

BAB I

PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi dan komunikasi yang semakin berkembang dengan pesat, ternyata memberikan pengaruh besar bagi kehidupan manusia dalam kehidupan sehari-hari. Perkembangan dalam teknologi saat ini yang berhubungan dengan jaringan dan internet memudahkan setiap orang agar dapat saling bertukar data, pesan atau informasi kepada orang lain tanpa membatasi jarak dan waktu dalam situasi yang berbeda.

Keamanan data dan kerahasiaan sebuah informasi yang diberikan merupakan aspek penting yang dibutuhkan dalam proses penyampaian atau pertukaran informasi melalui jaringan atau internet, karena pada jaman sekarang semakin berkembangnya kejahatan cyber dengan berbagai teknik seperti interupsi, penyadapan, modifikasi, maupun fabrikasi (Rakhmat, Basuki; Fairuzabadi, Muhammad;, 2010). Tanpa adanya jaminan keamanan, Setiap orang yang tidak berkepentingan dapat dengan mudah mendapatkan informasi yang dikirimkan melalui jaringan atau internet (LIU & TANG, 2012). Sudah banyak sekali teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan informasi agar aman serta terhindar dari orang yang tidak berkepentingan, salah satu teknik yang biasa digunakan yaitu steganografi (LIU & TANG, 2012). Menurut penelitian yang telah dilakukan, istilah steganografi berasal dari Bahasa Yunani yang artinya “tulisan tersembunyi” atau *covered writing*. Dalam

teknik steganografi membutuhkan wadah atau tempat penampung untuk data yang akan disembunyikan (Munir, 2004).

Menurut penelitian yang telah dilakukan, steganografi adalah ilmu untuk menyembunyikan teks pada media atau wadah lain yang telah ada sehingga teks yang tersembunyi dapat dimasukkan kedalam media atau wadah tersebut (Harjo, et al., 2016). Dalam teknik steganografi memiliki dua proses utama, yaitu *encoding* dan *decoding*. Maksud dari proses *encoding* adalah proses penyisipan pesan kedalam media penampung, dalam hal ini adalah gambar/citra digital, sedangkan proses *decoding* adalah proses untuk menampilkan pesan tersembunyi dari dalam gambar (Harjo, et al., 2016) (Pratiarso, et al., 2012). Metode yang sering digunakan dalam steganografi citra digital adalah *least significant bit* (LSB) dan *end of file* (EOF). Metode *least significant bit* merupakan teknik penyembunyian pesan pada *bit* terendah dalam gambar atau citra digital. Pesan tersebut dikonversi ke dalam bentuk *bit* biner dan disembunyikan pada gambar dengan menggunakan metode *least significant bit*. Penelitian untuk metode *least significant bit* tanpa keamanan yang baik dan tidak sesuai dengan standar atau prosedur yang ada akan berpeluang untuk dibongkar dengan mudah melalui teknik pemecahan analisis frekuensi yaitu membaca *bit* terendah dari contoh gambar tersebut (Basuki & Maranggani, 2011). Sedangkan metode *end of file* merupakan teknik yang dilakukan dengan cara menambahkan data pada akhir *file* di bit terakhir gambar. Pada penelitian yang dilakukan metode ini juga dapat digunakan untuk menambahkan data yang ukurannya sesuai dengan kebutuhan pengirim. Dalam perhitungannya data yang telah disisipkan dengan ukuran *file* yang berbeda akan sama dengan ukuran *file*

sebelum disisipkan data, kemudian ditambah ukuran data yang telah diubah menjadi *file encode* (Rahayu, et al., 2012).

Penelitian dan implementasi yang telah dilakukan terhadap teknologi telekomunikasi pun semakin pesat berkembang, dibuktikan dengan banyaknya perusahaan maupun individu yang ikut mengambil bagian dalam pesatnya kemajuan dalam teknologi informasi. Para ilmuwan semakin memusatkan penelitian dan pengembangan pada *platform* telepon genggam. Perkembangan telepon genggam pada saat ini semakin condong ke arah telepon pintar atau *smartphone*, hal ini dikarenakan *smartphone* memiliki fitur yang lebih menarik dan dilengkapi dengan dukungan perangkat keras yang lebih modern dibandingkan dengan telepon genggam sebelumnya sehingga mendukung untuk bekerja lebih kompleks dan akurat dalam pengoperasiannya (Rahmayun & Rahmayun, 2014). Oleh karena itu pada *smartphone* memiliki fitur dan teknologi terbaru dalam penyajian informasi untuk pengguna *smartphone*, salah satunya adalah bahasa pemrograman *java* dan *xml* (Winarno, 2009).

Dari permasalahan yang telah dipaparkan di atas, masalah yang diangkat dalam penelitian ini adalah bagaimana mengamankan pesan atau informasi tersebut agar keamanannya dapat terjamin dengan menerapkan teknik steganografi yang tepat. Penelitian ini menggunakan algoritma *least significant bit* (LSB) dan *end of file* (EOF) yang diterapkan pada aplikasi mobile. Indikator yang digunakan dalam algoritma ini adalah waktu proses, ukuran gambar carrier dan nilai PSNR.

Dalam penelitian ini, gambar atau citra digital akan disisipkan pesan teks kemudian dalam gambar tersebut terdapat sebuah informasi atau pesan rahasia setelah

melakukan proses *encode*. Informasi yang telah disisipkan dapat dibaca atau diproses dengan aplikasi steganografi yang dibuat menggunakan algoritma *least significant bit* dan *end of file* melalui proses *decode*.

Tujuan dalam penelitian ini adalah menerapkan teknik steganografi yang tepat dan memiliki kualitas yang baik. Selain itu, aplikasi ini diharapkan dapat membantu keamanan informasi yang bersifat rahasia tanpa diketahui oleh pihak yang tidak berkepentingan, agar informasi tersebut hanya dapat diketahui oleh penerima yang diinginkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan suatu permasalahan yaitu bagaimana merancang sebuah aplikasi keamanan informasi atau pesan menggunakan teknik steganografi pada citra dengan membandingkan metode *least significant bit* dan metode *end of file* berbasis *mobile*. Aspek-aspek yang dibandingkan adalah:

1. Ukuran *file*
2. Kualitas hasil rekonstruksi *image* (PSNR dan MSE)
3. Kecepatan proses *encode* dan *decode* dalam teknik steganografi, menggunakan metode *least significant bit* dan *end of file*

1.3 Batasan Masalah

Untuk memberikan ruang lingkup yang jelas terhadap suatu objek penelitian, maka dibuat batasan-batasan masalah dalam penelitian ini sebagai berikut :

- a. Pembangunan aplikasi pada *smartphone* berbasis *android* yang minimal berjalan pada operasi sistem *android 4.2 Jelly Bean*.
- b. Format media tempat penampung yang digunakan untuk menyisipkan pesan adalah format “.png”.
- c. Aplikasi ini membatasi resolusi *pixel* gambar yaitu maksimal 400 x 400.
- d. Penyisipan pesan atau informasi dalam gambar hanya dapat menyimpan maksimal 160 *character*.
- e. Saat melakukan pemilihan gambar yang ingin di sisipkan pesan atau *encode*, gambar tersebut harus tersimpan atau berada pada internal *storage*.
- f. Gambar hasil proses *encode* otomatis tersimpan pada internal *storage* dengan nama folder “TESIS”.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah membandingkan dua metode teknik steganografi pada citra dengan menggunakan metode *least significant bit* dan metode *end of file* berbasis *mobile*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah menerapkan teknik steganografi yang tepat dan memiliki kualitas yang baik, sehingga pesan yang telah disembunyikan tidak akan menarik perhatian orang jauh dari pikiran seseorang terhadap kerahasiaan pesan tersebut. Sebagai contoh, dapat digunakan dalam dinas rahasia atau pengamanan informasi dalam sebuah perusahaan, instansi atau pemerintah.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Metode Studi Literatur dan studi perangkat lunak

Metode ini dilakukan dengan cara memahami dari berbagai buku referensi, artikel yang didapatkan dari internet, membandingkan perangkat lunak yang sudah ada, dan media-media lain yang relevan dengan teknik steganografi citra dan algoritma yang mendukung.

2. Analisis dan perancangan algoritma

Menganalisis kebutuhan perangkat lunak dan algoritma yang tepat, merancang kebutuhan perangkat lunak meliputi data, arsitektur, kebutuhan antarmuka dan prosedural yang digunakan, implementasi *coding* berdasarkan analisis dan desain perangkat lunak berdasarkan kebutuhan.

3. Pengujian

Dalam pengujian ini dilakukan penyisipan pesan dalam gambar dengan proses *encoding* dan *decoding*, menggunakan gambar yang ingin di steganografi menggunakan dua metode penyisipan pesan yaitu *least significant bit* dan *end of file*.

1.7 Sistematika Penulisan

Laporan ini disusun secara sistematis berdasarkan tata cara penulisan laporan yang telah ditetapkan oleh pihak Pascasarjana Universitas Atma Jaya Yogyakarta dengan urutan penyajian sebagai berikut :

BAB I : PENDAHULUAN

Bab ini terdiri dari latar belakang dilakukannya penelitian, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam Bab ini berisi mengenai pembahasan yang mendukung permasalahan yang diteliti. Tinjauan pustaka digunakan sebagai pedoman atau acuan yang berguna untuk mengarahkan dan mendukung dalam penelitian ini.

BAB III : LANDASAN TEORI

Dalam Bab ini berisi penjelasan dan uraian singkat mengenai dasar teori yang digunakan untuk mendukung dan bermanfaat dalam penelitian ini.

BAB IV : METODOLOGI PENELITIAN

Dalam Bab ini dijelaskan mengenai analisis dan desain perangkat lunak yang akan dibuat, serta desain sistem yang akan diterapkan.

BAB V : HASIL DAN PEMBAHASAN

Pada Bab ini menjelaskan implementasi dari pembangunan sistem, hasil penelitian, dan evaluasi hasil penelitian.

BAB VI : PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan dan saran yang diperlukan untuk pengembangan lebih lanjut.

DAFTAR PUSTAKA

Bab ini berisi mengenai daftar pustaka atau referensi yang digunakan dalam penulisan penelitian.