JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Tinjauan Literatur: Evaluasi Metode Least Significant Bit (LSB) dalam Steganografi Berdasarkan Alasan Penggunaan dan Efektivitasnya terhadap Keamanan Data Digital

Hadaya Imtiyaza Syarifa [1*], Livia Febriati [2], Vannianti Nabilla Putri [3]
[1,2,3]Universitas Amikom Purwokerto, Indonesia
[1*]hadayaimtiyaza08@email.com, [2]liviafebyy@email.com, [3]vanniantinabilla06@email.com

ABSTRACT

The rapid development of information technology has facilitated the exchange of digital data, but it has also given rise to various threats to information security. Steganography is one technique used to hide confidential data, with the Least Significant Bit (LSB) method being the most widely used approach due to its simplicity. This article aims to evaluate the reasons for using the LSB method in steganography, its weaknesses, and its effectiveness in digital data security. This study uses the Systematic Literature Review (SLR) method by reviewing relevant scientific articles obtained through the Google Scholar database. The literature selection process was carried out systematically using the PRISMA protocol. The results of the study show that the LSB method is widely used because of its ease of implementation, processing speed, adequate insertion capacity, and ability to maintain the visual quality of the disguised image. However, this method has limitations, particularly low resistance to noise, lossy compression, image manipulation, and steganalysis attacks when used alone. Therefore, the LSB method is considered quite effective for visual concealment, but it needs to be combined with additional security techniques to improve digital data security.

Keywords:
Steganography, Least Significant Bit, Data Security, Systematic Literature Review, Digital Data Security.

PENDAHULUAN

Pada era digital seperti sekarang ini, teknologi informasi dan komunikasi berkembang dengan cepat, hal tersebut menjadikan pertukaran data-data digital semakin cepat dan mudah. Akan tetapi, dari kemudahan tersebut juga dapat menimbulkan berbagai permasalahan baru, terutama dalam aspek keamanan informasi data. Ancaman seperti penyadapan, manipulasi informasi, serta pencurian data sekarang marak terjadi melalui jaringan publik. Maka dari itu, keamanan data merupakan hal yang sangat penting untuk memastikan dalam menjaga kerahasiaan dan integritas pesan yang dikirim antar pengguna (Mohan & Saini, 2023; Zhao & Gao, 2024).

Salah satu teknik yang sering dipakai untuk menjaga keamanan data adalah dengan menggunakan steganografi. Steganografi merupakan salah satu metode yang dapat digunakan untuk menjaga kerahasiaan dan keamanan informasi penting maupun pribadi. Istilah steganografi sendiri berasal dari bahasa Yunani, yaitu "steganos" yang berarti menyembunyikan atau menutupi, serta "graphein" yang berarti menulis. Dengan demikian, steganografi dapat diartikan sebagai teknik untuk menyisipkan pesan ke dalam data lain tanpa menyebabkan perubahan yang terlihat pada data tersebut, sehingga data sebelum dan sesudah penyisipan tetap tampak serupa (Syawal et al., 2016).

Steganografi adalah bidang ilmu yang mempelajari cara menyembunyikan informasi rahasia dalam informasi lainnya. Sejarah steganografi hampir sama dengan kriptografi, keduanya sering digunakan pada masa perang (Syahril & Jaya, 2019).

Perkembangan teknologi yang pesat membuat pertukaran informasi lebih mudah, tetapi juga meningkatkan risiko terhadap keamanan data. Oleh karena itu, steganografi penting untuk menyembunyikan dan melindungi data, terutama dengan menggunakan algoritma ***Least Significant Bit (LSB)***. Algoritma ini bekerja dengan mengganti bit paling tidak signifikan dari piksel citra dengan bit data rahasia, sehingga kualitas gambar tidak berubah banyak (Prayogo et al., 2024).

Salah satu metode paling popular dalam Steganografi adalah ***Least Significant Bit (LSB).*** Cara kerja metode ini adalah dengan mengganti bit yang tidak signifikan dari setiap piksel citra dengan bit pesan rahasia. Teknik ini banyak digunakan karena prosesnya sederhana, cepat, dan perubahan yang terjadi sangat kecil, sehingga sulit terdeteksi (Ramadhani & Hasanuddin, 2021). Namun, metode LSB memiliki kekurangan. Salah satu kekurangan tersebut adalah metode ini rentan terhadap *noise* dan teknik kompresi (Joshi et al., 2013). Selain itu, kelemahan ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan berbagai jenis serangan, seperti *statistical attack* dan *visual attack* (Rantelinggi & Saputra, 2020). Metode LSB memiliki kelemahan besar ketika digunakan pada gambar yang memiliki format kompresi *lossy*, seperti JPEG. Kompresi *lossy* biasanya mengubah nilai bit-bit terakhir dari setiap piksel yang digunakan untuk menyembunyikan data, sehingga berpotensi merusak pesan yang disembunyikan (Wildan & Ashari, 2024).

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

KAJIAN LITERATUR

Tujuan tinjauan literatur ini adalah untuk menganalisis alasan penggunaan, kelemahan, dan efektivitas metode *Least Significant Bit (LSB)* dalam steganografi sebagai teknik untuk menjaga keamanan informasi digital. Melalui studi ini, diharapkan faktor-faktor yang membuat metode LSB banyak digunakan dan dapat dipahami, yaitu kemudahan penerapan, proses yang cepat, dan fakta bahwa perubahan yang dihasilkannya sulit dideteksi dari data asli. Di lain sisi, tinjauan ini juga bertujuan untuk mengidentifikasi kelemahan metode LSB, seperti resistansi yang rendah terhadap gangguan *(noise)*, proses kompresi, dan serangan potensial yang dapat mengungkap data tersembunyi. Secara keseluruhan, penelitian ini bertujuan untuk mengevaluasi sejauh mana metode LSB efektif dalam menjaga kerahasiaan dan kualitas media yang digunakan sebagai tempat penyisipan pesan rahasia.

METODE PENELITIAN

Penelitian ini menggunakan metode *Sytematic Literature Review (SLR)* untuk mengumpulkan dan menganalisis berbagai hasil penelitian sebelumnya tentang penerapan metode *Least Significant Bit (LSB)* dan steganografi, sehingga penulis dapat memperoleh kesimpulan terkait efektivitas dan kelemahannya terhadap keamanan digital. Tujuan utama dari metode Systematic Literature Review (SLR) adalah untuk menemukan dan menguraikan teori-teori yang relevan dengan konteks penelitian serta mengembangkan strategi yang dapat digunakan untuk memecahkan masalah penelitian.

Permasalahan yang akan diangkat pada penelitian ini merupakan alasan, efektivitas dan kelemahan pada penggunaan steganografi dengan metode Least Significant Bit (LSB). Tinjauan literatur ini disusun dengan tujuan untuk menjawab sejumlah pertanyaan penelitian, yaitu:

RQ1: Alasan mengapa banyak pengguna memilih metode LSB dalam steganografi untuk keamanan digital?
RQ2: Kelemahan apa saja yang ada pada metode LSB?
RQ3: Seberapa efektif metode LSB dalam melindungi data digital dari serangan?

Mengidentifikasi atau mencari literatur yang membahas tentang jurnal dan artikel yang dicari secara relevan menggunakan database-database yang tersedia seperti Google Scholar, dan Scopus (Habibi & Manurung, 2023).

Proses seleksi literatur dalam penelitian ini dilakukan secara sistematis dengan mengadopsi protokol PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) untuk menjamin akuntabilitas dan replikasi studi. Implementasi alur PRISMA mencakup empat tahapan krusial sebagai berikut:

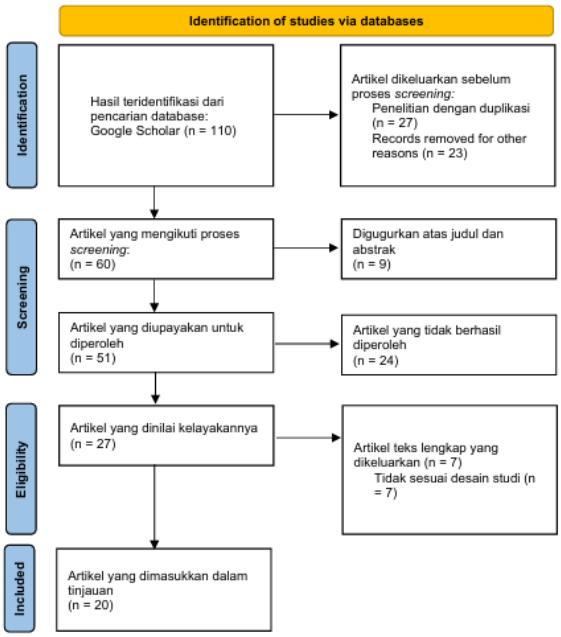
Identifikasi: Tahap awal melibatkan pencarian literatur secara komprehensif pada pangkalan data digital seperti Google Scholar untuk menemukan artikel yang relevan dengan steganografi LSB.

Skrining: Artikel-artikel yang ditemukan melalui pencarian awal kemudian diseleksi berdasarkan judul dan abstrak guna mengeliminasi literatur yang tidak memiliki korelasi langsung dengan evaluasi efektivitas metode LSB.

Kelayakan (Eligibility): Teks lengkap (full-text) dari artikel yang lolos tahap skrining dikaji secara mendalam untuk memastikan data tersebut mampu menjawab pertanyaan penelitian (RQ1, RQ2, dan RQ3) yang telah ditetapkan.

Inklusi: Literatur yang memenuhi seluruh kriteria kelayakan kemudian ditetapkan sebagai basis data utama untuk dianalisis lebih lanjut dalam proses sintesis hasil dan pembahasan.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026



Gambar 1. Diagram Alir Prisma

HASIL DAN PEMBAHASAN

Alasan Penggunaan Metode LSB Pada Steganografi

Metode Least Significant Bit (LSB) merupakan teknik fundamental dalam steganografi domain spasial yang menjadi pilihan utama bagi banyak peneliti dan pengguna dalam konteks keamanan data digital. Berdasarkan tinjauan literatur yang komprehensif, alasan utama pemilihan metode LSB dapat dikelompokkan ke dalam tiga aspek kunci, yaitu tingkat imperseptibilitas, kemudahan implementasi, dan kapasitas penyisipan yang memadai.

Aspek pertama dan paling krusial adalah kemampuan metode LSB dalam mempertahankan kualitas visual media penyamar (cover media), khususnya citra digital. Perubahan yang dilakukan oleh metode LSB, yaitu dengan mengganti bit paling tidak signifikan pada piksel citra, hanya menyebabkan perbedaan nilai warna yang sangat kecil sehingga tidak terdeteksi secara visual oleh mata manusia (Wati et al., 2020; Wibisono et al., 2020). Kualitas citra yang tetap terjaga atau tidak mengalami perubahan signifikan setelah penyisipan pesan merupakan indikator keberhasilan steganografi itu sendiri (Sidiq et al., 2023). Hal ini didukung oleh fakta bahwa metode LSB hanya memengaruhi bit dengan bobot terendah, sehingga hasil stego-image menjadi sulit untuk dideteksi (Ramadhani & Hasanuddin, 2021; Yusup et al., 2020).

Secara kuantitatif, berbagai penelitian menunjukkan bahwa implementasi metode LSB menghasilkan nilai Peak Signal-to-Noise Ratio (PSNR) yang tinggi dan berada pada kategori baik. Nilai PSNR yang tinggi menegaskan bahwa stego-image memiliki kualitas visual yang hampir identik dengan citra asli (Al Akbar et al., 2024; Prayogo et al., 2024; Santoso et al., 2022). Selain itu, hasil PSNR yang baik juga ditunjukkan dalam penelitian (Ramadhani & Hasanuddin, 2021). Oleh karena itu, metode LSB banyak digunakan dalam image steganography karena kemampuannya dalam menjaga kualitas visual media penyamar (Prayogo et al., 2024).

Aspek kedua yang mendukung penggunaan metode LSB adalah kemudahan dan efisiensi dalam implementasinya. Metode LSB dikenal sebagai teknik paling sederhana dalam steganografi domain spasial (Sulistyo & Aribowo, 2020) serta merupakan metode paling dasar dalam keseluruhan kajian steganografi (Wibisono et al., 2020). Kesederhanaan tersebut menjadikan metode LSB mudah diterapkan (Hasan et al., 2020; Rizqa et al., 2022; Wibisono et al., 2020), dengan proses penyisipan pesan yang relatif cepat (Wibisono et al., 2020). Selain itu, metode LSB memungkinkan proses penyisipan data dilakukan dengan cara yang sederhana dan efisien (Rantelinggi & Saputra, 2020).

Aspek ketiga adalah kapasitas penyisipan (payload). Metode LSB menawarkan keunggulan dalam menyembunyikan data dalam jumlah yang relatif lebih besar dibandingkan metode steganografi lainnya (Mido & Ujianto, 2022), yaitu hingga sekitar 1/8 dari total ukuran citra (Wibisono et al., 2020). Kemudahan implementasi yang dipadukan dengan kapasitas penyisipan yang memadai menjadikan metode LSB sering digunakan sebagai benchmark dalam pengembangan teknik steganografi.

Secara keseluruhan, tingginya penggunaan metode LSB dalam keamanan data digital didorong oleh kombinasi antara tingkat imperseptibilitas visual yang sangat baik serta algoritma yang sederhana, cepat, dan mudah

diimplementasikan, sehingga menjadikannya solusi data hiding yang efektif dari sisi implementasi dan kualitas stego-image.

Kelemahan apa saja yang ada pada metode LSB?

Metode Least Significant Bit (LSB) merupakan teknik steganografi domain spasial yang banyak digunakan karena kesederhanaan dan kemudahan implementasinya. Namun, berdasarkan hasil tinjauan literatur, metode LSB juga memiliki beberapa kelemahan yang perlu diperhatikan dalam penerapannya. Kelemahan metode LSB dibagi menjadi beberapa aspek. Mulai dari rendahnya tingkat robustness terhadap gangguan, keterbatasan ketahanan terhadap manipulasi citra, serta rendahnya tingkat keamanan apabila digunakan secara tunggal tanpa kombinasi metode pengamanan lain.

Aspek pertama yang menjadi kelemahan metode LSB adalah robustness terhadap gangguan. Metode Least Significant Bit (LSB) menyisipkan pesan dengan memodifikasi bit paling tidak signifikan pada setiap piksel citra digital (Sulistyo & Aribowo, 2020). Metode ini bekerja pada domain spasial dengan memanfaatkan perubahan nilai bit paling rendah yang tidak terlihat secara visual (Wibisono et al., 2020). Kondisi ini menunjukkan bahwa metode LSB memiliki keterbatasan dalam mempertahankan integritas pesan ketika citra mengalami gangguan.

Aspek kedua berkaitan keamanan terhadap pendeteksian pesan tersembunyi terhadap serangan steganalisis. Penyisipan pesan menggunakan metode LSB dilakukan secara langsung pada nilai piksel citra dengan memodifikasi bit paling tidak signifikan (Yusup et al., 2020). Proses penyisipan pada domain spasial tersebut tidak terlalu memengaruhi karakteristik statistik citra (Ramadhani & Hasanuddin, 2021). Berdasarkan karakteristik tersebut, keberadaan pesan tersembunyi berpotensi dianalisis dengan melakukan pendekatan statistik sederhana sehingga tingkat keamanan metode LSB terhadap deteksi masih memiliki keterbatasan.

Aspek ketiga yang menjadi kelemahan metode LSB adalah rendahnya ketahanan terhadap manipulasi citra. Ketergantungan terhadap struktur piksel menyebabkan perubahan citra seperti resizing, cropping, atau pengolahan ulang citra dapat memengaruhi bit LSB yang menyimpan pesan (Wibisono et al., 2020). Akibatnya, pesan yang disisipkan berpotensi mengalami kerusakan atau hilang setelah citra dimodifikasi.

Selain itu, metode LSB juga memiliki kelemahan dari aspek keamanan penggunaan metode secara tunggal. Kesederhanaan mekanisme penyisipan tersebut menyebabkan proses ekstraksi pesan dapat dilakukan dengan relatif mudah apabila teknik yang digunakan diketahui (Wibisono et al., 2020). Oleh karena itu, penggunaan metode LSB secara tunggal memiliki keterbatasan dari sisi keamanan dan memerlukan teknik pengamanan tambahan.

Secara keseluruhan, metode Least Significant Bit (LSB) memiliki beberapa kelemahan dalam penerapannya pada keamanan data digital, terutama rendahnya ketahanan terhadap noise, kompresi, dan manipulasi citra, serta kerentanannya terhadap deteksi pesan tersembunyi. Selain itu, penggunaan metode LSB secara tunggal dinilai kurang aman karena proses ekstraksi pesan relatif mudah apabila teknik yang digunakan diketahui. Oleh karena itu, metode LSB lebih efektif jika dilakukan kombinasi teknik pengamanan tambahan untuk meningkatkan tingkat keamanan data yang disisipkan.

Seberapa efektif metode LSB dalam melindungi data digital dari serangan?

Berdasarkan hasil tinjauan literatur, efektivitas metode Least Significant Bit (LSB) dalam melindungi data digital dari serangan dapat dikategorikan sebagai cukup efektif dalam scenario tertentu, namun masih memilliki keterbatasan apabila digunakan sebagai mekanisme pengamanan tunggal. Dalam konteks steganografi modern, efektifitas metode LSB dinilai dari kemampuannya menyamarkan keberadaan pesan serta mempertahankan data tersembunyi ketika menghadapi upaya pendeteksian atau manipulasi oleh pihak tidak berwenang.

Sejumlah penelitian menyatakan bahwa metode LSB masih efektif dalam menghadapi pengamatan visual langsung, karena perubahan bit paling tidak signifikan tidak menimbulkan perbedaan visual yang mencolok pada citra digital (Ramadhani & Hasanuddin, 2021; Yusup et al., 2020). Kondisi ini menunjukan bahwa dalam lingkungan dengan tingkat ancaman rendah, metode LSB mampu menyembunyikan keberadaaan pesan secara visual dan tetap menjaga kualitas media penyamar. Oleh karena itu, efektivitas metode LSB pada aspek penyamaran visual masih dinilai memadai. Namun demikian, beberapa penelitian terkini menunjukan bahwa efektivitas metode LSB meurun ketika dihadapkan pada serangan steganalysis dan manipulasi citra. (Rantelinggi & Saputra, 2020) menyatakan bahwa pola penyisipan LSB yang relative sederhana dapat dianalisis menggunakan pendekatan statistik tertentu, sehingga keberadaan pesan tersembunyi berpotensi terdeteksi. Selain itu, (Prayogo et al., 2024) mengungkapkan bahwa proses kompresi dan pengolahan ulang citra dapat memengaruhi bit-bit LSB yang menyimpan pesan, sehingga berdampak pada keberlangsungan data tersembunyi.

Temuan ini menunjukan bahwa efektivitas metode LSB terhadap serangan aktif masih memiliki keterbatasan. Untuk meningkatkan efektivitas perlindungan data digital, beberapa penelitian merekomendasikan penguatan metode LSB melalui kombinasi teknik tambahan. (Ramadhani & Hasanuddin, 2021) menunjukan bahwa modifikasi pola penyisipan LSB dapat meningkatkan ketahanan terhadap pendeteksian sederhana. Sementara itu, (Rantelinggi & Saputra, 2020) menegaskan bahwa penggabungan metode LSB dengan algortima kriptografi mampu meningkatkan

efektivitas perlindungan data, karena meskipun pesan berhasil diekstraksi, isi pesan tetap tidak dapat dipahami tanpa kunci deskripsi. Secara keseluruhan, metode Least Significant Bit (LSB) dinilai cukup efektif dalam menyamarkan data digital dari pengamatan langsung, namun belum sepenuhnya efektif dalam menghadapi serangan steganalisis dan manipulasi citra apabila digunakan secara tunggal. Efektivitas metode ini meningkatkan secara signifikan apabila dikombinasikan dengan teknik modifikasi penyisipan atau kriptografi. Oleh karena itu, metode LSB lebih tepat digunakan sebagai komponen pendukung dalam sistem keamanan steganografi, bukan sebagai satu-satunya mekanisme perlindungan data digital dari serangan.

KESIMPULAN

Berdasarkan hasil analisis sistematis terhadap berbagai literatur yang relevan, dapat ditarik kesimpulan bahwa metode Least Significant Bit (LSB) tetap memegang posisi sebagai teknik fundamental yang paling unggul dalam ranah steganografi domain spasial, khususnya pada aspek imperseptibilitas visual dan efisiensi komputasi. Kemampuan algoritma ini dalam menjaga kualitas citra pembawa (stego-image) telah teruji secara empiris melalui pencapaian nilai Peak Signal-to-Noise Ratio (PSNR) yang tinggi, yang mengindikasikan bahwa perubahan bit pada level terendah hampir tidak mungkin terdeteksi oleh persepsi visual manusia. Karakteristik utama lainnya yang menjadikan LSB sebagai standar acuan dalam penyembunyian data digital adalah kemudahan implementasinya serta kapasitas payload yang relatif besar, yakni mencapai 1/8 dari dimensi total citra asli.

Namun demikian, kajian ini juga berhasil memetakan sejumlah keterbatasan kritis yang menjadi kelemahan fundamental metode LSB. Penelitian menunjukkan adanya kerentanan yang signifikan terhadap aspek ketahanan (robustness) saat menghadapi manipulasi eksternal. Metode ini terbukti sangat sensitif terhadap gangguan noise, serangan steganalisis berbasis statistik, serta prosedur kompresi lossy seperti format JPEG yang secara langsung dapat merusak integritas pesan tersembunyi di dalam bit-bit tidak signifikan tersebut. Oleh karena itu, penerapan metode LSB secara mandiri atau tunggal tanpa adanya modifikasi protokol tambahan membawa risiko keamanan yang tinggi, mengingat mekanisme ekstraksi informasinya yang cenderung transparan bagi pihak-pihak yang memiliki pengetahuan teknis terkait steganografi.

Secara praktis, temuan ini memberikan panduan strategis bagi para praktisi keamanan informasi untuk tidak memposisikan LSB sebagai satu-satunya garda perlindungan dalam transmisi data rahasia. Manfaat utama dari evaluasi ini adalah mempertegas bahwa efektivitas perlindungan informasi digital akan meningkat secara eksponensial hanya jika metode LSB diintegrasikan dengan teknik pengamanan komplementer.

REFERENSI

Al Akbar, A., Sumadi, M. T., & Faldi, F. (2024). Implementation of Lsb and Playfair Methods To Secure Text Files Into Wav Audio Files. *Jurnal Teknik Informatika (Jutif)*, *5*(6), 1529–1537. https://doi.org/10.52436/1.jutif.2024.5.6.1793

Habibi, R., & Manurung, A. G. R. (2023). SLR Systematic Literature Review: Metode Penilaian Kinerja Karyawan Menggunakan Human Performance Technology. *Journal of Applied Computer Science and Technology*, *4*(2), 100–107. https://doi.org/10.52158/jacost.v4i2.511

Hasan, N. F., Dengen, C. N., & Ariyus, D. (2020). Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *11*(1), 20–29. https://doi.org/10.31849/digitalzone.v11i1.3413

Joshi, R., Gagnani, L., & Pandey, S. (2013). Image Steganography With LSB. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(1), 228–229.

Mido, A. R., & Ujianto, E. I. H. (2022). ANALISIS PENGARUH CITRA TERHADAP KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *9*(2), 279–286.

Mohan, K. J., & Saini, A. K. (2023). Assessing Information Security Governance in Public Sector Banks of India. *International Journal of Engineering Technology and Management Sciences*, *7*(5), 103–116. https://doi.org/10.46647/ijetms.2023.v07i05.012

Prayogo, A. I., Nugraha, A., Novanto, T. F., & Kurniawan, J. C. (2024). Enhancing Least Significant Bit Steganography Image Fidelity Using Brotli Compression. *Sinkron*, *9*(1), 285–295. https://doi.org/10.33395/sinkron.v9i1.13186

Ramadhani, A. M., & Hasanuddin, T. (2021). Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography. *Indonesian Journal of Data and Science (IJODAS)*, *2*(2), 91–102. https://doi.org/10.56705/ijodas.v2i3.48

Rantelinggi, P. H., & Saputra, E. (2020). Algoritma Kriptografi Triple Des dan Steganografi LSB sebagai Metode Gabungan dalam Keamanan Data. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(4), 661–666. https://doi.org/10.25126/jtiik.2020741838

Rizqa, I., Safitri, A. N., & Harkespan, I. (2022). Kriptostegano Menggunakan Data Encryption Standard dan Least

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Significant Bit dalam Pengamanan Pesan Gambar. *Jurnal Masyarakat Informatika*, *13*(2), 111–120. https://doi.org/10.14710/jmasif.13.2.44547

Santoso, K. A., Wiraga, A. T., & Riski, A. (2022). Penyembunyian Pesan Terenkripsi pada Citra menggunakan Algoritma LSB dan Transposisi Kolom. *Journal of Applied Informatics and Computing*, *6*(1), 25–30. https://doi.org/10.30871/jaic.v6i1.3819

Sidiq, R. F., Rahayu, R. E. G., & Supriatna, A. D. (2023). Implementasi Kriptografi Advanced Encryption Standard dan Least Significant Bit untuk Keamanan Pesan Email dalam Gambar. *Jurnal Algoritma*, *20*(2), 305–315. https://doi.org/10.33364/algoritma/v.20-2.1407

Sulistyo, I., & Aribowo, E. (2020). Implementasi Algoritma Hybrid dan Metode Least Significant Bit Untuk Keamanan Data. *Jurnal Informatika: Jurnal Pengembangan IT*, *5*(3), 70–76. https://doi.org/10.30591/jpit.v5i3.2050

Syahril, M., & Jaya, H. (2019). Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4. *Sensasi*, 505–509. http://prosiding.seminar-id.com/index.php/sensasi/issue/archivePage%7C505

Syawal, M. F., Fikriansyah, D. C., & Agani, N. (2016). Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB. *Jurnal TICOM*, *4*(3), 91–99. https://www.neliti.com/publications/93707/

Wati, V., Sa'diyah, H., & Ariyus, D. (2020). Pendekatan Stego-Kripto Mode Cipher Block Chaining Untuk Pengamanan Informasi Pada Citra Digital. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *5*(2), 197–204. https://doi.org/10.33480/jitk.v5i2.1160

Wibisono, G., Waluyo, T., & Ujianto, E. I. H. (2020). Kajian Metode Metode Steganografi Pada Domain Spasial. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *5*(2), 259–264. https://doi.org/10.33480/jitk.v5i2.1212

Wildan, M., & Ashari, W. M. (2024). Text Data Security Using LCG and CBC with Steganography Technique on Digital Image. *Journal of Applied Informatics and Computing*, *8*(2), 400–407. https://doi.org/10.30871/jaic.v8i2.8457

Yusup, I. M., Carudin, C., & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. *Jurnal Teknik Informatika Dan Sistem Informasi*, *6*(3), 434–441. https://doi.org/10.28932/jutisi.v6i3.2817

Zhao, D., & Gao, Y. (2024). Information Security and Privacy Protection Strategies in the Process of Electronic Archiving. *Journal of Electrical Systems*, *20*(6s), 374–380. https://doi.org/10.52783/jes.2658