitian: Bagaimana menyusun algoritma modifikasi bit yang dapat memaksimalkan daya tampung karakter dalam gambar steganografi? Dan bagaimana kualitas gambar steganografi setelah penerapan algoritma modifikasi bit tersebut?

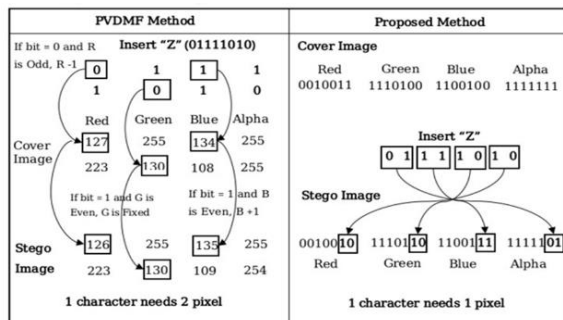
Dalam menjawab pertanyaan penelitian, peneliti merancang sebuah metode modifikasi bit yang melibatkan operasi geser bit, injeksi bit dengan operasi AND dan OR. Evaluasi kualitas gambar dilakukan dengan menganalisis Histogram Equalization dan membandingkan Peak Signal-to-Noise Ratio (PSNR) antara gambar cover dan gambar steganografi.

2. TINJAUAN PUSTAKA

Dalam metode PVD MF, jumlah bit yang dimodifikasi hanya sebanyak 3 bit per piksel, di mana bit yang dimodifikasi terdapat pada warna Merah, Hijau, dan Biru. Sementara itu, untuk metode yang ditingkatkan yang diusulkan dalam penelitian ini, jumlah bit yang dimodifikasi adalah 8 bit per piksel. Bit yang dimodifikasi dalam metode yang diusulkan terletak pada warna Merah, Hijau, Biru, dan Alpha. Untuk mendapatkan gambaran lengkap tentang perbedaan antara kedua metode ini, Anda dapat melihat pada Gambar 1.

Untuk mengimplementasikan metode steganografi ini, para peneliti menerapkan metode modifikasi bit yang terdiri dari 2 langkah, yaitu (1) operasi masker bit, (2) injeksi bit menggunakan operasi AND dan OR. Langkah pertama, yaitu operasi pergeseran bit, bertujuan untuk menggeser bit pesan rahasia agar posisinya sesuai dengan lokasi warna yang diinginkan. Langkah selanjutnya adalah menyisipkan bit pesan rahasia ke dalam gambar cover.

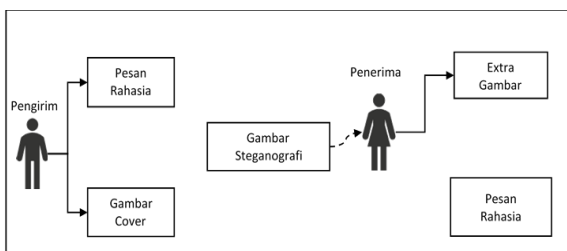
Untuk penyisipan ini, para peneliti memanfaatkan operasi logika AND dan OR. Persamaan matematika untuk proses encoding ini akan dijelaskan pada sub bab metodologi dibawah ini.



Gambar 1. Perbandingan Metode PVDMF dengan Metode yang Diusulkan

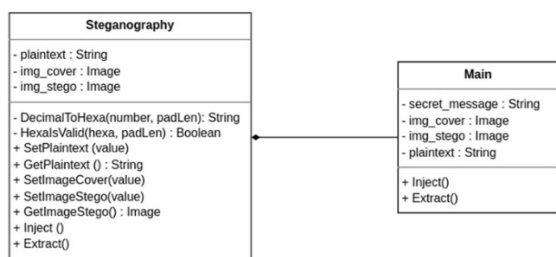
3. METODE PENELITIAN

Dalam topik pembahasan ini, para peneliti menyajikan optimasi operasi pergeseran bit LSB untuk menampung jumlah karakter yang lebih besar dibandingkan metode LSB dengan PVDMF. Alur keseluruhan metode dalam penelitian ini diilustrasikan dalam Gambar 1 di bawah ini.



Gambar 2. Model Sistem Steganografi

Sesuai dengan alur sistem seperti yang telah dijelaskan sebelumnya, desain sistem yang dikembangkan dalam penelitian ini mengikuti alur diagram kelas berikut.



Gambar 3. Diagram Kelas dari Sistem Steganografi

Penjelasan rinci mengenai setiap langkah dalam kontribusi penelitian pertama dapat dilihat pada persamaan matematika untuk proses encoding ini terlihat seperti persamaan 1 di bawah ini.

a. Initialization :

- `img = read image from cover image`
- `pixel = Convert from image array 3D to array 1D`

b. Convert Message Length to Hexadecimal Format :

- `data_length = format(len(secret_message), '06h')`
- `decimal_msg = encode_utf8(data_length + secret message)`

c. Insert Message into Pixel:

For `i in 0 ≤ i < length(decimal_msg)`

• Masking bit Operation :

- `asciiCode=decimal_msg[i].`
- `_maskR=(asciiCode & 3) >>>0`
- `_maskG=(asciiCode & 12) >>>2`
- `_maskB=(asciiCode & 48) >>>4`
- `_maskA=(asciiCode & 192) >>>6`

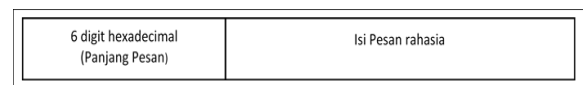
• Bit Injection

- `pixel[4× i + 0]=(pixel[4× i + 0] & 252) V _maskR`
- `pixel[4× i + 1]=(pixel[4× i + 1] & 252) V _maskG`
- `pixel[4× i + 2]=(pixel[4× i + 2] & 252) V _maskB`
- `pixel[4× i + 3]=(pixel[4× i + 3] & 252) V _maskA`

d. Result :

- `img = Convert from array pixel 1D to array 3D`
- `Save to file ('secret_image.png')`

Format data pesan tersembunyi terlihat seperti pada Gambar 4.



Gambar 4. Format Data Pesan Tersembunyi

Untuk mengekstrak pesan rahasia dari gambar, para peneliti menerapkan metode operasi AND dan menggeser bit dari piksel Alpha, biru, hijau, dan merah. Persamaan matematika untuk proses pengkodean ini terlihat seperti persamaan 2 di bawah ini.

a. Initialization :

- `img = read image from stego image`
- `pixel = Convert from image array 3D to array 1D`
- `i = 0, completed=false, hidden_msg = empty string, extract_bit = 0, number_of_hidden_msg = 0`

b. Extract bit into String Hidden Message:

while (`i < length(pixel) AND completed=false`)

- Get 2 digit of bit LSB from Pixel Alpha-Blue-Green-Red :

- `_2bit_A=(pixel[(4× i) + 0] & 3) <<< 0`
- `_2bit_B=(pixel[(4× i) + 1] & 3) <<< 2`
- `_2bit_G=(pixel[(4× i) + 2] & 3) <<< 4`
- `_2bit_R=(pixel[(4× i) + 3] & 3) <<< 6`

- Extract 8 digit of bit to ASCII :

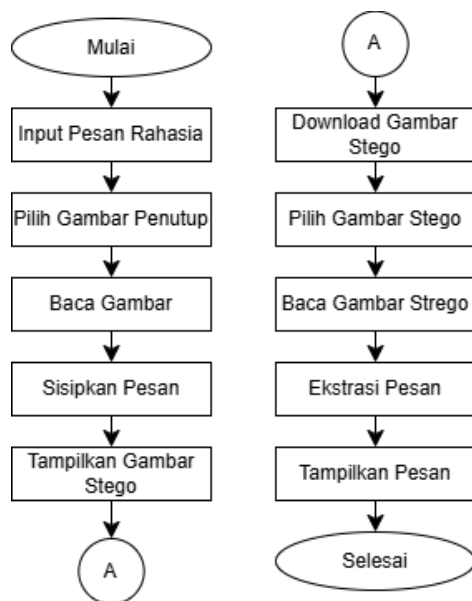
- `asciiCode=(((_2bit_A V _2bit_B) V _2bit_G)V _2bit_R)`

- Assembly ASCII to String Hidden Message:

- i. `hidden_msg += chr(asciiCode)`
- ii. `extract_bit += 1`
- Calculate the length of the hidden message
 - i. if (length of hidden_msg=6) AND (number_of_hidden_msg = 0)
 - 1. `number_of_hidden_msg=Convert to Integer(hidden_msg)`
 - 2. `hidden_msg=empty string`
 - ii. else
 - if (extract_bit ≥ (number_of_hidden_msg+6))
 - 1. `completed=true`
- 3. Completed extract of Hidden Message :
 - Return hidden_msg

4. HASIL DAN PEMBAHASAN

Dari Bab sebelumnya peneliti sudah menjelaskan langkah demi langkah dari Algoritma dan kelas diagram untuk mengembangkan metode penelitian yang diusulkan, berikut ini adalah Implementasi dari aplikasi Steganografi menggunakan bahasa Pemrograman Javascript. Ada 3 file yang digunakan untuk menjalankan program yang dimaksud diantaranya ada 2 file Javascript dan 1 file HTML sebagai berikut;



Gambar 5. Implementasi

Program dalam penelitian ini mendukung Antarmuka Pengguna Grafis (GUI). Studi eksperimental dilakukan dalam empat tahap menggunakan GUI. Tahap-tahap ini dijelaskan sebagai berikut:

- a. Gambar Cover: Pada tahap ini, gambar penutup diunggah dari kamera atau file menggunakan GUI.
- b. Pesan Rahasia: Pengguna mengunggah pesan yang ingin disembunyikan dalam gambar penutup secara manual.
- c. Menyembunyikan Data dengan Menggeser Bit LSB: Pada fase ini, pesan rahasia yang telah dienkripsi disisipkan ke dalam gambar penutup. Proses ini melibatkan pergeseran Bit Paling Tidak

Signifikan (LSB) dari nilai piksel dalam gambar penutup.

- d. Analisis: Bagian ini menyediakan analisis data tentang gambar stego. Nilai Peak Signal-to-Noise Ratio (PSNR) (Hore, 2010) dihitung untuk mengukur kualitas gambar stego dibandingkan dengan gambar penutup. Perhitungan nilai PSNR diberikan dalam Persamaan 3.

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \quad (3)$$

$$MSE = \frac{1}{n} \sum_{i=1}^n (Y_i - \hat{Y}_i)^2$$

Gambar 6. menampilkan gambar-gambar yang digunakan dalam studi eksperimental ini.



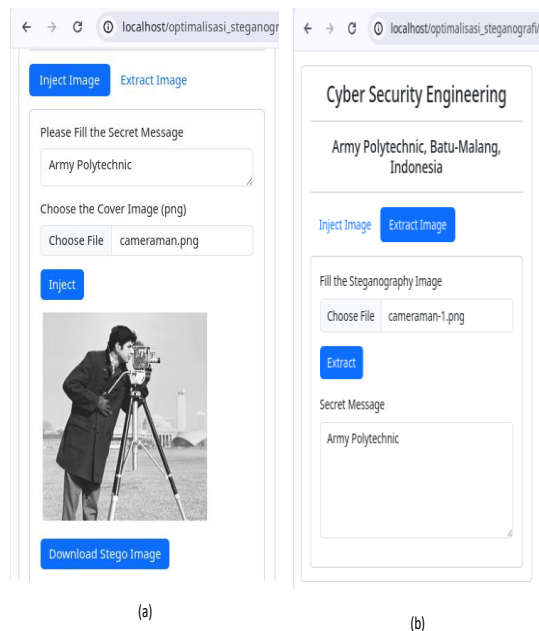
(a)



(b)

Gambar 6. Gambar dalam studi eksperimental (a) Cameraman (b) Lena

Pada Gambar 7, ditampilkan contoh gambar antarmuka pengguna (GUI) Steganografi.



Gambar 7. Antarmuka Pengguna (GUI) untuk Steganografi (a) *Inject* (b) *Extract*

4.1. Menyembunyikan Data dengan Menggeser Bit LSB

Kontribusi dalam penelitian ini berhasil menjawab rumusan masalah yaitu bagaimana mengembangkan algoritma modifikasi bit yang dapat memaksimalkan kapasitas karakter yang dapat disisipkan ke dalam gambar cover? Jika dalam penelitian sebelumnya kapasitas dapat ditingkatkan sebesar 3,1 bit per piksel (Sahu, 2019), dan 4 bit per piksel (Darwis, 2020), maka dalam penelitian ini kapasitas dapat ditingkatkan menjadi 8 bit per piksel (1 byte per piksel). Jadi, jika dalam penelitian sebelumnya dibutuhkan 2 piksel untuk menyisipkan 1 karakter (8 bit), maka dalam penelitian ini 1 karakter (8 bit) dapat disisipkan ke dalam 1 piksel (8 bit per piksel). Perbandingan jumlah piksel yang berubah ketika menggunakan metode PVDMF (Darwis, 2020) dengan metode yang diusulkan ditunjukkan dalam Gambar 6.

Berdasarkan penjelasan di atas, kontribusi dari penelitian ini berhasil memperbaiki kelemahan-kelemahan dari penelitian sebelumnya. Jika pada penelitian sebelumnya hanya mungkin menyisipkan 4 bit per piksel (Darwis, 2020), maka dalam penelitian ini dapat ditingkatkan menjadi 8 bit per piksel (1 byte per piksel).

Cover Image					Stego Image				
Pixel	R	G	B	A	Pixel	R	G	B	A
0	210	210	210	255	0	210	210	210	254
1	212	212	212	255	1	212	212	212	254
2	213	213	213	255	2	212	212	212	254
3	213	213	213	255	3	212	212	212	254
4	211	211	211	255	4	210	210	210	254
5	211	211	211	255	5	210	211	210	254
6	213	213	213	255	6	212	213	212	254
7	213	213	213	255	7	212	212	212	255
8	214	214	214	255	8	214	215	215	255
9	210	210	210	255	9	210	210	211	254
10	211	211	211	255	10	210	211	211	254
11	212	212	212	255	11	213	213	212	255
12	211	211	211	255	12	210	211	211	255
13	211	211	211	255	13	211	210	210	255
14	211	211	211	255	14	211	211	211	255
15	211	211	211	255	15	211	211	211	255

(a)

Cover Image					Stego Image				
Pixel	R	G	B	A	Pixel	R	G	B	A
0	210	210	210	255	0	208	208	211	252
1	212	212	212	255	1	212	212	215	252
2	213	213	213	255	2	212	212	215	252
3	213	213	213	255	3	212	212	215	252
4	211	211	211	255	4	208	208	211	252
5	211	211	211	255	5	208	209	211	252
6	213	213	213	255	6	213	212	212	253
7	213	213	213	255	7	214	212	215	253
8	214	214	214	255	8	213	215	214	253
9	210	210	210	255	9	209	210	211	253
10	211	211	211	255	10	211	211	211	255
11	212	212	212	255	11	212	212	212	255
12	211	211	211	255	12	211	211	211	255
13	211	211	211	255	13	211	211	211	255
14	211	211	211	255	14	211	211	211	255
15	211	211	211	255	15	211	211	211	255

(b)

Gambar 8. Perbandingan jumlah piksel (a) PVDMF (b) metode yang diusulkan

4.2. Analisis Kualitas Gambar

Analisis kualitas gambar yang dimaksud adalah membandingkan nilai PNSR (Peak Signal-to-Noise Ratio) dan MSE (Mean Squared Error) dari gambar steganografi menggunakan metode PVDMF dengan metode yang diusulkan. Untuk menghindari perbedaan dalam nilai PNSR dan MSE, pesan tersembunyi tidak dienkripsi. Adapun cara menganalisis kualitas gambar, dapat dilihat dari kedua nilai ini. Semakin tinggi nilai PNSR, semakin baik kualitas gambar. Di sisi lain, semakin rendah nilai MSE, semakin baik kualitas gambar. Hasil uji mengukur nilai MSE dan PNSR dapat dilihat pada tabel 1 di bawah ini.

Tabel 1. Perbandingan PNSR dan MSE Metode

Gambar Cover	Pesan Rahasia	Metode	PNSR	MSE
Cameraman.png (256x256 px)	Army Polytechnic	PVDMF	41.4030 dB	0.00034
		Metode yang diusulkan	39.7116 dB	0.00074
Lena.png (512x512 px)	Army Polytechnic	PVDMF	44.5128 dB	0.00013
		Metode yang diusulkan	42.0935 dB	0.00024

4.3. PVDMF dengan Metode yang Diusulkan

Dari hasil uji, ditemukan bukti bahwa kualitas citra steganografi dari metode yang diusulkan tidak lebih baik dibandingkan dengan metode sebelumnya (PVDMF). Hal ini terlihat dari nilai PNSR metode yang diusulkan, yang lebih rendah dibandingkan

dengan metode sebelumnya. Sementara itu, nilai MSE metode yang diusulkan lebih tinggi dibandingkan dengan metode sebelumnya.

5. KESIMPULAN DAN SARAN

Penelitian ini juga berhasil meningkatkan kapasitas penyisipan (HC) karakter pesan rahasia, sebanyak 8 bit per piksel (1 byte per piksel), dengan memanfaatkan saluran RGBA. Pada penelitian sebelumnya yang menggunakan metode PVD MF, kapasitas penyisipan (HC) hanya mencapai 3.1 bit per piksel (BPP). Meskipun demikian, jika dianalisis dari segi kualitas gambar, metode yang diusulkan tidak lebih baik daripada penelitian sebelumnya, yaitu metode Pixel Value Differentiating and Modulus Function (PVD MF). Ini terbukti dari hasil uji yang menunjukkan nilai PNSR dan MSE yang lebih buruk.

Penelitian selanjutnya disarankan untuk mengoptimalkan algoritma penyisipan agar menjaga keseimbangan antara kapasitas penyisipan dan kualitas gambar dengan menggunakan pendekatan hybrid atau kompresi pesan sebelum penyisipan, mengeksplorasi model warna seperti HSV atau YCbCr untuk meningkatkan efisiensi visual, menambahkan metode pengujian seperti SSIM untuk evaluasi yang lebih akurat, serta mempertimbangkan penggunaan teknik enkripsi guna meningkatkan keamanan pesan.

DAFTAR PUSTAKA

- [1] R.C. Jain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology, 2020
- [2] P.C. Mandal at al, (2022). "Digital image steganography: A literature survey" , Elsevier, Information Sciences Volume 609, Pages 1451-1488, <https://doi.org/10.1016/j.ins.2022.07.120>, <https://www.sciencedirect.com/science/article/abs/pii/S002002552200809X>
- [3] ALBaaj, Ghassan Faisal Falih, "A Model to Share Hidden Data in Image for Military Access", Texas Journal of Engineering and Technology 2022, Accessed on : <https://zienjournals.com/index.php/tjet/article/download/701/569/735>
- [4] Putra, Randi Rian, at al, (2018), "Implementation of LSB Steganography on Embedding Messages in Digital Image", Article in International Journal of Scientific Research in Science and Technology, Volume 4, Issue 11, Print ISSN: 2395-6011, Online ISSN: 2395-602X, DOI : <https://doi.org/10.32628/IJSRST18401112>
- [5] Zakaria, Abdul Alif, at al, (2018). High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution, MDPI, Appl. Sci. 2018, 8, 2199; doi:10.3390/app8112199
- [6] D. Darwis, N. B. Pamungkas, Wamiliana, (2020). Comparison of Least Significant Bit Pixel Value Differencing and Modulus Function on Steganography to Measure Image Quality Storage Capacity and Robustness, Journal of Physics: Conference Series, Volume 1751, The 3rd International Conference on Applied Sciences Mathematics and Informatics (ICASMI)
- [7] Sahu, A.K., Swain, G. (2019) An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. Wireless Pers Commun 108, 159–174. <https://doi.org/10.1007/s11277-019-06393-z>
- [8] Purba, Lia Cintia at al, (2021). Penggunaan Algoritma LSB dan Vigenere untuk Pengamanan Data melalui Pola Citra Digital, TECHSI: Vol. 13, No. 2, DOI: <https://doi.org/10.29103/techsi.v13i2.5162>
- [9] Hore, A. , Ziou, D., "Image quality metrics: PSNR vs. SSIM", In Pattern recognition (icpr) 20th international conference on IEEE, 2366-2369, 2010