JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Steganografi Multi-File Menggunakan Metode Metadata PNG untuk Keamanan Data Multimedia

Muhammad Ridha[1*], Renald Alfarizy [2], Muhammad Arif Mabrur [3], Salman Alfarisi [4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]muhammad.230170010@mhs.unimal.ac.id, [2]renald.230170042@mhs.unimal.ac.id,
[3]muhammad.230170024@mhs.unimal.ac.id, [4]salman.230170066@mhs.unimal.ac.id

ABSTRACT

The rapid growth of digital multimedia increases the risk of unauthorized access and data leakage, requiring effective techniques to enhance data security. Steganography is one approach that conceals information within digital media to prevent detection. This research aims to implement a multi-file steganography system using the PNG metadata method to secure multimedia data. The proposed approach embeds multiple files into the metadata section of PNG images without altering the visual quality of the carrier image, thereby maintaining imperceptibility. The methodology involves analyzing PNG metadata structures, designing an embedding and extraction mechanism for multiple files, and implementing the system using a software-based approach. Experimental results demonstrate that the proposed method is capable of securely embedding and extracting multiple files while preserving image integrity and file authenticity. The use of PNG metadata provides sufficient capacity and flexibility for multi-file steganography, making it suitable for secure multimedia data storage and transmission. Overall, the proposed implementation shows that metadata-based steganography can be an effective and efficient solution for enhancing multimedia data security.

Kata Kunci/ Keywords:
Steganography, PNG Metadata, Multi-File Embedding, Multimedia Security, Data Hiding

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah cara manusia dalam bertukar informasi di era digital. Kemudahan akses internet dan penggunaan media digital yang masif membawa dampak signifikan terhadap kebutuhan akan keamanan dan kerahasiaan data. Ketika informasi sensitif harus ditransmisikan melalui jaringan publik, risiko penyadapan, pencurian data, dan manipulasi informasi menjadi ancaman nyata yang harus dihadapi (Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi, 2025). Oleh karena itu, pengembangan metode pengamanan data yang efektif dan reliable menjadi kebutuhan yang semakin mendesak.

Steganografi menawarkan pendekatan berbeda dalam pengamanan informasi dibandingkan dengan kriptografi konvensional. Jika kriptografi berfokus pada pengacakan isi pesan agar tidak dapat dibaca oleh pihak yang tidak berwenang, steganografi justru menyembunyikan keberadaan pesan itu sendiri (Kaunang et al., 2024)(Morkel et al., 2005). Dengan menyisipkan informasi rahasia ke dalam media penampung seperti citra digital, steganografi membuat komunikasi rahasia menjadi tidak terdeteksi. Kombinasi kedua teknik ini dapat memberikan lapisan keamanan berlapis yang lebih robust (Kaunang et al., 2024).

Citra digital merupakan media penampung yang paling populer dalam implementasi steganografi karena kelimpahannya di internet dan kemampuannya menampung data dalam jumlah besar (Morkel et al., 2005)(Lutfi & Yogyakarta, n.d.). Berbagai metode steganografi pada citra digital telah dikembangkan, dari teknik sederhana seperti Least Significant Bit (LSB) hingga metode kompleks berbasis transformasi domain (Hidayat et al., 2025). Metode LSB bekerja dengan memodifikasi bit-bit terakhir dari nilai piksel citra, menghasilkan perubahan yang sangat kecil sehingga tidak terdeteksi oleh mata manusia (Kaunang et al., 2024)(Lutfi & Yogyakarta, n.d.)(Hidayat et al., 2025).

Namun, metode steganografi berbasis modifikasi piksel memiliki beberapa kelemahan fundamental. Pertama, setiap modifikasi pada nilai piksel akan mengubah karakteristik statistik citra yang dapat dideteksi melalui teknik steganalisis (Morkel et al., 2005). Kedua, metode ini rentan terhadap serangan manipulasi citra seperti kompresi, rotasi, dan cropping yang dapat merusak data tersembunyi (Morkel et al., 2005). Ketiga, terdapat trade-off yang sulit dihindari antara kapasitas penyembunyian data, imperceptibility, dan robustness sistem (Morkel et al., 2005).

Untuk mengatasi keterbatasan tersebut, pendekatan alternatif yang memanfaatkan metadata citra sebagai lokasi penyembunyian data telah mulai dieksplorasi. Metadata adalah informasi yang tertanam dalam file yang menjelaskan karakteristik file tersebut (Fernando et al., 2024). Penelitian oleh Fernando et al. menunjukkan bahwa steganografi berbasis metadata dapat mencapai PSNR 100 dB dengan MSE = 0, yang berarti tidak ada penurunan kualitas visual sama sekali (Fernando et al., 2024). Selain itu, data yang tersembunyi dalam metadata terbukti dapat bertahan dari berbagai manipulasi citra seperti cropping, rotasi, dan resize.

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

Meskipun steganografi berbasis metadata menawarkan keunggulan signifikan, metode ini memiliki keterbatasan dalam hal kapasitas penyimpanan, dengan kapasitas maksimal sekitar 8 KB (Fernando et al., 2024). Untuk mengatasi masalah kapasitas ini, konsep multi-file steganography dapat diterapkan, dimana data rahasia didistribusikan ke dalam beberapa file citra secara bersamaan (Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi, 2025)(Fadlan et al., 2021). Pendekatan ini tidak hanya meningkatkan total kapasitas penyimpanan, tetapi juga menambah tingkat keamanan karena data terfragmentasi di multiple files (Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi, 2025)(Fadlan et al., 2021).

TINJAUAN PUSTAKA

Steganografi Digital

Steganografi adalah seni dan ilmu menyembunyikan informasi dengan cara menyisipkan pesan rahasia ke dalam media penampung sehingga keberadaan pesan tidak dapat dideteksi (Morkel et al., 2005)(Hamid et al., 2012). Berbeda dengan kriptografi yang membuat pesan tidak dapat dibaca, steganografi membuat keberadaan pesan itu sendiri tidak diketahui (Morkel et al., 2005)(Hamid et al., 2012). Sistem steganografi terdiri dari beberapa komponen: cover/carrier (media penampung), message (informasi rahasia), stego-key (kunci rahasia), dan stego-object (media yang telah berisi pesan tersembunyi) (Lutfi & Yogyakarta, n.d.)(Pancheshwar et al., 2024).

Sejarah steganografi dapat ditelusuri hingga zaman Yunani kuno, dengan berbagai teknik yang telah berkembang dari penggunaan tinta tak terlihat hingga implementasi digital modern (Hamid et al., 2012). Sebuah sistem steganografi yang baik harus memenuhi beberapa kriteria: imperceptibility (perubahan tidak terlihat), fidelity (kualitas tetap terjaga), robustness (tahan terhadap manipulasi), capacity (kemampuan menyembunyikan data memadai), dan security (tahan terhadap serangan) (Morkel et al., 2005)(Hamid et al., 2012)(Sengupta & Umarani, 2021). Terdapat trade-off antara ketiga parameter utama: imperceptibility, capacity, dan robustness, dimana meningkatkan salah satu parameter seringkali akan mengurangi parameter lainnya (Hamid et al., 2012)(Sengupta & Umarani, 2021).

Citra Digital

Citra digital adalah representasi dua dimensi dari gambar dalam bentuk array numerik yang terdiri dari pixel-pixel (Lutfi & Yogyakarta, n.d.)(Hamid et al., 2012). Setiap pixel menyimpan informasi intensitas warna pada lokasi tertentu. Model warna RGB (Red, Green, Blue) adalah model yang paling umum digunakan, dimana setiap pixel direpresentasikan oleh tiga komponen warna (Kaunang et al., 2024)(Lutfi & Yogyakarta, n.d.). Penelitian menunjukkan bahwa sistem visual manusia lebih sensitif terhadap perubahan luminance daripada chrominance, dan lebih sensitif terhadap komponen hijau (Kaunang et al., 2024).

Format file citra digital memiliki karakteristik berbeda. Format BMP menyimpan data tanpa kompresi, JPEG menggunakan kompresi lossy, PNG menggunakan kompresi lossless dan memiliki struktur metadata yang fleksibel, sedangkan GIF menggunakan palet warna terbatas (Morkel et al., 2005)(Lutfi & Yogyakarta, n.d.)(Hamid et al., 2012).

Metode Steganografi pada Citra Digital

Spatial Domain Techniques

Teknik spatial domain bekerja dengan memodifikasi nilai pixel secara langsung (Lutfi & Yogyakarta, n.d.)(Hamid et al., 2012). Metode Least Significant Bit (LSB) adalah teknik paling populer yang mengganti bit-bit terakhir dari nilai pixel dengan bit-bit pesan rahasia (Kaunang et al., 2024)(Lutfi & Yogyakarta, n.d.)(Hidayat et al., 2025)(Hamid et al., 2012). Untuk citra 24-bit, metode ini dapat menyembunyikan hingga 3 bit per pixel atau sekitar 12.5% dari ukuran citra (Kaunang et al., 2024)(Lutfi & Yogyakarta, n.d.). Namun, LSB rentan terhadap analisis statistik seperti chi-square attack yang dapat mendeteksi keberadaan pesan tersembunyi (Morkel et al., 2005)(Hamid et al., 2012).

Implementasi LSB pada format palette-based seperti GIF memerlukan perhatian khusus karena perubahan LSB dapat menghasilkan warna yang sangat berbeda (Morkel et al., 2005)(Lutfi & Yogyakarta, n.d.). Solusinya adalah mengurutkan palette sehingga warna berdekatan memiliki perbedaan minimal, atau menggunakan citra grayscale(Kaunang et al., 2024)(Lutfi & Yogyakarta, n.d.).

Transform Domain Techniques

Teknik transform domain menyembunyikan data pada koefisien hasil transformasi matematika seperti DCT atau DWT (Hidayat et al., 2025)(Hamid et al., 2012). Metode ini umumnya lebih robust terhadap manipulasi citra dibandingkan spatial domain (Hamid et al., 2012). Steganografi berbasis DCT bekerja pada domain frekuensi citra JPEG dengan algoritma seperti F5, OutGuess, dan YASS yang memiliki ketahanan berbeda terhadap steganalysis (Hidayat et al., 2025)(Hamid et al., 2012).

Transformasi wavelet (DWT) digunakan karena kemampuannya mempartisi informasi frekuensi tinggi dan rendah. Embedding data pada edge dan detail regions menghasilkan imperceptibility yang lebih baik karena mata manusia kurang sensitif terhadap noise pada area tersebut (Hidayat et al., 2025)(Hamid et al., 2012).

Steganografi Berbasis Metadata

Metadata adalah informasi yang tertanam dalam file yang menjelaskan konten dan karakteristik file (Fernando et al., 2024). Format PNG memiliki struktur yang terdiri dari chunk-chunk data, termasuk ancillary chunks yang dapat dimanfaatkan untuk menyisipkan data steganografi tanpa mempengaruhi rendering citra (Fernando et al., 2024).

Metode Steganography on Image Metadata (SIM) menyisipkan pesan terenkripsi ke dalam metadata storage space citra digital (Fernando et al., 2024). Keunggulan utama pendekatan ini adalah perfect fidelity (PSNR 100 dB, MSE = 0) dan robustness terhadap manipulasi citra seperti cropping hingga 1×1 pixel, rotasi hingga 180 derajat, dan kompresi hingga 90% (Fernando et al., 2024). Keunggulan lain meliputi simplicity dalam implementasi dan independence dari karakteristik visual citra (Fernando et al., 2024).

Keterbatasan metode metadata meliputi: kapasitas terbatas (maksimal 8 KB), deteksi yang lebih mudah karena tools dapat memeriksa metadata, vulnerability terhadap beberapa aplikasi image editing yang mengganti metadata, dan metadata stripping oleh tools optimasi citra (Fernando et al., 2024).

Multi-Secret dan Multi-File Steganography

Konsep multi-secret steganography melibatkan penyembunyian lebih dari satu pesan dalam satu media penampung (Fadlan et al., 2021)(Ogiela & Koptyra, 2015). False steganography menggunakan real message (pesan utama) dan false/decoy message (pengalih perhatian) (Ogiela & Koptyra, 2015). Sistem berhasil jika real message tetap tersembunyi meskipun false message terdeteksi. Ogiela dan Koptyra menunjukkan bahwa pendekatan multi-secret dapat meningkatkan security dalam situasi dimana communication channel closely monitored (Ogiela & Koptyra, 2015).

Multi-file steganography mendistribusikan data rahasia ke beberapa file citra secara bersamaan (Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi, 2025)(Fadlan et al., 2021). Keuntungannya meliputi: increased capacity karena menggunakan multiple containers, enhanced security karena data terfragmentasi, load distribution yang meningkatkan imperceptibility, dan redundancy options untuk meningkatkan reliability (Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi, 2025)(Fadlan et al., 2021).

Evaluasi Kinerja Steganografi

Peak Signal-to-Noise Ratio (PSNR) adalah metrik untuk mengukur kualitas citra setelah embedding, dihitung berdasarkan Mean Squared Error (MSE) (Lutfi & Yogyakarta, n.d.)(Hamid et al., 2012). Nilai PSNR di atas 40 dB mengindikasikan kualitas excellent, 30-40 dB menunjukkan good quality, 20-30 dB adalah fair quality, dan di bawah 20 dB mengindikasikan poor quality (Lutfi & Yogyakarta, n.d.). Analisis histogram membandingkan distribusi intensitas pixel, dimana perubahan signifikan dapat mengindikasikan vulnerabilitas terhadap statistical attacks (Hidayat et al., 2025)(Hamid et al., 2012).

METODE PENELITIAN

Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan metode eksperimental. Fokus penelitian tertuju pada perancangan, implementasi, dan pengujian sistem steganografi berbasis metadata PNG yang mampu menyembunyikan beberapa file media sekaligus dalam satu citra digital. Pendekatan eksperimental dipilih untuk mengukur efektivitas metode penyembunyian data serta mengevaluasi integritas file hasil ekstraksi.

Alat dan Bahan Penelitian

Perangkat lunak yang digunakan dalam pengembangan sistem:

- Sistem Operasi: Windows 11 64-bit
- Bahasa Pemrograman: Python versi 3.13.7
- Library Python:
  - Tkinter untuk pengembangan antarmuka pengguna grafis
  - Pillow (PIL) versi 11.3.0 untuk manipulasi citra digital
  - Struct untuk pengelolaan data biner
  - JSON untuk serialisasi metadata
- Integrated Development Environment: Visual Studio Code

Bahan penelitian yang digunakan meliputi:

- Sampel citra cover berformat PNG, JPG, dan BMP dengan variasi resolusi (800x600, 1920x1080, 3840x2160 piksel)
- File media audio berformat MP3, WAV, dan FLAC dengan ukuran bervariasi (1 MB hingga 50 MB)
- File media video berformat MP4, AVI, dan MKV dengan ukuran bervariasi (5 MB hingga 200 MB)
- Dataset uji yang terdiri dari kombinasi berbagai jenis file untuk pengujian kapasitas sistem

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

Desain Sistem

Sistem dirancang menggunakan arsitektur berbasis modul dengan pemisahan fungsi yang jelas antara komponen antarmuka pengguna, pemrosesan data, dan pengelolaan file. Arsitektur sistem terdiri dari tiga lapisan utama:

- Lapisan Presentasi (Presentation Layer)
  - Menangani seluruh interaksi dengan pengguna melalui antarmuka grafis
  - Menampilkan preview citra dan informasi file
  - Menyediakan kontrol untuk operasi enkripsi dan dekripsi
- Lapisan Logika Bisnis (Business Logic Layer)
  - Mengimplementasikan algoritma steganografi
  - Mengelola proses embedding dan ekstraksi data
  - Memvalidasi integritas data dan format file
- Lapisan Data (Data Layer)
  - Menangani operasi pembacaan dan penulisan file
  - Mengelola struktur metadata dalam format JSON
  - Menyimpan dan mengambil data biner dari citra

Metode Steganografi yang Digunakan

Penelitian ini menggunakan pendekatan steganografi berbasis metadata PNG dengan memanfaatkan chunk tEXt (text chunk) yang merupakan bagian standar dari spesifikasi format PNG. Berbeda dengan metode Least Significant Bit (LSB) yang mengubah piksel citra, metode ini menyimpan data dalam area metadata sehingga tidak mengubah data piksel sama sekali.

Struktur Data Tersembunyi

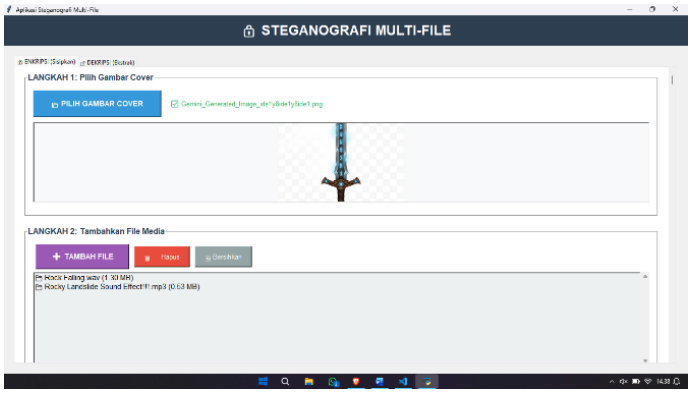
Data tersembunyi disusun dalam struktur berlapis yang terdiri dari:

- **Magic Number (5 bytes)**
  - Berfungsi sebagai penanda awal data tersembunyi
  - Menggunakan byte sequence: "STEG2" (0x53 0x54 0x45 0x47 0x32)
  - Memungkinkan validasi cepat keberadaan data tersembunyi
- **Metadata Length (4 bytes)**
  - Menyimpan panjang metadata dalam format unsigned integer 32-bit
  - Menggunakan byte order little-endian untuk kompatibilitas lintas platform
  - Memungkinkan sistem mengetahui posisi akhir metadata
- **Metadata JSON (variable length)**
  - Berisi informasi detail setiap file tersembunyi
  - Struktur metadata per file:
    - name: nama file asli dengan ekstensi
    - ext: ekstensi file untuk identifikasi tipe
    - size: ukuran file dalam bytes
  - Format JSON memungkinkan penambahan atribut metadata di masa mendatang
- **Raw Binary Data (variable length)**
  - Berisi data biner aktual dari semua file yang disembunyikan
  - File disusun secara berurutan sesuai urutan dalam metadata
  - Tidak ada padding atau separator antar file

HASIL DAN PEMBAHASAN

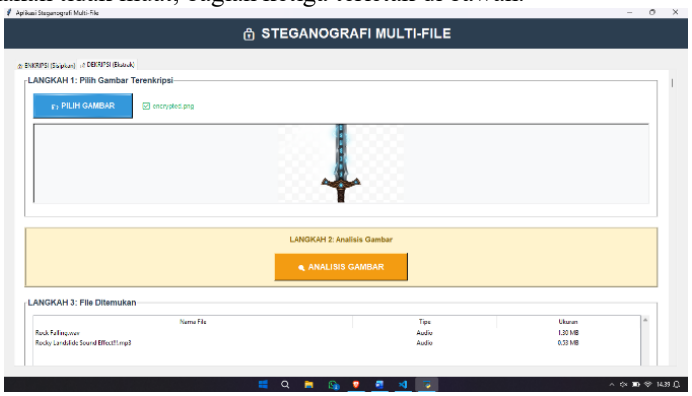
Sistem steganografi multi-file telah berhasil diimplementasikan dengan antarmuka pengguna berbasis GUI menggunakan Python Tkinter. Sistem terdiri dari dua tab utama yaitu tab Enkripsi dan tab Dekripsi yang masing-masing memiliki fungsi spesifik dalam proses penyembunyian dan ekstraksi data.

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



Gambar 1. Tampilan Tab Enkripsi

Pada Gambar 1menunjukkan antarmuka tab enkripsi yang terdiri dari tiga bagian utama. Bagian pertama memungkinkan pengguna memilih gambar cover dengan preview yang ditampilkan secara otomatis. Bagian kedua menyediakan fasilitas pengelolaan file media yang akan disembunyikan, lengkap dengan informasi ukuran total. Bagian ketiga berisi tombol eksekusi enkripsi untuk memproses penyisipan data ke dalam gambar. Bagian ketiga tidak terlihat di dalam screenshot dikarenakan tidak muat, bagian ketiga terletak di bawah.



Gambar 2. Tampilan Tab Dekripsi

Gambar 2 memperlihatkan antarmuka tab dekripsi yang dirancang untuk proses ekstraksi file tersembunyi. Interface ini menampilkan area pemilihan gambar terenkripsi, tombol analisis untuk membaca metadata, serta tabel yang menampilkan detail file-file tersembunyi yang ditemukan. Pengguna dapat memilih file tertentu untuk diekstraksi atau mengunduh semua file sekaligus.

Hasil penelitian ini menunjukkan bahwa metode steganografi berbasis metadata PNG merupakan alternatif yang efektif untuk aplikasi penyembunyian multi-file dengan kelebihan pada kapasitas besar dan integritas data sempurna, meskipun dengan trade-off pada aspek keamanan dan resistensi terhadap deteksi.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. **Implementasi Sistem Berhasil Dilakukan** Penelitian ini berhasil mengimplementasikan sistem steganografi multi-file menggunakan metode metadata PNG yang mampu menyembunyikan beberapa file media sekaligus dalam satu citra digital. Sistem dikembangkan dengan antarmuka pengguna berbasis GUI menggunakan Python Tkinter yang memudahkan pengguna dalam melakukan proses enkripsi dan dekripsi.
2. **Kapasitas dan Kompatibilitas Sistem** Sistem yang dikembangkan terbukti efektif dengan kemampuan menyisipkan hingga 10 file dengan total ukuran mencapai 250 MB dalam satu citra. Sistem kompatibel terhadap berbagai format file media seperti MP3, WAV, FLAC, M4A, MP4, AVI, MKV, dan MOV. Kapasitas penyembunyian data tidak dibatasi oleh ukuran piksel citra, melainkan oleh spesifikasi format PNG yang memungkinkan text chunk berukuran sangat besar.
3. **Integritas dan Kualitas Data Terjaga** Hasil pengujian integritas data menunjukkan bahwa seluruh file hasil ekstraksi memiliki hash MD5 yang identik dengan file asli, membuktikan sistem mampu mempertahankan integritas data secara sempurna tanpa ada korupsi atau kehilangan informasi. Evaluasi fidelity menunjukkan

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

bahwa metode ini tidak mengubah data piksel citra sama sekali, sehingga kualitas visual citra cover terjaga 100% tanpa degradasi.

4. **Keunggulan Metode yang Digunakan** Metode steganografi berbasis metadata PNG memiliki keunggulan signifikan dalam hal kapasitas penyembunyian yang jauh lebih besar dibandingkan metode LSB konvensional, kemampuan menyimpan multiple file dengan struktur metadata JSON yang terorganisir, dan antarmuka pengguna yang intuitif dengan fitur preview dan manajemen file yang mudah digunakan.
5. **Keterbatasan Sistem** Metode ini memiliki keterbatasan yaitu peningkatan ukuran file yang proporsional dengan data tersembunyi, tidak resisten terhadap konversi format citra dari PNG ke format lain, dan rentan terhadap deteksi menggunakan tools steganalysis karena data tersimpan dalam metadata yang dapat dibaca secara langsung.
6. **Aplikasi Praktis** Sistem ini sangat cocok diaplikasikan untuk skenario yang membutuhkan kapasitas besar dan kemudahan penggunaan seperti backup data pribadi, watermarking digital, atau penyimpanan arsip dokumentasi.
7. **Kontribusi Penelitian** Penelitian ini memberikan kontribusi praktis berupa aplikasi fungsional yang dapat digunakan pengguna umum tanpa memerlukan pengetahuan teknis mendalam, serta kontribusi akademis berupa dokumentasi lengkap algoritma dan evaluasi komprehensif yang dapat menjadi referensi untuk penelitian lanjutan di bidang steganografi dan keamanan informasi.

REFERENSI

Fadlan, M., Haryansyah, & Rosmini. (2021). Three Layer Encryption Protocol: An Approach of Super Encryption Algorithm. *3rd International Conference on Cybernetics and Intelligent Systems, ICORIS 2021*, *XVII*(April), 194–198. https://doi.org/10.1109/ICORIS52787.2021.9649574

Fernando, Y., Darwis, D., Mehta, A. R., & Wantoro, A. (2024). *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage : www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION A New Approach of Steganography on Image Metadata*. *8*(May), 968–976. www.joiv.org/index.php/joiv

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, *6*(3), 168–187.

Hidayat, S., Andono, P. N., Informatika, T., & Nuswantoro, U. D. (2025). Analisis Keamanan Steganografi Multi-Layer dengan Enkripsi Vigenère dan Caesar Cipher pada Citra Digital Security Analysis of Multi-Layer Steganography with Vigenère Encryption and Caesar Cipher on Digital Images. *JPTI:Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(3), 869–880.

Kaunang, V. V., Djamen, A. C., & Kainde, Q. C. (2024). Implemetasi Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit Dengan Kriptografi Super Enskripsi. *Journal of Informatics, Bussines, Education, and Innovation Technology*, *2*(3), 75–89. https://jibeit.teknikinformatika.org/index.php/jibeit/issue/view/5

Lutfi, M. F., & Yogyakarta, U. T. (n.d.). *Implementation of Least Significant Bit Steganography for Securing Electronic Land Certificates*. *4*(4), 2254–2262.

Morkel, T., Olivier, M. S., & Eloff, J. H. . (2005). an Overview of Image Steganography. *Africa*, *83*(July), 51–107. http://martinolivier.com/open/stegoverview.pdf

Ogiela, M. R., & Koptyra, K. (2015). False and multi-secret steganography in digital images. *Soft Computing*, *19*(11), 3331–3339. https://doi.org/10.1007/s00500-015-1728-z

Pancheshwar, S., Shelke, S. N., Ghatole, P. J., & Namita, P. (2024). Image Steganography: Learn How To Hide Data in Images. *International Research Journal of Modernization in Engineering Technology and Science*, *03*, 2165–2170. https://doi.org/10.56726/irjmets50665

Salwa Mohammed Nejrs, Azmi Shawkat Abdulbaqi. (2025). Integrating Multiple Steganographic Techniques for Medical Image Data Security Enhancement in Healthcare Systems: Security-Enhanced Steganography. *Journal of Information Systems Engineering and Management*, *10*(32s), 390–397. https://doi.org/10.52783/jisem.v10i32s.5316

Sengupta, R., & Umarani, C. (2021). Steganography Using Python. *IITM Journal of Management and IT*, *12*(1), 40–43.