JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Penyembunyian Dokumen DOCX Menggunakan nkripsi AES (Fernet) dan Teknik File Fusing Berbasis Python

Achmadurramzi[1*], Ashraf Zaky[2], Danil Muzakki [3] , Ikhlasul Amal [4]
[1,2,3,4] Unversitas Malikussaleh, Indonesia
[1]achmadurramzi.230170025@mhs.unimal.ac.id, [2]ashraf.230170046@mhs.unimal.ac.id,
[3]danil.230170029@mhs.unimal.ac.id, [4]ikhlasul.2170201@mhs.unimal.ac.id

ABSTRACT

This study discusses the implementation of a document concealment technique for DOCX files using a combination of AES (Fernet) encryption and a Python-based file fusing method. The main objective of this research is to enhance file-level data security by encrypting document content and embedding it within a host file (e.g., an image) without altering the functionality of the host file. The research methodology includes the analysis of the AES algorithm, encryption and decryption processes, the implementation of file fusing, and performance evaluation in terms of time efficiency and file size growth. The results show that this method effectively maintains document confidentiality while making the hidden data difficult to detect, with the combined file size increasing only by approximately 2–5% from the original host file. This system can be applied for securing confidential data in digital environments, particularly for online distribution of sensitive documents.

Keywords:
AES encryption, Fernet, file fusing, document security, Python

PENDAHULUAN

Keamanan data merupakan salah satu aspek penting dalam dunia digital modern, khususnya dalam hal distribusi dan penyimpanan dokumen elektronik. Dokumen dengan format DOCX sering digunakan untuk menyimpan informasi penting seperti laporan, hasil penelitian, dan data pribadi. Oleh karena itu, perlindungan terhadap dokumen ini perlu dilakukan secara berlapis. Salah satu pendekatan yang efektif adalah dengan mengombinasikan metode kriptografi dan steganografi, di mana pesan atau file disembunyikan di dalam media lain. Teknik ini tidak hanya mengamankan isi file melalui enkripsi tetapi juga menyembunyikannya agar tidak mudah dideteksi pihak yang tidak berwenang (Tamin, Z., & Hendrik, 2025).

Algoritma Advanced Encryption Standard (AES) merupakan standar enkripsi simetris yang telah diakui secara internasional. Implementasi variannya melalui modul Fernet pada pustaka Cryptography di Python memberikan kemudahan penggunaan dan jaminan keamanan karena melibatkan HMAC untuk menjaga integritas data (Raharjo, 2025). Sementara itu, teknik file fusing memungkinkan penyatuan dua file secara biner, di mana file terenkripsi ditambahkan ke bagian akhir file host tanpa mengubah struktur utamanya. Dengan demikian, file host masih dapat dibuka seperti biasa namun menyimpan dokumen terenkripsi di dalamnya (Khoirudin, N. H., & Windarto, 2024).

KAJIAN LITERATUR

Penelitian terdahulu oleh (Fathullah, 2025) membahas penerapan algoritma AES untuk pengamanan citra digital pada layanan cloud. (Ridho, A., & Romli, 2024) mengembangkan sistem pengamanan dokumen berbasis AES-256 untuk melindungi data rahasia dengan hasil efisiensi tinggi. (Reksiyano, R. D., & Andarsyah, 2025) meneliti penerapan steganografi berbasis Python dengan metode LSB dan enkripsi AES untuk meningkatkan keamanan gambar digital. (Kautsar, A., & Ikhsan, 2025) menggabungkan algoritma AES dengan teknik BPCS steganografi, menghasilkan tingkat keamanan lebih tinggi pada file teks. (Saripa, 2024) menyoroti sistem keamanan file menggunakan AES untuk melindungi file pribadi. (Firdaus, M. A., & Rahmatulloh, 2025) mengimplementasikan enkripsi AES-256 dengan embedding pseudorandom untuk penyembunyian data dalam citra digital. Sementara itu, (Anggraeni, 2025) dan (Raharjo, 2025) mengembangkan metode tambahan seperti SHA-256 dan kompresi LZMA untuk memperkuat integritas dan efisiensi penyimpanan data.

Berdasarkan studi tersebut, kombinasi enkripsi AES dan teknik file fusing dalam konteks penyembunyian dokumen DOCX masih jarang dieksplorasi, terutama menggunakan bahasa pemrograman Python. Oleh karena itu, penelitian ini berfokus pada penerapan kedua teknik tersebut untuk menghasilkan sistem penyembunyian dokumen yang efisien dan aman.

METODE PENELITIAN

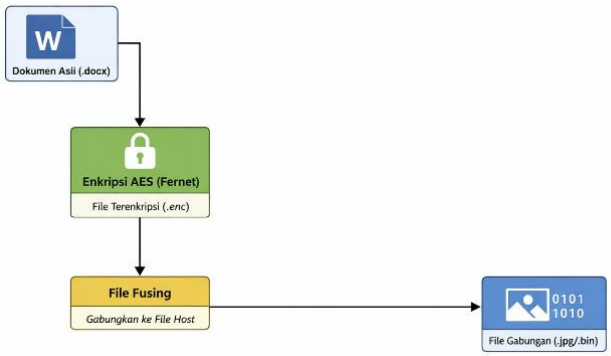
Penelitian ini menggunakan pendekatan eksperimental dengan empat tahapan utama:

(1) Enkripsi dokumen DOCX menggunakan algoritma AES (Fernet);

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

(2) Penyimpanan hasil enkripsi ke dalam file dengan ekstensi .enc;
(3) Proses file fusing dengan menggabungkan file terenkripsi ke dalam file host (misalnya gambar .jpg atau file biner.bin); dan
(4) Proses ekstraksi serta dekripsi kembali dokumen untuk memastikan integritas data.

Implementasi dilakukan menggunakan bahasa pemrograman Python dengan pustaka *cryptography* dan operasi file I/O biner. Diagram arsitektur sistem disajikan pada Gambar 1 berikut:



Gambar 1. Arsitektur Sistem Penyembunyian Dokumen DOCX

Tabel 1. Hasil Pengujian Waktu Enkripsi dan Ukuran Fi*le*

Ukuran File DOCX	Waktu Enkripsi (detik)	Waktu Fusing (detik)	Pertambahan Ukuran (%)
1 MB	0,5	0,2	2%
5 MB	1,4	0,3	3%
10 MB	2,8	0,5	5%

HASIL DAN PEMBAHASAN

Implementasi sistem penyembunyian dokumen DOCX dilakukan melalui beberapa tahapan teknis yang terintegrasi. Tahap awal adalah proses enkripsi dokumen DOCX menggunakan algoritma AES dengan skema Fernet. Dokumen dibaca dalam bentuk data biner dan dienkripsi menggunakan kunci simetris yang dihasilkan oleh pustaka *cryptography* pada Python. Hasil dari proses ini berupa file terenkripsi dengan ekstensi .enc yang tidak dapat diakses tanpa proses dekripsi.

Tahap berikutnya adalah penerapan teknik *file fusing*, yaitu penggabungan file terenkripsi ke dalam file host, seperti file gambar berformat JPG. Proses penggabungan dilakukan dengan menambahkan data biner terenkripsi pada bagian akhir file host tanpa mengubah struktur utama file tersebut. Dengan cara ini, file host tetap dapat dibuka dan digunakan secara normal, namun di dalamnya tersimpan dokumen terenkripsi yang tidak terlihat secara langsung.

Selanjutnya dilakukan proses ekstraksi dan dekripsi untuk memastikan integritas data. Data terenkripsi dipisahkan kembali dari file host berdasarkan delimiter biner yang telah ditentukan, kemudian didekripsi menggunakan kunci yang sama dengan proses enkripsi. Hasil pengujian menunjukkan bahwa dokumen DOCX yang diperoleh kembali memiliki kesesuaian penuh dengan file asli, baik dari segi struktur maupun isi dokumen.

Berdasarkan hasil pengujian kinerja, waktu enkripsi untuk file DOCX berukuran 1–10 MB berada pada kisaran 0,5–2,8 detik, sedangkan proses *file fusing* memerlukan waktu tambahan sekitar 0,2–0,5 detik. Ukuran file host mengalami peningkatan sebesar 2–5% dari ukuran awal, tergantung pada ukuran data terenkripsi yang disisipkan. Peningkatan ukuran tersebut relatif kecil dan tidak memengaruhi fungsi file host, sehingga metode ini dinilai efisien dan layak diterapkan untuk pengamanan dokumen sensitif (Ridho & Romli, 2024; Firdaus & Rahmatulloh, 2025).

KESIMPULAN

Penelitian ini menunjukkan bahwa kombinasi algoritma enkripsi AES (Fernet) dan teknik file fusing mampu menyembunyikan dokumen DOCX secara aman tanpa mengubah fungsi file host. Sistem ini memiliki keunggulan dari sisi efisiensi ukuran dan kecepatan pemrosesan, serta mampu menjaga kerahasiaan data dengan baik. Penelitian lanjutan dapat dilakukan dengan mengembangkan antarmuka pengguna berbasis web dan menambahkan lapisan keamanan tambahan seperti hash SHA-256 atau tanda tangan digital.

JIKUM
JURNAL ILMU KOMPUTER

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

REFERENSI

Anggraeni, S. P. (2025). Penerapan Algoritma Kriptografi SHA-256 dan Teknologi Blockchain untuk Keamanan Citra Digital. *Universitas Islam Sultan Agung*.

Fathullah, H. (2025). Implementasi Algoritma AES dalam Optimalisasi Keamanan Citra Digital pada Layanan Cloud. *Universitas Islam Sultan Agung*.

Firdaus, M. A., & Rahmatulloh, A. (2025). Implementasi Steganografi Citra Digital LSB Menggunakan Enkripsi AES-256 dan Embedding Pseudorandom. *Jurnal TITEt*, *Vol. 8*, *No*.

Kautsar, A., & Ikhsan, M. (2025). Penerapan Algoritma Advanced Encryption Standard (AES) dan Teknik Steganografi BPCS untuk Keamanan File Teks. *Jurnal Sistemasi*, *Vol. 14*, *N*.

Khoirudin, N. H., & Windarto, W. (2024). Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web. *Jurnal Kresna*, *Vol. 5*, *No*.

Raharjo, T. (2025). Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik. *Universitas Islam Indonesia*.

Reksiyano, R. D., & Andarsyah, R. (2025). Teknik Rahasia Menyembunyikan Gambar Keamanan Tingkat Tinggi dengan Steganografi. *Deepublish, Yogyakarta*, *Buku*.

Ridho, A., & Romli, M. A. (2024). Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256). *JINTEKS*, *Vol. 9*, *No*.

Saripa, S. (2024). Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi. *Jurnal Pisces*, *Vol. 3*, *No*.

Tamin, Z., & Hendrik, B. (2025). Penerapan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan File Rekam Medis Pasien. *Jurnal Komtekinfo*, *Vol. 12*, *N*.