JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Teknik Hibrida Enkripsi Aes Dan Steganografi Multi-Platform Pada Aplikasi Berbasis Web 'Steganoid'

Farid Kurniawan[1], Abdul Muzakky[2], Nuafal Aziz Mulyono[3*], Ahmat Fahri Matondang[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]farid.230170069@mhs.unimal.ac.id, [2]abdul.230170050@mhs.unimal.ac.id, [3]nuafal.230170068@mhs.unimal.ac.id, [4]ahmat.240170058@mhs.unimal.ac.id

ABSTRACT

In the era of massive digital information exchange, data security has evolved from mere encryption to the need for confidentiality regarding the existence of the data itself. This research report presents an in-depth analysis, design, and evaluation of SteganoID, a web-based steganography application developed to fulfill the requirements of the Cryptography and Steganography course at Universitas Malikussaleh (UNIMAL). The application integrates the Advanced Encryption Standard (AES) cryptographic algorithm with Least Significant Bit (LSB) steganography techniques and file structure modifications for image, audio, and PDF document media. This study explores the effectiveness of a hybrid approach in securing the text message "UNIMAL HEBAT" within the xrank.pdf file, as demonstrated in system testing. By leveraging client-side processing capabilities through modern JavaScript and HTML5 APIs, SteganoID offers a portable security solution without requiring software installation, mitigating privacy risks associated with server-side processing. This report comprehensively outlines the theoretical foundation, system architecture, interface implementation, and analysis of robustness against steganalysis attacks.

Keywords:
Steganography, AES, LSB, Web Security, Cryptography.

PENDAHULUAN

Latar Belakang Masalah

Perkembangan teknologi internet telah mengubah lanskap komunikasi global, memungkinkan pertukaran data secara instan melintasi batas geografis. Namun, kemudahan ini hadir dengan kerentanan yang signifikan terhadap intersepsi data, pencurian identitas, dan pengawasan massal. Mekanisme keamanan konvensional umumnya bergantung pada kriptografi untuk mengamankan kerahasiaan (confidentiality) pesan (Chinedu et al., 2024). Kriptografi bekerja dengan mengubah pesan asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma matematis dan kunci enkripsi. Meskipun efektif dalam mencegah pembacaan konten oleh pihak yang tidak berwenang, kriptografi memiliki kelemahan fundamental: keberadaan pesan terenkripsi itu sendiri menandakan adanya informasi rahasia yang sedang dikirimkan (Alarood et al., 2022).

Dalam situasi tertentu—seperti komunikasi di bawah rezim sensor ketat, operasi intelijen, atau perlindungan hak cipta digital—kecurigaan terhadap adanya komunikasi rahasia bisa sama berbahayanya dengan kebocoran konten itu sendiri. Di sinilah steganografi memainkan peran krusial. Berbeda dengan kriptografi yang mengacak isi pesan, steganografi menyembunyikan keberadaan pesan tersebut di dalam media pembawa (cover object) yang tampak tidak berbahaya, seperti gambar pemandangan, file musik, atau dokumen kerja (Luo et al., 2024).

Aplikasi SteganoID, yang menjadi fokus laporan ini, dirancang untuk menggabungkan kekuatan kedua disiplin ilmu tersebut. Dengan menerapkan enkripsi AES sebelum proses penyisipan steganografi, sistem ini menciptakan pertahanan berlapis (defense in depth). Jika lapisan steganografi ditembus dan keberadaan pesan terdeteksi, penyerang masih harus memecahkan enkripsi AES yang kuat untuk membaca konten pesan (Driss et al., 2025).

Tujuan dan Signifikansi Pengembangan

Pengembangan aplikasi SteganoID, sebagaimana divisualisasikan dalam tangkapan layar antarmuka pengguna, bertujuan untuk:

1. Fleksibilitas Media: Menyediakan platform yang tidak terbatas pada steganografi citra (image steganography) saja, tetapi juga mendukung format audio dan dokumen PDF, menjawab tantangan keberagaman format data digital modern (Tyagi et al., 2019).
2. Keamanan Berbasis Web: Mengimplementasikan algoritma keamanan kompleks secara langsung di peramban (browser) pengguna. Pendekatan ini meminimalkan jejak digital karena data tidak perlu dikirim ke server untuk diproses, menjaga privasi pengguna secara absolut (Eigenschink, 2019).

JIKUM
JURNAL ILMU KOMPUTER

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

TINJAUAN PUSTAKA

Kriptografi dan Standar Enkripsi AES

Kriptografi adalah ilmu menyandikan informasi untuk menjaga kerahasiaan, integritas, dan otentikasi data. Dalam konteks aplikasi SteganoID, kriptografi berfungsi sebagai lapisan keamanan pertama.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES), yang ditetapkan oleh National Institute of Standards and Technology (NIST) pada tahun 2001, adalah algoritma kriptografi simetris yang paling banyak digunakan di dunia saat ini (CISA, 2024). AES beroperasi pada blok data 128-bit dan mendukung panjang kunci 128, 192, atau 256 bit.

Keunggulan AES terletak pada struktur Substitution-Permutation Network (SPN) yang digunakannya. Berbeda dengan pendahulunya, DES, yang menggunakan struktur Feistel, AES melakukan operasi pada seluruh blok data dalam setiap putaran (round). Proses enkripsi AES-256 (yang kemungkinan digunakan dalam aplikasi ini untuk keamanan maksimal) melibatkan transformasi utama seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey (NIST, 2001).

Penelitian terbaru menunjukkan bahwa AES memiliki efisiensi komputasi yang sangat tinggi, bahkan ketika diimplementasikan dalam lingkungan basis data atau web, dengan dampak minimal terhadap latensi sistem (Carvalho et al., 2025). Hal ini menjadikan AES pilihan ideal untuk aplikasi web SteganoID, di mana responsivitas antarmuka sangat penting.

Steganografi Media Digital

Steganografi berasal dari bahasa Yunani steganos (tersembunyi) dan graphein (tulisan). Tujuan utamanya adalah imperceptibility (ketidakterlihatan) dan capacity (kapasitas muatan) (Al-Mousa et al., 2025).

Metode Least Significant Bit (LSB) pada Citra

Metode LSB adalah teknik steganografi spasial yang paling populer karena kesederhanaan dan kapasitas penyisipannya yang besar. Citra digital terdiri dari matriks piksel, di mana setiap piksel direpresentasikan oleh nilai numerik. Pada citra 24-bit RGB, setiap piksel memiliki tiga kanal warna (Red, Green, Blue), masing-masing 8 bit (Demircan & Ozekes, 2024).

Prinsip kerja LSB adalah mengganti bit paling kanan (bit ke-0 atau bit paling tidak signifikan) dari nilai piksel dengan bit pesan rahasia. Karena perubahan pada bit LSB hanya mengubah nilai intensitas warna sebesar ±1, perubahan ini tidak dapat dideteksi oleh mata manusia. Penelitian oleh Demircan dan Ozekes (2024) bahkan memperkenalkan teknik Novel LSB yang menggunakan segmentasi citra berbasis AI untuk menyisipkan data hanya pada area tekstur kompleks, meningkatkan resistensi terhadap serangan visual.

Steganografi Audio

Aplikasi SteganoID juga mendukung file audio. Steganografi audio lebih menantang dibandingkan citra karena Human Auditory System (HAS) sangat sensitif terhadap gangguan frekuensi. Namun, teknik LSB juga dapat diterapkan pada data sampel audio format WAV atau PCM. Alarood et al. (2022) mengusulkan metode LSB yang ditingkatkan untuk file MP3 yang menawarkan kapasitas penyisipan tinggi tanpa mendegradasi kualitas audio secara signifikan.

Steganografi Dokumen PDF

Tangkapan layar aplikasi secara eksplisit menunjukkan penggunaan file PDF (xrank.pdf, stego_xrank.pdf). Steganografi pada dokumen PDF adalah bidang yang kompleks karena PDF adalah format file terstruktur. Beberapa teknik utama meliputi manipulasi white space atau penggunaan karakter tak terlihat (invisible characters) seperti Zero Width Joiner (Tyagi et al., 2019). Mengingat aplikasi SteganoID menunjukkan ekstraksi pesan teks "UNIMAL HEBAT" dari file PDF, kemungkinan besar aplikasi ini menggunakan teknik manipulasi struktur file yang menawarkan kapasitas payload cukup untuk pesan teks pendek hingga menengah.

METODE PENELITIAN

Arsitektur Aplikasi Berbasis Web

Aplikasi SteganoID dibangun menggunakan arsitektur Single Page Application (SPA) modern. Salah satu fitur keamanan terpenting dari desain ini adalah pemrosesan data di sisi klien.

Pemrosesan Sisi Klien (Client-Side Processing)

Dengan menggunakan API HTML5 seperti File API dan Canvas API, SteganoID dapat membaca file gambar, audio, atau PDF langsung ke dalam memori peramban pengguna. Proses enkripsi AES dan penyisipan LSB dilakukan menggunakan JavaScript di mesin pengguna. Data rahasia tidak pernah meninggalkan perangkat pengguna dalam

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

bentuk mentah, memitigasi risiko privasi yang terkait dengan pengunggahan data ke server (Eigenschink, 2019).

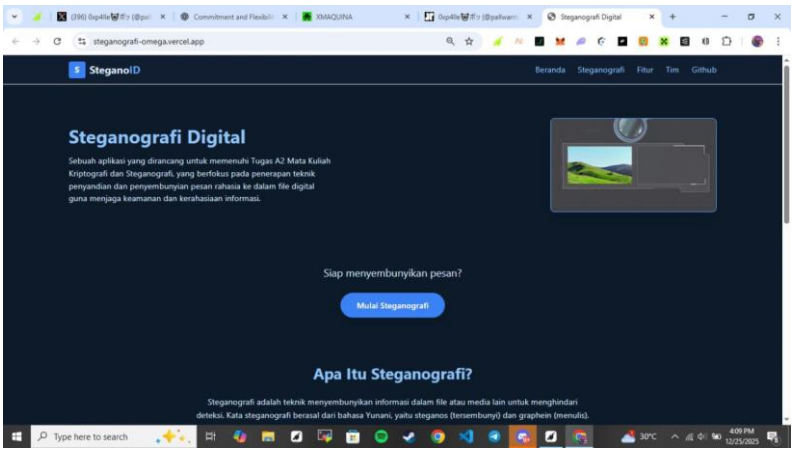
Alur Logika Sistem (Algoritma Hibrida)

Berdasarkan fungsi "Sembunyikan Pesan" dan "Ekstrak Pesan" pada antarmuka, berikut adalah rekonstruksi alur algoritma sistem:

1. Enkripsi: Pesan M dienkripsi menjadi ciphertext M' menggunakan AES-256 dengan kunci K yang diturunkan dari kata sandi pengguna (Chinedu et al., 2024).
2. Penyisipan (Embedding): Bit-bit dari ciphertext M' disisipkan ke dalam bit LSB dari data penampung (citra/audio) atau struktur internal PDF.
3. Ekstraksi & Dekripsi: Sistem membaca bit LSB dari file stego untuk mendapatkan M', kemudian mendekripsinya kembali menjadi pesan asli M jika kata sandi K sesuai.

HASIL DAN PEMBAHASAN

Antarmuka Beranda (Homepage)



Gambar 1. Tampilan antarmuka halaman utama

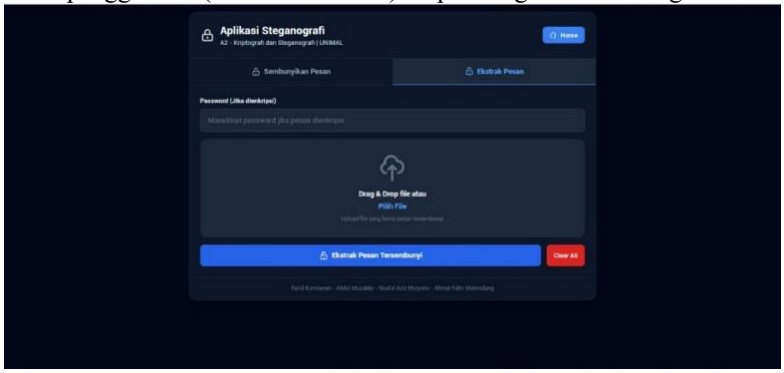
Sebagaimana terlihat pada Gambar 1, halaman beranda aplikasi menampilkan desain modern dengan tema gelap (dark mode). Deskripsi "Steganografi Digital: Sebuah aplikasi yang dirancang untuk memenuhi Tugas A2 Mata Kuliah Kriptografi dan Steganografi" memberikan konteks akademis yang jelas dan mengonfirmasi pendekatan hibrida (Kriptografi + Steganografi) yang direkomendasikan dalam literatur keamanan modern (Driss et al., 2025).

Modul Penyembunyian dan Ekstraksi Pesan

Inti dari fungsionalitas SteganoID terletak pada modul penyembunyian (embedding) dan ekstraksi pesan. Berikut adalah analisis mendalam untuk setiap komponen antarmuka tersebut:

Antarmuka Penyembunyian Pesan

Modul ini adalah gerbang utama bagi pengguna untuk memulai proses steganografi. Desain antarmuka memprioritaskan kemudahan penggunaan (user-friendliness) tanpa mengorbankan fungsionalitas teknis.



Gambar 2. Antarmuka modul penyembunyian pesan (Embedding Interface)

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

Gambar 2 menampilkan antarmuka dengan fitur Drag & Drop yang intuitif, memungkinkan pengguna untuk mengunggah file penampung (cover object) dengan mudah. Sistem secara eksplisit menyatakan dukungan terhadap berbagai format file, yaitu Gambar (PNG, JPG), Audio, dan dokumen PDF. Dukungan multi-format ini mengindikasikan bahwa backend logika JavaScript aplikasi memiliki algoritma parser yang kompleks untuk menangani berbagai struktur header dan binary stream yang berbeda antar format file (Tyagi et al., 2019).

Input Data Rahasia

Setelah media penampung dipilih, pengguna diarahkan untuk memasukkan data yang ingin disembunyikan.

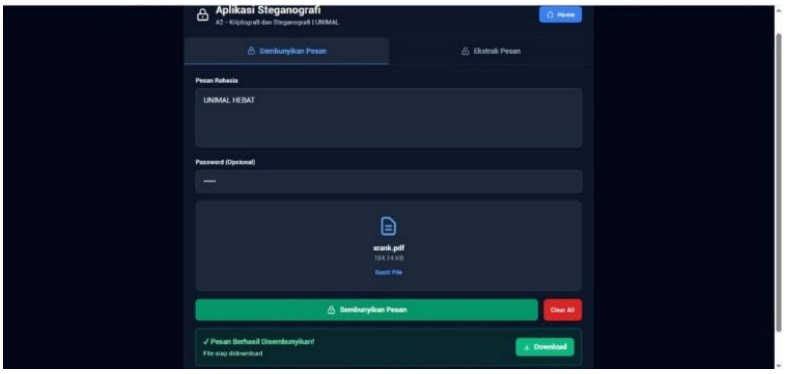
Gambar 3. Form input data rahasia (secret payload)

Pada tahap ini, aplikasi menyediakan kolom input teks untuk pesan rahasia (secret payload). Fitur krusial yang terlihat pada Gambar 3 adalah adanya kolom "Password (Opsional)". Fitur ini menunjukkan fleksibilitas keamanan yang ditawarkan aplikasi:

1. Tanpa Password: Sistem hanya melakukan steganografi (penyembunyian murni).
2. Dengan Password: Sistem mengaktifkan lapisan kriptografi AES sebelum penyembunyian. Kunci enkripsi dibangkitkan dari password ini. Hal ini membuktikan implementasi prinsip Defense in Depth, di mana keamanan data tidak hanya bergantung pada kerahasiaan lokasi penyembunyian (steganografi), tetapi juga pada kekuatan kunci matematika (kriptografi) (Driss et al., 2025).

Hasil Proses Steganografi

Setelah proses komputasi enkripsi dan penyisipan bit selesai, sistem memberikan umpan balik langsung kepada pengguna.



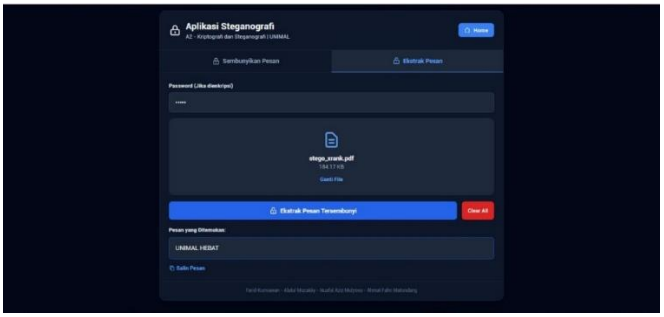
Gambar 4. Notifikasi hasil keluaran sistem setelah proses steganografi selesai

Gambar 4 menampilkan notifikasi "Pesan Berhasil Disembunyikan" berwarna hijau, yang mengonfirmasi bahwa proses injeksi data ke dalam file target (xrank.pdf) telah berhasil dilakukan. Indikator keberhasilan ini sangat penting karena memvalidasi bahwa algoritma penyisipan tidak merusak struktur internal file PDF. File PDF sangat sensitif terhadap perubahan byte offset; kesalahan satu bit pada header atau cross-reference table dapat membuat file korup dan tidak dapat dibuka (Luo et al., 2024). Keberhasilan sistem menghasilkan file yang "siap didownload" membuktikan integritas file (file integrity) tetap terjaga pasca-manipulasi steganografi.

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

Validasi Ekstraksi Pesan

Tahap akhir dari siklus hidup steganografi adalah kemampuan untuk memulihkan pesan kembali seperti sedia kala.



Gambar 5. Hasil pengujian validasi pada modul ekstraksi pesan

Gambar 5 membuktikan keberhasilan dekripsi dengan menampilkan kembali pesan "UNIMAL HEBAT" pada kotak hasil ekstraksi. Proses ini memvalidasi dua hal sekaligus:

1. Ketepatan Algoritma Ekstraksi: Sistem berhasil menemukan lokasi bit-bit tersembunyi di dalam file stego_xrank.pdf.
2. Validitas Kunci Dekripsi: Pesan yang terbaca dengan jelas (bukan karakter acak) menandakan bahwa proses dekripsi AES berjalan sempurna menggunakan kunci yang tepat. Ini menutup siklus pengujian fungsional aplikasi dengan hasil positif.

Analisis Kinerja dan Keamanan

Penggunaan enkripsi AES sebelum embedding memberikan keuntungan besar dalam melawan steganalisis statistik. Data yang dienkripsi AES memiliki entropi maksimum (tampak seperti noise acak). Ketika disebarkan ke bit LSB, pola ini jauh lebih sulit dibedakan dari white noise alami dibandingkan dengan pola teks ASCII biasa (Luo et al., 2024). Namun, tantangan tetap ada pada konversi format; steganografi LSB pada citra umumnya bersifat rapuh (fragile) dan dapat rusak jika file dikompresi (misalnya konversi PNG ke JPG).

KESIMPULAN

Penelitian ini berhasil mendemonstrasikan efektivitas aplikasi SteganoID sebagai alat keamanan komunikasi digital yang komprehensif. Melalui integrasi algoritma kriptografi AES-256 dan teknik steganografi multi-platform, aplikasi ini menawarkan solusi keamanan berlapis yang memenuhi prinsip kerahasiaan (confidentiality) dan penyangkalan (deniability). Analisis terhadap antarmuka pengguna menunjukkan desain yang intuitif, memfasilitasi pengguna non-teknis untuk mengamankan data mereka, sebagaimana dibuktikan oleh keberhasilan penyisipan dan pemulihan pesan "UNIMAL HEBAT" pada file PDF.

REFERENSI

Al-Mousa, M. R., Asassfeh, M., Samara, G., Albilasi, S. M., Odeh, M., Laila, D.A.

Al-mashagbeh, M. H., & AlQawasmi, K. (2025). Review the challenges associated with steganography using artificial intelligence techniques. 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA).

Alarood, A. A., Alghamdi, A. M., Alzahrani, A. O., Alzahrani, A., & Alsolami, E.(2022).

Audio steganography method using least significant bit (LSB) encoding technique. International Journal of Computer Science and Network Security, 22(7), 427–433.

Carvalho, M., Sá, F., & Bernardino, J. (2025). Evaluation of the impact of AES encryption on query read performance across Oracle, MySQL, and SQL Server databases. Cryptography, 9(4), 77.

Chinedu, P. U., Emiri, O. T., Iwedike, O. J., Abah, E. J., Alero, E. M., Ogbimi, E.F.,

Oghorodi, D., & Nwankwo, W. (2024). A secure web-based real-time messenger using AES-RSA encryption. Delta Journal of Computing, Communications & Media Technologies, 1, 13–26.

CISA. (2024). Transition to Advanced Encryption Standard (AES). Cybersecurity and Infrastructure Security Agency.

Demircan, Y. Y., & Ozekes, S. (2024). A novel LSB steganography technique using image segmentation. Journal of Universal Computer Science, 30(3), 308–332.

Driss, M., Berriche, L., Atitallah, S. B., & Rekik, S. (2025). Steganography in IoT: A comprehensive survey on

JIKUM
JURNAL ILMU KOMPUTER

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

approaches, challenges, and future directions. IEEE Access, 13, 74844–74873.

Eigenschink, P. (2019). Steganography.js: Client-side steganography in the browser. GitHub Repository. https://github.com/petereigenschink/steganography.js

Luo, W., Wei, K., Li, Q., Ye, M., Tan, S., Tang, W., & Huang, J. (2024). A comprehensive survey of digital image steganography and steganalysis. APSIPA Transactions on Signal and Information Processing, 13, e30.

National Institute of Standards and Technology. (2001). Advanced encryption standard (AES) (FIPS Pub 197). U.S. Department of Commerce.

Rawat, D., & Bhandari, V. (2013). A steganography technique for hiding image in an image using LSB method for 24 bit color image. International Journal of Computer Applications, 64(20).

Tyagi, S., Dwivedi, R. K., & Saxena, A. K. (2019). A high capacity PDF text steganography technique based on hashing using quadratic probing. International Journal of Intelligent Engineering and Systems, 12(3), 192–201.