BAB 1

PENDAHULUAN

1.1.Latar Belakang

Keamanan informasi merupakan salah satu faktor terpenting dari teknologi informasi dan komunikasi karena perkembangan pesat dari Web dan hak cipta. Kriptografi dibuat sebagai sebuah teknik untuk mengamankan kerahasiaan dari informasi. Namun, kadang-kadang diperlukan agar pihak lain tidak mengetahui bahwa terdapat informasi yang dirahasiakan. Untuk itu, maka dapat diterapkan metode steganografi.

Steganografi (*steganography*) adalah ilmu teknik atau seni untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diakses oleh orang lain yang tidak mempunyai kewenangan (Nizirwan Anwar, 2018). Teknik ini akan memodifikasi pembawa multimedia dengan cara yang tidak kelihatan sehingga tidak diketahui adanya proses penempelan pesan rahasia dan tidak diketahui letak dari pesan rahasia tersebut. Metode steganografi akan mengamankan data rahasia dengan cara menyembunyikannya pada sebuah media. Dua buah persyaratan yang harus dipenuhi oleh metode steganografi adalah sifat tidak terdeteksi dari citra stego dan kemampuan penyimpanan informasi rahasia yang efisien. Metode steganografi yang paling populer adalah metode LSB (*Least Significant Bit*) (Nizirwan Anwar, 2018). Namun, metode LSB sangat rentan terhadap penyerangan dengan menggunakan operasi dasar pengolahan citra. Jassim memperkenalkan metode *Five Modulus* yang diterapkan untuk mengkompresi citra (Jassim, 2012). Ide dasar dari metode ini yaitu bahwa piksel bertetangga biasanya berhubungan. Oleh karena itu, untuk citra *grayscale*, tetangga dari sebuah piksel cenderung mirip dengan piksel tersebut. Kemudian, pada tahun 2013, Jassim menerapkan metode *Five Modulus* ini dalam proses steganografi. Metode *Five Modulus* akan memecahkan sebuah citra digital menjadi sekumpulan subblok citra yang disebut *window* dengan ukuran n x n. Pesan rahasia akan disisipkan pada *window* tersebut. Menurut Jassim, semakin kecil ukuran *window*, maka semakin banyak pesan rahasia yang dapat disisipkan ke dalam citra tersebut. Pemilihan metode *Five Modulus* ini untuk melakukan penyembunyian *file* dengan pertimbangan bahwa metode *Five Modulus* memiliki tingkat keamanan yang lebih tinggi jika dibandingkan dengan metode LSB dimana data akan tersimpan secara teracak sesuai dengan

nilai data sehingga pihak lain akan kesulitan dalam menentukan posisi data rahasia dalam citra.

Algoritma lainnya yang dapat digunakan adalah algoritma *Pictorial Block*. Pada algoritma ini, informasi rahasia akan disimpan dalam sebuah *file* citra digital *grayscale* dan dikonversi ke bentuk nilai ASCII serta panjang informasi akan dihitung. Setelah itu, citra digital akan dibagi menjadi blok berukuran 2^n x 2^n menggunakan algoritma *block truncation coding* (BTC). Kemudian, blok tersebut akan dikonversi menjadi format biner dan menggabungkan informasi asli pada matriks dekomposisinya. Algoritma *steganography pictorial block* menggunakan algoritma BTC untuk mengubah blok citra *grayscale input* menjadi blok citra biner agar dapat dilakukan operasi penyisipan bit informasi rahasia. Konsep utama dari penyembunyian rahasia adalah berdasarkan pada pendekatan penempelan data rahasia pada media sampul dengan menggunakan sebuah kunci. (Mondal, et. al., 2012)

Berdasarkan uraian di atas, penulis tertarik untuk membandingkan algoritma steganografi *Five Modulus* dan *Pictorial Block* untuk mengamankan *file* rahasia dengan cara menyembunyikannya pada sebuah citra digital. Perangkat lunak yang dibuat juga menyediakan fasilitas penyerangan atau penambahan *noise* terhadap citra stego dan proses perbandingan citra, sehingga diharapkan perangkat lunak dapat memberikan gambaran mengenai kinerja dan performansi dari algoritma steganografi *Five Modulus* dan *Pictorial Block*. Oleh karena itu, penulis mengambil skripsi dengan judul "**Analisis Perbandingan Algoritma *Five Modulus* dan *Pictorial Block* untuk Penyembunyian Data pada Citra Digital**".

1.2.Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka permasalahannya adalah:

1. Bagaimana menyembunyikan dan menampilkan kembali *file* ke dalam citra digital menggunakan metode *Five Modulus*.
2. Bagaimana menyembunyikan pesan rahasia pada citra digital dengan menerapkan algoritma *Pictorial Block* sehingga pihak lain tidak dapat mengetahui bahwa ada informasi yang dirahasiakan.
3. Bagaimana melakukan pengujian terhadap algoritma steganografi *Five Modulus* dan *Pictorial Block* untuk mengetahui tingkat ketangguhan dari algoritma steganografi *Five Modulus* dan *Pictorial Block* terhadap *noise* ataupun penyerangan.
4. Bagaimana melakukan pengujian mengenai hasil perbandingan *Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) antara citra asli dan citra stego

beserta citra stego yang telah ditambah *noise* dan citra stego yang telah dihapus pikselnya.

1.3.Tujuan dan Manfaat

Tujuan dari penyusunan skripsi ini adalah membuat sebuah perangkat lunak untuk mengamankan data rahasia dengan cara menyembunyikannya pada citra digital dengan menggunakan algoritma steganografi *Five Modulus* dan *Pictorial Block*.

Manfaat dari penyusunan skripsi ini, yaitu:

1. Mempermudah pengamanan data rahasia agar tidak diketahui orang lain.
2. Mengetahui ketangguhan dari citra stego yang dihasilkan oleh algoritma steganografi *Five Modulus* dan *Pictorial Block* terhadap *noise*.
3. Mengetahui kualitas citra stego yang dihasilkan oleh algoritma steganografi *Five Modulus* dan *Pictorial Block*.

1.4.Batasan Masalah

Batasan masalah yang akan dibahas dalam skripsi ini mencakup :

1. *Input* citra sampul dalam format JPG, BMP dan PNG.
2. *Input file* rahasia berupa semua jenis *file* yang didukung oleh sistem operasi *Windows* 7, 8 dan 10.
3. Tipe *file* yang didukung mencakup file *.txt, *.doc, *.docx.
4. Ukuran citra yang dapat diproses merupakan citra berukuran n x n, dengan batasan nilai n mulai dari 100 piksel sampai 1000 piksel.
5. Aplikasi akan dibuat dengan menggunakan bahasa pemrograman Microsoft Visual Basic 2013.

1.5.Keterbaruan

Aliy Hafiz (2019) mempublikasikan penelitian mengenai Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode *Least Significant Bit* (LSB), dimana data yang ada akan disembunyikan sehingga tidak semua orang bisa melihat dan menggunakannya. Dengan metode Least Significant Bit, Steganografi bisa dilakukan dengan menyisipkan data kedalam gambar yang diinginkan. Proses yang terjadi adalah bit-bit data akan disisipkan ke dalam bit citra

digital sehingga bit data akan berada di dalam bit wadah citra digital tersebut untuk disembunyikan. Dengan adanya steganografi dan metode *Least Significant Bit*, data bisa disembunyikan kemuian diambil kembali untuk bisa dibaca oleh pemilik data.

Dendi Prana Yudha, Kiki Ahmad Baihaqi, Billy Ibrahim Hasbi (2019) mempublikasikan penelitian mengenai Penyisipan Pesan Rahasia pada Citra Gambar dengan Teknik Steganografi dan Algoritma Asimetris Enkripsi Rivest Shamir Adleman (RSA), dimana pada penelitian ini dikombinasikan algoritma RSA yang digunakan untuk mengenkripsi pesan rahasia dan teknik LSB digunakan untuk menyembunyikan pesan terenkripsi dengan tujuan untuk menghasilkan stego file yang lebih aman dan lebih baik secara kualitas. Berdasarkan hasil implementasi dan pengujian citra gambar yang dihasilkan sistem memiliki nilai diatas 40 dB sehingga kualitas citra gambar stego file memiliki kualitas yang baik.

Cahaya Jatmoko, L. Budi Handoko, Christy Atika Sari, De Rosal Ignatius Moses Setiadi (2018) mempublikasikan penelitian mengenai Uji Performa Penyisipan Pesan dengan Metode LSB dan MSB Pada Citra Digital Untuk Keamanan Komunikasi, dimana penelitian ini membahas tentang uji performa algoritma LSB dan MSB dalam steganografi, baik dari segi kulitas hasil steganografi, dan ketahanan terhadap serangan. Alat ukur yang digunakan dalam penelitian ini adalah, *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), dan *Coefficient Correlation* (CC). Berdasarkan hasil penelitian metode LSB terbukti lebih baik dari segi kulitas, sedangkan ketahanan terhadap serangan MSB lebih unggul pada jenis serangan *salt and pepper*.