JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

Penyisipan Pesan pada Citra Digital Menggunakan Kombinasi LSB dan Blum Blum Shub

Soeb Arifin

Teknik Informatika, Fakultas Ilmu Komputer & Teknologi Informasi, Universitas Budi Darma,Medan,Indonesia
Email: suefarifin@gmail.com
Email Penulis Korespondensi: suefarifin@gmail.com

Abstrak− Penyisipan pesan melalui steganografi citra digital bertujuan menyembunyikan keberadaan informasi tanpa menghasilkan perubahan visual yang mudah dikenali. Metode Least Significant Bit (LSB) memiliki implementasi sederhana, tetapi penyisipan pada lokasi berurutan dapat membentuk pola yang dapat diprediksi. Penelitian ini mengevaluasi kombinasi LSB dan generator Blum Blum Shub (BBS) untuk menentukan lokasi penyisipan secara pseudorandom, tanpa menambahkan algoritma enkripsi isi pesan. Pengujian menggunakan lima citra RGB sintetis berukuran 512 × 512 piksel dalam format PNG dan tiga ukuran pesan, yaitu 100, 500, dan 1.000 byte, sehingga diperoleh 15 skenario. Panjang pesan disimpan dalam header 32 bit; BBS membangkitkan indeks komponen warna yang unik dan LSB digunakan untuk mengganti satu bit pada setiap komponen terpilih. Kualitas citra diukur dengan Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), persentase perubahan komponen, dan keberhasilan ekstraksi. Rata-rata PSNR berturut-turut mencapai 80,94 dB, 74,09 dB, dan 71,11 dB; seluruh skenario berhasil diekstraksi ketika parameter BBS sesuai. Pengujian dengan seed berbeda pada pesan 1.000 byte menghasilkan bit error rate 49,86%. Hasil menunjukkan bahwa pengacakan lokasi dapat diterapkan dengan distorsi rendah pada citra sintetis, tetapi belum membuktikan ketahanan terhadap steganalisis maupun manipulasi citra.

Kata Kunci: Steganografi; Least Significant Bit; Blum Blum Shub; Citra Digital; Pengacakan Lokasi

Abstract− Digital image steganography aims to conceal the existence of information while minimizing perceptible changes to the cover image. Least Significant Bit (LSB) embedding is straightforward to implement; however, sequential embedding positions may produce predictable patterns. This study evaluates a combination of LSB and the Blum Blum Shub (BBS) generator for pseudorandom selection of embedding locations without incorporating message encryption. Five synthetic RGB images measuring 512 × 512 pixels in PNG format were tested with message sizes of 100, 500, and 1,000 bytes, resulting in 15 experimental scenarios. Message length was encoded in a 32-bit header; BBS generated unique color-component indices, while LSB replacement inserted one bit at each selected position. Image quality was assessed using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), percentage of modified components, and extraction success. Mean PSNR values were 80.94 dB, 74.09 dB, and 71.11 dB for the three payload sizes, respectively. All scenarios recovered the embedded messages correctly when the BBS parameters matched. A different extraction seed produced a bit error rate of 49.86% for the 1,000-byte message. The findings indicate that randomized embedding positions can be implemented with low distortion in synthetic images. Nevertheless, these findings do not establish resistance to steganalysis, lossy manipulation, or generalization to standard photographic datasets.

Keywords: Steganography; Least Significant Bit; Blum Blum Shub; Digital Image; Random Embedding

1. PENDAHULUAN

Pertukaran pesan dalam media digital menghadirkan dua persoalan yang berbeda, yaitu bagaimana melindungi isi informasi dan bagaimana menyembunyikan fakta bahwa informasi tersebut sedang dikirim. Kriptografi berfokus pada kerahasiaan isi dengan mengubah representasi pesan, sedangkan steganografi berupaya menyamarkan keberadaan pesan pada suatu media penampung. Citra digital merupakan media penampung yang relevan karena mengandung banyak sampel warna dan dapat dimodifikasi secara terbatas tanpa perubahan visual yang jelas. Literatur mengidentifikasi kapasitas muatan, ketakterlihatan perubahan, ketahanan, dan risiko deteksi sebagai dimensi evaluasi yang saling berkaitan [1], [2], [16]. Salah satu metode domain spasial yang sering digunakan adalah Least Significant Bit (LSB), yakni mengganti bit terendah nilai komponen piksel dengan bit pesan. Pada citra RGB delapan bit per kanal, perubahan satu bit terendah hanya menyebabkan perubahan intensitas sebesar nol atau satu. Keunggulan ini membuat implementasi LSB efisien dan biasanya menghasilkan galat kuadrat rata-rata yang rendah, khususnya ketika rasio muatan terhadap kapasitas citra kecil. Namun, penyisipan berurutan berpotensi menghasilkan lokasi modifikasi yang terstruktur dan memudahkan pihak lain menyusun hipotesis tentang letak pesan. Karena itu, penentuan lokasi embedding menjadi persoalan metodologis di samping pilihan teknik penggantian bit [3], [10], [12].

Penelitian terkini menawarkan beragam cara untuk mengurangi keteraturan lokasi penyisipan. Yanuar dkk. [3] menggunakan permutasi Josephus bersama skema LSB 3-3-2; Khalil dkk. [4] memanfaatkan chaotic maps untuk pemilihan lokasi; dan Molato dkk. [13] mengembangkan pemetaan acak berdasarkan modifikasi dugaan Collatz. Penelitian tentang penggunaan pseudo-random number generator (PRNG) pada citra berwarna juga memperlihatkan pentingnya pembangkit posisi dalam proses penyisipan [14]. Penelitian 2025 mengenai

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

pengacakan piksel dan hash LSB [17], serta teknik penyisipan acak berbasis segmentasi dan deteksi tepi [20], menunjukkan bahwa pengaturan lokasi tetap menjadi tema yang aktif. Blum Blum Shub (BBS) adalah pembangkit pseudorandom berdasarkan operasi kuadrat modular. Jika parameter primanya dan seed telah ditentukan, urutan hasilnya deterministik sehingga dapat direproduksi untuk ekstraksi. Nurdiansyah [5] memadukan ElGamal, LSB, dan BBS; Ardhiansyah [8] mengkombinasikan Vigenère Cipher, LSB, dan BBS; sedangkan Sina dkk. [11] menggunakan Triple DES bersama LSB dan BBS.

Penelitian tersebut memperlihatkan kegunaan BBS sebagai mekanisme pengacakan, tetapi karena digabungkan dengan enkripsi, pengaruh pengacakan posisi terhadap kualitas stego-image tidak selalu dibahas terpisah. Posisi penelitian ini bukan mengklaim BBS sebagai pembangkit baru, melainkan menyajikan pengujian terkontrol kombinasi LSB–BBS tanpa enkripsi tambahan. Kajian lain menunjukkan bahwa tujuan evaluasi dapat berbeda antarpenelitian. Alanzy dkk. [6] membahas kombinasi LSB dengan enkripsi hibrida, sedangkan Fahmi dkk. [7] menelaah Vigenère termodifikasi dan LSB. Al-Faydi dkk. [10] menitikberatkan ketakterlihatan dengan pencocokan cover–stego; Rustad dkk. [12] mengkaji adaptasi pola LSB. Penelitian 2024 membandingkan kualitas DCT dan LSB berdasarkan RMSE serta PSNR [19], sementara DualLSBStego pada 2025 melaporkan pengujian domain spasial pada dataset gambar standar [18]. Perbedaan konteks, ukuran muatan, dan media uji tersebut mengharuskan hasil antarmetode dibaca secara hati-hati; nilai PSNR yang lebih besar pada penelitian ini bukan bukti otomatis bahwa metode yang digunakan lebih unggul. Berdasarkan penelitian terdahulu, celah yang difokuskan pada artikel ini adalah dokumentasi terukur mengenai perilaku pengacakan posisi LSB–BBS dengan variasi ukuran pesan dan sensitivitas parameter ekstraksi dalam satu desain uji yang konsisten.

Tujuan penelitian adalah menerapkan generator BBS untuk pemilihan indeks komponen warna unik, mengukur perubahan kualitas citra pada tiga panjang pesan, serta mengevaluasi keberhasilan ekstraksi dengan parameter sama dan berbeda. Kontribusi artikel dibatasi pada verifikasi implementasi dan analisis distorsi pada citra RGB sintetis; hasil tidak dapat dianggap sebagai pembuktian keamanan steganografi terhadap serangan aktif maupun steganalisis statistik.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian dilakukan melalui identifikasi persoalan prediktabilitas lokasi LSB, kajian penelitian terkait, penyiapan citra dan pesan, pembangkitan posisi BBS, penyisipan bit, ekstraksi, pengukuran kualitas, dan interpretasi hasil. Alur tahapan diperlihatkan pada Gambar 1. Tahapan pengujian menggunakan rancangan deterministik sehingga parameter yang sama akan menghasilkan urutan posisi yang sama. Fokusnya adalah pemeriksaan kualitas keluaran pada kombinasi yang ditentukan, bukan pencarian parameter optimal.



Gambar 1. Tahapan penelitian penyisipan dan ekstraksi LSB–BBS

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

2.2 Data Uji dan Kapasitas

Data uji terdiri atas lima citra sintetis RGB 512 × 512 piksel yang disimpan sebagai PNG dan tiga variasi muatan teks/byte. Pemilihan citra sintetis bertujuan memverifikasi prosedur secara terkendali, bukan menggantikan pengujian pada citra fotografi standar. Dengan tiga kanal dan satu bit per komponen, kapasitas teoretis per citra adalah 512 × 512 × 3 = 786.432 bit atau 98.304 byte sebelum alokasi header dan batasan pengacakan. Header sepanjang 32 bit menampung panjang pesan sehingga proses ekstraksi mengetahui jumlah byte yang perlu diambil.

Tabel 1. Spesifikasi data dan pengujian

Komponen	Spesifikasi
Citra penampung	5 citra RGB sintetis, 512 × 512 piksel, PNG
Panjang pesan	100, 500, dan 1.000 byte
Kapasitas teoretis	786.432 bit (98.304 byte), sebelum header
Header panjang pesan	32 bit
Jumlah skenario	5 citra × 3 ukuran pesan = 15

2.3 Pembangkitan Lokasi dengan Blum Blum Shub

Generator BBS menggunakan dua bilangan prima p dan q yang masing-masing kongruen dengan 3 modulo 4; modulus ditentukan oleh $n = p \times q$. Seed s dipilih relatif prima terhadap n. Keadaan awal dihitung dari $x_0 = s^2 \bmod n$ dan keadaan berikutnya dengan $x_{i+1} = x_i^2 \bmod n$. Pada pengujian digunakan p = 1.000.003, q = 1.000.039, n = 1.000.042.000.117, dan s = 123.457. Nilai keadaan dipetakan ke indeks komponen citra melalui $x_i \bmod 786.432$. Indeks berulang ditolak hingga jumlah posisi unik sama dengan total bit yang disisipkan.

Pemilihan indeks unik penting agar sebuah lokasi tidak ditimpa dua kali sehingga rekonstruksi bit berlangsung sesuai urutan pembangkitan. Di sisi penerima, kecocokan nilai p, q, seed, aturan pengambilan indeks, serta format header merupakan syarat rekonstruksi. Parameter BBS pada studi ini berfungsi untuk menjaga konsistensi eksperimen. Penelitian tidak melakukan audit kriptografis atas ukuran modulus, manajemen seed, atau ancaman pengungkapan parameter; oleh sebab itu istilah “pseudorandom” di sini menjelaskan metode pemilihan posisi dan bukan klaim keamanan sistem secara menyeluruh.

2.4 Prosedur Penyisipan dan Ekstraksi

Pada penyisipan, pesan dikonversi menjadi deret byte dan bit; panjang pesan direpresentasikan sebagai header 32 bit. Generator BBS membangkitkan posisi unik untuk seluruh bit header dan pesan. Bit terendah setiap komponen warna yang terpilih diganti dengan bit muatan, dan hasil disimpan pada PNG agar nilai LSB tetap terjaga. Sebaliknya, ekstraksi membangkitkan kembali 32 posisi awal, membaca header, kemudian memperoleh posisi lanjutan sesuai panjang pesan dan mengelompokkan bit yang ditemukan menjadi byte. Hasil rekonstruksi dibandingkan dengan byte pesan asli secara langsung.

Satu hal penting dalam desain ini adalah keterkaitan header dan seed. Apabila seed yang berbeda dipakai untuk membaca header, panjang yang terdekode dapat berubah sehingga tahap ekstraksi berikutnya juga kehilangan sinkronisasi. Oleh karena itu, keberhasilan ekstraksi dengan seed benar dievaluasi terpisah dari sensitivitas bit terhadap seed lain. Angka bit error rate yang dilaporkan merupakan hasil pengujian khusus pada pesan 1.000 byte dan tidak dengan sendirinya menjelaskan semua perilaku header atau seluruh kemungkinan seed.

2.5 Metrik Evaluasi

Penelitian menggunakan Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), dan Structural Similarity Index Measure (SSIM) untuk mengukur kemiripan antara citra penampung dan stego-image. MSE menghitung rerata kuadrat selisih sampel; pada citra delapan bit, PSNR dinyatakan sebagai $10 \log_{10}(255^2/\mathrm{MSE})$. SSIM mengukur kemiripan struktur dan mendekati nilai satu untuk citra yang serupa. Persentase komponen berubah dihitung relatif terhadap keseluruhan komponen warna citra, sedangkan keberhasilan ekstraksi dinilai berdasarkan kecocokan pesan hasil ekstraksi dengan pesan awal.

Setiap kombinasi citra dan panjang pesan menghasilkan satu observasi sehingga terdapat 15 observasi. Rata-rata per panjang pesan merupakan rerata lima citra untuk masing-masing muatan. Penelitian juga melaporkan bit error rate sebesar 49,86% pada pengujian seed berbeda. Tidak tersedia hasil pembanding LSB berurutan, pengukuran waktu proses, uji serangan JPEG, cropping, resizing, maupun pengujian steganalisis; metrik tersebut tidak ditafsirkan seolah-olah telah diuji.

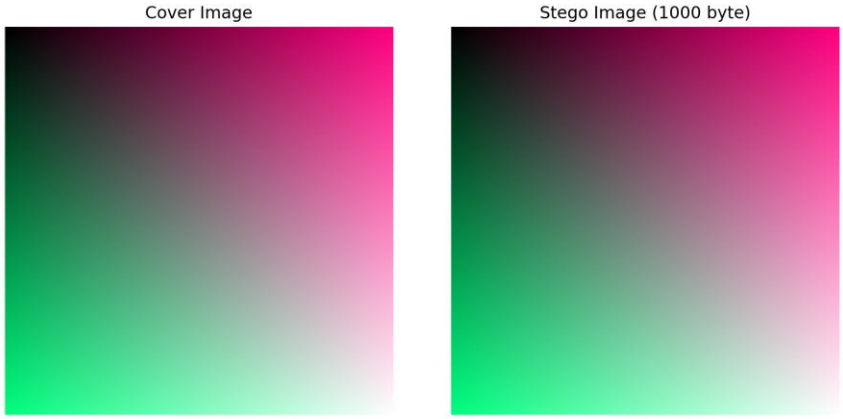
Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penyisipan dan Ekstraksi

Kelima citra sintetis berhasil digunakan sebagai media penampung untuk pesan 100, 500, dan 1.000 byte. Hasil laporan menunjukkan bahwa seluruh 15 skenario menghasilkan pesan ekstraksi yang identik ketika parameter BBS pada proses penyisipan dan pembacaan sama. Temuan ini menegaskan kebenaran operasional prosedur pembangkitan ulang posisi dan pembacaan LSB pada konfigurasi yang diuji. Kesimpulan keberhasilan di sini berkaitan dengan pemulihan data pada file PNG yang tidak mengalami pengolahan tambahan; pernyataan tersebut tidak mencakup pengujian setelah citra dikompresi, diubah ukurannya, atau diedit.



Gambar 2. Contoh perbandingan cover-image dan stego-image pada muatan 1.000 byte

Gambar 2 menampilkan salah satu pasangan citra penampung dan hasil penyisipan. Secara visual, keduanya tampak serupa pada skala tampilan dokumen. Perbandingan visual tidak menggantikan pengukuran numerik; evaluasi kuantitatif yang relevan ditunjukkan pada Tabel 2 dan Tabel 3. Kecilnya perubahan pada komponen RGB sejalan dengan sifat penggantian satu LSB, tetapi tingkat ketakterdeteksian oleh alat steganalisis tidak dapat dinyatakan hanya berdasarkan pengamatan visual.

3.2 Pengaruh Panjang Pesan terhadap Kualitas Citra

Tabel 2 memperlihatkan keseluruhan hasil pengujian yang dilaporkan. Terdapat pola penurunan PSNR ketika pesan bertambah panjang pada setiap citra. Pada citra C1, misalnya, PSNR turun dari 80,62 dB pada 100 byte menjadi 74,07 dB pada 500 byte dan 71,09 dB pada 1.000 byte. Pola serupa muncul pada C2 hingga C5. MSE meningkat karena lebih banyak komponen berpeluang berubah untuk menampung bit baru. Dengan kapasitas teoretis yang jauh melampaui panjang muatan, proporsi penggantian bit yang benar-benar mengubah intensitas tetap kecil.

Tabel 2. Hasil pengujian 15 skenario

Citra	Pesan (byte)	MSE	PSNR (dB)	SSIM	Perubahan	Ekstraksi
C1	100	0.000563	80.62	0.999991	0.0563%	Berhasil
C1	500	0.002547	74.07	0.999958	0.2547%	Berhasil
C1	1000	0.005054	71.09	0.999916	0.5054%	Berhasil
C2	100	0.000498	81.15	0.999996	0.0498%	Berhasil
C2	500	0.002468	74.21	0.999981	0.2468%	Berhasil
C2	1000	0.005030	71.11	0.999962	0.5030%	Berhasil
C3	100	0.000470	81.41	0.999994	0.0470%	Berhasil
C3	500	0.002322	74.47	0.999972	0.2322%	Berhasil
C3	1000	0.004627	71.48	0.999946	0.4627%	Berhasil
C4	100	0.000526	80.92	0.999991	0.0526%	Berhasil
C4	500	0.002622	73.94	0.999956	0.2622%	Berhasil
C4	1000	0.005205	70.97	0.999913	0.5205%	Berhasil
C5	100	0.000568	80.58	0.999992	0.0568%	Berhasil
C5	500	0.002725	73.78	0.999959	0.2725%	Berhasil
C5	1000	0.005319	70.87	0.999920	0.5319%	Berhasil

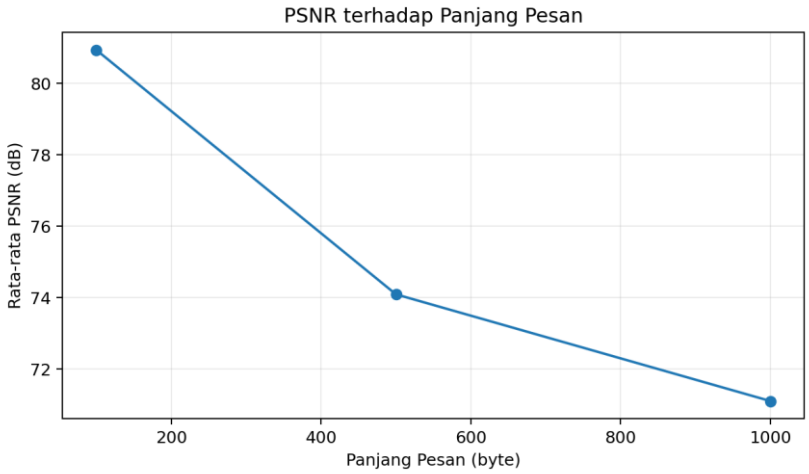
Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

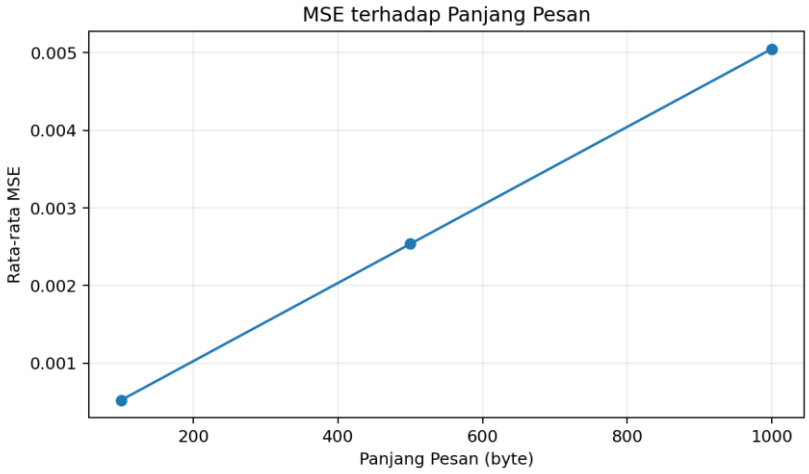
Ringkasan pada Tabel 3 memperlihatkan kenaikan MSE rata-rata dari 0,000525 ke 0,002537, lalu ke 0,005047. Pada saat yang sama, PSNR rata-rata turun dari 80,94 dB menjadi 74,09 dB dan 71,11 dB. Persentase komponen yang berubah meningkat dari 0,0525% menjadi 0,2537% dan 0,5047%. Secara mekanistis, bertambahnya panjang pesan memperbesar jumlah lokasi yang ditulisi dan karena itu meningkatkan frekuensi perubahan komponen. Tidak semua operasi penulisan LSB menimbulkan perubahan nilai, sebab bit pesan yang sama dengan LSB awal tidak mengubah intensitas.

Tabel 3. Rata-rata hasil berdasarkan panjang pesan

Pesan (byte)	MSE	PSNR (dB)	SSIM	Perubahan	Keberhasilan
100	0.000525	80.94	0.999993	0.0525%	100%
500	0.002537	74.09	0.999965	0.2537%	100%
1000	0.005047	71.11	0.999932	0.5047%	100%



Gambar 3. Rata-rata PSNR terhadap panjang pesan



Gambar 4. Rata-rata MSE terhadap panjang pesan

Gambar 3 dan Gambar 4 memperjelas hubungan berlawanan antara PSNR dan MSE pada tingkat muatan yang meningkat. Dengan tetapnya rentang intensitas maksimum, PSNR merupakan transformasi logaritmik dari MSE sehingga kedua metrik tidak boleh dianggap sebagai indikator yang independen. Selisih PSNR antara muatan terkecil dan terbesar sekitar 9,83 dB berdasarkan nilai rata-rata yang dilaporkan. Angka ini tidak dapat diekstrapolasi secara linear ke ukuran pesan di luar 100–1.000 byte, karena hubungan perubahan LSB dan distribusi nilai komponen dapat bergantung pada jenis citra serta isi pesan.

Nilai SSIM rata-rata berturut-turut sebesar 0,999993, 0,999965, dan 0,999932 mengindikasikan bahwa pola struktural citra sintetis tetap mendekati citra asal untuk setiap variasi muatan. Di seluruh pengamatan, SSIM berkisar 0,999913–0,999996, sedangkan PSNR berkisar 70,87–81,41 dB. Nilai tersebut perlu dipahami sesuai kondisi pengujian, yakni citra sintetis dengan perubahan satu bit, penyimpanan lossless, serta muatan relatif

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

rendah. Citra fotografi bertekstur kompleks, kompresi berbeda, dan pemilihan muatan adaptif dapat menghasilkan karakteristik yang berbeda.

3.3 Konsistensi Hasil Antarcitra

Terdapat variasi kecil antarcitra pada panjang pesan yang sama. Untuk muatan 1.000 byte, PSNR C1–C5 berturut-turut adalah 71,09; 71,11; 71,48; 70,97; dan 70,87 dB. C3 menghasilkan PSNR tertinggi, sementara C5 terendah pada kelompok tersebut. Perbedaan tersebut sejalan dengan variasi jumlah komponen yang nilainya benar-benar berubah setelah penulisan LSB. Penelitian tidak menyediakan analisis distribusi intensitas atau karakteristik tekstur kelima citra, sehingga penyebab rinci perbedaan antarcitra tidak dapat dipastikan.

Citra C3 juga menunjukkan MSE paling kecil pada muatan 1.000 byte, yaitu 0,004627; C5 memiliki MSE terbesar, yaitu 0,005319. Pada seluruh citra, hasil ekstraksi dengan parameter benar tetap berhasil meskipun nilai distorsi sedikit berbeda. Ini menunjukkan bahwa keberhasilan pemulihan pesan dan besarnya gangguan visual merupakan dua keluaran evaluasi yang tidak identik. Sebuah metode dapat mengekstraksi pesan dengan baik, tetapi tetap menghasilkan citra yang lebih mudah terdeteksi oleh analisis statistik; pengujian yang tersedia belum menilai aspek kedua tersebut secara langsung.

3.4 Sensitivitas Seed dan Batas Interpretasi Keamanan

Pada pengujian sensitivitas dengan panjang pesan 1.000 byte, laporan mencatat bit error rate (BER) sebesar 49,86% ketika seed untuk pembacaan berbeda dari seed yang digunakan pada penyisipan. Proporsi kesalahan yang mendekati separuh bit menunjukkan bahwa urutan lokasi yang dibangkitkan dari seed berbeda tidak menghasilkan pembacaan bit pesan yang sesuai pada pengujian itu. Kondisi tersebut mendukung persyaratan sinkronisasi seed dan parameter BBS antara pengirim dan penerima. Namun, nilai BER dari satu konfigurasi tidak dapat langsung dianggap sebagai bukti keamanan kriptografis atau ukuran ketahanan sistem terhadap penyerang.

BBS menentukan pemilihan posisi, bukan menyandikan isi pesan. Jika seed atau daftar posisi berhasil diperoleh, bit yang tersembunyi dapat dibaca tanpa harus mendekripsi isi. Selanjutnya, sifat pseudorandom pembangkit perlu dibedakan dari kualitas keamanan penerapannya: keselamatan sistem juga dipengaruhi pemilihan parameter, pertukaran seed, penanganan header, dan kemampuan deteksi terhadap perubahan statistik. Literatur tentang penggunaan kriptografi bersama LSB [5], [6], [8], [11], [17] relevan sebagai rute pengembangan, tetapi penelitian ini secara sengaja tidak menguji lapisan enkripsi.

3.5 Perbandingan dengan Penelitian Terdahulu

Kombinasi LSB–BBS dalam studi ini berkaitan paling langsung dengan karya Nurdiansyah [5], Ardhiansyah [8], dan Sina dkk. [11], yang menggunakan BBS bersama teknik steganografi dan algoritma sandi. Perbedaan pokoknya terletak pada pembatasan variabel: penelitian ini menggunakan LSB sebagai satu-satunya teknik modifikasi pesan dan BBS sebagai pembangkit lokasi, lalu mengukur MSE, PSNR, SSIM, tingkat perubahan, keberhasilan pemulihan, dan kepekaan seed. Dengan demikian, kontribusinya berupa pemisahan aspek pemilihan lokasi dari efek enkripsi tambahan, bukan penemuan konstruksi baru atau bukti performa lebih tinggi terhadap penelitian lain.

Pendekatan acak lain meliputi permutasi Josephus [3], chaotic maps [4], modifikasi Collatz [13], serta PRNG dan pemilihan piksel berbasis tepi [14], [20]. Komparasi yang adil memerlukan citra uji yang sama, payload identik, format penyimpanan seragam, dan ukuran keberhasilan yang setara. Studi LSB–BBS ini belum menjalankan eksperimen head-to-head sehingga tidak dapat menyimpulkan bahwa BBS mengungguli generator lain. Publikasi 2025 yang menggunakan pemilihan lokasi secara dinamis [17] maupun DualLSBStego [18] dapat dijadikan pembanding metode untuk rancangan lanjutan, bukan sebagai data pembanding yang telah dihasilkan pada eksperimen ini.

Aspek steganalisis juga perlu dipertimbangkan. Tinjauan Kombrink dkk. [16] membedakan metode penyembunyian dari strategi deteksi pesan tersembunyi. Nilai PSNR dan SSIM hanya menerangkan kemiripan citra, bukan probabilitas serangan steganalisis berhasil. Oleh karena itu, pelaporan kualitas citra yang baik perlu diikuti pemeriksaan statistik, perbandingan dengan baseline LSB berurutan, dan eksperimen terhadap manipulasi berkas sebelum klaim keamanan diperluas. Pembacaan demikian mencegah interpretasi berlebihan terhadap tingginya PSNR pada citra sintetis.

3.6 Keterbatasan dan Implikasi Penelitian

Keterbatasan utama penelitian adalah penggunaan lima citra sintetis sehingga temuan belum dapat digeneralisasi pada dataset citra fotografi standar. Kedua, tiga panjang pesan masih mewakili rasio muatan yang rendah dibandingkan kapasitas teoretis. Ketiga, tidak ada evaluasi baseline LSB sekuensial, generator acak alternatif, analisis waktu komputasi, uji steganalisis, maupun uji ketahanan terhadap modifikasi berkas. Keempat, pelaporan

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

sensitivitas seed terbatas pada hasil BER yang tersedia; penelitian belum menyajikan pengujian variasi seed dalam jumlah besar. Keterbatasan ini terutama berkaitan dengan kekuatan bukti ilmiah, bukan menghilangkan kegunaan pengujian implementasi yang telah dilakukan.

Secara praktis, rancangan yang dievaluasi lebih tepat digunakan untuk penyisipan pesan pada skenario yang mempertahankan integritas citra PNG. Mengonversi hasil ke JPEG, melakukan cropping, resizing, filtering, atau mengubah kanal warna berpotensi mengubah lokasi dan nilai bit terendah sehingga pesan tidak dapat dipulihkan. Untuk pengembangan berikutnya, diperlukan set data terstandar, pengujian terhadap beberapa tingkat kapasitas, pembandingan generator posisi pada citra sama, evaluasi steganalisis, serta manajemen kunci dan enkripsi pesan apabila target penelitian bergeser dari pengacakan lokasi menuju perlindungan kerahasiaan isi.

4. KESIMPULAN

Penelitian ini mengevaluasi penerapan gabungan Least Significant Bit (LSB) dan Blum Blum Shub (BBS) untuk menyisipkan pesan pada citra digital RGB. BBS digunakan untuk membentuk urutan posisi komponen warna secara pseudorandom, sedangkan LSB mengganti satu bit pada posisi yang terpilih. Berdasarkan lima citra sintetis berukuran 512 × 512 piksel dan tiga variasi pesan, seluruh 15 skenario berhasil mengekstraksi pesan secara identik ketika parameter pembangkit dipertahankan. Hasil tersebut membuktikan konsistensi implementasi dalam batas kondisi pengujian, khususnya penggunaan citra PNG tanpa manipulasi lanjutan. Nilai PSNR rata-rata tercatat 80,94 dB untuk 100 byte, 74,09 dB untuk 500 byte, dan 71,11 dB untuk 1.000 byte; SSIM rata-rata tetap melebihi 0,9999. Dengan bertambahnya muatan, MSE dan persentase komponen warna yang berubah meningkat, selaras dengan mekanisme substitusi satu bit. Penggunaan seed berbeda pada uji 1.000 byte menghasilkan BER sebesar 49,86%, yang menegaskan kebutuhan kesesuaian parameter ketika membaca pesan. Walaupun pengacakan posisi mengurangi keteraturan lokasi penyisipan, penelitian tidak mengenkripsi isi pesan dan belum mengevaluasi keamanan terhadap steganalisis maupun ketahanan terhadap kompresi lossy, pemotongan, dan perubahan ukuran citra. Penelitian lanjutan disarankan menggunakan dataset fotografi standar, pengujian payload lebih luas, baseline LSB berurutan dan pembangkit alternatif, serta evaluasi serangan dan biaya komputasi agar kontribusi metode dapat dibandingkan secara lebih kuat.

REFERENCES

[1] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “Image Steganography: A Review of the Recent Advances,” IEEE Access, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[2] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, “Digital image steganography: A literature survey,” Information Sciences, vol. 609, pp. 1451–1488, 2022, doi: 10.1016/j.ins.2022.07.120.

[3] M. R. Yanuar, S. MT, C. Apriono, and M. F. Syawaludin, “Image-to-Image Steganography with Josephus Permutation and Least Significant Bit (LSB) 3-3-2 Embedding,” Applied Sciences, vol. 14, no. 16, art. 7119, 2024, doi: 10.3390/app14167119.

[4] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, “A secure image steganography based on LSB technique and 2D chaotic maps,” Computers & Electrical Engineering, vol. 119, Part B, art. 109566, 2024, doi: 10.1016/j.compeleceng.2024.109566.

[5] M. F. Nurdiansyah, “Implementasi Kriptografi ElGamal dan Steganografi Kombinasi Least Significant Bit dan Blum Blum Shub untuk Pengamanan Pesan Rahasia dalam Gambar,” Skripsi S1, Universitas Pendidikan Indonesia, 2024.

[6] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, “Image Steganography Using LSB and Hybrid Encryption Algorithms,” Applied Sciences, vol. 13, no. 21, art. 11771, 2023, doi: 10.3390/app132111771.

[7] G. M. Fahmi, K. N. Isnaini, and D. Suhartono, “Implementation of Steganography on Digital Image with Modified Vigenere Cipher Algorithm and Least Significant Bit (LSB) Method,” Jurnal Teknik Informatika (JUTIF), vol. 4, no. 2, pp. 333–344, 2023, doi: 10.52436/1.jutif.2023.4.2.340.

[8] R. F. Ardhiansyah, “Implementasi Steganografi Kombinasi Least Significant Bit dan Blum Blum Shub dengan Kriptografi Vigènere Cipher untuk Penyisipan Pesan Rahasia dalam Gambar,” Skripsi S1, Universitas Pendidikan Indonesia, 2023.

[9] F. Kurniasih, R. Marwati, and R. Sispiyati, “Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar,” Jurnal EurekaMatika, vol. 11, no. 2, pp. 79–88, 2023.

[10] S. N. M. Al-Faydi, S. K. Ahmed, and H. N. Y. Al-Talb, “Improved LSB image steganography with high imperceptibility based on cover-stego matching,” IET Image Processing, vol. 17, no. 7, pp. 2072–2082, 2023, doi: 10.1049/ipr2.12773.

[11] D. R. Sina, G. A. Kiu, B. S. Djahi, and E. S. Y. Pandie, “Message Security Application (.txt) Using the Triple DES Method and the Combination of LSB and Blum-Blum-Shub Methods,” J-Icon: Jurnal Komputer dan Informatika, vol. 10, no. 2, pp. 204–209, 2022, doi: 10.35508/jicon.v10i2.8465.

[12] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, “Inverted LSB image steganography using adaptive pattern to improve imperceptibility,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 6, Part B, pp. 3559–3568, 2022, doi: 10.1016/j.jksuci.2020.12.017.

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 9, Nomor 1, Januari 2025, Page 01-08
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v9i1.8177

[13] A. D. Molato, F. B. Calanda, A. M. Sison, and R. P. Medina, "LSB-based Random Embedding Image Steganography Technique Using Modified Collatz Conjecture," in 2022 7th International Conference on Signal and Image Processing (ICSIP), 2022, pp. 367–371, doi: 10.1109/ICSIP55141.2022.9886754.

[14] S. Rani, A. Kurniawardhani, and Y. A. W. Rendani, "Steganography on Digital Color Image Using Modulo Function and Pseudo-Random Number Generator," International Journal on Advanced Science, Engineering and Information Technology, vol. 11, no. 6, pp. 2470–2475, 2021, doi: 10.18517/ijaseit.11.6.12687.

[15] S. Rahman et al., "A Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution Technique," Computers, Materials & Continua, vol. 64, no. 1, pp. 31–61, 2020, doi: 10.32604/cmc.2020.09186.

[16] M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, "Image Steganography Approaches and Their Detection Strategies: A Survey," ACM Computing Surveys, vol. 57, no. 2, art. 33, 2024, doi: 10.1145/3694965.

[17] J. G. Rajan and R. S. Ganesh, "Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework," Expert Systems with Applications, vol. 279, art. 127403, 2025, doi: 10.1016/j.eswa.2025.127403.

[18] A. N. Farzana, N. J. De La Croix, and T. Ahmad, "DualLSBStego: Enhanced Steganographic Model Using Dual-LSB in Spatial Domain Images," International Journal of Intelligent Engineering and Systems, vol. 18, no. 1, pp. 81–92, 2025, doi: 10.22266/ijies2025.0229.07.

[19] I. P. K. Putra and I. W. Supriana, "Analisis Perbandingan Kualitas Citra Hasil Steganografi DCT dan LSB Berdasarkan Parameter RMSE dan PSNR," Jurnal Nasional Teknologi Informasi dan Aplikasinya, vol. 2, no. 3, pp. 609–616, 2024, doi: 10.24843/JNATIA.2024.v02.i03.p20.

[20] J. Singh, A. K. Singh, and S. S. Chauhan, "Enhanced edge-based steganography using image segmentation and random LSB substitution for secure data hiding," International Journal on Smart Sensing and Intelligent Systems, vol. 18, no. 1, 2025, doi: 10.2478/ijssis-2025-0049.

Submitted: **12/08/2024**; Accepted: **28/12/2024**; Published: **28/01/2025**