IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

DISUSUN OLEH

THEO HASRI PRATAMA

NPM. 2209010071



PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2026

IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

THEO HASRI PRATAMA
NPM. 2209010071

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026

LEMBAR PENGESAHAN

Judul Skripsi	:	IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL
Nama Mahasiswa	:	THEO HASRI PRATAMA
NPM	:	2209010071
Program Studi	:	SISTEM INFORMASI

Menyetujui

Komisi Pembimbing

(Wilda Rina Hasibuan, S.kom., M.kom)

NIDN. 0105017703

Ketua Program Studi	Dekan
(Mahardika Prawira Tanjung, S.Kom., M.Kom.)	**(Dr. Al-Khowarizmi, S.Kom., M.Kom.)**
NIDN. 0117088902	**NIDN. 0127099201**

PERNYATAAN ORISINALITAS

IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 14 Juni 2026

Yang membuat pernyataan



Theo Hasri Pratama

NPM. 2209010071

PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Theo Hasri Pratama
NPM	: 2209010071
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 14 Juni 2026

Yang membuat pernyataan

Theo Hasri Pratama

NPM. 2209010071

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Theo Hasri Pratama
Tempat dan Tanggal Lahir	: Medan, 13 Mei 2004
Alamat Rumah	: Jln Pasar 5 Tembung gg salak 48
Telepon/Faks/HP	: 085277300186
E-mail	: dio966214@gmail.com
Instansi Tempat Kerja	:
Alamat Kantor	:

DATA PENDIDIKAN

SD	: SD Negeri 010150 Petatal	TAMAT: 2016
SMP	: MTs AL Washliyah Petatal	TAMAT: 2019
SMA	: SMK Swasta Mandiri	TAMAT: 2022

KATA PENGANTAR



Puji Syukur dipanjatkan kehadiran Allah SWT berkat Rahmat, hidayah dan karunia-nya sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul **"IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL".** Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Penulis menyadari bahwa dalam penyusunan skripsi ini terwujud berkat bantuan, arahan, bimbingan, dan doa dari berbagai pihak. Oleh karena itu penulis menyampaikan terimakasih kepada:

1. Bapak Prof. Dr. Akrim, M.Pd., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Dr. Firahmi Rizky, S.Kom., M.Kom Wakil Dekan I Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU
4. Bapak Mhd. Basri, S.Si., M.Kom Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU
5. Bapak Mahardika Prawira Tanjung, S.Kom., M.Kom. Ketua Program Studi Sistem Informasi
6. Bapak Mulkan Azhari, S.Kom., M.Kom. Sekretaris Program Studi Sistem Informasi
7. Ibu Wilda Rina Hasibuan. S.Kom., M.Kom. selaku dosen pembimbing skripsi yang dengan penuh kesabaran dan perhatian membimbing penulis hingga sampai pada titik ini. Terima kasih telah percaya, membantu, membimbing, dan selalu mendorong penulis untuk terus berkembang.

8. Ibu Yoshida Sary, S.E., S.Kom., M.Kom. selaku dosen pembimbing akademik yang telah telah memberikan bimbingan selama penulis menempuh Pendidikan di perguruan tinggi.
9. Bapak Mahardika Prawira Tanjung, S.Kom., M.Kom. selaku dosen pembahas yang telah memberikan kritikan dan saran yang konstruktif demi kesempurnaan penulisan dan penyusunan proposal hingga skripsi.
10. Dosen beserta Staff Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara yang tidak dapat penulis sebut satu persatu karena telah memberikan banyak ilmu dan masukan kepada penulis.
11. Teristimewa kepada Almarhumah Ibunda Suhartini tercinta, yang senantiasa memberikan kasih sayang, doa, dukungan, nasihat, serta pengorbanan yang tidak pernah putus kepada penulis. Terima kasih atas segala cinta, perhatian, dan semangat yang telah diberikan sehingga penulis dapat menyelesaikan pendidikan dan penyusunan skripsi ini.
12. Kepada teman-teman seperjuangan yang telah memberikan dukungan, bantuan, motivasi, serta menjadi tempat berbagi cerita dan pengalaman selama masa perkuliahan hingga proses penyusunan skripsi ini. Terima kasih atas kebersamaan, semangat, dan kenangan yang telah diberikan kepada penulis.

IMPLEMENTASI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN PIXEL VALUE DIFFERENCING (PVD) DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

ABSTRAK

Steganografi merupakan teknik penyembunyian pesan ke dalam media digital untuk menjaga kerahasiaan informasi. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem steganografi citra digital menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam penyisipan pesan berupa *file* SQL. Sistem yang dikembangkan mampu melakukan proses *embedding*, *extraction*, deteksi metode steganografi, analisis kapasitas penyisipan, pengukuran kualitas citra menggunakan parameter PSNR dan MSE, serta pemeriksaan integritas pesan.

Pengujian dilakukan menggunakan 50 citra digital dengan *file* SQL sebagai pesan yang disisipkan. Hasil penelitian menunjukkan bahwa metode LSB memiliki tingkat keberhasilan yang lebih baik dalam menjaga integritas pesan, dimana seluruh *file* SQL hasil *extraction* berhasil dikembalikan sesuai dengan *file* asli. Sementara itu, metode PVD menghasilkan 32 *file* SQL yang sesuai dan 18 *file* mengalami perubahan. Berdasarkan nilai PSNR dan MSE, kedua metode mampu menghasilkan citra stego dengan kualitas visual yang baik. Secara keseluruhan, metode LSB lebih stabil dalam mempertahankan keutuhan pesan, sedangkan metode PVD tetap mampu menjaga kualitas visual citra stego.

Kata Kunci: Steganografi; *Least Significant Bit* (LSB); *Pixel Value Differencing* (PVD); Citra Digital; *File* SQL.

IMPLEMENTATION OF LEAST SIGNIFICANT BIT (LSB) AND PIXEL VALUE DIFFERENCING (PVD) METHODS FOR MESSAGE EMBEDDING IN DIGITAL IMAGES

ABSTRACT

Steganography is a technique for hiding messages within digital media to maintain information confidentiality. This study aims to design and implement a digital image steganography system using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods for embedding SQL files as secret messages. The developed system is capable of performing embedding and extraction processes, steganography method detection, embedding capacity analysis, image quality measurement using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) parameters, as well as message integrity verification.

The testing process was conducted using 50 digital images with SQL files as the embedded messages. The results showed that the LSB method had a better performance in maintaining message integrity, where all extracted SQL files were successfully recovered without any changes. Meanwhile, the PVD method produced 32 SQL files that matched the original files, while 18 files experienced changes after the extraction process. Based on the PSNR and MSE values, both methods were able to produce stego images with good visual quality. Overall, the LSB method was more stable in preserving message integrity, whereas the PVD method was still able to maintain good visual quality of the stego images.

Keywords: Steganography; Least Significant Bit (LSB); Pixel Value Differencing (PVD); Digital Images; SQL Files.

DAFTAR ISI

LEMBAR PENGESAHAN ii

PERNYATAAN ORISINALITAS iii

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS iv

RIWAYAT HIDUP v

KATA PENGANTAR vi

ABSTRAK viii

ABSTRACT ix

DAFTAR ISI x

DAFTAR TABEL xii

DAFTAR GAMBAR xiii

BAB I PENDAHULUAN 1

1.1. Latar Belakang Masalah 1

1.2. Rumusan Masalah 4

1.3. Batasan Masalah 5

1.4. Tujuan Penelitian 6

1.5. Manfaat Penelitian 6

BAB II LANDASAN TEORI 9

2.1. Steganografi 9

2.2. Citra Digital 12

2.3. Metode Least Significant Bit (LSB) 19

2.4. Metode Pixel Value Differencing (PVD) 26

BAB III ANALISA DAN PERANCANGAN SISTEM 33

3.1. Analisis Permasalahan 33

3.2. Algoritma Sistem 35

3.3. Flowchart Sistem.....41

3.4. Pemodelan dan Perancangan Sistem.....46

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 47

4.1. Kebutuhan Sistem 55

4.2. Implementasi Sistem.....59

4.3. Pengujian Sistem.....68

BAB V PENUTUP.....90

5.1. Kesimpulan 90

5.2. Saran.....91

DAFTAR PUSTAKA.....93

DAFTAR TABEL

Table 1. Hasil PSNR dan MSE 83

Table 2. Hasil Pengujian Integrasi Pesan.....88

DAFTAR GAMBAR

Gambar 1. Algoritma Proses Penyisipan Pesan (Embedding) 38
Gambar 2. Algoritma Proses Pengambilan Pesan (Extraction) 40
Gambar 3. Flowchart Embedding 44
Gambar 4. Flowchart Extraction 46
Gambar 5. Use Case Diagram 49
Gambar 6. activity diagram 51
Gambar 7. Perancangan antarmuka 53
Gambar 8. Halaman Home 61
Gambar 9. Halaman Awal Penyisipan 62
Gambar 10. Halaman Upload Data 63
Gambar 11. Analisis Citra dan kapasitas 63
Gambar 12. Hasil Penyisipan 64
Gambar 13. Halaman Awal Pengambilan Pesan 66
Gambar 14. Proses Extraction 67
Gambar 15. Hasil Proses Extraction 68
Gambar 16. Hasil Pengujian Satu Embedding LSB 71
Gambar 17. Hasil Pengujian Kedua Embedding LSB 72
Gambar 18. Hasil Pengujian satu Extraction SLB 73
Gambar 19. Hasil Pengujian Kedua Extraction LSB 74
Gambar 20. Hasil Pengujian Satu Embedding PVD 76
Gambar 21. Hasil Pengujian Kedua Embedding PVD 77
Gambar 22. Hasil Pengujian Satu Extraction PVD 79
Gambar 23. Hasil Pengujian Kedua Extraction PVD 80

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi pada era digital saat ini telah membawa perubahan yang sangat besar dalam berbagai aspek kehidupan manusia. Berbagai sektor seperti pendidikan, pemerintahan, dunia usaha, serta aktivitas sosial masyarakat semakin bergantung pada teknologi dalam proses pengelolaan dan penyebaran informasi. Kemajuan teknologi tersebut memungkinkan proses pengolahan, penyimpanan, serta distribusi data dilakukan dengan lebih cepat, efisien, dan dalam kapasitas yang jauh lebih besar dibandingkan sebelumnya. Informasi digital bahkan telah menjadi salah satu aset penting yang memiliki nilai strategis bagi individu maupun organisasi karena dapat digunakan sebagai dasar dalam pengambilan keputusan dan mendukung berbagai aktivitas operasional.

Dalam konteks keilmuan Sistem Informasi, data dan informasi merupakan dua komponen utama yang saling berkaitan dan tidak dapat dipisahkan. Sistem informasi berperan dalam mengelola data sehingga dapat diolah menjadi informasi yang memiliki nilai guna bagi penggunanya. Seiring dengan meningkatnya pemanfaatan teknologi informasi dalam berbagai aktivitas, kebutuhan terhadap keamanan dan perlindungan informasi juga menjadi semakin penting. Informasi yang tidak dikelola dengan baik berpotensi menimbulkan berbagai permasalahan, seperti kebocoran data, penyalahgunaan informasi, hingga gangguan terhadap aktivitas organisasi maupun individu.

Menurut Akmal dkk. (2023) pesatnya perkembangan teknologi informasi menyebabkan proses pertukaran data dapat dilakukan tanpa dibatasi oleh jarak maupun waktu, sehingga potensi terjadinya pencurian dan penyalahgunaan informasi menjadi semakin tinggi. Informasi digital yang dikirimkan melalui jaringan terbuka memiliki berbagai kerentanan terhadap ancaman keamanan, seperti penyadapan, perubahan data, maupun akses yang tidak sah oleh pihak yang tidak memiliki otoritas. Oleh karena itu, keamanan informasi menjadi salah satu aspek yang sangat penting dalam pengelolaan sistem informasi.

Salah satu pendekatan yang dapat digunakan untuk meningkatkan keamanan informasi adalah melalui teknik steganografi**.** Steganografi merupakan metode penyembunyian pesan rahasia ke dalam suatu media tertentu sehingga keberadaan pesan tersebut tidak diketahui oleh pihak lain. Menurut Lasarus (2021) teknik steganografi memungkinkan pesan rahasia disisipkan ke dalam berbagai jenis media digital seperti citra, audio, maupun video tanpa menimbulkan kecurigaan dari pihak yang melihat media tersebut. Dengan demikian, teknik ini tidak hanya berfungsi untuk melindungi isi pesan, tetapi juga menyamarkan keberadaan pesan yang disembunyikan.

Media yang dapat digunakan dalam steganografi sangat beragam, antara lain teks, audio, video, maupun citra digital. Di antara berbagai media tersebut, citra digital merupakan salah satu media yang paling banyak digunakan dalam proses penyisipan pesan rahasia. Hal ini disebabkan karena citra digital memiliki jumlah piksel yang besar serta memiliki *bit-bit* yang dapat dimodifikasi tanpa menimbulkan perubahan visual yang signifikan. Menurut Purbaningrum dkk.

(2023) karakteristik citra digital memungkinkan adanya manipulasi pada *bit* tertentu sehingga citra dapat dimanfaatkan secara efektif sebagai media untuk menyembunyikan informasi rahasia.

Dalam penerapan steganografi pada citra digital terdapat berbagai metode yang dapat digunakan untuk melakukan proses penyisipan pesan. Salah satu metode yang cukup sederhana dan banyak digunakan adalah *Least Significant Bit* (LSB). Metode ini bekerja dengan cara mengganti *bit* paling rendah dari setiap piksel citra dengan *bit* pesan yang akan disisipkan. Perubahan pada *bit* tersebut hanya memberikan pengaruh yang sangat kecil terhadap nilai piksel sehingga secara visual citra hasil penyisipan tetap terlihat hampir sama dengan citra aslinya.

Selain metode LSB, terdapat metode lain yang juga dapat digunakan dalam penyisipan pesan pada citra digital, yaitu *Pixel Value Differencing* (PVD). Metode ini memanfaatkan perbedaan nilai antara dua piksel yang berdekatan untuk menentukan jumlah *bit* pesan yang dapat disisipkan ke dalam citra. Menurut Gustiawan dkk. (2023), metode *Pixel Value Differencing* melakukan pembagian citra menjadi pasangan piksel yang kemudian dianalisis selisih nilainya sehingga kapasitas penyisipan pesan dapat disesuaikan dengan karakteristik piksel yang terdapat pada citra digital.

Berdasarkan berbagai metode steganografi yang telah dikembangkan, setiap metode memiliki karakteristik serta kelebihan masing-masing dalam proses penyisipan pesan pada citra digital. Oleh karena itu, diperlukan suatu implementasi metode yang dapat digunakan untuk menyembunyikan pesan pada

citra digital sekaligus melakukan analisis terhadap hasil penyisipan pesan yang dihasilkan oleh metode tersebut.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengimplementasikan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam proses penyisipan pesan pada citra digital. Selain itu, penelitian ini juga melakukan analisis terhadap hasil penyisipan pesan yang dihasilkan oleh kedua metode tersebut untuk mengetahui karakteristik serta kinerja masing-masing metode dalam proses steganografi citra digital.

Oleh karena itu, penelitian ini mengangkat judul "Implementasi Metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam Penyisipan Pesan pada Citra Digital" dengan harapan dapat memberikan kontribusi dalam bidang sistem informasi, khususnya dalam penerapan teknik steganografi sebagai salah satu alternatif metode pengamanan data digital.

1.2. Rumusan Masalah

1. Bagaimana merancang sistem steganografi menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) untuk penyisipan pesan pada citra digital?
2. Bagaimana mengimplementasikan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam proses penyisipan pesan pada citra digital?

3. Bagaimana pengujian metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam proses pengambilan kembali pesan pada citra digital?
4. Bagaimana penerapan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) terhadap kualitas citra digital dan keberhasilan penyisipan pesan?

1.3. Batasan Masalah

1. Penelitian ini berfokus pada penerapan teknik steganografi pada media citra digital dengan memanfaatkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) sebagai teknik dalam proses penyisipan pesan.
2. Media yang digunakan sebagai tempat penyisipan pesan dibatasi pada citra digital dalam bentuk *file* gambar dengan format PNG dan BMP, sedangkan pesan rahasia yang disisipkan berupa *file* dengan format .sql.
3. Tahapan yang dilakukan dalam penelitian ini meliputi proses penyisipan pesan (*embedding*) serta pengambilan kembali pesan (*extraction*) dengan menggunakan metode LSB dan PVD melalui aplikasi steganografi yang dikembangkan dalam penelitian ini.
4. Pengujian terhadap sistem yang dibuat dibatasi pada penampilan nilai kualitas citra digital setelah proses penyisipan pesan, yang diukur menggunakan parameter PSNR (Peak Signal to Noise Ratio) dan MSE (Mean Square Error) yang dihasilkan oleh sistem.

5. Penelitian ini tidak membahas aspek lain di luar sistem yang dirancang, seperti penerapan teknik kriptografi, watermarking, keamanan jaringan, maupun analisis steganalisis terhadap citra hasil penyisipan.

1.4. Tujuan Penelitian

1. Merancang sistem steganografi pada citra digital dengan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) sebagai teknik penyisipan pesan.
2. Mengimplementasikan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) pada proses penyisipan pesan (*embedding*) serta pengambilan kembali pesan (*extraction*) pada citra digital.
3. Mengetahui tingkat keberhasilan penerapan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) dalam menyisipkan dan mengekstraksi pesan rahasia berupa *file* berformat SQL pada citra digital.
4. Mengetahui kualitas citra digital setelah proses penyisipan pesan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) berdasarkan nilai Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE) yang dihasilkan oleh sistem.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari pelaksanaan penelitian ini adalah sebagai berikut:

1. Manfaat Bagi Kampus

   Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan di lingkungan perguruan tinggi, khususnya pada bidang Sistem Informasi. Hasil penelitian ini dapat dimanfaatkan sebagai tambahan referensi akademik yang membahas penerapan teknik steganografi pada citra digital dengan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Selain itu, penelitian ini juga diharapkan dapat menjadi bahan rujukan bagi mahasiswa maupun peneliti selanjutnya yang ingin mengkaji lebih lanjut mengenai keamanan informasi digital, terutama yang berkaitan dengan teknik penyembunyian pesan pada media citra digital.

2. Manfaat Bagi Penulis

   Penelitian ini memberikan manfaat bagi penulis dalam memperluas pengetahuan serta pemahaman mengenai penerapan teknik steganografi pada citra digital, khususnya melalui penggunaan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Selain itu, penelitian ini juga menjadi sarana bagi penulis untuk meningkatkan kemampuan dalam merancang dan mengembangkan aplikasi berbasis sistem informasi, sekaligus menerapkan teori yang telah dipelajari selama masa perkuliahan ke dalam bentuk implementasi sistem yang nyata.

3. Bagi Masyarakat

   Penelitian ini diharapkan dapat memberikan tambahan wawasan kepada masyarakat mengenai pentingnya menjaga keamanan dan kerahasiaan

informasi dalam bentuk digital. Melalui penerapan teknik steganografi pada citra digital dengan menggunakan metode LSB dan PVD**,** penelitian ini memberikan gambaran mengenai salah satu alternatif metode yang dapat digunakan untuk menyembunyikan pesan rahasia, sehingga informasi yang bersifat pribadi atau penting dapat disampaikan dengan lebih aman serta tidak mudah diketahui oleh pihak yang tidak memiliki kewenangan.

BAB II

LANDASAN TEORI

2.1. Steganografi

Steganografi merupakan teknik dalam bidang keamanan informasi yang digunakan untuk menyembunyikan keberadaan pesan rahasia ke dalam suatu media pembawa. Tujuan utama steganografi tidak hanya melindungi isi pesan, tetapi juga menyamarkan keberadaan pesan agar tidak menimbulkan kecurigaan dari pihak yang tidak berwenang. Istilah steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti tersembunyi dan *graphein* yang berarti menulis, sehingga steganografi dapat dimaknai sebagai teknik penulisan pesan secara tersembunyi.

Berbeda dengan metode pengamanan informasi yang berfokus pada perlindungan isi pesan, steganografi menitikberatkan pada penyembunyian pesan itu sendiri. Pesan rahasia disisipkan ke dalam media digital sedemikian rupa sehingga media tersebut tetap tampak normal dan tidak menunjukkan adanya informasi tersembunyi. Dengan pendekatan ini, steganografi memberikan lapisan keamanan tambahan karena keberadaan pesan tidak mudah disadari.

Menurut Akmal dkk. (2023) steganografi merupakan teknik penyisipan pesan rahasia ke dalam media digital dengan memanfaatkan karakteristik media sehingga perubahan yang terjadi tidak dapat dikenali oleh indera manusia. Media pembawa pesan disebut *cover media*, pesan yang disisipkan disebut *secret message* sedangkan media hasil penyisipan dikenal sebagai *stego media*. Hal ini

sejalan dengan pendapat Wanandi da Rezan (2024) yang menyatakan bahwa steganografi mampu menyembunyikan pesan tanpa menimbulkan perubahan visual yang signifikan.

Steganografi dapat diterapkan pada berbagai media digital, seperti teks, audio, video, dan citra digital. Namun, citra digital merupakan media yang paling banyak digunakan karena memiliki struktur data yang besar serta toleran terhadap perubahan kecil. Perubahan kecil pada nilai piksel citra umumnya tidak dapat dibedakan secara visual, sehingga citra digital sangat sesuai digunakan sebagai media penyisipan pesan rahasia Satria dan Jovi (2022).

Citra digital tersusun atas piksel-piksel yang direpresentasikan dalam bentuk data biner, sehingga memungkinkan manipulasi pada *bit* tertentu tanpa menurunkan kualitas visual citra secara signifikan. Dalam konteks sistem informasi, steganografi dapat diintegrasikan sebagai mekanisme pengamanan data digital dengan cara menyembunyikan pesan sebelum proses penyimpanan atau pengiriman data dilakukan.

Berdasarkan uraian tersebut, steganografi dapat disimpulkan sebagai teknik pengamanan informasi yang berfokus pada penyembunyian keberadaan pesan rahasia di dalam media digital. Teknik ini relevan diterapkan dalam sistem informasi, khususnya pada penyisipan pesan rahasia ke dalam citra digital yang menjadi fokus penelitian ini.

2.1.1. Perbedaan Steganografi dan Kriptografi

Steganografi dan kriptografi merupakan dua metode yang digunakan dalam pengamanan informasi, namun memiliki fokus dan tujuan yang berbeda. Menurut

Akmal dkk. (2023) kriptografi bertujuan untuk melindungi isi pesan dengan cara mengubah pesan asli ke dalam bentuk terenkripsi sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci dekripsi. Meskipun demikian, pesan yang telah dienkripsi masih dapat dikenali keberadaannya secara langsung. Sebaliknya, Wanandi dan Reza (2024) menyatakan bahwa steganografi lebih menekankan pada upaya menyembunyikan keberadaan pesan itu sendiri. Pesan rahasia disisipkan ke dalam suatu media pembawa sedemikian rupa sehingga media tersebut tetap tampak normal dan tidak menunjukkan adanya informasi tersembunyi. Dengan pendekatan ini, pihak lain tidak hanya kesulitan membaca isi pesan, tetapi juga tidak menyadari keberadaan pesan rahasia.

Dalam implementasinya, steganografi dan kriptografi dapat digunakan secara bersamaan untuk meningkatkan keamanan informasi. Kriptografi berperan dalam menjaga kerahasiaan isi pesan, sedangkan steganografi berfungsi untuk menyamarkan keberadaan pesan. Kombinasi kedua teknik tersebut dapat memberikan tingkat perlindungan yang lebih baik dalam sistem informasi yang menangani data bersifat rahasia.

2.1.2. Steganografi Pada Citra Digital

Steganografi dapat diterapkan pada berbagai media digital, seperti teks, audio, video, dan citra digital. Di antara media tersebut, citra digital merupakan media yang paling banyak digunakan karena memiliki struktur data yang besar dan toleran terhadap perubahan kecil. Menurut Satria dan Jovi (2022) karakteristik ini memungkinkan penyisipan pesan rahasia tanpa menimbulkan perubahan visual yang signifikan.

Citra digital tersusun atas piksel-piksel yang menyimpan informasi warna dalam bentuk data biner. Representasi biner ini memungkinkan dilakukan manipulasi pada *bit* tertentu dengan dampak yang sangat kecil terhadap tampilan citra. Dalam penerapannya, pesan rahasia disisipkan ke dalam nilai piksel citra melalui modifikasi pada representasi binernya. Perubahan yang dilakukan bersifat minimal sehingga citra hasil penyisipan tetap tampak serupa dengan citra asli. Oleh karena itu, steganografi pada citra digital dinilai efektif dalam menyamarkan keberadaan pesan rahasia dan relevan diterapkan sebagai mekanisme pengamanan data dalam sistem informasi.

2.2. Citra Digital

Citra digital merupakan bentuk representasi visual dari suatu objek yang disimpan serta diolah dalam bentuk data digital menggunakan perangkat komputer. Dalam bidang sistem informasi, citra digital tidak hanya digunakan sebagai media penyampaian informasi visual, tetapi juga sebagai data yang dapat disimpan, diolah, dan dimanfaatkan untuk berbagai keperluan, termasuk dalam mendukung aspek keamanan informasi. Oleh karena itu, pemahaman mengenai citra digital menjadi sangat penting, terutama dalam penelitian yang memanfaatkan citra sebagai media untuk penyisipan pesan rahasia.

Menurut Suhada dkk. (2024), citra digital terdiri atas sekumpulan piksel, di mana setiap piksel memiliki nilai tertentu yang direpresentasikan dalam bentuk data biner. Kumpulan piksel tersebut membentuk suatu citra yang dapat ditampilkan, disimpan, dan diproses oleh sistem komputer sesuai kebutuhan.

Representasi dalam bentuk digital ini memungkinkan citra untuk dimodifikasi secara matematis maupun logis tanpa memberikan perubahan visual yang signifikan.

Selanjutnya, Lasarus (2021) menjelaskan bahwa citra digital dapat direpresentasikan sebagai matriks dua dimensi yang tersusun atas baris dan kolom piksel. Setiap elemen pada matriks tersebut menunjukkan posisi serta nilai piksel tertentu, sehingga citra dapat diproses secara komputasional melalui manipulasi nilai piksel yang ada.

Dalam penerapan steganografi, citra digital memiliki karakteristik yang mendukung proses penyisipan pesan rahasia. Hal ini dikarenakan citra digital memiliki tingkat redundansi data yang cukup tinggi, sehingga perubahan kecil pada nilai piksel tidak memberikan dampak yang signifikan terhadap kualitas visual citra. Dengan karakteristik tersebut, citra digital menjadi media yang sesuai untuk menyembunyikan pesan secara tersembunyi.

Selain itu, citra digital banyak digunakan dalam sistem informasi berbasis multimedia, seperti dokumentasi, arsip digital, maupun pertukaran informasi visual. Penggunaannya yang luas dalam kehidupan sehari-hari membuat citra digital tidak menimbulkan kecurigaan ketika dijadikan sebagai media pembawa pesan rahasia, sehingga dapat meningkatkan efektivitas penerapan steganografi.

Citra digital disimpan dalam bentuk representasi biner, di mana setiap nilai piksel terdiri dari deretan *bit* dengan bobot tertentu. Representasi ini memungkinkan manipulasi pada *bit-bit* tertentu tanpa menyebabkan perubahan

nilai piksel secara signifikan. Karakteristik tersebut menjadi dasar dalam penerapan teknik steganografi pada citra digital.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa citra digital merupakan data visual yang memiliki struktur dan karakteristik yang mendukung proses penyisipan pesan rahasia. Oleh karena itu, pemahaman mengenai citra digital menjadi landasan penting sebelum membahas struktur citra digital serta metode steganografi yang digunakan dalam penelitian ini.

2.2.1. Struktur Citra Digital

Struktur citra digital menjelaskan bagaimana suatu citra direpresentasikan, disusun, dan disimpan dalam sistem komputer. Pemahaman terhadap struktur ini menjadi hal yang penting dalam proses pengolahan citra, terutama pada penelitian yang memanfaatkan citra sebagai media penyisipan pesan rahasia. Seluruh tahapan pengolahan citra, baik dalam proses penyisipan maupun pengambilan kembali pesan, sangat bergantung pada struktur data yang membentuk citra tersebut.

Suhada dkk. (2024) menjelaskan bahwa citra digital tersusun atas elemen-elemen dasar yang disebut piksel (picture element), yaitu unit terkecil yang berfungsi menyimpan informasi visual pada posisi tertentu. Setiap piksel merepresentasikan nilai intensitas cahaya atau warna, dan kumpulan piksel tersebut membentuk tampilan visual citra secara keseluruhan. Piksel-piksel ini merupakan komponen utama dalam pembentukan citra digital pada sistem komputer.

Pendapat tersebut diperkuat oleh Lasarus (2021) yang menyatakan bahwa citra digital direpresentasikan dalam bentuk matriks dua dimensi yang terdiri atas baris dan kolom piksel. Setiap piksel memiliki posisi spasial tertentu dalam matriks, sementara nilainya menyimpan informasi visual yang dapat diproses secara komputasional. Representasi ini memungkinkan setiap piksel diakses dan dimodifikasi secara individual dalam proses pengolahan citra.

Selain susunan piksel dan bentuk representasi matriks, struktur citra digital juga dipengaruhi oleh resolusi citra. Resolusi menunjukkan jumlah piksel yang menyusun citra secara horizontal dan vertikal. Suhada dkk. (2024) menjelaskan bahwa citra dengan resolusi yang lebih tinggi memiliki jumlah piksel yang lebih banyak, sehingga mampu menampilkan detail visual yang lebih baik serta menyediakan kapasitas data yang lebih besar dalam proses pengolahan citra.

Dalam kaitannya dengan steganografi, struktur citra digital berkaitan erat dengan penyimpanan nilai piksel dalam bentuk data biner. Dewi dan Munir (2023) menjelaskan bahwa setiap nilai piksel direpresentasikan sebagai deretan *bit* yang memiliki bobot tertentu. Representasi biner ini memungkinkan perubahan pada *bit-bit* tertentu tanpa menimbulkan perubahan visual yang signifikan pada citra.

Dewi dan Munir (2023) juga menegaskan bahwa karakteristik citra digital yang tersusun atas banyak piksel serta memiliki toleransi terhadap perubahan kecil menjadikannya sesuai digunakan sebagai media steganografi. Perubahan pada *bit* dengan bobot rendah umumnya tidak dapat dibedakan secara kasat mata antara citra asli dan citra hasil penyisipan pesan.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa struktur citra digital mencakup susunan piksel, representasi matriks dua dimensi, resolusi citra, serta representasi biner dari nilai piksel. Pemahaman terhadap struktur ini menjadi dasar penting dalam penerapan steganografi, karena proses penyisipan pesan memanfaatkan karakteristik *bit* pada piksel citra. Oleh karena itu, pembahasan selanjutnya akan diarahkan pada model warna citra digital yang berperan dalam representasi nilai piksel dan proses penyisipan pesan.

2.2.2. Model Warna Citra Digital

Model warna citra digital merupakan metode yang digunakan untuk merepresentasikan informasi warna pada setiap piksel dalam sebuah citra. Model warna menentukan bagaimana nilai warna disimpan, diolah, dan ditampilkan oleh sistem komputer. Dalam pengolahan citra digital serta penerapan steganografi, pemahaman terhadap model warna menjadi penting karena proses penyisipan pesan dilakukan berdasarkan nilai piksel yang dibentuk oleh model warna tertentu.

Dewi dan Munir (2023) menjelaskan bahwa citra digital umumnya direpresentasikan menggunakan model warna RGB (Red, Green, Blue), di mana setiap piksel tersusun atas tiga komponen warna utama, yaitu merah, hijau, dan biru. Setiap komponen warna memiliki nilai intensitas tersendiri yang disimpan dalam bentuk data biner. Kombinasi ketiga komponen tersebut menghasilkan berbagai variasi warna yang dapat ditampilkan pada citra digital.

Pada model warna RGB, setiap kanal warna umumnya direpresentasikan menggunakan 8 *bit*, sehingga satu piksel memiliki kedalaman warna sebesar 24

bit. Dewi dan Munir (2023) menyatakan bahwa struktur ini memungkinkan sebuah piksel memiliki banyak kemungkinan variasi warna. Selain itu, kedalaman warna 24 *bit* juga menyediakan ruang yang cukup untuk melakukan manipulasi pada *bit-bit* tertentu tanpa menimbulkan perubahan visual yang mencolok.

Selain model warna RGB, citra digital juga dapat direpresentasikan dalam bentuk citra keabuan (*grayscale*). Suhada dkk. (2024) menjelaskan bahwa citra *grayscale* hanya memiliki satu kanal intensitas yang menunjukkan tingkat keabuan, mulai dari warna hitam hingga putih. Setiap piksel pada citra *grayscale* menyimpan satu nilai intensitas, sehingga struktur datanya lebih sederhana dibandingkan dengan citra berwarna.

Model warna *grayscale* sering digunakan dalam pengolahan citra karena lebih mudah dianalisis dan dimanipulasi. Meskipun hanya memiliki satu kanal, citra *grayscale* tetap direpresentasikan dalam bentuk data biner. Hal ini memungkinkan proses penyisipan pesan dilakukan pada *bit-bit* tertentu dari nilai intensitas piksel, sehingga citra *grayscale* juga dapat dimanfaatkan sebagai media steganografi sesuai dengan kebutuhan sistem.

Suhada dkk. (2024) juga menyatakan bahwa representasi warna pada citra digital, baik dalam bentuk RGB maupun *grayscale*, merupakan komponen penting dalam pengolahan data visual pada sistem komputer. Model warna menentukan cara penyimpanan nilai piksel dan memengaruhi teknik manipulasi data yang dapat diterapkan. Pemilihan model warna yang tepat dapat mendukung proses pengolahan citra secara efisien tanpa menurunkan kualitas tampilan visual.

Dalam kaitannya dengan steganografi, model warna citra digital berperan langsung dalam menentukan lokasi serta mekanisme penyisipan pesan rahasia. Nilai biner yang terdapat pada setiap kanal warna maupun tingkat keabuan menjadi media utama dalam proses manipulasi *bit* untuk menyisipkan pesan. Oleh karena itu, pemahaman mengenai model warna citra digital menjadi dasar penting sebelum membahas metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD).

Berdasarkan uraian tersebut, dapat disimpulkan bahwa model warna citra digital, seperti RGB dan *grayscale*, merupakan aspek fundamental dalam representasi dan pengolahan citra. Model warna menentukan struktur nilai piksel yang selanjutnya dimanfaatkan dalam teknik steganografi. Dengan demikian, pemahaman mengenai model warna ini menjadi penghubung antara struktur citra digital dan penerapan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) pada subbab berikutnya.

2.2.3. Format *File* Citra Digital

Format *file* citra digital merupakan cara penyimpanan data citra dalam bentuk berkas yang dapat dibaca serta diproses oleh sistem komputer. Format ini menentukan bagaimana informasi piksel, model warna, serta metode kompresi disusun dan disimpan di dalam suatu *file*. Dalam proses pengolahan citra digital, khususnya pada penerapan steganografi, pemahaman terhadap format *file* menjadi hal yang penting karena berpengaruh terhadap kualitas citra, ukuran *file*, serta keberhasilan dalam proses penyisipan dan pengambilan kembali pesan rahasia.

Menurut Dewi dan Munir (2023), format *file* citra digital pada umumnya dibedakan menjadi dua kategori, yaitu format tanpa kehilangan data (*lossless*) dan format dengan kehilangan data (*lossy*). Perbedaan karakteristik antara kedua jenis format tersebut memengaruhi kestabilan nilai piksel, yang merupakan aspek penting dalam penerapan teknik steganografi.

Format citra *lossless,* seperti BMP (*Bitmap*) dan PNG (*Portable Network Graphics*), mampu menjaga nilai piksel tetap utuh. Pada format BMP, data piksel disimpan tanpa melalui proses kompresi sehingga kualitas citra tetap terjaga, meskipun ukuran *file* relatif lebih besar. Sementara itu, format PNG menggunakan kompresi tanpa kehilangan data, sehingga ukuran *file* menjadi lebih efisien tanpa mengubah nilai piksel yang ada.

Sebaliknya, format citra dengan kompresi *lossy*, seperti JPEG atau JPG (*Joint Photographic Experts Group*), melakukan pengurangan data untuk memperkecil ukuran *file*. Proses ini menyebabkan perubahan pada nilai piksel yang dapat memengaruhi kestabilan data citra. Menurut Firdaus dan Rahmatulloh (2025), kompresi *lossy* berpotensi merusak informasi yang disisipkan karena adanya perubahan pada struktur data piksel.

Dalam penerapan steganografi, kestabilan nilai piksel menjadi faktor yang sangat penting karena proses penyisipan pesan dilakukan dengan memanfaatkan nilai atau *bit* pada piksel citra. Oleh karena itu, format citra *lossless* lebih disarankan dibandingkan format *lossy*, karena mampu menjaga keutuhan data sehingga pesan rahasia tetap dapat dipertahankan dan diekstraksi kembali dengan baik. Berdasarkan uraian tersebut, dapat disimpulkan bahwa format *file* citra

digital memiliki peranan penting dalam keberhasilan penerapan steganografi. Format *lossless* seperti BMP dan PNG lebih direkomendasikan karena mampu menjaga kestabilan nilai piksel, sehingga mendukung proses penyisipan serta pengambilan kembali pesan rahasia secara optimal.

2.3. Metode Least Significant Bit (LSB)

Metode *Least Significant Bit* (LSB) merupakan salah satu teknik steganografi yang paling umum digunakan pada citra digital. Metode ini bekerja dengan memanfaatkan *bit* dengan bobot terendah pada nilai piksel citra sebagai media penyisipan pesan rahasia. Penggunaan *bit* paling tidak signifikan dipilih karena perubahan pada *bit* tersebut hanya menyebabkan perbedaan nilai piksel yang sangat kecil, sehingga tidak menimbulkan perubahan visual yang dapat dikenali pada citra hasil penyisipan.

Menurut Purbaningrum dkk. (2023) metode LSB memanfaatkan representasi biner citra digital yang tersusun atas *bit-bit* dengan bobot yang berbeda. *Bit* dengan bobot terendah memiliki pengaruh paling kecil terhadap nilai piksel, sehingga dapat dimodifikasi tanpa mudah terdeteksi oleh penglihatan manusia. Karakteristik ini menjadikan metode LSB banyak diterapkan dalam proses penyisipan pesan rahasia pada citra digital.

Lasarus (2021) menyatakan bahwa metode *Least Significant Bit* (LSB) termasuk teknik steganografi yang sederhana dan mudah diimplementasikan. Proses penyisipan pesan dilakukan dengan mengganti *bit* paling tidak signifikan pada nilai piksel citra dengan *bit* pesan rahasia. Meskipun menggunakan

mekanisme yang sederhana, metode LSB mampu menghasilkan citra stego yang memiliki tingkat kemiripan visual yang tinggi dengan citra asli, sehingga keberadaan pesan rahasia sulit dikenali secara kasat mata.

Dalam penerapannya, metode LSB umumnya digunakan pada citra digital dengan model warna RGB, di mana setiap piksel terdiri atas tiga kanal warna, yaitu merah (Red), hijau (Green), dan biru (Blue). Setiap kanal warna direpresentasikan dalam bentuk data biner, sehingga memungkinkan proses penyisipan pesan dilakukan pada *bit* paling tidak signifikan dari masing-masing kanal. Pendekatan ini dapat meningkatkan kapasitas penyisipan pesan tanpa menurunkan kualitas visual citra secara signifikan.

Secara umum, metode *Least Significant Bit* (LSB) terdiri atas dua tahapan utama, yaitu proses penyisipan pesan (*embedding*) dan proses pengambilan kembali pesan (*extraction*). Kedua tahapan tersebut saling berkaitan dan menjadi bagian penting dalam sistem steganografi citra digital. Pembahasan lebih lanjut mengenai masing-masing proses akan dijelaskan pada subbab berikutnya.

2.3.1. Proses Penyisipan Pesan (*Embedding*) Metode LSB

Proses penyisipan pesan atau *embedding* merupakan tahapan awal dalam penerapan metode *Least Significant Bit* (LSB). Pada tahap ini, pesan rahasia yang akan dimasukkan ke dalam citra terlebih dahulu diubah ke dalam bentuk data biner. Pengubahan pesan ke bentuk biner dilakukan karena teknik LSB bekerja dengan memanipulasi *bit-bit* tertentu pada nilai piksel citra digital.

Menurut Lasarus (2021) proses *embedding* pada metode LSB dilakukan dengan mengganti *bit* paling tidak signifikan pada nilai piksel citra dengan *bit*

pesan rahasia secara berurutan. Penyisipan pesan dimulai dari piksel awal dan dilanjutkan ke piksel berikutnya hingga seluruh *bit* pesan berhasil dimasukkan. Karena modifikasi hanya dilakukan pada *bit* dengan bobot terendah, perbedaan antara citra asli dan citra hasil penyisipan umumnya tidak menimbulkan perubahan visual yang dapat dikenali.

Pada citra digital berwarna dengan model warna RGB, proses *embedding* dapat diterapkan pada satu atau beberapa kanal warna, yaitu merah (Red), hijau (Green), dan biru (Blue). Setiap kanal warna direpresentasikan dalam bentuk data biner, sehingga masing-masing kanal dapat digunakan untuk menyisipkan satu *bit* pesan rahasia. Pemanfaatan lebih dari satu kanal warna dalam satu piksel memungkinkan peningkatan kapasitas penyisipan pesan tanpa menurunkan kualitas visual citra secara signifikan.

Purbaningrum dkk. (2023) menjelaskan bahwa keberhasilan proses *embedding* sangat dipengaruhi oleh ukuran citra digital dan panjang pesan rahasia yang disisipkan. Citra dengan resolusi yang lebih tinggi memiliki jumlah piksel yang lebih banyak, sehingga menyediakan kapasitas penyisipan pesan yang lebih besar. Oleh karena itu, diperlukan kesesuaian antara ukuran citra dan panjang pesan agar proses penyisipan dapat berlangsung secara optimal tanpa melampaui kapasitas citra.

Hasil dari proses *embedding* adalah citra stego, yaitu citra digital yang secara visual tampak serupa dengan citra asli, namun telah mengandung pesan rahasia di dalamnya. Citra stego tersebut selanjutnya dapat disimpan atau

dikirimkan sebagai media penyampaian pesan rahasia tanpa menimbulkan kecurigaan dari pihak yang tidak mengetahui adanya proses penyisipan pesan.

2.3.2. Proses Pengambilan Pesan (*Extraction*) Metode LSB

Proses pengambilan pesan atau *extraction* merupakan tahapan yang dilakukan untuk memperoleh kembali pesan rahasia yang telah disisipkan ke dalam citra stego menggunakan metode *Least Significant Bit* (LSB). Pada tahap ini, sistem membaca kembali *bit* dengan bobot terendah pada nilai piksel citra stego sesuai dengan mekanisme penyisipan pesan yang telah diterapkan sebelumnya. Agar pesan dapat diekstraksi secara tepat, proses *extraction* harus mengikuti urutan piksel dan parameter yang sama seperti pada saat proses *embedding.*

Lasarus (2021) menjelaskan bahwa mekanisme *extraction* pada metode LSB dilakukan dengan menelusuri setiap piksel pada citra stego dan mengambil *bit* paling tidak signifikan dari nilai piksel tersebut. *Bit-bit* hasil pembacaan kemudian disusun kembali secara berurutan hingga membentuk rangkaian data biner yang merepresentasikan pesan rahasia. Selanjutnya, rangkaian data biner tersebut dikonversi kembali ke dalam bentuk pesan aslinya.

Pada citra digital dengan model warna RGB, proses *extraction* dilakukan dengan membaca *bit* paling tidak signifikan dari masing-masing kanal warna, yaitu merah (Red), hijau (Green), dan biru (Blue), sesuai dengan kanal yang digunakan pada proses *embedding*. Konsistensi dalam pemilihan kanal warna serta urutan piksel menjadi faktor penting agar pesan yang diperoleh dari proses *extraction* sesuai dengan pesan yang telah disisipkan.

Purbaningrum dkk. (2023) menjelaskan bahwa keberhasilan proses *extraction* sangat dipengaruhi oleh kondisi citra stego. Selama citra stego tidak mengalami perubahan, seperti kompresi ulang, perubahan ukuran, atau manipulasi piksel lainnya, pesan rahasia umumnya dapat diekstraksi dengan baik. Hal ini menunjukkan bahwa metode LSB memiliki ketergantungan yang tinggi terhadap kestabilan nilai piksel citra.

Proses *extraction* pada metode LSB tergolong sederhana dan tidak memerlukan perhitungan yang kompleks. Kelebihan ini menjadikan metode LSB mudah diimplementasikan dalam sistem informasi yang membutuhkan kecepatan dan efisiensi dalam pengolahan data. Namun demikian, kesederhanaan tersebut juga menjadi salah satu keterbatasan metode LSB, karena pesan rahasia berpotensi rusak apabila citra stego mengalami perubahan.

Dengan demikian, proses pengambilan pesan (*extraction*) merupakan tahapan akhir dalam metode *Least Significant Bit* (LSB) yang bertujuan untuk mengembalikan pesan rahasia dari citra stego. Keberhasilan proses ini sangat ditentukan oleh kesesuaian mekanisme *embedding* serta kondisi citra stego yang digunakan.

2.3.3. Kelebihan dan Keterbatasan Metode *Least Significant Bit* (LSB)

Metode *Least Significant Bit* (LSB) merupakan salah satu teknik steganografi pada citra digital yang banyak digunakan karena memiliki sejumlah keunggulan. Salah satu kelebihan utamanya terletak pada kemudahan dalam proses penerapannya. Proses penyisipan dan pengambilan pesan dilakukan dengan memodifikasi *bit* dengan bobot paling rendah pada nilai piksel, sehingga tidak

membutuhkan proses perhitungan yang kompleks. Hal ini menjadikan metode LSB mudah diimplementasikan pada sistem yang memerlukan proses penyisipan pesan secara cepat dan efisien.

Selain itu, metode LSB juga memiliki keunggulan dalam menjaga kualitas visual citra. Menurut Hakim dan Sholikhan (2024), penggunaan metode LSB mampu menghasilkan citra stego yang memiliki tingkat kemiripan yang tinggi dengan citra asli. Hal tersebut dapat dilihat dari nilai PSNR yang tinggi serta nilai MSE yang rendah, yang menunjukkan bahwa perubahan akibat penyisipan pesan tidak memberikan pengaruh yang signifikan terhadap tampilan visual citra.

Keunggulan lainnya adalah tingkat keberhasilan dalam proses ekstraksi pesan yang cukup tinggi, selama citra stego tidak mengalami perubahan. Hakim dan Sholikhan (2024) menyatakan bahwa pesan rahasia yang disisipkan menggunakan metode LSB dapat dikembalikan dengan baik apabila proses *embedding* dan *extraction* dilakukan secara konsisten serta citra stego tetap dalam kondisi asli. Oleh karena itu, metode ini efektif digunakan pada media citra yang tidak mengalami manipulasi lanjutan.

Di sisi lain, metode *Least Significant Bit* (LSB) juga memiliki beberapa keterbatasan. Menurut Satria dan Jovi (2022), metode ini memiliki tingkat ketahanan yang rendah terhadap perubahan pada citra stego. Proses seperti kompresi ulang, perubahan ukuran citra, maupun manipulasi piksel dapat menyebabkan pesan rahasia menjadi rusak atau tidak dapat diekstraksi secara sempurna. Hal tersebut disebabkan karena metode LSB sangat bergantung pada kestabilan nilai *bit* pada piksel citra. Oleh karena itu, metode ini lebih sesuai

digunakan pada citra stego yang tidak mengalami proses modifikasi setelah penyisipan pesan dilakukan.

Selain itu, metode LSB juga memiliki keterbatasan dari aspek keamanan. Pola penyisipan yang relatif sederhana membuat metode ini lebih mudah dianalisis apabila keberadaan pesan tersembunyi telah diketahui. Satria dan Jovi (2022), menyatakan bahwa metode LSB belum dirancang untuk menghadapi serangan steganalisis secara intensif, sehingga tingkat keamanannya masih tergolong terbatas apabila digunakan tanpa mekanisme perlindungan tambahan.

Berdasarkan kelebihan dan keterbatasan tersebut, dapat disimpulkan bahwa metode *Least Significant Bit* (LSB) sesuai digunakan pada sistem steganografi citra digital yang mengutamakan kemudahan implementasi, efisiensi proses, serta kualitas visual citra. Namun demikian, metode ini kurang optimal diterapkan pada kondisi yang rentan terhadap manipulasi citra atau serangan steganalisis, sehingga penggunaannya perlu disesuaikan dengan kebutuhan sistem yang akan dibangun.

2.4. Metode Pixel Value Differencing (PVD)

Metode *Pixel Value Differencing* (PVD) merupakan salah satu teknik dalam steganografi citra digital yang digunakan untuk menyisipkan pesan rahasia dengan memanfaatkan perbedaan nilai antara piksel-piksel yang berdekatan. Metode ini bekerja dengan cara menghitung selisih nilai dari dua piksel yang bertetangga, kemudian menggunakan nilai tersebut untuk menentukan jumlah *bit* pesan yang dapat disisipkan ke dalam citra. Dengan pendekatan ini, proses penyisipan pesan

dapat dilakukan secara adaptif sesuai dengan karakteristik masing-masing bagian citra.

Menurut Gustiawan dkk. (2023), metode PVD dilakukan dengan membagi citra digital ke dalam pasangan piksel yang saling berdekatan. Selanjutnya, selisih nilai antara kedua piksel tersebut dihitung dan digunakan sebagai dasar dalam menentukan kapasitas penyisipan pesan. Nilai selisih tersebut dapat dihitung menggunakan persamaan sederhana sebagai berikut:

$d = |p1 - p2|$ dimana *d* menyatakan nilai selisih antara dua piksel, sedangkan *p1* dan *p2* merupakan nilai piksel yang berdekatan. Nilai selisih ini kemudian digunakan untuk menentukan banyaknya *bit* pesan yang dapat disisipkan pada pasangan piksel tersebut. Semakin besar nilai selisih yang dihasilkan, maka semakin besar pula kapasitas *bit* yang dapat dimasukkan, sedangkan pada selisih yang kecil jumlah *bit* yang disisipkan menjadi lebih terbatas.

Pendekatan ini memungkinkan metode PVD menjaga keseimbangan antara kapasitas penyisipan dan kualitas citra. Pada area citra yang memiliki perubahan intensitas tinggi (*edge area*), lebih banyak data dapat disisipkan tanpa menimbulkan perubahan visual yang mencolok. Sebaliknya, pada area yang relatif halus (*smooth area*), penyisipan dilakukan secara lebih terbatas untuk menjaga kualitas citra tetap stabil.

Mulyono dkk. (2022) menyatakan bahwa metode PVD memanfaatkan pasangan piksel yang berdekatan dengan melakukan penyesuaian terhadap selisih nilai piksel sebagai dasar dalam proses penyisipan pesan. Melalui pendekatan ini,

metode PVD mampu meningkatkan kapasitas penyisipan sekaligus mempertahankan kualitas citra stego agar tetap mendekati citra aslinya.

Selain itu, metode PVD termasuk ke dalam teknik steganografi berbasis *domain* spasial, di mana proses penyisipan dilakukan secara langsung pada nilai piksel citra tanpa memerlukan proses transformasi tambahan. Hal ini membuat metode PVD relatif lebih sederhana dan efisien untuk diimplementasikan dalam sistem steganografi citra digital.

2.4.1. Proses Penyisipan Pesan (*Embedding*) Metode PVD

Proses penyisipan pesan (*embedding*) pada metode *Pixel Value Differencing* (PVD) merupakan tahap awal dalam memasukkan pesan rahasia ke dalam citra digital. Pada tahap ini, pesan yang akan disisipkan terlebih dahulu dikonversi ke dalam bentuk biner agar dapat diproses dan dimasukkan ke dalam nilai piksel citra.

Menurut Gustiawan dkk. (2023), proses *embedding* pada metode PVD dilakukan dengan membagi citra digital menjadi pasangan piksel yang saling berdekatan. Setiap pasangan piksel kemudian dihitung selisih nilainya sebagai dasar untuk menentukan jumlah *bit* pesan yang dapat disisipkan. Nilai selisih tersebut digunakan sebagai acuan dalam menentukan kapasitas penyisipan pada masing-masing pasangan piksel.

Setelah kapasitas penyisipan ditentukan, *bit-bit* pesan rahasia dimasukkan ke dalam pasangan piksel dengan cara menyesuaikan nilai selisih piksel tersebut. Proses ini dilakukan secara berurutan dimulai dari pasangan piksel pertama hingga seluruh pesan berhasil disisipkan. Dengan pendekatan ini, jumlah *bit* yang

disisipkan pada setiap pasangan piksel dapat berbeda-beda, tergantung pada nilai selisih yang dihasilkan.

Pada bagian citra yang memiliki selisih nilai besar, lebih banyak *bit* pesan dapat disisipkan tanpa menimbulkan perubahan visual yang mencolok. Sebaliknya, pada bagian citra dengan selisih kecil, jumlah *bit* yang disisipkan dibatasi agar kualitas citra tetap terjaga. Pendekatan ini membuat metode PVD mampu menyesuaikan proses penyisipan dengan karakteristik lokal citra.

Mulyono dkk. (2022) menjelaskan bahwa proses *embedding* pada metode PVD dilakukan dengan memodifikasi nilai piksel secara terkontrol sehingga citra hasil penyisipan (citra stego) tetap memiliki tingkat kemiripan yang tinggi dengan citra asli. Dengan demikian, pesan rahasia dapat disisipkan tanpa menimbulkan perbedaan visual yang signifikan.

Hasil dari proses *embedding* adalah citra stego, yaitu citra digital yang telah mengandung pesan rahasia di dalamnya. Citra stego tersebut selanjutnya dapat disimpan atau dikirimkan sebagai media penyampaian informasi tersembunyi tanpa menimbulkan kecurigaan dari pihak yang tidak berwenang.

2.4.2. Proses Pengambilan Pesan (*Extraction*) Metode PVD

Proses pengambilan pesan (*extraction*) pada metode *Pixel Value Differencing* (PVD) merupakan tahapan yang bertujuan untuk memperoleh kembali pesan rahasia yang telah disisipkan ke dalam citra stego. Pada tahap ini, sistem membaca kembali nilai piksel pada citra stego untuk mengambil informasi yang sebelumnya telah dimasukkan melalui proses penyisipan.

Menurut Gustiawan dkk. (2023) proses *extraction* pada metode PVD dilakukan dengan membagi citra stego menjadi pasangan piksel yang sama seperti pada saat proses *embedding*. Selanjutnya, selisih nilai antara dua piksel yang berdekatan dihitung kembali sebagai dasar untuk menentukan jumlah *bit* pesan yang tersimpan pada setiap pasangan piksel.

Nilai selisih yang diperoleh kemudian digunakan untuk mengetahui banyaknya *bit* yang harus diambil dari masing-masing pasangan piksel. *Bit-bit* tersebut diambil secara berurutan mengikuti urutan penyisipan hingga seluruh pesan berhasil direkonstruksi kembali. Oleh karena itu, kesesuaian antara proses *embedding* dan *extraction* menjadi faktor penting dalam keberhasilan pengambilan pesan.

Pada citra stego yang tidak mengalami perubahan, proses *extraction* umumnya dapat berjalan dengan baik dan menghasilkan pesan yang sama dengan pesan asli. Namun, jika citra mengalami perubahan seperti kompresi ulang, perubahan ukuran, atau manipulasi piksel lainnya, maka proses pengambilan pesan dapat terganggu sehingga informasi yang diperoleh menjadi tidak lengkap.

Mulyono dkk. (2022) menyatakan bahwa keberhasilan proses *extraction* pada metode PVD sangat bergantung pada kestabilan nilai piksel citra stego. Selama nilai piksel tidak mengalami perubahan yang signifikan, pesan rahasia dapat diambil kembali dengan baik sesuai dengan data yang telah disisipkan sebelumnya.

Dengan demikian, proses pengambilan pesan (*extraction*) pada metode PVD merupakan tahapan penting dalam sistem steganografi yang berfungsi untuk

mengembalikan pesan rahasia dari citra stego. Keberhasilan proses ini sangat ditentukan oleh kesesuaian mekanisme penyisipan serta kondisi citra yang digunakan.

2.4.3. Kelebihan dan Keterbatasan Metode *Pixel Value Differencing* (PVD)

Metode *Pixel Value Differencing* (PVD) merupakan salah satu teknik dalam steganografi citra digital yang memiliki berbagai keunggulan dalam proses penyisipan pesan. Salah satu kelebihan utama metode ini adalah kemampuannya dalam meningkatkan kapasitas penyisipan. Hal ini disebabkan karena metode PVD memanfaatkan perbedaan nilai antar piksel, sehingga jumlah *bit* yang disisipkan dapat menyesuaikan dengan karakteristik citra.

Menurut Mulyono dkk. (2022) metode PVD mampu menampung data dalam jumlah yang lebih besar dibandingkan metode sederhana seperti *Least Significant Bit* (LSB). Hal ini terjadi karena pada area citra yang memiliki perubahan intensitas tinggi (*edge area*), lebih banyak *bit* pesan dapat disisipkan tanpa menimbulkan perubahan visual yang signifikan. Dengan demikian, metode ini memiliki keunggulan dalam hal efisiensi kapasitas penyisipan.

Selain itu, metode PVD juga mampu mempertahankan kualitas visual citra dengan baik. Proses penyisipan dilakukan secara adaptif, di mana area citra yang relatif halus (*smooth area*) hanya mengalami perubahan kecil sehingga distorsi visual dapat diminimalkan. Pendekatan ini memungkinkan citra stego tetap memiliki tingkat kemiripan yang tinggi dengan citra aslinya.

Di sisi lain, metode *Pixel Value Differencing* (PVD) juga memiliki beberapa keterbatasan. Salah satu keterbatasannya adalah tingkat kompleksitas proses yang

lebih tinggi dibandingkan metode LSB. Hal ini dikarenakan metode PVD memerlukan perhitungan selisih nilai piksel serta penyesuaian nilai piksel dalam proses penyisipan maupun pengambilan pesan.

Selain itu, metode PVD juga sangat bergantung pada kestabilan nilai piksel citra. Apabila citra stego mengalami perubahan, seperti kompresi ulang, perubahan ukuran, atau manipulasi lainnya, maka pesan yang disisipkan berpotensi mengalami kerusakan atau tidak dapat diekstraksi secara sempurna. Menurut Gustiawan dkk. (2023) perubahan pada nilai piksel dapat memengaruhi hasil perhitungan selisih, Metode *Pixel Value Differencing* (PVD) juga memiliki sensitivitas terhadap perubahan selisih nilai antar piksel.

Perubahan kecil pada pasangan piksel dapat menyebabkan pergeseran hasil pembacaan *bit* pada proses *extraction*, sehingga pesan yang diperoleh berpotensi mengalami kerusakan meskipun citra stego masih terlihat normal secara visual. Oleh karena itu, diperlukan validasi integritas payload untuk memastikan bahwa pesan hasil *extraction* sesuai dengan pesan asli yang disisipkan.sehingga berdampak pada keberhasilan proses pengambilan pesan.

Berdasarkan kelebihan dan keterbatasan tersebut, dapat disimpulkan bahwa metode *Pixel Value Differencing* (PVD) sesuai digunakan pada sistem steganografi citra digital yang mengutamakan kapasitas penyisipan serta kualitas visual citra. Namun demikian, penggunaannya perlu mempertimbangkan kondisi citra dan kemungkinan perubahan yang dapat memengaruhi keberhasilan proses *extraction*.

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1. Analisis Permasalahan

Perkembangan teknologi informasi saat ini telah mendorong proses pertukaran data dan informasi menjadi semakin cepat dan mudah melalui media digital. Kondisi ini memberikan berbagai kemuhan dalam komunikasi, namun di sisi lain juga meningkatkan risiko terjadinya penyadapan, pencurian, serta penyalahgunaan informasi, terutama terhadap data atau pesan yang bersifat rahasia. Oleh karena itu, aspek keamanan informasi menjadi hal yang sangat penting dalam proses pengiriman data melalui jaringan terbuka, mengingat data berpotensi diakses oleh pihak yang tidak memiliki kewenangan Akmal dkk. (2023).

Dalam praktiknya, pengiriman pesan rahasia masih sering dilakukan dalam bentuk teks atau *file* digital biasa. Cara ini relatif mudah dikenali dan berpotensi menimbulkan kecurigaan, sehingga risiko kebocoran informasi menjadi lebih besar. Meskipun teknik kriptografi dapat digunakan untuk melindungi isi pesan, keberadaan pesan yang telah dienkripsi masih dapat diketahui, sehingga belum sepenuhnya mampu menyembunyikan keberadaan informasi tersebut.

Berdasarkan permasalahan tersebut, diperlukan suatu metode pengamanan yang tidak hanya menjaga isi pesan, tetapi juga mampu menyamarkan keberadaan pesan itu sendiri. Salah satu teknik yang dapat digunakan adalah steganografi, yaitu metode penyisipan pesan rahasia ke dalam media digital tanpa menimbulkan perubahan yang mencolok, sehingga pesan tidak mudah terdeteksi oleh pihak lain.

Citra digital dipilih sebagai media penyisipan karena memiliki karakteristik yang mendukung penerapan steganografi. Citra digital tersusun atas piksel yang direpresentasikan dalam bentuk data biner, sehingga memungkinkan dilakukan perubahan kecil pada nilai piksel tanpa memberikan pengaruh yang signifikan terhadap kualitas visual citra. Karakteristik ini menjadikan citra digital sebagai media yang efektif dalam menyembunyikan pesan rahasia.

Dalam penerapan steganografi pada citra digital, terdapat berbagai metode yang dapat digunakan, di antaranya metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Metode LSB bekerja dengan memodifikasi *bit* paling tidak signifikan pada nilai piksel citra, sehingga proses penyisipan dapat dilakukan secara sederhana dan efisien. Sementara itu, metode PVD memanfaatkan perbedaan nilai antar piksel yang berdekatan untuk menentukan jumlah *bit* pesan yang dapat disisipkan, sehingga proses penyisipan dapat dilakukan secara adaptif sesuai dengan karakteristik citra.

Penggunaan kedua metode tersebut memberikan pendekatan yang berbeda dalam proses penyisipan pesan. Metode LSB memiliki keunggulan dari sisi kemudahan implementasi, sedangkan metode PVD unggul dalam kapasitas penyisipan serta kemampuan menyesuaikan dengan kondisi citra. Oleh karena itu, diperlukan suatu sistem yang mampu mengimplementasikan kedua metode tersebut dalam proses steganografi citra digital.

Berdasarkan uraian tersebut, penelitian ini difokuskan pada perancangan dan implementasi sistem steganografi citra digital dengan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Sistem yang

dikembangkan bertujuan untuk melakukan proses penyisipan pesan (*embedding*) dan pengambilan kembali pesan (*extraction*) pada citra digital, serta menampilkan kualitas citra hasil penyisipan berdasarkan parameter PSNR dan MSE sesuai dengan batasan penelitian yang telah ditetapkan.

Selain proses penyisipan dan pengambilan pesan, sistem steganografi juga memerlukan mekanisme pendukung agar proses dapat berjalan dengan baik. Oleh karena itu, sistem yang dirancang pada penelitian ini dilengkapi dengan fitur pemeriksaan citra, analisis kapasitas penyisipan, deteksi metode steganografi, serta pengukuran kualitas citra menggunakan parameter MSE dan PSNR. Fitur-fitur tersebut bertujuan untuk memastikan proses *embedding* dan *extraction* dapat berjalan secara optimal sesuai dengan karakteristik citra digital yang digunakan.

3.2. Algoritma Sistem

Algoritma sistem merupakan rangkaian tahapan yang disusun secara logis dan sistematis untuk menangani permasalahan penyisipan serta pengambilan kembali pesan rahasia pada citra digital. Dalam penelitian ini, algoritma sistem dirancang untuk menerapkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) sebagai teknik steganografi dalam proses penyisipan pesan berupa *file* berformat *.sql* ke dalam media citra digital.

Secara umum, algoritma sistem yang dikembangkan terdiri atas dua proses utama, yaitu proses penyisipan pesan (*embedding*) dan proses pengambilan pesan (*extraction*). Proses *embedding* bertujuan untuk memasukkan pesan rahasia ke dalam citra digital dengan memanfaatkan *bit* paling tidak signifikan pada nilai

piksel citra serta perbedaan nilai antar piksel. Sementara itu, proses *extraction* digunakan untuk mengambil kembali pesan rahasia yang telah disisipkan ke dalam citra stego sehingga pesan dapat dikembalikan ke bentuk semula dan dibaca dengan benar.

Perancangan algoritma sistem dilakukan dengan mempertimbangkan kesederhanaan alur kerja, efisiensi waktu pemrosesan, serta kemampuan sistem dalam mempertahankan kualitas visual citra digital. Dengan algoritma yang disusun secara terstruktur, sistem steganografi yang dibangun diharapkan mampu berfungsi secara optimal dan sesuai dengan tujuan penelitian serta batasan masalah yang telah ditetapkan.

3.2.1. Algoritma Penyisipan Pesan (*Embedding*)

Algoritma penyisipan pesan (*embedding*) merupakan tahap utama dalam sistem steganografi yang digunakan untuk memasukkan pesan rahasia ke dalam citra digital dengan memanfaatkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Pada tahap ini, pesan rahasia berupa *file* berformat .*sql* disisipkan ke dalam citra melalui perubahan nilai piksel, di mana perubahan tersebut dirancang agar tidak menimbulkan perbedaan visual yang mencolok pada citra hasil penyisipan.

Proses *embedding* diawali dengan pemilihan citra digital yang akan digunakan sebagai media penyisipan (*cover image*). Citra tersebut kemudian diproses oleh sistem berdasarkan nilai piksel yang menyusunnya. Selanjutnya, *file* .*sql* yang akan disisipkan dikonversi ke dalam bentuk biner. Konversi ini

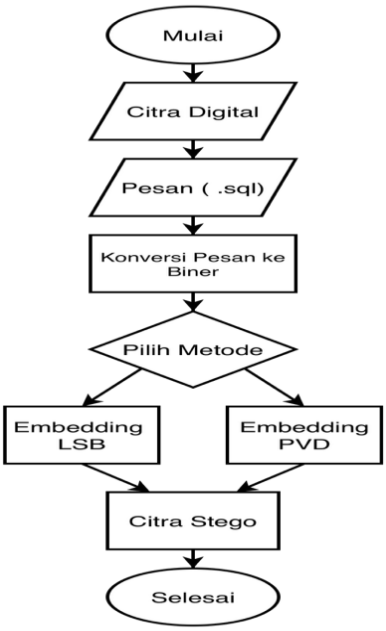
diperlukan karena metode steganografi bekerja pada tingkat *bit*, sehingga pesan harus direpresentasikan dalam format biner sebelum dilakukan penyisipan.
Setelah proses konversi selesai, sistem membaca nilai piksel citra dan mengubahnya ke dalam bentuk biner sesuai dengan kanal warna yang digunakan. Pada metode LSB, penyisipan dilakukan dengan mengganti *bit* paling tidak signifikan pada nilai piksel secara berurutan dengan *bit* pesan. Sementara itu, pada metode PVD, proses penyisipan dilakukan dengan memanfaatkan perbedaan nilai antar piksel untuk menentukan jumlah *bit* yang dapat dimasukkan ke dalam setiap pasangan piksel.

Penyisipan pesan dilakukan secara sistematis hingga seluruh *bit* pesan berhasil dimasukkan ke dalam citra tanpa melampaui kapasitas penyimpanan yang tersedia. Pendekatan ini memungkinkan metode LSB dan PVD digunakan secara efektif tanpa mengurangi kualitas visual citra secara signifikan.

Setelah seluruh proses penyisipan selesai, sistem menghasilkan citra baru yang disebut sebagai citra stego. Secara visual, citra stego tetap menyerupai citra asli, namun telah mengandung pesan rahasia di dalamnya. Selanjutnya, sistem melakukan pemeriksaan pesan dengan cara melakukan *extraction* ulang secara otomatis untuk memastikan bahwa pesan dapat dikembalikan dengan baik dan sesuai dengan *file* asli yang disisipkan. Setelah proses pemeriksaan selesai, citra stego dapat digunakan sebagai media penyimpanan maupun pengiriman informasi tersembunyi.

Dengan menerapkan algoritma penyisipan menggunakan metode LSB dan PVD, sistem mampu melakukan proses *embedding* secara efektif sekaligus

menjaga kualitas citra digital. Algoritma ini dirancang agar dapat diimplementasikan dengan baik sesuai dengan tujuan penelitian serta batasan masalah yang telah ditentukan.



Gambar 1. Algoritma Proses Penyisipan Pesan (*Embedding*)

Gambar 1. Algoritma ini menggambarkan proses penyisipan pesan ke dalam citra digital menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Proses dimulai dari *input* citra digital dan *file* pesan berformat .sql, kemudian pesan dikonversi ke dalam bentuk biner.

Selanjutnya, sistem melakukan pemilihan metode yang digunakan, yaitu LSB atau PVD, kemudian proses *embedding* dijalankan sesuai metode yang dipilih hingga menghasilkan citra stego yang telah mengandung pesan rahasia.

Setelah proses *embedding* selesai, sistem dapat melakukan pemeriksaan pesan untuk memastikan bahwa pesan yang disisipkan dapat dikembalikan dengan

baik melalui proses *extraction*. Proses diakhiri setelah citra stego berhasil terbentuk.

3.2.2. Algoritma Pengambilan Pesan (*Extraction*)

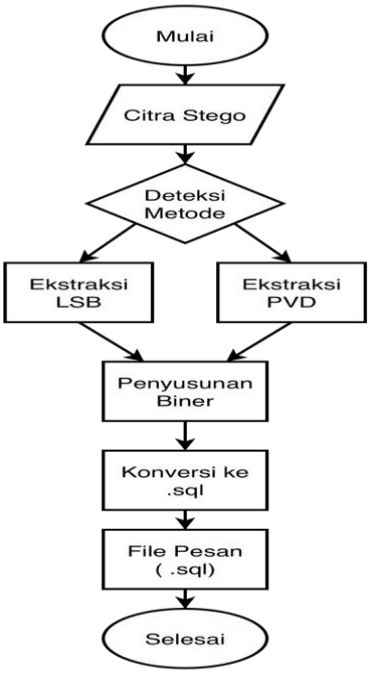
Algoritma pengambilan pesan (*extraction*) merupakan proses yang bertujuan untuk memperoleh kembali informasi rahasia yang telah disisipkan ke dalam citra stego. Pada penelitian ini, mekanisme *extraction* dirancang untuk mendukung dua metode steganografi, yaitu *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD), sehingga sistem dapat mengekstrak pesan sesuai dengan metode yang digunakan saat proses penyisipan.

Tahap *extraction* diawali dengan memasukkan citra stego sebagai data masukan ke dalam sistem. Citra tersebut kemudian diproses untuk membaca nilai piksel yang akan digunakan dalam proses pengambilan pesan. Setelah itu, sistem melakukan identifikasi metode yang digunakan, guna menentukan apakah citra tersebut menggunakan metode LSB atau PVD.

Jika metode yang terdeteksi adalah LSB, maka proses *extraction* dilakukan dengan mengambil *bit* paling tidak signifikan dari setiap piksel secara berurutan. *Bit-bit* yang diperoleh selanjutnya dikumpulkan hingga membentuk rangkaian data biner yang merepresentasikan pesan tersembunyi. Sementara itu, pada metode PVD, proses *extraction* dilakukan dengan menghitung selisih nilai antara pasangan piksel yang berdekatan. Nilai selisih tersebut digunakan sebagai acuan untuk menentukan jumlah *bit* pesan yang tersimpan, kemudian *bit* tersebut diambil sesuai dengan kapasitas yang dihasilkan.

Setelah seluruh *bit* berhasil diperoleh, data biner tersebut disusun kembali secara utuh hingga membentuk informasi lengkap. Selanjutnya, data biner dikonversi kembali ke dalam bentuk *file* asli, yaitu *file* dengan format .sql. Hasil akhir dari proses ini adalah pesan yang sama seperti yang telah disisipkan sebelumnya.

Dengan demikian, algoritma *extraction* pada penelitian ini mampu mengembalikan pesan rahasia dari citra stego dengan memanfaatkan metode *Least Significant Bit* (LSB) maupun *Pixel Value Differencing* (PVD). Keberhasilan proses ini sangat dipengaruhi oleh kesesuaian metode yang digunakan serta kondisi citra stego yang tetap terjaga tanpa mengalami perubahan yang signifikan.



Gambar 2. Algoritma Proses Pengambilan Pesan (*Extraction*)

Gambar 2. Flowchart ini menunjukkan proses pengambilan kembali pesan dari citra stego. Proses dimulai dengan memasukkan citra stego, kemudian sistem

mendeteksi metode yang digunakan, yaitu LSB atau PVD. Setelah itu, dilakukan proses ekstraksi sesuai metode yang terdeteksi untuk memperoleh *bit-bit* pesan. Data biner yang diperoleh kemudian disusun kembali dan dikonversi menjadi *file* .sql. Proses diakhiri dengan diperolehnya *file* pesan hasil ekstraksi.

3.3. Flowchart Sistem

Flowchart sistem merupakan bentuk visual yang digunakan untuk menggambarkan alur kerja dari sistem steganografi yang dikembangkan dalam penelitian ini. Diagram ini berfungsi untuk memberikan gambaran yang jelas mengenai tahapan-tahapan yang dilakukan oleh sistem, mulai dari proses *input* data, pengolahan, hingga menghasilkan output sesuai dengan tujuan yang telah dirancang.

Dalam penelitian ini, sistem steganografi dirancang untuk menangani dua proses utama, yaitu penyisipan pesan (*embedding*) dan pengambilan kembali pesan (*extraction*) pada citra digital. Kedua proses tersebut memiliki alur yang berbeda, sehingga divisualisasikan dalam flowchart yang terpisah agar lebih mudah dipahami.

Flowchart yang dibuat juga menggambarkan hubungan antara pengguna dan sistem, di mana pengguna memasukkan data berupa citra digital dan *file* pesan, kemudian sistem memprosesnya menggunakan metode yang dipilih, yaitu *Least Significant Bit* (LSB) atau *Pixel Value Differencing* (PVD). Hasil dari proses tersebut ditampilkan dalam bentuk citra stego pada tahap *embedding* dan *file* pesan pada tahap *extraction*.

Dengan adanya flowchart sistem ini, diharapkan alur kerja aplikasi dapat dipahami dengan lebih terstruktur dan sistematis, sehingga dapat membantu dalam proses perancangan, implementasi, serta evaluasi sistem yang dikembangkan.

3.3.1. Flowchart *Embedding*

Flowchart proses *embedding* menjelaskan alur kerja sistem dalam menyisipkan pesan rahasia ke dalam citra digital. Proses diawali dengan pengguna mengunggah citra digital sebagai media penyisipan serta *file* pesan berformat .*sql* yang akan dimasukkan ke dalam citra.

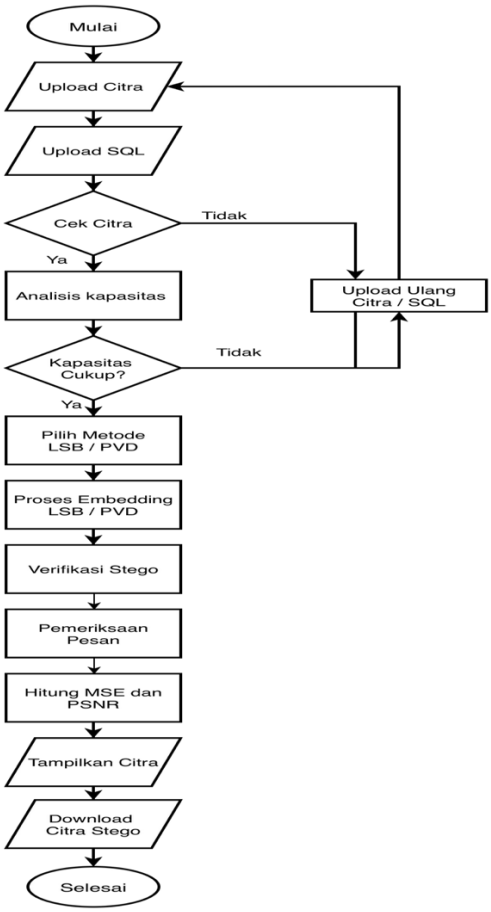
Setelah *input* diterima, sistem melakukan pengecekan terhadap citra untuk memastikan bahwa citra tersebut belum mengandung pesan steganografi. Jika citra masih dalam kondisi bersih, proses dilanjutkan. Sebaliknya, apabila citra telah berisi pesan, maka proses dihentikan dan pengguna diminta menggunakan citra lain.

Selanjutnya, sistem melakukan analisis kapasitas untuk mengetahui apakah ukuran pesan sesuai dengan kemampuan penyisipan citra. Perhitungan kapasitas dilakukan berdasarkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Apabila kapasitas tidak mencukupi, proses tidak dapat dilanjutkan dan pengguna perlu mengganti citra atau ukuran *file* pesan.

Jika kapasitas mencukupi, pengguna dapat memilih metode penyisipan yang diinginkan, yaitu LSB atau PVD. Sistem kemudian menjalankan proses *embedding* dengan menyesuaikan nilai piksel citra sesuai metode yang digunakan. Setelah proses penyisipan selesai, sistem melakukan verifikasi terhadap citra stego untuk memastikan bahwa pesan telah berhasil disisipkan. Selanjutnya, sistem

melakukan validasi integritas pesan dengan cara melakukan proses *extraction* ulang secara otomatis terhadap citra stego dan membandingkan hasil *extraction* dengan *file* asli yang disisipkan. Proses ini bertujuan untuk memastikan bahwa pesan dapat dikembalikan dengan baik tanpa mengalami kerusakan data. Setelah proses validasi selesai, sistem melakukan perhitungan kualitas citra menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR) untuk mengetahui tingkat perubahan yang terjadi pada citra stego.

Tahap akhir adalah menampilkan citra stego kepada pengguna serta menyediakan opsi untuk mengunduh hasil penyisipan. Proses *embedding* berakhir setelah citra stego berhasil dihasilkan dan siap digunakan sebagai media penyimpanan maupun pengiriman pesan.



Gambar 3. Flowchart *Embedding*

Gambar 3. Flowchart *embedding* menggambarkan proses penyisipan pesan ke dalam citra digital. Proses dimulai dari *input* citra dan *file* .sql, kemudian sistem melakukan pengecekan citra dan analisis kapasitas. Jika kapasitas mencukupi, pengguna memilih metode LSB atau PVD dan sistem melakukan proses *embedding*. Setelah proses *embedding* selesai, sistem melakukan verifikasi stego serta pemeriksaan pesan untuk memastikan hasil *extraction* sesuai dengan pesan asli yang disisipkan. Selanjutnya dilakukan perhitungan MSE dan PSNR untuk mengetahui kualitas citra stego, kemudian hasil ditampilkan dan dapat diunduh oleh pengguna.

3.3.2. Flowchart *Extraction*

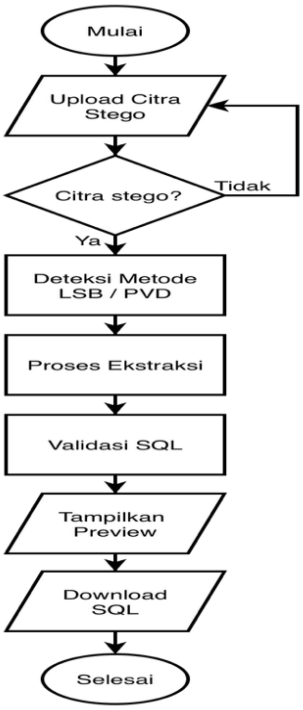
Flowchart proses *extraction* menggambarkan tahapan sistem dalam mengambil kembali pesan rahasia yang telah disisipkan ke dalam citra stego. Proses diawali dengan pengguna mengunggah citra stego sebagai *input* pada sistem.

Setelah citra dimasukkan, sistem melakukan pemeriksaan untuk memastikan bahwa citra tersebut benar-benar mengandung pesan steganografi. Apabila citra teridentifikasi sebagai citra stego, maka proses dilanjutkan. Namun, jika tidak terdapat pesan di dalam citra, maka proses dihentikan.

Selanjutnya, sistem mengidentifikasi metode yang digunakan pada saat penyisipan, yaitu *Least Significant Bit* (LSB) atau *Pixel Value Differencing* (PVD). Berdasarkan metode yang terdeteksi, sistem kemudian melakukan proses *extraction* untuk memperoleh data biner yang tersimpan dalam citra.

Data hasil *extraction* kemudian diperiksa untuk memastikan kesesuaiannya dengan format *file .sql*. Setelah validasi selesai, sistem menampilkan hasil dalam bentuk *preview* sehingga pengguna dapat melihat isi pesan yang berhasil diambil.

Tahap akhir adalah menyediakan fasilitas untuk mengunduh *file* pesan dalam format *.sql*. Proses *extraction* selesai setelah *file* berhasil dihasilkan dan dapat digunakan kembali sesuai kebutuhan.



Gambar 4. Flowchart *Extraction*

Gambar 4. Flowchart proses *extraction* menggambarkan alur pengambilan pesan dari citra stego. Proses dimulai dari *input* citra stego, kemudian sistem melakukan pengecekan apakah citra mengandung pesan. Jika citra terdeteksi mengandung pesan, sistem selanjutnya mendeteksi metode yang digunakan yaitu (LSB atau PVD) dan melakukan proses ekstraksi. Hasil ekstraksi kemudian divalidasi, ditampilkan dalam bentuk *preview*, dan dapat diunduh sebagai *file .sql*. Proses berakhir setelah pesan berhasil diperoleh.

3.4. Pemodelan dan Perancangan Sistem

Pada penelitian ini dilakukan tahap pemodelan serta perancangan sistem steganografi citra digital yang bertujuan untuk menyisipkan dan mengambil

kembali data berupa *file* SQL ke dalam media citra. Sistem yang dikembangkan memanfaatkan dua metode utama, yaitu *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) sebagai teknik dalam proses penyisipan pesan.

Permasalahan yang menjadi fokus dalam penelitian ini adalah bagaimana proses penyisipan data ke dalam citra dapat dilakukan tanpa memberikan penurunan kualitas citra yang signifikan, serta bagaimana memastikan bahwa data yang telah disisipkan dapat dikembalikan secara utuh dan tepat. Oleh karena itu, sistem yang dirancang harus mampu mendukung proses *embedding* dan *extraction* secara optimal, serta menyediakan fitur analisis kualitas citra dengan menggunakan parameter Mean Squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR).

Sistem ini dikembangkan berbasis *web* untuk memberikan kemudahan bagi pengguna dalam melakukan proses penyisipan maupun pengambilan pesan. Pada tahap penyisipan (*embedding*), pengguna dapat mengunggah citra sebagai media penyimpanan, mengunggah *file* SQL sebagai data yang akan disisipkan, menentukan metode yang digunakan (LSB atau PVD), serta memperoleh *output* berupa citra stego yang telah berisi pesan tersembunyi. Selain itu, sistem juga menampilkan hasil analisis kualitas citra guna memastikan bahwa perubahan yang terjadi masih dalam batas yang dapat diterima.

Sedangkan pada tahap pengambilan pesan (*extraction*), pengguna dapat mengunggah citra stego untuk mengambil kembali *file* SQL yang sebelumnya telah disisipkan. Sistem juga dilengkapi dengan mekanisme pendeteksian metode

yang digunakan pada saat penyisipan agar proses ekstraksi dapat dilakukan dengan tepat, serta dilengkapi dengan validasi terhadap hasil ekstraksi.

Untuk memberikan gambaran yang lebih terstruktur mengenai sistem yang dirancang, digunakan pemodelan berupa *Use Case* Diagram untuk menggambarkan interaksi antara pengguna dan sistem, *Activity* Diagram untuk menjelaskan alur proses yang terjadi, serta perancangan antarmuka sebagai representasi tampilan sistem yang akan digunakan oleh pengguna.

3.4.1. *Use Case* Diagram

Use Case Diagram digunakan untuk menggambarkan interaksi antara pengguna dengan sistem yang dirancang. Diagram ini menunjukkan fungsi-fungsi utama yang dapat dijalankan oleh pengguna dalam sistem steganografi citra digital.

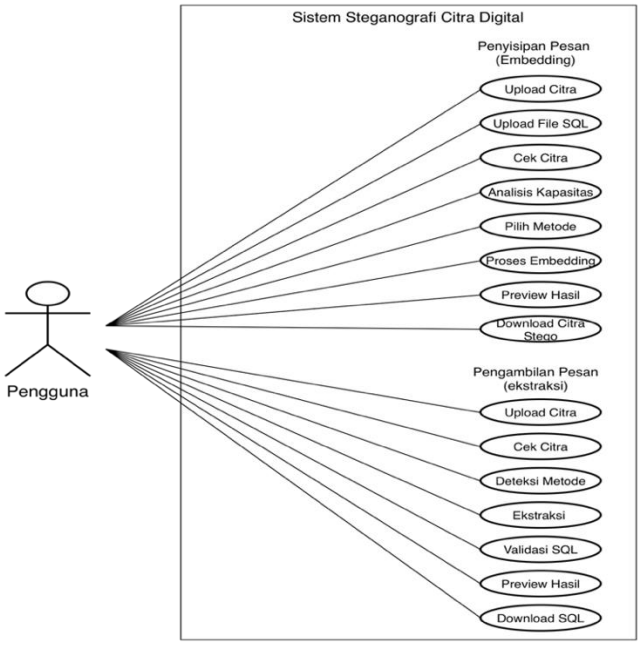
Pada sistem yang dibangun, terdapat satu aktor yaitu pengguna. Pengguna berperan sebagai pihak yang menjalankan seluruh proses dalam sistem, baik pada tahap penyisipan pesan (*embedding*) maupun pengambilan pesan (*extraction*).

Pada proses penyisipan pesan (*embedding*), pengguna dapat melakukan beberapa aktivitas, yaitu mengunggah citra sebagai media penampung, mengunggah *file* SQL sebagai data yang akan disisipkan, melakukan pengecekan citra, melakukan analisis kapasitas untuk mengetahui kemampuan citra dalam menampung data, memilih metode penyisipan yang digunakan yaitu *Least Significant Bit* (LSB) atau *Pixel Value Differencing* (PVD), serta menjalankan proses *embedding*. Setelah proses selesai, pengguna dapat melihat hasil

penyisipan melalui fitur *preview* dan mengunduh citra stego yang telah berisi pesan.

Sedangkan pada proses pengambilan pesan (*extraction*), pengguna dapat mengunggah citra stego, melakukan pengecekan citra, serta sistem akan melakukan deteksi metode yang digunakan pada saat penyisipan. Selanjutnya, pengguna dapat menjalankan proses ekstraksi untuk memperoleh kembali data yang telah disisipkan. Hasil ekstraksi kemudian divalidasi oleh sistem untuk memastikan keakuratan data, dan pengguna dapat melihat hasilnya melalui fitur *preview* serta mengunduh *file* SQL yang telah berhasil diekstrak.

Dengan adanya *Use Case* Diagram ini, diharapkan dapat memberikan gambaran yang jelas mengenai interaksi antara pengguna dan sistem, serta fungsi-fungsi yang tersedia dalam sistem steganografi citra digital yang dibangun.



Gambar 5. *Use Case* Diagram

Gambar 5. *Use Case* Diagram menggambarkan sistem yang melibatkan satu aktor yaitu pengguna yang dapat menjalankan proses penyisipan (*embedding*) dan pengambilan pesan (*extraction*). Pada tahap *embedding*, pengguna mengunggah citra dan *file* SQL untuk menghasilkan citra stego. Sementara itu, pada tahap *extraction*, pengguna mengunggah citra stego untuk mendapatkan kembali *file* SQL.

3.4.2. *Activity* Diagram

Activity diagram digunakan untuk menggambarkan alur kerja sistem serta interaksi antara pengguna dan sistem dalam aplikasi steganografi citra digital. Diagram ini terdiri dari dua bagian utama, yaitu proses penyisipan pesan (*embedding*) dan proses pengambilan pesan (*extraction*), yang masing-masing menunjukkan peran pengguna dan sistem.

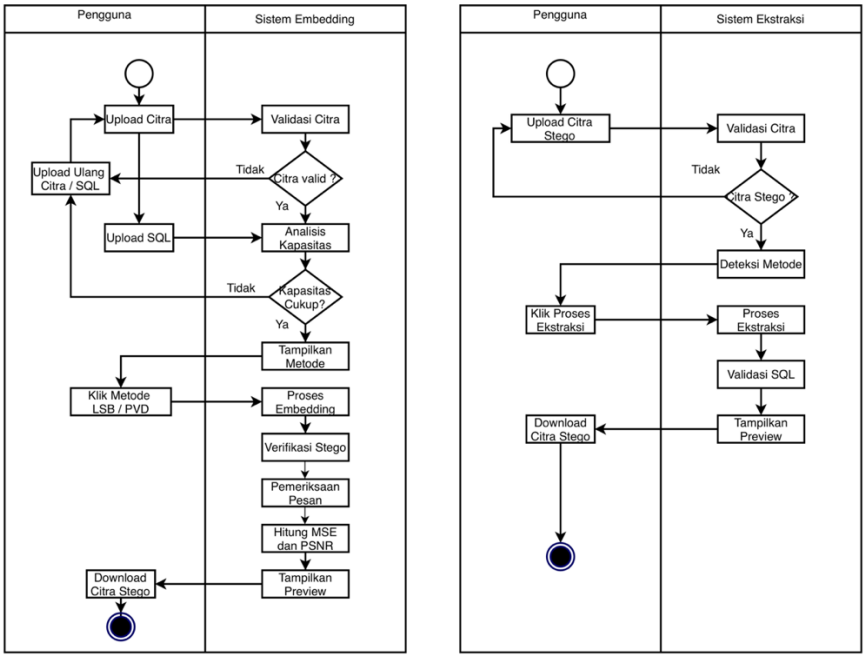
Pada proses *embedding*, alur dimulai dari pengguna yang mengunggah citra sebagai media penyimpanan serta *file* SQL sebagai data yang akan disisipkan. Selanjutnya, sistem melakukan validasi terhadap citra untuk memastikan bahwa citra tersebut dapat digunakan. Apabila citra tidak memenuhi syarat, pengguna diberikan kesempatan untuk mengunggah ulang citra atau data.

Setelah itu, sistem melakukan analisis kapasitas guna mengetahui apakah citra memiliki ruang yang cukup untuk menampung data. Jika kapasitas tidak mencukupi, pengguna dapat kembali melakukan pengunggahan data. Namun, jika memenuhi syarat, sistem akan menampilkan pilihan metode yang tersedia, kemudian pengguna memilih metode yang akan digunakan, yaitu LSB atau PVD, dan menjalankan proses *embedding*. Proses ini dilanjutkan dengan verifikasi hasil

stego serta pemeriksaan pesan untuk memastikan bahwa hasil *extraction* sesuai dengan *file* asli yang disisipkan. Setelah itu, sistem melakukan perhitungan nilai MSE dan PSNR serta menampilkan hasil citra sebelum pengguna mengunduh citra stego.

Pada proses *extraction*, alur dimulai dari pengguna yang mengunggah citra stego. Sistem kemudian melakukan validasi untuk memastikan bahwa citra tersebut mengandung pesan tersembunyi. Jika tidak valid, pengguna dapat melakukan pengunggahan ulang. Apabila citra valid, sistem akan mendeteksi metode yang digunakan dan pengguna dapat menjalankan proses ekstraksi. Selanjutnya, sistem mengekstrak data, melakukan validasi terhadap *file* SQL hasil ekstraksi, serta menampilkan hasilnya kepada pengguna. Setelah proses selesai, pengguna dapat mengunduh *file* SQL yang telah berhasil diperoleh.

Dengan adanya *activity* diagram ini, alur proses sistem dapat dipahami dengan lebih jelas, baik dari segi tahapan yang dilakukan maupun pembagian peran antara pengguna dan sistem.



Gambar 6. *activity* diagram

Gambar 6. *activity* diagram yang menggambarkan alur proses *embedding* dan *extraction* pada sistem. Pada proses *embedding*, pengguna mengunggah citra dan *file* SQL, kemudian sistem melakukan validasi serta analisis kapasitas. Jika tidak memenuhi syarat, pengguna dapat mengunggah ulang data. Jika memenuhi, pengguna memilih metode dan sistem menjalankan proses *embedding* hingga menghasilkan citra stego. Selanjutnya, sistem melakukan verifikasi stego dan pemeriksaan pesan untuk memastikan bahwa pesan dapat dikembalikan dengan baik melalui proses *extraction*. Setelah itu, sistem menghitung nilai MSE dan PSNR, kemudian hasil citra stego ditampilkan dan dapat diunduh oleh pengguna.

Pada proses *extraction*, pengguna mengunggah citra stego yang kemudian divalidasi oleh sistem. Jika citra mengandung pesan, sistem mendeteksi metode

dan melakukan proses ekstraksi. Hasil ekstraksi selanjutnya ditampilkan dan dapat diunduh dalam bentuk *file* SQL.

3.4.3. Perancangan Antarmuka

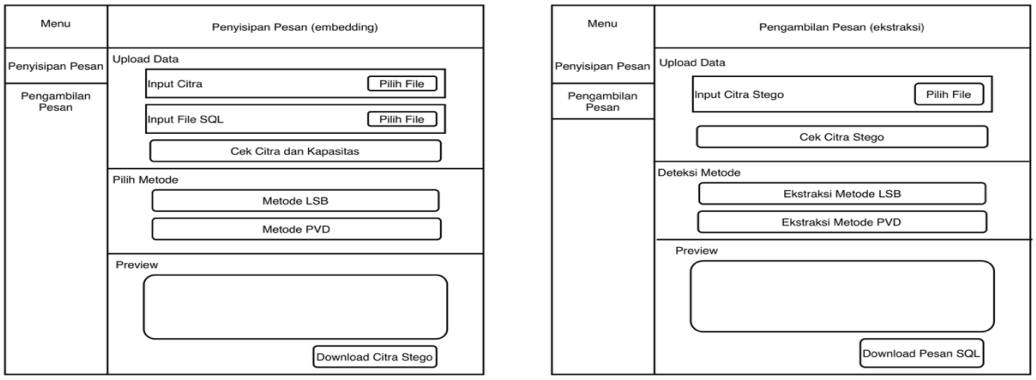
Perancangan antarmuka dibuat untuk memberikan gambaran mengenai tampilan sistem yang akan digunakan oleh pengguna dalam melakukan proses penyisipan maupun pengambilan pesan. Antarmuka dirancang dengan susunan yang sederhana dan terstruktur sehingga pengguna dapat dengan mudah memahami alur penggunaan sistem.

Pada halaman penyisipan pesan (*embedding*), antarmuka terdiri dari beberapa bagian utama, yaitu menu navigasi, bagian *input* data, proses pengecekan, pemilihan metode, serta tampilan hasil. Pada bagian *input* data, pengguna dapat mengunggah citra sebagai media penyimpanan dan *file* SQL sebagai data yang akan disisipkan melalui tombol yang tersedia. Setelah itu, pengguna dapat melakukan pengecekan citra dan kapasitas untuk memastikan bahwa citra layak digunakan. Jika telah memenuhi syarat, pengguna memilih metode yang digunakan, yaitu LSB atau PVD, kemudian sistem menjalankan proses *embedding*. Hasil penyisipan ditampilkan pada bagian *preview*, dan citra stego dapat diunduh melalui tombol yang disediakan.

Pada halaman pengambilan pesan (*extraction*), antarmuka memiliki struktur yang serupa, yaitu terdiri dari menu navigasi, bagian *input* citra stego, proses pengecekan, deteksi metode, serta tampilan hasil. Pengguna terlebih dahulu mengunggah citra stego melalui tombol pilih *file*, kemudian sistem melakukan pengecekan untuk memastikan adanya pesan tersembunyi. Selanjutnya, sistem

menampilkan metode ekstraksi berdasarkan hasil deteksi, yaitu LSB atau PVD, dan pengguna dapat menjalankan proses ekstraksi. Hasil ekstraksi ditampilkan pada bagian *preview*, dan *file* SQL yang diperoleh dapat diunduh oleh pengguna.

Dengan perancangan antarmuka tersebut, diharapkan pengguna dapat memahami alur penggunaan sistem dengan lebih mudah, mulai dari proses *input* hingga memperoleh hasil, baik pada proses *embedding* maupun *extraction*.



Gambar 7. Perancangan antarmuka

Gambar 7. Perancangan antarmuka sistem menggambarkan proses *embedding* dan *extraction*. Pada bagian *embedding*, pengguna mengunggah citra dan *file* SQL, melakukan pengecekan, memilih metode, serta mengunduh citra stego. Sementara itu, pada bagian *extraction*, pengguna mengunggah citra stego, melakukan pengecekan, menjalankan proses ekstraksi, dan mengunduh *file* SQL.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1. Kebutuhan Sistem

Kebutuhan sistem merupakan tahapan awal dalam proses perancangan yang bertujuan untuk mengidentifikasi seluruh komponen yang diperlukan agar sistem dapat beroperasi secara optimal. Pada tahap ini dilakukan analisis terhadap berbagai kebutuhan yang mencakup perangkat keras, perangkat lunak, serta kebutuhan fungsional yang mendukung proses penyisipan dan pengambilan pesan pada citra digital.

Sistem yang dikembangkan dalam penelitian ini berupa aplikasi steganografi berbasis komputer yang berfungsi untuk menyisipkan dan mengekstraksi pesan dalam bentuk *file* SQL ke dalam citra digital dengan memanfaatkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Selain itu, sistem juga dilengkapi dengan kemampuan untuk melakukan evaluasi kualitas citra hasil penyisipan menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR).

Kebutuhan sistem pada penelitian ini selanjutnya dikelompokkan menjadi beberapa bagian, yaitu kebutuhan perangkat keras (hardware), kebutuhan perangkat lunak (software), serta kebutuhan fungsional sistem yang mendukung proses implementasi dan pengujian.

4.1.1. Kebutuhan Perangkat Keras (Hardware)

Perangkat keras yang digunakan dalam pengembangan dan pengujian sistem pada penelitian ini berupa sebuah laptop dengan tipe MacBook Air M2. Perangkat

tersebut dimanfaatkan untuk menjalankan aplikasi steganografi yang telah dirancang, mulai dari proses penyisipan pesan hingga proses pengambilan kembali pesan pada citra digital. Adapun spesifikasi perangkat keras yang digunakan adalah sebagai berikut:

Processor : Apple M2 Chip

RAM : 8 GB

Storage : 256 GB SSD

Selain itu, perangkat ini juga dilengkapi dengan komponen *input* berupa keyboard dan touchpad yang berfungsi untuk mengoperasikan sistem, serta komponen *output* berupa layar (display) yang digunakan untuk menampilkan antarmuka aplikasi dan hasil dari proses yang dilakukan.

Secara umum, sistem yang dikembangkan tidak membutuhkan spesifikasi perangkat keras yang tinggi. Sistem ini masih dapat dijalankan pada perangkat dengan spesifikasi minimal, seperti processor dual-core atau setara, RAM minimal 4 GB, serta media penyimpanan minimal 128 GB. Dengan spesifikasi tersebut, sistem tetap dapat menjalankan seluruh fitur utama secara optimal.

4.1.2. Kebutuhan Perangkat Lunak (Software)

Perangkat lunak yang digunakan dalam proses pengembangan dan pengujian sistem pada penelitian ini berperan sebagai komponen utama dalam membangun serta menjalankan aplikasi steganografi. Perangkat lunak tersebut dimanfaatkan untuk mendukung proses pengembangan sistem, pengolahan data dalam proses penyisipan dan pengambilan pesan, serta penyajian antarmuka aplikasi kepada pengguna.

Adapun perangkat lunak yang digunakan dalam penelitian ini meliputi:

1. Sistem Operasi : macOS
2. Bahasa Pemrograman : Python
3. Framework : Streamlit
4. Library Pendukung : PIL (*Python Imaging Library*) untuk pengolahan citra dan Numpy untuk pengolahan data numerik
5. Code Editor : Visual Studio Code

Pemilihan bahasa pemrograman Python didasarkan pada kemampuannya dalam menyediakan berbagai pustaka yang mendukung pengolahan citra digital serta kemudahan dalam proses pengembangan aplikasi. Framework Streamlit digunakan untuk membangun antarmuka aplikasi berbasis *web* yang bersifat interaktif dan mudah digunakan oleh pengguna. Selain itu, pemanfaatan library seperti PIL berperan dalam proses manipulasi citra digital yang diperlukan dalam penerapan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD).

4.1.3. Kebutuhan Fungsional Sistem

Kebutuhan fungsional sistem merupakan kebutuhan yang berkaitan dengan fungsi-fungsi utama yang harus dimiliki oleh sistem agar dapat berjalan sesuai dengan tujuan penelitian yang telah ditetapkan. Dalam penelitian ini, sistem yang dikembangkan adalah aplikasi steganografi berbasis *web* yang digunakan untuk melakukan proses penyisipan dan pengambilan kembali pesan pada citra digital dengan memanfaatkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD).

Kebutuhan fungsional tersebut dirancang untuk mendukung keseluruhan proses kerja sistem, mulai dari tahap *input* data, proses pengolahan, hingga menghasilkan *output* berupa citra stego serta hasil ekstraksi pesan. Dengan adanya kebutuhan fungsional yang terdefinisi dengan baik, sistem diharapkan dapat beroperasi secara sistematis, efisien, dan sesuai dengan kebutuhan pengguna.

Adapun kebutuhan fungsional sistem dalam penelitian ini adalah sebagai berikut:

1. Sistem dapat menerima *input* berupa citra digital sebagai media penyisipan pesan.
2. Sistem dapat menerima *input* berupa *file* SQL sebagai pesan rahasia yang akan disisipkan.
3. Sistem dapat melakukan pengecekan terhadap citra untuk memastikan apakah citra telah mengandung pesan atau belum.
4. Sistem dapat menghitung kapasitas maksimum citra dalam proses penyisipan menggunakan metode LSB dan PVD.
5. Sistem dapat memberikan informasi mengenai kelayakan citra berdasarkan perbandingan kapasitas citra dengan ukuran pesan.
6. Sistem dapat melakukan proses penyisipan pesan menggunakan metode *Least Significant Bit* (LSB).
7. Sistem dapat melakukan proses penyisipan pesan menggunakan metode *Pixel Value Differencing* (PVD).
8. Sistem dapat menampilkan citra hasil penyisipan (citra stego).

9. Sistem dapat menghitung kualitas citra hasil penyisipan menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR).
10. Sistem dapat mengidentifikasi metode penyisipan yang digunakan pada citra stego.
11. Sistem dapat melakukan proses pengambilan kembali pesan (*extraction*) dari citra stego.
12. Sistem dapat menampilkan hasil ekstraksi pesan dalam bentuk *file* SQL.
13. Sistem menyediakan fitur untuk mengunduh citra stego dan *file* hasil ekstraksi pesan.
14. Sistem dapat melakukan pemeriksaan pesan untuk memastikan bahwa hasil *extraction* sesuai dengan *file* asli yang disisipkan.

Dengan adanya kebutuhan fungsional tersebut, sistem yang dikembangkan diharapkan mampu menjalankan seluruh proses steganografi secara optimal, mulai dari tahap penyisipan hingga proses ekstraksi pesan, serta tetap menjaga kualitas citra sesuai dengan tujuan penelitian.

4.2. Implementasi Sistem

Implementasi sistem merupakan tahapan penerapan dari hasil perancangan yang telah dilakukan sebelumnya ke dalam bentuk aplikasi yang dapat digunakan secara langsung oleh pengguna. Pada tahap ini, sistem steganografi yang telah dirancang direalisasikan dalam bentuk aplikasi berbasis *web* dengan memanfaatkan bahasa pemrograman Python dan framework Streamlit.

Sistem yang dikembangkan bertujuan untuk melakukan proses penyisipan (*embedding*) serta pengambilan kembali (*extraction*) pesan berupa *file* SQL ke dalam citra digital dengan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Selain itu, sistem juga dilengkapi dengan fitur untuk menganalisis kualitas citra hasil penyisipan menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR).

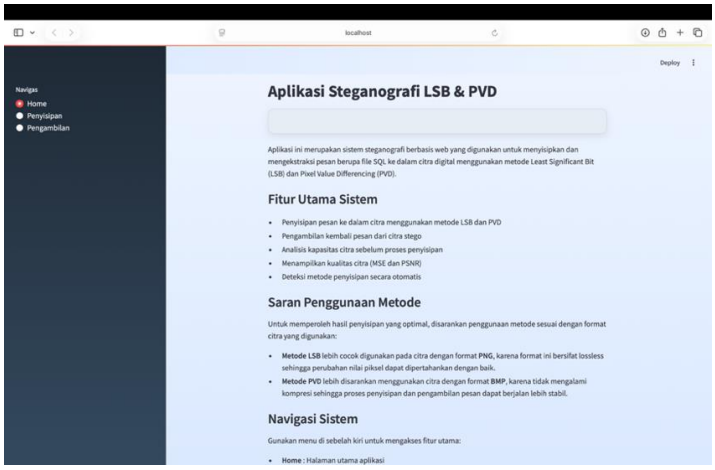
Dalam implementasinya, aplikasi dibagi ke dalam beberapa bagian utama, yaitu halaman Home, halaman Penyisipan (*Embedding*), dan halaman Pengambilan (*Extraction*). Setiap bagian dirancang untuk menjalankan fungsi tertentu sesuai dengan kebutuhan pengguna dalam melakukan proses steganografi.

4.2.1. Implementasi Halaman Home

Halaman Home merupakan tampilan awal yang muncul ketika aplikasi dijalankan. Halaman ini berfungsi sebagai halaman utama yang menyajikan informasi umum mengenai aplikasi steganografi yang dikembangkan. Melalui halaman ini, pengguna dapat memperoleh gambaran awal terkait fungsi dan tujuan sistem.

Tampilan halaman Home dirancang secara sederhana namun tetap informatif, sehingga memudahkan pengguna dalam memahami kegunaan aplikasi. Pada halaman ini ditampilkan judul aplikasi yaitu “Aplikasi Steganografi LSB & PVD” disertai dengan deskripsi singkat yang menjelaskan bahwa sistem digunakan untuk melakukan proses penyisipan dan pengambilan pesan pada citra digital.

Selain itu, halaman Home juga dilengkapi dengan menu navigasi yang terdapat pada bagian sidebar. Menu tersebut terdiri dari halaman Home, halaman Penyisipan (*Embedding*), dan halaman Pengambilan (*Extraction*). Keberadaan menu navigasi ini mempermudah pengguna dalam mengakses setiap fitur yang tersedia serta berpindah antar halaman sesuai dengan kebutuhan proses steganografi yang dilakukan. Dengan adanya halaman Home, pengguna dapat memahami fungsi dasar sistem sebelum memanfaatkan fitur utama yang disediakan dalam aplikasi.



Gambar 8. Halaman Home

Gambar 8. Halaman Home pada aplikasi steganografi menampilkan judul aplikasi, informasi umum mengenai fungsi sistem, serta fitur utama yang tersedia. Selain itu, terdapat menu navigasi pada bagian sidebar yang berfungsi untuk memudahkan pengguna dalam mengakses halaman Penyisipan dan Pengambilan sesuai dengan kebutuhan.

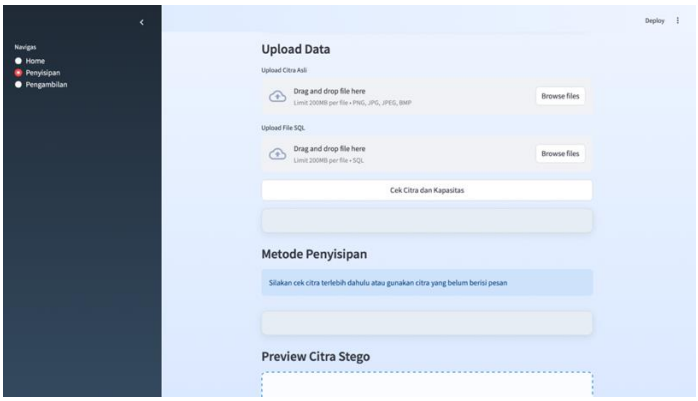
4.2.2. Implementasi Penyisipan (*Embedding*)

Halaman Penyisipan (*Embedding*) merupakan bagian dari sistem yang berfungsi untuk menyisipkan pesan berupa *file* SQL ke dalam citra digital. Pada

halaman ini, pengguna dapat melakukan proses penyisipan pesan dengan memanfaatkan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD).

Proses penyisipan diawali dengan mengunggah citra digital sebagai media penyisipan serta *file* SQL sebagai pesan yang akan disisipkan. Selanjutnya, sistem akan melakukan pengecekan terhadap citra serta menghitung kapasitas maksimum yang tersedia untuk memastikan bahwa ukuran pesan sesuai dengan kapasitas citra. Setelah proses pengecekan selesai, pengguna dapat memilih metode penyisipan yang akan digunakan.

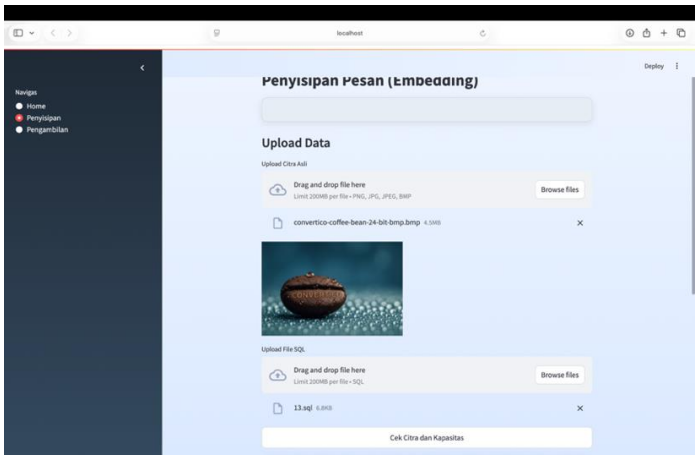
Apabila proses penyisipan berhasil, sistem akan menampilkan citra stego sebagai hasil akhir, disertai dengan analisis kualitas citra menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Selain itu, sistem juga melakukan pemeriksaan pesan secara otomatis untuk memastikan bahwa hasil *extraction* tetap sesuai dengan *file* asli yang disisipkan. Hasil pemeriksaan tersebut ditampilkan dalam bentuk notifikasi kepada pengguna.



Gambar 9. Halaman Awal Penyisipan

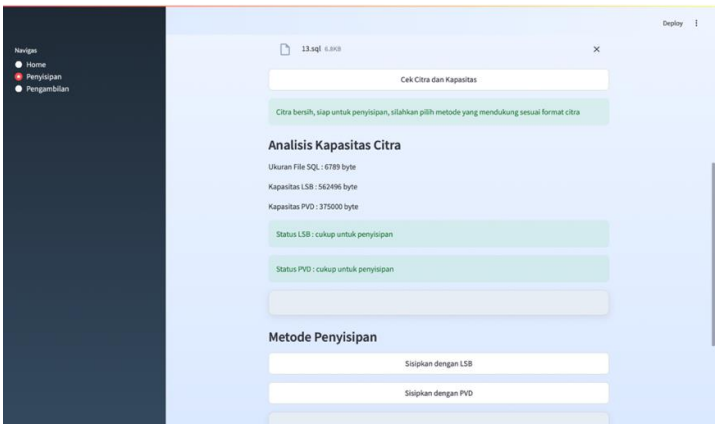
Gambar 9. menampilkan halaman awal proses penyisipan (*embedding*) pada aplikasi steganografi. Pada halaman ini, pengguna dapat mengunggah citra digital

serta *file* SQL yang akan digunakan dalam proses penyisipan pesan. Selain itu, sistem juga menyediakan fitur pengecekan citra dan kapasitas sebelum proses *embedding* dilakukan.



Gambar 10. Halaman Upload Data

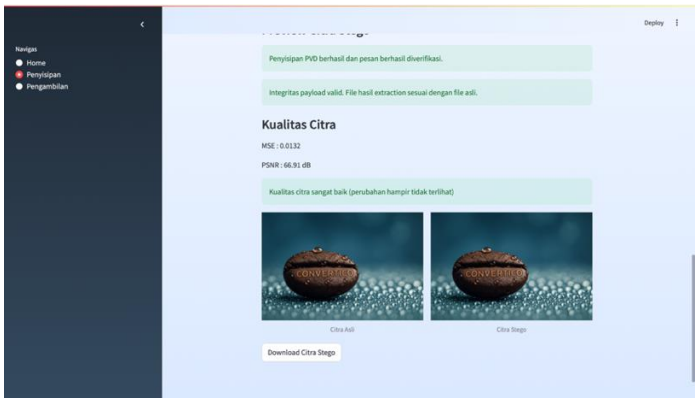
Gambar 10. menampilkan halaman *upload* data pada proses penyisipan. Pada tahap ini, pengguna diminta untuk mengunggah citra digital sebagai media penyisipan serta *file* SQL sebagai pesan yang akan disisipkan. Selain itu, sistem menampilkan pratinjau citra yang telah dipilih untuk memastikan bahwa citra yang digunakan sesuai dengan kebutuhan proses penyisipan.



Gambar 11. Analisis Citra dan kapasitas

Gambar 11. menampilkan proses pengecekan citra yang dilakukan sebelum penyisipan pesan. Pada tahap ini, sistem terlebih dahulu memverifikasi apakah citra yang digunakan masih dalam kondisi bersih atau telah mengandung pesan. Jika citra dinyatakan valid, maka sistem akan melanjutkan ke tahap analisis kapasitas citra.

Selanjutnya, sistem menghitung ukuran *file* SQL serta kapasitas maksimum citra menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD). Berdasarkan hasil perhitungan tersebut, sistem memberikan informasi mengenai kelayakan citra dengan membandingkan ukuran pesan terhadap kapasitas yang tersedia, serta menampilkan metode penyisipan yang dapat digunakan untuk proses penyisipan (*embedding*).



Gambar 12. Hasil Penyisipan

Gambar 12. menampilkan hasil proses penyisipan pesan ke dalam citra digital. Pada bagian awal, sistem menampilkan informasi kualitas citra berupa nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR) sebagai parameter untuk mengukur tingkat perubahan yang terjadi pada citra setelah proses penyisipan.

Berdasarkan nilai yang diperoleh, terlihat bahwa nilai PSNR cukup tinggi, yang menunjukkan bahwa perubahan yang terjadi pada citra relatif kecil sehingga kualitas citra tetap terjaga dan perbedaan secara visual tidak terlihat secara signifikan. Selain menampilkan kualitas citra, sistem juga memberikan informasi mengenai hasil pemeriksaan pesan setelah proses *embedding* selesai dilakukan. Pemeriksaan ini bertujuan untuk mengetahui apakah pesan yang telah disisipkan dapat dikembalikan kembali dengan baik melalui proses *extraction*.

Selanjutnya, sistem menampilkan perbandingan antara citra asli dan citra stego secara berdampingan untuk memudahkan pengguna dalam melihat perbedaan hasil penyisipan. Secara visual, perbedaan antara citra asli dan citra

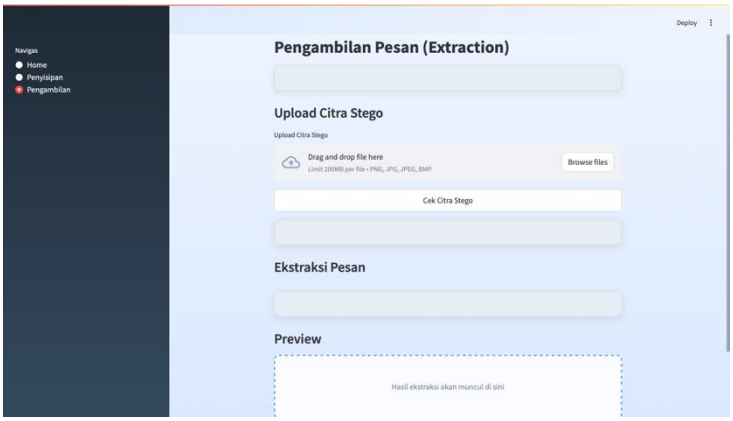
stego tidak terlihat secara signifikan sehingga kualitas citra tetap terjaga dengan baik setelah proses penyisipan dilakukan. Pada bagian akhir, sistem menyediakan fitur untuk mengunduh citra stego sebagai hasil dari proses penyisipan yang telah dilakukan.

4.2.3. Implementasi Pengambilan (*Extraction*)

Halaman Pengambilan (*Extraction*) merupakan bagian dari aplikasi yang digunakan untuk memperoleh kembali pesan rahasia yang telah disisipkan ke dalam citra stego. Pada halaman ini, pengguna dapat melakukan proses ekstraksi terhadap *file* SQL yang sebelumnya telah dimasukkan ke dalam citra digital menggunakan metode *Least Significant Bit* (LSB) maupun *Pixel Value Differencing* (PVD).

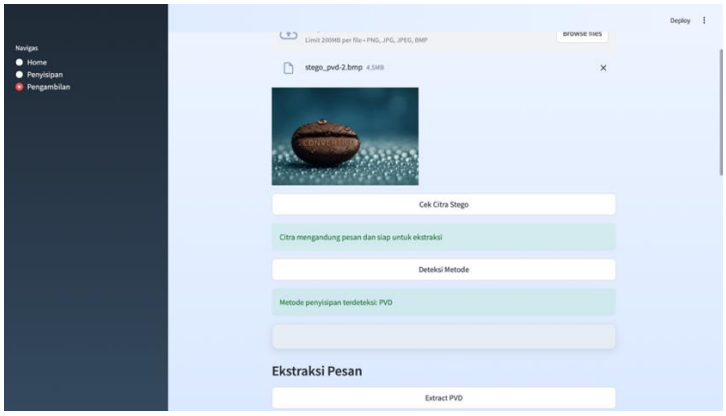
Tahap *extraction* dimulai dengan mengunggah citra stego ke dalam sistem. Setelah citra berhasil dimasukkan, sistem akan melakukan pemeriksaan untuk memastikan bahwa citra tersebut mengandung pesan steganografi. Selanjutnya, sistem melakukan identifikasi metode yang digunakan pada saat proses penyisipan pesan dilakukan.

Setelah metode berhasil dikenali, sistem menjalankan proses *extraction* sesuai dengan metode yang terdeteksi untuk mengambil kembali data yang tersimpan di dalam citra. Data hasil ekstraksi kemudian dikonversi kembali ke dalam bentuk *file* SQL dan ditampilkan kepada pengguna dalam bentuk *preview*. Selain itu, sistem juga menyediakan fitur untuk mengunduh *file* hasil *extraction* sehingga data yang berhasil diperoleh dapat digunakan kembali sesuai kebutuhan.



Gambar 13. Halaman Awal Pengambilan Pesan

Gambar 13. menampilkan halaman awal proses pengambilan pesan (*extraction*) pada aplikasi steganografi. Pada halaman ini, pengguna dapat mengunggah citra stego yang akan digunakan dalam proses *extraction*. Selain itu, sistem juga menyediakan fitur pengecekan citra stego sebelum proses pengambilan pesan dilakukan.



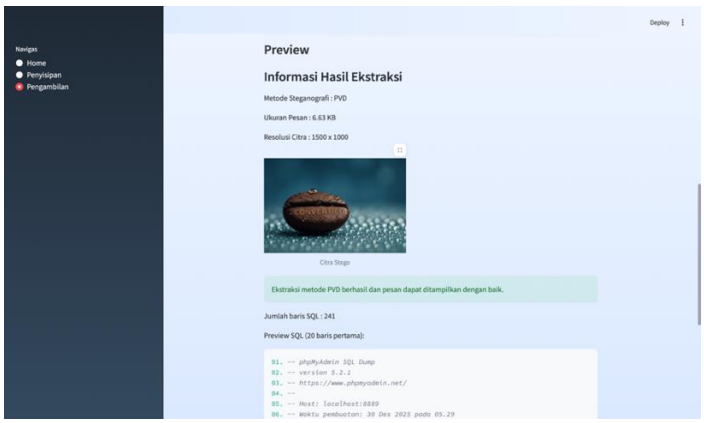
Gambar 14. Proses *Extraction*

Gambar 14. menampilkan halaman proses *extraction* pada aplikasi steganografi yang digunakan untuk mengambil kembali pesan yang telah

disisipkan ke dalam citra stego. Pada tahap ini, pengguna terlebih dahulu mengunggah citra stego yang akan digunakan dalam proses pengambilan pesan.

Setelah citra berhasil diunggah, sistem melakukan proses pengecekan untuk memastikan bahwa citra tersebut mengandung pesan steganografi dan siap untuk dilakukan *extraction*. Selanjutnya, pengguna dapat menjalankan fitur deteksi metode untuk mengidentifikasi metode penyisipan yang digunakan pada citra stego, yaitu metode *Least Significant Bit* (LSB) atau *Pixel Value Differencing* (PVD).

Berdasarkan hasil deteksi yang diperoleh, sistem kemudian menyediakan proses *extraction* sesuai dengan metode yang terdeteksi. Pada gambar terlihat bahwa metode yang berhasil diidentifikasi adalah *Pixel Value Differencing* (PVD), sehingga sistem menampilkan tombol Extract PVD untuk menjalankan proses pengambilan pesan dari citra stego.



Gambar 15. Hasil Proses *Extraction*

Gambar 15. menampilkan hasil proses *extraction* pada aplikasi steganografi setelah pesan berhasil diambil dari citra stego. Pada tahap ini, sistem

menampilkan informasi hasil ekstraksi yang meliputi metode steganografi yang digunakan, ukuran pesan, serta resolusi citra stego yang diproses.

Selain itu, sistem juga menampilkan *preview* isi *file* SQL hasil *extraction* untuk memastikan bahwa pesan berhasil diperoleh dengan baik. Pada bagian akhir, aplikasi menyediakan fitur *download* yang digunakan untuk mengunduh kembali *file* SQL hasil *extraction* sehingga data yang diperoleh dapat disimpan dan digunakan kembali oleh pengguna.

4.3. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa aplikasi steganografi yang dikembangkan mampu menjalankan fungsi sesuai dengan tujuan penelitian. Proses pengujian mencakup seluruh fitur utama sistem, mulai dari proses penyisipan pesan (*embedding*), pengambilan kembali pesan (*extraction*), hingga pengukuran kualitas citra stego menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR).

Pada tahap pengujian, digunakan sebanyak 50 citra digital yang terdiri dari format PNG dan BMP serta *file* SQL sebagai pesan yang akan disisipkan ke dalam citra. Pengujian dilakukan menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) untuk mengetahui tingkat keberhasilan proses *embedding* dan *extraction*, kualitas citra stego berdasarkan nilai Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE), serta hasil pemeriksaan integritas pesan pada setiap data uji.

Pengujian dilakukan dengan membandingkan *file* SQL hasil *extraction* dengan *file* SQL asli yang digunakan pada saat proses penyisipan. Selain itu, kualitas citra stego juga dianalisis berdasarkan nilai PSNR dan MSE yang diperoleh setelah proses *embedding* selesai dilakukan.

Berdasarkan hasil pengujian yang telah dilakukan, metode *Least Significant Bit* (LSB) mampu menjalankan proses *embedding* dan *extraction* dengan baik pada seluruh data uji yang digunakan. Sementara itu, metode *Pixel Value Differencing* (PVD) berhasil melakukan proses *embedding* pada seluruh citra uji, namun pada salah satu proses *extraction* ditemukan beberapa perubahan karakter pada *file* SQL hasil ekstraksi. Kondisi tersebut menunjukkan bahwa metode PVD memiliki tingkat sensitivitas yang lebih tinggi terhadap perubahan nilai piksel dibandingkan metode LSB pada proses pengambilan kembali pesan.

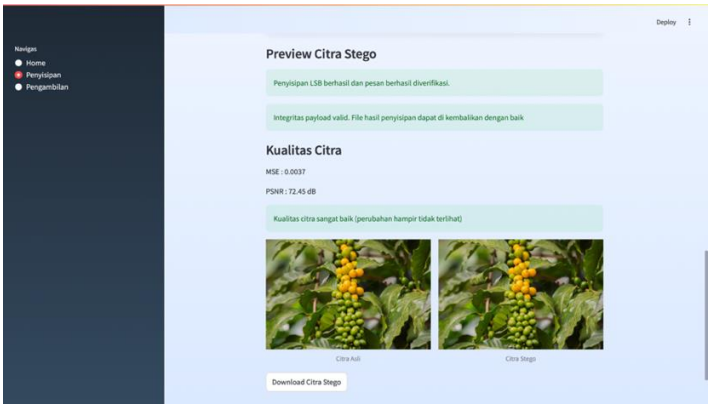
Berdasarkan hasil pengujian yang telah dilakukan, metode *Least Significant Bit* (LSB) mampu menjalankan proses *embedding* dan *extraction* dengan baik pada seluruh data uji yang digunakan. Sementara itu, metode *Pixel Value Differencing* (PVD) juga berhasil melakukan proses *embedding* pada seluruh citra uji, namun masih ditemukan beberapa hasil *extraction* yang mengalami perubahan pada *file* SQL hasil ekstraksi. Kondisi tersebut menunjukkan bahwa metode PVD memiliki tingkat sensitivitas yang lebih tinggi dibandingkan metode LSB dalam mempertahankan integritas pesan pada proses pengambilan kembali data.

4.3.1. Pengujian *Embedding* Menggunakan *Least Significant Bit* (LSB)

Pengujian *embedding* menggunakan metode *Least Significant Bit* (LSB) dilakukan untuk menguji kemampuan sistem dalam menyisipkan *file* SQL ke

dalam citra digital. Pada tahap pengujian ini, digunakan beberapa citra berformat PNG sebagai media penyisipan pesan rahasia.

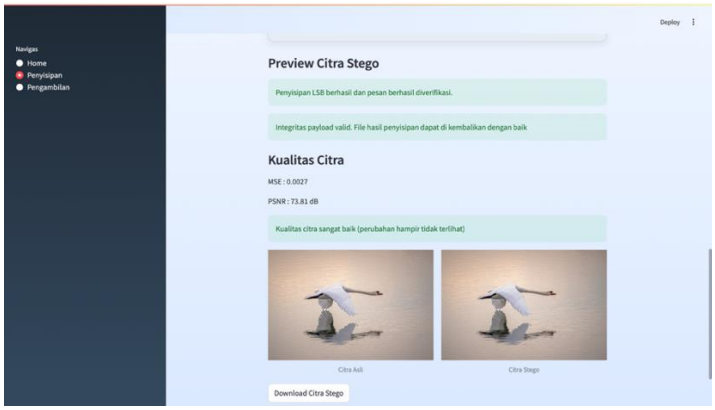
Dalam proses pengujian, *file* SQL disisipkan ke dalam citra digital menggunakan metode LSB sehingga menghasilkan citra stego sebagai *output*. Setelah proses *embedding* selesai dilakukan, sistem menampilkan informasi kualitas citra berupa nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Selain itu, sistem juga melakukan pemeriksaan pesan untuk memastikan bahwa *file* SQL hasil *extraction* tetap sesuai dengan *file* asli yang disisipkan. Pengujian ini bertujuan untuk mengetahui apakah proses penyisipan dapat berjalan dengan baik tanpa memberikan perubahan yang terlihat secara signifikan pada citra asli serta tetap mampu mempertahankan integritas pesan yang disisipkan.



Gambar 16. Hasil Pengujian Satu *Embedding* LSB

Gambar 16. memperlihatkan hasil pengujian proses *embedding* menggunakan metode *Least Significant Bit* (LSB) pada citra digital. Dari hasil pengujian yang

diperoleh, proses penyisipan pesan dapat dilakukan dengan baik dengan menghasilkan nilai PSNR sebesar 72.45 dB dan nilai MSE sebesar 0.0037. Nilai tersebut menunjukkan bahwa perubahan pada citra stego relatif sangat kecil sehingga kualitas citra tetap terlihat baik dan perbedaan visual hampir tidak dapat dibedakan dari citra asli. Selain itu, hasil pemeriksaan pesan menunjukkan bahwa *file* SQL hasil *extraction* tetap sesuai dengan *file* asli yang disisipkan sehingga proses *embedding* dan *extraction* dapat berjalan dengan baik.



Gambar 17. Hasil Pengujian Kedua *Embedding* LSB

Gambar 17. menampilkan hasil pengujian *embedding* metode *Least Significant Bit* (LSB) pada citra digital kedua. Berdasarkan hasil pengujian, proses penyisipan pesan berhasil dilakukan dengan nilai PSNR sebesar 73.81 dB dan nilai MSE sebesar 0.0027.

Hasil tersebut menunjukkan bahwa kualitas citra stego masih terjaga dengan baik karena perubahan yang terjadi setelah proses *embedding* tidak terlihat secara signifikan pada citra digital. Hasil pemeriksaan pesan juga menunjukkan

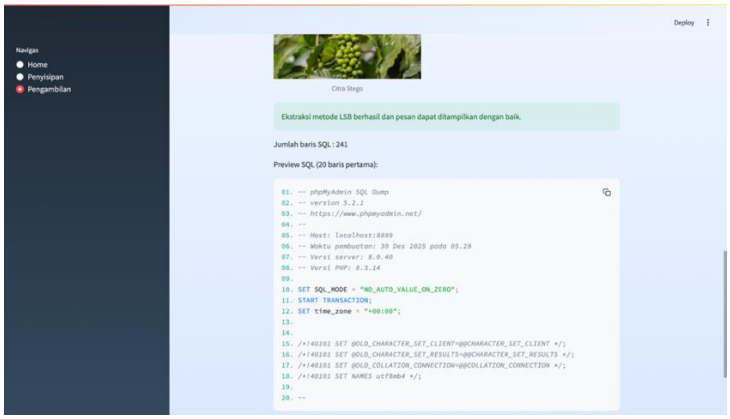
bahwa proses *extraction* dapat berjalan dengan baik tanpa mengalami perubahan data pada *file* SQL hasil ekstraksi.

4.3.2. Pengujian *Extraction* Menggunakan *Least Significant Bit* (LSB)

Pengujian *extraction* dengan metode *Least Significant Bit* (LSB) dilakukan untuk mengetahui kemampuan sistem dalam mengembalikan *file* SQL yang sebelumnya telah disisipkan ke dalam citra stego. Pada proses ini, citra stego hasil *embedding* metode LSB dimasukkan ke dalam sistem untuk dilakukan proses pengambilan pesan.

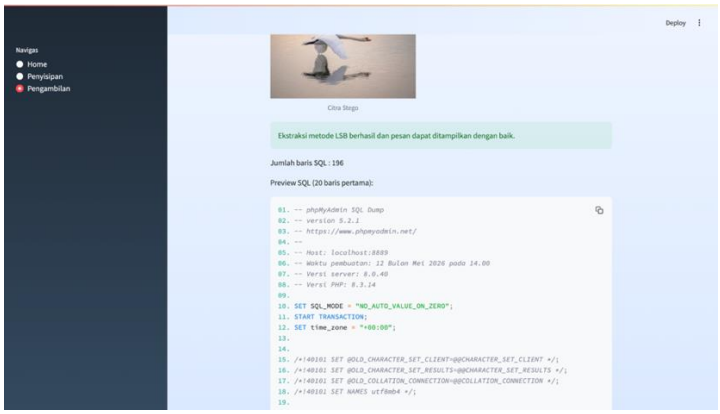
Tahap awal yang dilakukan sistem adalah memeriksa citra stego guna memastikan bahwa citra tersebut benar-benar mengandung pesan steganografi. Setelah metode penyisipan berhasil terdeteksi sebagai metode *Least Significant Bit* (LSB), sistem melanjutkan proses *extraction* untuk mengambil kembali data SQL yang tersimpan di dalam citra.

File hasil *extraction* kemudian ditampilkan dalam bentuk *preview* agar isi pesan dapat dilihat secara langsung oleh pengguna. Selain itu, aplikasi juga menyediakan fitur *download* untuk menyimpan kembali *file* SQL hasil *extraction*. Sistem selanjutnya melakukan pemeriksaan pesan dengan membandingkan *file* hasil *extraction* terhadap *file* asli guna memastikan bahwa data yang diperoleh kembali tidak mengalami perubahan selama proses penyisipan dan pengambilan pesan berlangsung.



Gambar 18. Hasil Pengujian satu *Extraction* SLB

Gambar 18. menampilkan hasil pengujian proses *extraction* menggunakan metode *Least Significant Bit* (LSB). Pada pengujian ini, sistem berhasil mendeteksi metode penyisipan yang digunakan serta mengambil kembali *file* SQL dari citra stego dengan baik. Hasil *extraction* kemudian ditampilkan dalam bentuk *preview* isi *file* SQL untuk memudahkan pengguna dalam melihat data yang berhasil diperoleh. Selain itu, hasil pemeriksaan pesan menunjukkan bahwa *file* SQL hasil *extraction* tetap sesuai dengan *file* asli yang disisipkan sehingga proses *extraction* menggunakan metode LSB dapat berjalan dengan baik tanpa mengalami perubahan data.



Gambar 19. Hasil Pengujian Kedua *Extraction* LSB

Gambar 19. menunjukkan hasil pengujian *extraction* kedua menggunakan metode *Least Significant Bit* (LSB). Berdasarkan hasil pengujian, sistem berhasil melakukan proses pengambilan kembali pesan dari citra stego dan menampilkan isi *file* SQL dalam bentuk *preview*. Sistem juga berhasil melakukan pemeriksaan pesan dengan baik sehingga *file* SQL hasil *extraction* dapat dikembalikan tanpa mengalami perubahan data. Hasil tersebut menunjukkan bahwa metode *Least Significant Bit* (LSB) mampu menjaga integritas pesan selama proses *embedding* dan *extraction* berlangsung.

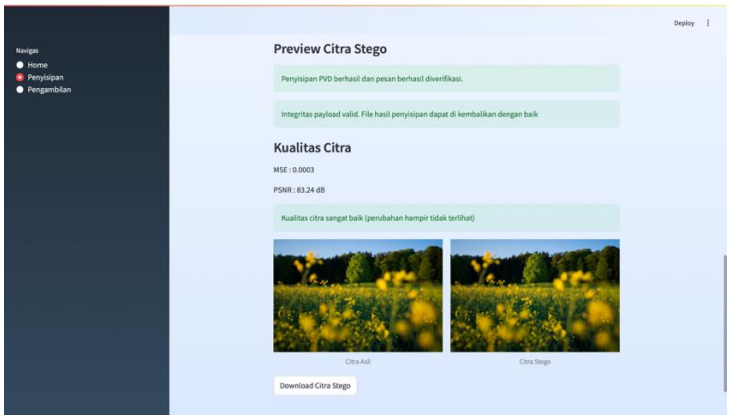
4.3.3 Pengujian *Embedding* Menggunakan Pixel Differencing (PVD)

Pengujian *embedding* dengan metode *Pixel Value Differencing* (PVD) dilakukan untuk mengetahui kemampuan sistem dalam menyisipkan *file* SQL ke dalam citra digital menggunakan metode PVD. Pada pengujian ini, beberapa citra dengan format BMP digunakan sebagai media penyisipan pesan rahasia.

Proses pengujian dilakukan dengan menyisipkan *file* SQL ke dalam citra sehingga menghasilkan citra stego sebagai keluaran sistem. Setelah proses

embedding selesai, aplikasi menampilkan informasi kualitas citra berupa nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR) untuk melihat tingkat perubahan yang terjadi pada citra stego. Selain itu, sistem juga melakukan pemeriksaan terhadap hasil *extraction* guna memastikan bahwa *file* SQL yang diperoleh kembali masih sesuai dengan *file* asli yang disisipkan.

Melalui pengujian ini, dapat diketahui kemampuan metode PVD dalam mempertahankan kualitas visual citra sekaligus menjaga keutuhan pesan setelah proses *embedding* dan *extraction* dilakukan.

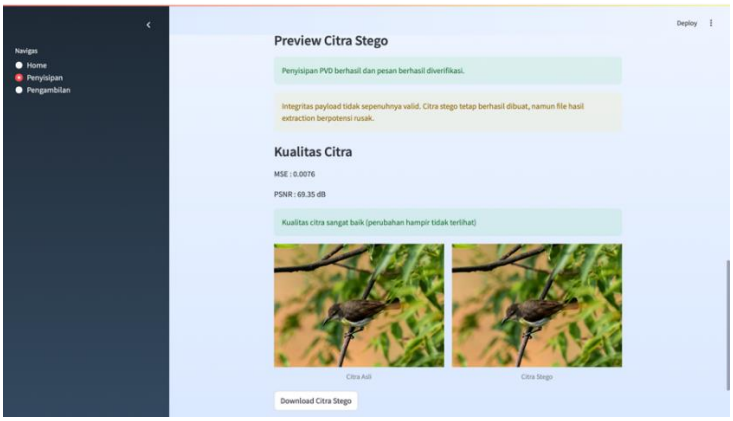


Gambar 20. Hasil Pengujian Satu *Embedding* PVD

Gambar 20. memperlihatkan hasil pengujian *embedding* menggunakan metode *Pixel Value Differencing* (PVD) pada citra digital. Dari hasil pengujian yang dilakukan, proses penyisipan *file* SQL berhasil dijalankan dengan menghasilkan nilai PSNR sebesar 83.24 dB dan nilai MSE sebesar 0.0003. Nilai tersebut menunjukkan bahwa perubahan pada citra stego sangat kecil sehingga

kualitas visual citra tetap terlihat baik dan perbedaan antara citra asli dengan citra stego hampir tidak dapat dibedakan secara visual.

Hasil pemeriksaan pesan juga menunjukkan bahwa *file* SQL hasil *extraction* dapat dikembalikan dengan baik tanpa mengalami perubahan data. Dengan demikian, metode PVD pada pengujian ini mampu menjalankan proses *embedding* dan *extraction* secara optimal sesuai dengan data yang digunakan.



Gambar 21. Hasil Pengujian Kedua *Embedding* PVD

Gambar 20. menunjukkan hasil pengujian kedua proses *embedding* menggunakan metode *Pixel Value Differencing* (PVD). Berdasarkan hasil yang diperoleh, sistem berhasil menghasilkan citra stego dengan nilai PSNR sebesar 69.35 dB dan nilai MSE sebesar 0.0076. Nilai tersebut menunjukkan bahwa perubahan pada citra setelah proses penyisipan masih relatif kecil sehingga kualitas visual citra stego tetap terlihat baik dan perbedaannya dengan citra asli tidak terlihat secara mencolok.

Meskipun demikian, hasil pemeriksaan pesan menunjukkan bahwa *file* SQL hasil *extraction* mengalami perubahan sehingga tidak sepenuhnya sama dengan

file asli yang disisipkan. Kondisi ini menunjukkan bahwa metode PVD masih dapat mengalami perubahan data pada proses *extraction* meskipun kualitas visual citra stego tetap terjaga dengan baik. Dengan demikian, kualitas citra yang tinggi tidak selalu menjamin bahwa integritas pesan dapat dipertahankan secara sempurna setelah proses *embedding* dan *extraction* dilakukan.

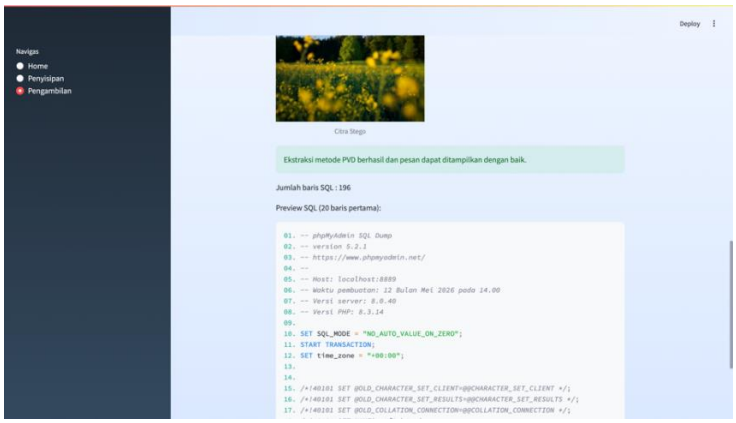
4.3.4 Pengujian *Extraction* Menggunakan *Pixel Value Differencing* (PVD)

Pengujian *extraction* dengan metode *Pixel Value Differencing* (PVD) dilakukan untuk mengukur kemampuan sistem dalam mengambil kembali *file* SQL yang sebelumnya telah disisipkan ke dalam citra stego menggunakan metode PVD. Pada tahap ini, citra stego hasil proses *embedding* dimasukkan ke dalam sistem untuk menjalankan proses *extraction*.

Sebelum proses *extraction* dilakukan, sistem terlebih dahulu memeriksa citra stego untuk memastikan bahwa citra tersebut mengandung pesan steganografi. Setelah metode penyisipan berhasil dikenali sebagai *Pixel Value Differencing* (PVD), sistem kemudian melakukan proses pengambilan kembali data SQL yang tersimpan di dalam citra stego.

Hasil *extraction* selanjutnya ditampilkan dalam bentuk *preview* isi *file* SQL agar pengguna dapat melihat isi pesan yang berhasil diperoleh. Selain itu, aplikasi juga menyediakan fitur *download* untuk mengunduh *file* hasil *extraction*. Sistem kemudian melakukan pemeriksaan pesan dengan membandingkan *file* hasil *extraction* terhadap *file* SQL asli guna mengetahui apakah data dapat

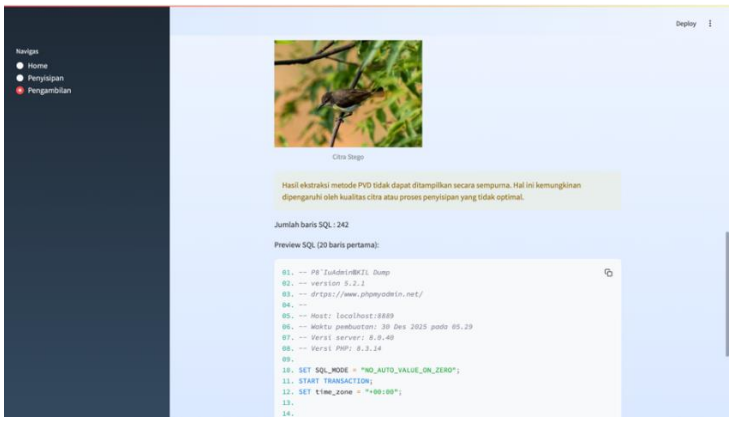
dikembalikan dengan baik tanpa mengalami perubahan selama proses *embedding* dan *extraction* berlangsung.



Gambar 22. Hasil Pengujian Satu *Extraction* PVD

Gambar 22. memperlihatkan hasil pengujian proses *extraction* menggunakan metode *Pixel Value Differencing* (PVD). Dari hasil pengujian yang dilakukan, sistem berhasil mengenali metode penyisipan yang digunakan serta mengambil kembali *file* SQL dari citra stego dengan baik. *File* hasil *extraction* kemudian ditampilkan dalam bentuk *preview* sehingga isi data yang berhasil diperoleh dapat dilihat secara langsung oleh pengguna.

Hasil pemeriksaan pesan juga menunjukkan bahwa *file* SQL hasil *extraction* masih sesuai dengan *file* asli yang sebelumnya disisipkan ke dalam citra. Dengan demikian, metode PVD pada pengujian ini mampu menjalankan proses *extraction* secara optimal tanpa menyebabkan perubahan data pada *file* SQL.



Gambar 23. Hasil Pengujian Kedua *Extraction* PVD

Gambar 23. memperlihatkan hasil pengujian kedua proses *extraction* menggunakan metode *Pixel Value Differencing* (PVD). Berdasarkan hasil pengujian, sistem berhasil menjalankan proses *extraction* dan menampilkan *preview* isi *file* SQL hasil ekstraksi. Akan tetapi, hasil pemeriksaan pesan menunjukkan bahwa *file* SQL yang diperoleh tidak sepenuhnya sama dengan *file* asli yang sebelumnya disisipkan ke dalam citra stego.

Kondisi tersebut menunjukkan bahwa walaupun proses *extraction* masih dapat dilakukan, terdapat beberapa perubahan karakter pada *file* SQL hasil *extraction*, seperti munculnya simbol **$**, **#**, ***** dan karakter lain yang tidak sesuai dengan *file* asli. Hal ini menunjukkan bahwa metode PVD mempengaruhi keutuhan data hasil *extraction.*

4.3.5 Pengujian Nilai PSNR dan MSE

Pengujian nilai Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE) dilakukan untuk mengetahui kualitas citra stego yang dihasilkan setelah proses penyisipan pesan menggunakan metode *Least Significant Bit* (LSB) dan

Pixel Value Differencing (PVD). Pengujian ini dilakukan untuk melihat seberapa besar perubahan yang terjadi pada citra setelah proses *embedding* dibandingkan dengan citra asli.

Nilai MSE digunakan untuk mengukur tingkat perbedaan nilai piksel antara citra asli dan citra stego. Semakin rendah nilai MSE yang diperoleh, maka perubahan yang terjadi pada citra stego semakin kecil. Sedangkan nilai PSNR digunakan untuk mengetahui tingkat kemiripan antara kedua citra tersebut. Semakin besar nilai PSNR, maka kualitas citra stego yang dihasilkan semakin baik karena perubahan visual yang terjadi sulit dikenali oleh penglihatan manusia.

Berdasarkan hasil pengujian yang telah dilakukan, metode *Least Significant Bit* (LSB) maupun *Pixel Value Differencing* (PVD) mampu menghasilkan citra stego dengan kualitas visual yang baik. Hal tersebut dapat dilihat dari nilai PSNR yang tinggi serta nilai MSE yang rendah, sehingga perubahan visual pada citra setelah proses penyisipan pesan tidak terlihat secara signifikan.

NO	Nama Gambar	PSNR LSB	MSE LSB	PSNR PVD	MSE PVD
1	Pengujian 1	72.47 dB	0.0037	67.85 dB	0.0107
2	Pengujian 2	72.45 dB	0.0037	67.33 dB	0.0120
3	Pengujian 3	86.33 dB	0.0002	81.78 dB	0.0004
4	Pengujian 4	74.56 dB	0.0023	69.37 dB	0.0075
5	Pengujian 5	72.45 dB	0.0037	59.98 dB	0.0654
6	Pengujian 6	72.94 dB	0.0033	66.59 dB	0.0143
7	Pengujian 7	72.45 dB	0.0037	66.62 dB	0.0142

8	Pengujian 8	73.00 dB	0.0033	67.12 dB	0.0126
9	Pengujian 9	72.76 dB	0.0034	66.36 dB	0.0150
10	Pengujian 10	73.03 dB	0.0032	66.12 dB	0.0159
11	Pengujian 11	72.48 dB	0.0037	67.25 dB	0.0122
12	Pengujian 12	72.46 dB	0.0037	66.29 dB	0.0153
13	Pengujian 13	72.49 dB	0.0037	66.23 dB	0.0155
14	Pengujian 14	72.49 dB	0.0037	67.96 dB	0.0104
15	Pengujian 15	72.47 dB	0.0037	66.92 dB	0.0132
16	Pengujian 16	71.76 dB	0.0043	67.55 dB	0.0114
17	Pengujian 17	72.49 dB	0.0037	66.33 dB	0.0151
18	Pengujian 18	72.50 dB	0.0037	66.83 dB	0.0135
19	Pengujian 19	71.96 dB	0.0041	65.55 dB	0.0181
20	Pengujian 20	72.46 dB	0.0037	66.65 dB	0.0141
21	Pengujian 21	72.47 dB	0.0037	62.61 dB	0.0356
22	Pengujian 22	72.41 dB	0.0037	66.96 dB	0.0131
23	Pengujian 23	72.29 dB	0.0038	66.82 dB	0.0135
24	Pengujian 24	72.45 dB	0.0037	66.58 dB	0.0143
25	Pengujian 25	73.09 dB	0.0032	66.75 dB	0.0137
26	Pengujian 26	73.03 dB	0.0032	66.45 dB	0.0147
27	Pengujian 27	72.44 dB	0.0037	66.61 dB	0.0142
28	Pengujian 28	72.45 dB	0.0037	66.10 dB	0.0160
29	Pengujian 29	72.31 dB	0.0038	66.90 dB	0.0133

30	Pengujian 30	72.59 dB	0.0036	61.22 dB	0.0491
31	Pengujian 31	82.38 dB	0.0004	76.61 dB	0.0014
32	Pengujian 32	72.48 dB	0.0037	66.65 dB	0.0141
33	Pengujian 33	72.43 dB	0.0037	66.03 dB	0.0162
34	Pengujian 34	72.42 dB	0.0037	67.39 dB	0.0119
35	Pengujian 35	72.38 dB	0.0038	66.05 dB	0.0161
36	Pengujian 36	72.45 dB	0.0037	66.93 dB	0.0132
37	Pengujian 37	72.51 dB	0.0036	66.05 dB	0.0161
38	Pengujian 38	72.42 dB	0.0037	65.34 dB	0.0190
39	Pengujian 39	72.44 dB	0.0037	66.17 dB	0.0157
40	Pengujian 40	72.11 dB	0.0040	67.19 dB	0.0124
41	Pengujian 41	72.74 dB	0.0035	67.96 dB	0.0104
42	Pengujian 42	72.48 dB	0.0037	67.08 dB	0.0127
43	Pengujian 43	72.45 dB	0.0037	66.08 dB	0.0161
44	Pengujian 44	72.51 dB	0.0036	66.28 dB	0.0153
45	Pengujian 45	72.50 dB	0.0037	66.38 dB	0.0150
46	Pengujian 46	72.83 dB	0.0034	66.45 dB	0.0147
47	Pengujian 47	72.44 dB	0.0037	66.29 dB	0.0153
48	Pengujian 48	72.98 dB	0.0033	67.03 dB	0.0129
49	Pengujian 49	72.32 dB	0.0038	67.02 dB	0.0129
50	Pengujian 50	72.46 dB	0.0037	67.38 dB	0.0119

Table 1. Hasil PSNR dan MSE

Berdasarkan Tabel 1. hasil pengujian yang dilakukan terhadap 50 citra digital menunjukkan bahwa metode *Least Significant Bit* (LSB) maupun *Pixel Value Differencing* (PVD) mampu menghasilkan citra stego dengan kualitas yang baik. Hal ini dapat dilihat dari nilai PSNR yang cenderung tinggi serta nilai MSE yang relatif rendah pada setiap data pengujian.

Metode LSB menghasilkan nilai PSNR yang cukup stabil, dengan rentang antara 71,76 dB sampai 86,33 dB dan nilai MSE berkisar antara 0,0002 hingga 0,0043. Sementara itu, metode PVD memiliki variasi nilai yang lebih beragam, dengan nilai PSNR berada pada rentang 59,98 dB hingga 81,78 dB dan nilai MSE antara 0,0004 sampai 0,0654.

Berdasarkan hasil tersebut, metode LSB dapat dikatakan lebih konsisten dalam mempertahankan kualitas citra stego dibandingkan metode PVD. Meskipun demikian, kedua metode masih mampu menjaga tampilan visual citra sehingga perbedaan antara citra asli dan citra stego tidak mudah dikenali secara langsung. Selain itu, hasil pengujian juga memperlihatkan bahwa kualitas visual citra yang baik tidak selalu menjamin pesan dapat dikembalikan secara utuh. Oleh karena itu, pemeriksaan integritas pesan setelah proses *extraction* tetap diperlukan untuk memastikan kesesuaian antara *file* hasil *extraction* dengan *file* asli yang disisipkan.

4.3.6 Pengujian Integritas Pesan

Pengujian integritas pesan dilakukan untuk mengetahui kemampuan sistem dalam mempertahankan *file* SQL agar tetap utuh setelah melalui proses *embedding* dan *extraction* menggunakan metode *Least Significant Bit* (LSB) dan

Pixel Value Differencing (PVD). Pengujian dilakukan dengan membandingkan *file* SQL hasil *extraction* dengan *file* SQL asli yang sebelumnya telah disisipkan ke dalam citra digital.

Dalam proses pengujian, sistem secara otomatis melakukan pemeriksaan pesan setelah proses *extraction* selesai dijalankan. Pemeriksaan ini bertujuan untuk memastikan bahwa *file* SQL hasil *extraction* masih sesuai dengan *file* asli dan tidak mengalami perubahan data selama proses penyisipan maupun pengambilan pesan dilakukan.

Berdasarkan hasil pengujian yang telah dilakukan, metode *Least Significant Bit* (LSB) mampu menjaga integritas pesan dengan baik pada seluruh data uji yang digunakan. Seluruh *file* SQL hasil *extraction* berhasil dikembalikan sesuai dengan *file* asli tanpa ditemukan adanya perubahan data.

Sedangkan pada metode *Pixel Value Differencing* (PVD), masih ditemukan beberapa hasil *extraction* yang mengalami perubahan data. Dari 50 data pengujian yang dilakukan, tidak seluruh *file* SQL hasil *extraction* dapat dikembalikan sesuai dengan *file* asli. Kondisi tersebut menunjukkan bahwa kualitas visual citra yang baik tidak selalu menjamin bahwa pesan dapat dipulihkan secara utuh setelah proses *extraction* dilakukan.

No	Nama Gambar	Status Pesan LSB	Status Pesan PVD
1	Pengujian 1	Sesuai	Tidak Sesuai
2	Pengujian 2	Sesuai	Sesuai
3	Pengujian 3	Sesuai	Sesuai

4	Pengujian 4	Sesuai	Tidak Sesuai
5	Pengujian 5	Sesuai	Tidak Sesuai
6	Pengujian 6	Sesuai	Sesuai
7	Pengujian 7	Sesuai	Sesuai
8	Pengujian 8	Sesuai	Tidak Sesuai
9	Pengujian 9	Sesuai	Sesuai
10	Pengujian 10	Sesuai	Tidak Sesuai
11	Pengujian 11	Sesuai	Sesuai
12	Pengujian 12	Sesuai	Sesuai
13	Pengujian 13	Sesuai	Sesuai
14	Pengujian 14	Sesuai	Sesuai
15	Pengujian 15	Sesuai	Tidak Sesuai
16	Pengujian 16	Sesuai	Tidak Sesuai
17	Pengujian 17	Sesuai	Sesuai
18	Pengujian 18	Sesuai	Sesuai
19	Pengujian 19	Sesuai	Sesuai
20	Pengujian 20	Sesuai	Sesuai
21	Pengujian 21	Sesuai	Tidak Sesuai
22	Pengujian 22	Sesuai	Tidak Sesuai
23	Pengujian 23	Sesuai	Tidak Sesuai
24	Pengujian 24	Sesuai	Sesuai
25	Pengujian 25	Sesuai	Sesuai

26	Pengujian 26	Sesuai	Sesuai
27	Pengujian 27	Sesuai	Sesuai
28	Pengujian 28	Sesuai	Sesuai
29	Pengujian 29	Sesuai	Sesuai
30	Pengujian 30	Sesuai	Tidak Sesuai
31	Pengujian 31	Sesuai	Sesuai
32	Pengujian 32	Sesuai	Sesuai
33	Pengujian 33	Sesuai	Sesuai
34	Pengujian 34	Sesuai	Sesuai
35	Pengujian 35	Sesuai	Sesuai
36	Pengujian 36	Sesuai	Sesuai
37	Pengujian 37	Sesuai	Sesuai
38	Pengujian 38	Sesuai	Tidak Sesuai
39	Pengujian 39	Sesuai	Tidak Sesuai
40	Pengujian 40	Sesuai	Tidak Sesuai
41	Pengujian 41	Sesuai	Tidak Sesuai
42	Pengujian 42	Sesuai	Sesuai
43	Pengujian 43	Sesuai	Sesuai
44	Pengujian 44	Sesuai	Sesuai
45	Pengujian 45	Sesuai	Sesuai
46	Pengujian 46	Sesuai	Tidak Sesuai
47	Pengujian 47	Sesuai	Tidak Sesuai

48	Pengujian 48	Sesuai	Sesuai
49	Pengujian 49	Sesuai	Tidak Sesuai
50	Pengujian 50	Sesuai	Sesuai

Table 2. Hasil Pengujian Integrasi Pesan

Berdasarkan Tabel 2. metode *Least Significant Bit* (LSB) menunjukkan kemampuan yang lebih baik dalam menjaga keutuhan pesan dibandingkan metode *Pixel Value Differencing* (PVD). Hal ini terlihat dari seluruh *file* SQL hasil *extraction* pada metode LSB yang berhasil dikembalikan sesuai dengan *file* asli, sehingga tingkat keberhasilan integritas pesannya mencapai 100%.

Berbeda dengan metode LSB, hasil pengujian pada metode PVD menunjukkan bahwa tidak semua *file* SQL dapat diekstraksi kembali secara utuh. Dari 50 data pengujian yang dilakukan, sebanyak 32 *file* SQL hasil *extraction* dinyatakan sesuai dengan *file* asli, sedangkan 18 *file* lainnya mengalami perubahan data. Kondisi tersebut mengindikasikan bahwa metode PVD lebih sensitif terhadap perubahan yang terjadi selama proses penyisipan dan pengambilan kembali pesan.

Berdasarkan table tersebut, dapat diketahui bahwa metode LSB memiliki tingkat kestabilan yang lebih baik dalam mempertahankan integritas pesan. Meskipun metode PVD mampu menghasilkan kualitas visual citra stego yang tetap baik, proses *extraction* pada metode ini masih berpotensi menyebabkan perubahan pada pesan yang dikembalikan sehingga perlu diperhatikan dalam penerapannya.

4.3.7 Analisis Perbandingan Metode LSB dan PVD

Berdasarkan hasil pengujian yang telah dilakukan, metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) sama-sama mampu melakukan proses *embedding* dan *extraction file* SQL ke dalam citra digital dengan kualitas citra stego yang baik. Hal tersebut dapat dilihat dari nilai PSNR yang tinggi serta nilai MSE yang rendah pada seluruh hasil pengujian yang dilakukan.

Metode *Least Significant Bit* (LSB) menunjukkan tingkat kestabilan yang lebih baik dalam menjaga integritas pesan. Seluruh *file* SQL hasil *extraction* menggunakan metode LSB berhasil dikembalikan sesuai dengan *file* asli tanpa mengalami perubahan data. Selain itu, dari hasil pengujian pada sistem yang dikembangkan, metode LSB juga menghasilkan kapasitas penyisipan yang lebih besar dibandingkan metode PVD pada citra yang digunakan.

Di sisi lain, metode *Pixel Value Differencing* (PVD) juga mampu menghasilkan citra stego dengan kualitas visual yang baik. Hal tersebut ditunjukkan oleh nilai PSNR yang cukup tinggi pada sebagian besar data pengujian yang telah dilakukan. Akan tetapi, hasil pemeriksaan integritas pesan memperlihatkan bahwa tidak semua *file* SQL hasil *extraction* dapat dikembalikan dalam kondisi yang sama seperti *file* aslinya. Dari 50 data pengujian, terdapat 18 data yang mengalami perubahan setelah proses *extraction* meskipun tampilan visual citra stego masih terlihat baik.

Hasil tersebut menunjukkan bahwa kualitas visual citra yang baik belum tentu diikuti dengan keberhasilan pengembalian pesan secara utuh. Secara keseluruhan, metode LSB memiliki tingkat kestabilan yang lebih baik dalam

mempertahankan integritas pesan. Sementara itu, metode PVD tetap mampu menjaga kualitas visual citra stego, namun masih terdapat kemungkinan terjadinya perubahan data pada pesan yang diekstraksi kembali.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil perancangan, implementasi sistem, serta pengujian yang telah dilakukan pada penelitian ini, maka dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Sistem steganografi citra digital menggunakan metode *Least Significant Bit* (LSB) dan *Pixel Value Differencing* (PVD) berhasil dirancang dan diimplementasikan untuk melakukan proses penyisipan pesan (*embedding*) dan pengambilan kembali pesan (*extraction*) berupa *file* SQL pada citra digital. Sistem yang dikembangkan juga mampu melakukan deteksi metode steganografi, analisis kapasitas penyisipan, pengukuran kualitas citra menggunakan parameter Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE), serta pemeriksaan integritas pesan hasil *extraction*.
2. Berdasarkan hasil pengujian integritas pesan terhadap 50 data citra uji, metode *Least Significant Bit* (LSB) menunjukkan tingkat keberhasilan yang lebih baik dalam mempertahankan keutuhan pesan. Seluruh *file* SQL hasil *extraction* menggunakan metode LSB berhasil dikembalikan sesuai dengan *file* asli sehingga tingkat keberhasilannya mencapai 100%.

Sementara itu, pada metode *Pixel Value Differencing* (PVD), sebanyak 32 *file* SQL hasil *extraction* dinyatakan sesuai dengan *file* asli, sedangkan 18 *file* lainnya mengalami perubahan setelah proses *extraction* dilakukan.

3. Berdasarkan pengujian kualitas citra stego, kedua metode mampu menghasilkan kualitas visual citra yang baik setelah proses penyisipan pesan. Metode LSB menghasilkan nilai PSNR yang lebih stabil dengan rentang 71,76 dB hingga 86,33 dB dan nilai MSE antara 0,0002 hingga 0,0043. Adapun metode PVD menghasilkan nilai PSNR antara 59,98 dB hingga 81,78 dB dengan nilai MSE antara 0,0004 hingga 0,0654. Hasil tersebut menunjukkan bahwa kualitas visual citra stego yang baik tidak selalu menjamin keberhasilan pengembalian pesan secara utuh.
4. Secara keseluruhan, metode *Least Significant Bit* (LSB) menunjukkan performa yang lebih stabil dalam mempertahankan integritas pesan dan keberhasilan proses *extraction*. Sementara itu, metode *Pixel Value Differencing* (PVD) tetap mampu menghasilkan kualitas visual citra stego yang baik, namun masih terdapat kemungkinan terjadinya perubahan data pada pesan yang diekstraksi. Oleh karena itu, pemilihan metode steganografi dapat disesuaikan dengan kebutuhan pengguna, baik dengan mengutamakan keutuhan pesan maupun kualitas visual citra stego yang dihasilkan.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dijadikan bahan pengembangan untuk penelitian maupun sistem di masa mendatang yaitu :

1. Penelitian selanjutnya diharapkan dapat membandingkan metode steganografi lainnya untuk mengetahui tingkat keamanan, kapasitas penyisipan, serta kestabilan proses *extraction* yang lebih optimal.
2. Sistem steganografi dapat dikembangkan dengan menambahkan proses enkripsi sebelum tahap *embedding* agar keamanan data yang disisipkan menjadi lebih baik.
3. Pengujian pada penelitian berikutnya disarankan menggunakan lebih banyak variasi citra digital dengan karakteristik yang berbeda sehingga hasil pengujian yang diperoleh menjadi lebih beragam dan akurat.
4. Metode *Pixel Value Differencing* (PVD) dapat dikembangkan lebih lanjut untuk meningkatkan kestabilan proses *extraction* sehingga kemungkinan terjadinya perubahan data pada *file* hasil *extraction* dapat dikurangi.
5. Sistem dapat dikembangkan agar mampu mendukung berbagai jenis format *file* selain *file* SQL sehingga penggunaan sistem steganografi menjadi lebih fleksibel dan luas.

DAFTAR PUSTAKA

Akmal, R. A., Furqan, Mhd. F., & Kurniawan R, R. (2023). Implementasi Metode *Least Significant Bit* Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital. *G-Tech: Jurnal Teknologi Terapan*, *7*(2), 543–553. https://doi.org/10.33379/gtech.v7i2.2300

Dewi, & Munir. (2023). *JIP (Jurnal Informatika Polinema) PERBANDINGAN BERBAGAI METODE STEGANOGRAFI PADA CITRA DIGITAL*.

Firdaus, M. A., & Rahmatulloh, A. (2025). IMPLEMENTASI STEGANOGRAFI CITRA DIGITAL LSB MENGGUNAKAN ENKRIPSI AES-256 DAN *EMBEDDING* PSEUDORANDOM. *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(1). https://doi.org/10.23960/jitet.v13i1.5620

Gustiawan, A., Wahyudi, J., Suryana, E., Dehasen Bengkulu, U., Meranti, J., No, R., Lebar, S., & Indonesia, B. (2023). Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode *Pixel Value Differencing* Oleh : Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode *Pixel Value Differencing*. *JUKI : Jurnal Komputer Dan Informatika*, *5*.

Hakim, F. N., & Sholikhan, M. (2024). Enhancing Data Security through Digital Image Steganography: An Implementation of the Two *Least Significant Bit*s (2LSB) Method. *International Journal of Graphic Design*, *2*(2), 222–235. https://doi.org/10.51903/ijgd.v2i2.2124

Lasarus. (2021). *Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)*.

Purbaningrum, A., Silvi Amalia, K., Ady Saputro, I., AMIKOM Surakarta, S., & Tengah, J. (2023). *Penerapan Metode Least Significant Bit (LSB) dalam Menyisipkan Pesan Rahasia pada Citra Digital: Sebuah Pendekatan Steganografi*.

Satria, & Jovi. (2022). STEGANOGRAFI METODE *LEAST SIGNIFICANT BIT* (LSB) DAN END OF *FILE* (EoF) PADA KEAMANAN DATA DIGITAL. *Glugur Kota, Kec. Medan Bar*, *6*(2).

Suhada, S., Laksono, A. W., & Zakaria, A. (2024). *IMPLEMENTASI METODE LEAST SIGNIFICANT BIT (LSB) DALAM TEKNIK STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN MATLAB*. *4*(1).

Utomo, I., Mulyono, W., Kusumawati, Y., & Widyatmoko, K. (2022). *PERBANDINGAN DAN KOMBINASI KINERJA ALGORITMA LEAST SIGNIFICANT BIT DENGAN PIXEL VALUE DIFFERENCING PADA STEGANOGRAFI CITRA WARNA*. http://sipi.usc.edu/database/

Wanandi dan Reza. (2024). *IMPLEMENTASI SISTEM STEGANOGRAFI CITRA DENGAN METODE SUBTITUSI LSB (LEAST SIGNIFICANT BIT)*. *2*(11), 10–20. https://ejournal.warunayama.org/kohesi