BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Kebutuhan keamanan informasi saat ini sangat tinggi, pimpinan Indonesia *Cyber Security* Forum (ICSF) mengatakan bahwa isu keamanan *cyber* adalah agenda mendesak yang harus menjadi perhatian untuk pemerintah Indonesia. Termasuk dalam isu perlindungan data, masih ada celah yang harus diperbaiki (KOMINFO, 2018). Peningkatan kejahatan *cyber* yang sangat tinggi, aktivitasnya kini semakin mengganggu privasi seseorang maupun organisasi, sehingga dibutuhkan suatu teknik untuk menjaga keamanan informasi.

Perkembangan teknik keamanan informasi sendiri telah digunakan sejak sekitar 3.000 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi oleh bangsa yunani kuno (Mishra and Mishra, 2012a). Secara umum, terdapat dua teknik yang digunakan sebagai solusi untuk mengatasi ancaman keamanan informasi, yaitu kriptografi dan steganografi. Kriptografi adalah salah satu teknik untuk menyandikan pesan ke dalam bentuk yang tidak dimengerti oleh pembacanya, namun karena pesan yang telah dienkripsi terlihat menyembunyikan suatu informasi rahasia maka akan menimbulkan kecurigaan oleh pembaca. Solusi alternatifnya adalah teknik steganografi atau teknik yang digunakan untuk menyembunyikan dan menjaga keamanan informasi di dalam *cover media* atau media pembawa pesan agar tidak terlihat oleh pihak yang tidak berwenang (Dharwadkar *et al.*, 2015). *Cover media* merupakan sebuah media yang digunakan untuk menyembunyikan pesan rahasia, seperti citra gambar,

video, teks, atau file media lainnya (Bansod and Bhure, 2014). *Cover media* yang paling populer digunakan adalah citra gambar, karena citra gambar memiliki lebih banyak bit tidak berguna dalam piksel yang terletak di paling ujung kanan dari larik piksel. Dengan banyaknya bit piksel yang tidak berguna, maka memudahkan dalam penyisipan pesan ke dalam *cover media* (Laskar and Hemachandran, 2014).

Teknik steganografi pada citra gambar dapat diklasifikasikan menjadi dua kategori, yaitu teknik *reversible* dimana penerima ingin mempertahankan pesan asli setelah mengekstraksi pesan tersembunyi dari *stego-image* (gambar yang telah disisipkan pesan) dan teknik *irreversible* dimana tujuan penerima hanya mengekstraksi pesan tersembunyi dari *stego-image*. Penulis akan mengadopsi teknik *reversible* karena tidak hanya penyembunyian dan pemulihan pesan yang dibutuhkan secara sempurna tetapi juga pemulihan citra asli atau media pembawa penting untuk pemeriksaan agar tidak menimbulkan kecurigaan (Kumar and Muttoo, 2013). Dalam teknik steganografi citra gambar terdapat beberapa kategori kualitas, seperti *fidelity*, *capacity*, dan *robustness*. *Fidelity* terkait dengan kualitas dari *stego-image* terhadap sistem visual manusia dan dapat dinilai dengan PSNR *(Peak Signal Noise Ratio)*. *Capacity* terkait dengan banyaknya jumlah data rahasia yang dapat disisipkan pada *cover media*. Sedangkan *robustness* mengacu pada kemampuan untuk memulihkan pesan tersembunyi meskipun adanya pemrosesan pada *stego-image*, seperti *cropping, scaling, filtering,* blur, dan bentuk pemrosesan gambar lainnya. Pada pemrosesan gambar secara blur terdapat dua jenis bentuk pemrosesan, yaitu *motion* blur dan gaussian blur. Gaussian blur merupakan salah satu serangan pada *stego-image* dengan proses mengaburkan

suatu gambar, sehingga memungkinkan pesan yang disisipkan tidak dapat diekstraksi atau diambil dari *stego-image* (Kasapbas, 2018).

Terdapat beberapa metode yang dapat diimplementasikan pada steganografi, salah satunya seperti metode LSB *(Least Significant Bit)* yang sering digunakan dalam steganografi karena mudah dimengerti, mudah diimplementasikan, dan *stego-image* yang dihasilkan hampir mirip dengan *cover-image* atau citra gambar pembawanya, sehingga secara kasat mata tidak dapat dibedakan oleh pembaca (Akhtar *et al.*, 2015).

Berdasarkan uraian di atas, penulis bertujuan untuk melakukan penelitian mengenai peningkatan ketahanan *stego-image* terhadap serangan gaussian blur menggunakan pengembangan metode LSB sehingga dapat mengekstraksi pesan pada *stego-image* tanpa merusak pesan tersebut.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini, yaitu :

1. Bagaimana mengembangkan metode LSB dalam mengatasi permasalahan gaussian blur pada *stego-image* ?
2. Apakah metode yang dikembangkan dapat memiliki ketahanan citra terhadap serangan gaussian blur ?

1.3. Batasan Masalah

Batasan masalah pada penelitian ini, yaitu :

1. *Cover-image* menggunakan RGB dan berekstensi .png.
2. Pesan yang akan disisipkan pada *cover-image* berupa teks dan berekstensi .txt.

3. *Range* radius *blur* yang digunakan pada serangan gaussian blur adalah 0-1 radius.
4. Metode yang digunakan untuk proses steganografi adalah metode LSB.
5. Perangkat lunak yang dipakai menggunakan bahasa pemrograman Python.

1.4. Tujuan Penelitian

Tujuan penelitian yang akan dicapai pada penelitian ini, yaitu :

1. Untuk mengetahui cara mengembangkan metode LSB dalam mengatasi permasalahan gaussian blur pada *stego-image*.
2. Untuk mengetahui proses pengujian ketahanan citra terhadap gaussian blur pada steganografi.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini, yaitu :

1. Dapat mengatasi serangan gaussian blur dengan meningkatkan ketahanan *stego-image* menggunakan pengembangan metode LSB.
2. Dapat menemukan metode baru dalam mengatasi serangan gaussian blur pada steganografi dengan memanfaatkan metode LSB.