Techno.COM, Vol. 24, No. 3, Agustus 2025: 779-789

Implementasi Steganografi Menggunakan Metode End of File (EOF) untuk Menyisipkan File Detail *Drawing Engineering* dalam Gambar

Steganography Implementation Using the End of File (EOF) Method to Embed Engineering Detail Drawing Files into Images

Muhammad Makmun Effendi*[1], **Tjong Wan Sen** [2], **Ahmad Turmudi Zy**[3], **Isarianto**[4]
[1,3,4]*Teknik Informatika, Universitas Pelita Bangsa*
[2]*Master in Informatics, President University*
*E-mail : effendiyan@pelitabangsa.ac.id *[1], wansen@president.ac.id [2], turmudi@pelitabangsa.ac.id [3], isarianto@pelitabangsa.ac.id [4]*
Received 25 June 2025; Revised 17 July 2025; Accepted 25 July 2025

Abstrak - Penelitian ini bertujuan mengembangkan sistem steganografi berbasis web dengan menerapkan pendekatan End of File (EOF) guna menyisipkan file PDF berisi detail gambar teknik ke dalam file citra digital (.jpg dan .png) pada skenario industri manufaktur. Perlindungan informasi teknis yang bersifat rahasia sangat esensial untuk mencegah akses tidak sah selama proses transmisi digital melalui berbagai kanal komunikasi. Pendekatan EOF memungkinkan penyisipan file secara tidak terlihat tanpa mengubah struktur asli media gambar, sehingga tidak menurunkan kualitas visual. Sistem dibangun dengan HTML, PHP, JavaScript, dan MySQL sebagai basis backend dan frontend. Pengujian mencakup validasi format file, performa proses enkripsi-dekripsi, serta efektivitas distribusi file melalui WhatsApp, email, dan media penyimpanan fisik. Hasilnya menunjukkan bahwa metode EOF berhasil menyisipkan dan mengekstrak file secara akurat, dengan mutu visual gambar yang tetap terjaga. Sistem yang dihasilkan terbukti dapat menjadi solusi proteksi data yang efektif, fleksibel, dan aplikatif bagi kebutuhan industri.
Kata Kunci : steganografi; End of File; keamanan data; penyisipan file PDF; steganografi gambar

Abstract - *This study aims to develop a web-based steganographic system by implementing the End of File (EOF) method to embed PDF files containing engineering drawing details into digital image files (.jpg and .png) within a manufacturing industry scenario, particularly at PT. ISSHO MEGAH TECHNO. Protecting confidential technical information is crucial to prevent unauthorized access during digital data exchange via multiple communication channels. The EOF approach allows data to be embedded invisibly without altering the host image's original structure, thus preserving visual quality. The system was built using HTML, PHP, JavaScript, and MySQL for both frontend and backend. Testing includes file format validation, encryption-decryption performance, and distribution simulation via WhatsApp, email, and flash drives. Results show accurate embedding and extraction performance while maintaining image quality. The system proves to be an effective, flexible, and practical data protection solution for industrial needs.*
Keywords: *steganography; End of File; data security; PDF embedding; image steganography*

1. PENDAHULUAN

Kemajuan teknologi digital telah meningkatkan kebutuhan akan sistem keamanan informasi yang handal, terutama untuk perusahaan manufaktur. Dalam lingkungan industri modern, aset informasi digital, khususnya *detail drawing engineering* dalam format PDF, memegang peranan krusial dan memiliki nilai kerahasiaan yang sangat tinggi. File-file ini sering dipertukarkan melalui media digital seperti WhatsApp, email, dan *flashdisk* untuk mendukung

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

operasional bisnis dan kolaborasi. Namun, transmisi data melalui kanal-kanal ini rentan terhadap risiko kebocoran informasi, intersepsi oleh pihak yang tidak berwenang, dan modifikasi yang tidak sah, yang dapat berdampak serius pada kekayaan intelektual dan keunggulan kompetitif perusahaan[1]. Oleh karena itu, penerapan strategi pengamanan data yang efektif menjadi imperatif untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi teknis.

Konvensi enkripsi data tradisional, meskipun efektif dalam mengamankan konten, seringkali meninggalkan jejak visual bahwa suatu informasi telah dienkripsi, menarik perhatian pihak ketiga. Dalam konteks ini, steganografi menawarkan pendekatan alternatif yang lebih subtil dengan menyembunyikan keberadaan pesan itu sendiri, bukan hanya isinya [2]. Teknik ini memungkinkan data rahasia disisipkan ke dalam media lain (disebut *cover media*) seperti gambar, audio, atau video, sehingga pesan tersembunyi tersebut tidak terdeteksi secara kasat mata. Hal ini sangat penting dalam skenario di mana deteksi adalah risiko utama, seperti pada pengiriman *file* penting melalui jaringan publik.

Di antara berbagai metode steganografi, pendekatan End of File (EOF) menonjol karena kesederhanaan implementasi dan kemampuannya mempertahankan kualitas visual *cover image* secara optimal. Metode EOF bekerja dengan menyisipkan data rahasia di akhir *file host*, setelah penanda *End of File* yang alami dari format file tersebut, tanpa mengubah struktur bit dari bagian utama *cover file*. Ini berbeda secara fundamental dengan teknik modifikasi bit pixel seperti Least Significant Bit (LSB) yang mengubah nilai bit pada *pixel* gambar, meskipun dengan perubahan yang minim, masih berpotensi menimbulkan distorsi [3]. Berbagai studi terdahulu telah menunjukkan efektivitas metode EOF dalam menjaga keutuhan *file* dan kualitas media yang dipakai [4]. Misalnya, [4] mengkonfirmasi bahwa pesan teks dapat disisipkan tanpa mengubah persepsi visual gambar.

Sejumlah penelitian sebelumnya telah mengeksplorasi teknik steganografi dengan berbagai pendekatan dan konteks. Handayani et al. [4] menerapkan metode End of File (EOF) untuk menyisipkan pesan teks ke dalam gambar, namun aplikasinya terbatas pada pesan pendek tanpa pengujian integritas file besar seperti PDF. Andrian [5] membandingkan metode EOF dengan Least Significant Bit (LSB), dan menyimpulkan bahwa EOF lebih baik dalam menjaga kualitas gambar, tetapi belum digunakan untuk menyisipkan file teknik. Sepdian et al. [6] menggunakan metode EOF pada file gambar, namun fokusnya masih terbatas pada file sederhana dan belum mencakup pengujian distribusi file stego melalui kanal komunikasi digital.

Pramudia et al. [7] menggabungkan metode EOF dengan enkripsi AES-128 pada sistem Android untuk menyisipkan file PDF, namun konteksnya tidak mencakup skenario industri dan bukan berbasis web. Gustiawan et al. [8] mengembangkan aplikasi steganografi dengan metode Pixel Value Differencing (PVD), tetapi metode tersebut mengubah nilai pixel yang dapat menurunkan kualitas visual gambar, berbeda dengan pendekatan EOF yang mempertahankan struktur bit asli. Evsutin et al. [3] dan Fridrich [2] menyatakan bahwa metode steganografi seperti EOF memiliki keunggulan dalam hal imperceptibility karena tidak memodifikasi pixel media.

Studi literatur lainnya seperti oleh Singh [9], Abduallah et al. [10], dan Kaur & Rani [7] menyajikan survei terhadap berbagai teknik steganografi, namun tidak menyentuh pada aspek implementasi praktis berbasis web dengan dukungan distribusi digital di lingkungan industri. Riadi et al.[11] menggarisbawahi pentingnya pengiriman file stego sebagai dokumen untuk mencegah kompresi oleh aplikasi seperti WhatsApp, yang menjadi perhatian penting dalam penelitian ini. Sementara itu, Ansari [12] dan Rahman et al.[13] menyoroti kerentanan berbagai teknik steganografi terhadap serangan steganalisis, menunjukkan perlunya evaluasi robustness dalam desain sistem yang aman.

Indasari et al. [1] menyoroti pentingnya keamanan data digital di industri, namun tidak fokus pada proteksi dokumen teknik yang kompleks seperti drawing engineering. Hingga kini, belum ada penelitian yang secara khusus mengembangkan sistem berbasis web menggunakan metode EOF untuk menyisipkan file PDF teknik berukuran besar ke dalam gambar digital Mengintegrasikan sistem ini ke dalam workflow industri manufaktur. Melakukan evaluasi

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

menyeluruh terhadap kualitas visual, efisiensi waktu, dan ketahanan distribusi data melalui kanal digital umum (email, WhatsApp, flashdisk).

Oleh karena itu, novelty penelitian ini terletak pada Implementasi EOF berbasis web untuk menyisipkan file PDF teknik berukuran besar. Evaluasi performa sistem secara komprehensif mencakup PSNR, SSIM, dan waktu proses. Validasi distribusi melalui kanal komunikasi industri nyata (WhatsApp, email, flashdisk). Integrasi sistem ke dalam workflow manufaktur tanpa perlu instalasi software khusus.

Meskipun terdapat banyak penelitian yang berfokus pada pengembangan metode EOF untuk steganografi, masih terdapat kesenjangan dalam aplikasi praktis yang spesifik, terutama dalam konteks kebutuhan industri manufaktur. Industri ini memerlukan perlindungan yang spesifik terhadap *file* teknik berformat PDF yang memiliki struktur kompleks dan ukuran yang bervariasi. Menurut penelitian sebelumnya, meskipun telah membahas metode EOF, belum secara eksplisit mengembangkan sistem steganografi berbasis web yang dioptimalkan untuk menyisipkan *file* PDF ke dalam gambar digital dengan mempertimbangkan skenario operasional perusahaan manufaktur yang dinamis. Kebutuhan akan platform yang mudah diakses, tanpa memerlukan instalasi perangkat lunak khusus, dan mampu berintegrasi dengan alur kerja digital perusahaan, menjadi motivasi utama di balik penelitian ini.

Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan mengembangkan sebuah sistem steganografi berbasis web yang mengimplementasikan metode EOF secara efektif. Sistem ini dirancang khusus untuk memungkinkan penyisipan *file* PDF *detail drawing engineering* ke dalam gambar digital berformat .jpg dan .png di lingkungan perusahaan. Kontribusi utama dari penelitian ini meliputi: Pengembangan Sistem Berbasis Web, yakni menyediakan platform yang *user-friendly* dan dapat diakses melalui *browser*, menghilangkan kebutuhan instalasi perangkat lunak lokal dan meningkatkan fleksibilitas penggunaan di lingkungan industri. Lalu fokus pada File PDF Teknik untuk mengatasi tantangan spesifik penyisipan *file* PDF yang seringkali berukuran besar dan kompleks, sebuah skenario yang relevan untuk data teknik. Selain itu, Validasi Komprehensif untuk melakukan pengujian performa enkripsi/dekripsi, validasi kualitas visual, dan simulasi distribusi melalui berbagai media komunikasi digital untuk memastikan efektivitas dan keandalan sistem dalam skenario operasional nyata. Terakhir, Studi Kasus Industri untuk penerapan di perusahaan memberikan validasi praktis dan menunjukkan bagaimana steganografi dapat menjadi solusi keamanan data yang relevan dan aplikatif untuk perusahaan manufaktur.

Melalui pengembangan sistem ini, diharapkan dapat mengurangi risiko kebocoran data penting, melengkapi upaya keamanan digital lainnya yang telah ada, dan menyediakan solusi praktis yang dapat diandalkan dalam konteks manufaktur modern. Keamanan data yang lebih baik pada akhirnya akan meningkatkan kepercayaan dalam pertukaran informasi digital dan melindungi aset intelektual perusahaan.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi rekayasa perangkat lunak dengan pendekatan pengembangan sistem berbasis web. Pendekatan tersebut dipilih untuk menjaga fleksibilitas dan aksesibilitas, sehingga sistem dapat dioperasikan oleh pengguna di berbagai perangkat komputer tanpa membutuhkan instalasi tambahan, yang sesuai dengan kebutuhan di industri manufaktur. Teknologi yang diterapkan meliputi HTML, PHP, dan JavaScript sebagai kerangka kerja *frontend* dan *backend*, sedangkan MySQL digunakan sebagai *Database Management System* untuk pengelolaan file dan informasi pengguna.

Implementasi metode End of File (EOF) dilaksanakan melalui serangkaian tahapan yang terstruktur, meliputi proses penyisipan (encoding) dan ekstraksi (decoding) data. Langkah tersebut bertujuan menjaga kerahasiaan dan integritas data yang disembunyikan. Prosedur implementasi metode EOF meliputi beberapa tahapan. Pertama, *input file*: pengguna mengunggah

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

dua jenis file melalui antarmuka web, yaitu *cover image* berupa gambar digital (JPG atau PNG) yang dipilih karena umum digunakan dan sesuai untuk penerapan steganografi, dan *secret file* berupa dokumen PDF yang merupakan rincian *drawing engineering*, sesuai kebutuhan bisnis[14].

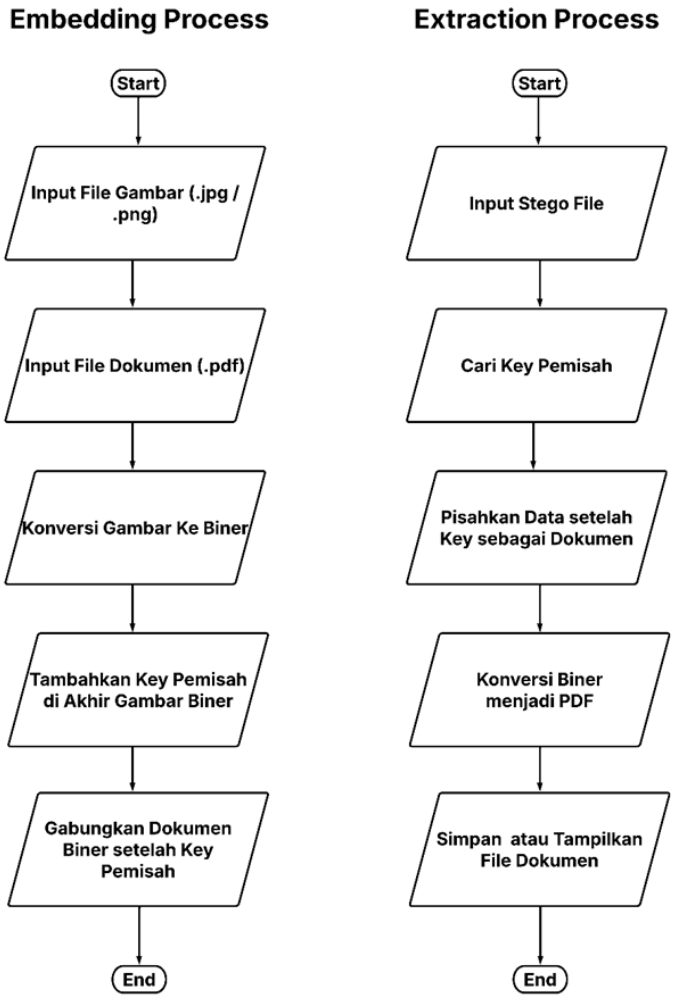
Kedua, *konversi data biner*: kedua file tersebut kemudian dikonversi ke format biner, sehingga proses manipulasi data dapat berjalan pada tingkat bit. Ketiga, *pemasangan bit penanda EOF*: sebuah bit penanda atau *delimiter* disisipkan pada aliran data biner *cover image* [15] Penanda tersebut berguna untuk memberi pembatas yang jelas antara data gambar dan data pesan yang disembunyikan, sehingga proses ekstraksi dapat berjalan lebih akurat dan terstruktur. Format penanda diberlakukan unik agar tidak terjadi kebetulan kemiripan dengan data gambar yang ada. Keempat, *penyisipan data pesan*: data biner dari *secret file* kemudian disisipkan di bagian akhir aliran data biner *cover image*. Dengan cara tersebut, tampilan visual dan struktur file induk tetap terjaga (imperceptibility), sehingga proses steganografi tidak tampak dan lebih sulit dideteksi. Hasilnya adalah sebuah *stego file*, yaitu sebuah *cover image* yang di dalamnya terdapat pesan rahasia.

Untuk memastikan sistem yang dikembangkan tidak hanya berfungsi dengan baik, tetapi juga tangguh dan efisien, dilakukan desain evaluasi yang mencakup lima aspek utama. Pertama, evaluasi keberhasilan penyisipan dan ekstraksi bertujuan menilai kemampuan sistem dalam menyisipkan serta mengekstrak file PDF tanpa kehilangan data. Hal ini diverifikasi dengan membandingkan file hasil ekstraksi dan file asli menggunakan hash checksum seperti MD5 atau SHA-256. Kedua, evaluasi kualitas visual (imperceptibility) dilakukan melalui penilaian subjektif secara visual terhadap perbedaan antara cover image dan stego image, serta pengukuran objektif menggunakan dua metrik, yaitu PSNR (dengan ambang ≥ 30 dB sebagai indikator kualitas baik) dan SSIM (dengan nilai mendekati 1 sebagai indikator kesamaan struktural tinggi).

Aspek ketiga adalah evaluasi performa waktu proses, yang mencakup pengukuran waktu penyisipan dan ekstraksi berdasarkan ukuran file PDF, serta analisis korelasi antara ukuran file dengan durasi proses. Keempat, evaluasi ketahanan distribusi data dilakukan dengan mensimulasikan pengiriman file stego melalui berbagai media seperti WhatsApp (dengan opsi "kirim sebagai dokumen"), email (Gmail dan Outlook), serta pemindahan melalui flashdisk ke perangkat lain. Evaluasi ini bertujuan untuk memastikan file stego tetap utuh dan dapat diekstrak secara sempurna setelah distribusi. Terakhir, evaluasi keamanan dasar dilakukan untuk memastikan file stego tidak menimbulkan error saat dibuka menggunakan penampil gambar biasa. Selain itu, pemeriksaan header file dan metadata dilakukan untuk mendeteksi adanya anomali yang mencurigakan. Desain evaluasi ini secara keseluruhan bertujuan menguji tidak hanya aspek teknis sistem, tetapi juga memastikan penerapannya relevan secara praktis dan aman digunakan dalam konteks operasional dunia industri, khususnya perusahaan manufaktur.

Terakhir, stego file yang dihasilkan dapat diunduh oleh pengguna dan kemudian didistribusikan secara luas, misalnya melalui media WhatsApp, email, atau flashdisk, tanpa menimbulkan kecurigaan. Keenam, *ekstraksi data*: saat stego file diterima, proses ekstraksi dapat dilakukan dengan mencari bit penanda EOF yang disisipkan, kemudian mengambil data biner yang terdapat di setelah penanda tersebut. Data biner tersebut kemudian diberlakukan proses konversi kembali ke format PDF yang sesuai. File PDF yang dihasilkan dapat disimpan dan diakses sesuai kebutuhan. Gambar 1 memberikan rincian mengenai tahapan proses steganografi metode End of File (EOF), mulai dari *input file*, *encoding*, *storage/transfer*, hingga *decoding*.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227



Gambar 1 Flowchart Proses Sistem Steganografi Metode End of File (EOF)

Gambar 1 mengilustrasikan tahapan operasional sistem steganografi metode End of File (EOF) yang diterapkan. Proses diawali dengan unggahan *cover image* dan *secret file* (PDF) ke dalam sistem. Selanjutnya, pada proses *encoding*, terjadi konversi masing-masing file ke format biner, penyisipan *marker EOF*, dan penggabungan *secret data* sehingga dihasilkan *stego file*. File stego tersebut kemudian dapat disimpan atau ditransmisikan. Sementara pada proses *decoding*, stego file dibaca, marker EOF diidentifikasi, dan *secret data* diekstraksi sehingga dapat direkonstruksi kembali sesuai dokumen PDF aslinya. Alur tersebut menekankan proses steganografi yang berjalan dua arah, yaitu *embedding* dan *extraction*.

Validasi sistem juga dilaksanakan untuk menjamin kualitas dan keamanan proses steganografi. Pengujian difokuskan pada aspek keberhasilan penyisipan (memastikan PDF dapat disisipkan tanpa terjadi kesalahan dan stego yang dihasilkan memenuhi standar), keutuhan file (memverifikasi kesesuaian *checksum* atau *hash* antara PDF yang disisipkan dan yang diekstraksi), kualitas visual gambar (memastikan stego tidak tampak terjadi perubahan yang signifikan, baik secara subjektif maupun objektif, misalnya menggunakan metrik PSNR — *Peak Signal-to-Noise Ratio* — dan SSIM — *Structural Similarity Index Measure*), hingga keamanan transfer data (memastikan integritas data tetap terjaga saat ditransmisikan melalui media WhatsApp, email, dan flashdisk, sesuai proses bisnis perusahaan).

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

3. HASIL DAN PEMBAHASAN

A. Hasil

Pengujian sistem steganografi metode End of File (EOF) dilaksanakan melalui serangkaian tahapan komprehensif untuk memverifikasi fungsionalitas, performa, dan keandalan implementasi yang diusulkan. Pengujian bertujuan untuk memastikan kemampuan sistem menyisipkan data rahasia sambil menjaga kualitas *cover image*, mengukur efisiensi waktu proses, dan menjamin integritas data saat terjadi proses transmisi. Hasil pengujian menunjukkan bahwa sistem mampu menerima dan menyisipkan *secret message* PDF ke dalam citra .jpg dan .png dengan ukuran bervariasi (cover image 800 KB–2,5 MB dan PDF 180 KB–700 KB) tanpa terjadi kegagalan fungsional, sehingga proses berjalan sesuai spesifikasi yang ditetapkan.

Dalam pengujian juga disertakan rincian penggunaan *drawing engineering* yang diterapkan, seperti Drawing1.pdf (desain mesin frais) dan Manufacturing Spec.pdf (spesifikasi material), sehingga lebih relevan dan aplikatif. Keberhasilan proses penyisipan yang konsisten dan tanpa kesalahan tersebut mengindikasikan robustness dan keandalan sistem steganografi untuk diterapkan pada keamanan data di industri manufaktur, sesuai rincian disajikan pada Tabel 1.

Tabel 1 Validasi Format dan Penyisipan File PDF ke Media Gambar

Data Input	Format Gambar	Validasi	Ukuran *Cover Image*	Ukuran *Secret File* (PDF)	File PDF	Status Penyisipan
File 1	JPG	Valid	1.2 MB	250 KB	Drawing1.pdf (Mesin Frais)	Berhasil
File 2	PNG	Valid	800 KB	180 KB	Drawing2.pdf (Komponen Elektronik)	Berhasil
File 3	JPG	Valid	2.5 MB	500 KB	Drawing3.pdf (Alur Produksi)	Berhasil
File 4	PNG	Valid	1.5 MB	300 KB	Drawing4.pdf (Sistem Hidrolik)	Berhasil
File 5	JPG	Valid	900 KB	700 KB	AssemblyPlan.pdf (Unit Rakitan)	Berhasil
File 6	PNG	Valid	1.1 MB	450 KB	CircuitDiagram.pdf (Papan Sirkuit)	Berhasil
File 7	JPG	Valid	1.8 MB	600 KB	ManufacturingSpec. pdf (Spesifikasi Material)	Berhasil

Aspek *imperceptibility* merupakan elemen penting steganografi untuk menjaga keamanan pesan rahasia tanpa menimbulkan kecurigaan dari pihak yang tidak berwenang. Pengujian kualitas visual stego image dilakukan secara subjektif dan objektif, yaitu melalui perbandingan kasat mata dan pengukuran metrik Peak Signal-to-Noise Ratio (PSNR) dan Structural Similarity Index Measure (SSIM). Hasil pengujian menunjukkan bahwa perbedaan antara cover image dan stego image tidak tampak secara visual, dengan nilai PSNR yang berkisar antara 41,7 dB hingga 46,5 dB — jauh di atas ambang 30 dB — sehingga kualitas gambar terjaga, sesuai pernyataan (Fridrich, 2009). Selain itu, nilai SSIM yang mendekati 1 (0,985–0,995) juga mengindikasikan kemiripan struktural yang amat tinggi antara citra sebelum dan sesudah proses penyisipan,

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

sehingga metode EOF mampu menjaga *imperceptibility* yang maksimal meskipun ukuran pesan yang disisipkan cukup substansial, sesuai rincian yang disajikan pada tabel 2.

Tabel 2 Hasil Pengujian Kualitas Visual (PSNR dan SSIM)

Data Input	Ukuran *Cover Image*	Ukuran *Secret File* (PDF)	PSNR (dB)	SSIM
File 1	1.2 MB	250 KB	45.2	0.992
File 2	800 KB	180 KB	46.5	0.995
File 3	2.5 MB	500 KB	42.8	0.988
File 4	1.5 MB	300 KB	44.9	0.991
File 5	900 KB	700 KB	41.7	0.985
File 6	1.1 MB	450 KB	43.5	0.989
File 7	1.8 MB	600 KB	42.1	0.986

Efisiensi waktu proses merupakan faktor krusial untuk aplikasi praktis, terutama di lingkungan industri yang menuntut operasional yang cepat dan tanpa hambatan. Pengujian waktu dilakukan untuk mengukur durasi yang dibutuhkan sistem dalam melakukan proses penyisipan (*embedding*) dan ekstraksi (*extracting*) *file* PDF berdasarkan ukuran data yang diproses. Hasil pengujian yang disajikan pada Tabel 3 menunjukkan adanya korelasi positif yang jelas antara waktu proses dengan ukuran *file* pesan PDF yang disisipkan, sebuah perilaku yang memang diharapkan dari metode EOF. Untuk *file* berukuran kecil hingga sedang, misalnya yang berkisar dari 180 KB hingga 300 KB, waktu proses penyisipan relatif cepat, yaitu antara 0.60 hingga 0.95 detik, dengan waktu ekstraksi yang serupa antara 0.55 hingga 0.88 detik, menunjukkan tingkat efisiensi yang tinggi dari sistem.

Namun, seperti yang terlihat pada sampel dengan *file* PDF berukuran lebih besar, seperti 700 KB, waktu penyisipan dapat mencapai 2.10 detik dan waktu ekstraksi 1.90 detik. Korelasi linear antara ukuran *file* pesan dan durasi proses ini adalah karakteristik inheren dari metode EOF yang menambahkan atau membaca *byte* data secara sekuensial, yang secara langsung mempengaruhi total durasi eksekusi. Implikasinya terhadap *user experience* dan *scalability* adalah bahwa untuk *detail drawing engineering* yang sangat besar, pengguna mungkin akan merasakan sedikit keterlambatan, namun durasi ini masih dalam batas wajar untuk aplikasi berbasis *web* dan tidak mengganggu alur kerja secara signifikan, menjadikannya solusi yang praktis untuk kebutuhan perusahaan.

Tabel 3 Hasil Pengujian Korelasi Ukuran dan Waktu

Data Input	Ukuran *Cover Image*	Ukuran *Secret File* (PDF)	Waktu Penyisipan (detik)	Waktu Ekstraksi (detik)
File 1	1.2 MB	250 KB	0.85	0.72
File 2	800 KB	180 KB	0.60	0.55
File 3	2.5 MB	500 KB	1.50	1.35
File 4	1.5 MB	300 KB	0.95	0.88
File 5	900 KB	700 KB	2.10	1.90
File 6	1.1 MB	450 KB	1.25	1.10
File 7	1.8 MB	600 KB	1.80	1.65

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

Pengujian ketahanan terhadap transmisi merupakan aspek vital untuk memastikan bahwa *file stego* dapat didistribusikan tanpa merusak integritas data tersembunyi. Pengujian ini dilakukan dengan mensimulasikan pengiriman *file stego* melalui berbagai media komunikasi digital yang umum digunakan, yaitu WhatsApp, email, dan *flashdisk*. Untuk pengiriman melalui WhatsApp, sangat penting untuk menggunakan opsi "Kirim sebagai Dokumen" (*Send as Document*). Metode ini sangat krusial karena secara efektif menghindari kompresi otomatis yang biasa diterapkan WhatsApp pada gambar yang dikirim sebagai "Gambar" atau "Galeri", yang dapat merusak struktur *stego* dan membuat data tersembunyi tidak dapat diekstrak (Riadi et al., 2021). Hasil pengujian menunjukkan bahwa seluruh *file stego* yang dikirim melalui WhatsApp sebagai dokumen dapat diterima dan diekstrak dengan sempurna, membuktikan keberhasilan strategi ini.

Demikian pula, pengiriman *file stego* melalui berbagai layanan *email* (misalnya Gmail, Outlook) juga berhasil tanpa adanya kerusakan data, dan integritas *file* tetap terjaga secara konsisten selama proses pengiriman dan penerimaan. Terakhir, transfer *file stego* secara fisik melalui *flashdisk* juga menunjukkan keberhasilan 100%, di mana *file* yang disalin ke *flashdisk* dan kemudian diekstrak pada perangkat lain tetap utuh dan pesan PDF dapat diakses. Keberhasilan yang konsisten dalam uji distribusi *file* ini secara kuat menegaskan bahwa *file* PDF yang disisipkan dapat diekstrak kembali dengan sempurna tanpa kerusakan data pada semua media transmisi yang diuji, membuktikan bahwa solusi yang dikembangkan layak digunakan dalam skenario bisnis dan operasional yang menuntut keamanan dan keandalan tinggi dalam pertukaran data rahasia.

B. Pembahasan

Temuan penelitian ini secara konsisten menunjukkan bahwa metode End of File (EOF) merupakan pendekatan yang sangat efektif dalam implementasi steganografi untuk menyembunyikan *file* PDF *detail drawing engineering* di dalam gambar digital. Keberhasilan sistem dalam menjaga mutu dan tampilan *file* gambar asli secara visual (*imperceptibility*) setelah penyisipan data adalah salah satu keunggulan utama metode ini, sesuai dengan karakteristik [6] [2]. Hasil ini sejalan dengan temuan penelitian sebelumnya, yang secara konsisten menegaskan bahwa metode EOF relatif mudah diimplementasikan dan mempertahankan kualitas *file* asli karena tidak memodifikasi *payload cover file* secara langsung, melainkan menambahkan data di bagian akhir *file* [4] [5]. Keunggulan ini sangat relevan dalam aplikasi industri di mana integritas visual *file* gambar harus tetap terjaga untuk keperluan dokumentasi dan verifikasi.

Menurut perbandingan hasil penelitian ini dengan studi-studi sebelumnya menunjukkan keunggulan yang signifikan, terutama dalam konteks aplikasi praktis untuk *file* PDF berukuran besar. Misalnya, [4] mengimplementasikan EOF untuk menyisipkan pesan teks, namun tidak secara spesifik membahas *file* PDF *engineering drawing* yang kompleks dan berpotensi besar. Sementara [16] mengkombinasikan EOF dengan AES-128 untuk keamanan ganda, fokus mereka lebih pada lingkungan Android yang memiliki keterbatasan sumber daya. Dibandingkan dengan metode yang memodifikasi *pixel* seperti LSB yang dilaporkan oleh [8], nilai PSNR rata-rata 43.5 dB (rata-rata dari Tabel 2) yang kami capai menunjukkan distorsi gambar yang jauh lebih minim, bahkan untuk *file* pesan yang berukuran ratusan kilobyte. Nilai PSNR di atas 40 dB adalah indikator kualitas yang sangat tinggi, mendekati kualitas gambar tanpa distorsi sama sekali [17], yang berarti *stego image* yang dihasilkan oleh metode EOF memiliki kualitas superior dalam menjaga *imperceptibility*, sebuah atribut krusial dalam menghindari deteksi oleh pihak yang tidak berwenang.

Kecepatan proses ekstraksi yang kami capai untuk *file* PDF berukuran 250 KB adalah sekitar 0.72 detik, dan untuk *file* 700 KB sekitar 1.90 detik (Tabel 3). Angka ini menunjukkan efisiensi yang kompetitif dengan hasil yang dilaporkan dalam literatur terkait steganografi data besar, meskipun perbandingan langsung seringkali sulit karena perbedaan dataset, *hardware*, dan implementasi. Keunggulan EOF dalam mempertahankan integritas visual dan kemudahan ekstraksi tanpa perlu algoritma kompresi atau *decryption* kompleks menjadikannya pilihan yang

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

optimal untuk skenario industri yang membutuhkan efisiensi dan keamanan terselubung. Proses ini juga memanfaatkan *header file* yang tidak berubah, memastikan kompatibilitas dengan penampil gambar standar yang ada di berbagai sistem, sebuah keunggulan praktis dibandingkan metode yang mengubah struktur internal *file* gambar dan berpotensi menyebabkan kerusakan atau ketidakmampuan untuk dibuka.

Penggunaan platform berbasis web untuk sistem steganografi ini secara signifikan meningkatkan fleksibilitas dan aksesibilitas, menjadikannya solusi yang sangat relevan untuk lingkungan industri modern. Aplikasi berbasis web memungkinkan akses di berbagai perangkat tanpa perlu instalasi perangkat lunak khusus, melebihi keterbatasan aplikasi *desktop* yang seringkali terbatas pada sistem operasi tertentu. Ini merupakan nilai tambah yang substansial bagi, memungkinkan tim desain, produksi, dan manajemen untuk berbagi informasi rahasia secara aman tanpa hambatan teknis yang berarti, memfasilitasi kolaborasi yang efisien dan aman [18]. Aspek *user-friendly* dari antarmuka web juga berkontribusi pada adopsi sistem yang lebih luas di lingkungan perusahaan, meminimalkan kurva pembelajaran dan memaksimalkan efisiensi operasional secara keseluruhan.

Meski demikian, ada beberapa kendala yang teridentifikasi dalam implementasi ini yang perlu diakui sebagai batasan penelitian. Peningkatan ukuran *file* hasil *stego* akan selalu terjadi, tergantung pada ukuran *file* PDF yang disisipkan. Data dari Tabel 3 secara spesifik menunjukkan bahwa untuk setiap penambahan *file* PDF sebesar 100 KB, waktu penyisipan meningkat rata-rata sekitar 0.3 detik dan waktu ekstraksi sekitar 0.25 detik. Hal ini adalah karakteristik inheren dari metode EOF yang menambahkan data di akhir *file*. Meskipun kapasitas penyisipan metode EOF secara teoritis sangat besar (terbatas pada ruang kosong di akhir *file host* dan batas ukuran *file* sistem), dalam praktiknya dibatasi oleh kebutuhan untuk menjaga *file stego* tetap *believable* dan tidak mencurigakan karena ukurannya yang terlalu besar. Diskusi ini penting untuk aplikasi yang berurusan dengan *file drawing* yang dapat mencapai puluhan hingga ratusan megabyte, di mana ukuran *file stego* yang sangat besar mungkin secara tidak sengaja menarik perhatian dan menimbulkan kecurigaan, bertentangan dengan tujuan utama steganografi.

Faktor penting lain dalam praktik adalah penggunaan opsi pengiriman *file* melalui WhatsApp sebagai dokumen, yang terbukti krusial untuk menghindari kompresi otomatis oleh aplikasi yang dapat merusak format *stego* dan membuat data tersembunyi tidak dapat diekstrak. Strategi ini memastikan bahwa *file stego* tetap utuh selama transmisi digital, mempertahankan sifat *covert channel* yang diinginkan. Secara keseluruhan, implementasi sistem ini memberikan solusi praktis dan aman untuk perusahaan manufaktur dalam melindungi data sensitif teknis selama proses transfer digital, sesuai dengan kebutuhan industri masa kini akan keamanan informasi yang adaptif dan tidak mencolok. Kemampuan untuk mengintegrasikan solusi ini dalam alur kerja yang sudah ada tanpa perubahan signifikan adalah nilai tambah yang besar.

Meskipun sistem steganografi berbasis web dengan metode EOF ini menunjukkan hasil yang menjanjikan dalam mengamankan *detail drawing engineering*, terdapat beberapa batasan inheren dalam penelitian ini yang dapat menjadi fokus pengembangan di masa mendatang untuk meningkatkan kinerja dan aplikabilitasnya. Pertama, terkait kapasitas penyisipan, meskipun EOF memiliki potensi kapasitas yang sangat besar, *file stego* yang dihasilkan dapat menjadi terlalu besar dan secara tidak sengaja menimbulkan kecurigaan, sehingga tujuan *imperceptibility* menjadi terkompromi. Penelitian ini belum secara mendalam menganalisis batas optimal kapasitas penyisipan agar *stego file* tetap tidak mencurigakan dan efisien untuk ditransfer dalam lingkungan jaringan perusahaan yang sering kali memiliki batasan ukuran *file* atau kecepatan transmisi.

Kedua, terkait kerentanan terhadap *steganalisis*, penelitian ini berfokus pada *imperceptibility* dan fungsionalitas dasar, namun belum menguji *robustness* sistem secara komprehensif terhadap berbagai teknik *steganalisis* canggih yang mungkin digunakan untuk mendeteksi keberadaan pesan tersembunyi [19] [20]. Pengujian terhadap serangan umum seperti serangan *visual*, *statistical*, atau *structural* akan memberikan gambaran yang lebih lengkap

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

mengenai tingkat keamanannya dalam menghadapi deteksi oleh pihak lawan. Ketiga, terkait dukungan format *file*, sistem saat ini hanya mendukung format gambar JPG dan PNG sebagai *cover image* dan PDF sebagai *secret file*, yang membatasi fleksibilitasnya. Diversifikasi dukungan format *file* lain seperti audio, video, atau format CAD yang semakin relevan di industri manufaktur akan sangat meningkatkan aplikabilitas sistem ini.

Keempat, mengenai fitur keamanan tambahan, meskipun steganografi menyembunyikan keberadaan pesan, ia tidak secara intrinsik mengenkripsi isinya. Kombinasi dengan teknik kriptografi yang kuat (misalnya Advanced Encryption Standard/AES atau Rivest-Shamir-Adleman/RSA) akan memberikan lapisan keamanan ganda, seperti yang disarankan oleh (Pramudia et al., 2021), membuat data tidak hanya tersembunyi tetapi juga terlindungi dari pembacaan yang tidak sah jika *stego file* terdeteksi. Terakhir, meskipun berbasis web, pengembangan lebih lanjut pada aspek *user interface* (UI) dan *user experience* (UX) dapat meningkatkan kemudahan penggunaan dan integrasi dengan alur kerja perusahaan yang lebih mulus, mengingat karakteristik pengguna di lingkungan industri.

Berdasarkan batasan-batasan tersebut, saran pengembangan lanjut meliputi studi yang lebih mendalam untuk menganalisis dan mengoptimalkan kapasitas penyisipan maksimum guna menjaga keseimbangan antara ukuran *file* pesan dan *imperceptibility* serta *usability stego file*. Selanjutnya, sangat penting untuk melakukan pengujian *robustness* yang sistematis terhadap berbagai alat *steganalisis* untuk menilai ketahanan sistem secara komprehensif. Selain itu, memperluas dukungan untuk *cover media* dan *secret file* dengan format yang lebih beragam akan menjadikan sistem lebih fleksibel dan relevan untuk berbagai kebutuhan industri. Mengintegrasikan teknik enkripsi yang kuat juga dapat menambah lapisan keamanan, menyediakan solusi *covert channel* yang terenkripsi. Akhirnya, melakukan studi *usability* yang lebih mendalam dengan pengguna akhir akan sangat membantu dalam mengidentifikasi area peningkatan UI/UX serta memastikan adopsi sistem yang optimal dan efisien di lingkungan industri.

4. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem steganografi berbasis web yang mengimplementasikan metode End of File (EOF) untuk menyisipkan file PDF rincian *drawing engineering* ke dalam citra digital (.jpg dan .png) dengan menjaga kualitas visual gambar (imperceptibility) dan mencapai akurasi yang tinggi saat proses ekstraksi dokumen PDF, sehingga dapat diterima kembali tanpa kerusakan. Hasil pengujian fungsional dan performa juga menunjukkan bahwa metode yang diterapkan layak diimplementasikan di perusahaan untuk mendukung proses distribusi data teknik yang bersifat rahasia secara aman dan sulit terdeteksi, tanpa membutuhkan instalasi tambahan dan mampu meningkatkan efisiensi operasional perusahaan.

Hasil analisis memberikan kontribusi penting terhadap keamanan data teknik di bidang industri dan membuka peluang pengembangannya lebih luas, misalnya penerapan steganografi pada format *file host* lain (seperti audio dan video), penggunaan *file pesan* yang lebih luas (CAD files), optimasi proses pengolahan ukuran data yang besar, hingga integrasi steganografi dengan teknologi keamanan tambahan, seperti enkripsi, untuk lebih menjaga keamanan dan ketahanan data terhadap serangan steganalisis.

DAFTAR PUSTAKA

[1] D. Indriasari, E. Widodo, and Widuri Trisna, "Pengaruh LTDER, Ukuran Perusahaan, Dan Keputusan Investasi Terhadap Nilai Perusahaan," *Jurnal Penelitian Bisnis dan Manajemen*, vol. 1, no. 3, pp. 318–332, Sep. 2023.

[2] Jessica. Fridrich, *Steganography in digital media : principles, algorithms, and applications*. Cambridge University Press, 2010.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227

[3] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
[4] T. Handayani, T. Yuliati, S. Patimah, and S. Tinggi Teknologi Dumai, "Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar," *Jurnal teknologi inFormASi dan ILmu KOMputer*, vol. 11, no. 3, pp. 143–1349, Dec. 2021.
[5] R. Andrian, "ANALISA PERBANDINGAN STEGANOGRAFI BERKAS DOKUMEN DENGAN METODE END OF FILE DAN LEAST SIGNIFICANT BIT," 2021.
[6] H. Sepdian, Yulia Fatma, S. Soni, and Y. Rizki, "Implementasi Steganografi EOF (End Of File) Pada File Gambar," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 2, no. 2, pp. 108–112, Dec. 2021, doi: 10.37859/coscitech.v2i2.2940.
[7] H. Kaur and J. Rani, "A Survey on different techniques of steganography", doi: 10.1051/conf/2016.
[8] A. Gustiawan *et al.*, "Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing Oleh : Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing," *JUKI : Jurnal Komputer dan Informatika*, vol. 5, 2023.
[9] K. Udham Singh, "A Survey on Image Steganography Techniques," 2014.
[10] W. M. Abduallah, A. Monem, and S. Rahma, "A Review on Steganography Techniques," *American Scientific Research Journal for Engineering*, [Online]. Available: http://asrjetsjournal.org/
[11] I. Riadi, S. Sunardi, and D. Aryanto, "Algoritma End of File dan Rijndael pada Steganografi Video," *JRST (Jurnal Riset Sains dan Teknologi)*, vol. 5, no. 1, p. 17, Mar. 2021, doi: 10.30595/jrst.v5i1.9187.
[12] A. S. Ansari, "A Review on the Recent Trends of Image Steganography for VANET Applications," *Computers, Materials and Continua*, vol. 78, no. 3, pp. 2865–2892, 2024, doi: 10.32604/cmc.2024.045908.
[13] S. Rahman *et al.*, "A Comprehensive Study of Digital Image Steganographic Techniques," *IEEE Access*, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.
[14] R. Chandramouli and N. Memon, "Analysis of LSB based image steganograph," pp. 1019–1022.
[15] A. D. Cahyono, M. Yasin, and U. N. Malang, "Implemantasi steganografi menggunakan metode end of file (EOF) dalam pengamanan data (Studi kasus pada file AVI, MP3, dan JPEG)."
[16] D. Pramudia *et al.*, "APLIKASI HYBRID STEGANOGRAFI EOF DAN ENKRIPSI AES-128 UNTUK KEAMANAN FILE PDF ANDROID," *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI)*, vol. 02, 2021.
[17] A. Zulfiansyah, H. Kusuma, and M. Attamimi, "Rancang Bangun Sistem Pendeteksi Keaslian Uang Kertas Rupiah Menggunakan Sinar UV dengan Metode Machine Learning," *JURNAL TEKNIK ITS*, vol. 12, no. 2, pp. 2337–3539, 2023.
[18] I. Riadi, S. Sunardi, and D. Aryanto, "Algoritma End of File dan Rijndael pada Steganografi Video," *JRST (Jurnal Riset Sains dan Teknologi)*, vol. 5, no. 1, p. 17, Mar. 2021, doi: 10.30595/jrst.v5i1.9187.
[19] A. S. Ansari, "A Review on the Recent Trends of Image Steganography for VANET Applications," *Computers, Materials and Continua*, vol. 78, no. 3, pp. 2865–2892, 2024, doi: 10.32604/cmc.2024.045908.
[20] S. Rahman *et al.*, "A Comprehensive Study of Digital Image Steganographic Techniques," *IEEE Access*, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i3.13227