

Pengembangan Aplikasi Steganografi Multiformat untuk Penyisipan Data pada Media Citra, Audio, dan Dokumen Digital

Tri Mayluddin Villanda^{1*}, Kelvin Alfarezy², Riski Agustio³, M. Alisud Nasution⁴

^{1,2,3,4}Program Studi Teknik Informatika, Fakultas Teknik, Universitas Malikussaleh, Indonesia

¹tri.230170114@mhs.unimal.ac.id, ²kelvin.230170195@mhs.unimal.ac.id, ³riski.230170056@mhs.unimal.ac.id,

⁴alisud.230170119@mhs.unimal.ac.id

ABSTRACT

Information security has become a critical issue in modern digital communication, especially with the massive exchange of multimedia data across open networks. Cryptography is widely used to protect message content; however, encrypted data often attracts attention and may raise suspicion. Steganography provides an alternative approach by concealing secret data within digital media in an imperceptible manner. This study aims to develop a multiformat steganography application capable of embedding and extracting confidential data in images, audio files, and digital documents. The proposed system supports image-based least significant bit (LSB) techniques, audio LSB embedding, and document-based methods using metadata and zero-width characters. The application is implemented using Python and designed with a modular architecture to ensure extensibility and usability. Experimental results show that the application successfully embeds and extracts hidden messages across all supported media formats without causing noticeable degradation in media quality. The findings demonstrate that multiformat steganography can enhance information security by providing flexible and covert data-hiding capabilities suitable for various digital communication scenarios.

Keywords:

steganography, information security, multimedia, data hiding, multiformat

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah meningkatkan volume pertukaran data digital secara eksponensial di seluruh dunia, termasuk Indonesia, sehingga memperluas ruang ancaman terhadap keamanan informasi (Halim & Lestari, n.d.). Pesan digital yang disampaikan melalui berbagai media seperti citra, audio, serta dokumen elektronik kini menjadi sasaran serangan dan pemantauan yang semakin canggih (Eka et al., 2025). Untuk melindungi data sensitif, berbagai teknik kriptografi telah diterapkan, namun kriptografi tradisional hanya menyamarkan isi pesan tanpa menyembunyikan keberadaannya secara keseluruhan, sehingga masih dapat terdeteksi melalui analisis lalu lintas informasi (Gusti et al., 2024).

Steganografi menyajikan pendekatan alternatif untuk keamanan data dengan menyembunyikan keberadaan pesan rahasia di dalam media penampung sehingga pesan menjadi tidak terlihat oleh pihak luar yang tidak berwenang (Rohayah, 2023). Teknik steganografi membawa pesan tersembunyi tanpa memodifikasi arti atau fungsi media secara signifikan, sehingga menghasilkan stego-media yang tampak sama seperti aslinya (Ardiansyah et al., n.d.). Studi di bidang steganografi menunjukkan bahwa konsep ini telah diterapkan dalam berbagai bentuk media digital, namun masih terbatas pada satu format media tertentu, terutama citra (Kusuma & Prayudi, 2025)(Luthfi & Jamarun, 2025).

Pendekatan yang hanya berfokus pada satu media berpotensi mengalami keterbatasan praktis dan teknis, terutama ketika steganalisis yang ditujukan terhadap media tersebut berkembang (Hajar Akbar, 2024). Hal ini menimbulkan kebutuhan akan steganografi yang lebih fleksibel dan adaptif terhadap beragam media, sehingga mampu merespons dinamika komunikasi digital multimodal yang semakin kompleks (Walad, 2025). Selain itu, kajian steganografi pada dokumen digital seperti PDF dan format teks modern masih relatif terbatas, padahal dokumen ini merupakan bagian penting dalam komunikasi formal dan institusional (Padmaja et al., n.d.).

Oleh karena itu, penelitian ini mengusulkan pengembangan steganografi multiformat untuk memperluas cakupan teknik penyisipan data tersembunyi pada berbagai media digital yang beragam, sekaligus mempertimbangkan aspek kemampuan adaptasi dan integrasi dalam satu kerangka aplikasi yang terpadu (Ishtiaq et al., 2025). Dengan demikian, penelitian ini bertujuan untuk mengembangkan aplikasi steganografi multiformat yang mampu menyisipkan serta mengekstrak pesan rahasia pada media citra, audio, dan dokumen dengan kualitas stego-media yang tetap imperceptible dan stabil.

KAJIAN LITERATUR

Steganografi merupakan teknik keamanan informasi yang berorientasi pada penyamaran keberadaan pesan rahasia di dalam media digital, dengan tiga prinsip utama yaitu kapasitas penyisipan, imperceptibility, dan ketahanan

terhadap manipulasi (robustness) (Izzul Haziq Rahim et al., 2025). Teknik steganografi telah berkembang dari metode tradisional seperti Least Significant Bit (LSB) hingga metode hybrid yang menggabungkan kriptografi dan steganografi untuk meningkatkan tingkat keamanan dan kapasitas penyisipan (Slb Steganography et al., 2025)(Karo et al., 2025).

Dalam domain steganografi citra digital, penelitian di Indonesia menunjukkan berbagai variasi metode penyisipan seperti kombinasi kriptografi AES dengan LSB yang menghasilkan kualitas visual yang tetap tinggi serta meningkatkan ketahanan stego terhadap deteksi. Penerapan steganografi pada konten gambar untuk pengamanan hak cipta di media sosial juga menunjukkan efektivitas tinggi pada skenario nyata komunikasi visual. Implementasi metode LSB pada format gambar modern juga menghasilkan keberhasilan penyisipan data dengan tingkat keberhasilan yang signifikan.

Berbagai teknik lain juga telah diterapkan pada steganografi audio, termasuk metode spread spectrum yang efektif menyembunyikan pesan pada file MP3 tanpa mengurangi kualitas suara, serta teknik evaluasi performa *improved spread spectrum* untuk audio coding yang menunjukkan peningkatan daya tahan terhadap gangguan (Firdaus et al., 2025). Selain itu, implementasi steganografi audio menggunakan metode masking dan filtering juga menunjukkan bahwa pesan tersembunyi dapat disisipkan pada spektrum audio dengan stabilitas yang baik.

Dalam konteks steganografi dokumen dan teks, teknik berbasis karakter tanpa lebar (*zero-width characters*) telah dikembangkan untuk meningkatkan kapasitas penyisipan pada teks digital tanpa mengubah tampilan visualnya (K & Tajuddin, 2022). Pendekatan ini meningkatkan kemampuan penyisipan dan mempertahankan tingkat imperceptibility yang tinggi dibandingkan dengan teknik steganografi teks klasik.

Selain itu, kombinasi steganografi dengan kriptografi pada citra digital berbasis metode LSB dan enkripsi juga telah dieksplorasi untuk meningkatkan kerahasiaan pesan sebelum disisipkan, memperluas kerangka aplikasi steganografi dalam skenario keamanan yang lebih kompleks.

Kajian literatur juga menunjukkan bahwa pengembangan steganografi multiformat semakin menarik perhatian peneliti, terutama dalam upaya menyatukan teknik yang berbeda untuk menghadapi beragam skenario ancaman digital (Dashtaki & Ghaemmaghami, 2025). Namun, meskipun banyak kemajuan pada penelitian monomedia, masih terdapat kesenjangan dalam penerapan teknik terintegrasi yang mampu memenuhi kebutuhan keamanan lintas media sekaligus mempertahankan kualitas stego pada tiap format.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan pendekatan rekayasa perangkat lunak (software engineering) untuk merancang, mengimplementasikan, dan mengevaluasi sebuah aplikasi steganografi multiformat. Pendekatan ini dipilih karena penelitian tidak hanya berfokus pada analisis teoritis, tetapi juga pada pembangunan sistem yang dapat diuji secara fungsional dan empiris melalui serangkaian eksperimen terkontrol.

Desain dan Arsitektur Sistem

Sistem steganografi dirancang menggunakan arsitektur modular untuk meningkatkan keterpisahan fungsi (separation of concerns), kemudahan pemeliharaan, serta kemungkinan pengembangan lanjutan. Arsitektur sistem terdiri dari beberapa modul utama, yaitu:

1. Modul Antarmuka Pengguna, yang berfungsi sebagai penghubung antara pengguna dan sistem untuk pemilihan media, input pesan rahasia, serta pengaturan proses penyisipan dan ekstraksi;
2. Modul Penyisipan Data, yang menangani proses encoding pesan rahasia ke dalam media penampung sesuai dengan jenis media dan teknik steganografi yang diterapkan;
3. Modul Ekstraksi Data, yang bertugas melakukan decoding pesan rahasia dari media stego;
4. Modul Manajemen Media, yang mengelola validasi format file, pembacaan dan penulisan media, serta penyimpanan hasil proses steganografi.

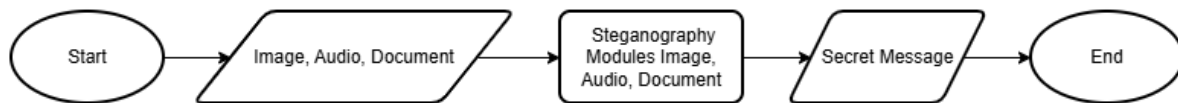
Pendekatan modular ini memungkinkan setiap jenis media (citra, audio, dan dokumen) diproses menggunakan mekanisme yang sesuai dengan karakteristik strukturnya, tanpa saling bergantung secara langsung.

Alur Proses Penyisipan Data dan Ekstraksi Data

Alur kerja sistem steganografi mencakup proses penyisipan dan ekstraksi data yang dirancang secara terpadu dalam satu mekanisme berurutan. Proses diawali dengan pemilihan media penampung oleh pengguna melalui antarmuka aplikasi, kemudian sistem melakukan validasi terhadap format dan struktur internal media tersebut. Setelah media dinyatakan valid, pengguna memasukkan pesan rahasia yang akan disisipkan ke dalam media penampung.

Pesan rahasia selanjutnya diproses melalui tahap prapemrosesan, termasuk konversi ke dalam representasi biner, sebelum dilakukan proses penyandian. Penyisipan data dilakukan dengan menerapkan teknik steganografi yang disesuaikan dengan karakteristik masing-masing media, seperti manipulasi bit tertentu pada media citra dan audio, serta

pemanfaatan elemen non-visual pada dokumen digital. Hasil dari proses ini adalah media stego yang secara visual, auditori, dan struktural tetap menyerupai media asli, namun telah mengandung informasi tersembunyi.



Gambar 1. Diagram Alur Proses Penyisipan dan Ekstraksi Data

Proses ekstraksi data dimulai dengan memuat media stego ke dalam sistem. Sistem mengidentifikasi jenis media dan menerapkan teknik decoding yang sesuai dengan metode penyisipan yang digunakan sebelumnya. Informasi tersembunyi diekstraksi dengan membalik proses penyandian dan kemudian dikonversi kembali ke bentuk pesan asli. Keberhasilan proses ekstraksi ditentukan oleh kesesuaian teknik ekstraksi dengan metode penyisipan serta keutuhan media stego. Seluruh proses dirancang agar ekstraksi data dapat dilakukan tanpa memerlukan media asli sebagai pembanding, sehingga meningkatkan fleksibilitas penggunaan sistem dalam skenario nyata.

Media dan Format yang Didukung

Penelitian ini mendukung beberapa jenis media digital, yaitu citra digital dengan format PNG dan JPG, audio digital dengan format WAV, serta dokumen digital yang meliputi TXT, DOCX, XLSX, dan PDF. Pemilihan format tersebut didasarkan pada tingkat penggunaan yang luas serta karakteristik teknis yang memungkinkan penerapan teknik steganografi.

Setiap jenis media diperlakukan dengan pendekatan yang berbeda sesuai dengan struktur datanya, sehingga sistem mampu beradaptasi terhadap heterogenitas media dalam satu kerangka kerja yang terpadu.

Lingkungan Pengembangan dan Implementasi

Aplikasi dikembangkan menggunakan bahasa pemrograman Python karena fleksibilitasnya dalam pengolahan multimedia serta dukungan pustaka yang luas. Implementasi dilakukan dengan memanfaatkan pustaka pengolahan citra, audio, dan dokumen digital untuk memastikan proses penyisipan dan ekstraksi berjalan secara efisien dan stabil.

Pengembangan sistem dilakukan secara bertahap, dimulai dari implementasi fungsi dasar, pengujian unit, hingga integrasi seluruh modul dalam satu aplikasi utuh.

Teknik dan Kriteria Pengujian

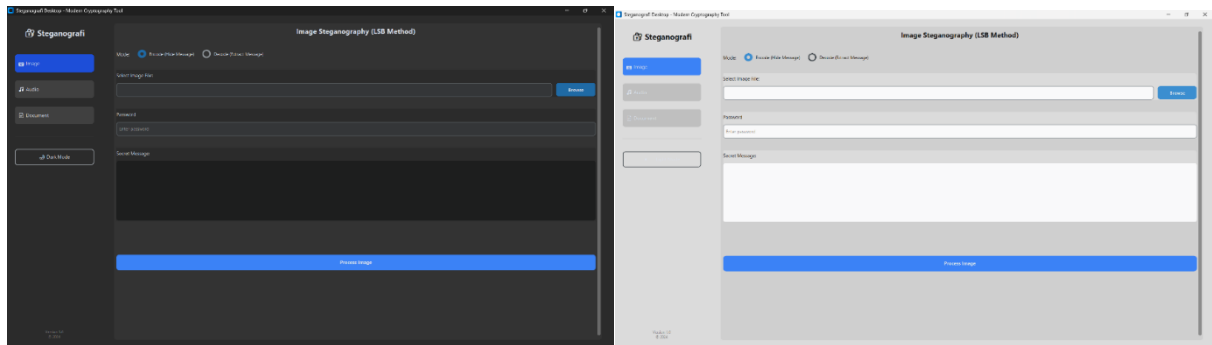
Pengujian sistem dilakukan untuk mengevaluasi kinerja dan keandalan aplikasi steganografi multiformat. Parameter pengujian meliputi:

1. Keberhasilan penyisipan dan ekstraksi, yang diukur berdasarkan kemampuan sistem untuk mengembalikan pesan rahasia secara utuh;
2. Kualitas media hasil penyisipan, yang dianalisis secara subjektif melalui pengamatan visual dan auditori terhadap media stego;
3. Stabilitas aplikasi, yang dievaluasi berdasarkan kemampuan sistem menangani berbagai ukuran pesan dan variasi media tanpa mengalami kegagalan proses.

Hasil pengujian digunakan sebagai dasar untuk menganalisis efektivitas pendekatan steganografi multiformat yang dikembangkan.

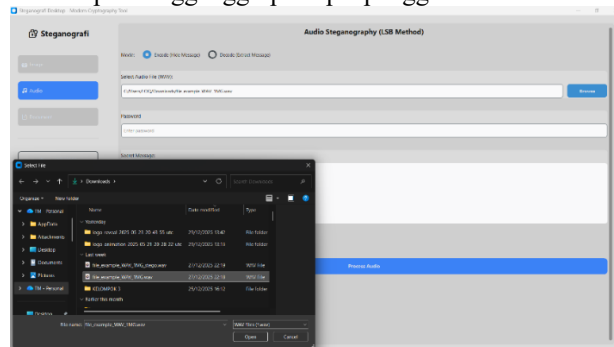
HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa aplikasi steganografi multiformat yang dikembangkan mampu berfungsi sesuai dengan tujuan perancangan sistem. Aplikasi berhasil mengimplementasikan proses penyisipan dan ekstraksi data rahasia pada berbagai jenis media digital, meliputi citra, audio, dan dokumen, dalam satu lingkungan aplikasi yang terpadu. Antarmuka pengguna dirancang secara intuitif sehingga memudahkan pengguna dalam memilih media penampung, memasukkan pesan rahasia, serta menentukan proses yang akan dijalankan.



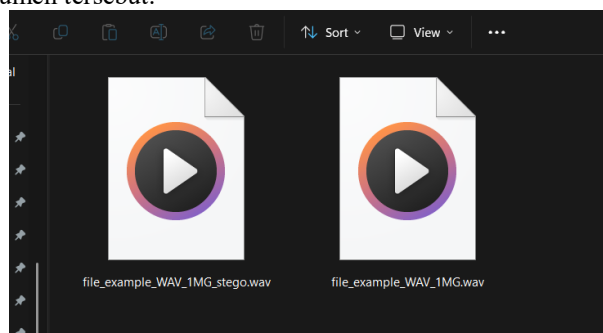
Gambar 2. Tampilan antarmuka utama aplikasi steganografi multiformat darkmode dan lightmode

Pada pengujian proses penyisipan data, sistem mampu menyisipkan pesan rahasia ke dalam media citra dan audio tanpa menimbulkan perubahan yang signifikan secara visual maupun auditori. Media hasil penyisipan tetap dapat dibuka dan digunakan secara normal, serta tidak menunjukkan perbedaan yang mencolok dibandingkan media asli. Hal ini menunjukkan bahwa teknik penyisipan yang diterapkan telah mempertimbangkan aspek imperceptibility, yaitu kemampuan menyembunyikan data tanpa mengganggu persepsi pengguna.



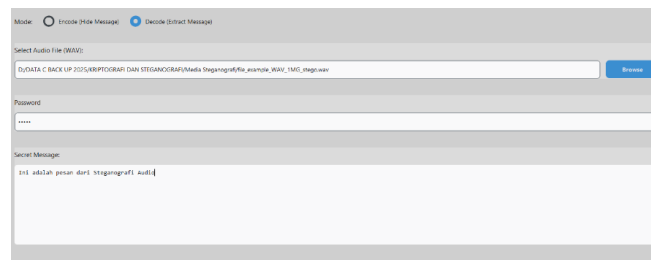
Gambar 3. Contoh proses penyisipan pesan rahasia pada media audio

Hasil pengujian pada media dokumen digital menunjukkan bahwa penyisipan data tidak memengaruhi struktur, format, maupun keterbacaan dokumen. Dokumen TXT, DOCX, XLSX, dan PDF tetap dapat dibuka menggunakan perangkat lunak standar tanpa menimbulkan kesalahan atau perubahan tampilan. Kondisi ini menegaskan bahwa pemanfaatan elemen non-visual dan metadata pada dokumen digital efektif untuk menyembunyikan informasi tanpa mengganggu fungsi utama dokumen tersebut.



Gambar 4. Contoh dokumen digital sebelum dan sesudah proses steganografi

Pada sisi ekstraksi data, aplikasi mampu mengembalikan pesan rahasia secara utuh dari seluruh media stego yang diuji. Proses ekstraksi dapat dilakukan tanpa memerlukan media asli sebagai pembanding, sehingga meningkatkan fleksibilitas penggunaan sistem dalam skenario komunikasi nyata. Keberhasilan ekstraksi menunjukkan bahwa mekanisme encoding dan decoding telah dirancang secara konsisten dan saling berkesesuaian dengan baik.



Gambar 5. Hasil/Output ekstraksi pesan rahasia dari media audio stego

Dari sudut pandang fungsional, pendekatan steganografi multiformat yang diterapkan memberikan keunggulan dibandingkan sistem steganografi satu media. Pengguna memiliki fleksibilitas dalam memilih jenis media yang sesuai dengan kebutuhan dan konteks komunikasi, sehingga risiko deteksi dapat diminimalkan melalui variasi media penampung. Namun demikian, hasil pengujian juga menunjukkan bahwa kapasitas penyisipan data sangat bergantung pada karakteristik masing-masing media, di mana media citra dan audio memiliki kapasitas yang relatif lebih besar dibandingkan dokumen teks.

Stabilitas aplikasi selama pengujian menunjukkan bahwa sistem mampu menangani variasi ukuran pesan dan jenis media tanpa mengalami kegagalan proses. Hal ini mengindikasikan bahwa arsitektur modular yang diterapkan berkontribusi terhadap keandalan sistem secara keseluruhan. Secara keseluruhan, hasil dan pembahasan ini menunjukkan bahwa aplikasi steganografi multiformat yang dikembangkan tidak hanya berfungsi secara teknis, tetapi juga memiliki potensi penerapan nyata dalam mendukung keamanan informasi digital secara terselubung.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penelitian ini berhasil mengembangkan sebuah aplikasi steganografi multiformat yang mampu menyisipkan dan mengekstraksi data rahasia pada berbagai jenis media digital, yaitu citra, audio, dan dokumen, dalam satu sistem yang terpadu. Aplikasi yang dibangun dapat berfungsi dengan baik pada seluruh media yang didukung, tanpa menimbulkan perubahan yang signifikan secara visual, auditori, maupun struktural, sehingga memenuhi prinsip utama steganografi, yaitu *imperceptibility*.

Hasil pengujian menunjukkan bahwa mekanisme penyisipan dan ekstraksi data berjalan secara konsisten dan andal, serta tidak memerlukan media asli sebagai pembanding pada saat ekstraksi. Pendekatan arsitektur modular yang diterapkan terbukti meningkatkan stabilitas dan fleksibilitas sistem, serta memungkinkan pengelolaan berbagai teknik steganografi sesuai dengan karakteristik masing-masing media. Dengan demikian, steganografi multiformat memberikan keunggulan dibandingkan pendekatan satu media, terutama dalam hal fleksibilitas penggunaan dan potensi pengurangan risiko deteksi.

Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan. Kapasitas penyisipan data sangat bergantung pada jenis dan karakteristik media penampung, di mana media citra dan audio memiliki kapasitas yang lebih besar dibandingkan dokumen digital. Selain itu, penelitian ini belum mengevaluasi tingkat ketahanan sistem terhadap serangan steganalisis secara kuantitatif maupun dampak transformasi lanjutan seperti kompresi lossy dan modifikasi media.

Untuk penelitian selanjutnya, disarankan pengembangan teknik steganografi yang lebih adaptif dan robust, khususnya terhadap serangan steganalisis dan manipulasi media. Integrasi steganografi dengan kriptografi juga dapat dipertimbangkan untuk meningkatkan lapisan keamanan data. Selain itu, pengujian kuantitatif terhadap kualitas media dan performa sistem perlu dilakukan guna memperoleh evaluasi yang lebih komprehensif. Secara keseluruhan, penelitian ini diharapkan dapat menjadi kontribusi awal dalam pengembangan sistem keamanan informasi berbasis steganografi multiformat yang lebih fleksibel dan aplikatif dalam konteks komunikasi digital modern.

REFERENSI

- Ardiansyah, B., Rafli, A. A., Anria, H., Langkasa, M. J. B., Banta-Bantaeng, K., Rapocini, K., & Makassar, K. (n.d.). Implementation of Steganography Techniques on Audio Files Using the Spread Spectrum Method through the Utilization of the Coagula Application. In *INNOVATION IN COMPUTER EDUCATION JOURNAL* (Vol. 1, Issue 1).
- Dashtaki, E. R., & Ghaemmaghami, S. (2025). A New Bit-Wise Approach for Image-in-Audio Steganography Using Deep Learning. *ISecure*, 17(2), 117–124. <https://doi.org/10.22042/isecure.2025.214367>
- Eka, G., Wijaya, P., Gusti, I., Gede, A., Kadnyanan, A., Raya, J., Unud, K., Jimbaran, B., & Selatan, K. (2025).

- Penerapan Steganografi untuk Pengamanan Konten Gambar dalam Media Sosial. *JNATIA*, 3(2).
- Firdaus, D. T., Croix, N. J. D. La, Ahmad, T., Mukanyiligira, D., & Sibomana, L. (2025). Steganographic model to conceal the secret data in audio files utilizing a fourfold paradigm: Interpolation, multi-layering, optimized sample space, and smoothing. *Journal of Safety Science and Resilience*, 6(2), 138–149. <https://doi.org/10.1016/j.jnlssr.2024.09.004>
- Gusti, I., Febri, N., Krisna, A., Karyawati, E., Program, A., Informatika, S., Matematika, F., Ilmu, D., Alam, P., Raya, J., Unud, K., Jimbaran, B., & Selatan, K. (2024). Penerapan Teknik Steganografi LSB pada Format Gambar Modern. *JNATIA*, 2(4). <https://file-examples.com/index.php/sample-images-download/>.
- Hajar Akbar, M. (2024). Investigasi Stego File Menggunakan Framework National Institute of Justice. *CONTEN: Computer and Network Technology*, 4(1). <http://jurnal.bsi.ac.id/index.php/conten>
- Halim, M., & Lestari, W. S. (n.d.). *JURNAL ARMADA INFORMATIKA STMIK Methodist Binjai Steganography Menggunakan Advanced Encryption Standard dan Metode Least Significant Bit pada File Bitmap 24-bit*. <https://doi.org/>
- Ishtiaq, S., Ejaz, N., Hashmi, M. U., & Shah, S. I. H. (2025). Enhancing Imperceptibility: Zero-width Character-based Text Steganography for Preserving Message Privacy. *Acta Informatica Pragensia*, 14(3), 445–459. <https://doi.org/10.18267/j.aip.271>
- Izzul Haziq Rahim, M., Abd Hamid, N., Dhalila Mohd Satar, S., Fadzil Abdul Kadir, M., Faisal Amri Abidin, A., Afendee Mohamed, M., & Mohamad, M. (2025). AUDIO STEGANOGRAPHY USING LEAST SIGNIFICANT BIT METHOD FOR CONFIDENTIAL DATA EMBEDDING. *International Journal of Multimedia & Its Applications (IJMA)*, 17(3). <https://doi.org/10.5121/ijma.2025.17303>
- K, S. H., & Tajuddin, M. (2022). A Literature Review on Image Steganography Using AES. *International Research Journal of Engineering and Technology*. www.irjet.net
- Karo, P. K., Simarmata, S., Faizah, N. M., & Fabrianto, L. (2025). Facial image protection with visual cryptography and random least significant bit (LSB) steganography. In *IT Independent Journal* (Vol. 13, Issue 4). www.ejournal.isha.or.id/index.php/Mandiri
- Kusuma, P., & Prayudi, Y. (2025). Implementasi Steganografi Dengan Menggunakan Metode Masking And Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram Audio. *AJIE*, 1–15. <https://doi.org/10.20885/ajie.vol9.iss1.art1>
- Luthfi, A., & Jamarun, N. (2025). Evaluasi Kinerja Improved Spread Spectrum Steganography pada Advanced Audio Coding. *Jurnal Nasional Teknologi Dan Sistem Informasi*, 10(3), 223–230. <https://doi.org/10.25077/teknosi.v10i3.2024.223-230>
- Padmaja, S., Mahaboob Basha, S., & History, A. (n.d.). A NOVEL HYBRID STEGANOGRAPHY APPROACH FOR SECURING TEXT, IMAGES, AND AUDIO WITH ROBUST ENCRYPTION IN AUDIO STEGANOGRAPHY ARTICLE INFO ABSTRACT. *Journal of Engineering and Technology for Industrial Applications ITEGAM-JETIA Manaus*, 52, 136–147. <https://doi.org/10.5935/jetia>
- Rohayah, S. (2023). *OKTAL: Jurnal Ilmu Komputer dan Science Implementasi Teknik Steganography Pada File Gambar Dan Audio Dengan Menggunakan Metode LSB*. 2(2).
- Slb Steganography, . ., Amalya, W. S., Astuti, N. R. D. P., & Aribowo, E. (2025). *Application of LSB Steganography for Encrypted Data Using Triple Transposition Vigenere on Digital Images* (Vol. 13).
- Walad, I. (2025). Implementasi Steganografi Berbasis Mobile Menyembunyikan Informasi. In *JURNAL INFORMATIKA LOGIKA* (Vol. 2, Issue 2).