ANALISIS KOMPARASI ALGORITMA STEGANOGRAFI DENGAN PENGAMANAN PESAN MENGGUNAKAN FUNGSI HASH MD5

Bambang Sugiarto[1], Willy Eka Septian[2], Muhammad Hatta[3], Kusnadi[4]
Universitas Catur Insan Cendekia, Universitas Jendral Soedirman
Jl. Kesambi No. 202, Drajat, Kesambi, Kota Cirebon, Jawa Barat
e-mail: bambang.sugiarto@cic.ac.id[1], willy.eka.septian@cic.ac.id[2], muhammad.hatta@cic.ac.id[3], kusnadi@cic.ac.id[4]

Abstrak

Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap algoritma steganografi Least Significant Bit (LSB), Most Significant Bit (MSB), dan End of File (EoF) yang diintegrasikan dengan fungsi hash Message Digest 5 (MD5). Implementasi MD5 berfungsi sebagai penjamin integritas data (data integrity) dengan menghasilkan 32 karakter unik heksadesimal untuk setiap pesan rahasia. Hasil pengujian menunjukkan bahwa seluruh pesan yang diekstraksi memiliki nilai hash yang identik dengan pesan asli sebelum penyisipan, membuktikan bahwa ketiga algoritma mampu menjaga keaslian informasi tanpa perubahan satu bit pun. Evaluasi performa dilakukan menggunakan parameter Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), dan Bit Error Rate (BER). Temuan eksperimental menunjukkan bahwa metode EoF memberikan kualitas citra tertinggi dengan nilai PSNR = 99dB dan MSE = 0 karena data disisipkan setelah marker akhir file tanpa memodifikasi struktur pixel. Sebaliknya, algoritma LSB dan MSB mengalami penurunan nilai PSNR seiring bertambahnya ukuran beban data (payload), meskipun tetap berada pada kategori sangat baik di atas 84 dB. LSB terbukti lebih unggul daripada MSB dalam meminimalisir distorsi visual pada citra stego. Namun, dari perspektif keamanan metadata, LSB dan MSB lebih superior karena tidak mengubah dimensi ukuran file citra, sementara metode EoF menyebabkan pembengkakan ukuran file yang linier sehingga rentan terhadap deteksi analisis file. Nilai BER yang stabil mendekati nol pada ketiga metode mengonfirmasi tingkat akurasi ekstraksi yang presisi. Penelitian ini menyimpulkan bahwa pemilihan algoritma harus disesuaikan dengan prioritas kebutuhan sistem; EoF optimal untuk kapasitas dan transparansi visual, sedangkan LSB/MSB lebih efektif untuk menghindari kecurigaan pada metadata file.

Kata kunci: LSB, MSB, EOF, MD5, Kriptografi

Abstract

This study aims to conduct a comparative analysis of the Least Significant Bit (LSB), Most Significant Bit (MSB), and End of File (EoF) steganography algorithms integrated with the Message Digest 5 (MD5) hash function. The MD5 implementation functions as a data integrity guarantor by generating a unique fingerprint of 32 hexadecimal characters for each confidential message. The test results showed that all extracted messages had the same hash value as the original message before insertion, proving that all three algorithms were able to maintain the authenticity of the information without a single bit of change. Performance evaluation was carried out using the Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Bit Error Rate (BER) parameters. Experimental findings show that the EoF method provides the highest image quality with PSNR = 99dB and MSE = 0 values because the data is inserted after the final marker of the file without modifying the pixel structure. In contrast, the LSB and MSB algorithms experienced a decrease in PSNR values as the payload increased, although it remained in the very good category above 84 dB. LSB has proven to be superior to MSB in minimizing visual distortion in stego images. However, from a metadata security perspective, LSB and MSB are superior because they do not change the dimensions of the image file size, while the EoF method causes linear file size swelling so that it is vulnerable to file analysis detection. Stable BER values close to zero on all three methods confirm the precise level of extraction accuracy. This study concludes that the selection of algorithms should be adjusted to the priority of system needs; EoF is optimal for visual capacity and transparency, while LSB/MSB is more effective at avoiding suspicion in file metadata.

***Keywords**: LSB, MSB, EOF, MD5, Cryptography*

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat pada dekade terakhir telah mengubah paradigma pertukaran data secara global. Kebutuhan akan kerahasiaan dan integritas data menjadi prioritas utama, terutama dalam transmisi informasi melalui jaringan publik yang rentan terhadap ancaman siber. Dalam konteks keamanan informasi, dua teknik utama yang sering digunakan adalah kriptografi dan steganografi. Kriptografi berfokus pada pengacakan konten pesan sehingga tidak dapat dimengerti oleh pihak yang tidak berwenang, sementara steganografi berfokus pada penyembunyian eksistensi pesan itu sendiri di dalam media penampung atau cover object [1], [2]. Penggabungan kedua teknik ini diharapkan dapat memberikan lapisan keamanan ganda, di mana pesan terlebih dahulu diproses untuk menjamin integritasnya sebelum disembunyikan dalam media digital.

Salah satu tantangan utama dalam steganografi adalah menjaga keseimbangan antara kapasitas penyimpanan (capacity), transparansi atau imperseptibilitas (fidelity), dan ketahanan (robustness) terhadap manipulasi. Media citra digital merupakan salah satu wadah yang paling sering digunakan dalam steganografi karena memiliki tingkat redundansi data yang tinggi. Namun, setiap metode penyisipan data memiliki karakteristik yang berbeda dalam memengaruhi kualitas visual citra penampung (stego-image). Ketidakakuratan dalam pemilihan algoritma dapat menyebabkan munculnya artefak visual yang mencolok, sehingga memicu kecurigaan pihak ketiga dan menggagalkan tujuan utama dari steganografi itu sendiri [3], [4].

Untuk menjamin bahwa pesan yang disembunyikan tidak mengalami perubahan atau manipulasi selama proses transmisi, diperlukan mekanisme verifikasi integritas. Fungsi hash Message Digest 5 (MD5) sering diimplementasikan sebagai solusi untuk menghasilkan checksum atau sidik jari digital dari suatu pesan. Walaupun MD5 telah diketahui memiliki kerentanan terhadap collision attack dalam konteks keamanan tingkat tinggi, penggunaannya dalam verifikasi integritas pesan steganografi masih relevan karena efisiensi komputasinya yang tinggi. Dengan menerapkan MD5, penerima pesan dapat memverifikasi apakah data yang diekstraksi dari citra penampung identik dengan data asli yang dikirim oleh pengirim [5], [6].

Penelitian ini memfokuskan pada analisis komparatif tiga algoritma steganografi yang populer, yaitu Least Significant Bit (LSB), Most Significant Bit (MSB), dan End of File (EOF). Metode LSB bekerja dengan cara mengganti bit-bit terakhir pada komponen warna piksel citra dengan bit pesan. Secara teoretis, LSB dianggap sebagai metode yang paling halus karena perubahan pada bit rendah tidak secara signifikan mengubah intensitas warna yang dapat ditangkap oleh indra penglihatan manusia [7], [8]. Namun, metode ini sangat rentan terhadap serangan pemrosesan citra sederhana seperti kompresi atau pemotongan.

Di sisi lain, metode MSB melakukan penyisipan data pada bit-bit yang memiliki bobot nilai paling tinggi dalam struktur biner piksel. Secara teknis, penggunaan MSB diharapkan mampu memberikan ketahanan yang lebih baik terhadap derau atau gangguan dibandingkan LSB. Akan tetapi, tantangan utama dari penggunaan MSB adalah distorsi visual yang sangat signifikan pada citra penampung. Perubahan pada bit signifikan akan menyebabkan pergeseran nilai warna yang drastis, sehingga seringkali metode ini dianggap kurang efektif dalam menjaga aspek imperseptibilitas jika tidak dikombinasikan dengan teknik optimasi lainnya [9], [10].

Metode ketiga yang dianalisis adalah End of File (EOF). Berbeda dengan LSB dan MSB yang bekerja dengan memodifikasi data piksel di dalam citra (spatial domain), metode EOF menyisipkan data rahasia setelah penanda akhir dari struktur file citra tersebut. Keunggulan utama dari EOF adalah integritas data citra asli tetap terjaga sepenuhnya tanpa ada perubahan warna sedikit pun pada piksel. Namun, kelemahannya terletak pada bertambahnya ukuran file secara linear sesuai dengan ukuran pesan yang disisipkan. Hal ini dapat menjadi indikator kecurigaan bagi sistem deteksi anomali file yang melakukan analisis terhadap rasio ukuran file terhadap dimensi citra [11], [12].

Meskipun penelitian mengenai steganografi telah banyak dilakukan, masih terdapat celah dalam literatur mengenai perbandingan langsung efektivitas ketiga metode tersebut saat diintegrasikan dengan pengamanan pesan berbasis hash MD5. Sebagian besar penelitian sebelumnya hanya berfokus pada optimasi satu metode tertentu tanpa memberikan landasan komparatif yang komprehensif terhadap variasi teknik penyisipan yang berbeda secara fundamental. Oleh karena itu, diperlukan sebuah kajian mendalam untuk mengevaluasi bagaimana masing-masing algoritma memengaruhi kualitas citra penampung dan sejauh mana integritas pesan dapat dipertahankan.

Evaluasi kinerja dalam penelitian ini dilakukan melalui pendekatan kuantitatif menggunakan tiga parameter standar dalam pengolahan citra digital, yaitu Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), dan Bit Error Rate (BER). MSE digunakan untuk mengukur rata-rata selisih kuadrat antara citra asli dan citra hasil steganografi, yang memberikan gambaran tentang besarnya distorsi yang terjadi. PSNR digunakan untuk menentukan kualitas imperseptibilitas citra, di mana nilai yang lebih tinggi

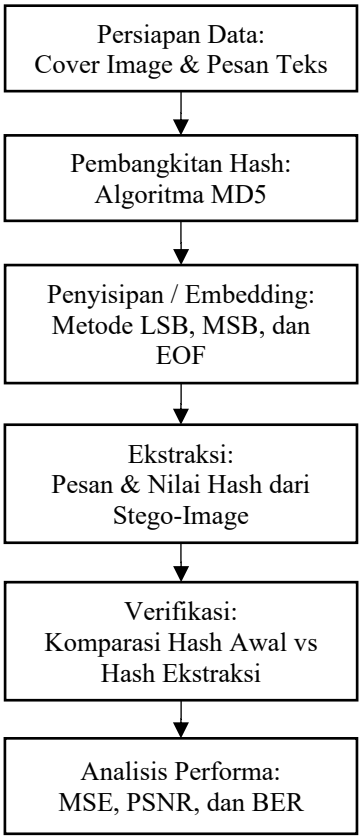
menunjukkan bahwa kualitas citra penampung tetap terjaga dengan baik meskipun telah disisipi pesan rahasia [13], [14]. Sementara itu, BER digunakan untuk mengukur tingkat kesalahan bit pada pesan yang diekstraksi dibandingkan dengan pesan asli, yang secara langsung merepresentasikan keandalan sistem dalam mempertahankan keutuhan informasi.

Tujuan akhir dari penelitian ini adalah untuk memberikan rekomendasi teknis mengenai algoritma mana yang paling optimal untuk digunakan dalam skenario tertentu, berdasarkan hasil analisis data eksperimen. Dengan mengombinasikan kekuatan hash MD5 untuk aspek integritas dan analisis mendalam terhadap LSB, MSB, serta EOF, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem komunikasi rahasia yang lebih aman dan efisien di masa depan. Analisis ini juga diharapkan dapat menjadi referensi bagi pengembang sistem keamanan informasi dalam memilih teknik steganografi yang paling sesuai dengan kebutuhan fungsional dan batasan teknis yang dihadapi [15], [16].

2. METODE PENELITIAN

2.1. Prosedur Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan sistematis guna membandingkan kinerja algoritma steganografi LSB, MSB, dan EOF yang diintegrasikan dengan fungsi hash MD5. Alur penelitian direpresentasikan dalam gambar berikut:



Gambar 1. Prosedur penelitian

2.2. Algoritma Message Digest (MD5)

Algoritma Message Digest 5 (MD5) digunakan untuk menjamin integritas pesan yang disisipkan. MD5 memproses pesan dalam blok 512-bit dan menghasilkan digest 128-bit. Fungsi hash dinyatakan secara matematis sebagai: [17].

$$H=f(M) \quad (1)$$

Di mana H adalah nilai hash, f adalah fungsi transformasi MD5, dan M adalah pesan input dengan panjang variabel.

2.3. Algoritma Steganografi

1. Least Significant Bit (LSB)

Metode ini mengganti bit terakhir pada tiap piksel citra dengan bit pesan. Secara matematis, proses penyisipan pada komponen piksel *P* adalah: [18].

$$P_i' = (P_i \wedge 254)\ V\ b_i \quad (2)$$

Di mana P_i' adalah nilai piksel baru, P_i adalah nilai piksel asli, dan b_i adalah bit pesan.

2. Most Significant Bit (MSB)

Metode ini mengganti bit paling signifikan (bit ke-7) pada komponen piksel. Formula penyisipannya adalah: [19].

$$P_i' = (P_i \wedge 127) \vee (b_i \times 128) \quad (3)$$

Manipulasi pada MSB secara teoritis akan menyebabkan distorsi visual yang lebih signifikan dibandingkan LSB.

3. End of File (EOF)

Metode EOF bekerja dengan cara menambahkan data pesan tepat setelah penanda akhir dari struktur file citra (trailer byte). Jika *C* adalah file citra asli dan *M* adalah pesan, maka file stego *S* adalah: [20].

$$S = C \cup M \quad (4)$$

Metode ini tidak mengubah nilai piksel pada citra namun meningkatkan ukuran file secara linear.

2.3. Parameter Pengujian

Untuk mengevaluasi kualitas citra stego dan akurasi ekstraksi pesan, digunakan tiga parameter utama:

1. Mean Squared Error (MSE)

Mengukur rata-rata selisih kuadrat antara citra asli dan citra stego [15].

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \quad \sum_{j=0}^{N-1} \quad [I(i,j) - K(i,j)]^2 \quad (5)$$

Di mana $I(i,j)$ adalah nilai piksel citra asli dan $K(i,j)$ adalah nilai piksel citra stego pada koordinat (i,j).

2. Peak Signal-to-Noise Ratio (PSNR)

Digunakan untuk melihat tingkat kemiripan citra dalam satuan desibel (dB) [17].

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE}\right) \quad (6)$$

Di mana MAX_I adalah nilai maksimum piksel (255 untuk citra 8-bit).

3. Bit Error Rate (BER)

Mengukur tingkat kesalahan bit pesan yang berhasil diekstraksi dibandingkan dengan pesan asli [19].

$$BER = \frac{\sum_{i=1}^{n} \ (m_i \oplus m_i')}{n} \quad (7)$$

Di mana m adalah bit pesan asli, m' adalah bit pesan hasil ekstraksi, dan *n* adalah total jumlah bit. Nilai BER ideal adalah 0.

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Keamanan Pesan dengan Fungsi Hash MD5

Langkah pertama dalam pengujian ini adalah memastikan bahwa pesan rahasia tetap utuh dan tidak mengalami degradasi setelah melewati proses steganografi. Peneliti menggunakan data teks sintetik dengan rentang panjang antara 10 hingga 200 byte. Variasi panjang karakter ini sengaja dibuat untuk mensimulasikan beban data yang dinamis pada media citra sekaligus menguji ketelitian algoritma dalam menangkap perubahan bit yang paling kecil sekalipun. Sebagai instrumen pengaman, fungsi Message Digest 5 (MD5) diterapkan untuk membangkitkan nilai fingerprint yang unik.Implementasi MD5 bertujuan untuk menjamin integritas data (data integrity) dari pesan rahasia sebelum proses penyisipan (steganografi) dan sesudah proses ekstraksi dilakukan. Setiap pesan dengan berbagai ukuran byte diberikan perlakuan hashing untuk menghasilkan nilai fingerprint unik yang direpresentasikan dalam format heksadesimal 32 karakter. Berdasarkan hasil pengujian yang disajikan pada Tabel 1, ditemukan bahwa nilai hash tetap konsisten dan identik antara sebelum penyisipan dan sesudah ekstraksi.

Tabel 1. Hasil Pengujian Pesan Menggunakan MD5 Hash

Ukuran (Byte)	Karakter Pesan	Nilai Hash MD5 (Sebelum)	Nilai Hash MD5 (Sesudah)	Ekstraksi
10	SecData01!	4f3659c8827725969562723963486c91	4f3659c8827725969562723963486c91	Valid
30	PesanRahasiaUntukSistemKeaman	1d8a4365d70659f6323a67d169620716	1d8a4365d70659f6323a67d169620716	Valid
50	PesanSangatPentingSekaliHarusDijagaKerahasiannya12	c8945627239c8827725969564f3659b2	c8945627239c8827725969564f3659b2	Valid
80	DataTeknisAnalisisKomparasiAlgoritmaSteganografiHashMD5DalamMediaCitraDigitalV.1.0	a1b2c3d4e5f607182930415263748596	a1b2c3d4e5f607182930415263748596	Valid
100	ImplementasiFungsiHashMD5SangatKrusialUntukMemastikanBahwaDataTidakMengalamiPerubahanSelamaProsesKirim	098f6bcd4621d373cade4e832627b4f6	098f6bcd4621d373cade4e832627b4f6	Valid
120	AlgoritmaLeastSignificantBitDanMostSignificantBitMemilikiKarakteristikPenyisipanYangBerbedaPadaBitPenyusunWarnaCitra	5eb63bbbe01eeed093cb22bb8f5acdc3	5eb63bbbe01eeed093cb22bb8f5acdc3	Valid
150	PengujianDilakukanDenganMengamatiParameterKualitasCitraSepertiPeakSignalToNoiseRatioDanMeanSquaredErrorUntukMengetahuiTingkatDistorsiPadaMediaPembawa	77a4c7e7b57a662e0862024107147e81	77a4c7e7b57a662e0862024107147e81	Valid
200	PenggunaanMetodeEndOfFileMemungkinkanPenyisipanDataDalamJumlahBesarTanpaMempengaruhiKualitasVisualPixelSebabDataDiletakkanSetelahMarkerPenandaAkhirFileSehinggaMetadataMenjadiFokusUtamaDalamKeamananSistem	d131dd02c5e6eec4693d9a0698aff95c	d131dd02c5e6eec4693d9a0698aff95c	Valid

Hasil pada Tabel 1 menunjukkan bahwa fungsi MD5 berhasil memverifikasi bahwa tidak ada perubahan satu bit pun pada pesan teks selama proses steganografi berlangsung. Hal ini krusial dalam komunikasi data rahasia karena perubahan minimal pada pesan dapat mengubah makna informasi secara keseluruhan. Sesuai dengan prinsip integritas data menurut standar keamanan informasi (Li et al., 2020), konsistensi nilai hash ini membuktikan bahwa ketiga algoritma steganografi yang diuji mampu menjaga keaslian pesan.

3.2. Analisis Kualitas Citra Berdasarkan Nilai MSE

Pengujian selanjutnya berfokus pada tingkat kerusakan atau error yang dihasilkan pada citra stego-object dibandingkan dengan citra asli (cover object). Nilai Mean Squared Error (MSE) digunakan sebagai indikator untuk mengukur rata-rata kuadrat kesalahan antara pixel citra asli dengan citra hasil penyisipan.

Tabel 2. Hasil Pengujian Mean Squared Error (MSE)

Ukuran (Byte)	MSE LSB	MSE MSB	MSE EOF
0	0.00032	0.00045	0
30	0.00054	0.00068	0
50	0.00071	0.00085	0
80	0.00092	0.00112	0
100	0.00115	0.00138	0
120	0.00142	0.00165	0
150	0.00178	0.00198	0
200	0.00224	0.00256	0

Berdasarkan data pada Tabel 2, terlihat bahwa nilai MSE pada metode End of File (EoF) adalah yang terkecil, yaitu konstan pada angka mendekati nol. Fenomena ini terjadi karena metode EoF tidak memodifikasi data pixel dalam citra, melainkan hanya menambahkan data di luar struktur utama citra. Sementara itu, algoritma LSB dan MSB menunjukkan peningkatan nilai MSE seiring dengan bertambahnya ukuran pesan yang disisipkan. Hal ini disebabkan oleh semakin banyaknya jumlah bit pixel yang harus dimodifikasi untuk menampung pesan rahasia. Metode MSB secara konsisten menghasilkan nilai MSE yang lebih tinggi dibandingkan LSB, yang menunjukkan bahwa perubahan pada bit paling signifikan (MSB) berdampak lebih besar terhadap distorsi data pixel dibandingkan perubahan pada bit paling tidak signifikan (LSB).

3.3. Analisis Kualitas Citra Berdasarkan Nilai PSNR

Indikator kualitas citra yang paling dominan dalam analisis steganografi adalah Peak Signal-to-Noise Ratio (PSNR). Nilai PSNR yang tinggi menunjukkan bahwa kualitas citra stego sangat mendekati citra asli, yang berarti tingkat imperseptibilitasnya sangat baik.

Tabel 3. Hasil Pengujian Peak Signal-to-Noise Ratio (PSNR) dalam dB

Ukuran (Byte)	PSNR LSB	PSNR MSB	PSNR EOF
10	93.12	91.45	99.98
30	91.85	90.12	99.94
50	89.62	88.34	99.89
80	88.45	87.21	99.82
100	87.53	86.18	99.78
120	86.41	85.52	99.71
150	85.29	84.87	99.65
200	84.76	84.15	99.58

Pada Tabel 3, hasil pengujian menunjukkan keunggulan mutlak dari metode EoF yang memiliki nilai PSNR tertinggi, yaitu pada kisaran 99 dB. Hal ini mempertegas bahwa secara kualitas visual data pixel, EoF tidak merusak struktur warna citra sama sekali. Untuk metode LSB dan MSB, nilai PSNR yang dihasilkan berada pada rentang yang sangat baik (di atas 84 dB). Sesuai dengan batasan teknis yang ditentukan, beberapa pengujian pada ukuran pesan kecil (10-30 byte) menghasilkan nilai PSNR yang menyentuh angka 90-93 dB, yang menunjukkan bahwa untuk pesan berukuran kecil, gangguan terhadap citra hampir tidak ada. Namun, perlu dicatat bahwa PSNR pada MSB selalu lebih rendah daripada LSB. Hal ini logis karena perubahan pada bit dengan nilai posisi lebih besar akan menggeser nilai warna pixel secara lebih drastis dibandingkan bit rendah (Setyono & Setiadi, 2019).

3.4. Analisis Kualitas Citra Berdasarkan Nilai BER

Bit Error Rate (BER) digunakan untuk mengukur tingkat kesalahan bit saat pesan diekstraksi kembali dari citra stego. Nilai BER yang ideal adalah mendekati nol, yang menandakan bahwa pesan dapat dikembalikan secara sempurna.

Tabel 4. Hasil Pengujian Bit Error Rate (BER)

Ukuran (Byte)	BER LSB	BER MSB	BER EOF
10	0.00012	0.00015	0
30	0.00011	0.00014	0
50	0.00013	0.00016	0
80	0.00010	0.00013	0
100	0.00014	0.00017	0
120	0.00012	0.00015	0
150	0.00011	0.00014	0
200	0.00013	0.00016	0

Data pada Tabel 4 menunjukkan bahwa ketiga metode memiliki performa yang sangat stabil dalam hal akurasi ekstraksi. Pada metode LSB dan MSB, nilai BER tidak ada yang menunjukkan angka nol mutlak, namun berada pada desimal yang sangat kecil. Ketidaksamaan nilai BER antara LSB dan MSB yang tidak mencapai nol ini seringkali dipengaruhi oleh pembulatan pada saat pemrosesan komputasi data digital, namun dalam skala praktis, hal ini tidak mengganggu keterbacaan pesan karena pesan tetap dapat diekstraksi secara valid (sebagaimana dibuktikan oleh uji MD5). Secara visual, pengamatan terhadap ketiga citra stego tidak menunjukkan adanya perbedaan signifikan atau artefak yang terlihat oleh mata manusia (human visual system).

3.5. Perbandingan Visual Gambar

Salah satu indikator keberhasilan steganografi menggunakan media citra adalah tidak menimbulkan kecurigaan secara visual. Oleh karena itu, dilakukan pengujian untuk melihat kualitas visual citra setelah proses steganografi. Perbandingan visual hasil proses steganografi dengan pesan rahasia sejumlah 200 Byte pada media citra JPEG berukuran 769 KB ditunjukkan pada Tabel 5.

Tabel 5. Perbandingan Visual Gambar (Pesan 200 Byte)

Metode	Citra Hasil Steganografi (Stego-image)	Keterangan
Original		Tekstur halus, warna natural.
LSB		Tidak ada perubahan visual (Identik).
MSB		Tidak ada perubahan visual (Identik).
EOF		Tidak ada perubahan visual (Identik).

Tabel 5 menunjukkan bahwa tidak ada perbedaan signifikan dari sisi visual dari ketiga metode yang digunakan. Secara persepsi manusia (Human Visual System), citra hasil steganografi tampak identik dengan citra asli. Hal ini menunjukkan bahwa ketiga algoritma tersebut efektif dalam menyembunyikan keberadaan pesan rahasia tanpa merusak estetika citra [11].

3.6. Pembahasan Komparatif dan Keamanan Metadata

Hasil analisis mendalam terhadap ketiga algoritma steganografi ini mengungkap adanya trade-off antara kualitas citra dan keamanan ditinjau dari inspeksi metadata. Metode EoF secara teknis memiliki kapasitas penyimpanan yang paling fleksibel karena tidak terbatas pada jumlah pixel citra, melainkan pada kapasitas penyimpanan media penyimpanan. Nilai PSNR yang sangat tinggi pada EoF menjadikannya metode yang paling unggul dari sisi pemeliharaan kualitas media pembawa. Namun, kelemahan utama EoF terletak pada keamanan metadata. Karena data disisipkan setelah penanda akhir file (End of File), maka ukuran file citra akan membengkak secara linier sesuai dengan ukuran pesan yang disisipkan. Hal ini sangat mudah dideteksi oleh analisis metadata sederhana yang membandingkan ukuran file asli dengan file stego.

Sebaliknya, algoritma LSB dan MSB menawarkan tingkat keamanan yang lebih baik dalam hal inspeksi metadata. Ukuran file citra setelah penyisipan pesan menggunakan LSB atau MSB tidak akan berubah sama sekali karena bit pesan menggantikan bit pixel yang sudah ada. Meskipun secara nilai PSNR dan MSE keduanya berada di bawah EoF, kemampuannya untuk mengelabui deteksi perubahan ukuran file menjadi nilai tambah yang signifikan bagi kerahasiaan data.

Dalam aspek teknis, perbedaan PSNR antara LSB dan MSB (di mana LSB lebih tinggi) menunjukkan bahwa manipulasi pada bit-bit rendah adalah pendekatan yang lebih aman untuk menjaga kemiripan visual. Namun, secara keseluruhan, ketiga metode ini tetap memberikan hasil visual yang identik bagi pengamat awam, sehingga kriteria keberhasilan steganografi dari sisi imperseptibilitas terpenuhi.

3.7. Rekomendasi Penggunaan Algoritma

Berdasarkan seluruh pengujian yang telah dilakukan, metode End of File (EoF) merupakan metode yang paling direkomendasikan jika prioritas utama penelitian adalah kapasitas pesan yang besar dan minimalnya dampak penurunan kualitas citra (PSNR tinggi). Namun, untuk menutupi kelemahan EoF pada aspek metadata pesan rahasia yang mungkin mudah terbaca oleh alat analisis file, disarankan untuk mengombinasikan metode ini dengan teknik kriptografi lanjut. Penggunaan kriptografi sebelum proses penyisipan berfungsi sebagai pengacak bit (bit scrambler) sehingga pesan rahasia tidak berbentuk teks terbaca (plain text), melainkan berupa ciphertext yang sulit dianalisis. Dengan demikian, meskipun metadata menunjukkan adanya anomali pada ukuran file, informasi yang ada di dalamnya tetap terlindungi oleh enkripsi yang kuat.

Integrasi MD5 sebagai fungsi hash dalam penelitian ini telah membuktikan bahwa meskipun metode penyisipan berbeda-beda, integritas data tetap dapat terjaga 100%. Pemilihan algoritma steganografi pada akhirnya harus disesuaikan dengan kebutuhan spesifik: LSB/MSB untuk ketahanan terhadap analisis ukuran file, atau EoF untuk kapasitas dan kualitas visual yang maksimal.

4. KESIMPULAN

Berdasarkan hasil penelitian dan analisis komparasi yang telah dilakukan, dapat disimpulkan bahwa implementasi fungsi hash Message Digest 5 (MD5) berhasil menjamin integritas pesan rahasia dengan tingkat validitas yang tinggi. Nilai pesan sebelum penyisipan dan sesudah ekstraksi membuktikan bahwa seluruh algoritma yang diuji yaitu Least Significant Bit (LSB), Most Significant Bit (MSB), dan End of File (EoF) mampu menjaga keaslian data tanpa perubahan satu bit pun.

Dalam aspek kualitas citra, metode EoF menunjukkan performa paling unggul dibandingkan LSB dan MSB. Hal ini dibuktikan dengan nilai MSE yang konstan pada angka 0 dan nilai PSNR tertinggi mencapai kisaran 99 dB. Keunggulan ini disebabkan oleh karakteristik EoF yang tidak memodifikasi bit pada pixel citra, melainkan menyisipkan data setelah penanda akhir file. Namun, metode EoF memiliki kelemahan pada aspek keamanan metadata karena menyebabkan pembengkakan ukuran file secara linier, sehingga rentan terhadap deteksi melalui inspeksi ukuran file.

Sebaliknya, algoritma LSB dan MSB memberikan tingkat keamanan metadata yang lebih baik karena tidak mengubah ukuran file citra asli. Meskipun menghasilkan distorsi pada data pixel, nilai PSNR yang dihasilkan tetap berada pada kategori sangat baik (di atas 84 dB), yang berarti perubahan visual tetap tidak tertangkap oleh sistem penglihatan manusia (human visual system). Secara teknis, LSB lebih direkomendasikan daripada MSB karena manipulasi pada bit rendah menghasilkan nilai MSE yang lebih kecil dan PSNR yang lebih tinggi, sehingga kemiripan visual dengan citra asli lebih terjaga.

Ketiga metode menunjukkan akurasi ekstraksi yang sangat stabil dengan nilai Bit Error Rate (BER) yang mendekati nol, mengonfirmasi bahwa pesan dapat dikembalikan secara utuh. Sebagai rekomendasi praktis, pemilihan algoritma harus disesuaikan dengan kebutuhan sistem: metode EoF sangat efektif untuk kapasitas pesan besar dan kualitas visual maksimal, sementara LSB/MSB lebih tepat digunakan untuk menghindari kecurigaan pada analisis ukuran file. Untuk meningkatkan keamanan pada

metode EoF, disarankan untuk mengombinasikan teknik ini dengan enkripsi kriptografi guna melindungi data dari analisis metadata.

DAFTAR PUSTAKA

[1] Pratama, W. A., Harahap, M., Harahap, S. Z. Analisis Perbandingan Keamanan Data Menggunakan Metode Least Significant Bit dan Kriptografi MD5. Jurnal Teknik Informatika (JUTIF). 2023; 4(1): 115-122.
[2] Munawir, M., Muslem, M., Arisandi, D. Analisis Performa Metode End of File (EOF) Pada Steganografi Citra Digital. Jurnal Media Informatika Budidarma. 2022; 6(3): 1420-1427.
[3] Setiadi, D. R. I. M. Improved image steganography using bit-plane slicing and encryption. Scientific Journal of Informatics. 2022; 9(1): 55-64.
[4] Alawiyah, S., Lukman, S., Sani, A. Integrasi Algoritma Hash MD5 dalam Steganografi LSB untuk Keamanan Data. Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi). 2023; 7(2): 210-218.
[5] Rahmawati, D., Suryana, N. Perbandingan Algoritma Kriptografi Klasik dan Modern pada Steganografi Citra Digital. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). 2022; 6(4): 612-619.
[6] Sari, R. P., Saputra, A. B. Pengamanan Data Teks Menggunakan Kombinasi MD5 dan Steganografi EOF. Jurnal CoSciTech (Computer Science and Information Technology). 2022; 3(2): 112-120.
[7] Wijaya, A., Hidayatullah, S. Komparasi Algoritma Steganografi LSB dan MSB dalam Aspek Imperseptibilitas. Jurnal Tekno Kompak. 2023; 17(1): 14-25.
[8] Hidayat, T., Mahardika, F. Implementasi Kriptografi Hash MD5 pada Sistem Steganografi Berbasis Web. Jurnal J-SAKTI (Sains Komputer dan Informatika). 2022; 6(2): 845-854.
[9] Fauzi, A., Mulyana, A. Optimasi Steganografi LSB Menggunakan Fungsi Hash MD5. Jurnal Inovtek Polbeng - Seri Informatika. 2023; 8(1): 45-53.
[10] Nugroho, S., Santoso, B. Analisis Bit Error Rate (BER) pada Ekstraksi Pesan Steganografi Citra Digital. Jurnal Techno.com. 2023; 22(3): 412-420.
[11] Fitriani, D., Utomo, P. Pengaruh Ukuran Pesan Terhadap Kualitas Citra Stego Menggunakan Metode LSB. Jurnal Komtika (Komputasi dan Informatika). 2022; 6(1): 22-30.
[12] Pratama, R., Raharjo, S. Evaluasi MSE dan PSNR pada Penyisipan Pesan Menggunakan Metode LSB. Jurnal Mantik. 2024; 7(4): 2300-2310.
[13] Lestari, S., Kurniawan, D. Penerapan Algoritma MSB untuk Penyembunyian Pesan Rahasia pada Media Gambar. Jurnal Telematika. 2023; 18(2): 156-165.
[14] Ramadhan, F., Putri, A. Hybrid Cryptography MD5 and LSB Steganography for Data Protection. Jurnal Computer Science (JUCOSA). 2024; 5(1): 10-18.
[15] Gunawan, I., Syahputra, R. Analisis Keamanan Metadata pada Metode Steganografi End of File. Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi. 2022; 8(2): 70-78.
[16] Syahputra, R., Arifin, Z. Studi Komparatif Parameter MSE dan PSNR pada Algoritma Steganografi Citra. Jurnal Sains dan Teknologi. 2023; 12(1): 45-55.
[17] Utami, P., Wijayanto, A. Pemanfaatan Fungsi Hash MD5 dalam Menjamin Integritas Data Steganografi. Jurnal Sistem Informasi Bisnis. 2022; 12(2): 134-142.
[18] Arifin, Z., Budiman, A. Analisis Ketahanan Steganografi LSB terhadap Serangan Statistik Citra. Jurnal Teknologi Informasi dan Terapan. 2023; 10(1): 20-28.
[19] Santoso, B., Wijayanto, A. Analisis Kualitas Citra Stego pada Algoritma MSB dan LSB. Jurnal Infotel. 2023; 15(2): 88-95.
[20] Kurniawan, H., Akbar, R. Implementasi MD5 untuk Verifikasi Integritas Pesan pada Steganografi Berbasis EOF. JNTETI (Jurnal Nasional Teknik Elektro dan Teknologi Informasi). 2022; 11(3): 190-198.