1. Pendahuluan

1.1 Latar Belakang

Steganografi merupakan salah satu teknik untuk menyisipkan pesan rahasia di dalam suatu media, teknik ini semakin berkembang dewasa ini. Dalam perkembangannya, data rahasia dapat disembunyikan pada media digital seperti citra, audio dan video[8]. Sayangnya tidak semua penggunanya menggunakan teknik steganografi untuk tujuan baik bahkan teknik ini sering kali dimanfaatkan beberapa pihak yang tidak bertanggung jawab untuk menyelundupkan data. Salah satu contohnya adalah data perusahaan yang sering diselundupkan oleh pegawai perusahaan tersebut ke berbagai pihak. Secara visual media digital biasa dan stego-objek pada teknik steganografi ini tidak dapat dibedakan secara kasat mata, sehinga kita tidak menyadari bahwa di dalam suatu data digital terdapat pesan rahasia. Oleh karena itu diperlukan suatu cara untuk mengawasi data digital yang kita anggap penting.

Steganalisis merupakan suatu teknik untuk mengetahui apakah di dalam suatu objek terdapat pesan yang telah disisipkan menggunakan steganografi atau tidak[3]. Kabar baiknya adalah menurut Avcibas[1] dari semua teknik steganografi ini terdapat pola-pola tertentu pada stego-objek yang memungkinkan untuk di deteksi dengan pendekatan tersendiri. Bentuk pendekatan yang ditawarkan adalah penggunaan Binary Similarity Measures – Support Vector Machine (BSM-SVM) untuk mendeteksi perubahan pada level biner. Metode Binary Similarity Measure – Support Vector Machine ini dipilih dikarenakan termasuk metode universal atau blind steganalisis yang artinya mampu mendeteksi semua jenis steganografi.

Dalam tugas akhir ini penulis mencoba melakukan implementasi dan analisis metode BSM-SVM (*Binary Similarity Measures-Support Vector Machine*) untuk mendeteksi steganografi yang paling umum digunakan dan paling sederhana yaitu metode LSB (*Least Significant Bit*)[15] dan metode steganografi yang memiliki ketahanan tinggi terhadap serangan visual maupun statistik yaitu F5[6]. Diharapkan nantinya penelitian ini dapat mengimplementasikan metode BSM-SVM sebagai metode steganalisis dalam mendeteksi perbedaan antara stego-objek dengan media digital biasa sehingga bisa mencegah terjadinya penyusupan data melalui teknik steganografi.

1.2 Perumusan Masalah

Pada penelitian Tugas Akhir ini, penelitian difokuskan pada analisis dan implementasi steganalisis citra *digital* menggunakan algoritma *Binary Similarity Measures – Support Vector Machine*. Berdasarkan latar belakang masalah, maka beberapa permasalahan utama yang akan dirumuskan antara lain:

a. Bagaimana menerapkan teknik steganalisis untuk mendeteksi adanya objek steganografi dalam sebuah media digital.
b. Bagaimana menerapkan teknik binary similarity measure untuk meng-ekstrak nilai statistik dari suatu media digital.
c. Bagaimana pembuatan klasifikasi dengan memanfaatkan support vector machine untuk membedakan kelas citra digital dengan objek steganografi dan kelas citra digital kosong.

1.3 Batasan Masalah

Yang menjadi batasan masalah dalam tugas akhir ini adalah :

a. File yang disisipkan pada Stego-Objek berbentuk text.
b. Objek atau file host yang digunakan untuk menyisipkan file berupa citra digital berformat BMP dan JPG.
c. Metode yang digunakan pada steganografi adalah Least Significant Bit(LSB) dan F5.

1.4 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan Tugas Akhir ini adalah sebagai berikut:

a. Mengimplementasikan steganalisis untuk mendeteksi adanya objek steganografi dalam suatu citra digital.
b. Menganalisis performansi sistem dengan melihat nilai akurasi-nya.

1.5 Hipotesis

Penggunaan BSM-SVM sebagai metode steganalisis dapat mendeteksi steganografi LSB dan F5 pada format JPG dan BMP.

1.6 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan untuk penyelesaian permasalahan diatas adalah dengan menggunakan langkah-langkah sebagai berikut :

1. Studi literatur

   Pada tahap ini dilakukan pencarian sumber-sumber bacaan atau referensi dari buku, artikel maupun paper-paper yang terdapat pada internet serta memahami dan mempelajarinya sehingga dapat digunakan sebagai dasar teori dalam penyusunan Tugas Akhir ini. Literatur yang dicari adalah yang terkait dengan algoritma *BSM*, steganalisis, steganografi citra *digital* , serta informasi lain yang menunjang pembuatan tugas akhir ini.
2. Perancangan program yang akan dibuat.

   Pada tahap ini dilakukan perancangan perangkat lunak dalam membangun aplikasi desktop yang dapat melakukan steganalisis menggunakan algoritma *Binary Similarity Measures – Support Vector Machine*.
3. Implementasi

   Mengimplementasikan perancangan dengan menggunakan diagram alir (*flowchart)* yang telah dibuat untuk membangun aplikasi ini menggunakan java.
4. Pengujian dan analisa hasil

   Menganalisis hasil pengujian untuk mengetahui sejauh mana tingkat detection rate dari sistem yang telah dibangun.
5. Penarikan kesimpulan dan penyusunan laporan tugas akhir

   Tahap ini merupakan tahap penarikan kesimpulan terhadap pengujian yang telah dilakukan dan pembuatan laporan.

1.7 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan menggunakan sistematika sebagai berikut:

1. BAB 1

   Membahas mengenai latar belakang yang melandasi pengerjaan tugas akhir ini, rumusan masalah, batasan masalah, tujuan, serta metode penyelesaian masalah.
2. BAB 2

   Berisi tentang teori-teori yang mendukung di dalam pengerjaan tugas akhir ini.
3. BAB 3

   Berisi tentang proses perancangan sistem dan parameter-parameter yang akan diuji dan dianalisis.

4. BAB 4

   Berisi tentang implementasi baik di dalam perangkat keras maupun perangkat lunak, skenario yang dibuat untuk simulasi, serta pengujian dan analisis terhadap sistem yang telah dibangun.

5. BAB 5

   Berisi kesimpulan dari hasil analisis yang telah dilakukan dan saran-saran yang dapat digunakan untuk penelitian selanjutnya.