BAB I

PENDAHULUAN

1. 1 Latar Belakang

Kerahasiaan dan keamanan data adalah salah satu aspek yang sangat penting dari suatu system infomasi. Saat pengguna melakukan pengiriman data, maka data tersebut tidak dapat dijamin keamanannya. Seiring berkembangnya teknologi saat ini, banyak cara yang dilakukan untuk menyadap sebuah informasi yang penting. Pihak lain dapat mengetahui, membaca dan mengubah isi dari informasi tersebut [1]. Apalagi di jaman modern seperti ini yang mana peretasan data sering kali terjadi. Peretasan data-data ini tidak hanya terjadi di sector indusri, perbankan, ritel, tetapi juga di lembaga pertahanan seperti militer, kepolisian, badan intelejen nasional dan sebagainya. Terdapat sumber dari *republika.co.id* terjadi kasus pencurian data di militer akibat serangan cyber. Hal ini membuat pentagon menjadi khawatir jika pencurinya sekelompok teroris. Pentagon mengatakan bahwa terjadi kebobolan 24000 data rahasia yang mana akan sangat membahayakan keamanan nasional. Data-data ini memiliki berbagai informasi rahasia mengenai strategi nasional negara, projek pembangunan peralatan tempur negara, dan data-data lainnya [2].

Peretasan data pengguna bisa terjadi jika system perlindungan dari situs tersebut tidak ketat, akibatnya data pribadi dapat diretas oleh pihak yang tidak bertanggung jawab. Undang-undang tentang jaminan perlindungan data sudah diatur dalam pasal 15 ayat 1 UU ITE yaitu mengharuskan setiap penyelenggara system elektronik untuk menjaga keamanan data [3].

Berbagai macam teknik untuk mengamankan data telah dikembangkan untuk melindungi data tersebut sehingga tetap terjaga oleh pihak ketiga yang tidak memiliki hak untuk mengetahuinya, salah satunya teknik Steganografi. Steganografi adalah ilmu untuk menyembunyikan pesan ke dalam suatu media seperti teks, gambar, audio maupun video

yang bertujuan untuk menghindari kecurigaan dari orang dan manipulasi data yang tidak bertanggung jawab. Steganografi memiliki dua proses yaitu proses *embedding* (menyisipkan) dan proses *ekstraksi* (mengeluarkan) pada sebuah media penampung (*cover*) [4]. Teknik Steganografi memiliki berbagai macam metode, salah satunya adalah Least *Significant Bit* (LSB). Metode *Least Significant Bit* (LSB) merupakan teknik menyisipkan pesan dengan melakukan perubahan pada bit paling kanan atau bit yang kurang berarti.

Berdasarkan dari latar belakang, bahwa peneliti bermaksud untuk menerapkan teknik Steganografi menggunakan metode *Least Significant Bit* (LSB) sebagai teknik untuk menyembunyikan data agar data tersebut dapat terjaga dengan baik dan tidak dapat diketahui oleh pihak lain, kecuali antar pengirim dan penerima pesan yang mengetahui data tersebut. Teknik ini sangat bermanfaat untuk diterapkan di dunia milter, yang mana kerahasian data harus selalu dijaga karena menyangkut keamanan nasional suatu negara. Teknik ini juga bisa digunakan di lembaga Kepolisian, Badan Intelejen Negeara terutama dalam membagikan pesan rahasia terhadap pihak lain untuk mananggulangi peretasan isi pesan. Penyimpanan data nantinya dapat diterapkan dengan menggunakan media audio, gambar, dan video. Media-media tersebut digunakan sebagai pengalih perhatian untuk menyembunyikan isi pesan yang sesungguhnya. Media penyimpanan yang digunakan untuk menyisipkan pesan adalah video, karena pesan yang akan disisipkan ke dalam media video dalam bentuk file .TXT.

1. 2 Rumusan Masalah

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

1. Bagaimana cara menyisipkan pesan teks ke dalam media video dengan algoritma *Least Significant Bit* (LSB)?
2. Bagaimana kualitas pada video stego (video output) setelah proses penyisipan pesan?

1. 3 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada, maka diketahui tujuan penelitian sebagai berikut:

1. Mengetahui proses dari *Least Significant Bit* (LSB) sebagai teknik penyembunyian pesan.
2. Mengetahui hasil pengujian dan analisa data dari metode *Least Significant Bit* (LSB).
3. Digunakan untuk mengetahui efisiensi dari metode yang diterapkan dari hasil pengujian dan analisa data yang didapat.
4. Mengetahui kualitas video yang dihasilkan dalam penyisipan pesan.

1. 4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian sesuai masalah-masalah yang ada diperoleh batasan masalah pada penelitian ini sebagai berikut:

1. Metode steganografi yang digunakan adalah *Least Significant Bit* (LSB).
2. Format video yang digunakan sebagai media cover bertipe .AVI dan MP4.
3. Ukuran file pada file .TXT yaitu maksimal 200 byte.
4. Format yang dipakai pada frame yang diekstrak pada setiap video yaitu “.png” dan “.jpg”.
5. Proses ekstraksi data berupa text yang terdapat di dalam *file* *.TXT.
6. Ukuran video yang digunakan maksimal 10 mb.
7. Tidak membahas tentang teknik kompresi.

1. 5 Manfaat Penelitian

Berdasarkan rumusan masalah di atas, maka dapat diketahui manfaat penelitian sebagai berikut:

1. Mampu menerapkan metode steganografi dalam penyembunyian pesan sebagai pencegahan terjadinya manipulasi data yang tidak bertanggung jawab.

2. Mampu menerapkan metode *Least Significant Bit* (LSB) sebagai teknik penyembunyian pesan, sehingga pesan tersebut dapat terjaga kerahasiaanya.
3. Penerima memperoleh file rahasia yang telah disisipkan oleh pengirim pada media video.
4. Memperoleh kesimpulan dari hasil pengujian sistem dari proses encoding dan decoding.