BAB I
PENDAHULUAN

1.1 Latar Belakang

Umumnya seseorang mengharapkan jika saat berkomunikasi dengan cara mengirimkan pesan kepada orang lain tidak menginginkan pesan tersebut diketahui oleh orang yang tidak berkepentingan (tidak berhak), apalagi sifat pesan tersebut merupakan pesan yang bersifat *privacy*. Dalam hal ini, isi pesan yang bersifat *privacy* merupakan pesan rahasia yang biasanya hanya diketahui oleh pengirim dan penerimanya saja, maka perlu dilakukan untuk menjaga kerahasiaan pesan tersebut dengan suatu teknik. Teknik tersebut dinamakan steganografi, dimana teknik ini merupakan suatu seni ataupun ilmu untuk melakukan penyisipan pesan terhadap suatu *cover* data dengan cara hanya 2 orang saja yang mengetahui, yakni pengirim dan penerima [1]. Bahkan, orang lain pun tidak dapat mengetahui ataupun menyadari bahwa dalam media yang dilakukan penyisipan tersebut didalamnya memiliki isi pesan rahasia. Dengan adanya teknik steganografi, banyak terjadi penyalahgunaan, salah satunya yaitu dengan cara menyisipkan suatu pesan tertentu terhadap sebuah informasi yang digunakan untuk kebutuhan kriminalitas. Oleh karena itu, dibutuhkan steganalisis dimana teknik ini digunakan untuk menyerang steganografi, yang bertujuan untuk menganalisis data yang disembunyikan pada stego sinyal agar dapat mengambil atau mengekstraksi data yang disembunyikan. Teknik yang berfungsi menganalisis dan juga dapat melakukan deteksi kemungkinan adanya suatu data yang disembunyikan ke dalam suatu citra digital dengan menggunakan suatu teknik steganografi dinamakan steganalisis. Steganalisis dibagi menjadi 3 tingkatan diantaranya yaitu deteksi, ekstraksi, dan menon-aktifkan atau menghancurkan data yang disembunyikan atau melakukan tindakan lain untuk mencegah data tersebut tersebar luas [2].

Berdasarkan permasalahan diatas, Tugas Akhir ini melakukan steganalisis untuk mendeteksi posisi keberadaan pesan dan volume blok yang tersisipi pada citra tersteganografi yang dilakukan melalui aplikasi *"Steganography"* android. *Discrete Wavelet Transform* (DWT) dipilih sebagai metode ekstraksi karena perubahan pada *wavelet* bisa mendapatkan informasi suatu sinyal dan juga bisa memberikan informasi terhadap frekuensi kerja yang digunakan [3]. Klasifikasi *Support Vector Machine* (SVM) dipilih karena algoritma yang dapat bekerja menggunakan *mapping*

non-linear dengan tujuan agar dapat merubah data latih asli ke dalam dimensi yang lebih tinggi [4]. Teknik pengklasifikasian ini memiliki suatu fungsi *hyperplane* atau fungsi pemisah terbaik diantara fungsi yang tidak terbatas, hal inilah yang akan mempermudah penelitian dalam melakukan deteksi posisi dan volume citra RGB tersteganografi.

1.2 Penelitian Terkait

Penelitian dengan topik steganografi dengan menggunakan metode yang sama telah dilakukan sebelumnya, adapun beberapa penelitian terkait ditunjukkan pada Tabel 1.1. Namun, beberapa penelitian tersebut belum membahas mengenai tingkat akurasi untuk deteksi posisi dan volume citra tersteganografi.

Tabel 1.1. Judul penelitian terkait dengan metode yang sama.

Judul Penelitian	Tahun	Metode
Kinerja Steganografi Audio Menggunakan Metode *Discrete Wavelet Transform* dan *Statistical Mean Manipulation* dengan Enkripsi RSA dan *Compressive Sampling*	2019	DWT
Analisis *Image* Steganografi Berbasiskan *Discrete Cosine Transform, Discrete Wavelet Transform*, *Singular Value Decomposition*, dan Algoritma *Orthogonal Matching Pursuit*	2019	DWT
Analisis Steganografi Ganda pada Citra Digital Menggunakan Metode *Discrete Wavelet Transform* dan *Singular Value Decomposition* dengan Penyisipan *Spread Spectrum IMage Steganography*	2018	DWT
Steganografi Citra Berdasarkan *Discrete Wavelet Transform* dan QR *Decomposition* Menggunakan *Least Significant Bit* dan Deret Fibonacci	2018	DWT
Steganografi Video pada File Berformat Audio Video *Interleave* Menggunakan Metode Transformasi *Wavelet* Diskrit	2007	DWT
Blind Steganalysis pada Citra Digital dengan Metode Support Vector Machine	2015	SVM
Implementasi Steganalisis dengan Menggunakan Metode BSM-SVM pada Steganografi Citra Digital	2013	SVM
Mendeteksi Keberadaan Pesan Tersembunyi dalam Citra Digital dengan *Blind Steganalysis*	2011	SVM

Pada Tugas Akhir ini, penelitian dilakukan untuk melakukan pengembangan atau melakukan inovasi dari penelitian sebelumnya. Adapun penelitian yang memiliki *case* sama tersebut telah membahas mengenai tingkat akurasi deteksi posisi dan volume, yaitu penelitian yang telah dilakukan oleh Wijayaning Bawono [5]. Dalam penelitian [5] telah dilakukan perancangan arsitektur dari metode *Discrete Cosine Transform* (DCT) dan pembagian blok untuk metode ekstraksi, juga menggunakan *Principal Component Analysis* (PCA) yang digunakan untuk pereduksi citra digital, sedangkan dalam hal pengklasifikasian menggunakan metode *K-Nearest Neighbor* (K-NN). *Windowing* pada penelitian ini untuk mendeteksi posisi dan volume citra tersteganografi. Berdasarkan hasil pengujian pada penelitian [5], hasil telah didapatkan untuk sistem steganalisis tingkat akurasi sebesar 75% dengan waktu komputasi sebesar 1.2012 *second*. Sedangkan untuk deteksi posisi dan volume didapatkan nilai akurasi sebesar 72%.

Penelitian kali ini, penulis melakukan implementasi steganalisis dengan merancang sistem dengan metode ekstraksi dan metode klasifikasi yang berbeda. Oleh karena itu, diharapkan nantinya dapat memperbaiki kekurangan pada penelitian sebelumnya yang sudah dilakukan, sehingga hal yang tidak diinginkan seperti terjadi penyusupan data melalui teknik steganografi dapat dicegah.

1.3 Rumusan Masalah

Permasalahan yang dirumuskan pada Tugas Akhir ini yaitu merancang dan melakukan penelitian sebuah simulasi dengan tujuan mendeteksi posisi keberadaan pesan dan volume blok yang tersisipi pada suatu *cover* data berupa citra RGB.

1.4 Tujuan dan Manfaat

Berikut akan dijelaskan mengenai tujuan dan manfaat dari penelitian ini, yang terdiri dari:

1. Membuat simulator teknik steganalasis dengan menggunakan metode *Discrete Wavelet Transform* (DWT) dan SVM yang dapat mendeteksi posisi dan volume pada citra tersteganografi.

2. Menganalisis pengaruh paramater ukuran gambar, ukuran pesan, jumlah blok tersisipi, tingkatan DWT, serta pengaruh jenis kernel terhadap akurasi steganalisis.

3. Dapat menanggulangi masalah bocornya ataupun rusaknya data rahasia yang disisipkan di sebuah citra.

1.5 Batasan Masalah

Pembahasan Tugas Akhir ini memiliki ruang lingkupnya, adapun rinciannya yaitu sebagai berikut:

1. Proses teknik steganografi didapat dari salah satu aplikasi bernama *"Steganography"* pada *platform* Play Store (Android) dengan menggunakan media steganalisis berupa citra RGB.
2. Penyisipan steganografi menggunakan pesan teks sebagai data steganografi dan menggunakan *cover* data berupa citra RGB.
3. Metode ekstraksi yang digunakan yaitu untuk mengetahui keberadaan pesan tersembunyi kedalam citra RGB adalah *Discrete Wavelet Transform* (DWT) dengan pengklasifikasian pada proses steganografi menggunakan metode *Support Vector Machine* (SVM).
4. Format citra .png dengan menggunakan ukuran citra 128x128, 256x256, dan 512x512.
5. Pesan rahasia menggunakan karakter yang berjumlah 28, 44, 108, 124.
6. Fokus dalam proses deteksi posisi dan volume pada citra tersteganografi.
7. Deteksi posisi diketahui dari *id* blok yang tersisipi pesan rahasia.
8. Volume pesan didapat dari jumlah *id* blok tersisipi.

1.6 Metode Penelitian

Tahap ini dilakukan untuk mengetahui metodologi dalam penelitian yang terdiri dari:

1. Tahap pertama yaitu melakukan studi literatur. Hal ini dilakukan dengan cara mengumpulkan dan memahami literatur-literatur yang berkesinambungan dengan permasalahan yang diangkat dalam penelitian, yang meliputi studi pustaka dan referensi mengenai pengolahan citra digital, metode DWT, dan SVM.

2. Analisis permasalahan dan perancangan sistem perangkat lunak steganalisis dengan metode DWT untuk mendeteksi ada atau tidak pesan tersembunyi pada citra tersteganografi, dan klasifikasi SVM.

3. Melakukan pengujian untuk menganalisis performa sistem steganalisis yang telah dibuat, juga melakukan pengukuran tingkat keberhasilan sistem dalam mengetahui manakah citra asli dan citra tersteganografi.

4. Setelah data sudah dianalisis maka mendapatkan kesimpulan terhadap desain yang telah dibuat, kemudian disusun kedalam bentuk laporan berupa buku Tugas Akhir.

1.7 Sistematika Penulisan

Tahap selanjutnya yaitu sistematika penulisan dalam penyusunan Tugas Akhir ini yaitu sebagai berikut:

Bab 1 PENDAHULUAN
Pada Bab ini terdiri dari latar belakang, penelitian terkait, permasalahan, tujuan dan manfaat, batasan masalah, metode penelitian, dan sistematika penulisan.

Bab 2 KONSEP DASAR
Pada Bab ini melakukan pembahasan konsep dasar dan literatur yang digunakan untuk menunjang penelitian pada Tugas Akhir ini.

Bab 3 PERANCANGAN SISTEM
Pada Bab ini membahas perancangan sistem yang digunakan untuk penelitian Tugas Akhir untuk melakukan realisasi sistem.

Bab 4 PENGUJIAN DAN ANALISIS SISTEM
Pada Bab ini membahasa mengenai pengujian sistem sesuai dengan skenario yang ada dan berdasarkan batasan masalah yang digunakan, serta menganalisis performa sistem dari hasil pengujian yang telah dilakukan.

Bab 5 KESIMPULAN DAN SARAN
Pada Bab ini akan ditarik kesimpulan dari hasil studi performa teknik steganalisis dan terdapat saran untuk melakukan penelitian dengan pengembangan lebih lanjut.