BAB I

PENDAHULUAN

1.1. Latar Belakang

Kerahasiaan dan keamanan suatu data dan informasi pada zaman globalisasi sekarang ini semakin menjadi kebutuhan dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek keputusan bisnis, keamanan ataupun kepentingan umum dan pribadi. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya [1]. Keamanan data dan informasi rentan akan kebocoran, seringkali kita menyimpan beberapa informasi dan data penting seperti kata sandi atau data pribadi pada fitur *notes* di *smartphone*. Hal tersebut sangatlah beresiko jika diketahui oleh pihak lain yang dapat dengan mudahnya membuka fitur *notes* tersebut. Oleh karena itu, kerahasiaan keamanan data dan informasi sangat penting terutama untuk pesan-pesan pribadi [2].

Ada berbagai cara yang dapat digunakan untuk melindungi suatu data dan informasi, salah satunya adalah dengan menggunakan teknik *cryptography*, *Cryptography* berasal dari bahasa yunani: "*cryptos*" yang artinya "I" (rahasia) dan "*graphein*" yang artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia). *Cryptography* merupakan ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*). Ilmu *cryptography* juga adalah suatu teknik untuk mengamankan data atau pesan dengan melakukan proses enkripsi dan proses deskripsi, enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti dan dekripsi adalah proses dengan algoritma yang sama untuk mengembalikkan informasi teracak menjadi bentuk aslinya [3]. *Cryptography* ini tidak hanya menyediakan alat untuk keamanan informasi tetapi juga sekumpulan teknik yang berguna untuk keamanan dan kerahasiaan informasi[4].

Teknik *cryptography* bertujuan mengubah pesan dengan naskah asli (*plaintext*) menjadi pesan dengan naskah acak yang sulit dibaca (*ciphertext*) sehingga informasi tidak dapat terbaca oleh oknum yang tidak bertanggungjawab. Namun kekurangan dari hasil teknik *cryptography* berupa pesan yang tidak bisa dimengerti atau pesan teracak (*ciphertext*) ini dapat menimbulkan rasa kecurigaan oleh oknum yang tidak bertanggungjawab, oknum tersebut akan berusaha memecahkan kode-kode penyandiannya, sehingga data tersebut dapat diketahui. Oleh karena itu untuk mengurangi kekurangan dari teknik *cryptography* yang dapat dengan mudah menimbulkan kecurigaan adalah dengan menggabungkan teknik *cryptography* dengan teknik *steganography*. *Steganography* berasal dari bahasa Yunani, yaitu dari kata *Stegan*os (tersembunyi) dan *Graptos* (tulisan). *Steganography* adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan suatu media lain (*cover-object*) yang hasilnya akan tampak seperti informasi normal lainnya [5]. Media lain (*cover-object*) yang dapat dipergunakan seperti citra digital, teks, suara atau video.

Adapun kelebihan dari penggabungan antara teknik *cryptography* dan teknik *steganography* adalah data atau informasi rahasia yang dihasilkan memiliki tingkat keamanan yang lebih tinggi karena telah dilakukannya proses enkripsi yang menghasilkan *ciphertext* kemudian keamanan pesan tersebut diperkuat dengan dilakukannya penyisipan pesan pada media lain (*cover-object*), sehingga mengurangi rasa kecurigaan oknum yang tidak bertanggungjawab.

Pada paper [4] telah melakukan penelitian tentang "Implementasi Kriptografi *Caesar Cipher* Menggunakan Matlab R2013a" pada penelitian ini menggunakan teknik keamanan data Kriptografi *Caesar Cipher* yang membahas tentang perbaikan atau modifikasi pada jumlah karakter yang semula hanya berjumlah 26 karakter alfabet yaitu A-Z menjadi 41 karakter dengan menambahkan karakter (titik, koma, tanda tanya, tanda seru, tanda petik serta angka 0-9) pada proses enkripsi dan dekripsi *Caesar Cipher*. Penelitian ini dilakukan dengan simulasi Matlab R2013a. Kekurangan pada penelitian ini terletak pada keterbatasannya jumlah karakter pada data dan informasi yang akan digunakan, sehingga keamanan data dan informasi hanya dapat dilakukan dengan

41 karakter saja. [5] Penelitian tentang "Sistem Keamanan Transmisi Data Menggunakan *Steganography* dengan Berbasis Android" yang membahas tentang proses penyisipan pesan dengan teknik *steganography Least Significant Bit* (LSB). Peneliti membuat sebuah aplikasi android menggunakan *open source* eclipse untuk melakukan keamanan pesan. Adapun file yang dipergunakan untuk melakukan penyisipan pesan berupa file gambar yang memiliki format JPG. Kelemahan pada penelitian ini terletak pada penggunaan teknik *steganography Least Significant Bit* (LSB) yang masih sangat sederhana, tanpa adanya proses modifikasi. [6] Telah melakukan penelitian tentang "Implementasi Kriptografi Berbasis *Caesar Cipher* Untuk Keamanan Data" yang membahas tentang implementasian Kriptografi *Caesar Cipher* dengan menggunakan 26 karakter huruf pada abjad atau a-z yang dibuat ke dalam bentuk aplikasi. Pada aplikasi ini, kekurangan pada penelitian ini terletak pada karakter yang dipergunakan masih sangat sederhana dan kurang aman. Peneliti tidak melakukan modifikasi atau penambahan jumlah karakter pada proses enkripsi dan dekripsinya. [7] Penelitian "Penerapan Metode LSB-2 Untuk Menyembunyikan *Ciphertext* pada Citra Digital" peneliti membahas tentang penerapan kombinasi metode atau penggabungan dua metode yang berbeda yaitu antara teknik kriptografi *triangle chain cipher* dan teknik steganografi modifikasi *Least Significant Bit* (LSB) yaitu LSB-2. Proses pada kombinasi ini adalah pesan rahasia yang telah dienkripsi berdasarkan algoritma *triangle chain cipher* disembunyikan dalam citra digital menggunakan metode LSB-2 sehingga pesan tidak mudah diketahui dan dipecahkan oleh orang lain. Kelemahan pada penelitian ini terdapat pada file citra cover yang digunakan, dalam penelitian ini file citra cover yang digunakan berjenis *bitmap* (*.bmp*) yang memiliki ukuran relatif besar. [8] Penelitian "Analisis Sistem Keamanan Teknik Kriptografi dan Steganografi Pada Citra Digital (*BITMAP*)" peneliti membahas tentang analisis penggabungan dua metode berbeda yaitu *Hill Cipher* dan *Least Significant Bit* -2 (LSB-2), pada penelitian ini didapatkan hasil proses penyembunyian pesan pada citra digital sulit diketahui secara kasat mata karena hasil steganografi tidak mengalami perubahan setelah

proses penyisipan biner teks ke dalam biner *bitmap*. Pada penelitian ini, peneliti hanya melakukan analisa secara teori, tanpa adanya pengimplementasian nyata.

Salah satu metode teknik *cryptography* paling sederhana dan paling terkenal adalah *caesar cipher* yang ditemukan oleh Julius Caesar. Metode *caesar cipher* termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet, setiap huruf pada *plaintext* digantikan dengan huruf lain sepanjang 26 karakter alfabet dengan data karakter A-Z [3]. Karena adanya keterbatasan penggunaan karakter pada metode *caesar cipher*, penulis bermaksud melakukan modifikasi pada jumlah karakter tersebut dengan menggunakan 256 karakter pada tabel ASCII.

Salah satu metode teknik *steganography* yang sangat umum digunakan adalah *Least Significant Bit* (LSB). *Least Significant Bit* (LSB) adalah salah satu metode *steganography* yang dapat digunakan untuk menanamkan pesan rahasia dalam sebuah citra digital. Proses memasukkan metode *Least Significant Bit* (LSB) adalah dengan memasukkan bit pesan ke setiap bit terakhir dari citra digital. Pemanfaatan metode *Least Significant Bit* (LSB) masih sangat mudah dipecahkan oleh pihak lain yaitu dengan menukar bit terakhir (bit ke delapan dari elemen warna citra) sehingga pesan yang tersembunyi dapat dihancurkan. Oleh karena itu dilakukannya modifikasi pada metode ini, adapun salah satu modifikasi metode *Least Significant Bit* (LSB) adalah metode *Least Significant Bit*-2 (LSB-2) yang bekerja dengan konsep menukarkan bit ke 8-2 (bit ke 6) dari setiap elemen warna *pixel* citra digital yang menjadi citra penampung dengan setiap bit pesan rahasia yang akan disembunyikan [7].

Pada implementasi metode *caesar cipher* dan LSB-2 penulis menggunakan citra digital berupa file gambar yang dipergunakan sebagai wadah atau cover untuk menyisipkan informasi yang telah tersandi (*ciphertext*). Adapun file gambar yang digunakan adalah format jpg atau jpeg. Alasan penulis menggunakan kedua metode ini antara lain karena metode *Caesar Cipher* dan metode LSB merupakan metode yang paling sederhana dari tiap-tiap tekniknya, sehingga penulis berharap dapat memperkuat kedua metode ini dengan melakukan perkembangan dan

melakukan kombinasi antar keduanya, sehingga menjadi teknik yang dapat diperhitungkan penggunaannya. Software yang digunakan pada pembuatan aplikasi dengan metode kombinasi antara *caesar cipher* dan LSB-2 ini adalah *software open source* android studio 3.5. Android studio 3.5 merupakan *software free* yang mensupport dalam pembuatan aplikasi-aplikasi untuk android dengan mendesain *layout* serta mengkoding perintah aplikasi yang akan dibuat. Adapun kelebihan dari penelitian ini yaitu, pengguna aplikasi kombinasi ini dapat melakukan penyisipan data, informasi ataupun pesan rahasia dengan menggunakan berbagai macam karakter, tidak hanya berpusat pada 26 karakter alfabet saja. Keamanan lebih terjamin karena menggunakan 2 metode keamanan data yang berbeda. Kelebihan lainnya adalah kemudahan dalam mengoperasikan aplikasi, karena aplikasi didesain dengan baik dengan bantuan *software open source* android studio 3.5 sehingga aplikasi ini dapat dipergunakan dan dimengerti dengan mudah tanpa terhubung dengan jaringan internet. Diharapkan kombinasi antara dua teknik ini (*caesar cipher* dan LSB-2) mampu meningkatkan keamanan data dan informasi dari orang yang tidak bertanggungjawab.

Berdasarkan uraian di atas, maka penulis tertarik untuk menarik judul **"IMPLEMENTASI *CAESAR CIPHER CRYPTOGRAPHY* DAN *LEAST SIGNIFICANT BIT-2* (LSB-2) *STEGANOGRAPHY* UNTUK KEAMANAN DATA BERBASIS ANDROID".**

1.2. Rumusan Masalah

Adapun rumusan masalah berdasarkan uraian di atas, terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut :

1. Bagaimana menyisipkan suatu pesan rahasia berupa *text* ke dalam sebuah file gambar agar tidak mudah diketahui oleh yang tidak berhak, tetapi mudah untuk dibuka oleh yang berhak?
2. Bagaimana cara melakukan keamanan data dengan menggabungkan metode *Caesar Cipher Cryptography* dan metode *Least Significant Bit*-2 (LSB-2) *Steganography*?

3. Apakah terjadi perubahan dalam file gambar hasil keluaran dan seberapa besar perubahan itu terjadi dalam penyisipan pesan rahasia tersebut?

1.3. Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka batasan-batasan masalah adalah sebagai berikut :

1. Informasi yang disisipkan berupa file *text* dan file penyisipan informasi tersebut berupa file gambar dengan format JPG .
2. Metode yang diambil adalah *Caesar Cipher Cryptography* dan *Least Significant Bit*-2 (LSB-2) *Steganography*.
3. Objek penelitian difokuskan pada perubahan file gambar keluaran.

1.4. Tujuan dan Manfaat

1.4.1. Tujuan

Setelah mengetahui permasalahan yang terjadi, tujuan yang hendak dicapai dari penelitian dalam rangka penyusunan tugas akhir ini adalah untuk membuat suatu aplikasi dengan metode kombinasi dari *Caesar Cipher Cryptography* dan *Least Significant Bit*-2 (LSB-2) *Steganography* dimana aplikasi ini dapat meningkatkan sistem keamanan data dan informasi dalam menggunakan media telekomunikasi khususnya pada *smartphone* android.

1.4.2. Manfaat

Dengan penelitian ini ini, data dan informasi akan lebih aman karena peneliti melakukan modifikasi pada masing-masing teknik keamanan data serta keamanan data dan informasi diperkuat dengan melakukan kombinasi antara dua teknik yang berbeda yaitu *Caesar Cipher Cryptography* dan *Least Significant Bit*-2 (LSB-2) *Steganography*.

1.5. Metodologi Penulisan

Metodologi penulisan yang digunakan untuk menyelesaikan tugas akhir ini adalah dengan langkah-langkah sebagai berikut:

1. Metode Studi Pustaka

   Yaitu pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

2. Konsultasi

   Yaitu melakukan konsultasi atau wawancara dengan dosen pembimbing ataupun pihak-pihak yang sebelumnya membuat penelitian yang serupa.

3. Rancangan Aplikasi

   Yaitu merancang aplikasi dengan menggabungkan dua metode keamanan data *Caesar Cipher Cryptography* dan *Least Significant Bit*-2 (LSB-2) yang dipergunakan pada android.

4. Pengujian Aplikasi

   Setelah proses pembuatan aplikasi keamanan data selesai, langkah selanjutnya adalah melakukan pengujian aplikasi guna mengetahui aplikasi yang dirancang sesuai dengan koding yang telah dibuat dan berhasil dijalankan atau bekerja dengan baik tanpa adanya error.