LAPORAN UAS

MATAKULIAH KRIPTOGRAFI

“Implementasi Vigenere Chiper Dan Steganografi LSB”

KELOMPOK 3

Dosen Pengampu : Saiful Nur Budiman, S.Kom,M.Kom

Disusun Oleh:

Zoulvia Hanest Khinanti	**22104410011**
Rizky Yuniz Teresya	**22104410013**
Umi Hanik	**22104410021**
Asshyffatul Aina Ni'mah	**22104410044**
Bintang Lailatul Mukaromah	**22104410062**
M. Lazuardi Al Ghiffary	**22104410045**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS ISLAM BALITAR

2026

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar belakang

Dalam era digital saat ini, keamanan data menjadi salah satu aspek yang sangat penting dalam proses pertukaran informasi. Setiap hari, data pribadi, pesan, dan informasi sensitif dikirimkan melalui jaringan internet yang sangat rentan terhadap ancaman penyadapan, manipulasi, maupun peretasan. Oleh karena itu, diperlukan suatu metode untuk melindungi data agar tidak mudah dibaca atau diubah oleh pihak yang tidak berwenang. Salah satu cara yang paling umum digunakan untuk menjaga kerahasiaan data adalah dengan menerapkan algoritma kriptografi, sementara steganografi menawarkan pendekatan pelengkap dengan menyembunyikan keberadaan data itu sendiri di dalam media carrier seperti gambar digital. Teknik steganografi Least Significant Bit (LSB) merupakan metode populer yang mengganti bit paling tidak signifikan pada piksel gambar dengan bit-bit pesan rahasia, sehingga perubahan visual hampir tidak terdeteksi oleh mata manusia (Munir, 2022).

Menurut Renaldi Munir (2019), kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti oleh pihak lain yang tidak berhak. Proses ini melibatkan dua tahap utama, yaitu enkripsi (penyandian pesan asli menjadi bentuk rahasia) dan dekripsi (pengembalian pesan rahasia ke bentuk aslinya). Dengan demikian, hanya pihak yang memiliki kunci tertentu yang dapat membaca isi pesan yang telah dienkripsi, dan integrasi dengan steganografi LSB dapat meningkatkan keamanan dengan menyembunyikan pesan terenkripsi tersebut ke dalam gambar.

Algoritma kriptografi klasik merupakan dasar dari perkembangan sistem keamanan modern. Algoritma ini bersifat berbasis karakter, yang artinya proses enkripsi dan dekripsi dilakukan terhadap setiap karakter di dalam pesan. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetris, karena kunci yang digunakan untuk proses enkripsi juga digunakan kembali pada proses dekripsi. Contoh algoritma kriptografi klasik antara lain Caesar Cipher, Affine Cipher, dan Vigenere Cipher, yang dapat dikombinasikan dengan LSB untuk lapisan keamanan ganda.

Salah satu algoritma yang terkenal dan sering digunakan dalam pembelajaran kriptografi klasik adalah Vigenere Cipher. Algoritma ini merupakan pengembangan dari Caesar Cipher yang menggunakan kunci polialfabetik, di mana setiap huruf pada pesan akan digeser sesuai dengan huruf kunci yang bersesuaian. Dengan demikian, tingkat keamanannya lebih tinggi dibandingkan Caesar Cipher yang hanya menggunakan satu nilai pergeseran tetap, dan penerapannya dapat diperkuat dengan penyembunyian melalui steganografi LSB.

Untuk memahami dan mengimplementasikan konsep tersebut secara praktis, dibuatlah sebuah program penerapan algoritma Vigenere Cipher menggunakan bahasa pemrograman Python. Python dipilih karena memiliki sintaks yang sederhana, mudah dipahami, serta banyak digunakan dalam bidang keamanan data dan penelitian akademik. Program ini dirancang agar pengguna dapat memilih menu interaktif untuk melakukan proses enkripsi dan dekripsi dengan mudah, dengan potensi perluasan ke modul steganografi LSB untuk pengujian integrasi.

Melalui penerapan program ini, diharapkan pengguna dapat memahami bagaimana proses penyandian pesan bekerja, mengenal konsep dasar kriptografi klasik dan steganografi LSB, serta mengetahui penerapan algoritma simetris dalam pengamanan data secara sederhana namun efektif.

1.2 Rumus Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam pembuatan program ini adalah:

1. Bagaimana cara menerapkan algoritma Vigenere Cipher untuk proses enkripsi dan dekripsi pesan menggunakan bahasa pemrograman Python, serta mengintegrasikannya dengan teknik steganografi *Least Significant Bit* (LSB) untuk menyembunyikan pesan terenkripsi ke dalam gambar digital?
2. Bagaimana program dapat membantu memahami konsep dasar kriptografi klasik berbasis karakter, sistem kriptografi simetris, dan penerapan steganografi LSB sebagai lapisan keamanan ganda?

1.3 Tujuan

Adapun tujuan dari pembuatan program ini adalah:

1. Mengimplementasikan algoritma Vigenere Cipher dalam bentuk program Python yang dapat melakukan proses enkripsi dan dekripsi pesan, serta

mengintegrasikannya dengan teknik steganografi *Least Significant Bit* (LSB) untuk menyembunyikan pesan terenkripsi ke dalam gambar digital.

2. Memberikan pemahaman praktis tentang penerapan kriptografi klasik berbasis karakter, mekanisme kerja sistem kriptografi simetris, dan integrasi dengan steganografi LSB sebagai lapisan keamanan ganda.

BAB II

DASAR TEORI

2.1 Kriptografi

Kriptografi berasal dari Bahasa Yunani dan memiliki makna seni dalam menulis pesan rahasia (The art of secret writing), dimana kriptografi terdiri dari 2 kata yaitu κρυπτοψανγ yang berarti rahasia atau tersembunyi dan γραφηyang berarti tulisan. Kriptografi juga disebut ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. (Putra dkk., 2023)

Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentiifikasi entitas dan autentifikasi keaslian data. (Mukhtar, 2018)

2.2 Kriptografi Klasik

Algoritma kriptografi klasik (classical cipher) merupakan jenis algoritma yang berbasis karakter, artinya proses enkripsi dan dekripsi dilakukan terhadap setiap karakter di dalam pesan. Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris, yaitu sistem yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini telah digunakan jauh sebelum ditemukannya sistem kriptografi kunci publik, sehingga pembahasan mengenai algoritma klasik juga erat kaitannya dengan sejarah perkembangan kriptografi.(Munir, 2019)

Pentingnya algoritma kriptografi klasik tidak hanya terletak pada nilai historisnya, tetapi juga pada pengaruhnya terhadap pengembangan algoritma kriptografi modern. Hal ini disebabkan karena hampir semua algoritma kriptografi modern, meskipun lebih kompleks, tetap menggunakan dua teknik dasar yang berasal dari algoritma klasik, yaitu substitusi dan transposisi.

2.3 Dua macam cipher algoritma kriptografi klasik

Berdasarkan kedua teknik dasar tersebut, algoritma kriptografi klasik dapat dikelompokkan menjadi dua macam cipher, yaitu:

a. Cipher Substitusi (Substitution Cipher), yaitu teknik yang mengganti setiap karakter dalam pesan dengan karakter lain sesuai pola atau kunci tertentu.
b. Cipher Transposisi (Transposition Cipher), yaitu teknik yang menyusun ulang posisi karakter dalam pesan tanpa mengubah karakter itu sendiri.(Nusa, 2019)

Salah satu contoh cipher substitusi yang terkenal adalah Vigenere Cipher, yang bekerja dengan cara menggantikan huruf dalam pesan menggunakan kombinasi kunci huruf yang berulang. Dengan prinsip tersebut, algoritma ini menjadi salah satu pondasi penting dalam memahami dasar-dasar keamanan data melalui kriptografi klasik.

2.4 Vigenere Cipher

Vigenere Cipher merupakan salah satu contoh terbaik dari cipher abjad-banyak (polyalphabetic cipher). Algoritma ini dipublikasikan oleh seorang diplomat dan kriptolog asal Perancis bernama Blaise de Vigenere pada tahun 1586, meskipun konsep awalnya telah diperkenalkan lebih dahulu oleh Giovan Batista Belaso pada tahun 1553 dalam bukunya La Cifra del Sig. Giovan Batista Belaso. Algoritma ini baru dikenal luas sekitar dua abad kemudian dan kemudian dinamakan Vigenere Cipher.(Munir, 2019)

Pada pertengahan abad ke-19, algoritma Vigenere berhasil dipecahkan oleh Charles Babbage dan Friedrich Kasiski (Piper, 2002). Cipher ini pernah digunakan oleh Tentara Konfederasi (Confederate Army) pada masa Perang Sipil Amerika, namun pesan-pesan yang dienkripsi dengan metode ini akhirnya berhasil diuraikan oleh pihak lawan.

Vigenere Cipher dikenal luas karena sederhana, mudah dipahami, dan mudah diimplementasikan. Proses enkripsi dilakukan menggunakan bujursangkar Vigenere, yaitu tabel alfabet di mana kolom paling kiri menyatakan huruf-huruf kunci dan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam tabel berisi hasil cipherteks yang diperoleh melalui prinsip Caesar Cipher. Jumlah pergeseran huruf plainteks ditentukan oleh nilai huruf pada kunci — misalnya, huruf kunci C (= 2) berarti setiap huruf plainteks digeser dua huruf ke kanan dari urutan alfabet untuk menghasilkan cipherteks.(V. M. Hidayah dkk., 2023)

2.5 Steganografi LSB

Steganografi merupakan teknik penyembunyian data dengan cara menanamkan informasi rahasia ke dalam media carrier seperti gambar digital, audio, atau video tanpa mengubah tampilan visual secara mencolok, berbeda dengan kriptografi yang

mengubah bentuk data menjadi tidak terbaca. Salah satu metode paling sederhana dan populer dalam steganografi citra adalah Least Significant Bit (LSB), yang memanfaatkan bit paling kanan atau paling tidak signifikan dari nilai piksel RGB (merah, hijau, biru) untuk disubstitusi dengan bit-bit pesan rahasia. Proses ini memungkinkan penyisipan data rahasia dengan kapasitas tinggi karena setiap piksel 24-bit dapat menyimpan hingga 3 bit pesan tanpa mengganggu kualitas visual gambar secara signifikan, sehingga perubahan hanya terdeteksi melalui analisis statistik mendalam.

Pada metode LSB, langkah utama meliputi konversi gambar menjadi array piksel biner, penggantian LSB dari setiap kanal warna dengan bit pesan secara berurutan, dan rekonstruksi gambar stego yang menghasilkan Peak Signal-to-Noise Ratio (PSNR) tinggi di atas 50 dB untuk menjaga kesamaan visual. Kelebihan LSB terletak pada kesederhanaan implementasi dan kapasitas embedding besar, tetapi kelemahannya adalah kerentanan terhadap serangan steganalisis seperti chi-square test atau RS analysis karena distribusi bit yang berubah secara statistik. Untuk meningkatkan keamanan, LSB sering dikombinasikan dengan enkripsi seperti Vigenere Cipher sebelum penyisipan, sebagaimana dijelaskan dalam literatur tentang steganografi digital (Munir, 2022).

2.6 Visual studio Code

Visual Studio Code merupakan editor kode sumber gratis dan *open source* yang dikembangkan oleh Microsoft. Ini tersedia untuk Windows, macOS, Linux, dan bahkan dapat dijalankan di web browser. VS Code dikenal dengan antarmuka yang ringan dan dapat disesuaikan serta berbagai fitur yang membantu programmer menulis kode dengan lebih efisien.

Dalam beberapa tahun terakhir, Visual Studio Code telah menjadi salah satu editor kode sumber yang paling banyak digunakan di kalangan pengembang. Meskipun demikian, masih ada beberapa aspek usability yang perlu dievaluasi untuk meningkatkan pengalaman pengguna.(N. A. Hidayah & Rofiqoh, 2024)

2.7 Proses Dasar Kriptografi

Kriptografi merupakan ilmu dan seni yang digunakan untuk mengamankan pesan ketika pesan dikirim dari suatu sumber ke tempat tujuan. Proses ini terdiri dari tiga fungsi dasar antara lain:

1. Enkripsi, proses mengubah pesan asli menjadi berbentuk kode-kode yang susah atau bahkan tidak bisa dimengerti.
2. Dekripsi, proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli.
3. Kunci, sekumpulan parameter yang digunakan dalam proses enkripsi maupun dekripsi. (Nusa, 2019)

2.8 Tujuan Keamanan Kriptografi

Kriptografi memiliki beberapa tujuan pada beberapa aspek keamanan sebagai berikut:

1. Kerahasiaan (confidentiality), bertujuan agar pesan tidak bisa dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (data integrity), bertujuan agar mendapat jaminan bahwa pesan masih asli/utuh dan tidak dimanipulasi saat pengiriman.
3. Otentikasi (authentication), bertujuan untuk mengidentifikasi kebenaran pihak-pihak yang saling berkomunikasi maupun mengidentifikasi kebenaran pesan.
4. Nirpenyangkalan (non-repudiation), bertujuan agar tidak ada penyangkalan oleh pihak-pihak yang berkomunikasi.(Harahap, 2016)

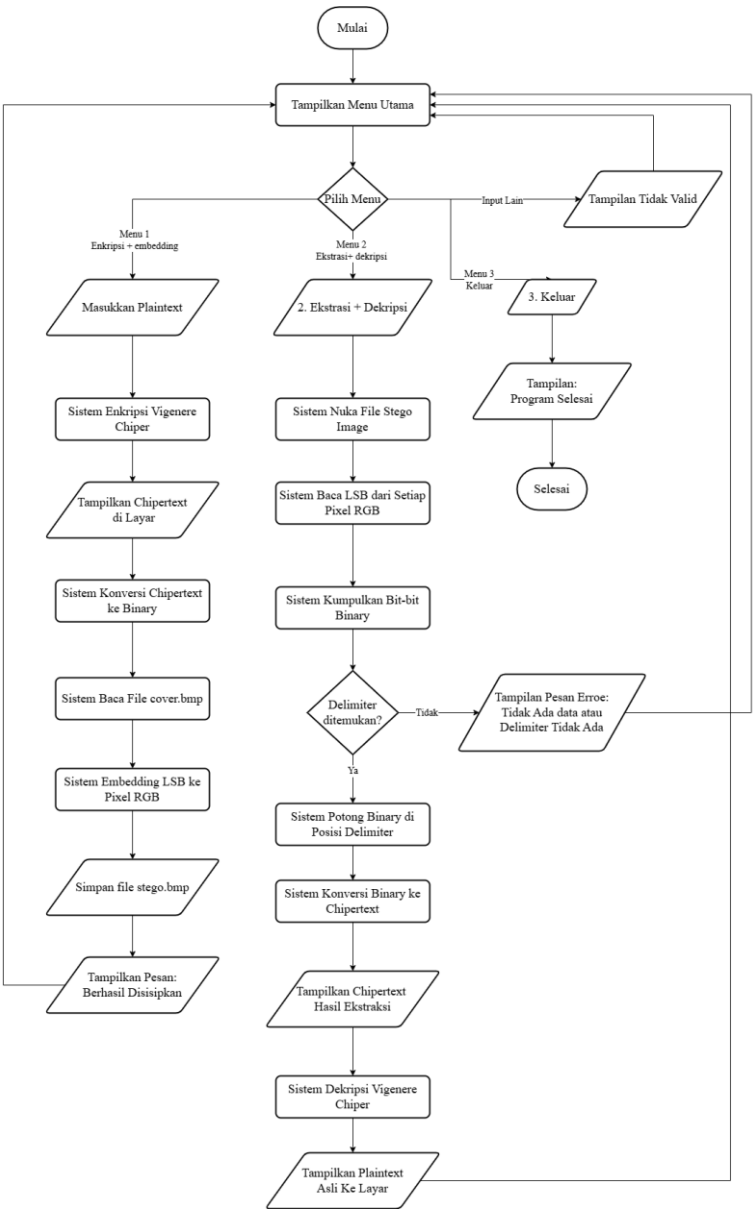
2.9 Python

Python merupakan bahasa pemrograman simpel untuk pembuatan aplikasi berbasis kercedasan buatan atau artifical intelligence. Python juga dianggap memiliki fleksibilitas untuk menangani pembuatan aplikasi-aplikasi kekinian yang mengandung kata kunci big data, data mining, deep learning, data science, hingga machine learning (Agung, 2021)

BAB III

PEMBAHASAN

3.1 Alur penggunaan aplikasi



A. Alur Menu 1 (Enkripsi + Embedding)

1) Menu Input plaintext dari user
2) Enkripsi menggunakan Vigenere Cipher
3) Konversi ciphertext ke binary
4) Embedding binary ke LSB pixel RGB gambar cover.bmp
5) Simpan hasil sebagai stego.bmp
6) Kembali ke menu

B. Alur Menu 2 (Ekstraksi + Dekripsi)

1) Input path stego image
2) Ekstraksi LSB dari setiap pixel RGB
3) Cek apakah delimiter ditemukan (decision point)
4) Jika ya: konversi binary ke ciphertext
5) Dekripsi menggunakan Vigenere Cipher
6) Tampilkan plaintext asli
7) Kembali ke menu

C. Menu 3

Keluar dari program

3.2 Source code Program Vigenere Chiper Dan Steganografi LSB

1. Source Code Enkripsi Vigenere Cipher

```
# ============================
# VIGENERE CIPHER + STEGANOGRAFI LSB RGB
# KELOMPOK 3 - UAS KRIPTOGRAFI
# ============================

from PIL import Image

# ======================
# KONFIGURASI
# ======================
KEY = "MOCHI"
DELIMITER = "1111111111111110"

# ======================
# VIGENERE CIPHER
# ======================

def vigenere_encrypt(plaintext):
    plaintext = plaintext.upper()
    ciphertext = ""
    key_index = 0

    for char in plaintext:
        if char.isalpha():
            p = ord(char) - 65
            k = ord(KEY[key_index % len(KEY)]) - 65
            c = (p + k) % 26
            ciphertext += chr(c + 65)
            key_index += 1
        else:
            ciphertext += char

    return ciphertext
```

Source code dimulai dengan *impor library* PIL.*Image* untuk mendukung pemrosesan gambar pada langkah berikutnya. Selanjutnya, didefinisikan variabel *KEY*

sebagai kunci enkripsi dan DELIMITER sebagai pemisah akhir data biner. Fungsi vigenere_encrypt(*plaintext*) menerima masukan string *plaintext* yang langsung diubah menjadi huruf besar melalui upper(), diikuti inisialisasi ciphertext sebagai wadah hasil enkripsi serta key_index sebagai penanda indeks kunci.

Lewat perulangan *for*, setiap karakter *plaintext* dibaca; pengecekan isalpha() memfilter agar hanya huruf yang diproses, kemudian ord() mengonversi karakter plaintext dan kunci ke nilai numerik, operasi modulo menghasilkan nilai terenkripsi, chr() mengubahnya kembali menjadi huruf, lalu disimpan ke ciphertext. Key_index bertambah pada setiap huruf yang berhasil dienkripsi untuk menggeser pemilihan kunci, sementara karakter non-huruf ditambahkan apa adanya. Pada akhir proses, fungsi mengembalikan ciphertext sebagai hasil enkripsi siap disisipkan ke citra.

2. Source Code Dekripsi Vigenere Cipher dan Konversi Teks ke Biner

```python
def vigenere_decrypt(ciphertext):
    plaintext = ""
    key_index = 0

    for char in ciphertext:
        if char.isalpha():
            c = ord(char) - 65
            k = ord(KEY[key_index % len(KEY)]) - 65
            p = (c - k) % 26
            plaintext += chr(p + 65)
            key_index += 1
        else:
            plaintext += char

    return plaintext

# ========================
# KONVERSI TEKS KE BINER
# ========================

def text_to_binary(text):
    binary = ""
    for char in text:
        binary += format(ord(char), '08b')
    return binary + DELIMITER

```

Pada gambar ini membentuk bagian program kriptografi yang menangani dekripsi melalui algoritma Vigenere Cipher, diikuti konversi hasil ke format biner. Tahap ini menghubungkan kriptografi dengan steganografi, sebab data terdekripsi

diubah menjadi biner untuk penyisipan ke gambar lewat metode Least Significant Bit (LSB).

Fungsi vigenere_decrypt(ciphertext) mengubah ciphertext kembali menjadi plaintext menggunakan kunci Vigenere yang telah ditetapkan. Prosesnya membaca karakter ciphertext secara berurutan untuk huruf alfabet, karakter dikonversi ke numerik, dikurangi nilai kunci sesuai rumus (c - k) mod 26, lalu diubah ulang menjadi huruf dan disimpan ke plaintext. Karakter non-alfabet seperti spasi atau simbol tetap dipertahankan untuk menjaga struktur pesan, hingga seluruh ciphertext selesai diproses.

Setelah dekripsi selesai, plaintext diproses oleh fungsi text_to_binary(text) yang mengonversi setiap karakter ke biner 8-bit berdasarkan nilai ASCII. Rangkaian bit hasil gabungan ditambahkan delimiter sebagai penanda akhir pesan, sehingga siap digunakan untuk penyisipan ke citra digital pada steganografi.

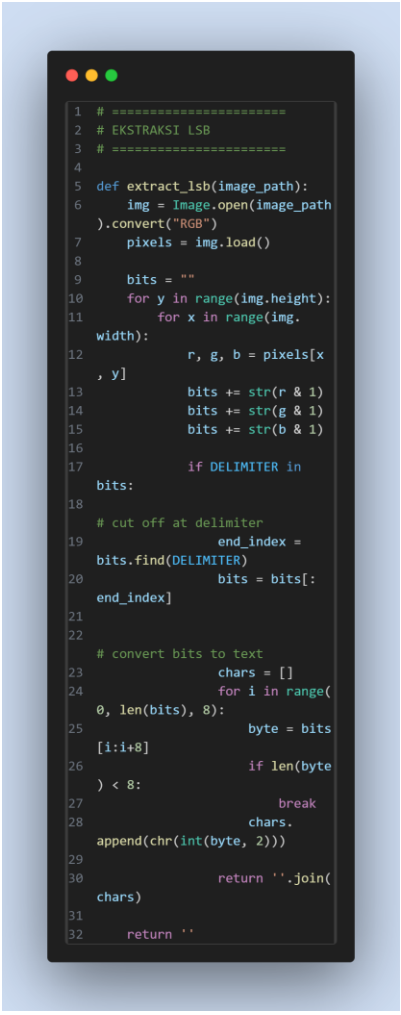
3. Source Code Proses Embedding Pesan Menggunakan Metode LSB

```
# ======================
# EMBEDDING LSB
# ======================

def embed_lsb(image_path, output_path, secret_text):
    img = Image.open(image_path).convert("RGB")
    pixels = img.load()

    binary_data = text_to_binary(secret_text)
    index = 0

    for y in range(img.height):
        for x in range(img.width):
            if index >= len(binary_data):
                img.save(output_path)
                return

            r, g, b = pixels[x, y]

            r = (r & ~1) | int(binary_data[index])
            index += 1

            if index < len(binary_data):
                g = (g & ~1) | int(binary_data[index])
                index += 1

            if index < len(binary_data):
                b = (b & ~1) | int(binary_data[index])
                index += 1

            pixels[x, y] = (r, g, b)

    img.save(output_path)
```

Gambar ini membahas menangani embedding pesan rahasia ke citra digital melalui metode Least Significant Bit (LSB), yang memodifikasi bit paling rendah pada komponen RGB piksel agar perubahan tak terlihat. Fungsi embed_lsb(image_path, output_path, secret_text) membuka gambar asli ke mode RGB, memuat data piksel untuk manipulasi R, G, B, serta mengonversi pesan rahasia ke biner via text_to_binary agar siap disisipkan bit per bit.

Proses penyisipan menggunakan perulangan bersarang atas koordinat lebar dan tinggi gambar; setiap piksel diambil nilai RGB, bit terakhir kanal merah, hijau, biru dimodifikasi bitwise untuk menyimpan bit pesan secara berurutan hingga habis, dengan indeks mengontrol penyelesaian. Gambar hasil embedding disimpan ke output_path, menyembunyikan pesan tanpa ubah visual signifikan, sehingga kode ini mendukung steganografi aman pasca-kriptografi.

4. Source Code Proses Ekstraksi Pesan Menggunakan Metode LSB



```
# ======================
# EKSTRAKSI LSB
# ======================

def extract_lsb(image_path):
    img = Image.open(image_path
).convert("RGB")
    pixels = img.load()

    bits = ""
    for y in range(img.height):
        for x in range(img.
width):
            r, g, b = pixels[x
, y]
            bits += str(r & 1)
            bits += str(g & 1)
            bits += str(b & 1)

            if DELIMITER in
bits:

# cut off at delimiter
                end_index =
bits.find(DELIMITER)
                bits = bits[:
end_index]


# convert bits to text
                chars = []
                for i in range(
0, len(bits), 8):
                    byte = bits
[i:i+8]
                    if len(byte
) < 8:
                        break
                    chars.
append(chr(int(byte, 2)))

                return ''.join(
chars)

    return ''
```

Gambar ini merupakan komponen steganografi yang melakukan ekstraksi pesan rahasia dari citra digital menggunakan metode *Least Significant Bit* (LSB). Proses ini membalik tahap embedding, memungkinkan pengambilan data tersembunyi sambil mempertahankan integritas gambar secara keseluruhan.

Fungsi extract_lsb(image_path) memulai dengan membuka gambar berpesan dan mengonversinya ke mode RGB, memuat data piksel untuk akses langsung nilai R, G, B. Program lalu melacak setiap piksel melalui perulangan, mengekstrak bit paling rendah dari kanal warna via operasi bitwise, dan menyusunnya menjadi rangkaian biner berurutan. Ekstraksi berhenti saat delimiter akhir pesan terdeteksi; biner divalidasi dengan pemotongan, dikelompokkan per 8 bit untuk konversi ASCII menjadi karakter, disimpan dalam list, serta digabung menjadi string pesan lengkap yang siap digunakan.

5. Source Code Menu Utama dan Alur Program Kriptografi dan Steganografi

```
# ======================
# MENU
# ======================

def menu():
    print("\n
==================================
=======")
    print(
" PROGRAM KRIPTOGRAFI & STEGANO
GRAFI "
)
    print(
"================================
========"
)
    print(
"1. Enkripsi + Embedding Pesan"
)
    print(
"2. Ekstraksi + Dekripsi Pesan"
)
    print("3. Keluar")

# ======================
# MAIN PROGRAM
# ======================

while True:
    menu()
    pilihan = input(
"Pilih menu (1/2/3): ")

    # ======================
    # MENU 1
    # ======================
    if pilihan == "1":
        print("\n
--- ENKRIPSI + EMBEDDING ---")
        plaintext = input(
"Masukkan plaintext: ")

        ciphertext =
vigenere_encrypt(plaintext)
        print("Ciphertext:",
ciphertext)

        embed_lsb("cover.bmp",
"stego.bmp", ciphertext)
        print(
"Pesan berhasil disisipkan ke s
tego.bmp"
)
        print(
"CATAT ciphertext di atas untuk
proses dekripsi!"
)

    elif pilihan == "2":
        print("\n
--- DEKRIPSI DARI STEGO IMAGE -
--"
)
        image_path = input(
"Masukkan path stego image (ent
er untuk 'stego.bmp'): "
)
        if not image_path:
            image_path =
"stego.bmp"

        ciphertext_extracted =
extract_lsb(image_path)
        if not
ciphertext_extracted:
            print(
"Tidak ada pesan yang ditemukan
di gambar atau delimiter tidak
ada."
)
        else:
            print(
"Ciphertext hasil ekstraksi:",
ciphertext_extracted)
            plaintext =
vigenere_decrypt(
ciphertext_extracted)
            print(
"Plaintext asli:", plaintext)

    elif pilihan == "3":
        print(
"Program selesai.")
        break

    else:
        print(
"Pilihan tidak valid!")
```

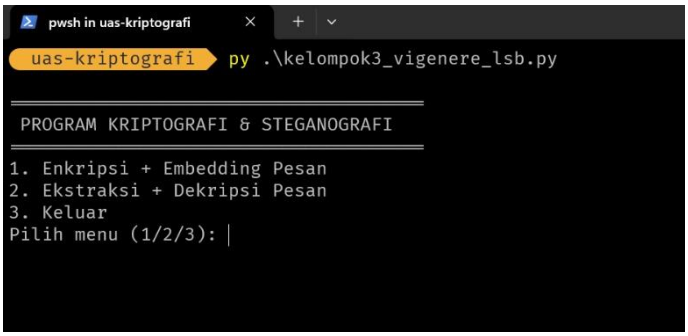
Pada gambar ini membentuk pengendali alur utama sistem kriptografi dan steganografi, menyediakan menu interaktif untuk pilihan proses enkripsi-embedding atau ekstraksi-dekripsi pesan, sehingga pengguna beroperasi mudah tanpa sentuh kode langsung. Fungsi menu() tampilkan tiga opsi nkripsi & embedding, ekstraksi &

dekripsi, keluar dalam perulangan *while True* hingga pilih keluar input pilihan tentukan langkah berikutnya.

Pada opsi pertama, masukkan plaintext untuk enkripsi Vigenere jadi ciphertext (ditampilkan), lalu embedding ke gambar via embed_lsb dengan konfirmasi sukses dan simpan ciphertext referensi. Opsi kedua ekstrak ciphertext dari stego-image pakai extract_lsb, dekripsi via vigenere_decrypt ke plaintext asli, atau tampilkan error jika tak temukan pesan/delimiter. Opsi ketiga hentikan program. Kode ini hubungkan semua fungsi sebelumnya enkripsi, embedding, ekstraksi, dekripsi untuk alur terstruktur, interaktif, dan user-friendly.

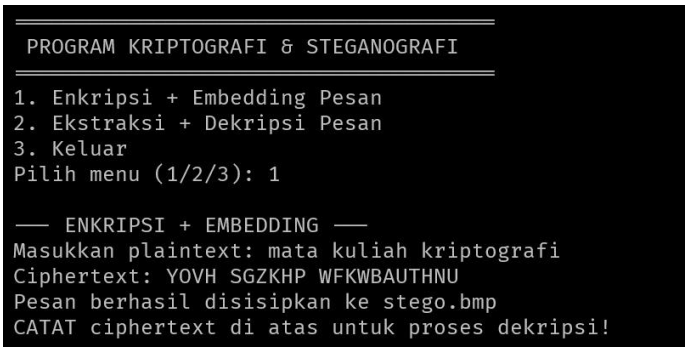
3.3 Implementasi Program Vigenere Chiper Dan Steganografi LSB

1. Tampilan Awal Program



Tampilan tersebut menunjukkan menu utama program kriptografi dan steganografi yang dijalankan melalui terminal PowerShell. Setelah program dieksekusi, sistem menampilkan judul aplikasi beserta daftar menu yang terdiri dari tiga pilihan, yaitu proses enkripsi dan penyisipan pesan, proses ekstraksi sekaligus dekripsi pesan, serta menu untuk mengakhiri program. Pada bagian bawah tampilan, program meminta user memilih salah satu menu dengan memasukkan angka sesuai pilihan yang tersedia. Tampilan ini menjadi tahap awal interaksi sebelum user melanjutkan ke proses pengolahan pesan sesuai dengan menu yang dipilih.

2. Pilihan Enkripsi Dan Embedding Pesan



Tampilan tersebut menunjukkan proses enkripsi dan embedding pesan pada program kriptografi dan steganografi yang dijalankan melalui terminal. User memilih menu pertama untuk memulai proses enkripsi sekaligus embedding pesan. Selanjutnya, program meminta user memasukkan plaintext berupa teks “mata kuliah kriptografi”. Teks tersebut kemudian diolah sehingga menghasilkan ciphertext “YOVH SGZKHP WFKWBAUTHNU”. Setelah proses enkripsi selesai, ciphertext disisipkan ke dalam file gambar *stego.bmp*. Program kemudian menampilkan informasi bahwa pesan telah berhasil dimasukkan ke dalam media gambar dan mengingatkan user untuk mencatat ciphertext yang dihasilkan sebagai bahan pada proses selanjutnya.

3. Pilihan Ekstraksi Dan Deskripsi Pesan

Tampilan program tersebut menunjukkan proses ekstraksi dan dekripsi pesan yang dilakukan melalui menu utama aplikasi kriptografi dan steganografi. Setelah program dijalankan, user memilih menu nomor 2 untuk melakukan dekripsi pesan. Program kemudian meminta user memasukkan lokasi file stego image yang berisi pesan tersembunyi, dalam hal ini file *stego.bmp*. Setelah file diproses, program menampilkan ciphertext hasil ekstraksi dari gambar, lalu melanjutkan dengan proses dekripsi hingga diperoleh plaintext asli. Pada contoh ini, pesan yang berhasil dikembalikan ke bentuk semula adalah “MATA KULIAH KRIPTOGRAFI”. Tampilan tersebut menunjukkan bahwa program mampu mengekstraksi pesan tersembunyi dari media gambar dan mengubahnya kembali menjadi pesan yang dapat dibaca.

4. Pilihan Keluar

Tampilan program tersebut memperlihatkan aplikasi kriptografi dan steganografi yang dijalankan melalui terminal. Pada bagian awal ditampilkan judul program yang menjelaskan fungsi utama aplikasi, yaitu mengamankan pesan melalui proses enkripsi dan penyisipan pesan menggunakan teknik steganografi. Program menyediakan tiga menu pilihan, meliputi proses enkripsi dan embedding pesan, proses dekripsi dengan memasukkan ciphertext secara manual, serta menu untuk mengakhiri penggunaan program. Pada tampilan ini, user memilih opsi keluar dengan memasukkan angka 3, sehingga program menghentikan proses dan menampilkan keterangan bahwa eksekusi telah selesai. Tampilan tersebut menunjukkan bahwa program dapat menerima dan menjalankan perintah sesuai dengan input yang diberikan oleh user.

3.4 Kelebihan Dan Kekurangan Program

A. Kelebihan

1. Keamanan Berlapis Menggunakan 2 lapisan proteksi: enkripsi Vigenere untuk mengacak pesan, dan steganografi LSB untuk menyembunyikan di gambar sehingga sulit dideteksi.
2. Sederhana & Mudah Digunakan Interface berbasis menu yang jelas dengan hanya 3 pilihan, cocok untuk pemula tanpa perlu pengetahuan teknis mendalam.
3. Delimiter Otomatis Sistem penanda akhir pesan memastikan ekstraksi berhenti tepat di akhir data, mencegah pembacaan noise.

B. Kekurangan

1. Enkripsi Lemah Vigenere Cipher mudah dipecahkan dengan analisis frekuensi atau metode Kasiski, tidak aman untuk data sensitif modern.
2. Kapasitas Terbatas Panjang pesan dibatasi jumlah pixel gambar (3 bit per pixel), gambar kecil hanya bisa menyimpan pesan pendek.
3. Program tidak memeriksa apakah file cover.bmp ada, ukuran pesan sesuai kapasitas gambar, atau format file benar sebelum diproses.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembuatan dan penerapan program Vigenere Cipher yang diintegrasikan dengan teknik steganografi Least Significant Bit (LSB) menggunakan bahasa pemrograman Python, dapat disimpulkan bahwa algoritma Vigenere Cipher mampu melakukan proses enkripsi dan dekripsi teks dengan baik menggunakan metode substitusi huruf polialfabetik berdasarkan kunci tertentu, sementara LSB berhasil menyembunyikan pesan terenkripsi ke dalam gambar digital tanpa mengubah tampilan visual secara signifikan. Program ini mempermudah pengguna dalam memahami cara kerja dasar kriptografi klasik simetris dan steganografi sebagai lapisan keamanan ganda, di mana proses enkripsi-dekripsi menggunakan kunci yang sama dan penyembunyian data dilakukan melalui substitusi bit paling tidak signifikan pada piksel gambar.

Melalui menu interaktif Enkripsi Teks, Deskripsi Teks, Steganografi LSB, Ekstraksi Pesan, dan Exit, pengguna dapat secara praktis mengubah teks asli menjadi teks sandi, menyembunyikannya ke dalam gambar, serta mengembalikan pesan rahasia dengan hasil yang akurat dan kualitas stego image terukur melalui metrik PSNR yang tinggi. Pembuatan program ini menunjukkan bagaimana konsep kriptografi klasik seperti Vigenere Cipher dapat diimplementasikan secara sederhana namun efektif dalam Python modern, dengan tambahan steganografi LSB untuk meningkatkan kerahasiaan data di era digital. Dengan demikian, program ini menjadi sarana pembelajaran yang komprehensif untuk memahami prinsip keamanan data melalui kombinasi penyandian pesan dan penyembunyian informasi.

.

DAFTAR PUSTAKA

Agung, G. (2021). *Belajar Sendiri Mengolah Data Dengan Python Dan Pandas Jubilee Enterprise*. PT Elex Media Komputindo.

Harahap, M. K. (2016). ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD. *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, *1*(1), 61–64. https://doi.org/10.30743/infotekjar.v1i1.43

Hidayah, N. A., & Rofiqoh, N. (2024). EVALUASI SOFTWARE VISUAL STUDIO CODE MENGGUNAKAN METODE QUETIONNAIRES NELSEN'S ATTRIBUTES OF USABILITY (NAU). *JURNAL PERANGKAT LUNAK*, *6*(3), 382–391. https://doi.org/10.32520/jupel.v6i3.3383

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks. *Journal on Education*, *5*(3), 8563–8573. https://doi.org/10.31004/joe.v5i3.1647

Mukhtar, H. (2018). *Kriptografi Untuk Keamamanan Data*. CV Budi Utama.

Munir, R. (2019). *KRIPTOGRAFI*. Informatika Bandung.

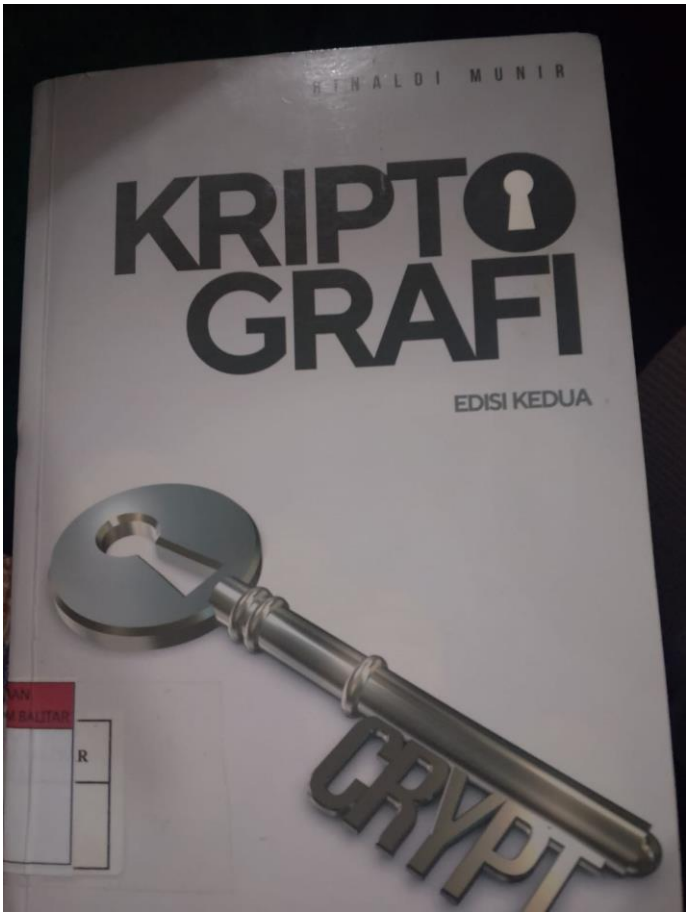
Munir, R. (2022). *Steganografi*.

Nusa, A. C. L. (2019). *Kriptoanalisis Algoritma Vigenere Cipher Perbandingan Multi Bahasa*.

Putra, N. B., Andika, B. C., Bagas, A. D. P., & Ridwan, M. (2023). IMPLEMENTASI SANDI VIGENERE CIPHER DALAM MENGENKRIPSIKAN PESAN. *Jurnal JOCOTIS - Journal Science Informatica and Robotics*.

LAMPIRAN

```python

def vigenere_encrypt(plaintext, key):
    plaintext = plaintext.upper()
    key = key.upper()
    ciphertext = ""
    key_index = 0
    for ch in plaintext:
        if ch.isalpha():
            p = ord(ch) - ord('A')
            k = ord(key[key_index % len(key)]) - ord('A')
            c = (p + k) % 26
            ciphertext += chr(c + ord('A'))
            key_index += 1
        else:
            ciphertext += ch
    return ciphertext

def vigenere_decrypt(ciphertext, key):
    ciphertext = ciphertext.upper()
    key = key.upper()
    plaintext = ""
    key_index = 0
    for ch in ciphertext:
        if ch.isalpha():
            c = ord(ch) - ord('A')
            k = ord(key[key_index % len(key)]) - ord('A')
            p = (c - k + 26) % 26
            plaintext += chr(p + ord('A'))
            key_index += 1
        else:
            plaintext += ch
    return plaintext


def main():
    while True:
        print("\n==============================")
        print("     KELOMPOK 3 KRIPTOGRFI ")
        print("    PROGRAM VIGENÈRE CHIPER")
        print("==================================")
        print("1. Enkripsi Teks")
        print("2. Dekripsi Teks")
        print("3. Keluar")
        print("==============================")

        pilihan = input("Pilih menu (1/2/3): ")

        if pilihan == "1":
            teks = input("\nMasukkan teks yang ingin dienkripsi: ")
            key = input("Masukkan kunci (key): ")
            hasil = vigenere_encrypt(teks, key)
            print(f"\nHasil Enkripsi : {hasil}")

        elif pilihan == "2":
            teks = input("\nMasukkan teks yang ingin didekripsi: ")
            key = input("Masukkan kunci (key): ")
            hasil = vigenere_decrypt(teks, key)
            print(f"\nHasil Dekripsi : {hasil}")

        elif pilihan == "3":
            print("\nTerima kasih telah menggunakan program ini! 👋")
            break

        else:
            print("\nPilihan tidak valid! Silakan coba lagi.")


if __name__ == "__main__":
    main()
```


RINALDI MUNIR
KRIPTO
GRAFI
EDISI KEDUA
CRYPT

Tabel Kontribusi

No	Nama Anggota	NIM	Kontribusi program dan laporan
1	Zoulvia Hanest Khinanti	22104410011	Menyusun BAB I (Pendahuluan) meliputi latar belakang, rumusan masalah, dan tujuan penelitian; merancang alur sistem kriptografi dan steganografi; serta mengatur struktur menu dan alur utama program
2	Rizky Yuniz Teresya	22104410013	Menyusun BAB II (Dasar Teori) terkait kriptografi klasik dan Vigenere Cipher; serta mengimplementasikan fungsi enkripsi dan dekripsi Vigenere Cipher pada program Python
3	Umi Hanik	22104410021	Menyusun BAB II mengenai proses dasar kriptografi dan bahasa Python; mengembangkan fungsi konversi teks ke biner serta mekanisme delimiter sebagai penanda akhir pesan
4	Asshyffatul Aina Ni'mah	22104410044	Menyusun BAB II tentang steganografi Least Significant Bit (LSB); mengimplementasikan proses embedding pesan terenkripsi ke dalam citra digital menggunakan metode LSB
5	Bintang Lailatul Mukaroma	22104410062	Menyusun BAB III (Pembahasan) bagian pengujian dan dokumentasi hasil program; mengimplementasikan proses ekstraksi pesan LSB dari citra stego dan konversi kembali ke teks
6	M. Lazuardi Al Ghiffary	22104410045	Menyusun BAB IV (Penutup) meliputi kesimpulan; melakukan integrasi seluruh modul program, pengujian akhir sistem, serta penyempurnaan laporan