JIKUM
JURNAL ILMU KOMPUTER

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

Desain dan Implementasi Aplikasi Steganografi Dual Mode Berbasis Java untuk Menyembunyikan Pesan Teks dan Gambar

Siti Sundari[1] , Mauliza Vazira[2], Monica Annisa Fitri[3*], Hafizah[4]
[1,2,3,4]Uviversitas Malikussaleh, Indonesia
[1]siti.230170032@mhs.unimal.ac.id, [2]mauliza.230170097@mhs.unimal.ac.id, [3]monica.230170143@mhs.unimal.ac.id, [4]hafizah.230170093@mhs.unimal.ac.id

ABSTRACT

Steganography is a method of protecting information by hiding secret messages within a carrier medium, making their presence difficult for others to detect. This research aims to design and build a Java-based dual-mode steganography application that can hide text messages within text (text-to-text) and image messages within text (text-to-image). This application was created using the Java programming language with an object-oriented programming approach, and utilizes the Base64 encoding technique as a means of embedding data. The research methods applied included requirements analysis, system design, implementation, and application testing. The test results demonstrated that this application can effectively hide and extract text messages and images, while using a password as an additional layer of security. We hope this application can be a practical solution for maintaining the confidentiality of digital data, while also serving as a useful steganography learning tool for students.

Keywords: *Steganography, Information Security, Java, Base64, Data Hiding.*

PENDAHULUAN

Perkembangan teknologi informasi yang begitu cepat telah memicu peningkatan pertukaran data digital di berbagai bidang kehidupan, mulai dari pendidikan, bisnis, hingga komunikasi sehari-hari. Namun, kemudahan dalam mengirim dan menyimpan data ini juga membawa risiko lebih besar terhadap kebocoran dan penyalahgunaan informasi. Oleh karena itu, kita memerlukan metode pengamanan data yang tidak hanya melindungi isi pesan, tetapi juga mampu menyamarkan keberadaannya agar tidak mudah ditemukan oleh pihak yang tidak berhak. Dalam era di mana data pribadi seperti foto, dokumen, atau pesan rahasia sering dikirim melalui internet, ancaman seperti peretasan atau pengintaian telah menjadi masalah umum, sehingga teknik keamanan yang lebih canggih diperlukan untuk melindungi privasi individu dan organisasi.

Salah satu pendekatan yang bisa diterapkan adalah steganografi. Teknik ini melibatkan penyembunyian pesan rahasia di dalam media lain, seperti teks, gambar, audio, atau video, sehingga pesan tersebut tidak tampak secara langsung(Kallapu et al., 2025)(Kallapu et al., 2025). Berbeda dari kriptografi yang mengubah pesan menjadi kode yang sulit dibaca, steganografi lebih menekankan pada penyamaran agar keberadaan pesan tidak menimbulkan kecurigaan. Dengan cara ini, steganografi menawarkan alternatif yang efektif untuk menjaga kerahasiaan informasi digital. Misalnya, dalam sejarah, steganografi telah digunakan untuk menyampaikan pesan rahasia selama perang, dan kini diterapkan dalam aplikasi modern seperti watermarking digital untuk melindungi hak cipta atau komunikasi aman di dunia maya(Krisna, I Gusti Ngurah Febri Ananda Karyawati, 2024).

Steganografi yang menggunakan teks dan gambar sebagai media adalah pendekatan populer karena keduanya mudah didapat dan sering digunakan dalam komunikasi harian. Penyembunyian pesan ke dalam teks bisa dilakukan melalui berbagai teknik, misalnya dengan encoding data sehingga pesan rahasia bisa disisipkan tanpa mengubah tampilan teks secara drastis(Muhammad et al., n.d.). Adapun penyembunyian gambar ke dalam teks melibatkan konversi data biner gambar menjadi representasi teks menggunakan metode encoding seperti Base64. Teknik ini memanfaatkan fakta bahwa teks adalah format universal di internet, sehingga data gambar bisa "disamarkan" sebagai string teks biasa, memungkinkan transmisi tanpa menarik perhatian, seperti dalam email atau pesan teks yang tampak normal tapi menyimpan informasi visual(Choudhari et al., 2023)(Aruna et al., 2023).

Dalam penelitian ini, kami mengembangkan aplikasi steganografi dual mode berbasis Java yang dapat menangani dua jenis penyembunyian data: menyembunyikan pesan teks ke dalam teks (text-to-text) dan menyembunyikan pesan gambar ke dalam teks (image-to-text). Aplikasi ini dilengkapi dengan fitur kata sandi sebagai lapisan keamanan ekstra untuk membatasi akses ke pesan rahasia. Penggunaan Java Swing sebagai antarmuka pengguna diharapkan memudahkan interaksi pengguna dan mendukung proses belajar di bidang keamanan informasi. Dengan pendekatan ini, aplikasi tidak hanya praktis untuk pengguna umum, tetapi juga edukatif bagi mahasiswa yang ingin memahami konsep steganografi melalui eksperimen langsung.

Melalui desain dan implementasi aplikasi ini, kami berharap bisa menghasilkan sistem steganografi sederhana yang efektif menjaga kerahasiaan pesan, sekaligus memberikan wawasan praktis tentang penerapan steganografi dalam

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

bentuk aplikasi desktop. Selain itu, aplikasi ini bisa menjadi fondasi untuk pengembangan lebih lanjut dalam keamanan data digital. Penelitian ini diharapkan berkontribusi pada literatur keamanan informasi, terutama dalam konteks aplikasi open-source yang dapat diakses oleh banyak orang, mendorong inovasi di bidang ini untuk menghadapi tantangan keamanan yang semakin kompleks.

TINJAUAN PUSTAKA

Steganografi adalah salah satu pendekatan dalam bidang keamanan informasi yang dirancang untuk menyembunyikan pesan rahasia di dalam media pembawa, sehingga keberadaannya tidak langsung terlihat. Media pembawa yang bisa digunakan termasuk teks, gambar, audio, atau video. Prinsip dasar steganografi adalah memastikan bahwa media tersebut tidak mengalami perubahan drastis setelah penyisipan pesan, agar tidak menarik perhatian dari pihak luar(Trithemius, n.d.). Dalam praktiknya, teknik ini telah digunakan sejak zaman kuno, seperti menyembunyikan pesan dalam tinta tak terlihat atau di bawah lapisan cat, dan kini berkembang dengan teknologi digital untuk melindungi data sensitif dari pengintaian.

Steganografi berbasis teks melibatkan penyembunyian pesan dengan memanfaatkan sifat-sifat unik dari teks itu sendiri. Teknik yang diterapkan bisa mencakup penyesuaian spasi, modifikasi format, atau proses encoding data. Keunggulan metode ini terletak pada kesederhanaannya dan kemudahan penerapannya, meskipun kapasitas penyimpanan data rahasia terbatas(Sari et al., 2025). Oleh sebab itu, dibutuhkan teknik yang dapat menyisipkan data tanpa merusak tampilan visual teks. Misalnya, dengan menggunakan algoritma seperti whitespace steganography, di mana spasi ekstra atau tabulasi dimanfaatkan untuk menyimpan bit-bit data, sehingga teks tetap terlihat normal bagi mata manusia tapi bisa didekode oleh sistem yang tepat.

Steganografi berbasis gambar menggunakan teknik penyembunyian pesan dengan memanfaatkan data piksel dalam citra digital. Salah satu metode populer adalah Least Significant Bit (LSB), yang melibatkan modifikasi bit terendah dari setiap piksel untuk menyisipkan pesan rahasia(Ashari et al., 2024). Metode ini sering dipilih karena dapat menjaga kualitas visual gambar meskipun data tambahan telah dimasukkan. Pada dasarnya, LSB bekerja dengan mengubah bit paling tidak signifikan dari nilai warna piksel, seperti merah, hijau, atau biru, tanpa mengubah tampilan gambar secara nyata, sehingga cocok untuk aplikasi di mana estetika penting dipertahankan.

Encoding Base64 adalah teknik pengkodean yang mengubah data biner menjadi representasi teks ASCII. Teknik ini umum digunakan dalam sistem komputer untuk mentransmisikan dan menyimpan data biner melalui saluran berbasis teks. Dalam konteks steganografi, Base64 bisa dimanfaatkan untuk mengonversi data gambar menjadi format teks, sehingga dapat disisipkan ke dalam media teks tanpa mengubah struktur data secara berarti(Satriyawibawa et al., 2024). Prosesnya melibatkan pembagian data biner menjadi grup 6-bit, yang kemudian dipetakan ke karakter ASCII, memungkinkan integrasi mulus antara data biner dan teks, seperti dalam protokol email atau penyimpanan file.

Java adalah bahasa pemrograman berorientasi objek yang populer untuk pengembangan aplikasi desktop, berkat sifat multiplatformnya dan pustaka yang komprehensif. Java Swing merupakan salah satu pustaka GUI di Java yang digunakan untuk membuat antarmuka pengguna yang interaktif dan user-friendly. Dengan Java Swing, pengembangan aplikasi steganografi dapat menghasilkan tampilan grafis yang mendukung interaksi langsung dengan pengguna. Pustaka ini menyediakan komponen seperti tombol, panel, dan dialog yang mudah dikustomisasi, memungkinkan pengembang untuk fokus pada logika aplikasi sambil memastikan pengalaman pengguna yang intuitif di berbagai platform.

Penerapan kata sandi dalam sistem steganografi berperan sebagai lapisan keamanan ekstra untuk mengontrol akses ke pesan rahasia. Mekanisme ini memastikan bahwa hanya mereka yang mengetahui kata sandi yang tepat yang bisa mengekstrak pesan(Patil & Sonaje, 2024). Hal ini tentu saja meningkatkan tingkat keamanan data dan mengurangi risiko akses yang tidak sah terhadap informasi yang tersembunyi. Kata sandi sering dikombinasikan dengan hashing atau enkripsi sederhana untuk mencegah brute-force attacks, sehingga bahkan jika seseorang menemukan media pembawa, mereka masih perlu kunci untuk mengakses isi rahasia.

Berdasarkan tinjauan literatur yang telah dilakukan, dapat disimpulkan bahwa steganografi yang memanfaatkan media teks dan gambar, didukung oleh teknik encoding serta mekanisme keamanan tambahan, merupakan pendekatan yang efektif untuk menjaga kerahasiaan informasi digital. Konsep-konsep ini menjadi fondasi bagi perancangan dan implementasi aplikasi steganografi dual mode dalam penelitian ini. Penelitian sebelumnya, seperti yang dilakukan oleh para ahli di bidang kriptografi, menunjukkan bahwa kombinasi steganografi dengan kriptografi dapat memberikan perlindungan ganda, membuat data tidak hanya tersembunyi tetapi juga tidak dapat dibaca tanpa kunci yang tepat.

JIKUM
JURNAL ILMU KOMPUTER

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

METODE PENELITIAN

Metode

Studi ini adalah metode pengembangan perangkat lunak (software development method). Pendekatan ini dipilih karena fokus penelitian adalah pada perancangan, pembuatan, dan pengujian aplikasi steganografi dual mode berbasis Java. Tahapan pengembangan sistem yang kami terapkan mencakup:

- **Analisis Kebutuhan:** Pada langkah ini, kami mengidentifikasi kebutuhan sistem, baik yang bersifat fungsional maupun nonfungsional. Kebutuhan fungsional mencakup kemampuan aplikasi untuk menyembunyikan dan mengekstrak pesan rahasia dalam format teks dan gambar dengan menggunakan kata sandi. Sedangkan kebutuhan nonfungsional meliputi kemudahan penggunaan, antarmuka yang menarik, serta keamanan data.
- **Perancangan Sistem:** Tahap ini dilakukan untuk menentukan struktur sistem, alur kerja, serta pembagian fungsi ke dalam kelas-kelas program. Tujuannya adalah agar sistem mudah dikembangkan dan dipelihara di masa depan.
- **Implementasi:** Di sini, kami menerapkan desain sistem ke dalam kode program menggunakan bahasa Java. Semua fungsi steganografi, pengamanan kata sandi, serta antarmuka pengguna diwujudkan sesuai dengan rencana sebelumnya.
- **Pengujian:** Pengujian dilakukan untuk memastikan setiap fitur aplikasi berfungsi dengan baik dan memenuhi kebutuhan. Ini meliputi uji coba proses penyembunyian dan ekstraksi data, baik untuk mode teks ke teks maupun teks ke gambar.

Perancangan Sistem

Aplikasi steganografi dual mode ini kami rancang dengan menggunakan konsep pemrograman berorientasi objek, dan terdiri dari tiga kelas utama, yaitu:

- **TextStego.java:** Kelas ini menangani proses steganografi pada media teks. Ini mencakup penyembunyian pesan rahasia ke dalam teks pembawa menggunakan teknik encoding, serta ekstraksi pesan dengan validasi kata sandi.
- **ImageStego.java:** Kelas ini bertugas mengelola konversi data gambar ke format Base64 dan sebaliknya. Kelas ini digunakan dalam mode steganografi teks ke gambar, di mana pesan rahasia disisipkan ke dalam representasi teks dari data gambar.
- **MainApp.java:** Kelas ini berfungsi sebagai antarmuka pengguna (Graphical User Interface) yang menghubungkan semua proses steganografi. Kelas ini mengatur interaksi pengguna, memanggil fungsi dari kelas TextStego dan ImageStego, serta menampilkan hasil proses kepada pengguna.

Alur Sistem

Alur kerja aplikasi steganografi dual mode ini bisa dijelaskan sebagai berikut:

- Pengguna memilih jenis steganografi yang ingin digunakan, apakah teks ke teks atau teks ke gambar.
- Pengguna memasukkan teks pembawa atau memilih file gambar sebagai media penyisipan.
- Pengguna memasukkan pesan rahasia dan kata sandi sebagai pengaman.
- Sistem kemudian melakukan proses penyembunyian data dengan menggabungkan pesan rahasia ke dalam media yang dipilih.
- Untuk ekstraksi, pengguna memasukkan media hasil steganografi beserta kata sandi.
- Sistem memverifikasi kata sandi dan menampilkan pesan atau gambar tersembunyi jika kata sandi cocok.

Alur kerja sistem dalam aplikasi steganografi dual mode ini diilustrasikan melalui flowchart untuk memfasilitasi pemahaman proses penyembunyian dan ekstraksi data. Flowchart ini menguraikan langkah-langkah mulai dari pemilihan mode, masukan data, verifikasi kata sandi, hingga tahap penyimpanan atau tampilan hasil. Dalam konteks pengembangan perangkat lunak, visualisasi seperti ini membantu pengguna dan pengembang untuk melihat alur logis secara sistematis, meminimalkan kesalahpahaman, dan memastikan bahwa setiap komponen terintegrasi dengan baik.

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

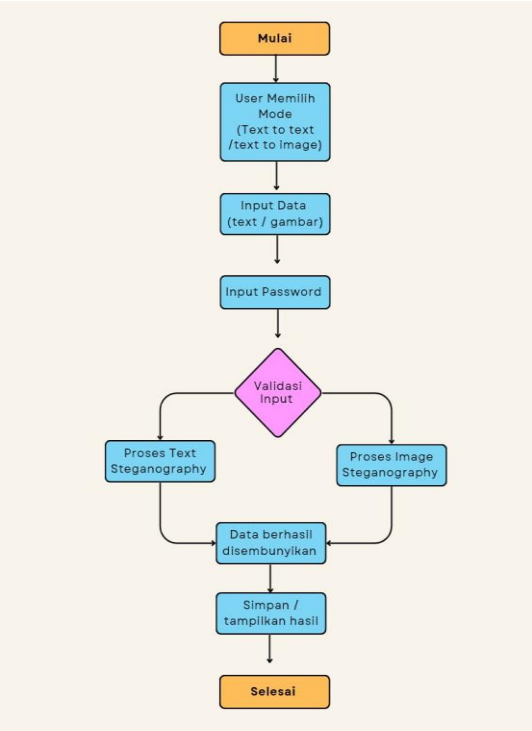

Fig. 1 Flowchart Sistem

Implementasi Sistem

Aplikasi steganografi dual mode ini kami implementasikan dengan menggunakan teknologi berikut:

- Bahasa pemrograman: Java
- Lingkungan pengembangan: Apache NetBeans
- Antarmuka pengguna: Java Swing

Fitur utama yang berhasil kami wujudkan dalam aplikasi ini meliputi:

- **Text to Text Steganography:** Penyembunyian pesan rahasia ke dalam teks pembawa.
- **Text to Image Steganography:** Penyembunyian pesan rahasia ke dalam data gambar melalui representasi Base64.
- **Proteksi kata sandi:** Untuk memastikan hanya pengguna yang tahu kata sandi yang bisa mengekstrak data tersembunyi.
- **Tampilan antarmuka modern:** Dengan desain GUI yang sederhana, intuitif, dan mudah digunakan. Metode penelitian menjelaskan rancangan kegiatan, ruang lingkup atau objek, bahan dan alat utama, tempat, teknik pengumpulan data, definisi operasional variabel penelitian, dan teknik analisis.

HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem

Dari penelitian ini, kami berhasil menghasilkan sebuah aplikasi steganografi dual mode berbasis Java yang bisa menyembunyikan data rahasia ke dalam media teks. Aplikasi ini dibangun menggunakan bahasa pemrograman Java dengan antarmuka grafis yang didasarkan pada Java Swing. Sistem ini menawarkan dua mode utama: penyembunyian teks ke dalam teks (Text to Text Steganography) dan penyembunyian gambar ke dalam teks (Text to Image Steganography), keduanya dilengkapi dengan fitur proteksi kata sandi.

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

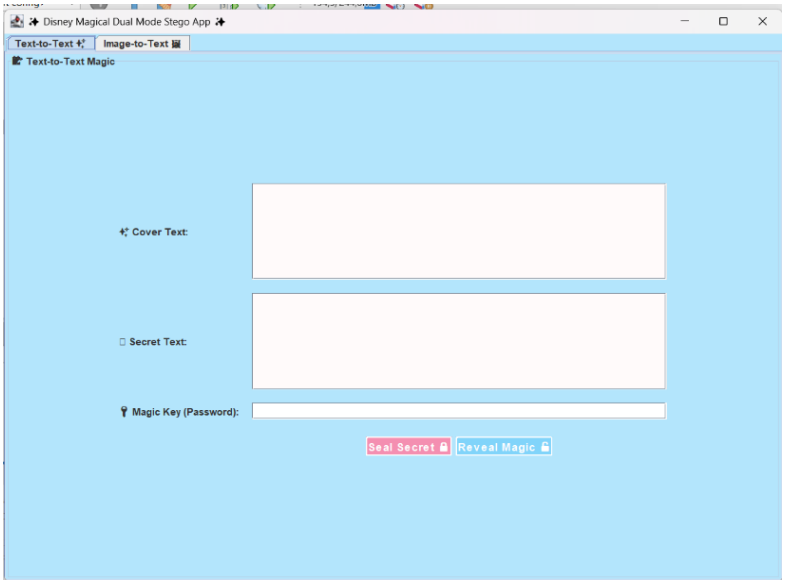

Fig. 2 Tampilan Utama Aplikasi

Pada mode Text to Text, pengguna bisa memasukkan teks pembawa (cover text), teks rahasia, dan kata sandi. Setelah proses penyembunyian selesai, sistem menghasilkan teks steganografi yang terlihat seperti teks biasa, tapi sebenarnya menyimpan pesan rahasia di dalamnya. Pesan itu hanya bisa diekstrak kembali jika pengguna memasukkan kata sandi yang tepat.

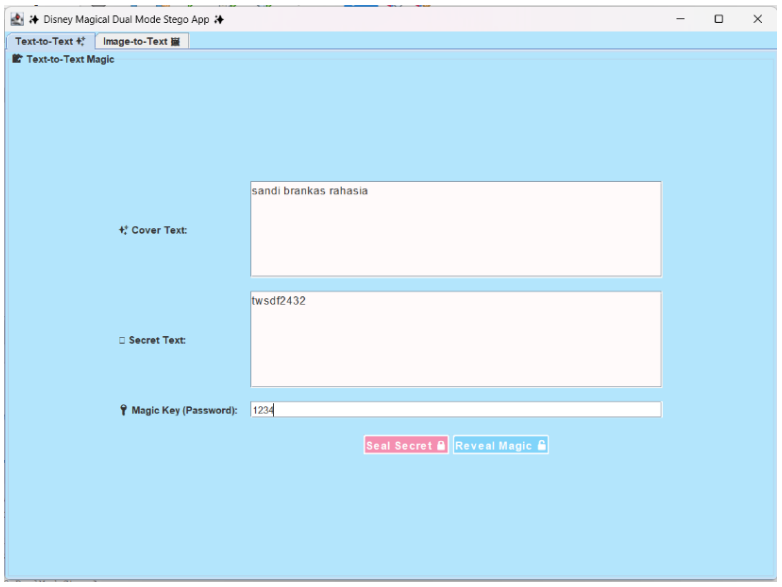

Fig. 3 Proses penyembunyian text to text

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

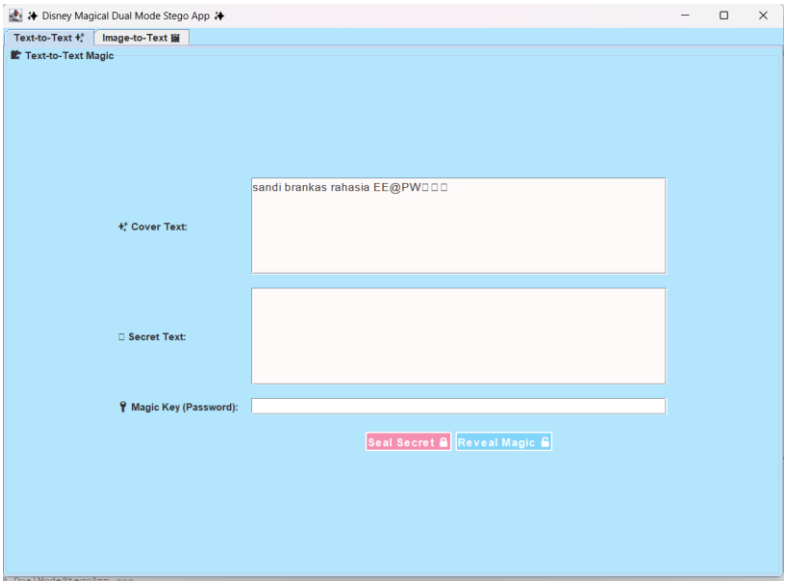

Fig. 4 Hasil ekstrasi text to text

Untuk mode Text to Image, sistem memungkinkan pengguna memilih file gambar, yang kemudian dikonversi ke format Base64 dan disisipkan ke dalam teks. Hasilnya adalah teks steganografi yang berisi representasi gambar tersembunyi. Ekstraksi dilakukan dengan memasukkan kata sandi yang benar, sehingga sistem bisa mendekode data Base64 dan menampilkan gambar asli.

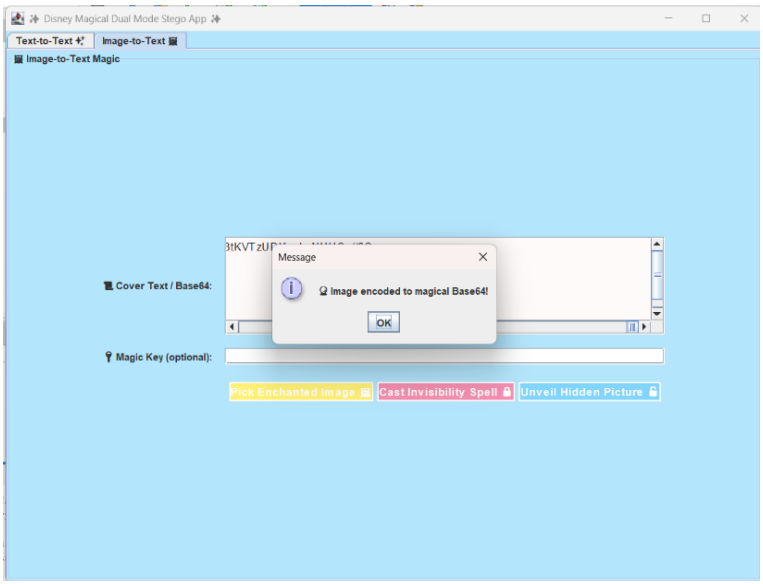

Fig. 5 Proses penyembunyian text to image

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

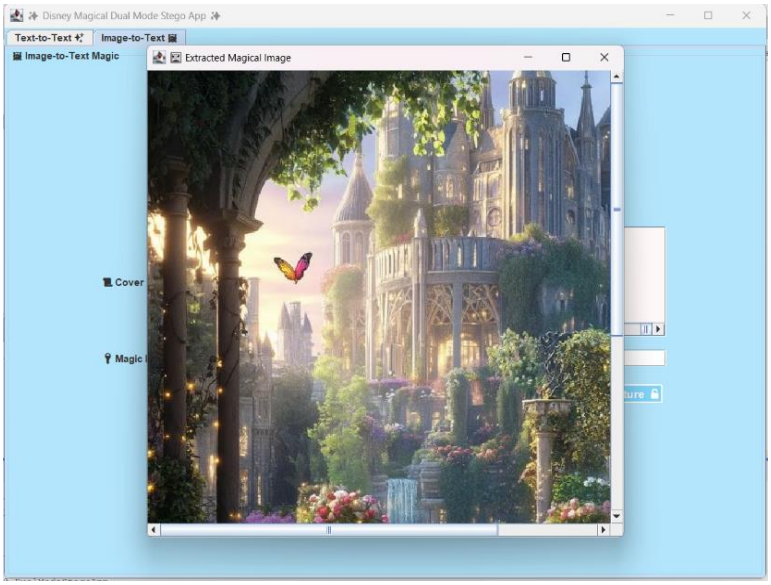

Fig. 6 Hasil ekstrasi image to text

Pengujian fungsional menunjukkan bahwa semua fitur utama aplikasi berjalan lancar sesuai rencana, termasuk proses penyembunyian data, ekstraksi, dan validasi kata sandi di kedua mode steganografi.

Pembahasan

Berdasarkan hasil implementasi dan pengujian, aplikasi steganografi dual mode yang kami kembangkan telah berhasil mencapai tujuan penelitian, yakni menyediakan cara untuk menyembunyikan informasi berbasis teks dengan keamanan tambahan melalui kata sandi. Penggunaan format Base64 di mode Text to Image ternyata efektif untuk mengubah data gambar menjadi teks, sehingga bisa disisipkan tanpa mengganggu struktur teks pembawa.

Fitur proteksi kata sandi sangat penting untuk mencegah akses yang tidak sah ke data tersembunyi. Hasil pengujian membuktikan bahwa data rahasia tidak bisa diekstrak jika kata sandi yang dimasukkan salah, baik di mode Text to Text maupun Text to Image. Ini menunjukkan bahwa sistem memiliki lapisan keamanan yang cukup baik di tingkat aplikasi.

Dari segi antarmuka pengguna, Java Swing membuat aplikasi stabil di lingkungan desktop dan mudah digunakan. Pembagian fitur ke dalam dua mode yang jelas membantu pengguna memahami fungsi aplikasi tanpa perlu konfigurasi rumit. Meski begitu, aplikasi ini masih punya keterbatasan, seperti ketergantungan pada teks sebagai media utama dan belum adanya mekanisme kompresi atau enkripsi lanjutan untuk meningkatkan keamanan data.

Secara keseluruhan, aplikasi yang kami buat telah menjadi solusi praktis untuk menyembunyikan informasi berbasis teks dan gambar, dan bisa dijadikan fondasi untuk penelitian lanjutan, seperti mengintegrasikan algoritma kriptografi yang lebih kuat atau menggunakan media lain sebagai pembawa data.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah kami lakukan, dapat disimpulkan bahwa aplikasi steganografi dual mode berbasis Java yang dikembangkan telah berhasil beroperasi sesuai dengan tujuan penelitian. Aplikasi ini mampu menyembunyikan dan mengekstrak data rahasia, baik dalam format teks maupun gambar, dengan menggunakan media teks sebagai wadah informasi.

Mode Text to Text memungkinkan penyembunyian pesan rahasia ke dalam teks biasa tanpa mengubah penampilannya secara drastis, sedangkan mode Text to Image dapat mengonversi data gambar ke format Base64 sehingga bisa disisipkan ke dalam teks dan kemudian diekstrak kembali menjadi file gambar. Penggunaan kata sandi di kedua mode menambahkan lapisan keamanan ekstra, dengan membatasi akses ke data tersembunyi hanya untuk mereka yang memiliki kata sandi yang benar.

Hasil pengujian menunjukkan bahwa semua fitur utama aplikasi berjalan lancar, termasuk validasi kata sandi, proses penyembunyian data, dan ekstraksi data. Dengan begitu, aplikasi ini bisa berfungsi sebagai solusi praktis untuk menyembunyikan informasi berbasis teks, sekaligus sebagai alat pembelajaran untuk memahami konsep steganografi.

Untuk pengembangan lebih lanjut, aplikasi steganografi ini masih bisa diperbaiki dari beberapa sisi. Kami sarankan untuk menambahkan algoritma kriptografi yang lebih tangguh sebelum proses penyembunyian data, agar

JIKUM
JURNAL ILMU KOMPUTER

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

tingkat keamanan informasi bisa ditingkatkan. Selain itu, memperluas penggunaan media pembawa lain seperti gambar atau audio sebagai cover juga bisa menjadi pilihan untuk menambah fungsi aplikasi.

Dari segi antarmuka, desain aplikasi bisa dikembangkan lebih jauh agar lebih interaktif dan responsif, mungkin dengan menggunakan framework GUI yang lebih canggih. Pengujian performa dan keamanan yang lebih mendalam juga kami rekomendasikan, untuk memastikan aplikasi tetap andal saat menangani data berukuran besar dan menghadapi ancaman analisis steganografi.berisi rangkuman tentang apa yang dipelajari dari hasil yang diperoleh, apa yang perlu ditingkatkan dalam penelitian selanjutnya. Ciri umum lain dari kesimpulan adalah manfaat dan penerapan penelitian, keterbatasan, dan rekomendasi berdasarkan hasil yang diperoleh.

REFERENSI

Aruna, M. T. N., Nandika, L. R., Sneha, C. I., Xavier, imothy J., & George, T. M. (2023). Text, Image and Audio Steganography. *International Journal for Research in Applied Science and Engineering Technology*, *11*(4), 4435–4439. https://doi.org/10.22214/ijraset.2023.51091

Ashari, I. F., Nugroho, E. D., Andrianto, D. D., Yusuf, M. A. N. M., & Alkarkhi, M. (2024). The Evaluation of LSB Steganography on Image File Using 3DES and MD5 Key. *JITCE (Journal of Information Technology and Computer Engineering)*, *8*(1), 8–18. https://doi.org/10.25077/jitce.8.1.8-18.2024

Choudhari, D., Hetvi Patel, H. P., Ghosh, A., Patil, N., Pawar, V., & Sonawane, Y. (2023). A Survey on Image Steganography using LSB Algorithm. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4671618

Kallapu, B., Janardhan, A. N., Hejamadi, R. M., Shrinivas, K. R. N., Saritha, Ramesh, R. K., & Gabralla, L. A. (2025). Multi-Layered Security Framework Combining Steganography and DNA Coding. *Systems*, *13*(5), 1–27. https://doi.org/10.3390/systems13050341

Krisna, I Gusti Ngurah Febri Ananda Karyawati, A. E. (2024). *Penerapan Teknik Steganografi LSB pada Format Gambar Modern*. *2*, 673–680.

Muhammad, A., Agus, A., Mujahid, M. R., Negeri, U., & Makassar, K. (n.d.). *The Security of Recent LSB Steganography Algorithms for Protecting Secret Text Messages*. *1*, 12–16.

Patil, H. V, & Sonaje, V. P. (2024). Crypto-Stego: A Hybrid Method for Encrypting Text Messages or Text Files within Images Using AES and LSB Algorithms. *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE*, *2024*(23s), 2780–2793. www.ijisae.org

Sari, I. P., Basri, M., & Syafrayani, P. R. (2025). *Implementasi Sistem Aplikasi Pengolahan Teks pada Gambar Menggunakan Modifikasi Metode LSB dan ROT13*. 0–7.

Satriyawibawa, M. Y., Andono, P. N., Soong, L. W., & Kiat, N. P. (2024). LSB-2 Steganography with Brotli Compression and base64 Encoding for Improving Data Embedding Capacity. *Sinkron*, *8*(2), 878–884. https://doi.org/10.33395/sinkron.v8i2.13264

Trithemius, J. (n.d.). *Steganography*.