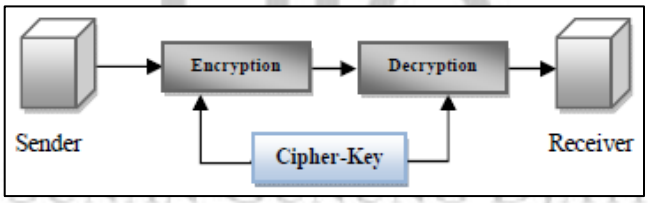
# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Data *multimedia* sering digunakan di internet, jadi dibutuhkan sebuah keamanan data sebelum di transmisi. Enkripsi adalah teknik paling tua dan banyak diketahui sebagai metode pengacak data yang sulit diketahui. Selama bertahun-tahun, enkripsi dikenal luas sering digunakan untuk area yang membutuhkan kemanan dan kerahasiaan. Enkripsi dapat merubah informasi menjadi sulit untuk dipahami oleh penyerangnya akan tetapi, itu sangat mudah untuk dideteksi. Dengan waktu dan alat yang tepat, pesan dapat didekripsi.

Salah satu cabang utama dari keamanan data atau informasi adalah kriptografi, seni dan sains untuk mengamankan data. Kriptografi memungkinkan data asli diubah menjadi data cipher yang dapat dikirim[1]. Contoh proses kriptografi seperti Gambar 1.1 dibawah ini.




*Gambar 1.1 Kriptografi*[1]

Salah satu contoh algoritma kriptografi yang didesain oleh Rivest untuk *RSA Security* adalah RC4. RC4 memproses input data, pesan atau informasi yang pada umumnya sebuah *byte* atau bahkan kadang-kadang bit. Ada beberapa kelemahan dan kelebihan dari model RC4, kelemahannya adalah lebih mudah

diserang dengan menggunakan analisa dari bagian dalam tabel, dalah satu dari 256 kunci dapat menjadi kunci yang lemah, sementara kelebihannya adalah sulitnya mengetahui sebuah nilai dalam tabel, sulitnya mengetahui lokasi mana di tabel yang digunakan untuk menyeleksi masing-masing nilai dan kunci RC4 tentu hanya dapat digunakan sekali[2]. Lalu ada kriptografi menggunakan algoritma Base 64 yang merupakan algoritma *Block Cipher* yang berupa operasi mode bit namun dengan implementasi yang lebih mudah.

Dengan mengkombinasikan dua algoritma kriptografi tersebut dapat meminimalisir kebocoran pesan atau informasi yang dikirim.

Meski menyembunyikan pesan dengan kriptografi dapat lebih memperbesar keamanan, namun masih ada celah-celah untuk dibongkarnya pesan rahasia tersebut. Salah satunya adalah pesan rahasia yang umumnya tidak dapat dibaca secara normal sehingga menimbulkan kecurigaan.

Steganografi yang dugakan adalah metode *Least Significant Bit (*LSB*)*, yaitu menyisipkan pesan dengan mengganti bit ke 8, 16 dan 24 pada representasi biner dengan pesan rahasia yang akan disembunyikan. Kelebihan dari metode LSB adalah cepat dan mudah, serta perbandingan antara sebelum dan sesudah diproses hampir tidak terlihat perbedannya[3].



Steganografi berbeda dari kriptografi, karena steganografi menyimpan keberadaan informasi rahasia sementara kriptografi menyimpan isi informasi. Dalam banyak kasus, steganografi tidak cukup kuat digunakan untuk menyembunyikan informasi.

Menurut jurnal Geetha C. R., steganografi di sisi lain mirip dengan kriptografi. Meskipun steganografi adalah metode kuno, teknologi komputer modern telah memberikan kehidupan baru. Kombinasi dari kedua kriptografi dan steganografi memberikan keamanan yang sangat tinggi[4]. Pada jurnal lain, menurut Jaspal Kaur Saini, makalah ini mengusulkan pendekatan hybrid untuk keamanan gambar. Setelah menerapkan konsep kriptografi, kami mengusulkan teknik steganografi untuk menyembunyikan gambar yang dienkripsi ke *cover image.* Modifikasi ini memberikan keamanan yang lebih besar terhadap serangan[1].

Bedasarkan latar belakang masalah di atas, maka diangkat tema tugas akhir yang berjudul "**KEAMANAN DATA *MULTIMEDIA* MENGGUNAKAN ALGORITMA STEGANOGRAFI DAN KRIPTOGRAFI**".

## 1.2. Rumusan Masalah

Dari latar belakang permasalah di atas, dirumuskan suatu masalah antara lain:

1. Bagaimana mengamankan data *multimedia* menggunakan algoritma Steganografi?
2. Bagaimana mengamankan data *multimedia* menggunakan algoritma Kriptografi?
3. Bagaimana kinerja algoritma untuk mengamankan data *multimedia*?

## 1.3. Tujuan Penelitian

Tujuan dari masalah yang dihadapi adalah:

1. Mengamankan data *multimedia* menggunakan algoritma Steganografi *Least Significant Bit (*LSB*).*
2. Mengamankan data *multimedia* menggunakan algoritma Kriptografi RC4 dan Base64.
3. Kinerja tiap algoritma untuk mengamankan data *multimedia* dibandingkan untuk mendapatkan hasil optimal.

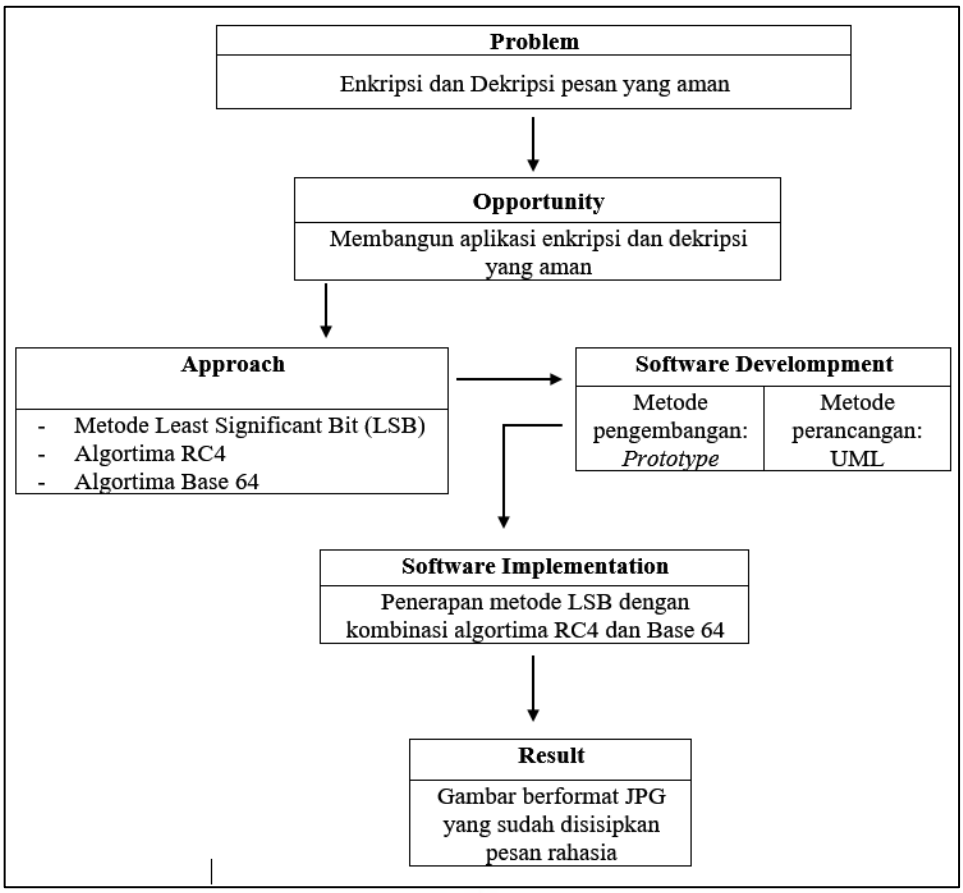
## 1.4. Batasan Masalah

Adapun batasan masalah dari penelitian ini agar tidak keluar dari ruang lingkup pembahasan, antara lain:

1. Metode steganografi yang digunakan adalah LSB (*Least Significant Bit*) pada berkas gambar dengan format JPG (*Joint Photographic Group*) sebagai berkas penampung.
2. Ukuran gambar maksimal yaitu 2000x2000 pixel.
3. Pengamanan data *multimedia* berupa text.
4. Panjang tulisan maksimal 186 karakter.
5. Metode kriptografi yang digunakan adalah RC4 dan Base64.
6. Output yang dihasilkan adalah *steganofile*, yaitu file image berformat JPEG yang telah disisipkan pesan enkripsi.
7. Aplikasi berbasis web.
8. Harus terkoneksi internet.

## 1.5. Kerangka Pemikiran

Adapun kerangka pemikiran dari aplikasi ini pada Gambar 1.2 dibawah ini.




*Gambar 1.2 Kerangka Pemikiran*

## 1.6. Metodologi Penelitian

### 1.6.1. Metode Pengumpulan Data

Untuk menyelesaikan permasalahan yang mengarah pada tujuan pembuatan program ini, maka metodelogi penyelesaian yang digunakan adalah Studi Literatur.

Pencarian informasi dan pemahaman literatur melalui berbagai media. Referensi dari buku, majalah, internet yang berupa artikel, jurnal ilmiah dan forum yang berkaitan dengan tugas akhir ini.

### 1.6.2. Metode Pengembangan Perangkat Lunak

Metode Prototype merupakan suatu paradigma baru dalam metode pengembangan perangkat lunak dimana metode ini tidak hanya sekedar evolusi dalam dunia pengembangan perangkat lunak, tetapi juga merevolusi metode pengembangan perangkat lunak yang lama yaitu sistem sekuensial yang biasa dikenal dengan nama SDLC atau waterfall development model[5].

Dalam Model Prototype, perangkat lunak yang dihasilkan kemudian dipresentasikan kepada *user*, dan *user* diberikan kesempatan untuk memberikan masukan sesuai keinginannya sehingga perangkat lunak yang dihasilkan sesuai dengan keinginan dan kebutuhan *user* tersebut. Proses prototype dapat dilakukan berkali-kali hingga mencapai suatu kesepakatan hasil akhir bentuk dari perangkat lunak yang akan dikembangkan.

Aplikasi dibuat sesuai dengan spesifikasi yang dibutuhkan *user* untuk bisa mengirimkan pesan rahasia tanpa diketahui oleh pihak yang tidak diingikan. Pesan akan dienkripsi menggunakan algoritma kriptografi RC4 lalu dienkripsi lagi dengan algoritma kriptografi Base 64, setelah itu pesan akan di sembunyikan pada gambar menggunakan algoritma steganografi dengan metode LSB. Lalu *user* memberikan revisi kekurangan dari aplikasi yang sudah dibuat untuk mengoptimalkan kinerja aplikasi.



## 1.7. Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun dalam beberapa bab yang masing-masing bab menguraikan beberapa pokok pembahasan. Adapun sistematika penulisan laporan ini yaitu sebagai berikut:

**BAB I PENDAHULUAN**

Bab ini berisikan tentang latar belakang permasalahan yang diambil penulis, perumusan masalah yang dihadapi, batasan masalah, tujuan, *state of the art*, kerangka pemikiran, metodologi penelitian serta bagaimana sistematika penulisan.

**BAB II LANDASAN TEORI**

Bab ini menjelaskan tentang konsep/teori apa saja yang berkaitan dengan topik yang diangkat oleh penulis yang telah dibuat berdasarkan hasil penelitian dan hal-hal yang berguna dalam proses penulisan tugas akhir ini.

**BAB III ANALISA DAN PERANCANGAN**

Pada bagian ini akan definisikan bagaimana sistem yang berjalan setelah itu dibuat suatu perancangan (*design*) baik Desain Sistem, Desain Basis Data, maupun Desain Rancangan Antar Muka (*Graphic User Interface*).

**BAB IV IMPLEMENTASI DAN PENGUJIAN**

Bab ini menjelaskan tentang pengujian sistem secara umum maupun terperinci. Pengujian sistem secara umum akan membahas mengenai lingkungan uji coba untuk menggunakan sistem ini. Selanjutnya secara lebih terperinci dijelaskan dalam pengujian sistem meliputi skenario pengujian baik user umum maupun admin, beserta langkah- langkah dalam uji coba sistem untuk mengetahui aplikasi tersebut telah dapat menyelesaikan permasalahan yang dihadapi sesuai dengan yang diharapkan.

## BAB V PENUTUP

Berisi tentang pernyataan singkat berupa kesimpulan dari pembahasan perangkat lunak yang dibuat secara keseluruhan dan saran untuk mengembangan perangkat lunak yang lebih baik.