BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini perkembangan teknologi sangat pesat, hampir semua individu maupun lembaga memanfaatkan teknologi yang ada. Teknologi dibuat untuk membantu manusia dalam mempermudah pekerjaan maupun sebagai sarana hiburan. Pesatnya perkembangan teknologi tidak lepas dari proses pertukaran informasi yang terus mengalami perubahan. Seiring berjalannya waktu dengan bergantinya media-media konvensional seperti pertukaran informasi surat-menyurat melalui pos sekarang telah berganti menjadi media digital yaitu internet. Melalui internet pertukaran informasi menjadi sangat cepat dan tidak terpengaruh oleh jarak maupun waktu. Setiap orang bisa mendapatkan informasi yang di perlukan dengan lebih cepat dimanapun dan kapanpun. Dengan adanya kemudahan tersebut maka teknologi memberikan dampak yang positif bagi kehidupan manusia, akan tetapi meskipun teknologi memberikan dampak positif bagi pengguna, teknologi juga memiliki sisi negatif terutama dari segi keamanan, sehingga keamanan merupakan salah satu aspek yang perlu diperhatikan. Terjadinya kasus penyadapan, pencurian bahkan perusakan terhadap data merupakan hal yang ditakutkan karena data bersifat rahasia dan pribadi. Oleh sebab itu data perlu diamankan agar terhindar dari gangguan oknum-oknum yang tidak bertanggung jawab.

Perkembangan teknologi yang begitu pesat mengakibatkan ancaman terhadap data dan informasi menjadi semakin besar pula, terutama ancaman terhadap data maupun informasi yang bersifat rahasia. Ancaman-ancaman terjadi didunia maya seperti ancaman dari *cracker* atau *hacker* sangat meresahkan masyarakat , karena mereka selalu berusaha untuk mencuri maupun merusak data-data atau informasi penting yang dimiliki oleh masyarakat melalui dunia maya atau internet.

Beberapa teknik yang dapat digunakan untuk melindungi data contohnya kriptografi dan steganografi. Menurut [1] kriptografi merupakan teknik mengamankan data dengan cara mengacak atau merubah isi datanya dengan menggunakan algoritma tertentu, sedangkan steganografi merupakan teknik mengamankan data dengan cara menyembunyikan data kedalam data yang lainya sehingga tidak menimbulkan kecurigaan. Ada beberapa jenis metode steganografi, yaitu *Least Significant Bit* (LSB), *End Of File (*EOF), *Discerete Cosine Transformation* (DCT), dan *Spread Spectrum* [2]. Dalam penelitian ini penulis mengunakan teknik steganografi dengan menggunkan metode *Least Significant Bit* (LSB). Pada metode *least significant bit,* bit-bit *embedded message* akan disisipkan pada bit terakhir (bit paling tidak berarti) dari setiap *byte* data *cover-object,* sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya [3]. Apabila bit-bit *embedded message* disisipkan secara berurutan dalam *byte cover-object*, maka kemungkinan untuk melacak *embedded message* akan sangat mudah. Proses penyisipan metode LSB memiliki perbedaan dengan metode lain, sehingga keunggulan lebih banyak didapatkan pada metode LSB dibandingkan dengan metode lain, karena citra setelah disisipkan pesan hanya mengalami sedikit penurunan kualitas yang tidak begitu berpengaruh secara siginificant bila dilihat oleh mata manusia. Model yang digunakan dalam penelitian ini adalah model *prototype.* Model ini cocok untuk mengembangkan sebuah aplikasi yang akan dikembangkan kembali [4], sedangkan *tool* yang digunakan adalah UML atau *Unified Modeling Language.* UML merupakan sebuah bahasa yang telah menjadi *standard* dalam industri visualisasi, merancang dan mendokumentasikan sistem piranti lunak [5].

Ada beberapa penelitian yang terkait dengan penulis lakukan, diantaranya penelitian [6], mengenai aplikasi steganografi penyembunyian pesan suara terenkripsi berbasis *android*. Hasil dari penelitian ini yaitu aplikasi berhasil melakukan proses enkripsi dan dekripsi pesan suara dengan menggunakan algoritma *serpent.* Aplikasi ini juga berhasil melakukan proses penyisipan dan ekstraksi pesan suara dengan mengimplementasikan teknik steganografi metode EOF (*End of File*) yang dapat berjalan pada sistem operasi android. Penelitian [7],

mengenai implementasi metode *spread spectrum* dalam steganografi pada *file* mp3 berbasis *android.* Dalam penelitian ini perangkat lunak yang mengimplementasikan steganografi dengan teknik *spread spectrum* pada berkas audio mp3 berhasil dibangun, data yang disisipkan dan di ekstraksi adalah sama jika penggunaan dan/atau *factor* pengali *cr* telah dilakukan dengan benar. Penelitian [8], mengenai analisis steganografi citra digital menggunakan metode *spread spectrum* berbasis *android.* Dimana dari pengujian dan analisis sistem yang telah dilakukan bahwa perangkat lunak yang dikembangkan dapat melakukan steganografi pada citra berwarna. Ukuran citra rahasia yang disisipkan pada citra *cover* mempengaruhi waktu penyisipan dan ekstraksi. Semakin besar ukuran maka semakin lama waktu diperlukan untuk penyisispan dan ekstraksi. Penelitian [9], mengenai impelementasi teknik steganografi dengan kriptografi kunci *private aes* untuk keamanan *file* gambar berbasis *android.* Pada penelitian ini aplikasi pengamanan gambar berformat *jpeg* dengan teknik steganografi menggunakan algoritma *aes* berbasis *android* telah berhasil dibangun sebagai aplikasi penyisipan teks gambar menggunkan perangkat mobile android. Dalam menentukan lokasi penyimpanan gambar yang terdapat dua pilihan yaitu penyimpanan kedalam *galerry smartphone* berbasis *android* dan penyimpanan gambar melalui media sosial atau dikirim melalui BBM dan lain-lain. Penelitian [10], mengenai implementasi steganografi berkas file mp3 menggunakan *metode least significant bit* (LSB) pada perangkat *mobile android.* Pada penelitian ini aplikasi mp3 steganografi pada perangkat andorid dengan menggunakan metode *Least Significant Bit* (LSB) sudah berhasil dilakukan, aplikasi mampu menyimpan pesan dan mengekstrak pesan maksimal pada *file* Mp3 dengan *size* paling kecil sebesar sesuai dari hasil pengujian. Penelitian [11] , mengenai *Face Identification For Presence Applications Using Violajenes and Eigenface Algorithm*, pada penelitian ini penerapan algoritma *viola-jones* dan *eigenface* untuk identifikasi wajah pada aplikasi presensi menggunakan *smartphone* berbasis android berjalan dengan baik dengan tingkatan akurasi sebesar 90,90 %.

Berdasarkan uraian diatas maka penulis membuat penelitian dengan judul "Penerapan Metode *Least Significant Bit* (LSB) Pada Aplikasi Keamanan Data Dengan Menggunakan Teknik Steganografi*"*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka dapat dirumuskan permasalahan yang akan diselesaikan yaitu :

1. Bagaimana cara membuat data atau informasi menjadi aman?
2. Bagaimana cara menerapkan metode *Least Significant Bit* (LSB) pada aplikasi keamanan data dengan menggunakan teknik steganografi?

1.3 Batasan Masalah

Adapun batasan masalah yang dapat diambil dari latar belakang di atas adalah:

1. Aplikasi hanya dapat menyisipkan data dalam bentuk pesan *text.*
2. Aplikasi ini menggunakan metode *Least Significant Bit* (LSB) pada proses steganografinya.
3. *File* yang digunakan sebagai *cover* adalah citra digital / *image.*

1.4 Tujuan dan Manfaat Penelitian

Pada penelitian ini terdapat berberapa tujuan dan manfaat yang diharapkan dapat memudahkan kita untuk menjaga keamanan data.

1.4.1 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah menerapkan metode *Least Significant Bit* (LSB) pada aplikasi keamanan data dengan menggunakan teknik steganografi yang mampu membuat data atau informasi bersifat rahasia menjadi aman dan tidak mudah diketahui oleh oknum-oknum yang tidak bertanggung jawab.

1.4.2 Manfaat penelitian

Adapun penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Teknik steganografi dapat diimplementasikan dalam menjaga data atau informasi menjadi lebih aman.
2. Hasil dari steganografi yang disisipkan di dalam sebuah gambar menjadi sulit dikenali oleh indra manusia.

1.5 Sistematika Penulisan Laporan

Untuk memudahkan pembahasan, keseluruhan perancangan sistem aplikasi ini dibagi menjadi lima bab dengan pokok pikiran dari sub-sub bab sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang penulisan laporan, rumusan masalah, batasan masalah, manfaat serta tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini, peneliti menjelaskan berbagai landasan teori yang berkaitan dengan topik penelitian yang dilakukan serta teori-teori pendukung sesuai dengan topik penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai model pengembangan sistem, metode pengembangan perangkat lunak dan *tools* pengembangan perangkat lunak pada penelitian ini. Model pengembangan sistem menggunakan model prototipe, metode pengembangan perangkat lunak menggunkan metode pemrograman berorientasi objek (*Object Oriented Programming*), metode steganografi yang digunakan yaitu metode *Least Significant Bit* (LSB) dan tools yang digunakan adalah *Unified Modeling Language* (UML).

BAB IV PEMBAHASAN DAN HASIL

Pada bab ini akan membahas mengenai analisa permasalahan, proses bisnis yang terkait dengan topik penelitian, berbagai perancangan sistem dan perancangan layar pada sistem, serta hasil dari penelitian.

BAB V PENUTUP

Dalam bab ini peneliti menarik kesimpulan dari keseluruhan bab, serta memberi beberapa saran yang diharapkan dapat bermanfaat bagi perkembangan sistem.