e-ISSN: 2597-6559
p-ISSN: 2406-7741

Implementasi Least Significant Bit pada Citra Digital dengan Enkripsi Vigenère Cipher Berbasis Application Programming Interface

Vidia[1], Ade Lailani[2], Rohmi Dyah Astuti[3], Yuliana[4], Moh Arif Yahya[5]

[1,2,3,4] *Program Studi Sains Data, Fakultas Sains Institut Teknologi Sumatera Lampung Selatan, Lampung – Indonesia.*

[1]vidia@sd.itera.ac.id,

[2]ade.lailani@sd.itera.ac.id

[3]rohmi.astuti@sd.itera.ac.id

[4]yuliana@sd.itera.ac.id

[5] *Sekolah Tinggi Manajemen Informatika dan Komputer Cirebon, Indonesia*

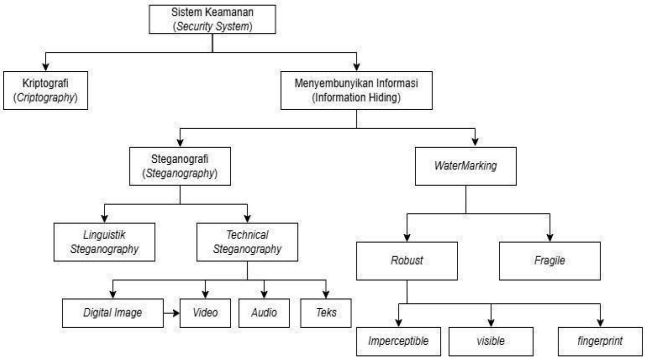
[5]*maarifyahya@gmail.com*

***Intisari*— Steganografi adalah teknik untuk menyembunyikan informasi dalam citra digital, dan salah satu metode yang digunakan adalah LSB (Least Significant Bit). Metode LSB menyisipkan bit terkecil ke dalam gambar digital, yang melibatkan dua algoritma utama, yaitu algoritma embedding dan ekstraksi. Untuk tahapan enkripsi, penelitian ini menggunakan sistem Vigenère cipher yang terdiri dari dua tahap yaitu enkripsi dan dekripsi. Penelitian ini mengintegrasikan metode steganografi dengan enkripsi menggunakan Vigenère cipher berbasis API. Tujuan dari integrasi ini adalah untuk menciptakan sistem yang tidak hanya menyembunyikan informasi dalam citra digital, tetapi juga melindungi informasi tersebut dari pihak yang tidak berhak mengaksesnya. Dengan menggunakan metode LSB, penelitian ini berhasil mempertahankan kualitas gambar yang digunakan, seperti yang terlihat pada metadata, di mana selisih ukuran file antara gambar asli dan gambar yang telah dienkripsi hanya sebesar 0,8 MB. Kata kunci:** Steganografi, LSB, Vigenère cipher, Citra Digital, API

***Abstract*—Steganography is a technique for hiding information within digital images, and one of the methods used is LSB (Least Significant Bit). The LSB method inserts the smallest bit into the digital image, involving two main algorithms: the embedding algorithm and the extraction algorithm. This research utilizes the Vigenère cipher system for the encryption process, which consists of two stages: encryption and decryption. This research integrates steganography with encryption using the Vigenère cipher based on an API. This integration aims to create a system that not only hides information within digital images but also protects that information from unauthorized access. Using the LSB method, this research successfully maintains the image quality, as seen in the metadata, where the file size difference between the original and the encrypted images is only 0.8 MB.**
Keywords: Steganography, LSB, Vigenère cipher, Digital Image, API.

I. PENDAHULUAN

Dalam bahasa yunani steganografi dapat diartikan dari dua kata yaitu *steganos* yang memiliki makna menutupi dan *graphia* yang dapat diartikan sebagai menulis. Jessica Fridrich pada tahun 2016 dalam bukunya mendefinisikan steganografi adalah teknik menyembunyikan informasi ke dalam objek atau gambar yang terlihat tidak berbahaya [1]. Teknik steganografi masuk ke dalam kategori sistem keamanan (sec*urity sistem*) yaitu pada bagian teknik menyembunyikan informasi yang dapat dilihat Gambar 1. Keamanan sistem steganografi meliputi gambar digital serta video, audio dan teks (Yahya, 2018)(Miftakhul Fahmi, Isnaini and Suhartono, 2023).

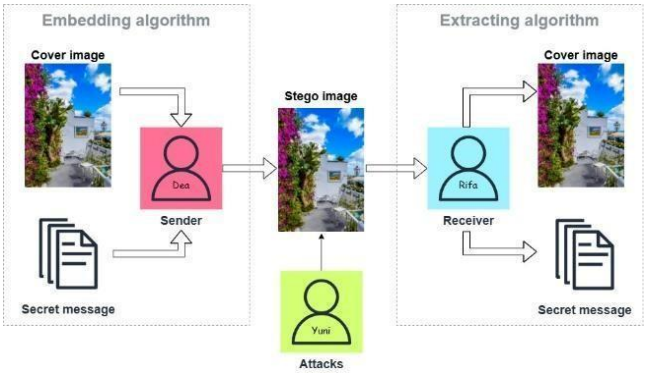


Gambar 1. Bagan Ilmu Sistem Keamanan

Citra digital adalah area dua dimensi yang menyimpan informasi penting dapat sebagai bukti kejahatan komputer, dengan risiko kehilangan atau kerusakan data (Lysander *et al.*, 2021)(Khairunnisak, Ashari and Kuncoro, 2020). Keamanan informasi sangat penting untuk dilindungi, dan salah satu cara yang dapat digunakan adalah steganografi. Saat ini, banyak

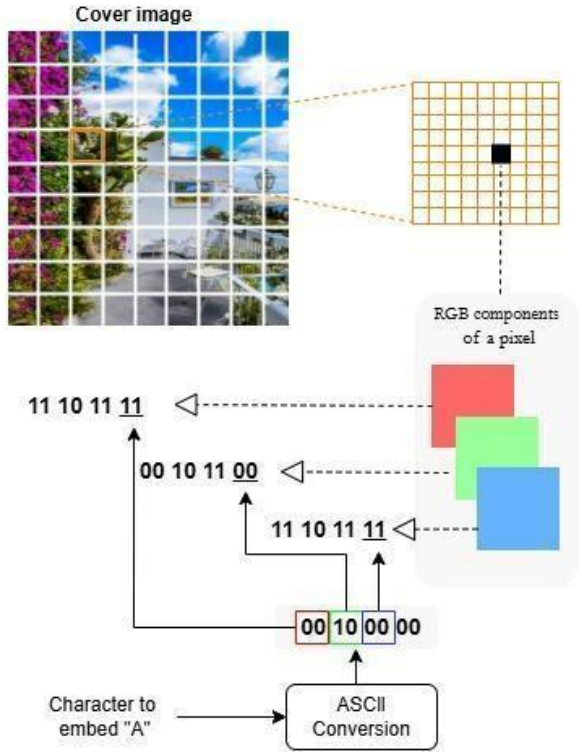
e-ISSN: 2597-6559
p-ISSN: 2406-7741

permasalahan terkait steganografi dan citra digital atau gambar, di mana steganografi memiliki sisi positif dalam membantu melindungi data rahasia (Hermansa, Umar dan Yudhana, 2020). Steganografi erat kaitannya dengan kriptografi, perbedaannya terletak pada pendekatannya. Kriptografi membuat data tidak dapat dibaca dan tidak dapat dipecahkan, meskipun teks sandi masih dapat dilihat oleh manusia. Sebaliknya, steganografi berfokus pada penyembunyian informasi rahasia sehingga tidak dapat dilihat oleh mata manusia dalam bentuk media tertentu. Salah satu media yang sering digunakan dalam steganografi adalah gambar atau citra digital (Akbar dan Haryanto, 2015). Secara sederhana steganografi terdiri dari beberapa tahapan umum dalam steganografi yaitu tahap pengcoveran biasanya terdiri dari algoritma menyembunyikan pesan (*embedding algorithm*) atau proses memasukan informasi ke dalam sebuah gambar atau dapat disebut gambar kover lalu gambar cover tersebut disisipi oleh informasi tersembunyi gambar dikirim kepada penerima lalu penerima menerima pesan yang telah disisipi oleh informasi tahap selanjutnya penerima melakukan proses ekstraksi menggunakan algoritma tertentu untuk mendapatkan informasi seutuhnya(Mahmoud Hassaballah, 2020).



Gambar 2. Gambaran Umum Steganografi.

Salah satu metode steganografi yang fundamental adalah metode *Least Significant Bit* (LSB) yang merupakan metode konvensional yang mampu menyembunyikan informasi kedalam sebuah gambar. Metode LSB ini memanfaatkan komponen kecil dalam gambar atau yang disebut bit, pada dasarnya LSB adalah teknik dengan merekayasa bit paling tidak signifikan, metode LSB ini masuk kedalam kategori steganografi untuk domain spasial yang melingkupi pixel maupun vertex dari citra gambar (Mahmoud Hassaballah, 2020).



Gambar 3. Mekanisme Menyembunyikan Informasi dalam Gambar Menggunakan Metode Lsb.

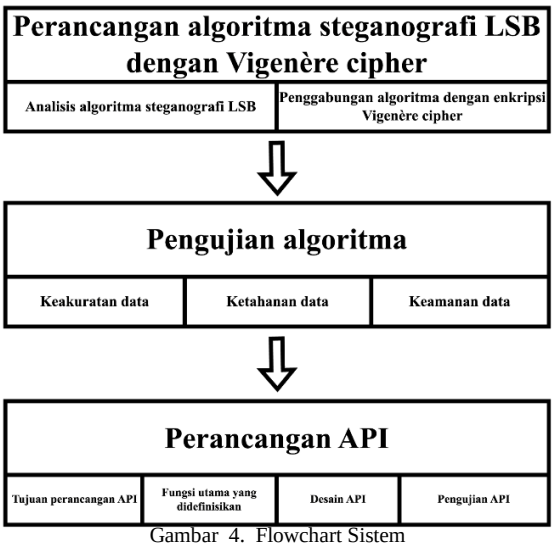
Metode LSB pada dasarnya mengganti bit dari gambar yang ditumpangi informasi dengan bit rahasia, penambahan bit rahasia ini dengan panjang yang sama dalam LSB piksel akan tetapi bit kemudian diubah dengan bit rahasia (Fridrich, 2009). Untuk membangun sistem yang lebih aman untuk menyembunyikan informasi kita gunakan metode enkripsi yaitu *Vigenère cipher* yang merupakan algoritma kriptografi dengan metode substitusi polialfabetik untuk mengenkripsi teks, algoritma ini mensubtitusi monoalfabetik terkait dengan pergeseran 0 sampai 25 dari 26 sandi caesar dengan setiap sandi dilambangkan dengan huruf kunci (Stallings, 2017). Penelitian ini dilakukan dengan mengkombinasi metode LSB untuk menyembunyikan informasi dan enkripsi *Vigenère cipher* dengan memanfaatkan media API yang merupakan antarmuka pemrograman aplikasi media dengan bentuk yang lebih sederhana dan dapat berinteraksi dengan media pembawa informasi yang beragam seperti gambar vidio bahkan gambar.

II. Metodologi Penelitian

Penelitian ini dimulai dengan perancangan algoritma steganografi *Least Significant Bit* (LSB) yang digabungkan dengan enkripsi *Vigenère cipher*. Steganografi LSB digunakan untuk menyisipkan data pada bit terkecil file digital, seperti gambar, sehingga perubahan tersebut tidak terlihat oleh mata manusia. *Vigenère cipher* diterapkan untuk mengenkripsi data sebelum disisipkan, meningkatkan keamanan informasi yang tersembunyi. Tahap perancangan ini melibatkan analisis

e-ISSN: 2597-6559
p-ISSN: 2406-7741

format file yang digunakan, pengembangan metode penyisipan data berbasis LSB, serta pengintegrasian proses enkripsi dengan *Vigenère cipher* agar algoritma dapat bekerja secara efisien dan aman.



Gambar 4. Flowchart Sistem

Tahap kedua adalah pengujian algoritma, yang bertujuan memastikan keandalan dan keamanan metode yang dirancang. Pengujian dilakukan untuk menilai keakuratan penyisipan dan ekstraksi data, ketahanan data terhadap perubahan pada file, efisiensi algoritma dalam hal waktu pemrosesan, serta tingkat keamanan terhadap upaya dekripsi yang tidak sah. Hasil pengujian ini digunakan untuk menyempurnakan algoritma sehingga dapat memenuhi kebutuhan praktis dan keamanan yang diinginkan.

Tahap terakhir adalah perancangan *Application Programming Interface* (API), yang berfungsi untuk mempermudah integrasi algoritma ke dalam aplikasi lain. Dalam tahap ini, fungsi utama seperti penyisipan data, ekstraksi data, serta enkripsi dan dekripsi didefinisikan secara jelas. Format input dan output API juga dirancang agar mudah digunakan oleh pengembang lain, dan protokol komunikasi ditentukan jika API akan digunakan secara online. Setelah dirancang, API ini diuji untuk memastikan setiap fungsi berjalan dengan baik dan dapat mendukung kebutuhan pengembangan aplikasi secara efektif.

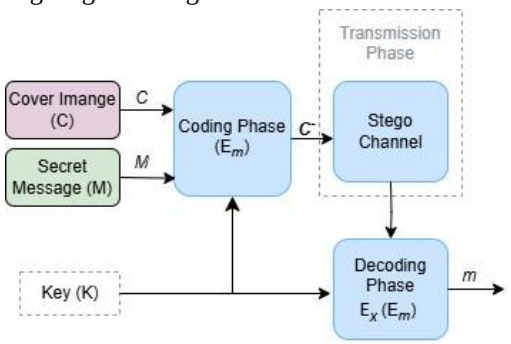
A. Steganografi

Metode steganografi gambar dikategorikan berdasarkan berbagai teknik sesuai dengan kategori penyembunyian yang digunakan dalam komunikasi rahasia. Atau, metode ini dilakukan dengan mengatur metode tersebut sesuai dengan kategori penyesuaian sampul yang sebelumnya digunakan selama prosedur penyisipan. Metode kedua diterapkan untuk klasifikasi yang ditawarkan dalam bab tiga, sementara, dalam beberapa keadaan, pengaturan yang tepat tidak mungkin dilakukan. Secara garis besar, prosedur grafis penyisipan dapat dijelaskan seperti yang disajikan dalam Gambar 2.3. Misalkan C mewakili pembawa sampul dan C~ menunjukkan gambar stego. Misalkan K mewakili benih yang digunakan untuk mengkodekan data atau menghasilkan derau pseudo-acak, yang dapat diatur ke {∅} untuk kesederhanaan, dan misalkan M mewakili data yang akan dikirim. Kemudian, EM dan EX masing-masing akan menunjukkan data yang disematkan dan diekstraksi (Stallings, 2017).

$$E_m : c \oplus K \rightarrow \tilde{C} \quad (1)$$

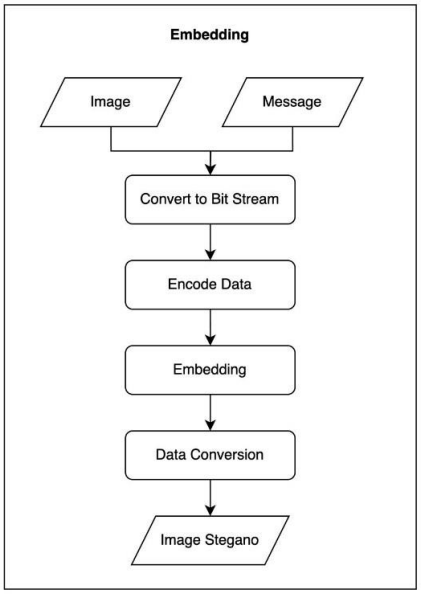
$$\therefore E_x(E_m(c, m, k) \approx m, \ \forall c \in C, \ m \in M, \ k \in K) \quad (2)$$

dari Persamaan (1) dan (2), kita dapat menggambarkan secara umum steganografi sebagai berikut:



Gambar 5. Metode Steganografi dengan Menggunakan Persamaan 1 dan 2

Pada proses ini, sesuai dengan Gambar 2, steganografi memiliki tahapan *embedding* dan *extraction*. Berikut adalah algoritma untuk proses *embedding* dengan lebih rinci.

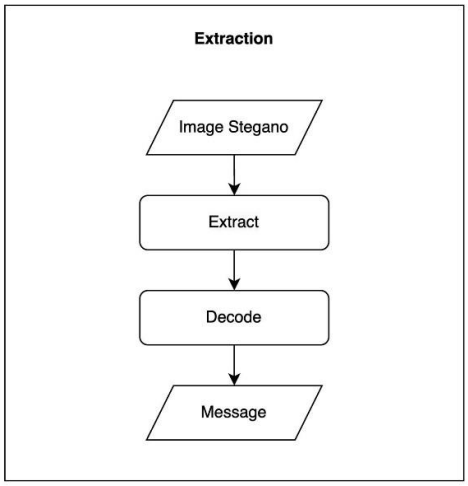


Gambar 6. Alur Embedding

Proses embedding dalam steganografi gambar terdiri dari menyembunyikan pesan rahasia ke dalam gambar. Pesan

e-ISSN: 2597-6559
p-ISSN: 2406-7741

dikonversi menjadi bit stream, kemudian dilakukan *encode* data dan disematkan ke dalam gambar menggunakan teknik seperti LSB. Hasil akhirnya adalah gambar stego (*image stegano*) yang tampak normal tetapi mengandung pesan tersembunyi, yang dapat diekstraksi kembali dengan algoritma atau kunci yang sesuai. Setelah pesan diterima penerima akan melakukan ekstraksi (*extraction*) dengan proses dibawah ini.



Gambar 7. Alur Ekstraksi

Proses ekstraksi dilakukan untuk mengambil kembali pesan tersembunyi dari gambar stego. Proses ini dimulai dengan gambar stego sebagai input, yaitu gambar yang mengandung pesan rahasia. Selanjutnya, data tersembunyi diekstraksi menggunakan metode yang sesuai dengan teknik embedding yang digunakan sebelumnya. Setelah data berhasil diambil, proses *decoding* dilakukan untuk mengubah data tersebut kembali ke bentuk aslinya, seperti teks atau informasi biner. Hasil akhir dari tahapan ini adalah pesan rahasia yang berhasil dipulihkan dari gambar stego.

B. Vigenére Cipher

Pada penelitian ini, penggunaan Vigenére cipher mengacu pada hitungan matematis dengan Persamaan (3) dan (4) berikut ini.

$$Ci \;\; E\,(Pi + Ki) \bmod 26 \qquad (3)$$

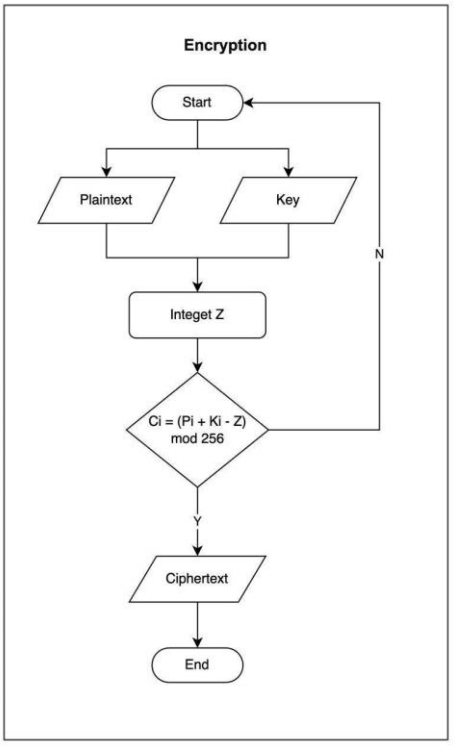
$$Pi = D(Ci\text{-}Ki) \bmod 26 \qquad (4)$$

C adalah chipertext, E merupakan fungsi enkripsi, K sebagai kunci dan P merupakan karakter dari plaintext serta D merupakan fungsi deskripsi. Teknik yang diterapkan di dalam enkripsi Vigenére cipher yaitu menambahkan pada setiap indeks karakter teks biasa ke indeks karakter dari kata sandi, enkripsi ini dapat digambarkan dengan menggunakan tabel kotak vigenere seperti Gambar 8.

	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 8. Tabel Kotak Vigenere

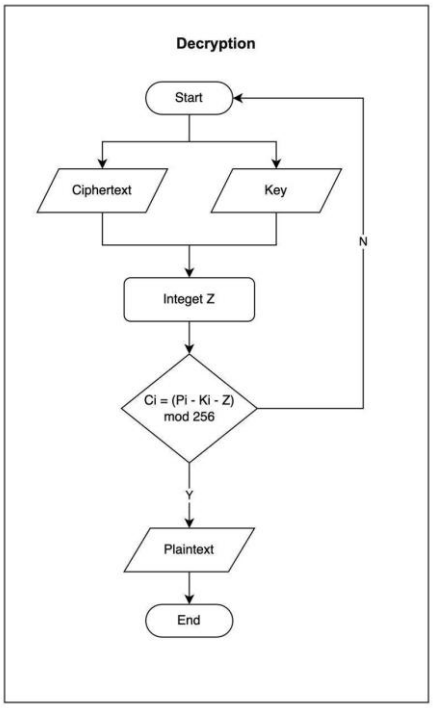
Dengan menggunakan Persamaan (3) kemudian tetapkan sebagai perumusan dari algoritma enkripsi (Maruf, Riadi and Prayudi, 2015), (Saputra; *et al.*, 2017), seperti pada Gambar (9).



Gambar 9. Alur Enkripsi

Persamaan (4) merupakan rumusan matematis untuk tahap deskripsi yang alurnya dapat dilihat pada Gambar 10.

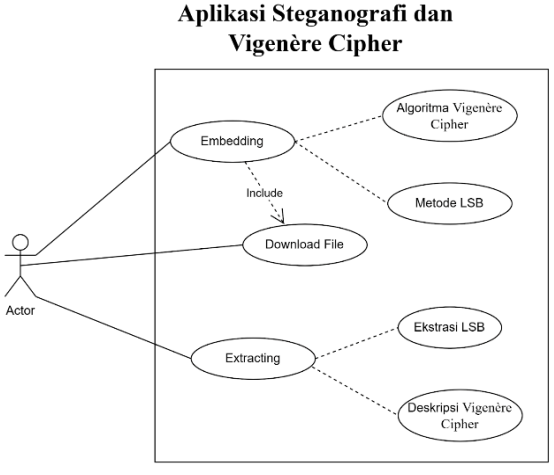
e-ISSN: 2597-6559
p-ISSN: 2406-7741



Gambar 10. Alur Deskripsi

III. Hasil dan Pembahasan

Pada penelitian ini, perancangan aplikasi steganografi yang mengkombinasikan algoritma Vigenere Cipher dan metode LSB diilustrasikan menggunakan UML. Pada penelitian ini terdapat satu aktor yang memiliki dua proses utama yaitu embedding dan extraction serta lima sub proses yang berkaitan dengan masing masing fungsi. *Use case* diagram pada penelitian ini ditunjukan pada Gambar 11.

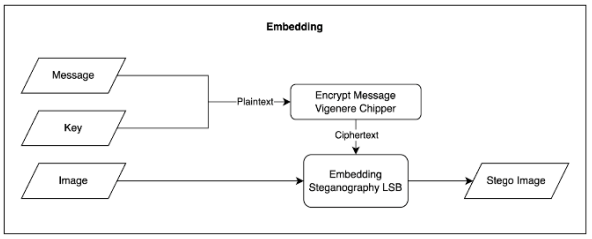


Gambar 11. *Use Case*

Diagram *use case* pada Gambar 11 merupakan alur kerja aplikasi steganografi yang dikombinasikan dengan algoritma *Vigenère cipher*. Dalam diagram ini, aktor (pengguna) dapat melakukan dua fungsi utama, yaitu embedding dan extracting. Pada proses embedding, pesan rahasia terlebih dahulu dienkripsi menggunakan algoritma *Vigenère Cipher*, kemudian disisipkan ke dalam gambar menggunakan metode LSB. Kemudian, pengguna memiliki opsi untuk mengunduh file hasil proses tersebut melalui fitur *Download File*. Sementara itu, pada proses extracting, pesan tersembunyi diekstraksi dari gambar stego melalui tahapan Ekstraksi LSB, kemudian didekripsi menggunakan deskripsi *Vigenère Cipher* untuk mengembalikan pesan ke bentuk aslinya. Diagram ini menunjukkan hubungan yang jelas antara proses utama dan fitur pendukung, seperti pengunduhan file, yang melibatkan teknik enkripsi dan steganografi untuk menjaga kerahasiaan data.

A. Perancangan Algoritma Steganografi LSB dan Vigenere Chiper

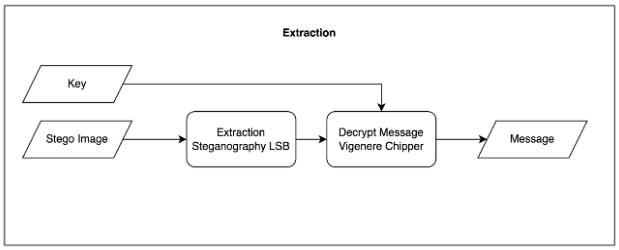
Dalam penelitian ini, file media yang digunakan untuk implementasi steganografi adalah gambar digital. Pemilihan gambar sebagai media didasarkan pada karakteristiknya yang memiliki ukuran data besar dan struktur piksel yang mendukung penyisipan informasi tanpa perubahan visual yang signifikan. Informasi rahasia terlebih berwenang. Pendekatan ini memungkinkan gambar berfungsi ganda, yaitu sebagai media visual biasa dan sebagai wadah data rahasia yang terenkripsi.



Gambar 12. Alur *Embedding*

Proses penyisipan (*embedding*) pada algoritma LSB dengan enkripsi Vigenère Cipher dimulai dengan mengenkripsi pesan rahasia menggunakan algoritma Vigenère. Pesan rahasia diubah ke dalam bentuk biner setelah dienkripsi menggunakan kunci tertentu. Setiap bit dari pesan terenkripsi ini kemudian disisipkan ke dalam *Least Significant Bit* (bit terakhir) dari komponen warna (*Red, Green, Blue*) pada setiap piksel gambar pembawa. Sebagai contoh, jika piksel awal memiliki nilai RGB (11001010, 10100100, 11101101) dan bit pesan terenkripsi adalah 0, maka komponen Blue diubah menjadi 11101100. Proses ini diulang hingga semua bit pesan terenkripsi disisipkan ke dalam gambar. Hasil akhirnya adalah gambar baru (stego image) yang tampak identik dengan gambar asli secara visual tetapi mengandung pesan rahasia terenkripsi di dalamnya.

e-ISSN: 2597-6559
p-ISSN: 2406-7741



Gambar 13. Alur *Extraction*

Proses ekstraksi (extraction) pada algoritma LSB dimulai dengan membaca gambar yang telah berisi pesan rahasia (stego image) dan mengekstrak Least Significant Bit (LSB) dari setiap komponen warna (Red, Green, Blue) pada setiap piksel secara berurutan. Bit-bit yang diekstrak ini kemudian disusun kembali menjadi sebuah bitstream lengkap. Setelah bitstream terbentuk, data biner ini dikonversi kembali menjadi teks atau format asli pesan. Hasil ekstraksi akan berupa teks terenkripsi yang kemudian dekripsi menggunakan kunci yang sama dengan kunci yang digunakan saat penyisipan. Hasil akhirnya adalah pesan rahasia asli yang berhasil dipulihkan.

A. Pengujian Algoritma

Perancangan algoritma steganografi dengan Vigenère cipher pada file media gambar yang sudah dibuat kemudian diuji untuk mengetahui keandalan, efisiensi, dan keamanan metode yang dirancang. Hasil dari proses enkripsi dan dekripsi steganografi dapat dilihat pada gambar berikut:

Gambar 14. Gambar Asli

Gambar 15 berikut adalah setelah hasil embedding.

Gambar 15. Gambar Sesudah Enkripsi

Hasil pada metadata gambar dapat dilihat metadata pada Tabel 1 berikut.

Tabel 1 Metadata

Metadata	Asli	Hasil Embedding
file name	images.png	image_c5973d0f-7bc7-4e7d-8f02-2b21a0f6a8de.png
file size	9.9 MB	8.7 MB
file type	PNG	PNG
image size	1881x2690	1881x2690
bit depth	8	8
megapixels	5.1	5.1

Perbedaan paling mencolok terletak pada ukuran gambar hasil embedding yang telah disisipi pesan. Ukurannya jauh lebih kecil dibandingkan gambar asli, meningkat lebih dari 0.8 MB.

B. Perancangan API

Perancangan aplikasi steganografi LSB dan *Vigenère Cipher* berbasis API dilakukan berdasarkan metode *RESTful API Design*, di mana setiap fitur dari aplikasi ini akan diimplementasikan sebagai layanan yang dapat diakses melalui endpoint HTTP yang jelas dan konsisten. Pada desain ini, setiap operasi (seperti penyisipan pesan dan ekstraksi pesan) akan diwakili oleh endpoint yang dapat dipanggil menggunakan metode HTTP standar seperti POST, GET, dan PUT. Berikut adalah Fitur Utama Aplikasi:

1. Hiding Message into Image

Endpoint : POST /api/hide
Parameter Body:

Tabel 2 Parameter Body Hiding Image

Parameter	Tipe	Deskripsi
image	File (PNG)	Gambar pembawa untuk menyisipkan pesan.
message	String	Pesan rahasia yang akan disisipkan.
key	String	Kunci enkripsi untuk mengenkripsi pesan.

Contoh Request:

```
> curl --location --request POST '127.0.0.1:3000/api/hide' \
--form 'image=@"/Users/marlfyahya/Desktop/images.png"' \
--form 'message="Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris mollis arcu eu tincidunt tincidunt. M
aecenas id enim laoreet, tincidunt augue vel, congue elit. Pellentesque justo nulla, finibus vitae ante vitae, malesua
da fermentum tellus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Etiam matt
is vehicula malesuada. Integer ac nunc vitae mi lacinia faucibus. Suspendisse sem magna, pretium sit amet neque at, te
mpor suscipit nulla. Mauris ultrices fringilla risus, quis blandit lectus consectetur semper. Aliquam blandit leo magn
a, sed cursus justo suscipit a. Ut egestas, risus quis varius tempus, ex erat pharetra enim, at dapibus augue quam qui
s velit. Phasellus porttitor, est tempus condimentum dignissim, ipsum ipsum tincidunt diam, vel convallis lacus mauris
 vitae leo. Morbi ut ultrices mi, ac sodales eros. Morbi ut eros at lacus hendrerit malesuada ac eget libero. Nam id i
nterdum sapien. Nam mauris lectus, luctus a consequat ac, finibus nec nibh."' \
--form 'key="secret"'
```

Gambar 16. *embedding request*

e-ISSN: 2597-6559
p-ISSN: 2406-7741

Pengguna (*User*) dapat mengirim *request* ke *endpoint hide* dengan parameter berupa *image*, *message*, *dan key*. Parameter *image* adalah file gambar dalam format Base64 yang akan digunakan sebagai media untuk menyisipkan pesan. Parameter *message* adalah teks rahasia yang ingin disembunyikan, sementara *key* adalah kunci yang digunakan untuk mengenkripsi pesan dengan algoritma *Vigenère cipher*.

Contoh Response:

Gambar 17.*embedding response*

Setelah menerima request, API akan mengenkripsi pesan menggunakan kunci yang diberikan dan kemudian menyisipkan hasil enkripsi ke dalam bit-bit terkecil dari gambar menggunakan metode steganografi LSB. Gambar baru yang telah berisi pesan rahasia kemudian dikembalikan kepada pengguna berupa url berisi gambar dengan pesan tersembunyi yang bisa diunduh melalui response API.

2. Extracting Message from Image

Endpoint : POST /api/reveal
Parameter Body:

Tabel 3 Parameter body

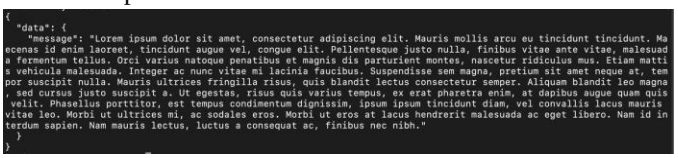
Parameter	*Tipe*	Deskripsi
image	*File (PNG)*	Gambar yang mengandung pesan rahasia.
key	*String*	Kunci dekripsi jika pesan terenkripsi.

Contoh Request:

Gambar 18. *extraction request*

Pada endpoint reveal, pengguna mengirimkan request dengan parameter image dan key. Parameter image berisi gambar dengan pesan tersembunyi dalam format Base64, sedangkan key adalah kunci yang digunakan untuk mendekripsi pesan.

Contoh Response:



Gambar 19. *extraction response*

API akan mengekstrak data terenkripsi dari gambar menggunakan teknik LSB dan mendekripsi data tersebut dengan algoritma Vigenère cipher menggunakan kunci yang diberikan. Jika proses berhasil, API akan mengembalikan pesan asli dalam response.

IV. KESIMPULAN

Dalam penelitian ini terdapat beberapa hal yang dijadikan rumusan permasalahan, yaitu bagaimana merancang sistem yang mengimplementasikan metode LSB dengan menggunakan *Vigenère cipher* berbasis API. Gambar 11 menunjukkan use case dari sistem yang dibangun, di mana terdapat satu aktor dengan dua proses utama. Proses pertama adalah *embedding* yang memiliki dua subproses, yakni penggunaan *Vigenère cipher* untuk mengenkripsi pesan sebelum disisipkan dan penggunaan metode LSB untuk menyisipkan informasi ke dalam gambar. Teknik LSB ini bekerja dengan menyisipkan bit terkecil pada gambar digital sehingga perbedaan antara gambar asli dan gambar setelah proses *embedding* tidak signifikan, seperti yang terlihat pada gambar 14 dan 15. Berdasarkan tabel metadata, perubahan hanya terlihat pada ukuran file dengan selisih sebesar 0,8 MB. Penelitian ini berfokus pada perancangan sistem yang dapat mengintegrasikan kedua metode tersebut untuk membangun sistem yang aman, efisien, dan efektif. Sistem ini tidak hanya berfungsi untuk menyembunyikan informasi tetapi juga mengamankan data melalui enkripsi Vigenère cipher, sehingga terhindar dari upaya dekripsi oleh pihak yang tidak berwenang, sambil tetap mempertahankan kualitas gambar digital.

Saran pengembangan lebih lanjut mencakup pengoptimalan algoritma *Vigenère cipher* dengan kunci yang lebih kompleks atau penambahan teknik enkripsi lain untuk meningkatkan keamanan. Selain itu, eksperimen dengan berbagai format gambar dan ukuran file perlu dilakukan untuk menguji efektivitas teknik LSB tanpa mengorbankan kualitas gambar .

REFERENSI

[1] Fridrich, J. (2009) *Steganography in Digital Media*, *Steganography in Digital Media*. Available at: https://doi.org/10.1017/cbo9781139192903.

[2] Hermansa, Umar, R. and Yudhana, A. (2020) 'Pangamanan Pesan Menggunakan Kriptografi', *Jurnal Sains Komputer & Matematika* , Vol 4, pp. 1–13.

[3] Khairunnisak, K., Ashari, H. and Kuncoro, A.P. (2020) 'Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist', *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, 3(2), pp. 72–81. Available at: https://doi.org/10.31598/jurnalresistor.v3i2.634.

[4] Lysander, K. *et al.* (2021) 'Pengamanan Citra Dengan Kombinasi Modified Serpent IWT Dengan Modified Logistic Chaotic Map', *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 8(3), pp. 1090–1104. Available at: https://doi.org/10.35957/jatisi.v8i3.1019.

[5] Mahmoud Hassaballah (ed.) (2020) *Digital Media Steganography*. 1st Editio. Qena, Egyp: Elsevier. Available at: https://doi.org/10.1016/C2018-0-04865-3.

[6] Maruf, F., Riadi, I. and Prayudi, Y. (2015) 'Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Documents', *International Journal of Computer Applications*, 132(1), pp. 27–33. Available at: https://doi.org/10.5120/ijca2015907262.

[7] Miftakhul Fahmi, G., Isnaini, K.N. and Suhartono, D. (2023)

e-ISSN: 2597-6559
p-ISSN: 2406-7741

'Implementation of Steganography on Digital Image With Modified Vigenere Cipher Algorithm and Least Significant Bit (Lsb) Method', *Jurnal Teknik Informatika (Jutif)*, 4(2), pp. 333–344. Available at: https://doi.org/10.52436/1.jutif.2023.4.2.340.

[8] Saputra;, I. *et al.* (2017) 'Vigenere Cipher Algorithm with Grayscale Image', 6(01), p. International Journal of Engineering Research & Te.

[9] Stallings, W. (2017) *Cryptography and Network Security: Principles and Practice 7th Global Edition*.

[10] Yahya, A. (2018) *Steganography techniques for digital images, Steganography Techniques for Digital Images*. Available at: https://doi.org/10.1007/978-3-319-78597-4.

[11] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[12] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[13] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.