

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Saat ini keamanan data dan informasi telah menjadi hal yang sangat penting dan harus diperhatikan. Upaya yang biasa dilakukan untuk mengamankan data dan informasi yang dikirim adalah dengan cara mengenkripsi data tersebut sehingga hanya orang yang mengetahui kunci untuk mendekripsikannya saja yang dapat membacanya. Hal ini memang cukup efektif tetapi algoritma enkripsi yang digunakan juga memiliki kelemahan. Beberapa penyerang dapat menggunakan teknik tertentu dengan memanfaatkan kelemahan algoritma tadi untuk memecah data yang dienkripsi, sehingga penyerang dapat mengetahui data yang sebenarnya tanpa harus mengetahui kuncinya terlebih dahulu.

Steganografi adalah teknik yang digunakan untuk menyembunyikan file kedalam file lain. Dengan menggunakan steganografi kita dapat menyembunyikan file yang telah dienkripsi kedalam file lain sehingga penyerang tidak akan sadar jika terdapat pesan rahasia di dalam file meskipun penyerang berhasil mendapatkan file yang kita kirim. Dengan begitu akan meningkatkan keamanan data dan informasi yang dikirim.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana membuat aplikasi yang menggabungkan teknik steganografi LSB dan algoritma enkripsi gabungan AES, Blowfish, RSA dan SHA2 untuk mengamankan data dan informasi.

## 1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Aplikasi yang dibuat berbasis desktop dengan menggunakan bahasa pemrograman Java dan menggunakan JCE (*Java Cryptography Extension*).
2. Teknik steganografi dilakukan pada file gambar atau citra dengan output bertipe data png.
3. Panjang kunci yang digunakan algoritma RSA adalah 2048 bit dan 4096 bit.
4. Tipe SHA2 yang digunakan adalah SHA-256 dan SHA-512.

## 1.4 Tujuan Penelitian

Tujuan yang akan dicapai peneliti dalam penelitiannya adalah menghasilkan aplikasi yang dapat melakukan enkripsi data dan menyembunyikannya ke dalam file lain.

## 1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat meningkatkan keamanan data dan informasi serta menurunkan kemungkinan serangan terhadap data dan informasi.

### 1.6 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Studi literatur
2. Perancangan dan desain sistem
3. Implementasi dari sistem yang telah di rancang
4. Testing terhadap system yang telah dibuat
5. Menganalisa hasil penelitian, evaluasi dan pembahasan

