BAB I

PENDAHULUAN

1.1 Latar Belakang

Komunikasi digital adalah sebuah bagian infrastruktur yang sangat mendasar akhir-akhir ini, banyak aplikasi yang berbasis internet dan ini penting bahwa komunikasi harus dibuat rahasia. Internet umumnya tidak menggunakan *link* yang aman, sehingga informasi yang berjalan rentan terhadap pemotongan. Pentingnya mengurangi kemungkinan informasi terdeteksi selama masa transmisi menjadi masalah. Sebagai hasilnya, keamanan informasi yang melewati saluran terbuka sudah menjadi masalah yang mendasar (Mishra and Singh, 2013).

Sebagai contoh data multimedia sudah berkembang dengan cepat dan luas melalui internet dalam bentuk yang bermacam-macam seperti gambar, audio, video dan text. Dalam komunikasi digital yang menggunakan *internet*, segala sesuatu terlihat dan dapat diakses oleh setiap pengguna. Sehingga, keamanan informasi adalah suatu hal yang penting dan diperlukan. Ada tiga tujuan dari keamanan informasi yakni *confidentiality*, *integrity and availability* (CIA). *Confidentiality* (Kerahasiaan) berarti bahwa informasi harus aman dan tidak dapat diakses oleh pengguna yang tidak memiliki hak. *Integrity* berarti keakuratan dari informasi dan *Availability* (ketersediaan), berarti bahwa informasi itu dapat diakses tepat waktu oleh pengguna yang berhak. Keamanan jaringan sederhana tidaklah cukup untuk komunikasi informasi yang *reliable* seperti text, audio, video dan gambar digital (Razzaq and Shaikh, 2017).

Ada banyak teknik yang dapat digunakan untuk mengamankan informasi diantaranya *encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganografi* dan lain-lain. Pada penelitian ini penulis membahas mengenai *steganografi*.

Steganografi adalah ilmu dan seni menyembunyikan komunikasi yang melibatkan dua prosedur. Pertama, membutuhkan pesan yang disembunyikan dalam pembawa tertentu, contohnya gambar, suara, text dan lain-lain, yang biasa disebut *steganographic cover.* Prosedur kedua terkait dengan pengiriman *cover* kepada penerima tanpa memunculkan kecurigaan. Penerapan *steganografi* dapat diterapkan pada teknologi digital seperti audio, gambar, video dan setiap file yang tersimpan dalam bentuk *bit* (Desoky, 2012).

Pada *steganografi* gambar, file rahasia disembunyikan dalam sebuah *cover image* untuk menyamarkan file dari penyerang (orang yang tidak memiliki hak terhadap informasi) dan file yang sudah disisipkan pada *cover image* disebut sebagai *stego-image.* Pada dasarnya, tujuan *steganografi* bukan untuk menghindari musuh dari mendecode pesan tersembunyi, tetapi mencegah musuh mencurigai keberadaan pesan tersebut.

Teknik dalam *steganografi* secara umum dikategorikan menjadi dua yaitu teknik daerah spasial dan teknik daerah transform. Teknik daerah spasial tidak kompleks dan simpel. Sedangkan teknik daerah transform membutuhkan komputasi atau perhitungan yang lebih tetapi memiliki keunggulan dalam *imperceptibility* (ketidak terlihatan data) dan *robustness* (ketahanan data) terhadap serangan *image processing* yang bermacam-macam seperti *filtering, Gaussian Blur, Cropping, Noise,*

Rescaling dan lain-lain. Sehingga informasi yang tersembunyi dalam *stego cover* tidak hilang atau rusak (Singh and Siddiqui, 2013).

Penerapan teknik-teknik tersebut tentunya tidak lepas dari algoritma yang digunakan. Baik itu menggunakan algoritma yang sudah ada, kombinasi dua algoritma atau lebih maupun memodifikasi algoritma. Diantara algoritma yang paling sering digunakan adalah *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT) dan lain-lain. Beberapa penelitian sering menggunakan beberapa algoritma diatas, dengan memodifikasi atau mengkombinasikan dengan algoritma lain. Kumar dan Kumar (2010) mengusulkan kombinasi algoritma DCT dan DWT. Eksperimen dilakukan menggunakan serangan *image processing* yang berbeda-beda. Hasil simulasi menunjukkan bahwa ada peningkatan yang besar pada nilai PSNR *stego-image*.

Serangan yang dilakukan pada *stego-image* dapat membuat pesan yang tersembunyi pada *cover* menjadi rusak. Salah satu serangan pada *stego-image* yang sangat efektif adalah serangan *cropping. Cropping* adalah salah satu *image processing* yang membuang sebagian atau potongan pada gambar tertentu. Umumnya pesan yang tersembunyi pada *stego-image* berada pada bit yang paling akhir dan berlokasi pada pojok kiri atas gambar. Sehingga, ketika sebuah *stego-image* dipotong maka pesan yang tersembunyi pada gambar tersebut akan sulit untuk diekstrak bahkan sampai hilang.

Berdasarkan uraian di atas, maka penulis ingin mengimplementasikan dan mengembangkan teknik steganografi yang dapat bertahan terhadap serangan *cropping*

pada *stego image*. Sehingga pesan yang berada pada *stego image* masih dapat diekstrak dan utuh.

1.2 Rumusan Masalah

Berdasarkan permasalahan di atas, maka penulis merumuskan masalah yaitu :

1. Bagaimana mengembangkan metode steganografi yang dapat bertahan terhadap serangan *cropping*?
2. Berapa persentase ketahanan citra digital terhadap serangan *cropping* pada steganografi ?
3. Bagaimana kualitas citra dari *stego image*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini diantaranya

1. Mengatasi masalah serangan *cropping* pada *stego-image*.
2. Meningkatkan persentase ketahahan citra digital terhadap serangan *cropping*.

1.4 Batasan Masalah

Agar pembahasan tidak keluar dari permasalahan, maka batasan masalah yang terkait antara lain

1. Media penampung data dan pesan rahasia yang disisipkan adalah gambar, baik berupa format .png.
2. Serangan *image processing* yang dibahas adalah serangan *cropping.*

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini diantara lain

1. Dapat digunakan sebagai salah satu cara dalam pengamanan pesan atau data penting.
2. Hasil penelitian dapat digunakan sebagai media pembanding untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

Bagian utama skripsi terdiri atas bab-bab pendahuluan, landasan teori, metode penelitian, hasil penelitian, kesimpulan dan saran.

1.6.1 Pendahuluan

Bab pendahuluan memuat latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan

1.6.2 Landasan Teori

Bagian ini berisi tinjauan pustaka berupa *review* terhadap literatur-literatur yang terkait dengan penelitian dan landasan teori yang terkait dalam penelitian ini.

1.6.3 Metode Penelitian

Pada bab ini penulis secara lengkap menyajikan tahap eksperimen yang akan dilakukan dalam penelitian ini.

1.6.4 Hasil Penelitian dan Pembahasan

Bagian ini merupakan bagian yang paling penting dari penelitian, karena bagian ini memuat semua temuan ilmiah yang diperoleh sebagai data hasil penelitian. Bagian ini diharapkan dapat memberikan penjelasan ilmiah, yang secara logis dapat menerangkan alasan diperolehnya hasil-hasil tersebut.

1.6.5 Simpulan dan Saran

Kesimpulan memuat secara singkat dan jelas tentang hasil penelitian yang diperoleh sesuai dengan tujuan penelitian. Apabila diperlukan, saran digunakan untuk menyampaikan masalah yang dimungkinkan untuk penelitian lebih lanjut.