

Pemanfaatan Metode Least Significant Bit dan Kriptografi Fernet dalam Steganografi

Galih Ragasiwi¹, Timotius Fergiwana N.S², Virgiawan Aditya L.^{3*}

¹Teknik Informatika/Ilmu
Komputer

Universitas Duta Bangsa

¹220103059@mhs.udb.ac.id

² Teknik Informatika/ Ilmu
Komputer

Universitas Duta Bangsa

²220103078@mhs.udb.ac.id

³Teknik Informatika/Ilmu
Komputer

Universitas Duta Bangsa

³220103079@mhs.udb.ac.id

Abstrak— Dalam era digital saat ini, perlindungan informasi sangat krusial mengingat meningkatnya ancaman kejahatan siber dan pencurian data. Steganografi LSB menyembunyikan informasi rahasia dalam bit paling tidak signifikan dari file digital seperti gambar atau audio, sehingga perubahan yang terjadi tidak terlihat oleh mata manusia. Meskipun teknik ini sederhana, keamanannya bisa terancam jika diketahui oleh pihak yang tidak berwenang. Untuk meningkatkan keamanan, kriptografi digunakan sebelum steganografi, dengan algoritma Fernet yang memastikan bahwa pesan terenkripsi tidak dapat dimanipulasi tanpa kunci yang tepat. Penelitian ini mengimplementasikan sistem menggunakan bahasa Python dengan library Stegano dan cryptography.fernet, serta antarmuka pengguna menggunakan Tkinter dan PIL untuk manajemen gambar. Uji coba sistem dilakukan untuk memastikan bahwa data yang dienkripsi dan disisipkan dalam gambar dapat diekstraksi dan didekripsi kembali tanpa kehilangan informasi. Hasil penelitian menunjukkan bahwa kombinasi teknik steganografi dan kriptografi ini efektif dalam meningkatkan keamanan informasi digital.

Kata kunci— Steganografi, Kriptografi, Least Significant Bit, Fernet, Keamanan Data.

Abstract— In today's digital age, information protection has become very important given the increasing threat of cybercrime and data theft. LSB steganography hides secret information in the least significant bits of a digital file such as an image or audio, making the changes invisible to the human eye. Although this technique is simple, its security can be compromised if it becomes known to unauthorized parties. To increase security, cryptography is used before steganography, with the Fernet algorithm ensuring that the encrypted message cannot be manipulated without the right key. This research implements the system using the Python language with the Stegano library and cryptography.fernet, as well as a user interface using Tkinter and PIL for image management. System testing was conducted to ensure that the data encrypted and inserted in the image can be extracted and decrypted again without losing information. The results show that this combination of steganography and cryptography techniques is effective in improving the security of digital information.

Keywords— Steganography, Cryptography, Least Significant Bit, Fernet, Data Security.

I. PENDAHULUAN

Di zaman digital saat ini, perlindungan informasi menjadi sangat penting karena meningkatnya ancaman kejahatan siber dan pencurian data. Keamanan informasi adalah aspek yang sangat penting dalam pertukaran informasi, seperti pengiriman pesan melalui media elektronik. Tanpa keamanan, sering terjadi penyalahgunaan informasi yang merugikan sumbernya. Oleh karena itu, menjaga keamanan informasi yang dipertukarkan menjadi sangat penting agar hanya orang yang berhak yang dapat mengakses informasi tersebut.[1] penggunaan yang massif dalam skala besar-besaran dan tidak terkontrol membuat teknologi menjadi media yang rawan akan tindakan kriminal dan illegal[2], [3].

Dua teknik utama yang sering digunakan untuk meningkatkan keamanan data adalah steganografi dan kriptografi. Teknik steganografi adalah salah

satu teknik yang digunakan untuk melindungi data dengan cara menyisipkan atau menyembunyikannya pada suatu objek tanpa harus mengubah bentuk objek tersebut[4]. Sementara itu, Ilmu yang digunakan untuk memanipulasi data atau informasi secara tidak dapat diuraikan adalah kriptografi. Kriptografi mempelajari teknik-teknik matematika yang berkaitan dengan keamanan informasi, termasuk kerahasiaan, keabsahan, integritas, dan autentikasi data[5], [6].

Salah satu teknik steganografi yang banyak digunakan adalah metode Least Significant Bit (LSB). LSB adalah suatu teknik yang digunakan agar data yang disisipkan ke dalam objek tidak dapat dicurigai oleh pihak-pihak yang tidak berwenang[7]. Teknik ini menyisipkan informasi rahasia ke dalam bit-bit paling tidak signifikan dari file digital, seperti gambar atau audio, sehingga perubahan yang terjadi tidak terlihat oleh

mata manusia. Meskipun metode ini cukup sederhana dan mudah diimplementasikan, keamanan data yang disembunyikan menggunakan LSB dapat terancam jika teknik ini diketahui oleh pihak yang tidak berwenang.

Untuk meningkatkan keamanan data yang disembunyikan, pendekatan umum adalah menggunakan kriptografi sebelum menerapkan steganografi. Salah satu algoritma kriptografi yang populer dan sering digunakan adalah Fernet. Metode enkripsi Fernet, juga dikenal sebagai algoritma Fernet, mirip dengan algoritma AES. Fernet menyediakan rotasi kunci yang dihasilkan melalui MultiFernet selama penyandian atau enkripsi biasa. Untuk mendekripsi teks yang disandikan, Fernet mengeksekusi fungsi kebalikannya konversi teks yang disandikan ke teks biasa, dan keluarannya ditampilkan sebagai nilai "string" dari byte [8], [9], [10].

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi implementasi steganografi menggunakan metode Least Significant Bit (LSB) yang dikombinasikan dengan kriptografi Fernet. Diharapkan bahwa penggabungan kedua teknik ini akan meningkatkan tingkat keamanan data yang disembunyikan dengan efektif.

Kombinasi kedua teknik ini diharapkan dapat meningkatkan keamanan data yang tersembunyi, dengan memanfaatkan kekuatan masing-masing metode untuk membangun sistem keamanan informasi yang lebih kuat.

II. METODOLOGI PENELITIAN

A. Metode Pengumpulan Data

Metode yang digunakan dalam penelitian ini adalah dengan menggunakan pendekatan dalam bentuk studi literatur atau studi kepustakaan.

Penelitian sebelumnya Pada tahun 2020, telah dilakukan penelitian yang berjudul "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android" oleh Endar Nirmala. Studi kasus dari penelitian ini adalah ada begitu banyak modus kejahatan yang berhubungan dengan keamanan dan kerahasiaan data komputer dalam pertukaran data informasi elektronik atau media

internet, diantaranya modus-modus tersebut adalah Interupsi dimana penyerangan yang dilakukan dengan cara merusak suatu data, Interception dimana ancaman dari pihak yang tidak berwenang mendapatkan akses guna mengambil data atau informasi. Dengan demikian, perlu diperlukan teknik atau metode untuk melindungi informasi/data. Dengan mengaplikasikan perpaduan antara teknik Algoritma Kriptografi Advanced Encryption Standard (AES) dan diintegrasikan pada metode Least Significant Bit (LSB). Pada penelitian ini berhasil dibuat satu aplikasi bernama "StegoKripto" yang mana merupakan gabungan dari steganografi dan kriptografi. Aplikasi ini berjalan pada platform Android yang mampu mengenkripsi pesan teks dan menyembunyikan informasi dalam bentuk gambar dengan format .jpg dan .png. [11]

B. Metode pengembangan Sistem

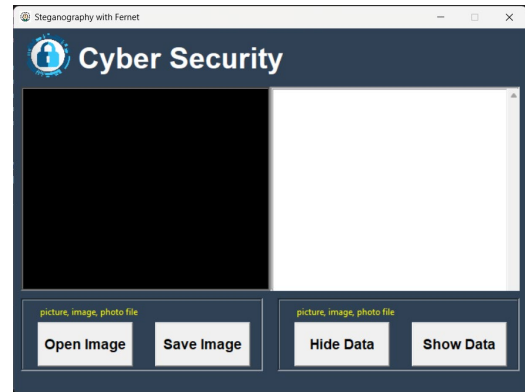
Tahapan dalam metode pengembangan sistem ini terdiri dari beberapa tahap, dimulai dari

1. Analisis kebutuhan
Pengembangan sistem bertujuan untuk memberikan keamanan ganda dalam penyimpanan dan transmisi data melalui penggunaan metode steganografi dan kriptografi. Sistem ini mampu menyembunyikan data di dalam media seperti gambar dengan menggunakan menyisipkannya di setiap bit gambar, serta memastikan data sulit dibaca tanpa enkripsi yang benar.
2. Perancangan
Sistem dirancang dengan menggabungkan teknik steganografi dengan metode Least Significant Bit (LSB) dan kriptografi Fernet yang berfungsi untuk meningkatkan keamanan dan kerahasiaan data. Sistem ini memiliki kemampuan untuk mengenkripsi data, menyembunyikan data terenkripsi di dalam gambar, dan mengekstrak data yang tersembunyi, serta mendekripsi data ke bentuk semula.
3. Implementasi
Pengimplementasian sistem menggunakan bahasa python, untuk menggunakan lsb dan

fernet, penulis menggunakan library Stegano dan cryptography.fernet. untuk membuat tampilan ui sistem, penulis menggunakan tkinter yang disediakan oleh python dan dalam membuka dan menyimpan gambar penulis menggunakan library PIL.

4. Uji coba

Pengujian cobaan sistem dilakukan dengan cara mengujinya secara langsung untuk memastikan bahwa sistem dapat mengenkripsi dan menyisipkan data dalam gambar dengan benar, serta untuk melihat data yang diekstraksi dan didekripsi bisa kembali ke bentuk semulanya tanpa kehilangan informasi.



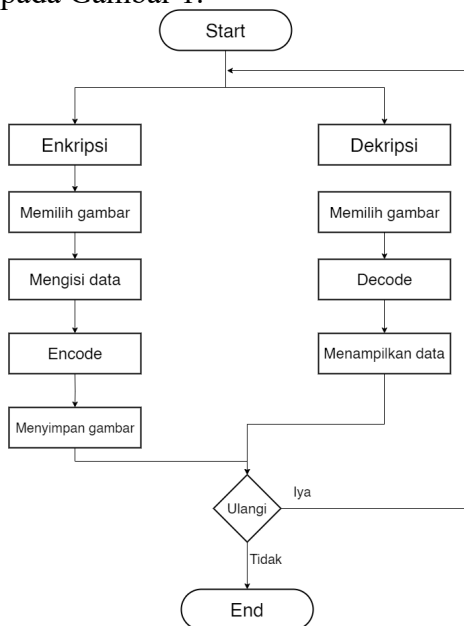
Gambar 2. Halaman Home

Pada halaman home memiliki tampilan yang sederhana, di dalam halaman home terdapat beberapa icon seperti icon open image, save image, hide data, dan show data.

Saat user memencet icon open image untuk memilih gambar yang akan di enkripsi maka munculah halaman baru seperti pada gambar 3.

III. HASIL DAN PEMBAHASAN

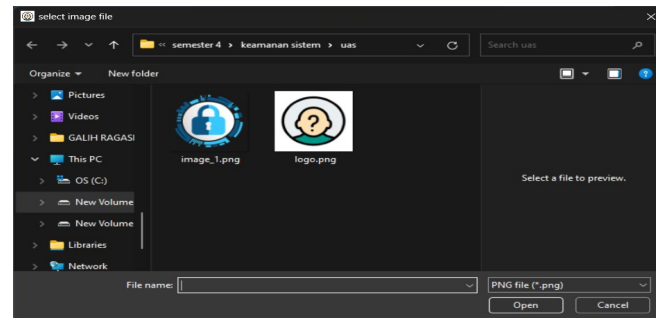
Untuk memahami alur sistem dengan jelas bisa dilihat pada Gambar 1.



Gambar 1. Flowchart Alur Sistem Aplikasi

Pada gambar 1 berisi flowchart alur sistem dimulai dari start lalu user bisa memilih ingin mengenkripsi atau mendekripsi setelah selesai user ingin mengulang atau tidak jika iya maka kembali ke awal dan jika tidak maka sistem berhenti.

Sistem hanya memiliki satu halaman yaitu halaman home yang bisa dilihat pada gambar 2.



Gambar 3. Halaman Untuk Memilih Gambar

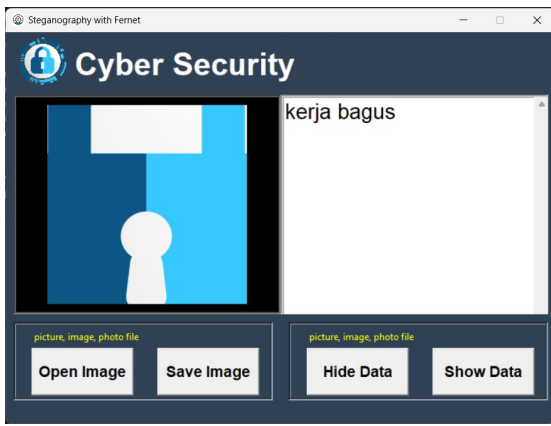
Pada gambar 3 berisi halaman baru untuk memilih gambar dan cara kerjanya menggunakan library PI, untuk lebih jelas bisa dilihat pada gambar 4.

```

def showimage():
    global filename
    filename = filedialog.askopenfilename(initialdir=os.getcwd(),
                                         title='select image file',
                                         filetype=(("PNG file", "*.png"), ("JPG file", "*.jpg"),
                                                    ("All file", "*.txt")))
    img = Image.open(filename)
    img = ImageTk.PhotoImage(img)
    lbl.configure(image=img, width=250, height=250)
    lbl.image = img
    
```

Gambar 4. Source Code Open Image

Setelah memilih gambar user diminta untuk mengisi data apa yang mau diisi .



Gambar 5. Pengisian Data

langkah selanjutnya setelah mengisi data yaitu mengenkripsi, jikalau user ingin mengenkripsi user bisa memencet icon Hide data, untuk mengenkripsi data, penulis menggunakan lsb yang disediakan oleh library dan untuk memperkuat keamanan data penulis menambahkan fernet encryption dengan menggunakan library cryptography.fernet, untuk lebih jelasnya bisa dilihat pada gambar 6.

```
key = Fernet.generate_key()
cipher_suite = Fernet(key)

def hide():
    global secret
    message = text1.get(1.0, END)
    encrypted_message = cipher_suite.encrypt(message.encode())
    secret = lsb.hide(str(filename), encrypted_message.decode('latin-1'))
```

Gambar 6. Source Code Hide Data

setelah selesai mengenkripsi apabila user ingin menyimpan gambar yang telah dienkripsi maka user harus memencet icon save image. Seperti namanya icon save image berfungsi untuk menyimpan gambar, gambar yang disimpan memiliki nama hidden1.png, untuk lebih jelas bisa dilihat pada gambar 7.

```
def save():
    global secret
    secret.save("hidden1.png")
```

Gambar 7. Source Code Save image

Selain enkripsi sistem juga memiliki fitur dekripsi yang berfungsi untuk mengetahui isi pesan yang telah dienkripsi, untuk lebih detailnya bisa dilihat pada gambar 8.

```
def show():
    encrypted_message = lsb.reveal(filename)
    if encrypted_message:
        clear_message = cipher_suite.decrypt(encrypted_message.encode('latin-1')).decode()
        text1.delete(1.0, END)
        text1.insert(END, clear_message)
    else:
        text1.delete(1.0, END)
        text1.insert(END, "No hidden message found.")
```

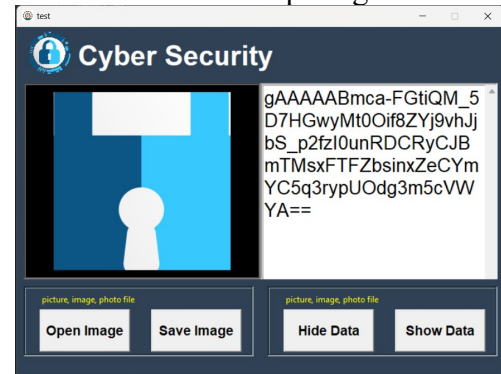
Gambar 8. Source Code Dekripsi

Setelah proses dekripsi selesai maka data yang dienkripsi akan muncul, bisa dilihat pada gambar 9.



Gambar 9. Tampilan Setelah Proses Dekripsi Selesai

Apabila user mendekripsi tanpa menggunakan fernet maka akan muncul seperti gambar 10.



Gambar 9. Tampilan Dekripsi Tanpa Fernet

IV. KESIMPULAN

Penelitian ini bertujuan untuk meningkatkan keamanan data tersembunyi dengan memberikan keamanan ganda. Dengan menggunakan bahasa Python dan library Stegano serta Cryptography.fernet, sistem ini berhasil mengenkripsi, menyisipkan, mengekstrak, dan mendekripsi data dalam file gambar tanpa kehilangan informasi, menjadikan kombinasi kedua teknik ini sebagai solusi yang efektif untuk

perlindungan informasi digital di tengah meningkatnya ancaman kejahatan siber.

REFERENSI

- [1] A. R. Mido, E. Iman, and H. Ujjianto, "ANALISIS PENGARUH CITRA TERHADAP KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB," vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.
- [2] C. Umam and D. Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," 2 st Proceeding STEKOM, vol. 2022, 2022.
- [3] F. Al Isfahani and F. Nugraha, "Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK," 2019. [Online]. Available: <https://www.researchgate.net/publication/338138947>
- [4] Y. R. Nasution, M. Furqan, and M. Sinaga, "Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital," 2020.
- [5] D. Erdriani, M. Ulhusna, and Y. Retno Sari, "PENGUNAAN OPERASI BINER X-OR DAN N-OR PADA KRIPTOGRAFI HILL CIPHER," EDUSAINTEK: Jurnal Pendidikan, Sains dan Teknologi, vol. 10, no. 1, pp. 329–352, Jan. 2023, doi: 10.47668/edusaintek.v10i1.702.
- [6] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi Comparative Analysis of Symmetric and Asymmetric Cryptographic Algorithms in Improving Information System Security," 2023.
- [7] R. A. Akmal, Mhd. F. Furqan, and R. Kurniawan R, "Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital," G-Tech: Jurnal Teknologi Terapan, vol. 7, no. 2, pp. 543–553, Mar. 2023, doi: 10.33379/gtech.v7i2.2300.
- [8] S. Munirah Mohd et al., "THE PERFORMANCE OF THE 3DES AND FERNET ENCRYPTION IN SECURING DATA FILES," J Theor Appl Inf Technol, vol. 15, no. 3, 2024, [Online]. Available: www.jatit.org
- [9] Pronika and S. S. Tyagi, "Enhancing security of cloud data through encryption with AES and fernet algorithm through Convolutional-Neural-Networks (CNN)," International Journal of Computer Networks and Applications, vol. 8, no. 4, pp. 288–299, Aug. 2021, doi: 10.22247/ijcna/2021/209697.
- [10] N. R. Ananthanarayanan and C. Nivetha, "CIPHER AND DECIPHER USING CRYPTOGRAPHY FERNET APPLICATION FOR SECURE DATA", [Online]. Available: www.irjmets.com
- [11] E. Nirmala, J. Surya, K. No, and T. Selatan, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android", [Online]. Available: <http://openjournal.unpam.ac.id/index.php/informatika36>