BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi dan internet saat ini membuat berbagai macam terobosan baru di bidang komunikasi data. Komunikasi merupakan salah satu kebutuhan penting dalam kehidupan manusia untuk saling berhubungan satu sama lain. Pada saat melakukan komunikasi, maka akan terjadi pertukaran informasi antara kedua belah pihak dan seringkali terdapat informasi – informasi penting yang bersifat rahasia. Keamanan dan kerahasiaan data atau informasi merupakan hal yang sangat penting dalam sistem informasi dan komunikasi data. Dalam dunia digital, informasi atau data penting tersebut sangat rentan untuk dicuri oleh orang lain. Salah satu kasus pembajakan dan pencurian informasi melalui internet (*email*) terjadi di Jawa Timur, di mana terjadi komunikasi transaksi jual beli melalui *email* antara dua perusahaan, misalnya perusahaan A dan perusahaan B. Namun, komunikasi tersebut dibajak oleh pihak ketiga dan informasi yang didapat disalahgunakan, kemudian meminta perusahaan A untuk mengalihkan pembayaran tagihan ke rekening yang sudah dikirim oleh pihak ketiga melalui *email*, sehingga terjadi kerugian pada perusahaan A [1]. Berdasarkan kasus tersebut, saling berbagi informasi yang bersifat penting melalui internet (dalam kasus tersebut melalui *email*) rentan dibajak oleh orang lain. Oleh karena itu, dibutuhkan pengamanan data pada saat berbagi informasi untuk mencegah terjadinya pencurian data.

Salah satu cara yang umumnya digunakan untuk mengamankan data tersebut adalah menggunakan kriptografi. Kriptografi merupakan seni untuk menjaga keamanan atau kerahasiaan data. Kriptografi akan mengubah data menjadi kode tertentu dan hanya ditujukan untuk pihak yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali menjadi sebuah data [2]. Kunci

yang digunakan bukanlah sebuah benda, tetapi merupakan sebuah kode rahasia yang diketahui oleh pihak yang melakukan pertukaran informasi atau data dan nantinya digunakan untuk melakukan enkripsi atau dekripsi data. Enkripsi merupakan proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*), sedangkan dekripsi merupakan proses mengubah *ciphertext* menjadi *plaintext* [3]. Salah satu kelemahan dari kriptografi adalah dapat mengundang kecurigaan oleh pihak lain karena perubahan bentuk menjadi tak bermakna sangat mengundang kecurigaan [4]. Kecurigaan tersebut dapat memicu pihak lain untuk memecahkan enkripsi tesebut walau membutuhkan waktu yang cukup lama. Oleh karena itu, dibutuh kan teknik lain sebagai upaya dalam pengamanan data yaitu menggunakan teknik steganografi [5].

Steganografi (*steganography*) merupakan salah satu cara untuk menyembunyikan suatu pesan atau data rahasia ke dalam data atau pesan lain yang tampak tidak mengandung apa – apa, kecuali bagi orang yang mengetahui kuncinya [6]. Tujuan dari steganografi adalah untuk menyembunyikan pesan dalam pesan berbahaya lainnya dengan cara yang tidak memungkinkan seseorang untuk mendeteksi bahwa ada pesan atau data tersebut di dalamnya [7]. Pada teknik steganografi terdapat 2 cara yaitu *embedding* dan *extracting*. *Embedding* merupakan proses untuk menyisipkan data rahasia ke dalam sebuah media. *Extracting* merupakan proses untuk mendapatkan data rahasia yang sudah disisipkan dari sebuah media. Media yang dapat digunakan dalam steganografi yaitu, teks, gambar, suara, dan video [8]. Ada beberapa metode dalam steganografi, antara lain adalah metode *End of File* (EOF), *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), dan lain – lain.

Kelebihan metode EOF adalah pesan yang dapat disisipkan tidak terbatas, sedangkan kekurangan metode ini adalah kapasitas *file* akan bertambah. Kelebihan metode DCT adalah memiliki keamanan yang baik, sedangkan kekurangan dari metode ini memiliki nilai PSNR yang kecil sehingga citra hasil

steganografi kurang menyerupai citra hasil aslinya. Kelebihan metode LSB adalah memiliki nilai MSE yang kecil dan nilai PSNR yang besar sehingga kualitas citra setelah penyisipan tidak jauh berbeda dengan citra aslinya. Kelebihan lain dari metode ini adalah proses penyisipan dan ekstraksi pesan cepat dan memiliki resolusi citra yang sama antara citra asli dengan citra yang sudah disisipi pesan. Kekurangan dari metode LSB adalah mudah diserang dan memiliki kapasitas pesan yang terbatas [9]. Oleh karena itu, dipilih metode *Least Significant Bit* (LSB) karena kelebihan yang sudah disebutkan sebelumnya.

Pada penelitian ini, akan dibuat sebuah aplikasi menggunakan bahasa Python untuk menyisipkan sebuah *file* yang sudah terenkripsi menggunakan kriptografi ke dalam video yang sudah ditentukan menggunakan teknik steganografi atau lebih dikenal dengan Video Steganografi. Video steganografi merupakan teknik menyembunyikan atau menyisipkan data ke dalam sebuah video. Pada sebuah video terdapat *frame – frame* yang dapat disisipi pesan rahasia, sehingga apabila ada seseorang yang akan mengekstrak pesan tersebut harus mengecek setiap *frame* yang ada pada video tersebut. Video yang digunakan yaitu video dengan format MP4. Format tersebut dipilih karena sering digunakan oleh banyak orang dan mudah ditemukan di internet. *File* yang digunakan dalam penyisipan pesan ke dalam video adalah *file* dengan format *.docx* dan *.pdf*. Pemilihan *file* dengan format tersebut adalah karena dapat menampung banyak pesan/data dibandingkan dengan format *.txt* yang hanya dapat disi dengan pesan teks saja. Metode yang digunakan pada video steganografi ini yaitu *Least Significant Bit* (LSB). Metode LSB bekerja dengan cara mengganti bit terakhir dari masing – masing *pixel* dengan bit data yang akan disisipkan. Kelebihan dari metode ini adalah kualitas dan ukuran dari gambar setelah disisipi pesan terlihat tidak jauh berbeda [10]. Teknik video steganografi ini juga dikombinasikan juga dengan kriptografi yaitu menggunakan metode Fernet *Encryption* sehingga mempersulit seseorang atau pihak lain yang melakukan ekstraksi data dari video yang sudah disisipi pesan

rahasia. Fernet merupakan implementasi dari kriptografi *symmetric* (dikenal juga sebagai "*secret key*") *authentication* [11], yaitu algoritma HMAC (*Hash-based Message Authentication Code*) dengan SHA256 untuk otentikasi, AES-128 simetris dalam mode CBC (*Cipher Block Chaining*) dan padding PKCS7 [12]. Fernet *encryption* dipilih karena terdiri dari algoritma yang beragam dalam pengamanan data seperti yang telah disebutkan sebelumnya, sehingga lebih menjamin keamanan data dan juga sangat sesuai untuk melakukan enkripsi pada data yang berukuran kecil. Untuk pengujian kualitas video asli dengan video setelah disisipi pesan adalah dengan menggunakan *Peak Signal to Noise Ratio* (PSNR). Dengan dibuatnya aplikasi Video Steganografi ini diharapkan dapat lebih menjaga kerahasiaan sebuah data sehingga proses pertukaran informasi berjalan dengan aman.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat diidentifikasikan rumusan masalah pada penelitian ini, yaitu:

1. Berapa lama waktu yang dibutuhkan pada saat penyisipan dan juga ekstraksi pesan dari sebuah video? Apakah resolusi video setelah penyisipan pesan mengalami perubahan?
2. Bagaimana cara untuk mengimplementasikan metode LSB ke dalam teknik video steganografi?
3. Apakah perbedaan antara video asli dengan video yang telah disisipi pesan rahasia secara kasat mata dan menggunakan PSNR?

1.3. Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah yang telah dipaparkan di atas, maka batasan masalah yang digunakan pada penelitian ini, yaitu:

1. Bahasa pemrograman yang digunakan saat pembuatan aplikasi dalam penelitian ini yaitu Python.
2. Format video yang digunakan adalah *.mp4* dengan durasi maksimal 30 detik.
3. Format *file* yang akan digunakan dalam penyisipan pesan rahasia ke dalam video adalah *.docx* dan *.pdf.*

4. Ukuran *file* yang digunakan adalah ±200 kb (*kilo byte*) atau menyesuaikan dengan ukuran *frame* yang akan disisipi pesan.
5. *Frame* yang diekstrak dari video memiliki format *.png*.

1.4. Tujuan Penelitian

Berdasarkan pertanyaan penelitian yang sudah dijabarkan di atas, maka tujuan penelitian ini adalah sebagai berikut:

1. Mengetahui cara penerapan teknik kriptografi dan teknik steganografi.
2. Mengetahui cara untuk mengimplementasikan metode LSB ke dalam teknik steganografi.
3. Mengetahui perbedaan antara video asli dengan video yang telah disisipi pesan, baik secara kasat mata maupun dengan menggunakan PSNR.

1.5. Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1.5.1. Manfaat Teoritis

Hasil dari penelitian ini dapat menggambarkan tentang penerapan teknik video steganografi pada sebuah *file* dalam rangka menjaga kerahasiaan dan keamanan suatu informasi.

1.5.2. Manfaat Praktis

A. Bagi Penulis

Manfaat dari penelitian ini bagi penulis adalah sebagai karya ilmiah yang berasal dari ilmu yang telah diperoleh selama belajar di Institut Teknologi Telkom Purwokerto.

B. Bagi Institut Teknologi Telkom Purwokerto

1. Penelitian ini dapat digunakan sebagai salah satu bahan pustaka bagi mahasiswa Institut Teknologi Telkom Purwokerto.
2. Penelitian ini juga bisa digunakan sebagai tema skripsi bagi mahasiswa Institut Teknologi Telkom Purwokerto, dengan cara melakukan penelitian lanjutan untuk lebih menyempurnakan hasil penelitian ini.