Jurnal Informasi, Sains dan Teknologi
Vol. 7 No. 1 Juni 2024
ISSN: 2828-7207, ISSN: 2829-2758, Hal 121-130
DOI: https://doi.org/10.55606/isaintek.v7i1.201

Penggabungan Algoritma *Vigenere Cipher* dan *Least Significant Bit* untuk Penyisipan Pesan Rahasia pada Gambar

Juwita Nurqomariah
Universitas Trunojoyo Madura

Muhlis Tahir
Universitas Trunojoyo Madura

Nur Azizah Mawar Andini
Universitas Trunojoyo Madura

Ferdiansyah
Universitas Trunojoyo Madura

Siti Rohimah
Universitas Trunojoyo Madura

Ridho Aqil Zakariya
Universitas Trunojoyo Madura

Ira Sentiawati
Universitas Trunojoyo Madura

Alamat: Jl. Raya Telang, Perumahan Telang Inda, Telang, Kec. Kamal, Kabupaten Bangkalan, Jawa Timur 69162
Korespondensi penulis: juwitanurqomariah21@gmail.com

Abstract. *The development of time has significantly impacted human needs for information, especially with the ease of internet access and advancements in information technology. However, this has also posed threats to information security, such as the proliferation of viruses, eavesdropping, and hacker activities. To address these challenges, cryptography and steganography methods have become commonly used approaches. Cryptography plays a role in securing information through message encryption, while steganography aims to conceal data within media to make it difficult for others to discern. This research combines both techniques using the Vigenere Cipher algorithm and LSB steganography method on images. The process successfully produces an additional layer of security, where messages are not only hidden but also encrypted. This implementation demonstrates that messages can be embedded into images without significant visual distortion, effectively enhancing information security.*

Keywords: *Encryption, Least Significant Bit, Vigenere Ciphe.*

Abstrak. Perkembangan zaman telah membawa dampak signifikan terhadap kebutuhan manusia akan informasi, terutama dengan kemudahan akses internet dan kemajuan teknologi informasi yang cepat dan mudah. Namun, hal ini juga memunculkan ancaman terhadap keamanan informasi, seperti serangan virus, penyadap, dan aktivitas hacker yang semakin merajalela, yang

Received April 30, 2024; Revised Mei 09, 2024; Accepted Juni 30, 2023
*Juwita Nurqomariah, juwitanurqomariah21@gmail.com

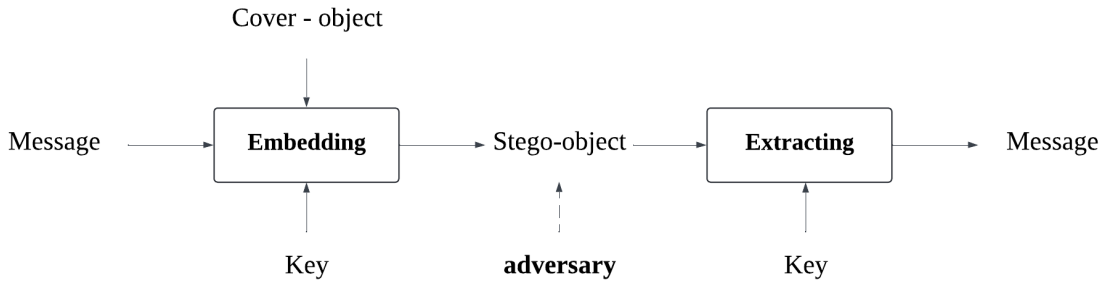
dapat menyebabkan kerugian finansial yang besar dan kehilangan data sensitif. Untuk mengatasi tantangan ini, metode kriptografi dan steganografi menjadi pendekatan yang umum digunakan. Kriptografi berperan dalam mengamankan informasi melalui enkripsi pesan, sementara steganografi bertujuan untuk menyembunyikan data ke dalam media agar sulit dikenali oleh orang lain. Penelitian ini menggabungkan kedua teknik tersebut dengan menggunakan algoritma *Vigenere Cipher* dan metode LSB steganografi pada gambar. Proses ini berhasil menghasilkan lapisan keamanan tambahan, di mana pesan tidak hanya tersembunyi tetapi juga terenkripsi. Implementasi ini menunjukkan bahwa pesan dapat disisipkan ke dalam gambar tanpa distorsi visual yang signifikan, meningkatkan keamanan informasi secara efektif.

Kata kunci: Enkripsi, Least Significant Bit, Vigenere Cipher.

LATAR BELAKANG

Sejalan dengan perkembangan zaman, kebutuhan manusia terkait informasi melaju sangat pesat, terutama dengan kemajuan teknologi informasi dan akses internet yang semakin mudah. Hal ini membawa konsekuensi bahwa potensi untuk terjadinya tindak kejahatan yang menyerang sistem pengguna semakin meningkat. Kemungkinan keamanan informasi melalui internet tidak lagi dapat dijamin secara mutlak karena mesin pencari terus berkembang, sementara serangan virus, penyadap, spam, dan aktivitas hacker semakin merajalela, mengancam pencurian data rahasia.

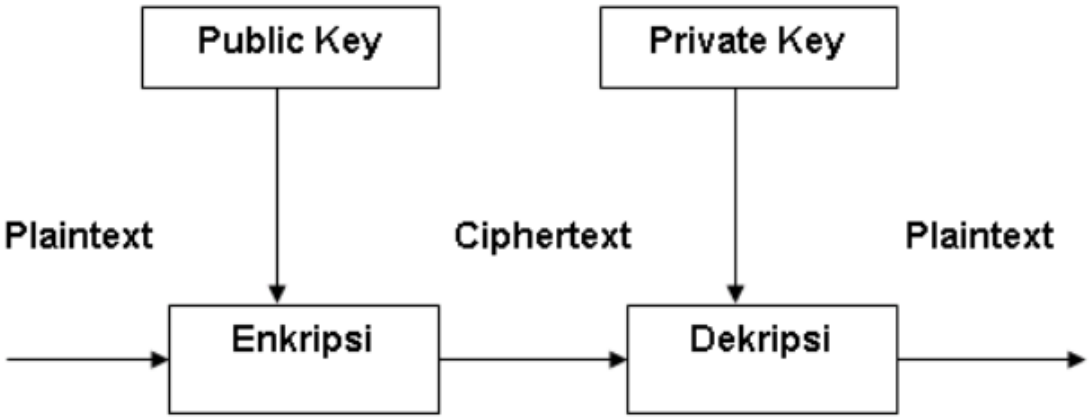
Untuk mengatasi tantangan ini, salah satu pendekatan yang umum digunakan adalah menggunakan metode kriptografi dan steganografi. Kriptografi merupakan sebuah ilmu yang berfungsi untuk menjaga keamanan sebuah informasi, data dan bahkan pesan (Minarni *et al*., 2023). Sedangkan steganografi merupakan sebuah metode untuk menyembunyikan sebuah data ke dalam sebuah media dengan tujuan agar data tersebut sulit dikenali oleh mata manusia (Ramadhani & Susilawati, 2020).



Gambar 1. Skema Steganografi

Dalam Gambar 1. skema steganografi tersebut, dijelaskan bahwa steganografi memiliki 2 proses, yaitu : proses penyisipan (*embedding*) dan proses deskripsi (*extracting*). Proses penyisipan (*embedding*) adalah sebuah metode untuk

menyembunyikan *message* di dalam sebuah *cover-object* dengan memasukan *key*, dengan demikian menciptakan sebuah citra dengan pesan tersembunyi di dalamnya (*stego-obejct*). Sedangkan, proses deskripsi (*extracting*) adalah sebuah metode untuk mendeskripsikan pesan yang telah disembunyikan pada proses penyisipan (*embedding*). Proses *extracting* pada stego-object melibatkan penggunaan key yang sama pada proses penyisipan (*embedding*), sehingga memungkinkan pesan tersembunyi dapat dipulihkan kembali (Utomo & Erwanto, 2019).



Gambar 2. Skema Kriptografi

Sama halnya dengan steganografi kriptografi juga memilki 2 proses dalam cara kerjanya yakni proses enkripsi dan deskripsi seperti yang ada pada Gambar 2. Skema Kriptografi. Proses enkripsi merupakan alur penyembunyian pesan dengan menggunakan key tertentu, di mana *plaintext* akan di ubah menjadi *ciphertext* dengan menggunakan sebuah *key*. Sedangkan, proses deskripsi adalah alur untuk mendeskripsikan *ciphertext* dengan menggunakan *key* sehingga menghasilkan kembali *plaintext* (Cahyadi, 2012).

Steganografi dan kriptografi merupakan dua pendekatan utama dalam menjaga keamanan informasi. Steganografi adalah teknik yang digunakan untuk menyembunyikan pesan rahasia di dalam media yang tampaknya biasa, seperti gambar, sementara kriptografi digunakan untuk mengenkripsi pesan tersebut sehingga hanya penerima yang memiliki kunci yang tepat yang dapat membacanya. Dalam konteks penelitian ini, kedua teknik ini digunakan bersama-sama untuk menciptakan lapisan tambahan keamanan. Pesan tidak hanya tersembunyi dari mata orang yang tidak berwenang, tetapi juga terenkripsi sehingga hanya penerima yang memiliki kunci yang tepat yang dapat membacanya.

Dalam proses pengimplementasian penggabungan steganografi dan kriptografi pada penelitian ini, peneliti menggunakan algoritma kriptografi *Vigenere Cipher* dan metode steganografi *Least Significant Bit* (LSB) pada gambar (Gede Wiryawan *et al*., 2019). Algoritma *Vigenere Cipher* dipilih sebagai algoritma kriptografi utama dalam penelitian ini karena keamanannya yang relatif tinggi dan fleksibilitasnya dalam menangani pesan-pesan yang lebih panjang. Metode LSB (*Least Significant Bit*) kemudian digunakan untuk menyisipkan pesan terenkripsi ke dalam piksel-piksel gambar tanpa menyebabkan distorsi visual yang signifikan. Dengan demikian, kombinasi antara kriptografi dan steganografi dalam penelitian ini bertujuan untuk mencapai tingkat keamanan informasi yang lebih tinggi.

Algoritma *Vigenere Cipher* merupakan pengembangan dari metode algoritma kriptografi *caesar cipher,* yang berfungsi menyandikan teks alfabet berdasarkan huruf-huruf pada kata kunci dengan menggunakan deretan sandi caesar (Alawiyah *et al*., 2020).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 3. Bujur Sangkar Vigenere

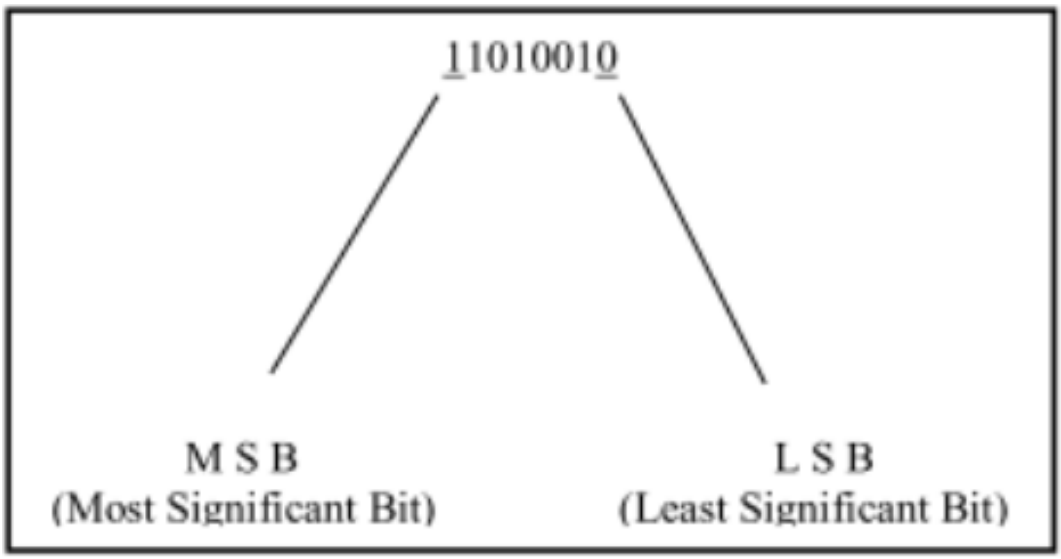
Dalam proses enkripsi dan deskripsi, algoritma *vigenere cipher* dapat diimplentasikan menggunakan 2 metode, yakni secara manual dengan menggunakan tabula recta (bujur sangkar *vigenere*), seperti yang ditunjukkan dalam Gambar 3.

Bujursangkar *Vigenere*. Sedangkan metode lainya ialah metode subtitusi angka secara matematis, yang mana algoritma dalam proses deskripsinya menggunakan persamaan sebagai berikut :

$$Ci = (Pi + Ki) \bmod 26$$

$$Pi = (Ci - Ki) \bmod 26$$

Least Significant Bit (LSB) merupakan bagian dari urutan data biner yang paling kecil atau memiliki nilai yang kurang signifikan, terletak di ujung kanan dari deretan bit (Ramadhani & Susilawati, 2020). LSB biasanya disimpan dalam media penyimpanan seperti citra digital atau gambar. Pada setiap byte (1 byte) terdiri dari 8 bit, ututan bit adalah b7b6b5b4b3b2b1b0, di mana bit b0 adalah yang memilki nilai yang kurang signifikan atau yang paling kecil (LSB), sedangkan bit b7 adalah yang memiliki nilai yang paling signifikan atau yang paling besar (MSB) (Yusup *et al*., 2020).

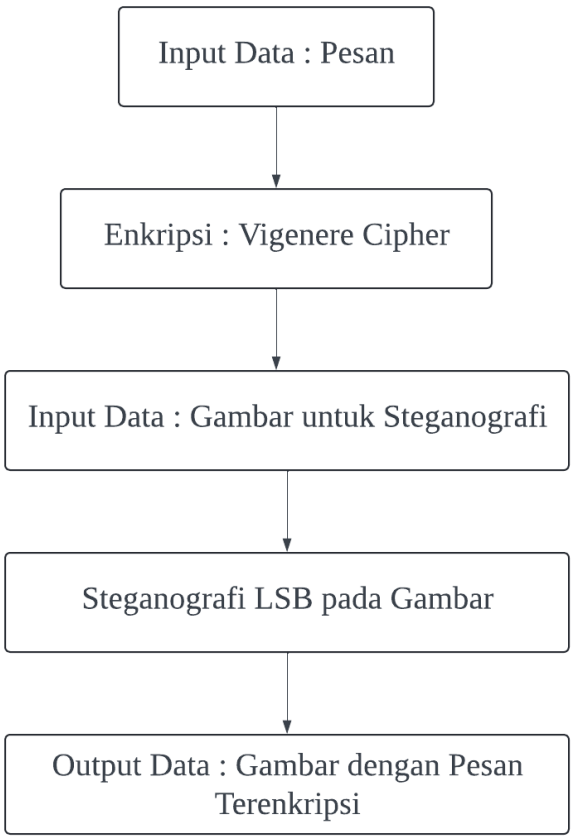


Gambar 4. Susunan Bit

Gambar 4. Susunan Bit, menunjukkan perbedaan antara MSB dan LSB yang mana dari barisan angka 1 paling kanan bernilai 0 yang merupakan bagian dari LSB, sedangkan paling kiri bernilai 1 merupakan bagian dari MSB.

METODE PENELITIAN

Dalam penelitian ini, peneliti menggabungkan dua teknik utama dalam proses implementasi penyisipan gambar, yaitu steganografi LSB dan kriptografi Vigenere Cipher, untuk mencapai tingkat keamanan yang lebih tinggi.



Gambar 5. Tahapan Implementasi Enkripsi

Berikut adalah penjelasan dari tahapan yang terdapat pada Gambar 5. Tahapan implementasi enkripsi di atas sebagai berikut :

a. **Input Data : Pesan**

   Tahap pertama dalam proses pengimplementasian adalah dengan menyisipkan pesan ke dalam gambar dan dimasukkan ke dalam sistem.

b. **Enkripsi : Vigenere Cipher**

   Tahap ini menunjukkan langkah di mana pesan yang dimasukkan di enkripsi menggunakan algoritma Vigenere Cipher

c. **Input Data : Gambar Untuk Steganografi**

Tahap ini menggambarkan langkah di mana gambar yang akan digunakan untuk menyembunyikan pesan dimasukkan ke dalam sistem.

d. **Steganografi LSB pada Gambar**

Tahap ini menunjukan langkah di mana pesan yang telah dienkripsi disisipkan ke dalam gambar menggunakan metode steganografi LSB.

e. **Output Data : Gambar dengan Pesan Terenkripsi**

Tahap ini menunjukkan output dari proses, yaitu gambar yang telah dimodifikasi dengan menyembunyikan pesan terenkripsi di dalamnya..

HASIL DAN PEMBAHASAN

Dalam tahap implementasi steganografi dan kriptografi, peneliti mengimplementasikan algoritma *Vigenere Cipher* untuk mengenkripsi pesan dan metode LSB steganografi untuk menyisipkan pesan terenkripsi ke dalam gambar. Berikut adalah potongan kode yang peneliti gunakan untuk melakukan enkripsi menggunakan *Vigenere Cipher* dan metode LSB:

```python
from PIL import Image

# Fungsi untuk mengenkripsi pesan menggunakan algoritma Vigenere Cipher
def vigenere_encrypt(plain_text, key):
    encrypted_text = ""
    key_index = 0
    for char in plain_text:
        # Jika karakter adalah huruf alfabet
        if char.isalpha():
            # Enkripsi karakter dengan menggeser sesuai kunci
            encrypted_char = chr((ord(char) + ord(key[key_index])) % 26 + ord('A'))
            encrypted_text += encrypted_char
            key_index = (key_index + 1) % len(key)
        else:
            # Jika karakter bukan huruf alfabet, biarkan tidak berubah
            encrypted_text += char
    return encrypted_text
```

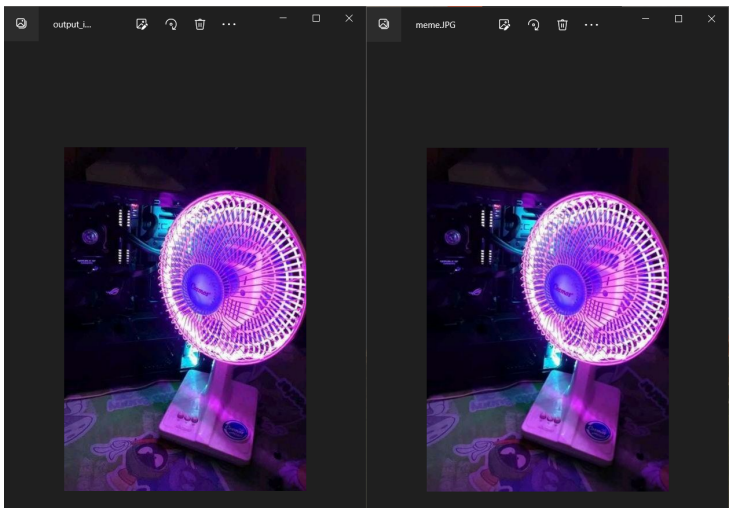
Gambar 6. Syntax 1

Syntax yang ditampilkan pada Gambar 6. Syntax 1 merupakan fungsi pengambilan pesan dan kunci, yang kemudian pesan tersebut di enkripsi menggunakan algoritma Vigenere Cipher. Setiap karakter pesan yang merupakan huruf alfabet akan digeser sesuai dengan karakter kunci yang sesuai

```python
# Fungsi untuk menyisipkan pesan ke dalam gambar menggunakan metode LSB steganografi
def embed_message(image_path, message):
    # Baca gambar
    img = Image.open(image_path)
    width, height = img.size

    # Enkripsi pesan menggunakan Vigenere Cipher
    key = "kuncirahasia"  # Kunci enkripsi
    encrypted_message = vigenere_encrypt(message.upper(), key)

    # Konversi pesan terenkripsi menjadi biner
    binary_message = ''.join(format(ord(char), '08b') for char in encrypted_message)

    # Periksa apakah pesan dapat disisipkan dalam gambar
    max_message_length = width * height * 3  # 3 karena 3 saluran warna (RGB)
    if len(binary_message) > max_message_length:
        raise ValueError("Pesan terlalu besar untuk disisipkan dalam gambar ini.")

    # Mulai menyisipkan pesan ke dalam gambar
    pixels = img.load()
    index = 0
    for y in range(height):
        for x in range(width):
            # Ubah nilai piksel menjadi tuple RGB
            r, g, b = pixels[x, y]

            # Sisipkan bit pesan ke bit LSB dari nilai piksel
            if index < len(binary_message):
                pixels[x, y] = (r & ~1 | int(binary_message[index]), g, b)
                index += 1
            else:
                break

    # Simpan gambar yang telah dimodifikasi
    output_image_path = "output_image.jpg"
    img.save(output_image_path)
    print("Pesan berhasil disisipkan ke dalam gambar:", output_image_path)
```

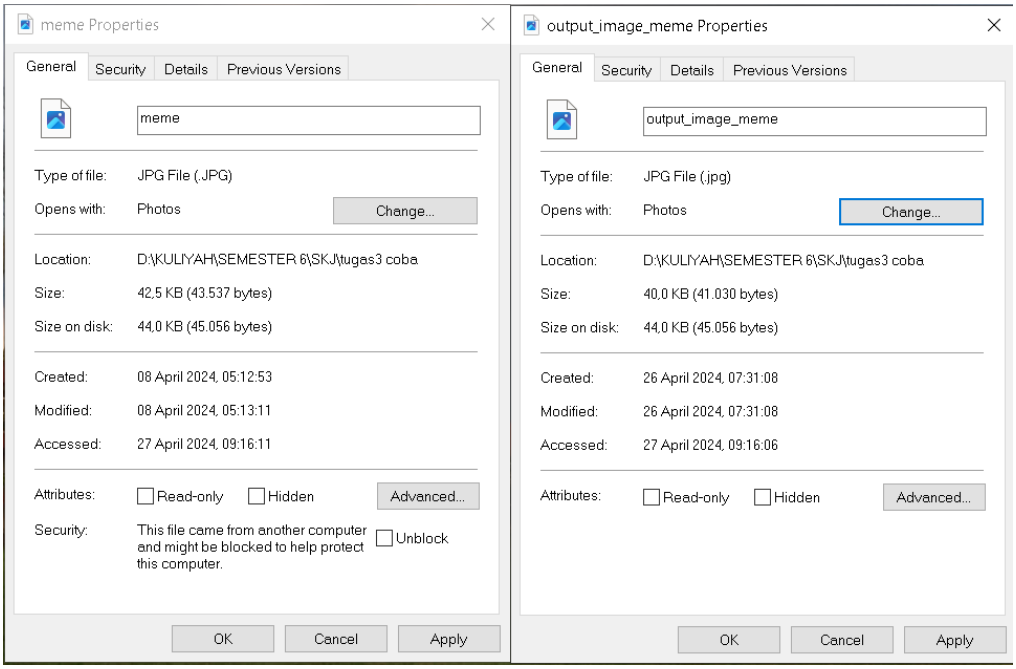
Gambar 7. Syntax 2

Pada syntax yang ditampilkan pada Gambar 7. Syntax 2 menjelaskan proses enkripsi, di mana fungsi '*embed_message'* adalah untuk membuka gambar sumber, serta proses enkripsi pesan yang akan disisipkan ke dalam gambar menggunakan algoritma *Vigenere Cipher*, dan kemudian menyisipkan pesan terenkripsi ke dalam piksel – piksel gambar menggunakan metode LSB steganografi. Setelah menyisipkan pesan, gambar yang dimodifikasi disimpan dalam file baru dengan format JPEG.



Gambar 8. Hasil Implementasi Enkripsi

Hasil dari pengimplementasian syntax sebelumnya ditunjukan pada Gambar 8. Hasil Implementasi enkripsi di atas, yang mana jika dilihat secara kasat mata kedua gambar tersebut terlihat sama, akan tetapi jika dilihat berdasarkan sizenya maka kedua gambar tersebut memilki perbedaan. Perbedaan antara kedua gambar tersebut ditunjukkan oleh Gambar 9. Perbedaan.



Gambar 9. Perbedaan

KESIMPULAN

Kesimpulan Dalam tahap implementasi steganografi dengan menggunakan algoritma *Vigenere Cipher* dan metode LSB pada gambar, penelitian ini berhasil menjalankan proses enkripsi pesan menggunakan *Vigenere Cipher* dan menyisipkan pesan terenkripsi ke dalam gambar menggunakan metode steganografi LSB. Hasil dari implementasi ini menunjukkan bahwa proses penyisipan pesan dilakukan tanpa menghasilkan distorsi visual yang signifikan pada gambar, sehingga gambar termodifikasi terlihat sama seperti gambar asli tanpa adanya tanda-tanda bahwa pesan telah disisipkan di dalamnya.

DAFTAR REFERENSI

Alawiyah, T., Ardianto, R., & Purnia, D. S. (2020). Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi Least Significant Bit. *Jurnal Informatika*, *7*(1), 37-45.

Cahyadi, T. (2012). Implementasi steganografi LSB dengan enkripsi vigenere cipher pada citra JPEG. *Transient: Jurnal Ilmiah Teknik Elektro*, *1*(4), 281-288.

Minarni, M., Ikram, A., Warman, I., & Swara, G. Y. (2023). Implementasi Algoritma Vigenere Cipher Dan End Of File Pada Steganografi Video. *Jurnal Minfo Polgan*, *12*(1), 432-441.

Ramadhani, N. A., & Susilawati, I. (2019). Penerapan Steganografi untuk Penyisipan Pesan Teks pada Citra Digital dengan Menggunakan Metode Least Significant Bit. *Jurnal Multimedia & Artificial Intelligence*, *4*(1), 21-27.

Utomo, Y. B., & Erwanto, D. (2019). Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor. *Generation Journal*, *3*(1), 16-22.

Wiryawan, I. G. (2019). Steganografi berdasarkan metode least significant bit (LSB) pada citra digital dengan Teknik kompresi lossless. Jurnal Ilmi Komputer Indonesia, *4*(1), 34-40.

Yusup, I. M., Carudin, C., & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. *Jurnal Teknik Informatika dan Sistem Informasi*, *6*(3).