

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Komputer sering kali digunakan sebagai media atau alat dalam dunia teknologi informasi, keamanan data atau pesan sangat penting bagi sistem teknologi informasi. Sering kali, informasi atau pesan yang akan dikirim terancam keamanan atau kerahasiaannya (Dakhi, et al., 2020).

Salah satu cara yang dapat digunakan untuk mengamankan data digital ini adalah dengan pemanfaatan Steganografi dan Kriptografi. Steganografi merupakan seni untuk menyelundupkan atau menyembunyikan suatu informasi, informasi tersebut disembunyikan dalam suatu media atau bisa juga citra digital yang tampak seperti biasa saja (Kaunang, et al., 2024).

Kriptografi merupakan suatu cara untuk mengamankan sebuah data atau pesan agar tidak mudah dimengerti oleh orang-orang yang tidak berkepentingan. Data atau pesan akan dikirim dari suatu tempat ke tempat yang lain dengan cara menyembunyikan informasi pada media lain atau dengan menyandikan informasi menjadi kode-kode yang tidak mudah dipahami (Alfiah, et al., 2020).

*3D Playfair Cipher* merupakan salah satu metode kriptografi yang dapat digunakan untuk melakukan proses enkripsi dan dekripsi, kunci akan dituliskan dalam format 4 x 4 yang mendukung 10 digit angka (0-9), 26 huruf (A-Z), dan 26 karakter khusus yang akan digunakan sebagai acuan untuk proses enkripsi dan dekripsi (Sukmawati, et al., 2021).

Steganografi adalah cara merahasiakan atau menyembunyikan keberadaan dari sebuah pesan atau sebuah informasi penting. Dalam penerapannya, agar membuat orang yang tidak bertanggung jawab tidak dapat melihat isi pesan, kebanyakan pesan disembunyikan dengan membuat perubahan kecil terhadap data digital lain (Kasma, et al., 2023).

Steganografi merupakan suatu cara menyembunyikan sebuah pesan atau data digital seperti halnya teks, audio agar tidak tampak dari luar. Metode *Least Significant Bit* (LSB) adalah salah satu metode dalam steganografi. Metode ini

bekerja dengan cara menyisipkan informasi ke dalam suatu citra digital (Laksono, et al., 2024).

Penelitian ini diusulkan dengan menggabungkan dua teknik yaitu Steganografi dengan metode *Last Significant Bit* (LSB) dan Kriptografi *3D Playfair Cipher* yang diharapkan mampu menjaga keamanan pesan yang dikirimkan sehingga terhindar dari kebocoran informasi yang terkandung didalamnya dari pihak yang tidak berkepentingan. Serta dengan tidak melupakan kualitas citra setelah dilakukan proses steganografi dan kriptografi didalamnya dengan menggunakan perhitungan *Peak Signal to Ratio* (PSNR). PSNR merupakan sebuah perhitungan yang digunakan untuk menentukan nilai dari sebuah citra yang dihasilkan (Nurhidayah, 2020)

## 1.2 Rumusan Masalah

Beberapa rumusan masalah berdasarkan latar belakang di atas ialah sebagai berikut:

- Berapa nilai derau yang dihasilkan citra hasil enkripsi menggunakan metode *Peak Signal to Noise Ratio* (PSNR) ?

## 1.3 Batasan Penelitian

Adapula batasan masalah dari penulisan tugas akhir ini adalah :

- a. Pesan yang diolah berbentuk teks menggunakan karakter yang terdapat pada ASCII.
- b. Pesan teks yang diolah memiliki kapasitas maksimal 1600 karakter.
- c. Media digital yang digunakan sebagai objek yang disisipkan berekstensi .png.
- d. Media digital yang digunakan memiliki resolusi  $1080 \times 720$  piksel.
- e. Program bantu yang digunakan ialah MATLAB 2018.
- f. Pesan sudah melalui proses kriptografi menggunakan metode *3D Playfair Cipher* dan steganografi menggunakan metode *Least Significant Bit* (LSB).

#### 1.4 Tujuan Penelitian

- a. Melakukan penyembunyian pesan teks dengan gabungan metode kriptografi *3D Playfair Cipher* dan steganografi *Least Significant Bit (LSB)*.
- b. Melakukan proses pengujian menggunakan *Peaks Signal Noise to Rasio (PSNR)*.

#### 1.5 Manfaat Penelitian

Manfaat yang diharapkan dari dilakukannya tugas akhir ini adalah :

- Memberikan alternatif pengamanan pesan menggunakan gabungan metode *3D Playfair Cipher* dengan *Least Significant Bit (LSB)*.

