**Seminar Nasional Informatika (SENATIKA)**
**Prosiding Senatika 2025** **QRSBN:62-0151-02942-8**

# Rancang Bangun Aplikasi Stegano Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES)

**Sihar Daniel Pardede[1], Roni Sanjaya[2]**
[1,2]Fakultas Ilmu KomputerInstitutBisnis dan Teknologi Pelita Indonesia
e-mail: [1]sihar.daniel@student.pelitaindonesia.ac.id, [2]roni@lecturer.pelitaindonesia.ac.id

***Abstrak***

*Perkembangan teknologi informasi yang semakin pesat membawa tantangan baru dalam hal keamanan data digital. Berbagai kasus kebocoran data menunjukkan pentingnya penerapan sistem keamanan yang tidak hanya melindungi isi pesan, tetapi juga menyamarkan keberadaannya. Penelitian ini bertujuan untuk merancang dan membangun aplikasi steganografi dengan menggabungkan metode Least Significant Bit (LSB) untuk penyisipan pesan pada media citra digital dan algoritma kriptografi Advanced Encryption Standard (AES) 128-bit untuk menjaga kerahasiaan pesan. Aplikasi ini dikembangkan berbasis desktop dengan menggunakan bahasa pemrograman PHP Desktop dan diuji melalui metode Black Box Testing serta User Acceptance Test (UAT). Hasil penelitian menunjukkan bahwa aplikasi dapat menjalankan fungsi enkripsi, penyisipan pesan, ekstraksi, dan dekripsi dengan baik sesuai kebutuhan. Pengujian membuktikan bahwa kualitas citra setelah penyisipan tetap terjaga, dan pesan yang disembunyikan berhasil diekstraksi kembali tanpa perubahan. Dengan demikian, aplikasi ini mampu meningkatkan keamanan data digital dan dapat diterapkan pada instansi pemerintahan maupun pengguna umum yang membutuhkan kerahasiaan komunikasi data.*

***Kata kunci:*** *Steganografi, Least Significant Bit (LSB), Advanced Encryption Standard (AES), Keamanan Data, Kriptografi..*

***Abstract***

*The rapid development of information technology has brought new challenges in securing digital data. Various cases of data breaches highlight the importance of implementing security systems that not only protect the content of messages but also conceal their existence. This research aims to design and develop a steganography application by combining the Least Significant Bit (LSB) method for embedding messages into digital image media and the Advanced Encryption Standard (AES) 128-bit cryptographic algorithm to maintain message confidentiality. The application was developed as a desktop-based system using PHP Desktop and tested through Black Box Testing and User Acceptance Testing (UAT). The results show that the application can successfully perform encryption, message embedding, extraction, and decryption according to the requirements. The testing also proved that the quality of the image after embedding remains intact, and the hidden message can be extracted accurately without alteration. Therefore, this application enhances digital data security and can be applied in governmental institutions as well as for general users who require confidentiality in data communication.*

***Keywords:*** *Steganography, Least Significant Bit (LSB), Advanced Encryption Standard (AES), Data Security, Cryptography.*

## 1. Pendahuluan

Perkembangan teknologi informasi yang semakin pesat pada era global-isasi telah membawa dampak signifikan terhadap cara manusia berinteraksi, berkomunikasi, serta bertukar informasi. Pertukaran data digital kini menjadi kebutuhan utama dalam berbagai bidang kehidupan, baik dalam dunia pen-didikan, bisnis, pemerintahan, maupun layanan publik. Internet sebagai jaringan global memang memberikan kemudahan dalam berbagi informasi tanpa batas ruang dan waktu. Namun, di balik kemudahan tersebut, muncul tantangan besar dalam hal keamanan informasi.

Kasus-kasus kebocoran data di Indonesia dalam beberapa tahun tera-khir menunjukkan betapa rentannya informasi digital jika tidak dikelola dengan baik. Misalnya, insiden kebocoran data pribadi dari instansi pemerintah dan lembaga pelayanan publik yang tersebar di internet telah menimbulkan keresahan masyarakat. Kondisi ini menegaskan bahwa kea-manan data bukan hanya kebutuhan teknis, tetapi juga menyangkut aspek privasi, kepercayaan publik, serta citra lembaga [1]. Jika tidak ada langkah pencegahan yang memadai, maka kerahasiaan doku-men penting dan informasi strategis dapat dengan mudah disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dalam konteks perlindungan data digital, kriptografi merupakan salah satu teknik yang telah lama digunakan. Kriptografi mempelajari cara menyandikan pesan agar hanya bisa dibaca oleh pihak yang memiliki kunci tertentu. Salah satu algoritma kriptografi modern yang paling banyak digunakan adalah Advanced Encryption Standard (AES). Dengan panjang kunci 128 bit, algoritma ini terbukti kuat dan digunakan di berbagai sistem keamanan data. Namun demikian, kelemahan utama kriptografi adalah ben-tuk ciphertext yang dihasilkan masih jelas terlihat berbeda dari data biasa. Hal ini dapat menimbulkan kecurigaan pihak ketiga, walaupun isi pesan tetap aman [2].

Sebagai alternatif lain, dikenal metode steganografi, yaitu teknik me-nyembunyikan pesan ke dalam media lain seperti gambar, audio, atau video. Teknik ini memiliki keunggulan utama, yaitu tidak hanya menjaga kerahasi-aan isi pesan, tetapi juga menyamarkan keberadaan pesan itu sendiri. Metode Least Significant Bit (LSB) merupakan salah satu teknik steganografi yang paling sederhana dan populer, dengan cara menyisipkan pesan ke da-lam bit paling rendah suatu citra digital. Teknik ini relatif mudah diimplemen-tasikan dan tidak merusak kualitas visual gambar secara signifikan [3]. Akan tetapi, jika digunakan tanpa enkripsi, pesan yang dis-embunyikan masih bisa diekstraksi oleh pihak yang paham teknik steganalisis.

Karena itu, muncul gagasan untuk menggabungkan kriptografi dan ste-ganografi dalam satu sistem. Dengan kombinasi ini, pesan terlebih dahulu dienkripsi menggunakan algoritma AES, lalu hasil enkripsi (ciphertext) disisipkan ke dalam citra digital dengan metode LSB. Dengan cara ini, mes-kipun pesan berhasil ditemukan, isi pesan tetap tidak dapat dibaca tanpa kunci enkripsi. Pendekatan ini membuat keamanan data menjadi berlapis dan lebih sulit ditembus. Sejumlah penelitian sebelumnya telah membuktikan efektivitas kombinasi ini. Misalnya, penelitian oleh [4] mengimplementasikan metode LSB dengan algoritma AES untuk pengamanan data digital, dan hasilnya menunjukkan bahwa kombinasi kedua metode ini lebih aman dibandingkan penggunaan metode tunggal. Selanjutnya, [5] membuktikan bahwa aplikasi penyembunyian pe-san dengan metode AES dan Enhanced LSB lebih tahan terhadap analisis statistik. Penelitian oleh [6] juga menegaskan bahwa kombinasi AES dan LSB mampu meningkatkan ketahanan sistem terhadap serangan brute force. Bahkan, [7] menunjukkan bahwa pen-erapan kombinasi LSB dan AES pada citra digital mampu menjaga integritas serta kerahasiaan pesan dengan tingkat keberhasilan ekstraksi mencapai 100%. Penelitian lain oleh [8] menambahkan bahwa metode hybrid kriptografi–steganografi dapat memperkuat keamanan data pada lingkungan pemerintahan yang sering menangani dokumen sensitif.

Berdasarkan permasalahan di atas, penelitian ini diarahkan untuk merancang dan membangun aplikasi steganografi berbasis metode LSB dan algoritma kriptografi AES. Aplikasi ini akan diuji langsung pada Kantor Lurah Tanjung Rhu, yang memiliki kebutuhan nyata dalam

menjaga kerahasiaan data administrasi kependudukan dan komunikasi internal. Dengan adanya aplikasi ini, diharapkan Kantor Lurah dapat memiliki sistem keamanan infor-masi yang lebih baik, yang tidak hanya melindungi kerahasiaan isi pesan, tetapi juga menyamarkan keberadaan pesan itu sendiri. Dengan demikian, aplikasi ini tidak hanya relevan bagi kantor lurah, tetapi juga dapat menjadi model penerapan teknologi keamanan data pada instansi pemerintahan lainnya di Indonesia.

## 2. Metode Penelitian

### 2.1 Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Kantor Lurah Tanjung Rhu, Kecamatan Limapuluh, Kota Pekanbaru sebagai lokasi studi kasus, karena instansi ini memiliki kebutuhan tinggi dalam menjaga kerahasiaan data administrasi kependudukan dan komunikasi internal. Selain itu, sebagian besar proses pelayanan publik di instansi pemerintahan saat ini sudah terdigitalisasi, sehingga isu keamanan data menjadi sangat relevan.

Untuk proses perancangan aplikasi, penelitian dilaksanakan di lingkungan pengembangan pribadi peneliti dengan memanfaatkan perangkat komputer yang memiliki spesifikasi memadai, yaitu:

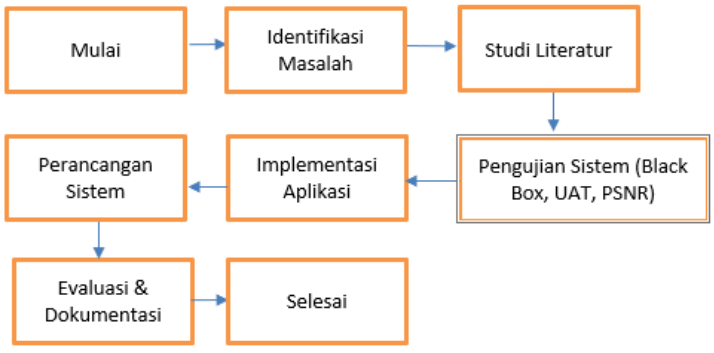
1. RAM: minimal 8 GB
2. Penyimpanan: SSD 256 GB
3. Sistem Operasi: Windows 10/11
4. Tools pengembangan: Visual Studio Code, PHP Desktop, serta library pendukung kriptografi dan manipulasi citra

Waktu penelitian berlangsung selama lima bulan, dimulai dari Agustus 2024 hingga Desember 2024, yang mencakup tahapan:

a. Identifikasi masalah dan studi literatur (Agustus 2024)
b. Perancangan sistem dan desain aplikasi (September 2024)
c. Implementasi algoritma LSB dan AES (Oktober 2024)
d. Pengujian aplikasi dan analisis data (November 2024)
e. Penyusunan laporan akhir (Desember 2024)

### 2.2 Kerangka Penelitian

Kerangka penelitian ini menggambarkan alur sistematis dalam merancang dan membangun aplikasi steganografi berbasis Least Significant Bit (LSB) dan kriptografi Advanced Encryption Standard (AES). Aplikasi ini dibuat untuk menyisipkan pesan rahasia ke dalam citra digital sekaligus mengenkripsi pesan agar lebih aman.




Gambar 1. Kerangka Penelitian

1. Identifikasi Masalah dan Tujuan
   Memahamu pentingnya pengamanan data digital serta perlunya penerapan metode steganografi dan kriptografi secara bersamaan.
2. Studi Literatur

Mengumpulkan teori dan penelitian terdahulu tentang LSB, AES, steganografi, kriptografi, dan teknik pengujian sistem.

3. Perancangan Sistem
   Mendesain sistem steganografi yang terintegrasi dengan algoritma AES, meliputi desain antarmuka, alur enkripsi, penyisipan, serta ekstraksi pesan.
4. Implementasi Aplikasi
   Membuat aplikasi desktop berbasis PHP yang dapat mengenkripsi pesan teks menggunakan AES-128 bit lalu menyisipkannya ke dalam gambar dengan metode LSB.
5. Pengujian Sistem
   Menguji aplikasi dari aspek fungsionalitas, performa, dan keamanan menggunakan teknik black-box testing, user acceptance testing, serta analisis kualitas citra.
6. Evaluasi dan Dokumentasi
   Mengevaluasi hasil pengujian, menganalisis tingkat keberhasilan sistem, serta menyusun dokumentasi penelitian.

### 2.3 Metode Penelitian

Penelitian ini menggunakan pendekatan Research and Development (R&D) yang bertujuan untuk menghasilkan sebuah produk perangkat lunak berupa aplikasi steganografi dengan metode Least Significant Bit (LSB) yang dipadukan dengan algoritma kriptografi Advanced Encryption Standard (AES). Metode R&D dipilih karena penelitian ini tidak hanya menganalisis permasalahan, tetapi juga menghasilkan sebuah aplikasi yang bisa dimanfaatkan secara langsung sebagai solusi dalam meningkatkan keamanan data digital.

Secara umum, tahapan metode R&D yang digunakan dalam penelitian ini diadaptasi menjadi beberapa langkah sebagai berikut:

1. Identifikasi Potensi dan Masalah
   Pada tahap ini dilakukan identifikasi permasalahan yang terjadi terkait keamanan data digital, khususnya pada instansi pemerintahan seperti di Kantor Lurah Tanjung Rhu, Kecamatan Limapuluh, Kota Pekanbaru. Permasalahan yang muncul adalah masih banyaknya data penting yang rentan disalahgunakan atau bocor ketika tidak dilindungi dengan mekanisme keamanan yang baik. Hal ini menjadi potensi sekaligus masalah yang mendorong penelitian ini dilakukan.
2. Pengumpulan Informasi
   Tahap berikutnya adalah melakukan studi literatur dengan menelaah berbagai sumber, baik berupa jurnal, buku, maupun penelitian terdahulu, yang berhubungan dengan steganografi, metode LSB, serta kriptografi AES. Informasi ini menjadi dasar dalam memahami konsep serta memilih pendekatan terbaik untuk mengembangkan aplikasi.
3. Perancangan Produk (Desain Sistem)
   Pada tahap ini dibuat rancangan aplikasi yang akan dibangun, meliputi arsitektur sistem, diagram alur proses, desain antarmuka pengguna (user interface), serta pemetaan integrasi antara algoritma kriptografi AES dan metode steganografi LSB. Perancangan dilakukan secara sistematis agar aplikasi yang dihasilkan memiliki fungsi yang jelas, mudah digunakan, dan sesuai dengan kebutuhan pengguna.
4. Implementasi Sistem
   Setelah perancangan selesai, tahap implementasi dilakukan dengan membangun aplikasi menggunakan bahasa pemrograman desktop (Java). Proses implementasi mencakup pengkodean algoritma AES untuk enkripsi/dekripsi serta integrasi metode LSB untuk penyisipan data ke dalam media gambar.
5. Pengujian Sistem
   Pengujian aplikasi dilakukan untuk memastikan bahwa sistem yang dibangun berjalan sesuai dengan tujuan. Penelitian ini menggunakan Black Box Testing untuk menguji setiap fungsi aplikasi, seperti proses enkripsi, penyisipan data, ekstraksi data, serta dekripsi. Selain itu, dilakukan pula User Acceptance Testing (UAT) dengan melibatkan

beberapa pengguna untuk menilai apakah aplikasi mudah digunakan, bermanfaat, dan sesuai kebutuhan.

6. Evaluasi dan Penyempurnaan Produk
   Berdasarkan hasil pengujian, dilakukan evaluasi menyeluruh terhadap kinerja aplikasi. Jika ditemukan kekurangan, maka dilakukan perbaikan agar sistem menjadi lebih optimal dan siap digunakan.
7. Produk Akhir
   Tahap terakhir adalah menghasilkan produk akhir berupa aplikasi steganografi berbasis desktop dengan metode LSB yang dipadukan dengan algoritma AES. Produk ini diharapkan mampu menjadi solusi alternatif dalam menjaga kerahasiaan data digital.

### 2.3 Pengumpulan Data

Data dikumpulkan menggunakan pendekatan kualitatif dan kuantitatif dengan teknik:

1. Studi Literatur – memperoleh teori dan referensi dari buku, jurnal, serta penelitian terdahulu terkait LSB, AES, dan pengamanan data digital.
2. Wawancara Terstruktur – dengan akademisi dan praktisi di bidang keamanan informasi untuk memahami kebutuhan sistem.
3. Observasi Langsung – mengamati proses kerja aplikasi mulai dari enkripsi, penyisipan, hingga ekstraksi pesan.
4. Eksperimen – melakukan uji coba aplikasi dengan berbagai variasi gambar (format JPG/PNG, ukuran berbeda) dan panjang pesan.

### 2.4 Teknik Pengujian

Pengujian aplikasi dilakukan dengan beberapa metode Black Box Testing. Untuk menguji apakah fungsi sistem bekerja sesuai spesifikasi, tanpa memperhatikan kode program.

1. User Acceptance Testing (UAT)
   Dilakukan dengan meminta pengguna mencoba aplikasi secara langsung untuk menilai kemudahan penggunaan dan efektivitas sistem.
1. Perbandingan Hasil
   Membandingkan citra hasil steganografi dengan pesan terenkripsi dan pesan biasa untuk mengevaluasi tingkat keamanan.
2. Analisis Kualitas Citra (PSNR – Peak Signal to Noise Ratio)
   Digunakan untuk mengukur perbedaan kualitas gambar sebelum dan sesudah penyisipan pesan. Semakin tinggi nilai PSNR, semakin baik kualitas citra hasil.

### 2.4 Perhitungan Pengujian Manual

Sebagai bentuk validasi, dilakukan perhitungan manual untuk menghitung kapasitas penyisipan data serta nilai PSNR.

Kapasitas Penyimpanan Data dalam Gambar (bits): Kapasitas=(M×N)×3 dengan M = lebar gambar, N = tinggi gambar, dan 3 = jumlah channel RGB.

Rumus PSNR (dB):

$$PSNR = 10 \log 10 \frac{MAX2}{MSE} \quad (1)$$

dengan MAX = nilai intensitas maksimum (255 untuk citra 8-bit), MSE = mean squared error antara citra asli dan citra hasil penyisipan. Perhitungan manual ini dilakukan pada beberapa sampel gambar untuk memverifikasi hasil yang diperoleh dari sistem.

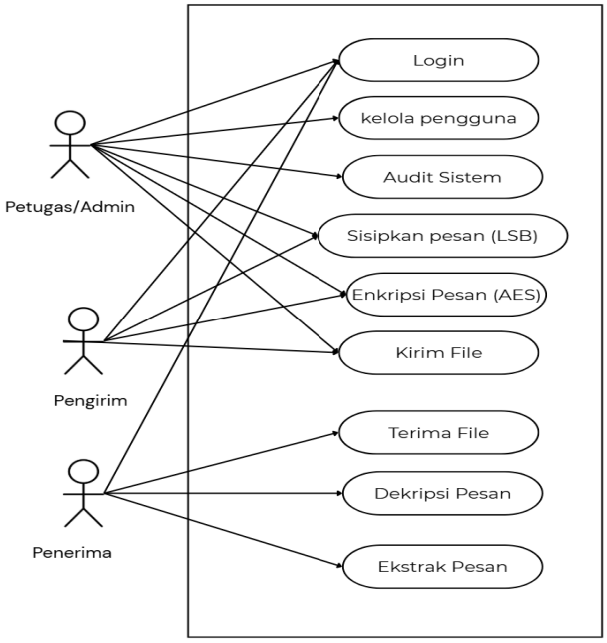
## 3. Hasil dan Pembahasan

### 3.1 Perancangan Sistem

a. *Use Case Diagram*

*Use case diagram* bekerja dengan cara mendeskripsikan tipikal interaksi antar pengguna dengan sistem melalui sebuah cerita yang menggambarkan bagaimana sebuah

sistem dipakai. Diagram ini tidak hanya menunjukkan siapa saja aktor yang terlibat, tetapi juga menjelaskan alur kegiatan, tujuan yang ingin dicapai, serta hubungan antara pengguna dan fungsi-fungsi utama yang ada di dalam sistem, sehingga memudahkan dalam memahami kebutuhan serta ruang lingkup dari sistem yang akan dibangun.



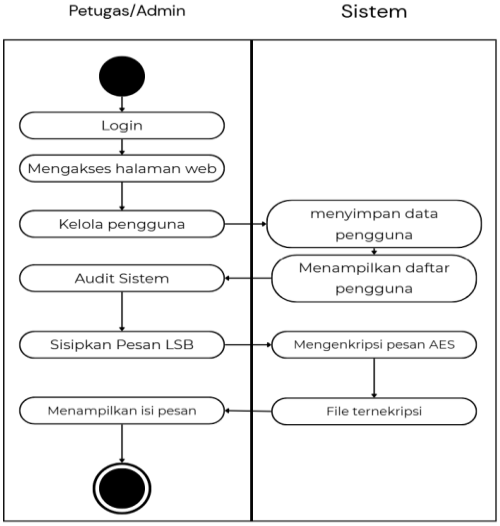

Gambar 2. *Use Case Diagram*

b. *Activity Diagram*

*Activity diagram* menggambarkan berbagai alur aktifitas dalam system yang sedang dirancang, bagaimana masing-masing alur berawal, decision yang mungkin terjadi dan bagaimana proses proses tersebut selesai. Berikut penggambaran activity diagram dari beberapa proses :

a. *Activity Diagram* Admin

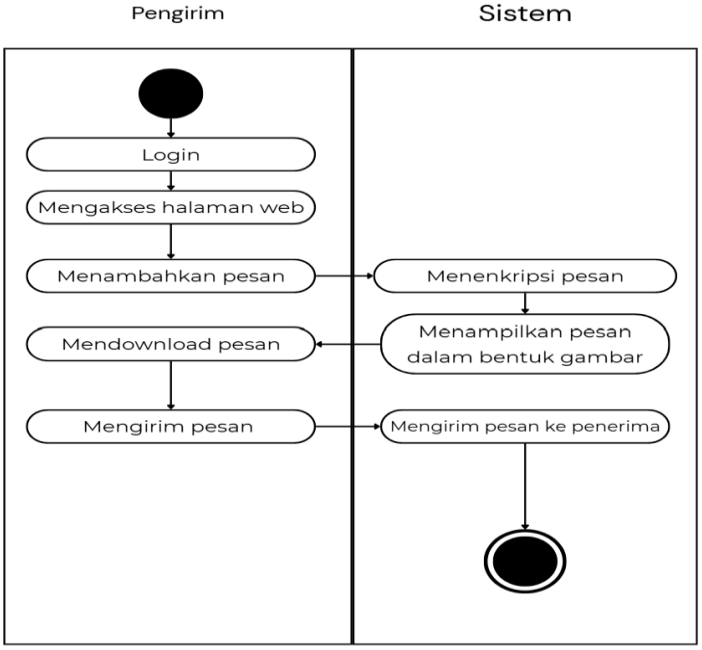
Activity diagram login admin ke Rancang Bangun Aplikasi Stegano Menggunakan Metode Least Significant Bit (Lsb) Dan Algoritma Kriptografi Advanced Encryption Standard (Aes). Untuk lebih jelasnya dapat dilihat pada activity diagram sebagai berikut.




Gambar 3. *Activity Diagram* Admin

b. *Activity Diagram* Pengirim

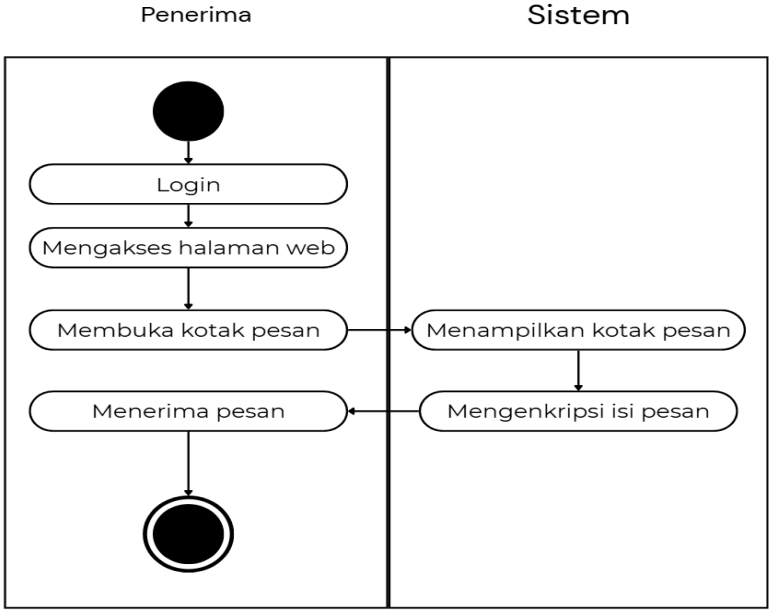
Activity diagrampengirim menginputkan pesan yang ada pada Rancang Bangun Aplikasi Stegano Menggunakan Metode Least Significant Bit (Lsb) Dan Algoritma Kriptografi Advanced Encryption Standard (Aes). Untuk lebih jelasnya dapat dilihat pada activity diagram sebagai berikut.




Gambar 4. *Activity Diagram* Pengirim

c. *Activity Diagram* Penerima

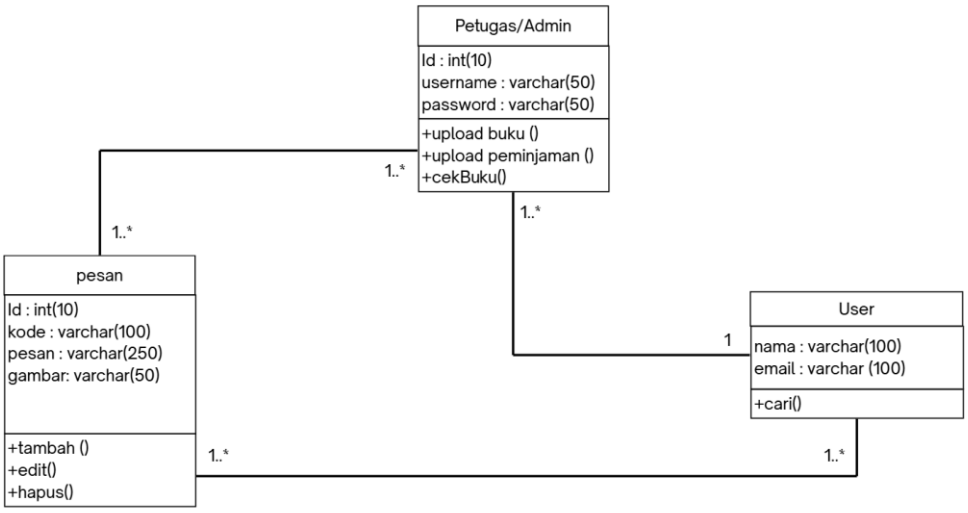
Activity penerima admin menerima pesan yang ada pada sistem Rancang Bangun Aplikasi Stegano Menggunakan Metode Least Significant Bit (Lsb) Dan Algoritma Kriptografi Advanced Encryption Standard (Aes). Untuk lebih jelasnya dapat dilihat pada activity diagram sebagai berikut.




Gambar 5. *Activity Diagram* Penerima

c. *Class Diagram*

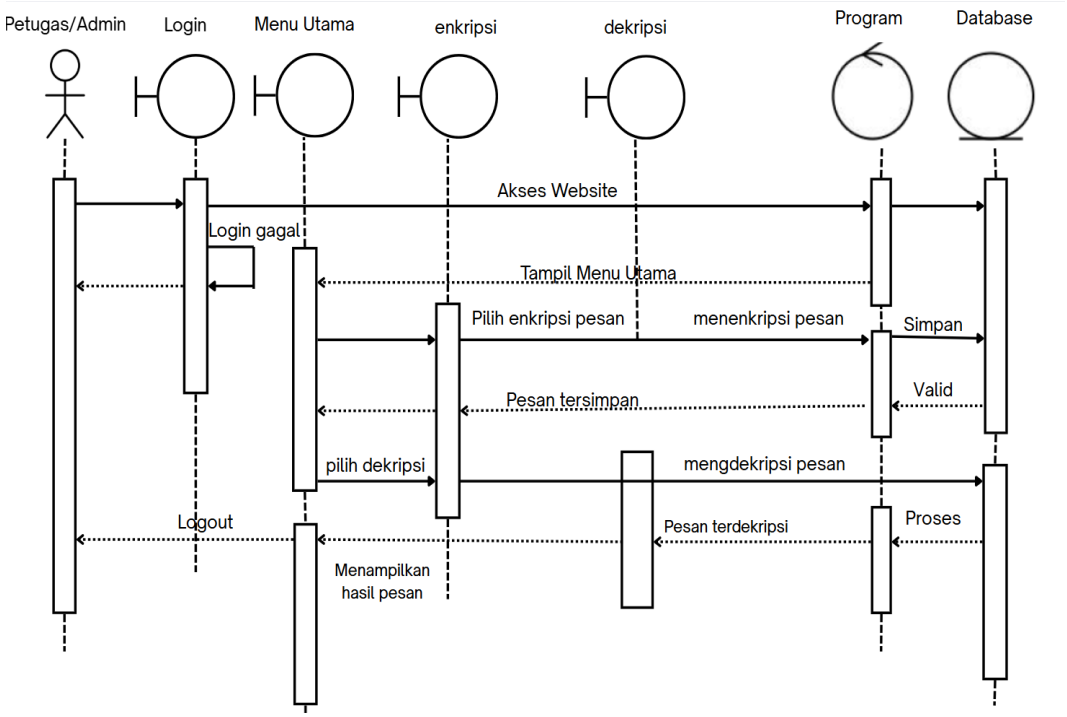
Class diagram berfungsi untuk mendapatkan gambaran database yang digunakan untuk Rancang Bangun Aplikasi Stegano Menggunakan Metode Least Significant Bit (Lsb) Dan Algoritma Kriptografi Advanced Encryption Standard (Aes) yang terkomputerisasi sehingga nantinya akan memberikan kemudahan dalam penyelesaian pembangunan aplikasi web. Untuk lebih jelasnya dapat dilihat pada class diagram sebagai berikut




Gambar 6. *Class Diagram*

d. *Sequence Diagram*

Diagram sequence yang Anda lampirkan menggambarkan alur interaksi antara aktor Petugas/Admin dengan sistem aplikasi steganografi yang melibatkan modul login, menu utama, dekripsi, enkripsi, program, dan database

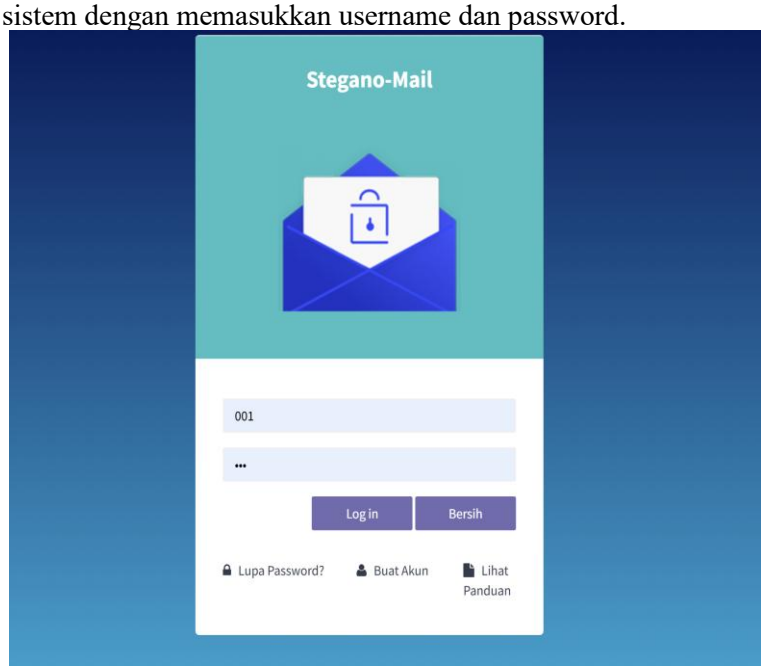



Gambar 7. *Seqeunce Diagram*

### 3.2 Implementasi Sistem

1. Login

   Gambar 8. menampilkan tampilan halaman Login Admin yang digunakan untuk mengakses sistem dengan memasukkan username dan password.




Gambar 8. *Login*

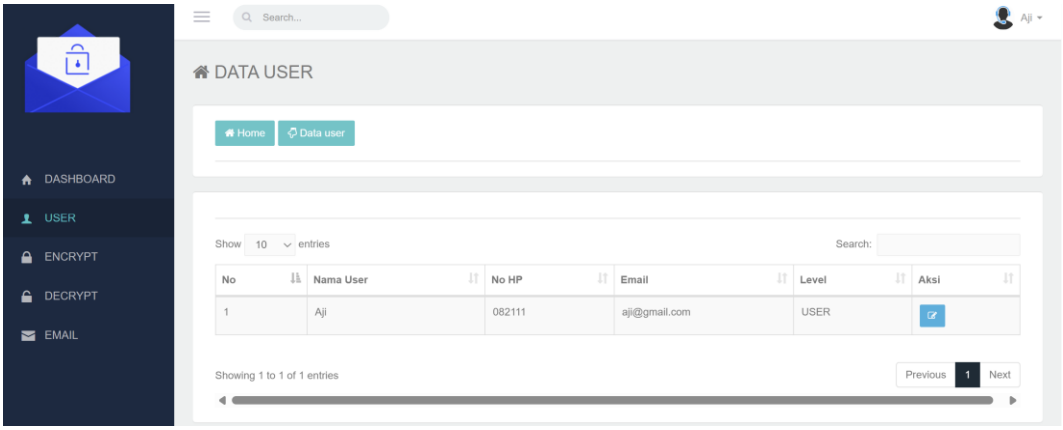
2. Tampilan Dashboard

   Tampilan dashboard ini merupakan menu dasboard saat memasuki aplikasi yang terlihat pada gambar 9.


Gambar 9. Tampilan Dashboard

3. Tampilan user

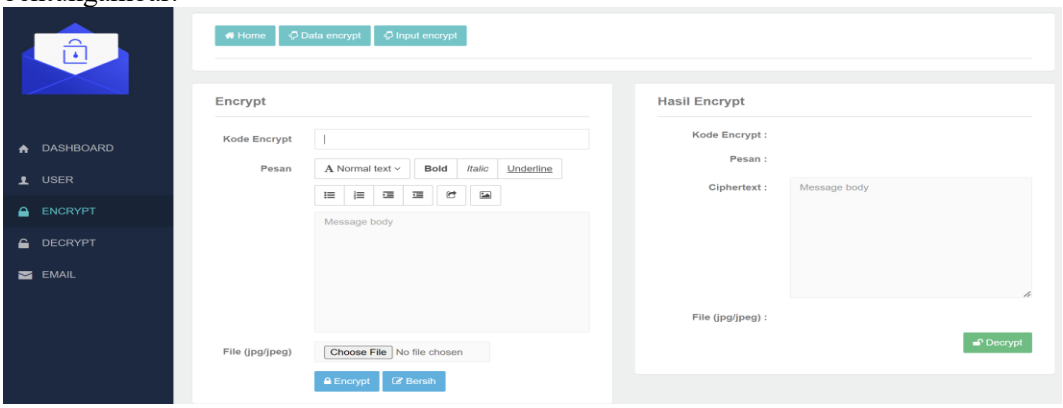
   Tampilan data user merupakan form input untuk mengisi, menambahkan data yang terlihat pada gambar 10.




Gambar 10. Tampilan user

4. Tampilan Edit Data

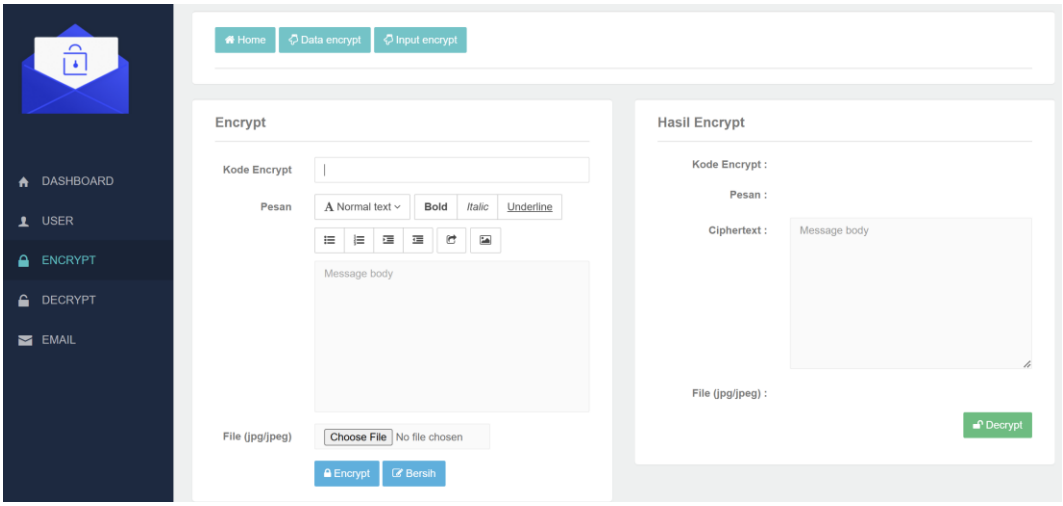
Halaman encrypt merupakan halaman yang bisa mengenkripsi pesan rahasia dalam bentukgambar.




Gambar 11. Tampilan Encrypt Data

5. Tampilan Decrypt

Halaman decrypt merupakan halaman untuk mendekripsi pesan yang sudah dienkripsi menggunakan kode, dapat dilihat pada gambar 12.




Gambar 12. Tampilan Decrypt Data

### 3.2 Pengujian Sistem

Pengujian sistem dilakukan untuk membuktikan bahwa hasil implementasi sistem sudah berhasil dilakukan sesuai dengan yang sudah dirancang sebelumnya. Pengujian yang akan dilakukan adalah black box testing. Dimana pengujian ini berfokus pada tampilan interface dan fungsionalitasnya.

Tabel 1. Pengujian Sistem

| No | Fitur yang Diuji | Input | Ekspektasi Output | Status (Berhasil/Tidak Berhasil) |
|---|---|---|---|---|
| 1 | Login Admin | Username & Password benar | Masuk ke dashboard admin | Berhasil |
| 2 | Login Admin | Username atau Password salah | Muncul pesan error | Berhasil |
| 3 | Enkripsi Pesan | Masukkan teks + kunci enkripsi | Pesan terenkripsi tampil | Berhasil |
| 4 | Penyisipan Pesan ke Gambar (LSB) | File gambar + pesan terenkripsi | Gambar hasil steganografi terbentuk | Berhasil |
| 5 | Ekstraksi Pesan dari Gambar | File gambar stego + kunci | Pesan terenkripsi berhasil diekstrak | Berhasil |
| 6 | Dekripsi Pesan | Ciphertext + kunci enkripsi | Pesan asli tampil | Berhasil |
| 7 | Kirim Email (opsional) | Masukkan data email + file | Email terkirim dengan lampiran | Berhasil |
| 8 | User Interface | Navigasi menu aplikasi | Semua tombol & menu berfungsi | Berhasil |
| 9 | UAT (User Acceptance Test) | Uji coba oleh pengguna | Aplikasi mudah digunakan | Berhasil |

## 4. Kesimpulan

Berdasarkan hasil implementasi dan evaluasi Aplikasi Pengentasan Masalah Mahasiswa berbasis web yang telah dilakukan, kesimpulan yang dapat ditarik adalah sebagai berikut :

1. Sistem berhasil menerapkan metode steganografi LSB yang digabungkan dengan algoritma AES 128-bit sehingga mampu menyembunyikan pesan rahasia ke dalam media digital dengan aman.
2. Aplikasi yang dibuat berbasis desktop telah berjalan sesuai perancangan dan dapat melakukan proses enkripsi, penyisipan, ekstraksi, serta dekripsi pesan dengan baik.
3. Hasil pengujian black-box menunjukkan seluruh fitur utama, mulai dari login admin, enkripsi, penyisipan pesan, ekstraksi, hingga dekripsi, dapat digunakan sesuai harapan.
4. Uji coba oleh pengguna (User Acceptance Test) menyatakan bahwa aplikasi mudah digunakan dan memiliki antarmuka yang cukup intuitif.

## Daftar Pustaka

[1] R. Purnomo, “Rancang Bangun Aplikasi Steganografi Untuk Mengamankan Pesan Menggunakan Metode Least Significant Bit (Lsb) Berbasis Android,” *Technol. J.*, vol. 1, no. 1, pp. 1–6, 2024.

[2] S. P. Sari, P. M. Winarno, and D. Z. Sudirman, “Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard,” *Ultim. J. Tek. Inform.*, vol. 4, no. 1, pp. 24–32, 2012, doi:

10.31937/ti.v4i1.305.

[3] S. Anwar, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES," *J. Format*, vol. 6, no. 1, pp. 65–74, 2017.

[4] R. A. Indra and W. Pramusinto, "Aplikasi Pengamananan Email Dengan Algoritma Advanced Encryption Standard (Aes), Rivest Cipher 4 (Rc4) Dan Caesar Cipher," *Pros. Sains Nas. dan Teknol.*, vol. 1, no. 1, pp. 273–278, 2018, doi: 10.36499/psnst.v1i1.2412.

[5] I. Rizqa, A. N. Safitri, and I. Harkespan, "Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar," *J. Masy. Inform.*, vol. 13, no. 2, pp. 111–120, 2022, doi: 10.14710/jmasif.13.2.44547.

[6] L. Lovebbi and D. Z. Sudirman, "Rancang Bangun Aplikasi Steganografi dengan Metode Least Significant Bit di Audio pada Sistem Operasi Android," *Ultim. J. Tek. Inform.*, vol. 4, no. 1, pp. 7–16, 2012, doi: 10.31937/ti.v4i1.303.

[7] I. A. Pardosi, S. Megawan, N. P. Sembiring, and S. L. Barbara Purba, "Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi," *J. SIFO Mikroskil*, vol. 16, no. 2, pp. 135–144, 2015, doi: 10.55601/jsm.v16i2.243.

[8] D. Novianto and Y. Setiawan, "Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jiig.v9i2.561.