BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi kini menunjukan kemajuan yang sangat pesat, kini hampir semua orang beralih ke data digital, seperti teks, citra, audio dan video. Saat ini dengan adanya pertukaran data digital tersebut sehingga resiko untuk penduplikasian data digitalpun tinggi. Contohnya informasi yang bersifat rahasia, atau tidak umum disebar luaskan oleh pihak-pikah notabene tidak memiliki kepentingan.

Agar terhindar dari hal-hal tersebut maka perlu adanya sistem kemanan untuk menjaga keseluruhan asetnya, terutama data penting yang bukan untuk umum. Informasi yang saat ini mudah didapat maka menuntut tingginya pengamanan dari data tersebut. Peningkatan keamanan dapat dilakukan dengan penyandia pesan yang disebut dengan proses enkipsi kriptografi.

Kriptografi merupakan ilmu untuk memberikan memproteksi terhadap pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan[1].

Oleh karena itu untuk menjaga keamanan data atau pesan rahasia, maka sebaiknya pesan yang akan dikirim harus terlebih dahulu dilakukan proses enkripsi, dengan mengkombinasikan kriptografi dan steganografi akan memberikan proteksi ganda pada pesan kemudian disembunyikan dalam sebuah objek gambar, pesan dapat diekstraksi, di dekripsi kembali persis sama seperti aslinya dengan menggunakan kunci yang sama. Proteksi pesan rahasia ini menggunakan algoritma

AES (*Advanced Encryption Standard*) dan untuk penyisipan pesan rahasia kedalam objek citra menggunakan metode steganografi yaitu *Least Significant Bit* (LSB). Banyaknya algoritma dan metode yang dapat digunakan, maka kriptografi yang dipakai dalam penelitian ini yaitu Algoritma *Advanced Encryption Standard* (AES) dikarenakan AES merupakan *cipher* yang berorientasi pada bit, sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware*. AES memiliki ketahanan terhadap semua jenis serangan yang diketahui. Disamping itu kesederhanaan rancangan, kekompakan kode yang sederhana dan kecepatan pada berbagai platform dimiliki oleh algoritma AES. AES terbukti kebal menghadapi serangan konvensional (*linear* dan *diferensial attack*) yang menggunakan statistik untuk memecahkan sandi, dan dalam setiap proses enkripsi dan dekripsi harus melakukan 10 perputaran atau 10 iterasi (10 *Round*) dalam melakukan pengamanan maupun untuk membuka pengamanan tersebut[2]**.**

Metode pengamanan data lainnya yang juga dapat digunakan dengan menggunakan steganografi. Steganografi yang digunakan yaitu metode *Least Significant Bit* (LSB) karena dirasakan cocok dimana perubahan yang dilakukan hanya mengganti byte terakhir lebih rendah atau lebih tinggi satu byte dari sebelumnya. Metode ini menafaatkan ketidakmampuan mata manusia dalam menemukan perbedaan antara citra asli dengan yang sudah dimasukan pesan[3]**.**

Seperti ysng pernah dilakukan pada penelitian sebelumnya, yaitu tentang Implementasi Pengamanan Data dan Informasi dengan Metode Steganografi *Least Significant Bi*t dan Algoritma *Advanced Encryption Standard* (AES) Berbasis Desktop, dimana pada penelitian tersebut membahas mengenai meningkatkan kemanan data. Namun pada penelitian ini masih terdapat kekurangan diantaranya

pada metode *Least Significant Bi*t hasil uji coba hanya mampu mengamankan data rahasia dalam satu formatan file gambar, serta menyulitkan user yang tidak mempunyai formatan file gambar BMP dan file gambar tidak dapat dikirim secara online.

Dengan adanya kekurangan tersebut, maka pada penelitian ini mencoba untuk memperkuat tingkatan kemanan dengan cara menambahkan fitur format *file* JPG dan PNG karena dengan adanya penembahan fitur format *file* gambar akan memudahkan dalam menyisipkan sebuah teks kedalam gambar yang format *file* nya berbeda.

Melakukan kombinasi teknik kriptografi dan teknik steganografi sehingga menjadikan data bersifat rahasia, karena penggabugan kedua teknik tersebut memberikan keamanan lebih atau berlapis.

Sistem dibangun berbasis *Mobile* yang bertujuan untuk membantu pengguna agar mudah mengakses aplikasi yang dibuat karena bersifat *online* dan *multiuser*. Berdasarkan latar belakang masalah diatas peneliti bermaksud untuk mengangkat tema tugas akhir yang berjudul : **Implementasi Proteksi Penyandian Pesan dengan Algoritma AES (*Advanced Encryption Standard*) untuk Penyisipan Pesan Berbasis Image Cover.**

1.2. Perumusan Masalah

Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka diambil rumusan masalah pada penelitian ini adalah :

1. Bagaimana Penerapan Algoritma *Advanced Encryption Standard* (AES) untuk penyandian pesan dan penyisipan pesan ke dalam gambar jpg dan png menggunakan metode *Least Significant Bit* (LSB)

1.3. Tujuan

Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka diambil tujuan pada penelitian ini adalah :

1. Menerapkan Algoritma *Advanced Encryption Standard* (AES) untuk penyandian pesan dan penyisipan pesan ke dalam gambar jpg dan png menggunakan metode *Least Significant Bit* (LSB)

1.4. Batasan Masalah

Adapun batasan masalah dalam penelitian ini yaitu sebagai berikut :

a. Algoritma Kriptografi yang digunakan dalam enkripsi dekripsi pesan ialah Algoritma *Advanced Encryption Standard* (AES) 256 bit.
b. Metode Steganografi yang digunakan untuk penyisipan pesan ke dalam citra ialah metode *Least Significant Bit* (LSB)
c. Pesan yang disisipkan berupa Teks.
d. File citra yang digunakan sebagai penyembunyian pesan ialah berformat citra JPG, PNG, Bitmap.
e. Maksimal ukuran file citra 10 Mb.

f. Maksimal pesan rahasia 1160 karakter.

g. Aspek masukan yaitu *key*, *plaintext*, *image*

h. Aplikasi Berbasis *Mobile*

1.5. Metodologi Penelitian

1.5.1. Teknik Pengumpulan Data

Untuk Kelancaran dalam pembuatan tugas akhir ini ada beberapa teknik pengumpulan data yang akan dilakukan sehingga hasil yang didapatkan menjadi maksimal.

1. Studi Literatur

   Dalam penilitian ini, metode pengumpulan data yang digunakan adalah studi pustaka dimana pengumpulan data dengan cara literatur dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, paper, situs di internet dan bacaan-bacaan yang ada kaitannya dengan penelitian ini.

   Pada tahapan ini akan dilakukan pencarian secara literatur dan pustaka mengenai kriptografi dan steganografi pada teks, teknik AES (*Advanced Encryption Standard*) dan *Least Significant Bit (LSB).*

2. Dokumentasi

   Pada tahapan ini, dokumentasi dilakukan untuk memperjelas hasil dari penelitian yang telah dilakukan dan dituangkan kedalam sebuah bentuk laporan, sehingga lebih mudah untuk dianalisis serta untuk kepentingan pengembangan penelitian selanjutnya.

1.5.2. Model Proses Perangkat Lunak

Untuk membuat perangkat lunak ini, metode pengembangan perangkat lunak yang digunakan yaitu *Rapid Application Development*, karena metode ini lebih memudahkan dalam proses membangun perangkat lunak yang cakupannya tidak terlalu besar dan pengembangannya yang relatif singkat[4]. Dimana keuntungan menggunakan metode *Rapid Application Development* yaitu sebagai berikut :

1) Lebih mudah untuk diamati karena menggunakan model *prototype*, sehingga *user* dapat lebih mengerti akan sistem yang dikembangkan.
2) Lebih fleksibel karena pengembangan dapat melakukan proses desain ulang pada saat yang bersaman.
3) Bisa mengurangi penulisan kode yang kompleks karena menggunakan *wizard*.
4) Keterlibatan *user* semakin meningkat karena merupakan bagian dari tim secara keseluruhan.
5) Mampu meminimalkan kesalahan-kesalahan dengan menggunakan alat-alat bantuan *(CASE tools*).
6) Mempercepat waktu pengebangan sistem secara keseluruhan karena cenderung mengabaikan kualitas.

Proses Metode *Rapid Application Development*

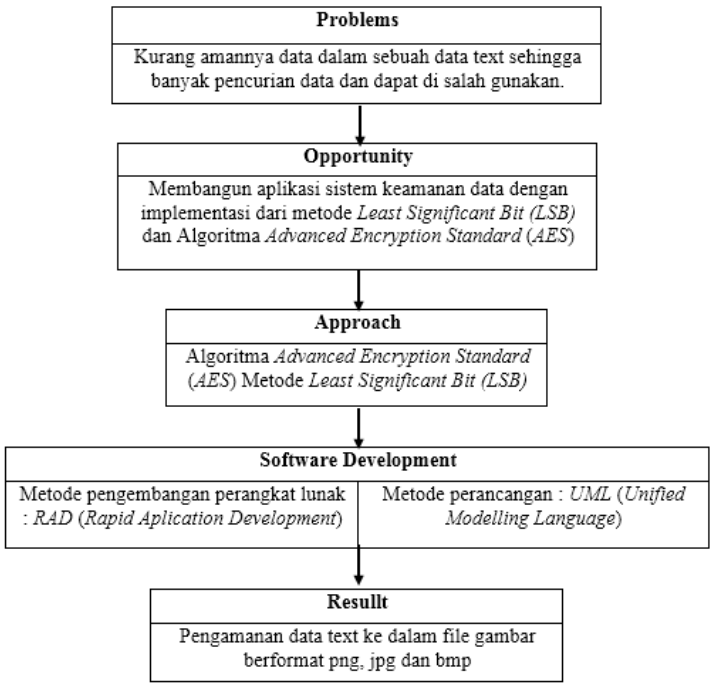
a) Rencana kebutuhan *(Requitments Planning)* pada tahapan ini, *user* dan *analyst* melakukan identifikasi tujan dari aplikasi ataupun sistem dan melakukan identifikasi kebutuhan informasi untuk mencapai tujuan.

b) Proses desain (*Design Workshop*) pada tahapan ini adalah melakukan proses desain dan perbaikan-perbaikan apabila masih terdapat ketidak sesuaian desain antara *user* dan *analyst.* Proses desain menggunakan UML (*unified modeling language*)

c) Implementasi (*Implementation*) Setelah desain dari sistem yang akan dibuat sudah disetujui baik itu oleh *user* dan *analyst.* Maka pada tahapan ini *programmer* mengembangkan desain menjadi suatu program.

1.6. Kerangka Pemikiran

Kerangka pemikiran adalah suatu diagram yang menjelaskan secara garis besar alur logika sebuah penelitian. Adapun kerangka pemikiran dari aplikasi ini yaitu di jelaskan pada Gambar 1.1.



1.7. Sistematika Penulisan

Adapun untuk memberikan gambaran dan sistematika dalam menyusun penelitian ini terbagi menjadi lima bab dengan urutan sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini berisi uraian tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, kerangka pemikiran, metodologi penelitian, dan sistematika penulisan.

BAB II : STUDI PUSTAKA

Dalam bab ini akan diuraikan secara singkat mengenai teori, state of the art, landasan, paradigma, dan cara pandang serta metode-metode yang telah ada atau akan digunakan dalam penyelesaian laporan pembuatan sistem aplikasi, perangkat keras, dan perangkat lunak yang dibangun.

BAB III : PERANCANGAN SISTEM

Bab ini mengungkapkan permasalahan lebih khusus guna mencari alternatif pemecahan masalah serta rancangan suatu pemecahan masalah yang mungkin dilakukan.

BAB IV : IMPLEMENTASI SISTEM

Bab ini memuat implementasi dari perancangan yang telah dibuat dan pembahasannya. Bab ini juga mencakup gambar tampilan dari program serta modul program yang mendukung.

BAB V : PENUTUP

Dalam bab ini berisi kesimpulan yang merupakan rangkuman keseluruhan isi yang sudah dibahas serta saran seputar perluasan, pengembangan, pendalaman, dan pengkajian ulang.