BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi telah berkembang dengan pesat dan telah mendominasi sebagai alat pendukung bagi seluruh kehidupan manusia. Seperti salah satu contohnya adalah berkembangnya jaringan internet yang memungkinkan setiap orang mampu bertukar data atau informasi melalui jaringan internet tersebut (Sukrisno dalam Purba dkk, 2012).

Perkembangan jaringan internet yang kian meningkat pun, juga dibayangi dengan maraknya kasus kejahatan atas teknologi informasi dan komunikasi. Adapun para pelaku kejahatannya yang kita kenal pada umumnya seperti *hacker*, *cracker*, *carder*, *phreaker* dan sebagainya (Sukrisno dalam Purba dkk, 2012).

Disamping itu perusahaan iNewsTV yaitu salah satu televisi nasional, juga memiliki jaringan televisi lokal terbanyak di seluruh Indonesia. Stasiun televisi ini dipastikan akan mengangkat dan menonjolkan konten lokal dari masing-masing daerah. Dengan menjadikan misi perusahaan tersebut menjadi stasiun televisi yang mengunggulkan program-program berita dan informasi yang cepat, akurat, informatif, mendidik serta menginspirasi. Dan dalam memperkuat keunggulannya sebagai televisi berita dan informasi, iNewsTV juga di-*support* oleh *news centre* dan *news gathering* terbesar di Indonesia (Web iNewsTV, 2015). Namun, dari pengamatan langsung yang saya lakukan selama lebih dari 1 minggu di iNewsTV bagian IT *Broadcasting*, terdapat kekurangan pada segi keamanan distribusi "*As Run Log*" yang hal ini akan memungkinkan terjadinya penyerangan oleh pihak

lain. *As Run Log* sendiri merupakan laporan data tayang iklan dimana setiap kali iNews TV menayangkan iklan, maka data tersebut masuk kedalam *As Run Log*. Data ini sangat beresiko apabila sampai terdeteksi & dimanipulasi oleh pihak lain yang hal ini akan mengakibatkan kesalahpahaman antara divisi IT *Broadcasting* dengan divisi lain yang bersangkutan.

Untuk menutupi kemungkinan ini, komunikasi rahasia seperti salah satu contohnya adalah dengan menyembunyikan informasi yang sebenarnya pada informasi lain yang disebut juga dengan steganografi. Steganografi merupakan ilmu menulis atau menyisipkan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia yang disembunyikan. Pesan yang disisipi ini merupakan tulisan yang diselubungi atau ditutupi. Steganografi digunakan dengan tujuan agar informasi bisa tersampaikan tanpa diketahui oleh pihak lain (Septian dkk, 2012).

Ada beberapa peningkatan yang cukup tajam dalam ketertarikan pada komunikasi rahasia selama 10 tahun terakhir. Hal ini disebabkan oleh dua alasan utama. Alasan pertama adalah industri percetakan dan *broadcasting* menjadi lebih berminat pada teknik steganografi, tanda hak cipta dan nomor seri pada film digital, *audio recording*, buku, dan produk-produk multimedia lainnya. Tanggapan terhadap prospek keuntungan dagang yang baru, yakni distribusi secara digital masih banyak memberikan kecemasan terhadap perusahaan yang bersangkutan bahwa karya dalam bentuk digital akan sangat mudah untuk di-*copy* (digandakan) oleh pihak lain. Dan alasan kedua yaitu berdasarkan peraturan pemerintah dalam pembatasan ketersediaan layanan enkripsi (kriptografi), telah memotivasi masyarakat untuk mempelajari metode-metode dengan pesan rahasia yang bisa disisipkan pada pesan lainnya (steganografi). Kemudahan yang bisa dilakukan ini bisa

menjadi argumen dalam melawan peraturan pembatasan yang diberlakukan oleh pemerintah (Wolfgang dalam Sara et al, 2011).

Berbagai kegunaan lain steganografi dalam berbagai bidang seperti komunikasi rahasia, penyimpanan data rahasia, perlindungan perubahan data, sistem kontrol akses untuk distribusi konten digital, sistem *database* media dll. Pengaplikasian lainnya dari steganografi ini adalah sinkronisasi audio-*video*, sirkulasi aman dari kerahasiaan data milik sebuah perusahaan, paket TCP/IP (misalnya sebuah ID unik dapat dimasukkan ke dalam sebuah gambar untuk menganalisis lalu lintas jaringan dari pengguna tertentu) (Johnson dalam Bajpai et al, 2012).

Seperti contoh pengaplikasiannya adalah mengenai aplikasi *Medical Imaging System* dimana privasi dianggap perlu antara data berupa gambar milik pasien dan keterangan mereka seperti misalnya nama dokter, nama pasien, hal-hal mengenai penyakit dan keterangan-keterangan lainnya (Peticolas dalam Sanjay et al, 2012). Pada umumnya, steganografi digital bekerja dengan cara menggantikan *bit* berlebih dalam media penampung dengan data rahasia yang ingin disisipkan (Dasgupta et al, 2012).

Penggunaan gambar digital sebagai *carrier* (media penampung) sangat tepat dalam steganografi. Informasi secara visual dan gambar memegang peranan penting di tiap lini kehidupan kita. Karena substansial peningkatan penggunaan komputer, ada kecenderungan peningkatan keamanan dan verifikasi ketelitian suatu gambar. Gambar yang ditransmisikan mungkin memiliki aplikasi yang berbeda, seperti aplikasi untuk komersial, militer dan medis. Namun, gambar digital lebih mudah dibandingkan dengan teks sebagai *carrier*-nya, yang lebih banyak menggunakan daya dan *bandwidth* untuk prosesnya. Dalam beberapa tahun terakhir sejumlah skema *encode* gambar digital yang berbeda telah diusulkan untuk mengatasi masalah *encode* gambar digital tersebut (Jolfaei & Abdolrasoul, 2011).

Metode EOF (*End-Of-File*) merupakan salah satu teknik steganografi yang bekerja dengan cara menyisipkan data rahasia pada akhir *carrier*. *EOF* merupakan pengembangan dari pada *metode LSB* (*Least Significant Bit*). Teknik ini dapat digunakan untuk menyisipkan data rahasia yang ukurannya sesuai dengan kebutuhan. Ukuran *carrier* yang telah disisipkan data rahasia memiliki kesamaan dengan ukuran *carrier* sebelum disisipkan data rahasia ditambah dengan ukuran data rahasia yang akan disisipkan ke dalam *carrier* tersebut (Muslih, 2016).

Manfaat Steganografi akan lebih mengurangi kecurigaan karena pesan disembunyikan dalam media penampung (Adiputra, 2010). Maka dari itu, pembahasan **"Steganografi Untuk Kebutuhan Pengamanan *As Run Log* Pada Divisi IT *Broadcasting* iNews TV"** akan dapat memberikan solusi baru untuk menjaga keamanan maupun keaslian data dengan menggunakan sampel perusahaan iNewsTV.

1.2 Perumusan Masalah

Dari latar belakang diatas kita dapat melihat permasalahannya yakni:

a. Bagaimana caranya agar data *As Run Log* tidak mudah teridentifikasi oleh pihak lain?
b. Bagaimana hasil dari *carrier* setelah ter-*encode* implementasi steganografi dengan data *As Run Log* tersebut?
c. Bagaimana hasil *decode* data *As Run Log* setelah mengalami proses implementasi steganografi tersebut?

1.3 Tujuan dan Manfaat Penelitian

Tujuan yang ingin dicapai dalam penelitian ini antara lain:

a. Membuat aplikasi yang mengimplementasikan steganografi menggunakan *carrier* berupa gambar digital.

b. Menganalisis hasil *encode carrier* yang telah disisipkan data *As Run Log*.
c. Menganalisis data *As Run Log* dari hasil *decode carrier* yang telah disisipkan sebelumnya.

Sedangkan manfaat yang ingin dicapai dalam penelitian ini antara lain :

a. Memberikan solusi pengamanan data *As Run Log*.
b. Menghilangkan keberadaan data *As Run Log* dari pihak lain.
c. Menjaga data *As Run Log* dari kemungkinan teridentifikasi maupun pemanipulasian oleh pihak lain.

1.4 Ruang Lingkup Penelitian

Pada penelitian ini, masalah yang dibahas akan dibatasi pada pembahasan steganografi berupa:

a. Media penampung yang digunakan untuk proses steganografi adalah berupa *file* gambar.
b. Aplikasi steganografi yang ingin dibangun menggunakan metode EOF (*End-of-File*).
c. Aplikasi steganografi yang ingin dibangun merupakan aplikasi *desktop*.
d. Menggunakan bahasa pemrograman Java.
e. Pesan rahasia yang ingin disisipkan adalah data *As Run Log*, yang merupakan *file* teks laporan data tayang iklan dari sampel studi kasus IT *Broadcasting* iNews TV.

1.5 Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, tujuan dan manfaat penelitian, ruang lingkup penelitian, dan sistematika penulisan yang akan digunakan.

BAB II Landasan Teori

Bab ini berisi tinjauan pustaka dan studi literatur penelitian yang telah dilakukan yang berkaitan dengan penelitian ini.

BAB III Metodologi Penelitian

Bab ini berisi tentang tahapan penelitian, tempat penelitian, visi & misi perusahaan, langkah-langkah pelaksanaan, metode pengumpulan data, metode analisis, *As Run Log* dan perancangan aplikasi.

BAB IV Hasil Analisis dan Pembahasan

Dalam bab ini berisi tentang hasil analisis dan pembahasan dari aplikasi yang telah dibangun.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan dan saran dari hasil penelitian yang telah dibuat.