# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Barang bukti suatu kejahatan merupakan sebuah syarat penting dalam pengungkapan suatu tindak kejahatan. Bukti forensik dapat berupa berkas, benda, sidik jari, transaksi, serta file dalam melakukan tindak kriminal. Selain berkembangnya teknik forensik dalam menemukan barang bukti, ternyata berkembang pula teknik anti forensik untuk membantu pelaku tindak kejahatan dalam menyulitkan penyidik menemukan barang bukti yang terkait terutama dalam kasus kejahatan digital (*Cyber Crime*), seperti penghapusan otomatis, pengacakan isi bukti, penyembunyian bukti, dan berpindahnya bukti sehingga tidak dapat ditemukan [1].

Semakin berkembangnya dunia digital, anti forensik yang bertujuan untuk menyulitkan penyidik dalam menemukan barang bukti terus berkembang. Anti Forensik adalah kumpulan alat dan teknik yang berkembang untuk menggagalkan alat forensik, investigasi, dan investigator [2]. Anti forensik merupakan lawan dari komputer forensik, jika komputer forensik bertujuan untuk menemukan sebuah bukti digital, sedangkan anti forensik adalah bagaimana mengamankan sebuah data digital agar tidak dapat ditemukan. Anti forensik adalah ilmu dalam mengamankan sebuah data agar dapat terjaga dan tidak diketahui oleh pihak lain. Anti forensik dapat dimanfaatkan dalam berbagai hal yang bertujuan untuk mengamankan sebuah data, sehingga menjadikannya legal dalam pembelajaran dibidang Teknologi Informasi untuk dikembangkan.

Anti forensik dapat didefinisikan sebagai upaya negatif untuk mempengaruhi pemeriksaan barang bukti menjadi sulit atau tidak mungkin dilakukan. Sehingga dapat diambil kesimpulan bahwa teknik anti forensik digunakan untuk melawan dari proses investigasi forensik [3]. Terdapat beberapa metode anti forensik yang dapat digunakan dalam mengamankan sebuah file, seperti pengacakan data, penyembunyian data, memalsukan identitas, pemisahan data, dan menghapus data. Dengan banyaknya metode yang dapat digunakan, maka penyidik akan kesulitan dalam menemukan sebuah bukti digital.

Teknik anti forensik akan bermanfaat dalam berbagai bidang terutama dalam menjaga rahasia sebuah data yang terkandung didalamnya. Menjadikan anti forensik sebagai bidang ilmu yang dapat dimanfaatkan oleh berbagai pihak untuk mendukung keamanan sebuah data adalah langkah yang tepat agar tidak sembarang orang yang tidak memiliki hak, untuk menemukan data tersebut.

Di dalam teknik anti forensik terdapat beberapa metode dalam meyulitkan penyidik dalam menemukan barang bukti, seperti steganografi dan kriptografi yang berguna untuk menyembunyikan serta mengacak data yang ada agar tidak dapat dengan mudah diketahui oleh orang biasa [2]. Ada berbagai macam algoritma yang bisa digunakan untuk menyembunyikan ataupun mengacak isi data. Dalam menyembunyikan pesan, metode LSB yang diterapkan pada proses penyembunyian pesan tidak mempengaruhi kualitas dari *cover image* secara signifikan [4]. Sedangkan dalam mengacak pesan, kemampuan algoritma AES berdasarkan parameter waktu proses enkripsi dan dekripsi jauh lebih baik dibandingkan dengan algoritma lain [5]. Teknik kriptografi yang akan digunakan memiliki kemampuan dalam mengacak data dengan cepat, jika dipadukan dengan teknik steganografi LSB yang menyisipkan pesan dengan tidak mempengaruhi kualitas dari *cover image* secara signifikan diharapkan dapat menemukan algoritma kriptografi dan steganografi yang efektif serta mudah digunakan.

Dengan kombinasi dari dua algoritma keamanan yang akan diimplementasikan, peneliti berharap mempunyai sistem keamanan untuk mengamankan data dan mengetahui batasan berapa kapasitas pesan yang dapat ditampung oleh suatu media citra serta berapa bit yang dibutuhkan untuk memaksimalkan kapasitas dari suatu citra yang masih dapat ditolerir perubahannya. Sistem dibangun dengan tujuan dapat mengamankan serta menyembunyikan teks rahasia dengan cepat, aman, dan mudah.

## 1.2 Rumusan Masalah

Begitu banyak teknik untuk mengamankan data didalam ilmu anti forensik, namun membangun sebuah aplikasi menggunakan algoritma AES-256 yang memiliki karakteristik hasil penyandian yang besar dan metode LSB dengan karakteristik penyisipan yang terbatas menjadi kendala dalam memaksimalkan kapasitas informasi yang akan disembunyikan.

## 1.3 Tujuan

Dapat membangun dan memaksimalkan kapasitas penyimpanan dari implementasi algoritma AES-256 dan metode LSB yang digunakan untuk mengamankan sebuah informasi sebagai model anti forensik.

## 1.4 Batasan Masalah

1. Media implementasi dalam penyisipan pesan terbatas pada media citra PNG.
2. Bahasa pemrograman yang digunakan adalah Python.
3. Pembuatan *User Interface* menggunakan Qt Designer.