JIKUM
JURNAL ILMU KOMPUTER

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

Rancang Bangun Sistem Steganografi Multi-format LSB dan Enkripsi Fernet Berbasis Python

Divaul Khaira[1*], Melinda[2], Isyatul Muna [3] , Kharina [4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]divaul.230170019@mhs.unimal.ac.id,[2]melinda.230170039@mhs.unimal.ac.id,[3]isyatul.230170039@mhs.unimal.ac.id,
[4]kharina.230170129@mhs.unimal.ac.id

ABSTRACT

This research designs a data security system using Python by integrating Fernet Encryption and LSB Steganograph. The system features multi-format capabilities, allowing users to embed text or files into image and audio media. The process begins by encrypting data using a password-based key, which is then embedded into the least significant bits of the carrier media. Experimental results demonstrate that the system effectively maintains data confidentiality with high visual quality. However, the embedding capacity is strictly limited by the size of the carrier media; oversized files cannot be processed if they exceed the available LSB bit space. This system provides an effective solution for small to medium-scale data protection through double-layer security.

Keywords:
Steganography, LSB, Fernet, Python, Multi-format

PENDAHULUAN

Pertukaran data melalui jaringan publik saat ini menghadapi tantangan besar berupa ancaman penyadapan dan pencurian informasi sensitif. Fenomena ini mendorong pengembangan teknik keamanan data yang tidak hanya mengandalkan kriptografi untuk mengacak pesan, tetapi juga steganografi untuk menyembunyikan keberadaan pesan tersebut. Penelitian sebelumnya telah banyak mengeksplorasi penggunaan metode *Least Significant Bit* (LSB) pada citra digital karena kemampuannya menjaga kualitas visual. Namun, teknik LSB murni sering kali gagal memberikan perlindungan jika pihak lawan melakukan analisis statistik (*steganalysis*), sehingga pesan rahasia yang tidak terenkripsi dapat dengan mudah dibaca setelah di ekstraksi . Hipotesis dalam penelitian ini adalah bahwa penggabungan enkripsi berbasis kunci dengan steganografi multi-media akan menciptakan lapisan pertahanan yang jauh lebih kuat dibandingan metode tunggal.

Masalah utama yang diangkat dalam penelitian ini adalah kerentanan keamanan pada bit LSB dan kurangnya fleksibilitas sistem steganografi yang ada, yang umumnya hanya terbatas pada satu jenis format media atau satu tipe pesan saja. Selain itu, muncul kendala teknis terkait kapasitas simpan (payload) di mana pengguna sering kali tidak menyadari batasan ukuran file yang dapat ditampung oleh media tertentu. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang bangun sebuah sistem multi-format menggunakan bahasa pemrograman Python. Penelitian ini berupaya menjawab bagaimana algoritma Fernet dapat mengamankan pesan sebelum disisipkan dan bagaimana efektivitas metode LSB dalam menangani berbagai format media seperti gambar dan audio. Melalui sistem ini, diharapkan integritas data tetap terjaga meskipun menghadapi batasan kapasitas simpan pada media penampung.

KAJIAN LITERATUR

Keamanan Data

Keamanan data merupakan aspek penting dalam pertukaran informasi melalui jaringan digital. Informasi yang dikirim tanpa perlindungan berisiko mengalami penyadapan, manipulasi, atau pencurian oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan mekanisme pengamanan untuk menjaga kerahasiaan dan integritas data selama proses transmisi.

Perkembangan teknologi informasi yang pesat juga meningkatkan risiko kejahatan siber, sehingga penerapan teknik kemanan data menjadi kebutuhan utama dalam sistem komunikasi digital(Saputra et al., 2024).

Steganografi

Steganografi adalah seni dan ilmu menyembunyikan pesan rahasia ke dalam suatu media digital sehingga keberadaan pesan tersebut tidak disadarai oleh pihak ketiga(*1,2 1 , 2*, 2020). Berbeda dengan kriptografi yang memfokuskan pada pengacakan data, steganografi berfokus pada penyamaran data. Dalam sistem modern, steganografi dapat di implementasikan pada berbagai media multimedia seperti citra, audio, video, hingga dokumen digital(Latha & Reddy, 2025)(Dan et al., 2016).

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

Enkripsi Fernet

Fernet merupakan skema enkripsi simetris yang memastikan bahwa pesan yang di enkripsi tidak dapat dibaca atau dimodifikasi tanpa kunci yang sah. Algoitma ini bekerja dengan mengubah teks biasa menjadi nilai string dari *byte*(Ragasiwi et al., 2024). Selain menjamin kerahasiaan, Fernet menggunakan algoritma *Advanced Encryption Standard* (AES) dan *Hash-based Message Authentication Code* (HMAC) untuk menjamin integritas data, sehingga data terlindungi dari perubahan ilegal selama transmisi(Ragasiwi et al., 2024). Selain Fernet, algoritma kunci publik seperti *Rivest Shamir Adleman* (RSA) juga sering digunakan untuk menjaga karahasiaan informasi melalui proses enkripsi dan dekripsi yang sulit dipecahkan(Mulyana et al., 2022)

Metode Least Significant Bit (LSB)

Metode LSB bekerja dengan cara mengganti bit paling tidak signifikan pada nilai piksel gambar atau data audio dengan bit bit data rahasia. Teknik in memanfaatkan keterbatasan indra manusia yang tidak mampu mendeteksi perubahan kecil pada intensitas warna atau frekuensi suara(Ragasiwi et al., 2024). Meskipun efesien, metode LSB murni rentan terhadap deteksi statis, sehingga pengoptimalan sering dilakukan dengan menyesuaikan ukuran muatan (*payload*) secara dinamis berdasarkan format file pembawa(Latha & Reddy, 2025). Implementasi LSB pada Python sering dilakukan dengan memodifikasi nilai piksel gambar sedemikian rupa sehingga perubahan tersebut tidak terlihat oleh mata manusia(Python, n.d.). Teknik ini juga dapat diterapkan pada gambar format PNG untuk memberikan solusi pengamanan data berbasis *client-side*(*E-Issn : 2988-1986*, 2025)

Steganografi Multi-Format

Stegnografi multi-format memungkinkan sistem untuk mengamankan berbagai jenis data tanpa terbatas pada satu format tertentu. Menurut penelitian Latha et al.(2025), sistem *SilentPixels* mampu menyembunyikan data pada berbagai format multimedia dengan menggunakan kalkulator kapasitas adaptif yang mengurangi keterdeteksian statistik hingga 40%. Hal ini sejalan dengan penelitian Aryanto et al. (2023) yang menunjukkan bahwa enkripsi dapat diterapkan pada berbagai format file seperti .pdf, .docx, .jpg, dan .xls untuk meningkatkan keamanan file dokumen.

Python sebagai Bahasa Pemrograman

Python diunggulkan karena sintaksnya yang sederhana dan pustaka yang luas untuk manipulasi piksel gambar dan enkripsi data(Python, n.d.). Python juga dipilih sebagai bahasa utama dalam pengembangan sistem keamanan data. Pustaka seperti *cryptography* untuk enkripsi fernet, PIL (Pillow) untuk pengolahan citra, serta *Tkinter* untuk antarmuka pengguna, memungkinkan pengembangan aplikasi steganografi yang efisien dan fleksibel(Ragasiwi et al., 2024)(Yusri et al., 2025).

Penelitian Terkait

Integrasi antara kriptografi dan steganografi telah terbukti meningkatkan keamanan data secara signifikan melalui perlindungan berlapis. Penelitian oleh Ragasiwi et al. (2024) membuktikan bahwa kombinasi Fernet dan LSB efektif menjaga kerahasiaan informasi digital. Sementara itu, Achmady & Qadriah (2020) menyoroti bahwa penggunaan domain wavelet dalam steganografi audio dapat meningkatkan kapasitas penyimpanan informasi tanpa merusak transparansi kualitas audio asli.

METODE PENELITIAN

Rancangan Penelitian

Penelitian ini menggunakan metode penelitian rekayasa perangkat lunak (research and development) dengan pendekatan ekperimental. Penelitian berfokus pada perancangan, implementasi, dan pengujian sistem steganografi yang menggabungkan metode *Least Significant Bit* (LSB) dan enkrpsi Fernet untuk pengamanan data digital berbasis Python

Tahapan penelitian meliputi:

1. Analisis kebutuhan sistem
2. Perancangan sistem steganografi
3. Implementasi metode LSB dan enkripsi Fernet
4. Pengujian fungsional sistem
5. Evaluasi hasil penyisipan dan ekstraksi data

Ruang Lingkup dan Objek Penelitian

Ruang lingkup penelitian dibatasi pada:

- Penyisipan teks dan file digital ke dalam media penampung berupa citra digital
- Proses enkripsi data menggunakan algoritma Fernet
- Proses ekstraksi dan dekripsi data dari media steganografi

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

Objek penelitian adalah sistem steganografi bebasis Python yang dikemabnagkan untuk mengamankan data digital melalui kombinasi teknik steganografi dan kriptografi.

Alat dan Bahan Penelitian

Alat utama

Alat yang digunakan dalam penelitian ini meliputi:

- Bahasa Pemrograman Python
- Library Python: Pillow (pengolahan citra), cryptography (Fernet), dan Tkinter (antarmuka pengguna)
- Perangkat Keras: Laptop dengan sistem operasi Windows
- Text editor / IDE: Command Prompt dan Notepad

Bahan Penelitian

Bahan yang digunakan antara lain:

- File citra digital berformat PNG
- File audio digital berformat WAV
- Data berupa teks dan file digital sebagai pesan rahasia
- Password sebagai kunci enkripsi dan dekripsi

Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah:

1. Studi Literatur
   Mengkaji jurnal, buku, dan artikel ilmiah terkait steganografi, metode LSB , serta enkripsi Fernet.
2. Eksperimen
   Melakukan pengujian sistem dengan menyisipkan dan mengekstrak data pada berbagai ukuran file dan citra.
3. Observasi

   Mengamati perubahan kualitas citra serta keberhasilan proses ekstraksi data.

Defenisi Operasional Variabel Penelitian

Table 1. Operasional Variabel Penelitian

Variabel	Definisi Operasional
Media Penampung	Citra digital yang digunakan untuk menyisipkan data rahasia
Data Rahasia	Teks atau file digital yang di enkripsi dan disisipkan
Metode LSB	Teknik steganografi dengan memodifikasi bit terendah piksel
Enkripsi Fernet	Algoritma enkripsi simetris berbasis AES
Keberhasilan Ekstraksi	Keamampuan sistem mengembalikan data asli tanpa perubahan

Teknik Analisis Data

Teknik analisis data dilakukan dengan:

- Analisis fungsional, untuk memastikan sistem dapat melakukan proses enkripsi, penyisipan, ekstraksi, dan dekripsi dengan benar
- Analisis akurasi, dengan membandingkan data sebelum dan sesudah proses steganografi
- Analisis visual, dengan mengamati perbedaan citra sebelum dan sesudah penyisipan data

Hasil analisis digunakan untuk menilai efektivitas metode LSB dan enkripsi Fernet dalam menjaga kerahasiaan data digital.

HASIL DAN PEMBAHASAN

Implementasi Sistem

Implementasi sistem merupakan tahap penerapan dari perancangan sistem yang telah dibuat. Pada tahap ini, sistem steganografi dikembangkan menggunakan bahasa pemrograman Python dengan mengombinaskan metode enkripsi Fernet dan steganografi Least Significant Bit (LSB). Sistem ini dirancang untuk melakukan proses enkripsi data, penyisipan data ke dalam media penampung, serta ekstraksi dan dekripsi data.

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

Lingkungan Implementasi

Sistem dikembangkan dan dijalankan pada perangkat laptop dengan spesifikasi sebagai berikut:

- Sistem Operasi: Windows
- Bahasa Pemrograman: Python
- Media Penampung
- Citra PNG dan Audio WAV
- Jenis Data Rahasia: Dokumen (DOC)

Lingkungan implementasi ini digunakan untuk memastikan bahwa sistem dapat berjalan dengan baik pada perangkat komputasi standar.

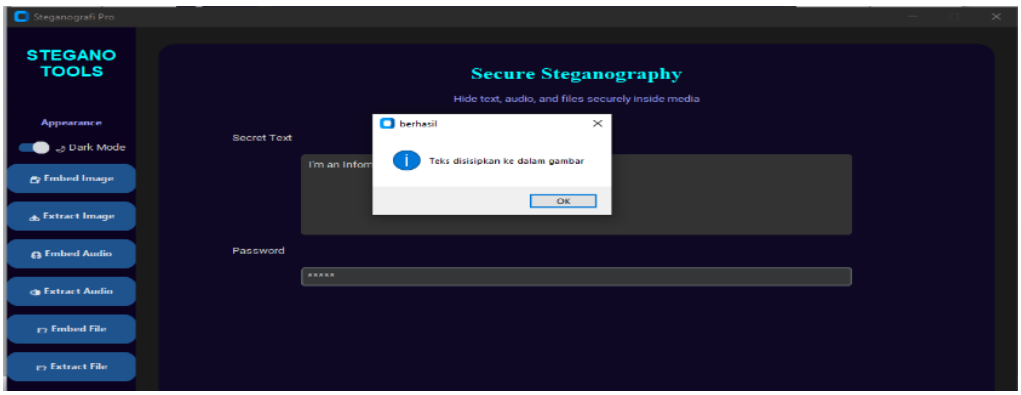
Tampilan Utama Aplikasi

Aplikasi steganografi yang dikembangkan memiliki tampilan antarmuka yang sederhana dan mudah digunakan. Pada tampilan utama, pengguna dapat memilih fitur yang tersedia, yaitu proses penyisipan (embedding) dan proses ekstraksi (exttracting) data rahasia. Tampilan utama aplikasi ditunjukkan pada Gambar 1.

Gambar 1. Tampilan utama aplikasi steganografi berbasis Python

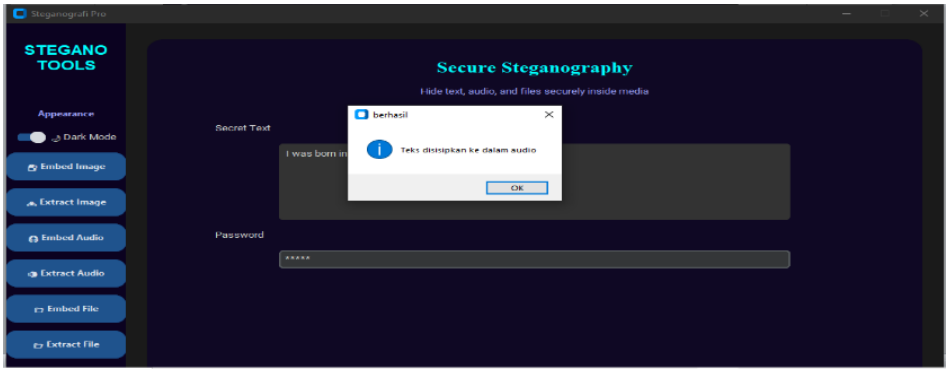
Implementasi Proses Embedding

Proses embedding merupakan tahap penyisipan data rahasia ke dalam media penampung. Pada tahap ini, data rahasia terlebih dahulu dienkripsi menggunakan algoritma Fernet untuk menjaga kerahasiaan isi data. Selanjutnya, data hasil enkripsi disisipkan ke dalam media penampung menggunakan metode LSB. Pengguna memilih media penampung berupa citra PNG atau audio WAV serta file rahasia yang selesai, sistem menghasilkan stego yang telah mengandung data rahasia. Proses embedding pada aplikasi ditunjukkan pada gambar 2, 3, dan 4M.

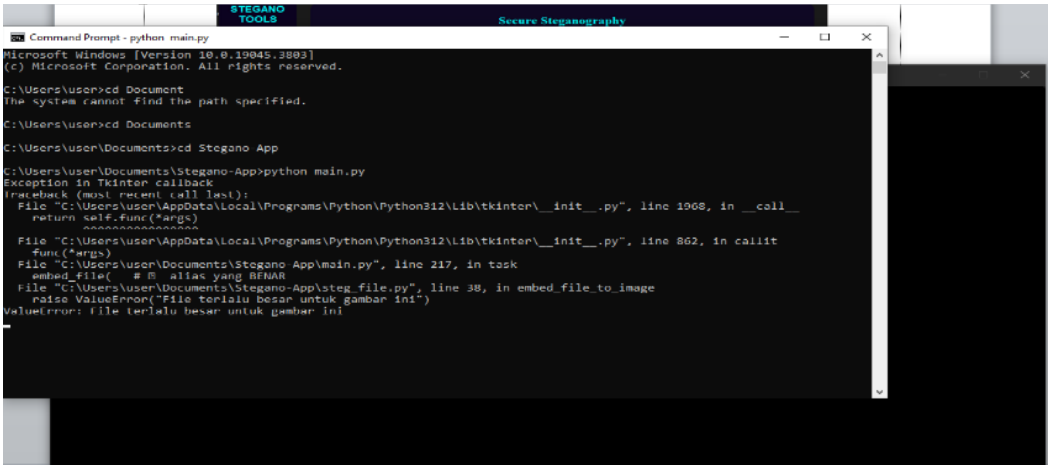


Gambar 2. Proses embedding teks ke image

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



Gambar 3. Proses embedding teks ke audio

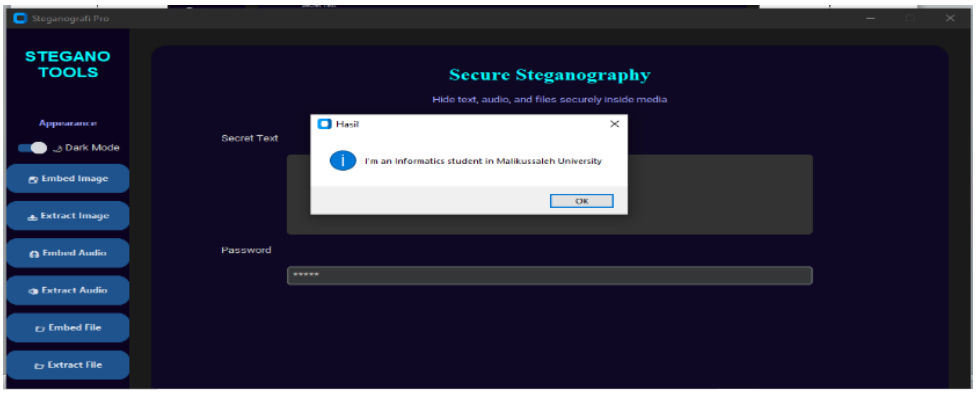


Gambar 4. Proses embedding image ke file docx

Implementasi Proses Ekstraksi

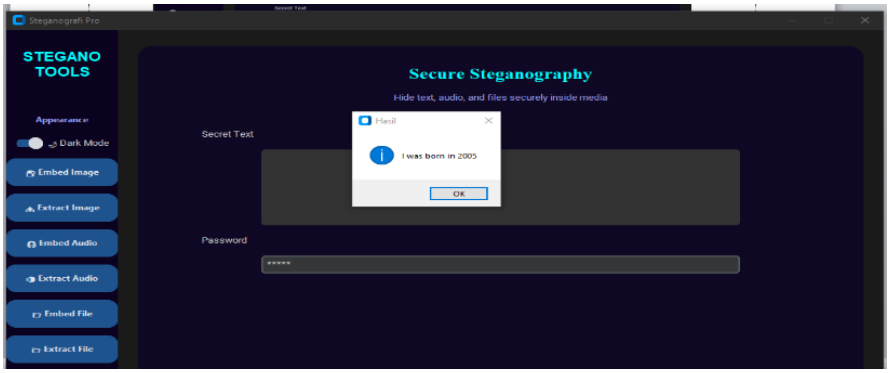
Proses ekstraksi merupakan tahap pengambilan kembali data rahasia dari media stego. Pada tahap ini, sistem membaca bit-bit LSB dari media penampung untuk memperoleh data terenkripsi. Data tersebut kemudian didekripsi menggunakan kunci Fernet yang sesuai.

Pada pengujian yang dilakukan, proses ekstraksi berhasil dijalankan oleh sistem. Namun, pada kondisi tertentu, khususnya ketika ukuran file rahasia melebihi kapasitas media penampung, file hasil ekstrak tidak dapat dikembalikan secara utuh. Proses ekstraksi pada aplikasi ditunjukkan pada gambar 5 dan gambar 6.



Gambar 5. Hasil ekstrak dari stego image

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



Gambar 6. Hasil ekstrak dari stego audio

Hasil Penelitian

Hasil Proses Embedding dan Extracting

Pada tahap ini dilakukan dengan pengujian terhadap sistem steganografi yang dikombinasikan dengan enkripsi Fernet. Data yang digunakan berupa teks dan dokumen (multi-format) yang terlebih dahulu dienkripsi, kemudian disisipkan ke dalam citra digital menggunakan metode *Least Significant Bit* (LSB).

Hasil pengujian menunjukkan bahwa seluruh data berhasil disisipkan ke dalam citra dan dapat diekstraksi. Namun, pada tahap proses penyisipan (embedding) dan tahap ekstrak (extracting) untuk file dokumen, file hasil tidak dapat dibuka dengan baik dan mengalami kerusakan. Ringkasan hasil pengujian penyisipan dan ekstraksi data ditunjukkan pada tabel 2.

Tabel 2. Hasil pengujian

Jenis Data	Ukuran Data	Embedding	Extracting
Teks (.txt)	5 KB	Berhasil	Berhasil
Audio (WAV)	36,5 KB	Berhasil	Berhasil
File (.docx)	230 KB	Gagal	Gagal
PNG	219 KB	Berhasil	Berhasil

Perbandingan Cover Image dan Stego Image

Selain pengujian keberhasilan data, dilakukan pula pengamatan terhadap kualitas visual citra sebelum dan sesudah proses steganografi. Secara visual, tidak terlihat perbedaan yang signifikan antara cover image dan stego image. Hal ini menunjukkan bahwa perubahan bit pada LSB piksel tidak memengaruhi tampilan citra secara kasat mata. Perbandingan antara citra asli dan citra hasil steganografi ditunjukkan pada gambar 7.

Gambar 7. Cover Image

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

Gamabr 8. Stego Image

Hasil ini menunjukkan bahwa metode LSB efektif dalam menyembunyikan data tanpa menurunkan kualitas visual citra, sehingga keberadaan pesan sulit dideteksi oleh pengamat.

Pembahasan

1. Analisis keberhasilan proses embedding

Berdasarkan hasil penelitian, proses embedding data rahasia ke dalam media penampung berupa citra PNG dan audio WAV dapat dijalankan dengan baik oleh sistem. Keberhasilan ni menunjukkan bahwa implementasi metode steganografi *Least Significant Bit* (LSB) telah sesuai dengan rancangan program.

Pada proses embedding, data rahasia terlebih dahulu dienkripsi menggunakan algoritma Fernet, kemudian disisipkan ke dalam media penampung dengan memodifikasi bit paling rendah. Proses ini tidak memengaruhi tampilan media secara signifikan, sebagaimana ditunjukkan pada hasil perbandingan cover image dan stego image. Hal ini membuktikan bahwa metode LSB efektif untuk menyembunyikan data tanpa menurunkan kualitas visual media.

2. Analisis keberhasilan proses embedding

Berdasarkan hasil penelitian, proses embedding data rahasia ke dalam media penampung berupa citra PNG dan audio WAV dapat dijalankan dengan baik oleh sistem. Keberhasilan ini menunjukkan bahwa implementasi metode steganografi *Least Significant Bit* (LSB) telah sesuai dengan rancangan sistem.

Pada proses embedding, data rahasia terlebih dahulu dienkripsi menggunakan algoritma Fernet, kemudian disisipkan ke dalam media penampung dengan memodifikasi bit paling rendah. Proses ini tidak memengaruhi tampilan media secara signifikan, sebagaimana ditunjukkan pada hasil perbandingan cover image dan stego image. Hal ini membuktikan bahwa metode LSB efektif untuk menyembunyikan data tanpa menurunkan kualitas visual media.

3. Analisis kegagalan proses ekstraksi

Meskipun proses embedding berhasil, hasil penelitian menunjukkan bahwa proses ekstraksi mengalami kegagalan ketika ukuran file rahasia lebih besar dibandingkan kapasitas media penampung. Metode LSB memiliki keterbatasan kapasitas penyimpanan data yang bergantung pada ukuran media dan jumlah bit yang digunakan untuk penyisipan.

Kegagalan ini terjadi karena data rahasia yang disisipkan melebihi kapasitas maksimum media penampung, sehingga data yang tersimpan menjadi terpotong dan tidak dapat direkonstruksi secara utuh pada tahap ekstraksi. Dengan demikian, kegagalan ekstraksi yang terjadi bukan disebabkan oleh kesalahan implementasi sistem, melainkan oleh keterbatasan metode steganografi LSB itu sendiri.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa metode LSB efektif untuk penyisipan data berukuran kecil hingga menengah, namun memiliki keterbatasan dalam menangani data berukuran besar tanpa mekanisme tambahan seperti kompresi atau pembagi data.

4. Implikasi dan pengembangan sistem

Hasil pembahasan menunjukkan bahwa sistem steganografi yang dikembangkan telah berfungsi sesuai dengan tujuan perancangan, khususnya dalam aspek penyisipan data dan menjaga kualitas media penampung. Namun, sistem masih memiliki keterbatasan dalam menangani file rahasia berukuran besar.

Sebagai pengembangan lebih lanjut, sistem dapat ditingkatkan dengan menambahkan proses kompresi data sebelum penyisipan, menggunakan media penampung dengan resolusi atau kapasitas yang lebih besar, atau menerapkan metode steganografi lain yang memiliki kapasitas penyimpanan lebih tinggi. Pengembangan tersebut diharapkan dapat meningkatkan keberhasilan proses ekstraksi pada data berukuran besar.

JIKUM
JURNAL ILMU KOMPUTER

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

KESIMPULAN

Penelitian ini menghasilkan sistem rancang bangun steganografi berbasis Python yang mengombinasikan enkripsi Fernet dan metode *Least Significant Bit* (LSB) untuk pengamanan data. Hasil pengujian menunjukkan bahwa proses penyisipan data ke dalam media citra dan audio dapat dilakukan dengan baik tanpa menurukan kualitas visual media secara signifikan.

Namun, penelitian ini memiliki keterbatasan pada kapasitas media penampung. Proses ekstraksi gagal ketika ukuran file rahasia melebihi kapasitas metode LSB, karena algoritma Fernet membutuhkan data terenkripsi yang utuh untuk proses dekripsi. Meskipun demikian, sistem ini bermanfaat sebagai solusi pengamanan data berlapis untuk penyembunyian data berukuran kecil hingga menengah.

Untuk penelitian selanjutnya, disarankan penambahan mekanisme kompresi data, penggunaan media penampung berkapasitas lebih besar, atau penerapan metode steganografi lain agar sistem mampu menangani data berukuran lebih besar secara optimal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing dan seluruh pihak yang telah memberikan bimbingan, araham, serta dukungan selama proses penelitian ini. Ucapan terima kasih juga disampaikan kepada pihak institusi dan rekan-rekan yang telah membantu dalam penyediaan fasilitas dan masukan sehingga peneltian ini dapat diselesaikan dengan baik.

REFERENSI

1,2 1 , 2. (2020). *10*(April), 45–50.

Aryanto, M. B., Tahir, M., Devita, S. I., & Mustofa, Z. N. (2023). *Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)*. *3*(1).

Dan, L. S. B., Des, K., & Citra, P. (2016). *MENINGKATKAN KEAMANAN DATA MENGGUNAKAN METODE STEGANOGRAFI*. *2016*, 9–13.

E-issn : 2988-1986. (2025). *10*(6), 1–5.

Latha, A. G., & Reddy, S. (2025). *Research Digest on Engineering Management and Social Innovations A SECURE , MULTI-FORMAT SYSTEM FOR COVERT COMMUNICATION : IMPLEMENTING ADAPTIVE LSB STEGANOGRAPHY WITH END-TO- END AES ENCRYPTION Research Digest on Engineering Management and Social Innovations*. *October*, 27–50. https://doi.org/10.46647/cy1d5n42

Mulyana, D. I., Heryani, A. P., & Khoirunnisa, V. (2022). *Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text*. *03*(01), 32–39.

Python, L. S. B. P. (n.d.). *Image steganography dengan menggunakan metode lsb pada python*. 1–7.

Ragasiwi, G., S, T. F. N., & L, V. A. (2024). *Pemanfaatan Metode Least Significant Bit dan Kriptografi Fernet dalam Steganografi*. 461–465.

Saputra, R. D., Putra, R. N., Fatma, Y., Informatika, T., Komputer, I., & Riau, U. M. (2024). *Jurnal Computer Science and Information Technology (CoSciTech)*. *5*(1), 36–41.

Yusri, F., Muttaqin, A., Hafiz, A., Syamil, A., & Luqman, M. N. (2025). *Implementasi Algoritma Advanced Encryption Standard (AES) Secara Manual Menggunakan Python*. *1*(1), 12–16.