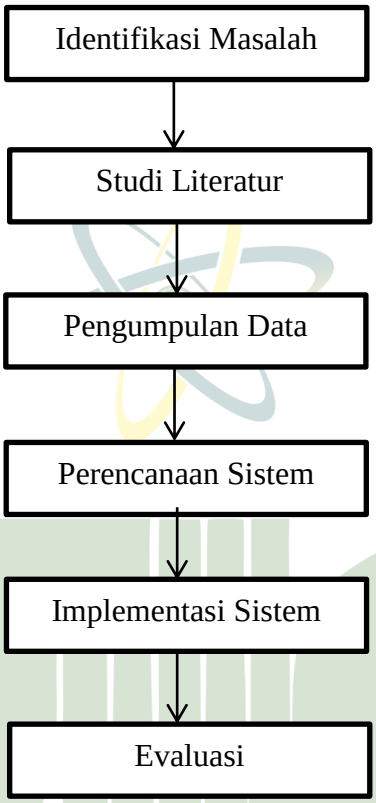
BAB III
METODOLOGI PENELITIAN

3.1 Kerangka Penelitian



Gambar 3.1 Kerangka Penelitian

Berikut adalah konteks untuk kerangka penelitian ini:

1. Identifikasi Masalah

   Penelitan dimulai dengan menentukan masalah yang ingin diselesaikan, yaitu bagaimana meningkatkan keamanan data dengan menggabungkan enkripsi AES dan steganografi BPCS.

2. Studi Literatur

   Penelitian dimulai dengan studi literatur yang menyelidiki literatur terkait, fokus pada metode enkripsi AES (*Advanced Encryption Standard*) dan teknik steganografi BPCS (*Bit-Plane Complexity Segmentation*). Tujuannya adalah untuk memahami dasar-dasar kedua teknik ini dan melihat bagaimana mereka telah diterapkan dalam konteks keamanan data sebelumnya.

3. Pengumpulan Data

   Peneliti mengumpulkan sumber dari berbagai publikasi yang sesuai dengan topik penelitian. Khususnya yang membahas tentang AES dan BPCS.

4. Perancangan Sistem

   Peneliti merancang aplikasi yang dapat mengamankan dan menyisipkan file teks dengan menggunakan enkripsi AES dan steganografi BPCS. Bahasa pemrograman PHP dipilih dalam tahap perancangan sistem.

5. Implementasi Sistem

   Pada tahap ini, aplikasi diuji untuk memastikan prosedur enkripsi dan dekripsi berhasil dilaksanakan. Hasil dari pengujian ini akan memberikan gambaran mengenai sistem dalam mengamankan dan menyisipkan data.

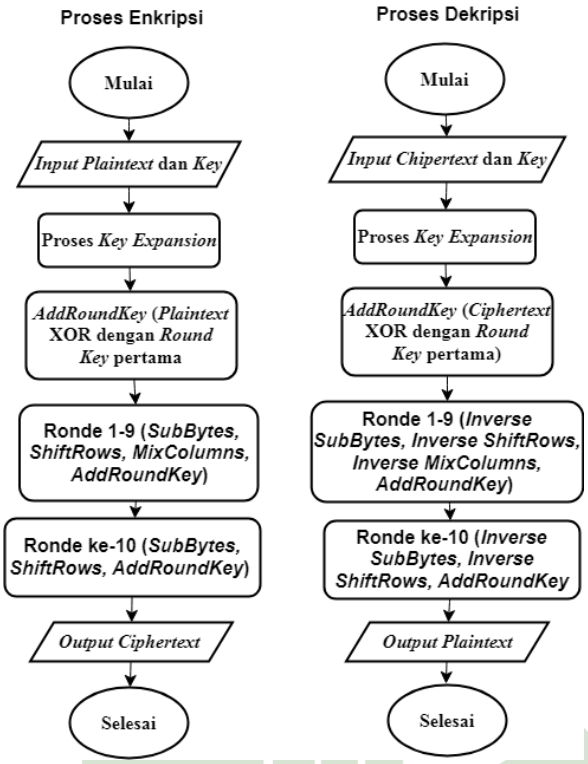
6. Evaluasi

   Peneliti menguji sistem yang telah dibangun, meliputi pengujian keamanan data, penyisipan, serta kinerja sistem.

3.2 Rencana Pembahasan

Keamanan data masih sering menjadi isu yang serius, dengan banyaknya kebobolan data yang terjadi, di mana akses informasi jatuh ke tangan pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan pengembangan aplikasi yang dapat melindungi data dari serangan tersebut. Dalam konteks ini, program kriptografi telah dirancang dengan menggunakan teknik enkripsi sebagai langkah perlindungan. Untuk menjaga tingkat keamanan yang tinggi, aplikasi ini menggunakan *Advanced Encryption Standard* (AES) dan *Bit Plane Complexity Segmentation* (BPCS).

3.2.1 *Flowchart* Proses Enkripsi dan Dekripsi AES



Gambar 3.2 *Flowchart* Proses Enkripsi dan Dekripsi AES

Proses Enkripsi AES

1. Mulai: yaitu menunjukkan titik awal program.
2. *Input Plaintext* dan *Key*: yaitu memasukkan *plaintext* (teks asli yang akan dienkripsi) dan *key* (kunci enkripsi).
3. Proses *Key Expansion*: yaitu proses kunci yang dimasukkan diperluas menjadi beberapa *round key* yang akan digunakan pada setiap ronde enkripsi.
4. *AddRoundKey* (*Plaintext* XOR dengan *Round Key* pertama): yaitu *plaintext* digabungkan dengan *round key* pertama menggunakan operasi XOR untuk memulai proses enkripsi.
5. Ronde 1-9 (*SubBytes, ShiftRows, MixColumns, AddRoundKey*): yaitu setiap ronde terdiri dari empat tahap berikut:
   a. *SubByte*: Setiap *byte* dalam blok *plaintext* digantikan dengan nilai dari tabel substitusi (*S-Box*), yang bertujuan menambah keamanan dengan meningkatkan keacakan.

c. *Inverse MixColumns*: Setiap kolom pada blok *ciphertext* dicampurkan dengan operasi matriks terbalik untuk mengembalikan penyebaran data.
d. *AddRoundKey*: Blok data digabungkan dengan *round key* ronde menggunakan XOR.

6. Ronde ke-10 (*Inverse SubBytes, Inverse ShiftRows, AddRoundKey*): yaitu ronde terakhir memiliki tiga tahap yang sama dengan ronde sebelumnya, tetapi *inverse mixcolumns* tidak diterapkan. Ini mencerminkan struktur yang sama pada proses enkripsi.
7. *Output Plaintext*: yaitu hasil akhir dimana *ciphertext* kini dikembalikan menjadi *plaintext* (teks asli).
8. Selesai: yaitu titik akhir dari *flowchart* yang menandakan proses dekripsi selesai.

3.2.2 *Flowchart* Proses Penyisipan dengan Steganografi BPCS

Gambar 3.3 *Flowchart* Proses Penyisipan dengan Steganografi BPCS

Proses Penyisipan dengan BPCS

1. Mulai: yaitu menunjukkan titik awal program.
2. *Input* Gambar: yaitu langkah untuk memasukkan gambar dan pesan teks yang telah dienkripsi dengan AES. Gambar akan digunakan sebagai media

untuk menyisipkan pesan teks terenkripsi menggunakan teknik steganografi BPCS.

3. Konversi Gambar ke Format Biner: yaitu untuk mengonversi gambar penampung menjadi bentuk biner, yaitu bit-plane, sehingga dapat dianalisis kompleksitasnya dan digunakan untuk menyisipkan data.
4. Menghitung Kompleksitas Bit-*Plane*: yaitu tahap untuk menghitung kompleksitas dari setiap bit-*plane* gambar untuk menentukan bit-*plane* mana yang cukup kompleks dan dapat digunakan untuk penyisipan pesan tanpa terlihat oleh pengamat biasa.
5. Pilih Bit-*Plane* dengan Kompleksitas Tinggi: yaitu hasil perhitungan kompleksitas, bit-*plane* yang memiliki kompleksitas tinggi akan dipilih. Bit-*plane* yang lebih kompleks lebih mampu menyembunyikan data tanpa terdeteksi karena sudah memiliki pola yang tidak beraturan.
6. Penyisipan Data Enkripsi ke Bit-*Plane* Terpilih: yaitu menyisipkan data terenkripsi ke dalam bit-*plane* yang telah dipilih.
7. Rekonstruksi Gambar dengan Pesan yang Tersembunyi: yaitu setelah penyisipan data selesai, gambar dikonstruksi kembali menjadi file gambar yang mengandung pesan terenkripsi.
8. *Output Stego Image*: yaitu hasil akhir dari proses, berupa gambar *stego* yang berisi pesan tersembunyi. Gambar ini terlihat seperti gambar biasa namun telah mengandung data terenkripsi.
9. Selesai: yaitu titik akhir dari *flowchart* yang menandakan bahwa proses sudah selesai.

3.3 Lokasi Penelitian

Lokasi penelitian dilakukan di wilayah Gedung Fakultas Sains dan Teknologi (FST) Universitas Islam Negeri Sumatera Utara yang terletak di Jalan Lapangan Golf, Desa Durian Jangak, Kecamatan Pancur Batu, Kabupaten Deli Serdang, Kota Medan.

3.4 Waktu Penelitian

Waktu yang digunakan untuk penelitian ini dilaksanakan sejak tanggal dikeluarkannya izin penelitian.

Tabel 3.1 Jadwal Pelaksanaan Penelitian

No	Jenis Kegiatan	September 2024				Oktober 2024				November 2024				Desember 2024				Januari 2024			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Identifikasi Masalah																				
2.	Pengajuan Judul																				
3.	Penyusunan Proposal																				
4.	Bimbingan Proposal																				
5.	Seminar Proposal																				

3.5 Rencana Penerbitan

Rencana penerbitan dilakukan pada beberapa rumah jurnal diantaranya:

Tabel 3.2 Rencana Penerbitan Rumah Jurnal

No	Rumah Jurnal	Akreditasi Jurnal	Publish	Link
1.	Jurnal Al-azhar Indonesia	SINTA 3	Januari, May, September	https://jurnal.uai.ac.id/index.php/SST
2.	Jurnal Manajemen Teknologi Dan Informatika	SINTA 3	Maret, Juli, November	https://ojs.pnb.ac.id/index.php/matrix/about
3.	Jurnal Informatika Mulawarman	SINTA 3	Februari, September	https://ejournals.unmul.ac.id/index.php/JIM/about