Jurnal Teknologi Informasi dan Multimedia

p-ISSN : 2715-2529

e-ISSN : 2684-9151

https://journal.sekawan-org.id/index.php/jtim

Penerapan Teknik *Steganografi* dalam Gambar pada Aplikasi Telegram Menggunakan Metode *Least Significant Bit* (LSB)

Lu'lu' Atik Fitriyani [1*], Fahmi Fachri [1]

[1] Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia

* Korespondensi: luluatik716@gmail.com

Sitasi: L. A. Fitriyani and F. Fachri, "Penerapan Teknik *Steganografi* Dalam Gambar Pada Aplikasi Telegram Menggunakan Metode *Least Significant Bit* (LSB)", *Jurnal Teknologi Informasi Dan Multimedia*, vol. 8, no. 2, pp. 357-368, 2026. https://doi.org/10.35746/jtim.v8i2.1021

Diterima: 29-04-2026
Direvisi: 14-05-2026
Disetujui: 22-05-2026

Copyright: © 2026 oleh para penulis. Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License. (https://creativecommons.org/licenses/by-sa/4.0/).

Abstract: In the digital era, the threat of data leakage demands secure information exchange mechanisms on instant messaging applications. This study aims to implement and test the robustness of the Least Significant Bit (LSB) steganography method on image media transmitted through the Telegram platform to ensure information confidentiality and create secure cyber communication against eavesdropping. The novelty of this research lies in the comparative analysis of the pure LSB method's robustness against Telegram's compression protocols, which frequently corrupt lower bits in digital media. This study employs an experimental quantitative approach by testing 15 digital image samples in PNG, BMP, and JPG formats sourced from the Google public repository. The experimental process involves embedding text messages using StegOnline tools, transmission via Telegram, extraction, and image quality analysis based on Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) metrics. The test results indicate that the LSB method achieves a 100% extraction success rate and a Bit Error Rate (BER) of 0 when utilizing the "send document" feature due to its lossless transmission nature, with optimal visual quality indicated by PSNR values above 58 dB. Conversely, transmission through the "send image" feature causes extraction failure due to the platform's compression that corrupts the secret bits. This study concludes that the accuracy stability of LSB steganography highly depends on selecting a lossless transmission format to fully guarantee data integrity.

Keywords: *Steganography, Least Significant Bit (LSB), Telegram, Information Security, PSNR.*

Abstrak: Di era digital, ancaman kebocoran data menuntut mekanisme pertukaran informasi yang aman pada aplikasi pesan instan. Penelitian ini bertujuan untuk mengimplementasikan dan menguji ketahanan teknik *steganografi* metode *Least Significant Bit* (LSB) pada media gambar yang dikirimkan melalui platform Telegram guna menjamin kerahasiaan informasi dan menciptakan komunikasi siber yang aman dari penyadapan. Kebaruan dari penelitian ini terletak pada analisis komparatif ketahanan metode LSB murni terhadap protokol kompresi Telegram yang sering kali merusak bit rendah pada media digital . Penelitian ini menggunakan pendekatan kuantitatif eksperimental dengan menguji 15 sampel citra digital berformat PNG, BMP, dan JPG yang bersumber dari repositori publik Google. Proses eksperimen meliputi tahapan *embedding* pesan teks menggunakan *tools* StegOnline, transmisi via Telegram, ekstraksi, hingga analisis kualitas citra berdasarkan metrik *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Hasil pengujian menunjukkan bahwa metode LSB mencapai tingkat keberhasilan ekstraksi 100% dan BER 0 saat menggunakan fitur "kirim dokumen" karena sifat transmisinya yang *lossless*, dengan kualitas visual optimal pada nilai PSNR di atas 58 dB. Sebaliknya, pengiriman melalui fitur "kirim gambar" menyebabkan kegagalan ekstraksi akibat kompresi platform yang merusak bit rahasia. Penelitian ini menyimpulkan bahwa stabilitas akurasi steganografi LSB sangat bergantung pada pemilihan format pengiriman *lossless* untuk menjamin integritas data secara utuh.

Kata kunci: *Steganografi*, *Least Significant Bit* (LSB), Telegram, Keamanan Informasi, PSNR.

1. Pendahuluan

Di era digital yang semakin berkembang pesat, keamanan informasi menjadi aspek yang sangat penting dalam kehidupan sehari-hari, informasi birokrasi di media sosial dapat disampaikan melalui dokumen berbasis teks atau gambar, yang dianggap lebih praktis dan efisien [1] . Ancaman terhadap keamanan data di era digital merupakan masalah serius yang terus berkembang seiring dengan pesatnya kemajuan teknologi informasi dan meningkatnya aktivitas manusia di dunia maya [2]. Saat ini, hampir seluruh aspek kehidupan mulai dari komunikasi, pendidikan berbisnis, hingga pemerintahan bergantung pada sistem digital yang menyimpan dan mengelola data dalam jumlah yang besar [3]. Ketergantungan tersebut menjadikan data sebagai asset berharga, namun sekaligus rentan terhadap serbagai bentuk ancaman yang dapat mengakibatkan kebocoran, kehilangan, atau bisa juga sampai ke penyalahgunaan informasi.

Merujuk pada Laporan Situasi Hak Digital Indonesia Triwulan I 2025 yang dirilis oleh *Southeast Asia Freedom of Expression Network* (*SAFEnet*) terkait situasi hak digital di Indonesia periode awal 2025, tercatat lonjakan signifikan sebanyak 139 insiden serangan siber, yang menunjukkan kenaikan lebih dari 100% dibandingkan dengan kuartal yang sama pada tahun 2024 (60 kasus), tren lima tahun terakhir mengkonfirmasi adanya eskalasi serangan yang persisten : dimulai dari 40 kasus di awal 2021, naik menjadi 57 di 2022, sempat merosot ke 33 di tahun 2023, kasus di awal 2021, naik menjadi 57 di tahun 2022, sempat merosot ke 33 di tahun 2023, sebelum akhirnya melonjak kembali , data tersebut juga mengungkap fakta krusial bahwa mayoritas serangan 59,71% menyasar pada kelompok yang kritis terhadap pemerintahan. Dengan adanya sistem keamanan yang baik, kerahasiaan pesan dapat terjaga sehingga hanya pihak tertentu atau pihak tertuju saja yang dapat mengaksesnya, serta integritas data tetap terjamin tanpa adanya perubahan selama proses pengiriman [4] . Di era modern komunikasi digital ini ada beberapa teknik yang digunakan untuk menyembunyikan informasi dalam media tertentu, salah satu teknik tersebut adalah *steganografi* [5] . *Steganografi* ini berfokus pada menyembunyikan keberadaan pesan itu sendiri, sehingga orang lain bahkan tidak menyadari bahwa ada informasi rahasia yang tersembunyi didalam suatu media [6]

Permasalahan pada penelitian ini adalah meningkatnya aktivitas komunikasi daring dan ancaman siber seperti peretasan, penyadapan, serta kebocoran data yang di Indonesia sendiri terus meningkat. Aplikasi pesan instan seperti Telegram banyak digunakan karena kecepatan, fleksibelitas dan fitur keamanannya. Namun tetap berpotensi menjadi sasaran penyadapan sehingga diperlukan lapisan keamanan tambahan. Solusi pada permasalahan ini adalah menerapkan Teknik *steganografi* (menyembunyikan pesan ke dalam suatu media atau gambar tanpa menimbulan perubahan visual yang menolok).

Tujuan utama *steganografi* adalah untuk menjaga kerahasiaan komunikasi dan mencegah pihak tidak berwenang mengetahui bahwa suatu pesan sedang dikirim ke aplikasi Telegram [7] . Data digital kini menjadi salah satu asset paling berharga, karena didalamnya tersimpan berbagai informasi sensitif yang sangat penting untuk keberlangsungan aktivitas individu maupun organisasi, dimana aplikasi pesan instan seperti Telegram menjadi salah satu alat utama untuk pertukaan informasi cepat dan global [8] . Telegram dipilih sebagai platform aplikasi karena memiliki berbagai keunggulan yang mendukung kebutuhan komunikasi modern, terutama dalam hal keamanan, kecepatan, dan fleksibilitas [9] . Pada penelitian kali ini, peneliti menggunakan metode *Least Significant Bit* (LSB).

Secara keseluruhan metode ini dipilih karena sederhana, mudah diterapkan, efisien dalam penggunaan ruang, efektif, dan memiliki tingkat keberhasilan yang tinggi dalam menyembunyikan pesan [10]. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan teknik *steganografi* metode *Least Significant Bit* (LSB) pada media gambar yang di transmisikan melalui aplikasi Telegram, untuk menciptakan media komunikasi siber yang aman, tersembunyi, dan tahan terhadap penyadapan. Secara spesifik, penelitian ini akan berfokus pada proses penyisipan pesan kedalam *cover image* dengan menggunakan metode *Least Significant Bit* . Melalui instegrasi teknik ini diharapkan dapat mengurangi risiko *cybercrime* dan meningkatkan keamanan pesan terutama untuk tujuan sensitif seperti pertukaran data birokrasi, bisnis, atau informasi pribadi di tengah meningkatnya serangan siber di Indonesia.

Berikut beberapa ringkasan terkait kajian literatur pada penelitian ini yaitu seperti yang dilakukan oleh [11] penelitian ini menerapkan teknik *masking* pada *spectrogram* audio sebagai sarana untuk menyembunyikan pesan, dengan proses analisis yang didukung oleh bahasa pemrograman *phyton* serta pustaka *librosa*. Meskipun metode ini terbukti efektif dalam menyisipkan informasi, hasil pengujian menunjukkan adanya perbedaan yang terukur pada tampilan visual dan data statistik sinyal audio jika dibandingkan dengan versi originalnya. Penelitian selanjutnya menurut [12] riset ini berfokus pada pengembangan sistem keamanan citra RGB berbasis *GUI MATLAB* melalui skema keamanan berlapis yang mengintegrasikan kriptografi *Arnold Cat Map* (*ACM*) dan *steganografi Least Significant Bit* (*LSB*). Melalui pengujian terhadap 25 sampel citra (dimensi 100x100 hingga 500x500), hasil menunjukkan integritas data yang sempurna dengan nilai (MSE=0, PSNR yang tertinggi (140-173 dB), durasi pemrosesan meningkat secara signifikan selaras dengan bertambahnya dimensi citra. Temuan ini merekomendasikan penggunaan perangkat keras berkinerja tinggi untuk optimasi komputasi pada penelitian di masa mendatang.

Penelitian lain juga dilakukan oleh [13] penelitian ini ditujukannya teruntuk memanfaatkan penggunaan *steganografi* dengan metode LSB perihal mengamankan berkas audio yang berformat .AAC kedalam citra digital yang berformat .BMP serta .PNG. Ukuran dari citra digital dan durasi dari berkas audio berbeda-beda, melalui perbedaan tersebut dihasilkannya proses penyisipan serta pengekstraksian yang berbeda. Keseluruhan pengujian dilakukannya dengan cara melaluinya tahapan penyisipan dengan ukuran piksel citra digital yang berbeda. Maka daripada itu jika semakin besar ukuran dari citra digital yang dipakai, maka akan lama juga tahapan dalam waktu pengekstraksiannya dan juga sebaliknya. Hal serupa juga dilakukan oleh [14] studi ini mengintegrasikan algoritma kriptografi *Rivest Shamir Adleman* (*RSA*) dan algoritma *steganografi* LSB untuk menjamin keamanan pesan. Hasil pengujian menunjukkan bahwa skema kombinasi ini mampu melakukan rekonstruksi data dengan sangat baik.

Secara teknis, citra beresolusi besar 1024x1024 mencatatkan tingkat error (MSE) paling rendah dan nilai PSNR diatas 40 dB, yang menandakan kualitas visual yang sangat tinggi. Sebaliknya, pengujian SSIM dan NCC yang mendekati angka 1 pada citra besar membuktikan bahwa hampir tidak ada perbedaan signifikan antara gambar asli dan gambar hasil steganografi. Dalam penelitiannya [15] penelitian ini merancang aplikasi yang menggabungkan *steganografi* LSB dan kompresi *Huffman* untuk melindungi pertukaran informasi pada media audio WAV. Integrasi kedua metode ini dilakukan untuk menutupi celah keamanan dari akses pihak ketiga sekaligus mengatasi masalah pemborosan ruang penyimpanan pada file audio. Prosedur utamanya melibatkan penyisipan 100 byte data teks kedalam format WAV, sehingga dihasilkan stego-audio yang aman namun tetap memiliki ukuran teroptimasi. Pemilihan Telegram sebagai objek penelitian didasari oleh fenomena meluasnya penggunaan platform ini untuk pertukaran dokumen birokrasi dan informasi sensitif, sementara kajian *steganografi* pada media sosial lain seperti WhatsApp dan Instagram sudah terlalu umum.

Meskipun penelitian terdahulu telah berhasil mengimplementasikan metode *Least Significant Bit* (LSB) untuk mengamankan data melalui berbagai kombinasi algoritma seperti kriptografi Arnold Cat Map, RSA, hingga kompresi Huffman, pengujiannya secara umum masih terbatas pada lingkungan simulasi lokal atau *offline*. Di sisi lain, kajian *steganografi* pada aplikasi pesan instan masih didominasi oleh platform seperti WhatsApp dan Instagram, sehingga menyisakan celah penelitian (*research gap*) yang nyata terkait ketahanan metode LSB pada arsitektur jaringan Telegram. Padahal, Telegram memiliki karakteristik unik dalam menangani transmisi media melalui fitur pengiriman dokumen (*lossless*) dan gambar (*lossy*) yang rentan memengaruhi susunan bit tidak signifikan pada piksel citra. Berdasarkan kesenjangan tersebut, kebaruan (*novelty*) dari penelitian ini terletak pada analisis eksperimental kuantitatif untuk menguji ketahanan metode LSB murni terhadap protokol kompresi Telegram menggunakan 15 sampel data. Melalui pendekatan ini, pengujian tidak hanya berfokus pada kualitas visual citra stego secara statis, melainkan mengevaluasi secara real keutuhan serta sinkronisasi bit informasi setelah melewati proses transmisi, sehingga mampu memvalidasi efektivitas metode LSB dalam menyediakan solusi komunikasi siber yang aman dari ancaman penyadapan.

Penelitian ini secara khusus mengeksplorasi ketahanan metode LSB terhadap protokol transmisi data di Telegram, yang memiliki fitur unik berupa pengiriman "dokumen" (*lossless*) dan "gambar" (*lossy*). Fokus utamanya adalah menganalisis sejauh mana pengaruh kompresi platform terhadap integritas data tersembunyi, guna memastikan pesan rahasia tetap utuh dan tidak mengalami degradasi bit selama proses pengiriman berlangsung. Tujuan utama dari penelitian ini adalah untuk memvalidasi efektivitas metode LSB dalam melindungi pesan digital dari ancaman penyadapan dan kebocoran data pada platform Telegram. Dengan menjaga prinsip kerahasiaan, keutuhan, dan ketersediaan informasi, penelitian ini bertujuan menyediakan solusi teknis bagi pengguna untuk mengirimkan data sensitif melalui media gambar secara aman. Hasil yang diharapkan penelitian ini dapat membuktikan keandalan transmisi Telegram dalam mempertahankan sinkronisasi bit rahasia, sehingga informasi yang diekstraksi memiliki tingkat akurasi yang tinggi tanpa adanya kerusakan karakter.

2. Bahan dan Metode

Penelitian ini menggunakan metode kuantitatif eksperimental yang menekankan pengujian secara terstruktur, terkontrol, dan berbasis statistik untuk melihat hubungan sebab-akibat antarvariabel. Penelitian eksperimental ini bertujuan untuk menguji efektivitas metode LSB melalui proses manipulasi, kontrol, dan pengacakan guna memperoleh data yang valid serta objektif. Dalam pelaksanaan eksperimen ini, objek penelitian difokuskan dengan menguji 15 sampel citra digital berformat PNG, BMP, dan JPG yang bersumber dari repositori publik Google . Ke-15 sampel data gambar tersebut digunakan sebagai media penampung (*cover image*) untuk disisipi pesan teks rahasia, yang kemudian dikirim melalui platform *instant messaging* Telegram. Pengujian terhadap 15 sampel ini dilakukan untuk menganalisis pengaruh kompresi, kapasitas, dan kualitas citra secara statistik, sehingga dapat membuktikan batas optimal serta ketahanan metode LSB dalam skenario pengiriman pesan instan secara nyata. Melalui pendekatan dengan 15 sampel data ini, penelitian dapat memberikan bukti teknis yang kuat dan tidak ambigu mengenai kinerja metode LSB, proses tersebut digambarkan pada diagram alur berikut :

Gambar 1. Alur Penelitian

Berikut tahapan-tahapan atau alur pada penelitian ini meliputi ;

a) Tahap I : Embedding (Penyisipan Pesan)

Tahap Embedding (Penyisipan Pesan) adalah tahap untuk menyembunyikan atau memasukkan informasi rahasia (pesan teks, file, atau citra lain) ke dalam suatu media penampung (cover object) tanpa mengubah karakteristik media tersebut secara kasat mata.

b) Tahap II : Uploading (Pengunggahan ke Sosial Media)

Tahap pengunggahan ke sosial media ini adalah proses mengirimkan media yang telah disisipi pesan rahasia (*stego-object*, misalnya *stego-image*) dari perangkat lokal pengguna ke server media social seperti Telegram.

c) Tahap III : Downloading (Pengunduhan Gambar)

Selanjutnya tahap pengunduhan gambar tahap ini adalah proses di mana penerima mengunduh file *stego-object* dari server media sosial ke perangkat lokal mereka sebelum melakukan tahap ekstraksi.

d) Tahap IV : Extracting (Ekstraksi Pesan)

Tahap ekstraksi pesan ini proses mengambil, membaca, atau mengeluarkan kembali pesan rahasia yang telah disembunyikan di dalam media penampung (*stego-object*). Pada tahap ini, penerima pesan yang dituju akan memproses *stego-image* (atau media lain) yang telah diunduh dari media sosial/platform komunikasi untuk mendapatkan informasi rahasia yang dikirimkan oleh pengirim pesan tersebut.

e) Tahap V : Analysis

Tahap analysis adalah tahap akhir,dimana tahap ini untuk menguji, mengukur, dan mengevaluasi kualitas serta keamanan dari media penampung yang telah disisipi pesan rahasia (*stego-object*). Fokus utamanya adalah menyeimbangkan tiga sudut yang saling berkaitan keamanan, kapasitas, dan ketahanan.

2.1. Perhitungan PSNR (Peak Signal Noise Ratio)

Kualitas citra hasil pemampatan dapat diukur secara kuantitatif menggunakakan besaran PSNR (*Peak Signal to Noise Ratio*). PSNR mengukur perbandingan anatara nilai maksimum sinyal (kualitas gambar asli) dengan derau noise yang dihasilkan oleh penyisipan pesan [16] . Hasilnya dinyatakan dalam satuan Desibel (Db). Logikanya semakin

tinggi nilai PSNR, berarti gangguan (pesan rahasia) itu semakin kecil dibandingkan dengan gambar aslinya.

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

2.2. Perhitungan MSE (Mean Square Error)

MSE digunakan untuk menghitung rata-rata selisih kuadrat antara citra asli (*cover image*) dan citra yang sudah disisipi pesan (*stego image*). Semakin kecil nilai MSE, maka semakin sedikit perubahan yang terjadi pada citra.

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [c(i,j) - s(i,j)]^2$$

Indikator : Semakin mendekati 0, maka sempurna. Artinya, hampir tidak ada perubahan antara foto asli dan foto berisi pesan.

2.3. Akurasi Pesan (Bit Error Rate)

$$Akurasi = \left(\frac{Total\ bit\ yang\ benar}{Total\ bit\ pesan} \right) \times 100\%$$

Keterangan : Kalau kamu menyisipkan kata "HALO" (4 huruf) dan saat diambil kembali dan keluarnya tetap "HALO", maka akurasimu 100%. Tetapi jika keluarnya "HAKO", berarti ada kesalahan pada bit.

Kesimpulan Sederhana :

Penelitian *steganografi* LSB dianggap berhasil jika :

1. Gambar tidak rusak : Ditandai dengan MSE kecil dan PSNR tinggi (idealnya > 30 dB).
2. Nilai PSNR > 40 dB : Menunjukkan kualitas yang sangat baik (hampir identik).
3. Akurasi Ekstraksi : Selain kualitas citra, kita juga harus menghitung *Bit Error Rate* (BER). Jika pesan yang diambil kembali (ekstraksi) sama persis dengan pesan asli, maka nilai BER adalah 0, yang berarti akurasinya 100%.

2.4. Alat dan Bahan Penelitian

Dalam penelitian ini terdapat beberapa alat dan bahan yang diperlukan, adapun rincian alat dan bahan yang akan digunakan adalah sebagai berikut :

Tabel 1. Alat dan Bahan Penelitian

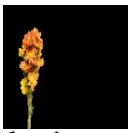
Kategori	Spesifikasi
Hardware	Laptop Acer Aspire A314-22
Software	Windows 11 Home Single Language, StegOnline

3. Hasil dan Pembahasan

Eksperimen pengujian teknik steganografi *Least Significant Bit* (LSB) terhadap 15 sampel citra digital (PNG, BMP, JPG) melalui dua skenario transmisi di platform Telegram menunjukkan hasil kuantitatif yang kontras pada parameter metrik visual dan akurasi ekstraksi. Pada skenario fitur "Kirim sebagai Dokumen" (*lossless transmission*), kualitas visual citra stego sangat optimal dengan nilai *Mean Squared Error* (MSE) mendekati nol, nilai *Peak Signal-to-Noise Ratio* (PSNR) stabil di atas 58 dB, serta mencapai tingkat akurasi ekstraksi pesan tepat sebesar 100% tanpa adanya kerusakan karakter

biner. Sebaliknya, pengujian menggunakan fitur standar "Kirim sebagai Gambar" (*lossy transmission*) menunjukkan penurunan kualitas statistik pada nilai MSE dan PSNR yang disertai penyusutan ukuran file file citra, serta mengakibatkan kegagalan total proses pengekstrakan data rahasia dengan tingkat akurasi ekstraksi sebesar 0%. Berikut hasil dari penelitian yang akan kita bahas sebagai berikut ;

Tabel 2. citra asli dan isi pesan

Citra Asli	Isi Pesan	Citra Asli	Isi Pesan
 bunga .bmp	Jangan lupa datang	 asoka .bmp	Isi pesan ini jangan sampai bocor
 mawar 4.png	Temui saya di taman	 biru.bmp	Jangan sembarangan screenshot dan sebar isi chat pribadi
 ungu 7.jpg	Jangan lupa makan	 aster.jpg	Jangan sembarangan memberikan akses akun chat ke orang
 merah .jpg	Kirimi saya alamatmu	 anggrek.jpg	Selalu waspada dengan siapa kamu bertukar pesan
 matahari .jpg	Tolong simpan pin yang saya kirim	 tulip.png	Simpan bukti chat hanya jika benar-benar diperlukan
 kuning .png	Jangan temui saya beberapa hari ini	 tunas.bmp	Tetap tenang dan waspada kalau ada ancaman lewat pesan
 gunung .png	Hati-hati saat kirim data pribadi lewat aplikasi chat	 cantik.bmp	Hati-hati dengan tawaran pinjaman online lewat pesan
 merah muda .bmp	Tetap waspada agar privasi pesan kamu tidak terganggu		

Pada tabel 2. data ini menyajikan kumpulan citra bunga dan pemandangan sebelum di ekstraksi yang masing-masing dipasangkan dengan potongan teks pesan tertentu. Setiap baris data menunjukkan hubungan antara file gambar dengan format yang bervariasi seperti BMP, PNG, dan JPG dengan isi pesan singkat yang berbeda-beda. Penelitian ini memilih Telegram sebagai media transmisi karena platform ini menawarkan fleksibelitas dalam pengiriman data melalui fitur "kirim gambar" dan "kirim dokumen". Pengiriman sebagai dokumen ini menjadi fokus utama karena menggunakan metode pengiriman *lossless,* dimana Telegram tidak melakukan kompresi atau perubahan bit pada file yang dikirim. Hal ini sangat penting bagi metode LSB karena integritas bit terendah pada piksel gambar tetap terjaga, sehingga pesan rahasia seperti "Jangan lupa datang" pada gambar 8. dapat diektraksi kembali dengan ektraksi sempurna (100%) tanpa ada data yang korup. Disisi lain, penggunaan fitur kirim gambar biasa (sebagai media) berfungsi sebagai parameter pengujian untuk melihat sejauh mana platform media sosial (Telegram) melakukan manipulasi data. Berbeda dengan dokumen, pengiriman gambar biasa sering kali mengalami proses kompresi otomatis yang dapat mengubah susunan bit dalam gambar. Dengan membandingkan kedua metode pengiriman ini, penelitian ini dapat membuktikan bahwa pengiriman melalui format dokumen di Telegram adalah cara yang paling aman dan efektif untuk menjaga kerahasiaan serta keutuhan pesan dalam teknik *steganografi* yang dapat kita lihat pada tabel 3.

Tabel 3. Hasil ekstraksi, isi pesan, dan media kirim

Hasil Ekstraksi	Isi pesan	Media kirim	Hasil Ekstraksi	Isi pesan	Media kirim
 ekstraksi .png	Ascii (readable only): Jangan L upa Data ng	Dokumen	 ekstraksi .png	Ascii (readable only): Jangan t emui say a bebera pa hari ini	Dokumen
 ekstraksi .png	Ascii (readable only): Temui sa ya di ta man	Dokumen	 ekstraksi .jpg	Ascii (readable only): $...nW.. .R..%"n. $..... ....@..V .....M.. ...'m... .. .m... ....Z. ...qU.Y. ...A...$.@..)R.Z ./...;... ?..k..@. pP...jx.	Gambar
 ekstraksi .jpg	Ascii (readable only): .....h.. .i..$.I' ..$.H..$ ..i...%% .$..H..J ~.%..... 8..... ....FIU$ ..... $.I...$. ...0.b.. ..... Z...$%.. .I$...n. ..JI.d.m	Gambar	 ekstraksi .png	Ascii (readable only): Tetap wa spada ag ar priva si pesan kamu ti dak terg anggu	Dokumen
 ekstraksi .png	Ascii (readable only): Isi pesa n ini ja ngan sam pai boco r.	Dokumen	 ekstraksi .jpg	Ascii (readable only): .8..I$m. #q...D.N ..$..(. .)m..... .....J .Uq.UI+. $.q....9 $...R$.. p..... '..U{&.. 1$.TI+b. .*.+..n. ...VG... ..H..6.. @BQUm.I.	Gambar
 ekstraksi .jpg	Ascii (readable only): ...i..pL "..V..... ..... 4..$..}' ..'Z2... c...!X?r. .....[.. .....m J.I&.... J..I\.II S.^.:3.{ h.*....!. .....Gm. ....c &X w:...?..	Gambar	 ekstraksi .png	Ascii (readable only): Simpan b ukti cha t hanya jika ben ar-benar diperlu kan	Dokumen

Hasil Ekstraksi	Isi pesan	Media kirim	Hasil Ekstraksi	Isi pesan	Media kirim
 ekstraksi .png	Ascii (readable only): Jangan s embarang an membe rikan ak ses akun chat ke orang	Dokumen	 ekstraksi .jpg	Ascii (readable only): m.I.I$.% mI$...vI $.I$.I$. ...-.k$. .I$..... @.;.@... $..I$.I$ ..@..$.$.$.p...I ....~... RI\I;.I. -.$..I\I ..... m.6.m... .mI$.I$.	Gambar
 ekstraksi.png	Ascii (readable only): Kirimi s aya alam atmu	Dokumen	 ekstraksi .png	Ascii (readable only): Hati-hat i dengan tawaran pinjama n online lewat p esan	Dokumen
 ekstraksi .jpg	Ascii (readable only):	Gambar			

Berdasarkan data hasil ekstraksi pada tabel 3. tersebut, hasil ekstraksi menunjukkan perbedaan yang signifikan antara penggunaan format file .png yang dikategorikan sebagai "dokumen" menunjukkan tingkat keberhasilan ekstraksi yang tinggi. Hal ini disebabkan oleh sifat format .png yang menggunakan kompresi *lossless*, sehingga nilai bit pada LSB tetap konsisten selama proses penyimpanan dan transmisi data. Sebaliknya, hasil ekstraksi pada format .jpg yang dikategorikan sebagai "gambar" cenderung menunjukkan karakter acak atau simbol yang tidak bermakna karena adanya kompresi data yang merusak integritas bit pesan. Fenomena ini secara teknis disebabkan oleh algoritma kompresi *lossy* pada .jpg yang melakukan kuantifisasi terhadap koefisien transformasi, sehingga menyebabkan perubahan nilai bit pada lapisan terendah yang menjadi tempat penyimpanan pesan. Kuantifikasi keberhasilan ekstraksi dapat diukur melalui perbandingan antara pesan asli dengan hasil ekstraksi. Dalam pengujian yang disajikan pada tahap I dan gambar 5., pesan asli "Jangan lupa datang" terdiri dari 18 karakter (termasuk spasi). Jika hasil ekstraksi menunjukkan teks yang sama persis tanpa ada perubahan atau kehilangan karakter, maka tingkat keberhasilan ekstraksi tersebut mencapai 100%. Akurasi yang sempurna ini membuktikan bahwa metode LSB mampu mengembalikan informasi secara utuh selama media penampungnya tidak mengalami manipulasi data. Keberhasilan ekstraksi sebesar 100% ini secara konsisten tercapai ketika file dikirim melalui fitur "kirim dokumen" di Telegram. Dokumen ini menjelaskan bahwa fitur ini menggunakan transmisi *lossless*, yang berarti setiap bit dalam file gambar dipertahankan sesuai aslinya. Karena tidak ada pergeseran atau perubahan nilai pada bit terendah, algoritma ekstraksi dapat membaca kembali urutan biner pesan rahasia dengan presisi tinggi, sehingga menghasilkan *bit error rate* (BER" sebesar 0. Sebaliknya, jika terdapat karakter yang berubah atau spasi tambahan, persentase keberhasilan akan menurun sesuai dengan jumlah karakter yang korup. Hal ini biasannya ditemukan pada pengujian dengan fitur "kirim gambar" yang melibatkan kompresi *lossy*. Kompresi tersebut merusak susunan bit pada piksel gambar, sehingga saat proses ekstraksi dilakukan, bit yang terbaca sudah tidak sinkron lagi dengan pesan asli. Berikut data hasil pengujiannya yang dapat kita lihat pada tabel 4.

Tabel 4. Hasil Pengukuran PSNR dan MSE metode LSB

Dataset	Citra Asli	Citra Kompresi	MSE (dB)	PSNR (dB)
bunga 2.bmp	819 kb	819 kb	0,0850	58,84 dB
mawar 4.png	597 kb	597 kb	0,0778	59,22 dB
ungu 7.jpg	117 kb	178 kb	1,3617	46,79 dB
merah.jpg	172 kb	1,79 mb	0,0825	58,97 dB
matahari.jpg	1,83 mb	173 kb	0,0952	58,34 dB
kuning.png	493 kb	531 kb	0,0712	59,61 dB
asoka.bmp	3,32 mb	1,61 mb	0,0821	58,99 dB
biru.bmp	3,09 mb	168 kb	0,0654	59,98 dB
aster.jpg	57,1 kb	635 kb	0,0624	60,18 dB
gunung.png	4,24 mb	439 kb	1,3289	46,89 dB
merah muda.bmp	2,32 mb	1,01 mb	0,0635	60,10 dB
anggrek.jpg	38,2 kb	53,0 kb	0,5842	50,47 dB
tulip.png	2,85 mb	3,76 mb	0,0845	58,86 dB
tunas.bmp	2,32 mb	126 kb	0,4215	51,88 dB
cantik.bmp	2,32 mb	924 kb	0,0621	60,20 dB

Berdasarkan analisis data eksperimen yang terlampir pada tabel 4. implementasi *steganografi* metode LSB menunjukkan bahwa integritas informasi yang diekstraksi sangat dipengaruhi oleh karakteristik kompresi media pembawa (*cover object*). Data menunjukkan bahwa penggunaan format citra bertipe *lossless* seperti .png dan .bmp, yang dikategorikan sebagai "dokumen" , secara konsisten menghasilkan ekstraksi pesan tekstual yang utuh dan akurat. Hal ini mengkonfirmasi bahwa skema LSB bekerja optimal pada media yang tidak mengalami modifikasi nilai piksel secara permanen, sehingga bit-bit rahasia yang disisipkan pada lapisan bit terendah dapat dipulihkan tanpa distorsi.

Sebaliknya pengujian pada format citra *lossy* seperti .jpg , yang dikategorikan sebagai "gambar" , menunjukkan penurunan performa ekstraksi yang ditandai dengan munculnya karakter acak atau simbol tidak bermakna. Secara teknis, fenomena ini berkorelasi dengan metrik kualitas citra yang tercatat dalam data penelitian, dimana dataset seperti "ungu 7.jpg" menunjukkan nilai MSE tertinggi sebesar 1,3617 dan nilai PSNR terendah sebesar 46,79 dB. Rendahnya nilai PSNR tersebut mengindikasikan adanya interferensi yang signifikan akibat proses kuantisasi pada kompresi .jpg yang mengakibatkan hilangnya sinkronisasi bit rahasia selama proses ekstraksi. Berdasarkan hasil pengujian, penelitian ini mendukung temuan sebelumnya bahwa metode LSB efektif menjaga kualitas visual citra dengan nilai PSNR yang tinggi. Namun, hasil ini juga memberikan kontribusi baru dengan membuktikan bahwa keberhasilan ekstraksi pesan di Telegram sangat bergantung pada penggunaan fitur kirim dokumen untuk menghindari kompresi sistem. Sebagai kesimpulan dari data penelitian tersebut, pemilihan format media menjadi parameter krusial dalam menentukan keberhasilan komunikasi rahasia berbasis LSB. Hasil eksperimen ini membuktikan bahwa mayoritas citra dengan nilai PSNR di atas 58 dB, seperti pada dataset "biru .bmp" dan "kuning.png" , mampu mempertahankan kualitas visual sekaligus menjamin keamanan integritas pesan. Dengan demikian, meskipun teknik LSB menawarkan kapasitas penyimpanan yang efisien, ketahanannya terhadap manipulasi format file sangat terbatas, sehingga penggunaan format non-kompresi atau *lossless* tetap menjadi syarat utama untuk menghindari kegagalan pemulihan informasi (data *loss*). Oleh karena itu, penelitian ini menyimpulkan bahwa stabilitas akurasi sangat bergantung pada pemilihan format pengiriman yang menjaga integritas data bit gambar dan jenis manipulasi atau kompresi yang diterapkan.

4. Kesimpulan dan Saran

Berdasarkan hasil penelitian yang dilakukan terkait penerapan *steganografi* metode LSB pada citra digital, dapat disimpulkan bahwa metode *Least Significant Bit* (LSB) sangat efektif dalam menyembunyikan informasi rahasia ke dalam citra digital tanpa merusak kualitas visual, dengan capaian nilai PSNR di atas 58 dB yang menjaga tampilan gambar tetap natural. Keberhasilan ekstraksi mencapai tingkat sempurna (100%) dengan *Bit Error Rate* (BER) sebesar 0, namun hal ini hanya dapat dicapai jika file dikirim melalui fitur "Kirim Dokumen" di Telegram yang bersifat *lossless*. Sebaliknya, fitur "Kirim Gambar" memicu kompresi platform yang merusak sinkronisasi bit rahasia sehingga pesan gagal diekstraksi. Dengan demikian, integritas data dalam *steganografi* LSB sangat bergantung pada pemilihan jalur transmisi yang menjaga keaslian setiap bit citra. Oleh karena itu, pemilihan teknik *steganografi* harus mempertimbangkan keseimbangan antara kerahasiaan informasi dan ketahanan terhadap pelacakan. Diperlukan pengembangan atau penelitian lanjutan guna memperkuat sistem keamanan data tanpa menurunkan kualitas tampilan gambar aslinya sehingga dapat tercipta sistem keamanan yang lebih tangguh tanpa menurunkan kualitas citra asli.

Referensi

[1] Y. B. Pratama and F. Fachri, "Analisis Keamanan Steganografi Pada Gambar Yang Diunggah Ke Media Sosia Menggunakan Least Significant Bit (LSB)," *Jurnal Mahasiswa Teknik Informatika*, vol. 9, no. 1, pp. 725–732, 2025, https://doi.org/10.36040/jati.v9i1.12370.

[2] A. Vivienne and A. K. J. Tas'an, "Analisis Kerjasama ASEAN Cybersecurity Cooperation Strategy dalam Menangani Serangan Siber di Kawasan Asia Tenggara," *Journal of International and Local Studies*, vol. 10, no. 1, pp. 25–32, 2026, https://doi.org/10.56326/jils.v10i1.5762.

[3] K. N. Limbong, Stefani, N. Atikah, S. D. Hasibuan, and Nurbaiti, "Etika Digital dan Keamanan Data salam Pemanfaatan Teknologi Informasi di Era Transformasi Digital," *Current Research on Practice Economics and Sharia Finance (CAPITAL)*, vol. 3, no. 3, pp. 6–14, 2025, https://malaqbipublisher.com/index.php/CAPITAL/article/view/872

[4] Maulidan, S. Akbar, A. Mauliyani, R. Alma, and M. F. Hasibuan, "Eksplorasi Keamanan Ganda melalui Verifikasi Dua Langkah dalam Menjaga Kerahasiaan Komunikasi Digital pada Aplikasi WhatsApp," *JIKUM: Jurnal Ilmu Komputer*, vol. 2, no. 1, pp. 26–32, 2026, https://doi.org/10.62671/jikum.v2i1.147.

[5] M. A. Firdaus and A. Rahmatulloh, "Implementasi Steganografi Citra Digital Lsb Menggunakan Enkripsi Aes-256 Dan Embedding Pseudorandom," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, pp. 411–418, 2025, https://doi.org/10.23960/jitet.v13i1.5620.

[6] F. Tambunan, Yudi, and Ratna Sri Hayati, "Penerapan Keamanan Pesan menggunakan Algoritma Triangle Chain Cipher Dan LSB Kedalam Citra RGB," *KETIK : Jurnal Informatika*, vol. 2, no. 06, pp. 15–23, 2025, https://doi.org/10.70404/ketik.v2i06.305.

[7] A. K. Siregar, M. R. Pasha, A. Asrovi, F. Rahmadayani, and M. R. Azhari, "Analisis Keamanan Layanan, Sistem Operasi, Kriptografi, dan Steganografi dalam Pengelolaan Informasi Modern," *JIKUM: Jurnal Ilmu Komputer*, vol. 2, no. 1, pp. 6–12, 2026, https://doi.org/10.62671/jikum.v2i1.139.

[8] S. L. Sari, "Implementasi Bot Telegram Berbasis PHP Untuk Pemantauan Pergerakan BITCOIN Secara Real-Time," *Seminar Nasional Informatika Bela Negara*, vol. 5, no. 2, pp. 232–236, 2025, https://santika.upnjatim.ac.id/submissions/index.php/santika/article/view/890

[9] J. W. Fathoni, N. I. ER, and I. W. Sukerayasa, "Implementasi Api Telegram Sebagai Antarmuka Manusia-Mesin Untuk Sistem Monitoring Dan Notifikasi Kondisi Real-Time Infrastruktur Publik," *Jurnal SPEKTRUM*, vol. 12, no. 3, pp. 12–20, 2025, https://doi.org/10.24843/SPEKTRUM.2025.v12.i03.p2.

[10] I. Utami, S. Destya, and M. K. Putro, "Peningkatan Steganografi DCT pada JPEG menggunakan Adaptive LSB Matching untuk Resistensi Deteksi Entropi," *Jurnal Sistem Informasi*, vol. 15, no. 3, pp. 886–895, 2026, https://doi.org/10.32520/stmsi.v15i3.6002.

[11] P. Kusuma and Y. Prayudi, "Implementasi Steganografi Dengan Menggunakan Metode Masking And Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram," *Ajie*, vol. 9, no. 1, pp. 1–53, 2025, https://doi.org/10.20885/ajie.vol9.iss1.art1.

[12] A. D. S. De Yosep, S. Y. Doo, and M. O. Odja, "Perancangan Gui Matlab Untuk Keamanan Citra RGB Menggunakan Algoritma ACM Dan Metode LSB Dalam Berbagai Ukuran," *Jurnal Sistem Informasi dan Teknologi Komputasi*, vol. 2, no. 2, pp. 51–56, 2025, https://doi.org/10.61124/sinta.v2i2.45.

[13] R. A. Akmal, Mhd. F. Furqan, and R. Kurniawan R, "Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital," *G-Tech: Jurnal Teknologi Terapan*, vol. 7, no. 2, pp. 543–553, 2023, https://doi.org/10.33379/gtech.v7i2.2300.

[14] A. R. Mido and E. I. H. Ujianto, "Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA Dan Steganografi LSB," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 2, pp. 279–286, 2022, https://doi.org/10.25126/jtiik.202294852.

[15] K. Azra, B. Pramono, and Sutardi, "Implementasi Algoritma Huffman Coding Dan Metode Steganografi Least Significant Bit (LSB) Untuk Pengamanan Pesan Teks Pada Berkas Audio WAV," *ANIMATOR*, vol. 3, no. 1, pp. 27–34, 2025, https://animator.uho.ac.id/index.php/journal/article/view/1246

[16] M. Ilham and C. Kirana, "Perbandingan Kualitas Citra Grayscale Steganografi Metode LSB Dan DCT Berdasarkan PSNR Dan SSIM," *JOISM*, vol. 7, no. 2, pp. 330–337, 2026, https://doi.org/10.24076/joism.2026v7i2.2492.