

Peningkatan Kualitas *Stego-image* Menggunakan *Advanced Least Significant Bit*

Cahya Adhi Bintang Husada¹, Alamsyah²

Jurusan Teknik Informatika, FMIPA, Universitas Negeri Semarang, Indonesia
Kampus Sekaran Gunungpati, Semarang 50229

*E-mail: ¹bintang_h@students.unnes.ac.id, ²alamsyah@mail.unnes.ac.id

Diterima 12 Januari 2022

Disetujui 10 Maret 2022

Dipublikasikan 28 April 2022

Abstrak

Steganografi merupakan suatu ilmu menyembunyikan pesan atau menulis pesan secara tersembunyi, sehingga hanya pengirim dan penerima pesan yang dapat memahami isi dari pesan tersebut dan tidak ada orang lain yang dapat menyadari atau mengetahui bahwa ada suatu pesan yang disembunyikan. Modifikasi metode LSB mengembangkan metode LSB sebelumnya dengan penginputan pesan diberi jarak satu piksel yang memuat *red, green, blue* (RGB) tiap piksel pada media *cover* (media untuk menyembunyikan pesan). Pada penelitian ini menggunakan delapan dataset berupa gambar PNG 24-bit dan 32-bit. Pada akhir baris piksel disisipkan *password* sebagai pengaman sekaligus *counter* pesan yang akan dipanggil. Penyisipan dilakukan selang-seling antara piksel secara kontinu hingga semua pesan tersisipkan. Rekonstruksi ulang gambar *cover-image* harus mempertahankan nilai *cover-image* ketika didekomposisi menjadi sebuah *stego-image*. Penyimpanan pada tahap ini menggunakan format *file .bmp* karena kompresi tipe file ini lebih tahan terhadap perubahan. Modifikasi metode LSB dalam penelitian ini dapat meningkatkan tingkat akurasi yang diukur dengan nilai *Mean Squared Error* (MSE) sebesar 0.000607464 sampai dengan 0.465577667 dan *Peak Signal-to-Noise Ratio* (PSNR) sebesar 64,49 dB sampai dengan 129,53 dB. Berdasarkan data ini, algoritma yang diusulkan mengalami peningkatan kualitas *stego-image*.

Kata Kunci: Steganografi, *advanced LSB*, kualitas, *stego-image*

Abstract

Steganography is a science of hiding messages or writing messages hiddenly, so that only the sender and recipient of the message can understand the contents of the message and no one else can realize or know that there is a hidden message. Modification of the LSB method developed the previous LSB method by inputting messages at a distance of one pixel containing red, green, blue (RGB) per pixel on the media cover (media to hide messages). In this study, eight datasets were used in the form of 24-bit and 32-bit PNG images. At the end of the pixel line, a password is inserted as a security as well as a counter message to be called. Insertion is done alternately between pixels continuously until all messages are inserted. Reconstruction of the cover-image image must retain the value of the cover-image when decomposed into a stego-image. Storage at this stage uses the .bmp file format because the compression of this file type is more resistant to changes. Modification of the LSB method in this study can increase the level of accuracy as measured by the Mean Squared Error (MSE) value of 0.000607464 to 0.465577667 and Peak Signal-to-Noise Ratio (PSNR) of 64.49 dB to 129.53 dB. Based on these data, the proposed algorithm has improved the quality of the stego-image.

Keyword: Steganografi, *advanced LSB*, quality, *stego-image*

How to cite:

Husada C.A.B., & Alamsyah. (2022). Peningkatan kualitas *stego-image* menggunakan advanced least significant bit. *Indonesian Journal of Mathematics and natural Sciences*, 45(1), 30-37

PENDAHULUAN

Steganografi adalah teknik yang menyembunyikan komunikasi dengan menyembunyikan informasi dalam informasi lain (Morkel *et al.*, 2005). Akhir-akhir ini steganografi banyak disalahgunakan, salah satunya digunakan untuk menyisipkan pesan-pesan tertentu berdasarkan kejahatan. Oleh karena itu, analisis steganografi diperlukan untuk mengendalikan penyalahgunaan

steganografi (Nasution *et al.*, 2017). Perkembangan Steganografi saat ini semakin meluas. Salah satu media yang dapat digunakan untuk steganografi adalah citra digital. Secara matematis, bayangan merupakan fungsi kontinu dengan intensitas cahaya pada bidang dua dimensi (Chen, 2011).

Algoritma teknologi steganografi LSB yang canggih mengembangkan algoritma steganografi yang ada seperti LSB dengan memanfaatkan rentang nilai piksel di media sampul (gambar yang digunakan sebagai gambar untuk menyembunyikan pesan). Semakin tinggi nilai piksel, semakin banyak bit pesan yang disembunyikan, dan sebaliknya semakin kecil nilai piksel, semakin sedikit bit pesan yang disembunyikan (Fadlil *et al.*, 2021). *Advanced* LSB adalah teknik penyembunyian pesan yang menampilkan pengembangan LSB standar, di mana pesan disembunyikan atau disisipkan secara bergantian ke dalam gambar dan jarak antara setiap piksel ditentukan, seperti dijelaskan di atas. Kualitas gambar Stego-image lebih baik.

Susunan algoritma *Advanced* LSB modifikasi yang dapat meningkatkan kemampuan menyembunyikan pesan (Odat & Otair, 2016). Error yang dihasilkan LSB standar lebih tinggi untuk nilai error, sedangkan LSB modifikasi memiliki error rendah. Untuk hasil *stego-image*, kualitas gambar yang dihasilkan biasanya kurang baik, sedangkan LSB yang dimodifikasi memiliki kualitas yang baik. Dalam penyisipan pesan, setiap pesan dibaca sebagai nilai ASCII sehingga dapat diubah menjadi nilai biner untuk diproses dalam algoritma (Arya & Soni, 2018).

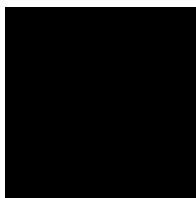
Pesan dari standar LSB yang disampaikan hasilnya kurang baik untuk pengambilan kembali pesan, sedangkan pesan LSB yang dimodifikasi hasilnya bagus. Sebuah *stego-image* yang baik dapat diekstraksi kembali setelah dikirim melalui *cloud* atau media perpesanan (Hassaballah, 2020).

Metode *masking* tergantung pada ekstraksi tiga saluran berwarna RGB untuk setiap piksel dan menentukan tempat di mana bit pesan enkripsi akan disembunyikan (Fadlil *et al.*, 2021). Teknik steganografi yang berbeda telah disajikan berdasarkan gambar RGB karena gambar dianggap sebagai penutup yang aman untuk data yang tersembunyi (Almazaydeh, 2020).

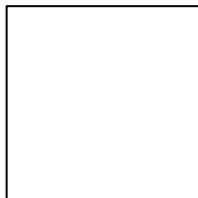
METODE

Dataset

Data dalam penelitian ini diperoleh dari www.imageprocessingplace.com dengan tambahan 2 gambar. Data yang digunakan adalah 8 citra yang kemudian dibagi menjadi 4 kategori berdasarkan jenis citra dan ukuran pikselnya, citra greyscale berukuran 512 x 512 piksel, citra berwarna berukuran 594 x 400 piksel, citra berwarna berukuran 768 x 512 piksel, citra berwarna gambar berukuran 512 x 512 piksel. Data yang digunakan ditunjukkan pada Gambar 1 sampai dengan Gambar 8.



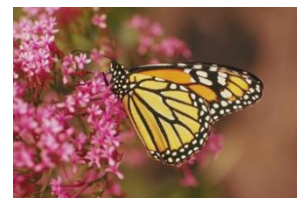
Gambar 1. *Black*



Gambar 2. *White*



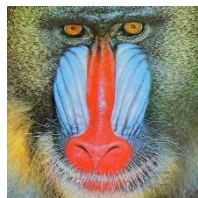
Gambar 3. *Artichere*



Gambar 4. *Monarch*



Gambar 5. *Airplane*



Gambar 6. *Baboon*



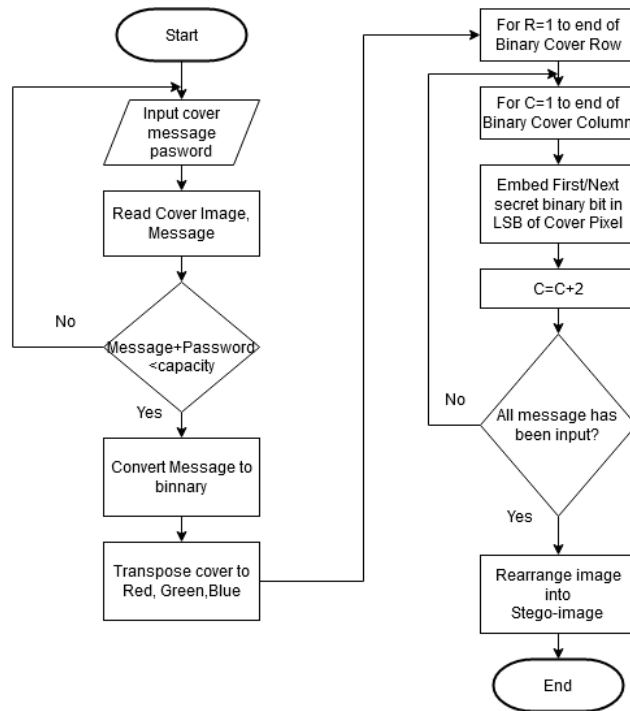
Gambar 7. *Lena*



Gambar 8. *Peppers*

Tahap Eksperimen

Pada tahap ini menggunakan *Advanced* LSB untuk meningkatkan kualitas *stego-image*. Flowchart yang digunakan pada metode ini ditunjukkan pada Gambar 9.



Gambar 9. Flowchart Advanced LSB

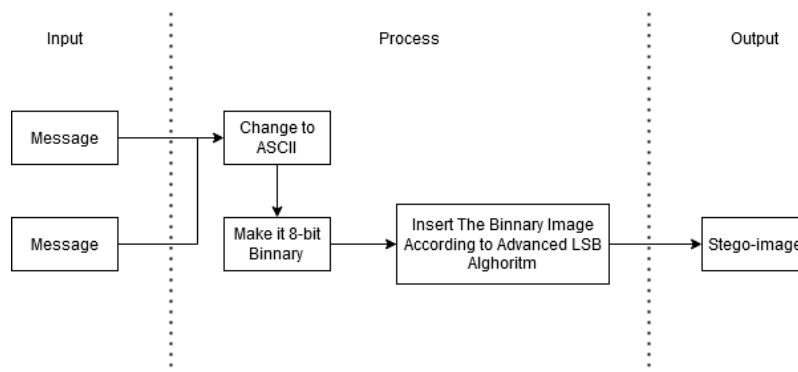
Data dibaca dan ditulis sebaris dari piksel awal atau piksel kiri atas (0,0) ke kanan hingga ujung lebar citra pada baris pertama kemudian ke baris kedua dan seterusnya hingga piksel terakhir atau bawah piksel sudut kanan (lebar, panjang) dalam satu saluran warna hingga saluran warna terakhir (Alamsyah *et al.*, 2020). Nilai piksel yang dibaca atau ditulis berada pada rentang yang diproses 0 - 255. Pada penyisipan pesan, setiap pesan dibaca sebagai nilai ASCII sehingga dapat diubah menjadi nilai biner untuk diproses dalam algoritma (Yosanny, 2010).

Advanced LSB

Metode LSB lanjutan adalah teknik penyembunyian pesan yang dikembangkan dari LSB dimana metode ini menggunakan delapan bit kunci dan menjalankan proses XOR dengan semua byte pesan yang akan dimasukkan dan juga memiliki aturan dalam penyisipan pesan (Kekre *et al.*, 2012).

Penyisipan

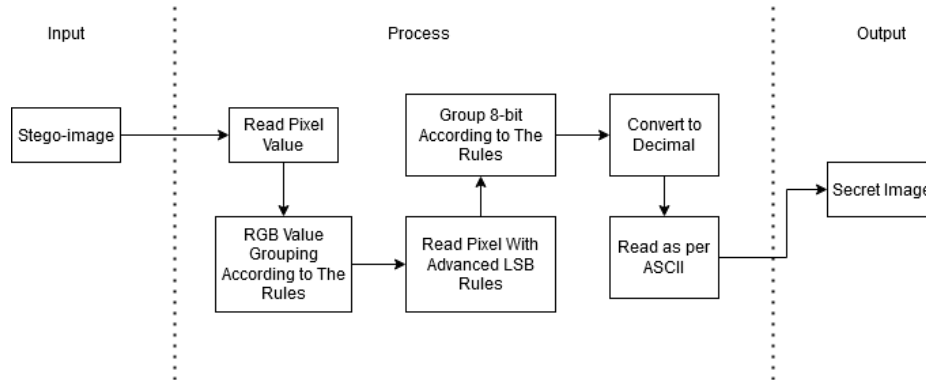
Penyisipan pesan untuk rentang piksel dengan jumlah bit pesan maksimum yang dapat kita sembunyikan adalah dijelaskan dalam aturan yang ditulis dalam metode LSB lanjutan (Langi, 2013). Proses embedding ditunjukkan pada Gambar 10.



Gambar 10. Proses Penyisipan

Ekstraksi

Untuk mengambil pesan rahasia, itu dapat diambil dengan memeriksa empat bit pertama MSB dan menggunakan langkah penyisipan untuk mengambil bit data rahasia (Lemire, 2010). Jadi empat bit pertama bernilai 1, kemudian 4 bit akan diambil dari belakang sebagai pesan rahasia. Itu adalah kecocokan untuk 3 bit, 2 bit, dan 1 bit. Proses ekstraksinya adalah ditunjukkan pada Gambar 11.



Gambar 11. Proses Ekstraksi

MSE dan PSNR

Mean square error (MSE) mengacu kepada kuadrat error antara pesan sampel dengan *stego-image*. MSE membantu mengukur tingkat distorsi pada citra. Rumus dari MSE dapat dilihat pada Persamaan 1.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (1)$$

$I(i, j)$ dan $K(i, j)$ adalah nilai piksel dari citra asli dan *stego-image* masing-masing. M dan N merepresentasikan jumlah baris dan kolom pada citra masukan. *Peak signal to noise ratio* (PSNR) didefinisikan sebagai rasio puncak atau sinyal maksimum terhadap noise yang terkait dengan citra asli dan citra stego. PSNR diukur dalam desibel (dB). Rumus PSNR pada Persamaan 2.

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) = 20 \log_{10} \left(\frac{MAX}{\sqrt{MSE}} \right) \quad (2)$$

MAX adalah nilai kemungkinan tertinggi pada citra, MSE adalah rata-rata kuadrat error piksel antara dua citra (Bala, 2017).

HASIL DAN PEMBAHASAN

Bagian ini membahas hasil penelitian dengan menggunakan metode LSB Standar dan metode *Advanced* LSB. Implementasi metode menggunakan Matlab 2019a. Hasil penelitian yang telah didapatkan antara lain penyisipan LSB standar, penyisipan dengan *Advanced* LSB.

Nilai Biner Pesan Teks dan Nilai Biner Kunci

Untuk pengujian kali ini, pesan yang disisipkan terdiri dari karakter, pesan yang disisipkan adalah “Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan.” Dan untuk kunci menggunakan 6 karakter “unnes”. Pesan ditunjukkan pada Tabel 1, dan untuk kunci ditunjukkan pada Tabel 2.

Tabel 1. Nilai Biner Pesan

No.	PEsan	ASCII	Nilai Biner
1	S	83	01010011
2	t	116	01110100
3	e	101	01100101
4	g	103	01100111
5	a	97	01100001
:	:	:	:
86	.	46	00101110

Tabel 2. Nilai Biner Kunci

No	Kunci	ASCII	Nilai Biner
1	u	117	1110101
2	n	110	1101110
3	n	110	1101110
4	e	101	1100101
5	s	115	1110011

Penyisipan Dengan LSB Standar

Hasil pengujian algoritma LSB standar dihitung menggunakan nilai MSE dan PSNR. Nilai MSE dan PSNR digunakan untuk mengukur kesamaan dan *error* yang terjadi pada suatu citra digital setelah melewati proses *image processing*. MSE adalah akar kumulatif nilai *error* antara gambar yang mengandung pesan dengan gambar asli. Pada citra RGB nilai MSE dihitung dengan menjumlahkan nilai MSE masing-masing komponen *Red*, *Green*, dan *Blue* dibagi tiga. Sementara PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR dinyatakan dalam satuan 34ecibel (dB). Rekapitulasi hasil pengujian MSE sebelum modifikasi dapat dilihat pada Tabel 3, sedangkan untuk nilai PSNR dapat dilihat pada Tabel 4.

Tabel 3. Nilai MSE LSB Standar

Gambar	Kunci	MSE			
		Red	Green	Blue	Average
<i>White</i>	unnes	0.005957	0.005121	0.0027	0.004579
<i>Black</i>	unnes	0.004256	0.00498	0.0043	0.004499
<i>Airplane</i>	unnes	0.727528	0.335185	0.3616	0.474783
<i>Artichare</i>	unnes	0.001079	0.000993	0.0008	0.000944
<i>Baboon</i>	unnes	0.245038	0.435162	0.2352	0.305131
<i>Lena</i>	unnes	0.211516	0.913144	0.831	0.651892
<i>Monarch</i>	unnes	0.045931	0.360575	0.3364	0.24764
<i>Peppers</i>	unnes	0.060146	0.191573	0.5194	0.257044
		Rata-rata			0.243314077

Tabel 4. Nilai PSNR LSB Standar

Gambar	Kunci	PSNR (dB)			
		Red	Green	Blue	Average
<i>White</i>	unnes	109.34	110.109	115.42	111.6243
<i>Black</i>	unnes	69.8923	74.6514	74.153	72.89887
<i>Airplane</i>	unnes	57.1985	66.1535	65.578	62.9767
<i>Arctichare</i>	unnes	128.25	126.67	129.12	128.0147
<i>Baboon</i>	unnes	69.1434	62.5185	83.151	71.6043
<i>Lena</i>	unnes	70.0197	57.7112	59.146	62.29237
<i>Monarch</i>	unnes	85.9562	65.664	66.424	72.68137
<i>Peppers</i>	unnes	85.5247	74.3516	60.995	73.62383
		Rata-rata			81.96455

Penyisipan dengan Advanced LSB

Rekapitulasi hasil pengujian nilai MSE *Advanced* LSB dapat dilihat pada Tabel 5, sedangkan untuk hasil pengujian nilai PSNR *Advanced* LSB dapat dilihat pada Tabel 6.

Tabel 5. Nilai MSE *Advanced* LSB

Gambar	Kata Kunci	MSE			
		Red	Green	Blue	Average
white	unnes	0.003357	0.00316	0.002106	0.00287374
black	unnes	0.002274	0.00270	0.002426	0.00246684
airplane	unnes	0.625378	0.26389	0.261097	0.38345333
arctichare	unnes	0.000572	0.00070	0.000551	0.00060746
baboon	unnes	0.195038	0.36936	0.053459	0.20595307
lena	unnes	0.171906	0.69379	0.531033	0.46557767
monarch	unnes	0.036936	0.29050	0.276594	0.20134413
peppers	unnes	0.040234	0.13517	0.499214	0.22487253
		Rata-rata			0.185893597

Tabel 6. Nilai PSNR *Advanced* LSB

Gambar	Kata Kunci	PSNR (dB)			
		Red	Green	Blue	Average
white	unnes	109.34	110.109	115.424	111.6243
black	unnes	69.8923	74.6514	74.1529	72.89887
airplane	unnes	57.1985	66.1535	65.5781	62.9767
arctichare	unnes	128.25	126.67	129.124	128.0147
baboon	unnes	69.1434	62.5185	83.151	71.6043
lena	unnes	70.0197	57.7112	59.1462	62.29237
monarch	unnes	85.9562	65.664	66.4239	72.68137
peppers	unnes	85.5247	74.3516	60.9952	73.62383
		Rata-rata			83.81517

Dari Tabel 5 nilai MSE rata-rata delapan citra menggunakan *advanced* LSB yaitu 0.1859 dan pada Tabel 6 untuk nilai PSNR rata-rata menggunakan *advanced* LSB yaitu 83.8151 dB.

Analisis Hasil

Untuk mendapatkan hasil yang lebih detail, hasil akhir dari masing-masing metode pada algoritma 1 dan algoritma 2 dibandingkan satu sama lain. Hasil perbandingan MSE masing-masing algoritma ditunjukkan pada Tabel 7 dan hasil perbandingan PSNR metode pengujian untuk masing-masing algoritma ditunjukkan pada Tabel 8.

Tabel 7. Perbandingan Nilai MSE

MSE	Standard	<i>Advanced</i>
white	0.00457917	0.002873737
black	0.004499253	0.00246684
airplane	0.474783333	0.383453333
artichare	0.000943643	0.000607464
baboon	0.305130667	0.205953067
lena	0.651891733	0.465577667
monarch	0.24764048	0.201344133
peppers	0.257044333	0.224872533
average	0.243314077	0.185893597

Tabel 8. Perbandingan Nilai PSNR

PSNR	Standard (dB)	<i>Advanced</i> (dB)
white	111.6243	114.1377
black	72.89887	74.46517
airplane	62.9767	65.32053
artichare	128.0147	129.53
baboon	71.6043	73.6858
lena	62.29237	64.49133
monarch	72.68137	74.38047
peppers	73.62383	74.51037
Average	81.96455	83.81517

SIMPULAN

Hasil akhir dari masing-masing metode pengujian menggunakan LSB standar dan *Advanced* LSB dibandingkan untuk mendapatkan hasil perbandingan yang detail dari masing-masing metode. Untuk perbandingan kedua metode yang digunakan dapat disimpulkan bahwa *Advanced* LSB memiliki nilai MSE yang lebih baik 0.185893597 dari pada LSB standar 0.243314077, dan untuk nilai PSNR 83.81517 dB terhadap 81.96455 dB.

DAFTAR PUSTAKA

- Alamsyah, Budi, P., & Ardian, M. N. (2020). Enhancement security AES algorithm using a modification of transformation shiftrows and dynamic S-Box. *Journal of Physics Conference Series*, 1567(3), 032025
- Almazaydeh, L. (2020). Secure RGB image steganography based on modified LSB substitution. *International Journal of Embedded Systems*, 12(4), 453-457
- Arya, A., Soni, S. (2018). A literature review on various recent steganography techniques. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4(1), 143-149.
- Chen, S.-K. (2011). A module-based LSB substitution method with lossless secret data compression. *Computer Standards & Interfaces*, 33(1).
- Fadlil, A., Prasetyo, B., Alamsyah (2021). Increasing message capacity in images using advanced least. *Scientific Journal of Informatics*, 892), 268-274

- Hassaballah, M. (2020). *Digital media steganography*. eBook ISBN: 9780128194393: Elsevier
- Kekre, H.B., Mishra, D., Khanna, R., Khanna, S., & Hussaini, A. (2012). Comparison between the basic LSB replacement technique and increased capacity of information hiding in LSB's method for images. *International Journal of Computer Application*, 45(1), 33-38.
- Langi, A. Z. (2013). Lossless compression performance of a simple counter-based entropy coder. *Journal of ICT Research and Applications*, 5(3), 173-184.
- Lemire, D. A. (2010). Introduction to the special issue on learning and the social web. *Journal of Emerging Technologies in Web Intelligence*, 2(1), 1-2
- Morkel, T., Eloff, J.H.P., & Olivier, M.S. (2005). An overview of image steganography. Conference: Proceedings of the ISSA 2005 New Knowledge Today Conference, 29 June - 1 July 2005, Balalaika Hotel, Sandton, South Africa.
- Nasution, S.B., Hidayat, B., & Ramatryana, I.N.A. (2017). Steganalisis citra digital berbasis Discrete Cosine Transform dengan menggunakan metode K-Nearest Neighbor. *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri*, Book-1.
- Odat, A., & Otair, M. (2016). Image steganography using modified Least Significant Bit. *Indian Journal of Science and Technology*, 9(39), 1-5.
- Yosanny, A. (2010). Perancangan enkripsi pada citra Bitmap dengan Algoritma Des, Triple Des, dan Idea. *Comtech: Computer, Mathematics And Engineering Applications*, 1(2), 853-866.