JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Teknik Penyembunyian Data Non-Destruktif pada Citra Digital Menggunakan Metode End-of-File (EOF) dan Enkripsi AES-256

Muhammad Ulya Farhan[1], Fathul Barri Akbar[2],Ammar Fatin[3], Ariifah Yaasir Harahap[4]
[1,2,3,4] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Malikussaleh, Indonesia.
[1]muhammad.240170155@mhs.unimal.ac.id, [2]fathul.240170221@mhs.unimal.ac.id,
[3]ammar.240170164@mhs.unimal.ac.id, [4]ariifah.240170219@mhs.unimal.ac.id

ABSTRACT

Conventional cryptography and LSB steganography often suffer from detectability and visual distortion. This study proposes a non-destructive solution integrating End-of-File (EOF) steganography with AES-256 encryption to ensure data security without compromising carrier media quality. The method functions by appending encrypted data after the image file terminator, leaving the original pixel structure intact. Security is reinforced using AES-256 (CBC mode) and PBKDF2-HMAC-SHA256 with 100,000 iterations. Experimental results using the "PrivaSel" interface demonstrate perfect visual integrity, evidenced by identical histograms between original and stego images. Validation via Hex Editor confirms data insertion through a unique "AES-EOF" marker. Consequently, this system achieves an optimal balance between confidentiality and invisibility, preserving 100% of carrier media integrity for secure digital exchange.

Keywords: *Non-Destructive, EOF Steganography, AES-256 Encryption, Image Integrity, Data Security.*

PENDAHULUAN

Dalam era pertukaran informasi digital yang masif, melindungi kerahasiaan data menjadi prioritas utama. Kriptografi telah lama digunakan untuk mengacak informasi agar tidak terbaca, namun *ciphertext* yang dihasilkan seringkali menarik perhatian pihak ketiga karena sifatnya yang mencurigakan. Steganografi hadir sebagai solusi untuk menyembunyikan eksistensi pesan tersebut di dalam media lain, seperti citra digital(Cheddad et al., 2010; Stallings, 2017).

Meskipun demikian, teknik steganografi yang populer seperti *Least Significant Bit* (LSB) memiliki kelemahan mendasar: teknik ini memodifikasi bit-bit data warna pada citra. Sekecil apapun modifikasi tersebut, hal ini bersifat "destruktif" karena mengubah nilai asli piksel, yang berpotensi menimbulkan distorsi visual atau terdeteksi melalui analisis statistik atau *steganalysis* (Fridrich, 2009).

Penelitian ini berfokus pada pendekatan non-destruktif menggunakan metode *End-of-File* (EOF). Metode ini memanfaatkan karakteristik format file gambar yang memiliki penanda akhir (*terminator*). Data disisipkan setelah penanda ini, sehingga tidak mengganggu struktur data piksel sama sekali. Untuk memastikan keamanan data yang disisipkan, penelitian ini mengintegrasikan algoritma AES-256 (*Advanced Encryption Standard*) dengan penguatan kunci berbasis PBKDF2. Tujuan akhirnya adalah menghasilkan sistem yang tidak hanya aman dari upaya peretasan, tetapi juga menjaga integritas visual media pembawa secara sempurna.

TINJAUAN PUSTAKA

Konsep Steganografi Non-Destruktif (EOF) Steganografi EOF bekerja dengan cara menambahkan data di bagian ekor file atau *append*(Al-Othmani et al., 2012). Format file gambar seperti JPEG dan PNG memiliki byte penanda akhir (misalnya 0xFFD9 untuk JPEG). Aplikasi penampil gambar (*image viewer*) akan berhenti memproses data setelah menemukan penanda ini. Oleh karena itu, data apa pun yang ditambahkan setelahnya tidak akan diproses secara visual, sehingga gambar tetap terlihat 100% identik dengan aslinya.

Kriptografi AES-256 dan Derivasi Kunci AES-256 adalah standar enkripsi simetris yang menggunakan blok 128-bit dan kunci 256-bit. Keamanannya sangat bergantung pada kerahasiaan kunci. Untuk menghindari kelemahan akibat kata sandi pengguna yang pendek atau mudah ditebak, digunakan PBKDF2 (*Password-Based Key Derivation Function 2*) sesuai standar RFC 2898 (Kaliski, 2000). Algoritma ini melakukan *hashing* berulang (iterasi) terhadap kata sandi dan *salt*, menghasilkan kunci yang resisten terhadap serangan *brute-force* dan *dictionary att ack*.

METODE PENELITIAN

Penelitian ini menerapkan metode pengembangan sistematis yang terdiri dari perancangan modul kriptografi, modul steganografi, dan integrasi sistem.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Perancangan Modul Enkripsi (crypto_service.py) Proses pengamanan data dilakukan dengan langkah-langkah berikut:

- Pembangkitan Kunci: Kata sandi pengguna diproses menggunakan PBKDF2-HMAC-SHA256 dengan 100.000 iterasi dan *salt* acak 16-byte.
- Enkripsi Data: Data rahasia dienkripsi menggunakan AES-256 mode CBC (*Cipher Block Chaining*) (Dworkin, 2001) dengan IV (*Initialization Vector*) acak 16-byte.
- Pengemasan: Hasil enkripsi digabungkan dalam format: Salt (16B) + IV (16B) + Ciphertext.

Perancangan Modul Penyisipan (steganography_service.py) Teknik penyisipan dilakukan tanpa memuat seluruh file gambar ke memori untuk efisiensi:

- File gambar host dibuka dalam mode append binary (ab).
- Data terenkripsi dituliskan tepat di akhir file gambar.
- Sistem menambahkan metadata berupa ukuran payload (8 byte) dan penanda unik MAGIC_MARKER = b"AES-EOF" (7 byte) di ujung file untuk keperluan identifikasi saat ekstraksi.

Mekanisme Integritas Data (utils.py) Untuk menjamin data yang diekstrak dapat digunakan kembali, sistem membungkus konten asli bersama nama filenya sebelum dienkripsi. Jika terjadi kerusakan metadata, sistem dilengkapi fungsi heuristik detect_file_type yang memindai *signature* file (misalnya %PDF, PNG, PK..) untuk mengembalikan ekstensi file yang tepat.

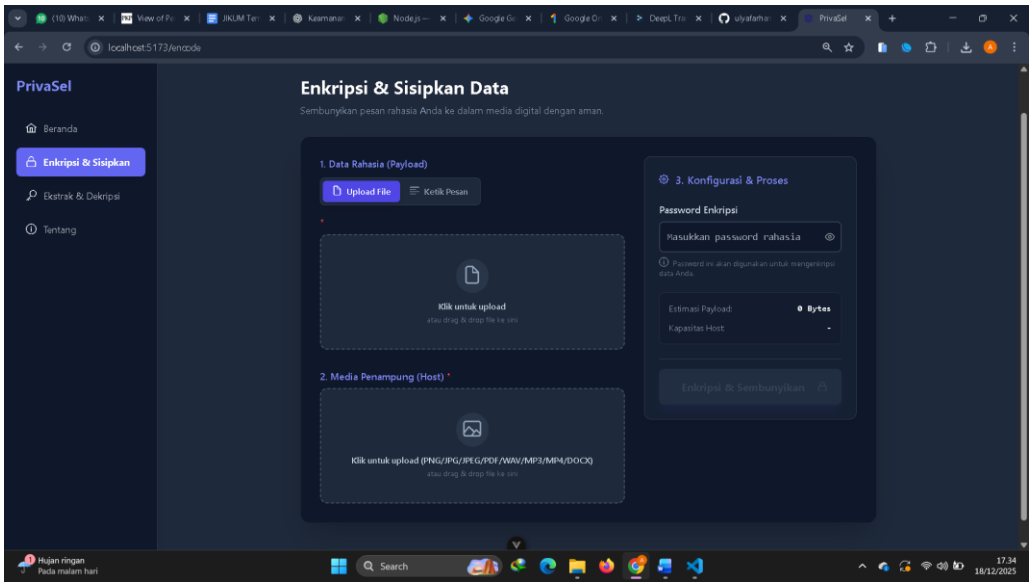
HASIL DAN PEMBAHASAN

Implementasi Antarmuka Sistem

Aplikasi PrivaSel telah berhasil diimplementasikan menggunakan Vue.js sebagai antarmuka pengguna. Pengguna dapat dengan mudah mengunggah file rahasia dan gambar *host* melalui fitur *drag-and-drop*.

Analisis Integritas Citra (Non-Destruktif)

Salah satu parameter keberhasilan utama metode EOF adalah tidak adanya perubahan visual pada citra. Pengujian dilakukan dengan membandingkan file gambar sebelum (*pre-stego*) dan sesudah (*post-stego*) penyisipan data.



Gambar 1. Tampilan Antarmuka (GUI) Menu Encode pada Aplikasi PrivaSel

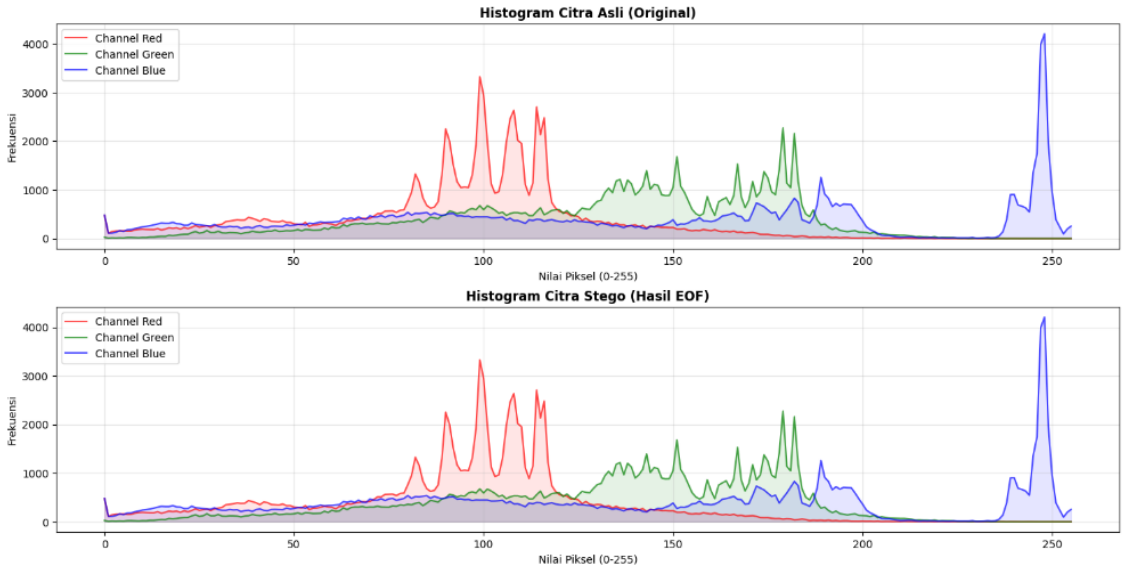
Gambar 1. memperlihatkan antarmuka pengguna saat proses pemilihan file dan input kata sandi sebelum proses enkripsi dimulai.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Gambar 2. Perbandingan Visual Citra Asli (Kiri) dan Citra Stego (Kanan)

Seperti terlihat pada Gambar 2, secara kasat mata tidak terdapat perbedaan visual sedikitpun antara citra asli dan citra hasil steganografi. Hal ini dikarenakan data piksel penyusun gambar tidak mengalami modifikasi.
Untuk membuktikan hal ini secara matematis, dilakukan analisis histogram pada kedua citra.



Gambar 3. Grafik Histogram Citra Asli (Atas) dan Citra Stego (Bawah) yang Identik.

Gambar 3 menunjukkan bahwa distribusi warna (histogram) pada kedua citra adalah identik. Ini membuktikan bahwa metode yang diusulkan bersifat sepenuhnya non-destruktif terhadap kualitas citra.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Bukti Penyisipan Data (Analisis Hex)

Meskipun secara visual identik, pembuktian teknis diperlukan untuk memastikan data benar-benar tersimpan. Analisis menggunakan *Hex Editor* dilakukan untuk melihat struktur biner file.

Tabel 1. Tampilan Hex Editor Menunjukkan Marker 'AES-EOF' di Akhir File

OFFSET	HEXADECIMAL	ASCII
0000626B	0F 8D 46 4C 36 52 EE E5 C6 74 A7 73 F3 EF 83 20	..FL6R...t.s...
0000627B	34 2E F1 44 EA 2D 50 BA 72 DF 96 82 D3 A7 C7 D3	4..D.-P.r.....
0000628B	EA F9 1C 80 1F 13 D1 B7 D5 DF 78 E3 CC 98 8D F1	.....x.....
0000629B	AD 00 00 00 00 00 00 **1A 00 41 45 53 2D 45 4F 46**	.....**AES-EOF**

Tabel 1. menampilkan hasil analisis forensik digital menggunakan Hex Editor pada berkas citra hasil steganografi ('encoded_alam.jpg'). Pada offset terakhir (0000629B), terlihat jelas keberadaan string penanda 'AES-EOF' (0x41-0x46) yang disisipkan di akhir struktur file. Tepat sebelum penanda tersebut, terdapat metadata ukuran payload sepanjang 8-byte dengan nilai 0x1A00 (area yang ditandai), yang mengindikasikan bahwa terdapat data terenkripsi sebesar 6.656 byte yang disisipkan sebelum metadata. Struktur ini membuktikan bahwa metode append-insertion berhasil dilakukan tanpa mengubah header atau data piksel asli citra.

Analisis Keamanan Data

Implementasi AES-256 dengan PBKDF2 memberikan jaminan keamanan yang kuat. Penggunaan *Initialization Vector* (IV) acak memastikan bahwa meskipun file yang sama disisipkan berulang kali ke dalam gambar yang sama dengan *password* yang sama, hasil biner yang tersimpan akan selalu berbeda. Hal ini mencegah penyerang melakukan analisis pola (*pattern analysis*) untuk mendekripsi data.

Efektivitas Deteksi dan Ekstraksi

Sistem berhasil mendeteksi keberadaan data tersembunyi dengan memvalidasi *marker* AES-EOF di akhir file. Fitur deteksi tipe file otomatis pada utils.py juga berfungsi efektif mengenali format dokumen umum (PDF, DOCX) dan multimedia (MP3, MP4) ketika metadata nama file sengaja dihapus atau rusak, memastikan data yang diekstrak tetap *usable*.

KESIMPULAN

Metode steganografi *End-of-File* (EOF) yang dikombinasikan dengan enkripsi AES-256 terbukti menjadi solusi efektif untuk penyembunyian data yang bersifat non-destruktif. Keunggulan utama pendekatan ini adalah jaminan integritas visual citra *host* yang tetap 100% terjaga, berbeda dengan metode berbasis modifikasi piksel. Ditambah dengan mekanisme penguatan kunci PBKDF2, sistem ini menawarkan keseimbangan yang optimal antara keamanan data (*confidentiality*) dan penyamaran (*invisibility*) (Stallings, 2017). Sistem ini cocok diterapkan untuk pengamanan dokumen rahasia, hak cipta digital, dan komunikasi privat yang membutuhkan tingkat integritas media yang tinggi.

REFERENSI

Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M. (2012). Datatype/end-of-file based steganography method. In *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)* (pp. 312-316). IEEE.

Cadullah, M. R. (2023). *Hybrid end of file steganography and super encryption cryptography*. Universitas Sam Ratulangi. https://repo.unsrat.ac.id/5036/

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*(3), 727-752.

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES - The advanced encryption standard*. Springer-Verlag.

Dworkin, M. (2001). *Recommendation for block cipher modes of operation: Methods and techniques* (NIST Special Publication 800-38A). National Institute of Standards and Technology.

Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms, and applications*. Cambridge University Press.

Handayani, T., & Sakti, D. V. S. (2014). Penerapan steganografi metode end of file (EOF) dan enkripsi metode data encryption standard (DES) pada aplikasi pengamanan data gambar. *Konferensi Nasional Sistem Informasi (KNSI)*, 1743–1753.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Kaliski, B. (2000). *PKCS #5: Password-based cryptography specification version 2.0* (RFC 2898). Internet Engineering Task Force (IETF).

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

Pramudia, A., Hariady, M., & Astuti, I. F. (2021). Aplikasi hybrid steganografi EOF dan enkripsi AES-128 untuk keamanan file PDF android. *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI)*, *2*(3).

Purba, G. C. M., Hadiana, A. I., & Santikarama, I. (2022). Pengamanan citra medis berbasis steganografi dan kriptografi dengan menggunakan metode end of file dan advanced encryption standard. *Informatics and Digital Expert (INDEX)*, *4*(1), 1-9.

Putri, A. R., & Darwis, D. (2023). Implementasi AES dan EOF (end of file) untuk mengamankan file dokumen dan gambar. *Jurnal Teknologi dan Sistem Informasi*, *4*(2).

Rouk, M. Y., Bau Berek, M. M. S., Neno, M. C. G., Naikofi, A. R., Nesi, N., & Piris, W. A. (2025). Mengamankan pesan rahasia dengan enkripsi AES-256 dan teknik steganografi teks. *Jurnal Ilmiah Multidisiplin Terpadu*, *9*(6), 129.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

UPI Kampus Cibiru. (2025). Implementasi steganografi PDF dengan manipulasi stream dan enkripsi AES-256 untuk keamanan data. *Artikel Tekkom*. https://kd-cibiru.upi.edu/

Rouk, M. Y., Bau Berek, M. M. S., Neno, M. C. G., Naikofi, A. R., Nesi, N., & Piris, W. A. (2025). Mengamankan pesan rahasia dengan enkripsi AES-256 dan teknik steganografi teks. *Jurnal Ilmiah Multidisiplin Terpadu*, *9*(6), 129.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

UPI Kampus Cibiru. (2025). Implementasi steganografi PDF dengan manipulasi stream dan enkripsi AES-256 untuk keamanan data. *Artikel Tekkom*. https://kd-cibiru.upi.edu/