Penerapan Teknik Steganografi LSB pada Format Gambar Modern

I Gusti Ngurah Febri Ananda Krisna[a1], AAIN Eka Karyawati[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]febrianandak552@gmail.com
[2]eka.karyawati@unud.ac.id

Abstract

As the digital era advances, protecting sensitive information becomes crucial. One approach used is the steganography technique, which involves hiding secret messages in plain-looking media. In this context, the LSB (Least Significant Bit) steganography technique emerged as a common choice, exploiting changes in the least significant bits of media such as images to hide secret messages. This research aims to analyze and apply LSB steganography techniques in modern image formats such as PNG, WEBp, JPEG, BMP, TIFF, HEIF, GIF, and SVG. Through implementation in the form of a computer program with the python programming language, this research evaluates the performance of the technique and makes it applicable in various real-world scenarios. It is hoped that this research can contribute to the development of more effective information security solutions and become the basis for further research in the field of steganography and information security as a whole. The results obtained from this research are that the encryption process of modern image formats has a success rate of 81.25% with an average successful sample encryption speed of 1.55 seconds. and the modern image format decryption process has a success rate of 81.25% with a text match rate of 69.23%.

Keywords: *Steganography,LSB,Python,Gambar,Format Gambar Modern*

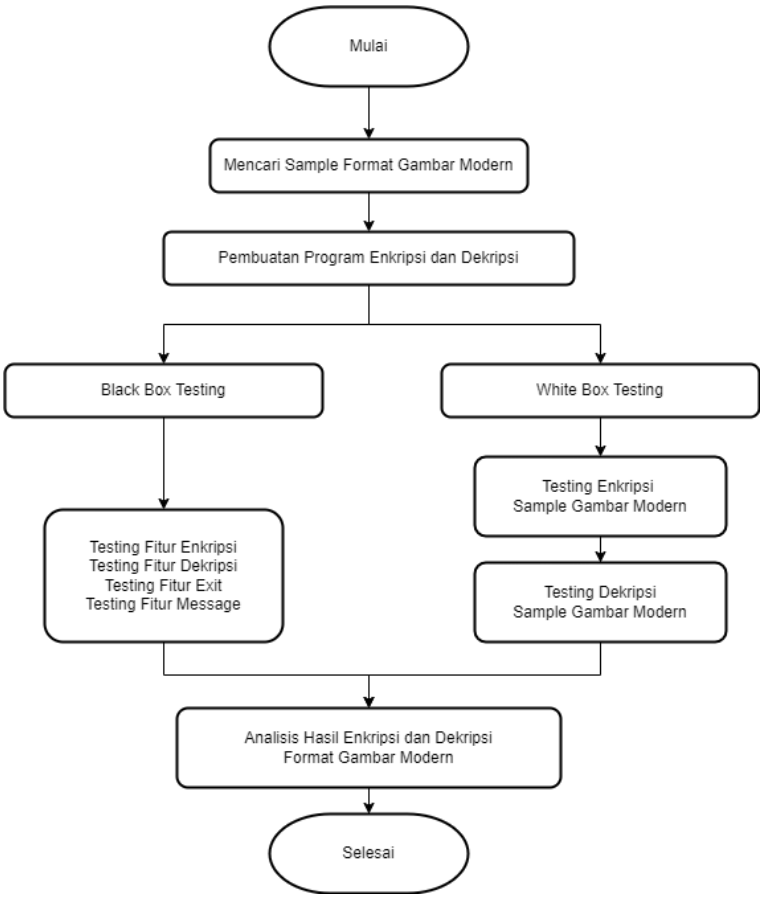
1. Pendahuluan

Di era digital yang semakin canggih, melindungi informasi sensitif menjadi semakin penting. Salah satu pendekatan untuk melindungi data sensitif adalah dengan menggunakan teknik steganografi. Steganografi adalah seni menyembunyikan pesan rahasia di media yang terlihat biasa saja sehingga hanya penerima pesan yang mengetahui keberadaan pesan tersebut [1]. Salah satu teknik steganografi yang paling umum digunakan adalah steganografi *LSB (Least Significant Bit)*, teknik Ini melibatkan perubahan bagian bawah judul media (seperti gambar) untuk menyembunyikan pesan rahasia [2]. Tujuan dari penelitian ini adalah untuk menganalisis dan menerapkan teknik steganografi *LSB (Least Significant Bit)* dalam format gambar modern, seperti Format gambar *JPEG (Joint Photographic Expert Group), PNG (Portable Network Graphics)*, *WebP, BMP, TIFF, HEIF, GIF,* dan *SVG* [3], dimana data dari penelitian ini didapat dari laman website https://file-examples.com/index.php/sample-images-download/. Selain itu, penelitian ini juga mengimplementasikan teknik tersebut kedalam bentuk program komputer untuk mengevaluasi kinerjanya dan menjadikannya dapat diterapkan pada berbagai skenario dunia nyata.Dengan memahami prinsip dasar teknik steganografi dan karakteristik format gambar modern, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan solusi keamanan informasi yang lebih kuat dan efektif serta hasil penelitian ini diharapkan dapat menjadi landasan bagi penelitian selanjutnya di bidang steganografi dan keamanan informasi secara keseluruhan.

2. Metode Penelitian

Metode yang digunakan pada penelitian ini menggunakan metode *Black box* dan *White Box* testing pada program metode enkripsi steganografi *LSB (Least Significant Bit)* pada format

gambar modern yaitu *JPEG (Joint Photographic Expert Group), PNG (Portable Network Graphics)*, *WebP, BMP, TIFF, HEIF, GIF,* dan *SVG.*



Gambar 1. Flowchart Metode Penelitian

2.1 Kajian Pustaka

a. Steganografi
Steganografi berasal dari bahasa Yunani *steganos* yang berarti “tersembunyi atau tertutup” dan *graph* berarti "tulisan", dimana Steganografi berarti ilmu yang mempelajari, meneliti, dan mengembangkan teknik untuk menyembunyikan informasi dan dapat digolongkan sebagai bagian dari ilmu komunikasi [5].

b. *LSB (Least Significant Bit)*
Least Significant Bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya di sebelah paling kiri [4].

Contohnya: Terdapat Sebuah bilangan Biner dari angka 255 yaitu 11111111 yang berarti *(1 + 2^7 + 1 + 2^6 + 1 + 2^5 + 1 + 2^4 + 1 + 2^3 + 1 + 2^2 + 1 + 2^1 + 1 + 2^0 =* ***128 + 64 + 32 + 16 + 8 + 4 + 2 + 1****)*. berdasarkan barisan angka 1 tersebut, dapat dilihat bahwa angka 1 paling kanan bernilai 1 yang mengartikan bahwa angka tersebut merupakan *LSB (Least Significant Bit)* atau bit yang paling tidak berarti. sedangkan angka 1 paling kiri bernilai 128 yang disebut sebagai *Most Significant Bit* atau bit yang paling berarti [2].

p-ISSN: 2986-3929
e-ISSN: 3032-1948

2.2 Analisis Kebutuhan

a. Kebutuhan non-Fungsional:

1. Hardware:
   - Intel(R) Core (TM) i5-1035G4
   - RAM 8 GB
   - HDD 500 GB

2. Software:
   - Windows 10
   - Visual Studio Code
   - Python

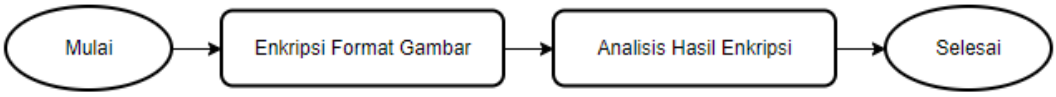
b. Kebutuhan Fungsional:

1. Kemampuan Enkripsi Format Gambar Modern
2. Kemampuan Dekripsi Format Gambar Modern

2.3 Rancangan Program

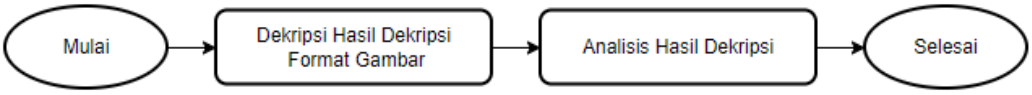
Program yang akan dibuat pada Penelitian menggunakan Aplikasi Visual Studio Code dengan bahasa pemrograman Python, yang kemudian akan dibagi menjadi 2 Rancangan yaitu enkripsi dan dekripsi:

a. Enkripsi: pada rancangan enkripsi, pertama akan dilakukan proses enkripsi dari format gambar modern, kemudian dilanjutkan dengan mengecek hasil enkripsi dari format gambar modern.



Gambar 2. Flowchart Enkripsi

b. Dekripsi: pada rancangan dekripsi, pertama akan dilakukan proses dekripsi dari enkripsi format gambar modern sebelumnya, kemudian dilanjutkan dengan mengecek hasil dekripsi dari format gambar modern.



Gambar 3. Flowchart Dekripsi

3. Hasil dan Diskusi

Program ini dibuat dengan Bahasa pemrograman Python untuk melakukan proses Enkripsi dan dekripsi format gambar modern dengan data sample seperti dibawah

Tabel 1. Tabel Data Sample Gambar

Data Sample	Format	Ukuran
png1	PNG	512 KB
png2	PNG	4,54 MB

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Data Sample	Format	Ukuran
png3	PNG	34,2 MB
bmp1	BMP	798 KB
bmp2	BMP	3,12 MB
bmp3	BMP	51,2 MB
jpeg1	JPEG	86,6 KB
jpeg2	JPEG	750 KB
jpeg3	JPEG	5,29 MB
tiff1	TIFF	799 KB
tiff2	TIFF	7,03 MB
tiff3	TIFF	51,2 MB
webp1	WEBP	10,2 KB
gif1	GIF	190 KB
heif1	HEIF	2,38 MB
svg1	SVG	117 KB

Tabel 1. diatas merupakan tabel data sample gambar yang akan digunakan pada program ini, berupa gambar dengan format dan ukuran yang berbeda-beda yaitu, format gambar PNG, BMP, JPEG, TIFF, WEBp, GIF, HEIF, dan SVG.

3.1. Penerapan Program

a. Blackbox Testing

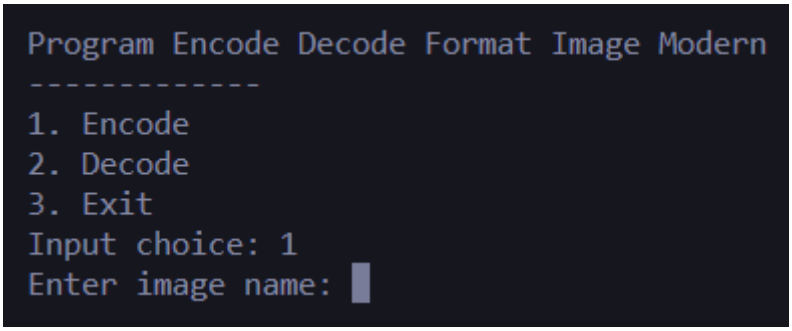
- Pengujian Program

Tabel 2. Tabel Testing Program

No	Modul	Berhasil	Gagal
1	Fitur Enkripsi	●	
2	Fitur Dekripsi	●	
3	Fitur Exit	●	
4	Error Message	●	
Total		4	0

Pada tabel 2 terlihat beberapa fitur program akan diujikan dengan menggunakan blackbox testing yaitu fitur Enkripsi, Dekripsi, Exit, dan Error Message

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 4. Tampilan Program

Pada Gambar 3 merupakan tampilan yang akan muncul saat program enkripsi dan dekripsi ini dijalankan, dimana terdapat fitur Encode/Enkripsi, Decode/Dekripsi, dan Exit yang digunakan untuk keluar dari program

b. White Box Testing

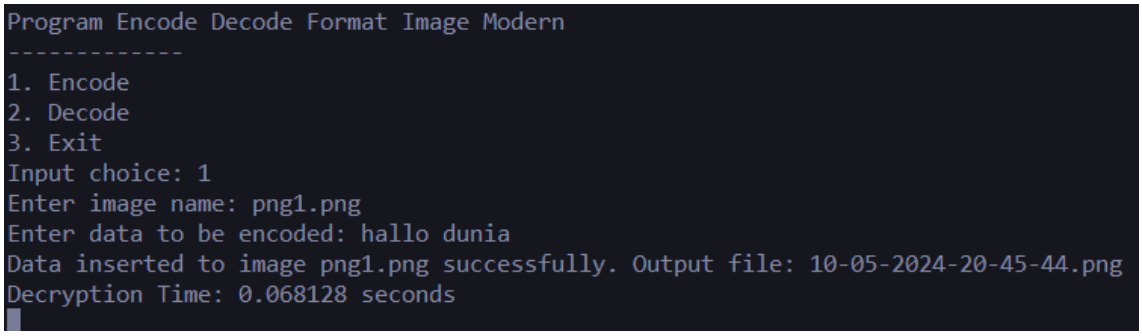
- Enkripsi

Tabel 3. Tabel Enkripsi Data Sample Gambar

No	Data Sample	Format	Ukuran	Berhasil	Gagal	Waktu Enkripsi	Text Yang Dienkripsi
1	png1	PNG	512 KB	●		0.068 detik	hallo dunia
2	png2	PNG	4,54 MB	●		0.594 detik	hallo bumi
3	png3	PNG	34,2 MB	●		4.510 detik	hallo dunia
4	bmp1	BMP	798 KB	●		0.061 detik	hallo teman
5	bmp2	BMP	3,12 MB	●		0.264 detik	hallo kawan
6	bmp3	BMP	51,2 MB	●		4.319 detik	hallo teman
7	jpeg1	JPEG	86,6 KB	●		0.066 detik	satu
8	jpeg2	JPEG	750 KB	●		0.572 detik	dua
9	jpeg3	JPEG	5,29 MB	●		4.487 detik	tiga
10	tiff1	TIFF	799 KB	●		0.077 detik	angin
11	tiff2	TIFF	7,03 MB	●		0.589 detik	udara
12	tiff3	TIFF	51,2 MB	●		4.521 detik	wind
13	webp1	WEBP	10,2 KB	●		0.018 detik	jakarta
14	gif1	GIF	190 KB		●	-	bandung
15	heif1	HEIF	2,38 MB		●	-	-
16	svg1	SVG	117 KB		●	-	-
Total Percobaan Enkripsi				**16**			
Total Sample Sukses				**13**			
Total Sample Gagal				**3**			
Presentase Sukses				**81.25%**			
Rata – Rata Kecepatan Enkripsi				**1,55 detik**			

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Pada tabel 3. diatas merupakan tabel hasil enkripsi dari setiap data sample gambar sebelumnya yang berisi sukses dan gagalnya sample dalam melakukan proses enkripsi, kecepatan enkripsi, dan pesan yang dimasukan kedalam sample gambar. Berdasarkan tabel diatas tingkat kesuksesan proses enkripsi pada data sample gambar adalah 81.25% dengan rata-rata tingkat kecepatan enkripsi sample yang berhasil adalah 1,55 detik dengan kecepatan enkripsi paling cepat adalah 0.061 detik



Gambar 5. Tampilan Enkripsi

Gambar 4. merupakan salah satu hasil enkripsi yang dilakukan pada sample gambar yaitu png1, dimana pada gambar diatas dapat dilihat pesan yang dimasukan serta kecepatan dalam proses enkripsinya

- Dekripsi

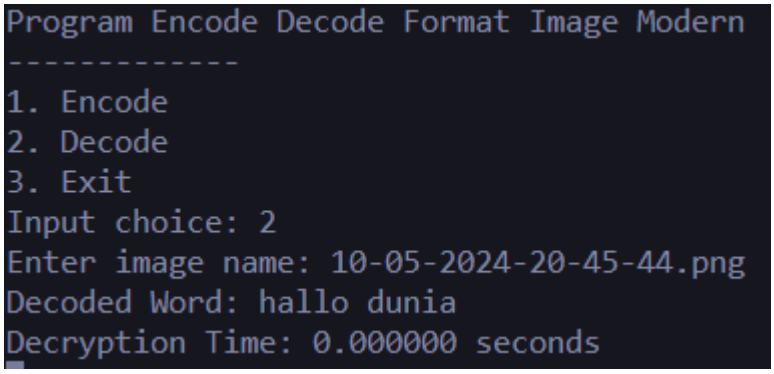
Tabel 4. Tabel Dekripsi Data Sample Gambar

No	Data Sample	Format	Ukuran	Berhasil	Gagal	Waktu Dekripsi	Kesesuaian Text
1	png1	PNG	512 KB	●		0 Detik	●
2	png2	PNG	4,54 MB	●		0 Detik	●
3	png3	PNG	34,2 MB	●		0 Detik	●
4	bmp1	BMP	798 KB	●		0 Detik	●
5	bmp2	BMP	3,12 MB	●		0 Detik	●
6	bmp3	BMP	51,2 MB	●		0 Detik	●
7	jpeg1	JPEG	86,6 KB	●		0 Detik	
8	jpeg2	JPEG	750 KB	●		0 Detik	
9	jpeg3	JPEG	5,29 MB	●		0 Detik	
10	tiff1	TIFF	799 KB	●		0 Detik	●
11	tiff2	TIFF	7,03 MB	●		0 Detik	●
12	tiff3	TIFF	51,2 MB	●		0 Detik	●
13	webp1	WEBP	10,2 KB	●		0 Detik	
14	gif1	GIF	190 KB		●	-	
15	heif1	HEIF	2,38 MB		●	-	
16	svg1	SVG	117 KB		●	-	
Total Percobaan Dekripsi				**16**			
Total Sample Sukses				**13**			

p-ISSN: 2986-3929
e-ISSN: 3032-1948

No	Data Sample	Format	Ukuran	Berhasil	Gagal	Waktu Dekripsi	Kesesuaian Text
Total Teks Dekripsi yang Sesuai				**9**			
Total Sample Gagal				**3**			
Tingkat Kesuksesan				**81.25%**			
Tingkat Kecocokan Teks				**69.23%**			

Tabel 4 diatas merupakan tabel hasil dekripsi dari setiap sample gambar. sama seperti proses enkripsi, tabel dekripsi ini juga memperlihatkan sukses dan gagalnya sample dalam melakukan proses dekripsi, kecepatan dekripsi, dan kesesuain pesan yang diinput pada proses enkripsi sebelumnya. Berdasarkan tabel diatas tingkat kesuksesan proses dekripsi pada data sample gambar adalah 81.25% dengan rata-rata tingkat kecepatan dekripsi sample yang berhasil adalah 0 detik dengan kecepatan enkripsi paling cepat adalah 0 detik, serta tingkat kecocokan teks yang di enkripsi sebelumnya adalah 69.23%



Gambar 6. Tampilan Dekripsi

Gambar diatas merupakan tampilan dari salah satu proses dekripsi sample gambar yaitu sample gambar png1, dimana dapat dilihat pesan yang terdapat dalam sample gambar serta waktu dekripsinya

4. Kesimpulan

Kesimpulan dari penelitian ini adalah bahwa penerapan teknik Steganografi *LSB (Least Significant Bit)* pada format gambar modern yang diterapkan menggunakan program Python dengan proses Enkripsi dan Dekripsi memberikan hasil sebagai berikut

a. Format Gambar *PNG, BMP, JPEG, TIFF,* dan *WEBp* sukses dalam melalui proses Enkripsi teks kedalam gambar menggunakan teknik Steganografi *LSB (Least Significant Bit),* dengan kecepatan enkripsi bervariasi tergantung dengan ukuran File. Sedangkan Format Gambar *GIF, HEIF,* dan *SVG* tidak sukses dalam melalui proses Enkripsi teks kedalam gambar menggunakan teknik Steganografi *LSB (Least Significant Bit*)
b. Format Gambar *PNG, BMP, JPEG, TIFF,* dan *WEBp* sukses dalam melalui proses dekripsi teks yang ada di dalam gambar menggunakan teknik Steganografi *LSB (Least Significant Bit)* dengan kecepatan yang sama pada ukuran file manapun, dimana Format Gambar *PNG, BMP,* dan *TIFF* memberikan output text yang sama dengan text yang dimasukan saat proses enkripsi tadi, sedangkan *JPEG,* dan *WEBp* tidak memberikan output text yang berbeda dengan text yang dimasukan saat proses enkripsi tadi. Sedangkan Format Gambar *GIF, HEIF,* dan *SVG* tidak sukses dalam melalui proses dekripsi menggunakan teknik Steganografi *LSB (Least Significant Bit*)
c. Tingkat kesuksesan proses enkripsi pada data sample gambar adalah 81.25% dengan rata-rata tingkat kecepatan enkripsi sample yang berhasil adalah 1,55 detik dengan kecepatan enkripsi paling cepat adalah 0.061 detik

d. Tingkat kesuksesan proses dekripsi pada data sample gambar adalah 81.25% dengan rata-rata tingkat kecepatan dekripsi sample yang berhasil adalah 0 detik dengan kecepatan enkripsi paling cepat adalah 0 detik, serta tingkat kecocokan teks yang di enkripsi sebelumnya adalah 69.23%

Daftar Pustaka

[1] Sasmal, Mr Milan, and Mrs Debasmita Mula. "An enhanced method for information hiding using LSB steganography." *Journal of Physics: Conference Series*. Vol. 1797. No. 1. IOP Publishing, February 2021.

[2] Hafiz, Aliy. Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendekia*, 2019, 17.1: 194-198.

[3] Ratnasari, Anita Putri, and Felix Andika Dwiyanto. "Metode steganografi citra digital." *Sains, Apl. Komputasi dan Teknol. Inf* 2.2 (2020): 52.

[4] Basri, Muh; Gushari, Muhammad Fadhlil. “Penerapan Steganografi Gambar Berwarna pada Delapan Image Cover Menggunakan Metode LSB”. *Jurnal Sintaks Logika*, 2021, 1.3: 153-158.

[5] Ramadhani, A. Muh; Hasanuddin, Tasrif. “Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography”. *Indonesian Journal of Data and Science*, 2021, 2.2: 91-102.