Jurnal Quancom
Vol.3, No.2, Desember 2025, pp. 19~25
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI : https://doi.org/10.62375/jqc.v3i2.420

Penerapan Teknik Steganografi Teks pada Format File PDF

Frans Panjaitan[1], Calvin Silaen[2], Marihot Tambunan[3]
[1,2,3] Teknologi Rekayasa Perangkat Lunak, Institut Teknologi Del
franspanjaitan21z@gmail.com

Article Info

Article history:

Received 14 November 2025
Revised 05 Desember 2025
Accepted 30 Desember 2025

Keyword:

AES, Enkripsi, Metadata, PDF

ABSTRACT

This research aims to implement steganography by embedding text messages into PDF files using metadata methods and securing the messages through AES encryption. The project consists of several stages, beginning with the selection of a PDF file to serve as the medium for embedding. Users can then input the message they wish to embed. This message will subsequently be encrypted using the AES method, which is designed to protect the content from unauthorized access. Following this, the encrypted message will be embedded into the PDF file via metadata, ensuring that the structure and appearance of the PDF remain unchanged. During the extraction phase, users possessing the appropriate key can retrieve the embedded message and decrypt it to read its content. The implementation results demonstrate that this method successfully maintains the confidentiality of the message without compromising the structure or appearance of the PDF file, ensuring that the message is accessible only to those with the correct decryption key, thereby enhancing the security of sensitive information storage and transmission.

PENDAHULUAN

Steganografi adalah suatu metode yang kompleks untuk menyembunyikan informasi atau pesan dalam media lain dengan cara yang membuatnya tidak dapat dideteksi oleh pihak yang tidak berwenang. Berdasarkan definisi yang komprehensif steganografi adalah seni dan ilmu komunikasi tersembunyi yang bertujuan menyembunyikan keberadaan pesan itu sendiri [1]. Perkembangan teknologi digital telah memperluas penggunaan steganografi ke dalam berbagai jenis media digital, seperti gambar, audio, teks, dan dokumen. Format PDF (Portable Document Format) kini menjadi salah satu pilihan yang paling menarik untuk penerapan teknik steganografi, berkat strukturnya yang kompleks dan kemampuannya untuk menyimpan informasi tambahan yang tidak terlihat.

Kemajuan yang cepat dalam bidang teknologi informasi dan komunikasi telah menimbulkan tantangan baru terkait keamanan data. Ancaman seperti pemerasan, pencurian data, dan penyadapan informasi sensitif semakin meningkat, yang mendorong para peneliti untuk menciptakan metode perlindungan yang inovatif. Dalam hal ini, steganografi muncul sebagai solusi yang menjanjikan untuk menjaga kerahasiaan informasi. Steganografi tidak sekadar menyembunyikan pesan, tetapi mengaburkan bahkan eksistensi komunikasi itu sendiri [2], memberikan lapisan keamanan yang unik dan efektif.

Dokumen PDF memiliki struktur internal yang sangat rumit, yang mencakup berbagai komponen seperti metadata, anotasi, dan lapisan tersembunyi yang dapat digunakan untuk menyembunyikan informasi. Struktur multilayer PDF memberikan peluang unik untuk steganografi digital, karena memungkinkan penyisipan data pada elemen yang tidak terlihat tanpa mengganggu integritas dokumen [3]. Format ini memberikan fleksibilitas yang memungkinkan pengembangan teknik steganografi yang lebih canggih, di mana pesan dapat disembunyikan dalam elemen-elemen dokumen yang tidak mudah dikenali oleh pengguna umum.

Penerapan steganografi dalam dokumen PDF menghadapi berbagai tantangan teknis yang cukup signifikan. Tantangan utama dalam steganografi digital adalah menjaga integritas dokumen sambil mengimplementasikan metode komunikasi terselubung" [4]. Risiko yang paling signifikan mencakup kemungkinan kerusakan pada file, kehilangan fungsi dokumen, serta potensi deteksi oleh perangkat lunak analisis yang canggih. Dengan demikian, pengembangan metode

steganografi harus dilakukan dengan pendekatan yang memperhatikan aspek keamanan, efisiensi, dan pelestarian dokumen.

Risiko utama termasuk potensi kerusakan file, hilangnya fungsionalitas dokumen, dan kemungkinan deteksi oleh perangkat lunak analisis canggih. Oleh karena itu, pengembangan metode steganografi memerlukan pendekatan yang mempertimbangkan keamanan, efisiensi, dan preservasi dokumen. Alan & Hung menegaskan bahwa teknik steganografi mutakhir sangat kritis dalam menghadapi tantangan keamanan informasi yang berkembang [5].

Kontribusi utama dari penelitian ini adalah menawarkan solusi yang menyeluruh untuk penyembunyian informasi dalam dokumen digital, yang tidak hanya meningkatkan tingkat keamanan tetapi juga memperluas pemahaman dalam bidang steganografi. Mengingat meningkatnya ancaman terhadap keamanan siber, penelitian ini diharapkan dapat menjadi dasar metodologis untuk pengembangan teknik perlindungan data di masa yang akan datang.

METODE

A. Metode yang Digunakan

Steganografi merupakan suatu metode yang digunakan untuk menyembunyikan informasi di dalam media lain, sehingga informasi tersebut tidak dapat terdeteksi oleh pihak yang tidak berwenang. Steganografi merupakan teknik menyembunyikan informasi rahasia dalam media penutup sedemikian rupa sehingga keberadaan informasi yang disematkan tetap tak terdeteksi [6]. Steganografi berbeda dari kriptografi yang hanya bertujuan untuk menyembunyikan makna dari pesan. Steganografi lebih menekankan pada penyembunyian eksistensi pesan itu sendiri. Tujuan utama steganografi berbeda dari kriptografi. Sementara kriptografi berfokus pada melindungi isi pesan, steganografi bertujuan menyembunyikan keberadaan komunikasi itu sendiri, menjadikannya teknik penting untuk transmisi data aman" [7].

Dalam konteks aplikasi ini, teknik steganografi digunakan pada berkas PDF dengan memanfaatkan struktur internal PDF untuk menyembunyikan data rahasia. steganografi PDF memberikan pendekatan inovatif untuk penyembunyian informasi dengan memanfaatkan kompleksitas struktural format file PDF [8]. Proses penyisipan informasi dilakukan dengan memodifikasi metadata atau struktur objek PDF tanpa mengubah tampilan visual dokumen tersebut. Teknik steganografi dalam format dokumen melibatkan metode canggih untuk menyematkan data dalam metadata, definisi font, atau aliran objek, memastikan informasi tersembunyi tetap tak terdeteksi oleh pengamat biasa [9].

Sebelum informasi tersebut disisipkan, biasanya dilakukan proses enkripsi untuk meningkatkan tingkat keamanannya. Proses ini sangat penting karena enkripsi berfungsi untuk melindungi data dari akses yang tidak sah. Meningkatnya pengawasan digital dan ancaman keamanan informasi, steganografi memberikan metode kritis untuk melindungi informasi sensitif dengan menyembunyikan keberadaannya dalam media yang tampak tidak berbahaya" [10].

Proses pengambilan informasi mencakup analisis terhadap struktur PDF yang telah diubah, pengambilan data yang tersembunyi, serta mendekripsi data tersebut untuk mengembalikannya ke bentuk informasi yang semula. Kegiatan ini memerlukan pemahaman yang mendalam mengenai struktur file dan algoritma dekripsi yang diterapkan.

Teknologi Utama dan Perpustakaan Salah satu metode yang efisien dalam steganografi adalah Teknik Penyuntikan Metadata, yang memanfaatkan struktur metadata PDF sebagai sarana untuk menyimpan informasi yang tersembunyi. PDF metadata steganography provides a sophisticated approach to hiding information within document metadata, offering a non-intrusive method of covert communication that preserves the visual integrity of the document [11]. Metadata dalam format PDF menawarkan area penyimpanan yang tidak tampak secara langsung dalam tampilan dokumen, menjadikannya sangat cocok untuk keperluan steganografi. Metode ini memungkinkan penyembunyian informasi tanpa mempengaruhi tampilan visual dokumen, sehingga keberadaan data tersebut menjadi sulit untuk dideteksi oleh pihak ketiga.

Implementasi Detail Salah satu langkah krusial dalam penerapan teknik ini adalah pengembangan Custom Metadata Field. Custom metadata fields in PDF documents present a unique opportunity for steganographic data embedding, as they can be created and manipulated without altering the document's visual representation. [12]. Dalam konteks ini, sebuah field metadata khusus yang disebut '/Secret' telah dibuat. Field ini tidak termasuk dalam standar spesifikasi PDF, sehingga sulit untuk terdeteksi. Untuk melakukan manipulasi metadata, digunakan pustaka PyPDF2, yang memungkinkan pengguna untuk dengan efisien mengedit dan mengelola metadata PDF, Python libraries like PyPDF2 offer powerful tools for PDF metadata manipulation, enabling sophisticated steganographic techniques with minimal computational overhead [13]. Struktur penyimpanan pesan dirancang secara teliti, dengan memanfaatkan format yang terstruktur dan pemisah khusus untuk memisahkan elemen-elemen data, sehingga proses ekstraksi di masa mendatang menjadi lebih mudah.

Sistem Enkripsi Multi-Layer Untuk memperkuat keamanan data yang disimpan, sistem ini menerapkan Sistem Enkripsi Multi-Lapis. Multi-layer encryption techniques, combining Base64 encoding, AES encryption, and integrity verification, provide a robust framework for secure information hiding in digital documents. [14]. Lapisan pertama adalah Lapisan Pengkodean Base64, yang berfungsi untuk mengubah pesan teks menjadi format Base64. Proses ini memastikan bahwa karakter-karakter dalam satu metadata

PDF tetap kompatibel dan mencegah terjadinya kerusakan data selama penyimpanan. Selanjutnya, diterapkan Lapisan Enkripsi AES, yang menggunakan algoritma enkripsi AES dengan kunci simetris. Pemilihan algoritma AES didasarkan pada efisiensi dan kemampuannya untuk dibalik, sehingga memberikan lapisan keamanan tambahan yang sangat penting. Terakhir, sistem ini juga menyertakan Verifikasi Checksum untuk memastikan integritas data. Dengan adanya checksum, keutuhan pesan dapat diperiksa selama proses ekstraksi, sehingga menjamin bahwa informasi yang diambil tetap akurat dan tidak mengalami distorsi.

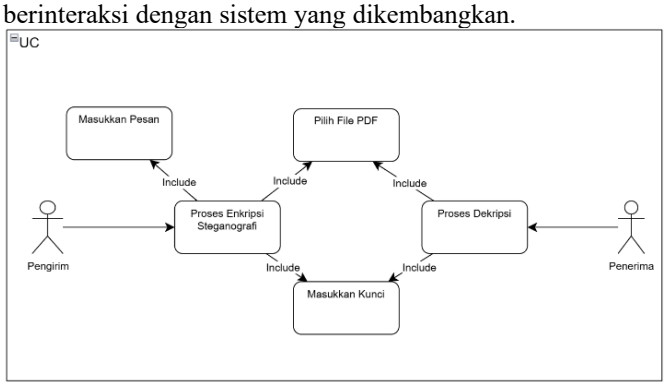
B. Use Case Diagram

Diagram Kasus Penggunaan adalah alat dasar dalam rekayasa perangkat lunak yang berfungsi untuk menggambarkan interaksi sistem steganografi secara menyeluruh. Use case diagram memiliki peran kritis dalam merancang arsitektur keamanan informasi yang kompleks, khususnya dalam konteks steganografi digital[15].

Diagram use case lebih dari sekadar representasi visual, melainkan "mekanisme penting untuk mengidentifikasi alur kerja, potensi kerentanan, dan strategi perlindungan informasi dalam sistem penyembunyian data. Diagram ini memberikan kesempatan kepada peneliti untuk menggambarkan setiap fase transformasi dan pergerakan informasi yang bersifat rahasia.

Use case diagram dalam konteks steganografi berperan penting untuk "mengeksplorasi interaksi kompleks antara pengguna, sistem, dan mekanisme keamanan.

Berikut adalah gambaran bagaimana pengguna berinteraksi dengan sistem yang dikembangkan.

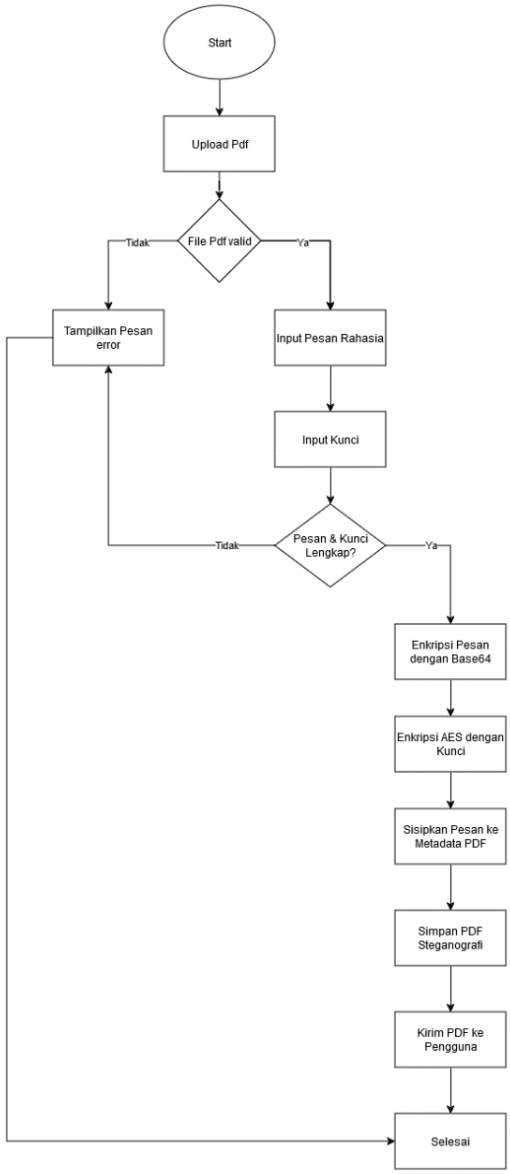


Gambar 1. *Use case* diagram

C. Alur Proses Teknik Steganografi

1. Proses Embbeding

   Pada proses embedding, langkah pertama adalah mengunggah file PDF yang akan digunakan. Pengguna dapat memilih file PDF dari penyimpanan lokal. Setelah file diunggah, sistem akan membaca nilai dari file tersebut. Selanjutnya, pesan rahasia yang ingin disisipkan akan dikonversi menjadi bentuk yang sesuai untuk disisipkan ke dalam metadata PDF. Nilai pesan tersebut kemudian dimasukkan ke dalam metadata di bagian akhir file PDF. Hasil akhir dari proses ini adalah file PDF yang telah disisipi pesan, yang kemudian disimpan di lokasi yang telah ditentukan oleh pengguna. Alur progres dapat dilihat di bawah ini.

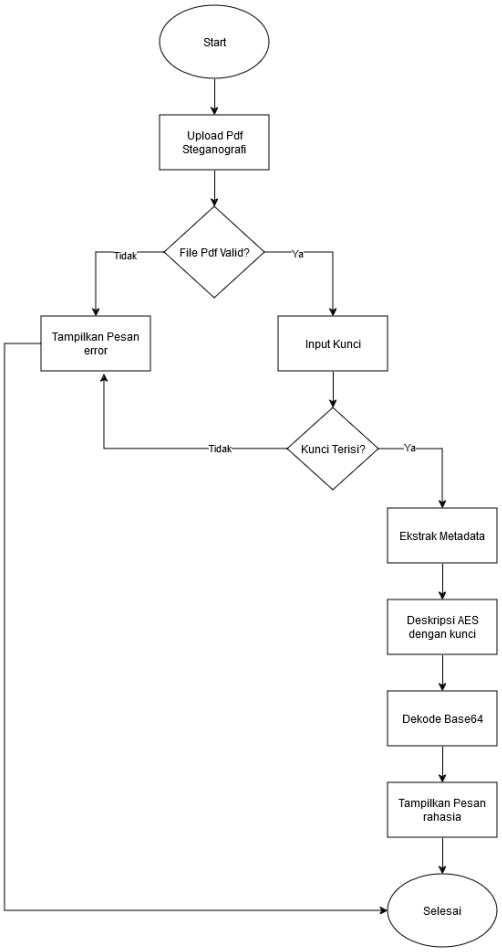


Gambar 2. Proses embedding

2. Proses Ekstraksi

   Pada tahap ekstraksi, langkah awal yang harus dilakukan adalah mengunggah file PDF steganografi yang menyimpan pesan rahasia. Sistem akan melakukan verifikasi untuk memastikan kevalidan file PDF tersebut. Apabila file dinyatakan valid, pengguna akan diminta untuk memasukkan kunci yang digunakan selama proses

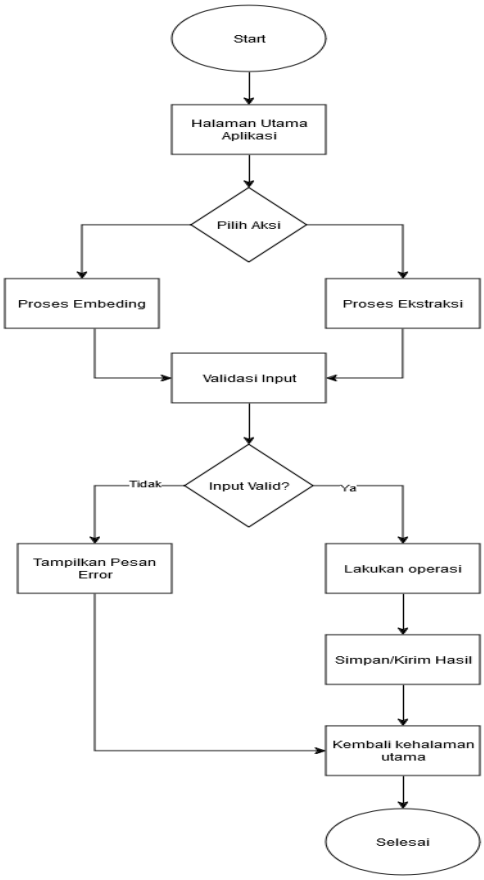
embedding. Jika kunci tidak dimasukkan, sistem akan menampilkan pesan kesalahan. Setelah kunci diinput, sistem akan mengekstrak metadata dari file PDF tersebut. Selanjutnya, sistem akan mendekripsi pesan dengan menerapkan metode AES menggunakan kunci yang telah diberikan. Setelah proses dekripsi selesai, pesan akan dikeluarkan dari format Base64 sehingga dapat dibaca. Pesan rahasia kemudian akan ditampilkan kepada pengguna, menandakan bahwa proses ekstraksi telah berhasil. Apabila terjadi kesalahan selama proses, sistem akan memberikan informasi yang relevan sebelum menyelesaikan tahapan tersebut. Untuk alur progres dapat dilihat dibawah ini.



Gambar 3. Proses ekstraksi

3. Proses Sistem Keseluruhan

Pada keseluruhan alur sistem, proses dimulai dari halaman utama aplikasi. Pengguna diberikan opsi untuk melakukan tindakan, yaitu menyisipkan pesan atau mengekstrak pesan. Apabila pengguna memilih untuk menyisipkan pesan, sistem akan melanjutkan ke tahap embedding. Sebaliknya, jika pengguna memilih untuk mengekstrak pesan, sistem akan beralih ke tahap ekstraksi. Dalam kedua situasi tersebut, langkah berikutnya adalah validasi input untuk memastikan bahwa semua data yang dimasukkan adalah akurat. Sistem kemudian akan memverifikasi keabsahan input. Jika input dinyatakan valid, sistem akan melanjutkan untuk melakukan operasi yang sesuai, baik itu embedding maupun ekstraksi. Setelah proses selesai, hasilnya akan disimpan atau dikirim sesuai dengan pilihan pengguna. Jika input tidak valid, sistem akan menampilkan pesan kesalahan dan mengarahkan pengguna kembali ke halaman utama. Proses akan berakhir setelah semua langkah dilaksanakan dan pengguna kembali ke halaman utama aplikasi.Untuk alur diagramnya dapat dilihat di bawah ini.



Gambar 4. Proses ekstraksi

HASIL DAN PEMBAHASAN

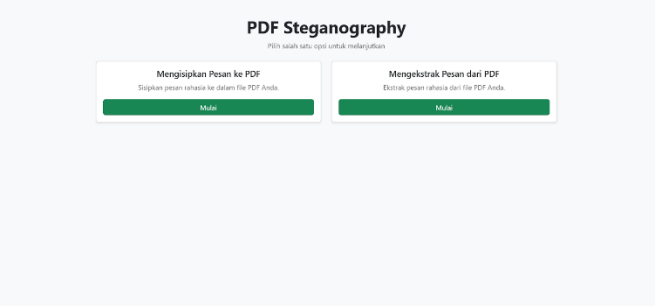
Berdasarkan hasil penerapan metode steganografi teks ke dalam file PDF melalui penggunaan metadata dalam proyek ini, dapat disimpulkan bahwa metode ini efektif untuk

menyisipkan pesan teks tanpa mengubah atau mempengaruhi tampilan visual file PDF tersebut.

Pengujian telah dilakukan pada berbagai file PDF dengan ukuran dan konten yang berbeda-beda. Proses penyisipan pesan melalui metadata berhasil dilaksanakan tanpa mempengaruhi elemen-elemen visual file PDF, seperti teks atau gambar. Hal ini menunjukkan bahwa penyisipan pesan dalam metadata dapat dianggap sebagai metode yang aman dan tidak terlihat.

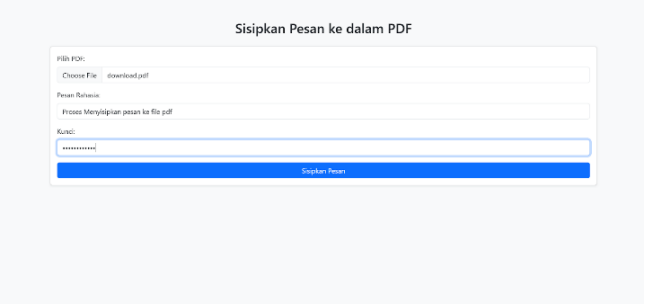
Pengujian dan Evaluasi Keberhasilan Implementasi

Pada fase pengujian, sistem mampu menyisipkan pesan teks ke dalam file PDF melalui metadata dengan baik, tanpa mengubah tampilan file tersebut. Setelah melakukan pengujian pada berbagai jenis file PDF, baik yang hanya berisi teks, gambar, maupun kombinasi dari keduanya, pesan tersebut berhasil disisipkan dan terenkripsi dengan tepat.



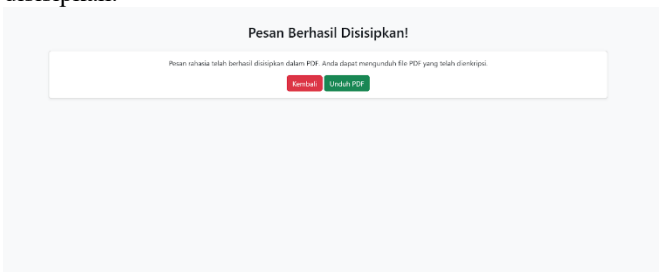
Gambar 5. Tampilan awal/home

Gambar diatas merupakan tampilan awal ketika aplikasi diakses. Halaman ini menawarkan dua pilihan utama terkait Steganografi PDF, yaitu menyisipkan pesan rahasia ke dalam berkas PDF dan mengekstrak pesan rahasia dari berkas PDF. Pengguna dapat memilih opsi yang sesuai dengan kebutuhan mereka.



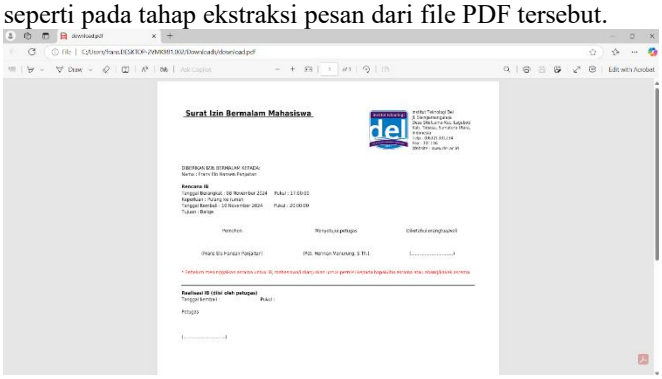
Gambar 6. Tampilan menyisipkan pesan ke file PDF

Pada gambar di atas, ditampilkan antarmuka untuk menyisipkan pesan ke dalam file PDF menggunakan metadata. Proses ini memungkinkan pengguna untuk memilih file PDF yang akan digunakan sebagai media penyisipan pesan. Selanjutnya, pengguna dapat mengisi pesan yang ingin disisipkan, serta menentukan kunci sebagai langkah pengamanan. Penambahan kunci ini bertujuan untuk memastikan kerahasiaan dan keamanan pesan yang disisipkan.

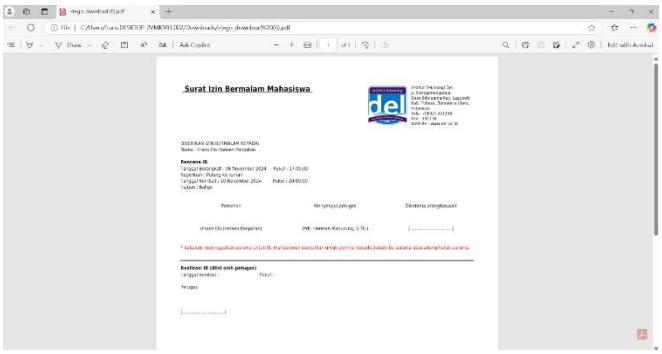


Gambar 7. Tampilan setelah berhasil menyisipkan pesan

Gambar di atas menunjukkan antarmuka setelah pesan berhasil disisipkan ke dalam file PDF. Pada tahap ini, pengguna memiliki opsi untuk mengunduh file PDF yang telah dimodifikasi untuk digunakan atau diproses lebih lanjut, seperti pada tahap ekstraksi pesan dari file PDF tersebut.



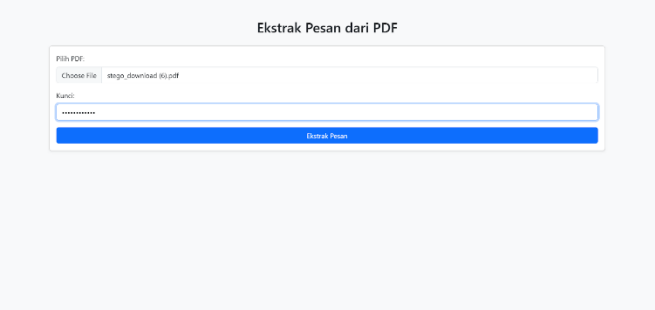
Gambar 8. Tampilan file pdf sebelum proses penyisipan



Gambar 9. Tampilan untuk mengekstrak pesan yang disisipkan

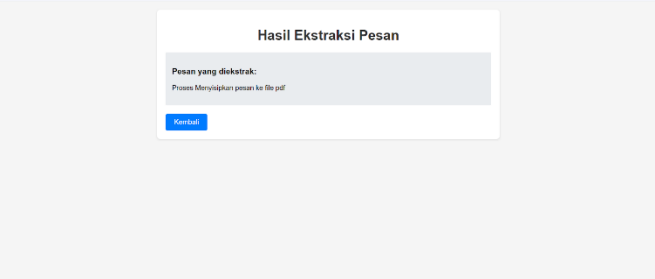
Pada kedua gambar di atas, terdapat perbandingan antara file PDF sebelum dan sesudah proses penyisipan pesan. Jika diamati, tidak ada perbedaan visual yang terlihat antara kedua file tersebut. Hal ini mengindikasikan bahwa penyisipan pesan tidak memengaruhi tampilan file PDF, sehingga memastikan keamanan pesan tersebut. Pesan yang disisipkan hanya dapat diakses dengan kunci yang sesuai, sehingga tidak

dapat diakses oleh pihak yang tidak berwenang.



Gambar 10. Tampilan untuk mengekstrak pesan yang disisipkan

Gambar di atas menunjukkan tampilan antarmuka yang digunakan untuk mengekstrak pesan yang disisipkan dalam file PDF. Pengguna memiliki opsi untuk memilih file PDF yang mengandung pesan tersembunyi dan memasukkan kunci yang relevan guna memastikan keberhasilan proses ekstraksi. Hanya dengan kunci yang benar, pesan tersembunyi dapat diakses, sehingga menjaga kerahasiaan dan keamanan informasi tersebut.



Gambar 11. Tampilan untuk mengekstrak pesan yang disisipkan

Setelah berhasil mengekstrak pesan dengan menggunakan kunci yang tepat, pengguna dapat mengakses dan membaca pesan yang sebelumnya disisipkan ke dalam file PDF. Proses ini menjamin bahwa pesan hanya dapat diakses oleh individu yang memiliki kunci yang valid.

SIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, metode penyisipan pesan melalui metadata pada file PDF terbukti sangat efektif. Pesan dapat disisipkan ke dalam file tanpa mengganggu struktur atau tampilan dari file PDF itu sendiri. Hal ini memastikan bahwa keberadaan pesan tidak dapat terdeteksi oleh pihak yang tidak berwenang, sehingga keamanan pesan dapat terjaga dengan baik.

Keamanan pesan semakin ditingkatkan dengan penerapan enkripsi AES. Proses enkripsi ini menjamin bahwa hanya pengguna yang memiliki kunci yang tepat yang dapat mengakses pesan yang disisipkan. Tanpa kunci tersebut, pesan akan tetap dalam keadaan terenkripsi dan tidak dapat diakses. Oleh karena itu, metode ini sangat sesuai untuk menjaga kerahasiaan pesan dalam file PDF, terutama pada dokumen-dokumen penting seperti kontrak bisnis atau informasi pribadi.

Lebih lanjut, proses penyisipan dan ekstraksi pesan dirancang dengan antarmuka yang intuitif. Pengguna hanya perlu mengunggah file, memasukkan pesan yang ingin disisipkan, dan menentukan kunci enkripsi untuk menyelesaikan proses penyisipan. Proses ekstraksi juga cukup mudah, yaitu dengan memilih file dan memasukkan kunci enkripsi yang sesuai untuk mendapatkan pesan.

Pengujian yang dilakukan menunjukkan bahwa integritas file PDF tetap terjaga setelah proses penyisipan pesan. File dapat digunakan seperti biasa tanpa menunjukkan perubahan yang signifikan. Dengan demikian, metode ini menawarkan solusi yang praktis dan aman untuk kebutuhan penyisipan pesan rahasia pada file PDF, baik untuk keperluan pribadi maupun profesional.

UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, kami mengucapkan puji dan syukur ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat-Nya, sehingga jurnal ini dapat diselesaikan dengan baik. Kami juga menyampaikan terima kasih yang sebesar-besarnya kepada dosen pengampu atas arahan serta bimbingan yang telah diberikan. Harapan kami, jurnal ini dapat memberikan manfaat dan berkontribusi dalam pengembangan ilmu pengetahuan.

DAFTAR PUSTAKA

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography,", 2003.
[2] M. A. A. Al-Husainy, "Information hiding using PDF file format," *International Journal of Computer Applications*, 2014.
[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, 2010.
[4] M. H. Shirali-Shahreza and S. Shirali-Shahreza, "Text steganography in image by changing characters," in *2007 IEEE International Conference on Signal Processing and Communications*, 2007.
[5] W. Mazurczyk, L. Caviglione, and S. Wendzel, *Information hiding: Techniques for steganography and watermarking*. Norwood, MA: Artech House, 2016.
[6] Mazurczyk, W., & Caviglione, L. (2015). "Information Hiding: Techniques for Steganography and Side-Channel Attacks.
[7] Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2007). "A New Approach to Persian/Arabic Text Steganography". 2007 International Conference on Convergence Information Technology.
[8] *Johnson, N. F., Zhi, Z., & Tompsett, E. (2009). "Steganography, Security, and Challenges". In Multimedia Security: Steganography and Digital Watermarking Techniques for Protecting Intellectual Property.*
[9] Chandramouli, R., & Memon, N. (2003). "Digital Steganography: Concepts and Techniques".
[10] Petitcolas, F. A. P., et al. (1999). "Information Hiding: A Survey"
[11] Johnson, N. F., & Jajodia, S. (1998). "Exploring Steganography: Seeing the Unseen".
[12] Alan, M., & Hung, C. C. (2018). "Innovative Steganographic Techniques in Digital Documents".

[13] Chen, X., et al. (2020). "Advanced Information Hiding Techniques in Digital Systems", IEEE Transactions on Information Forensics and Security.
[14] Wayner, P., & Rodriguez, M. (2019). "Steganographic Systems Design and Analysis", ACM Computing Surveys Wayner, P., & Rodriguez, M. (2019). "Steganographic Systems Design and Analysis", ACM Computing Surveys
[15] Kumar, R., & Zhang, L. (2021). "Modeling Security Interaction in Digital Steganography", International Journal of Information Security