BAB I
PENDAHULUAN

1.1 Latar Belakang

Kehadiran komputer memberi perhatian yang lebih bukan hanya dalam pengolahan data saja melainkan juga dengan keamanan data. Teknologi jaringan komputer yang saat ini berkembang, memungkinkan satu komputer dapat terhubung dengan komputer lainnya di belahan dunia ini untuk saling berbagi data dan informasi.

Semenjak kehadiran internet pada kehidupan manusia, kontrol atas informasi bergerak dengan amat cepat. Termasuk pula informasi-informasi yang harus mendapatkan "perhatian" khusus karena nilai informasi tersebut yang sangat penting semisal informasi intelijen, militer, dan berbagai macam informasi yang sering dilabeli *TOP SECRET*.

Kehidupan sekarang pun, orang-orang banyak yang menyimpan suatu pesan pada media *digital*. Terkadang ada juga pesan yang merupakan informasi rahasia yang disimpan pada media gambar namun sang pemilik pesan tersebut hanya mengizinkan beberapa orang saja yang dikehendaki untuk mengetahuinya. Tetapi ada saja pihak maupun orang yang ingin mengetahui isi pesan tersebut untuk kepentingan tertentu namun sebenarnya tidak diberi hak oleh sang pemilik pesan.

Adanya masalah di atas memunculkan ilmu baru pada dunia informatika yang disebut kriptografi yang merupakan pengembangan dari kriptologi. Berbagai pakar kriptografi telah mengembangkan berbagai macam algoritma enkripsi. *Advanced encryption standar* atau yang sering di sebut AES merupakan algoritma yang pernah menjadi sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia.

Teknologi *Watermark* juga merupakan suatu solusi didalam melindungi kerahasiaan dari tanda kepemilikan. *Watermark* dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan kecuali orang yang telah mengetahui

kuncinya, karena hasil keluaran *Watermark* adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia, namun berbeda apabila dilihat dengan perangkat pengolah data digital seperti komputer, sedangkan perubahan pesan dalam kriptografi dapat dilihat dan disadari langsung oleh indera manusia.

Penggunaan teknik *Watermark* dan kriptografi secara bersamaan dimaksudkan untuk memberikan keamanan berlapis dalam pengamanan pesan sebagai tanda kepemilikan. Pada skripsi ini akan dibahas mengenai penyisipan data yang sudah di enkripsi dengan kriptografi algoritma *AES* ke dalam sebuah citra dengan metode penyisipan *Least Significant Bit* atau yang sering di singkat *LSB*.

1.2 Rumusan Masalah

Dalam pelaksanaan penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan ini, diantaranya adalah sebagai berikut :

1 Bagaimana mengimplementasi teknik kriptografi AES dan Watermark metode LBS pada data citra RGB (Red Green Blue)?

2 Bagaimana kualitas dan perbedaan citra sebelum dan sesudah disisipkan teks?

3 Bagaimana perfoma teknik kriptografi AES dan Watermark dengan metode LBS?

1.3 Batasan Masalah

Dalam penulisan skripsi ini penulis membatasi sebagai berikut :

1. Data rahasia yang akan disisipkan hanya berupa teks.
2. Citra masukan berupa citra berwarna RGB yang akan disisipi oleh data rahasia.
3. Penelitian ini hanya sebatas pengimplementasikan algoritma AES ke dalam teknik Watermark LBS dan tidak membahas tentang distribusi kunci.

4. Diimplementasikan ke dalam bahasa pemrograman java dan di jalankan di sistem operasi windows.
5. Tipe Watermark yang digunakan adalah invisible.
6. Tidak membahas masalah keamanan pada algoritma AES dan metode LBS.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk menawarkan alternative dalam hal penyisipan pesan maupun penyadian pesan. Selain itu, penelitian ini juga bertujuan untuk menganalisis kinerja dan perfoma algoritma AES dan Watermark metode LBS dengan data terbatas.

1.5 Manfaat Penelitian

Manfaat yang diharapkan adalah alternative enkripsi data menggunakan algoritma AES dan Watermark metode LBS mampu diterapkan secara tepat oleh pihak-pihak maupun instansi yang menginginkan kerahasiaan dari informasi tetap terjaga. Selain itu mendapatkan alternatif cara yang unik dalam penyembunyian pesan.

1.6 Metode Pengumpulan Data

Dalam kasus ini penulis menggunakan beberapa metode 2 metode pengumpulan data, yaitu :

1. Metode Kepustakaan

   Penulis melakukan studi literatur dari dari berbagai tulisan ilmiah dan melakukan download data dari berbagai macam sumber dari internet.
2. Metode Eksperimental

   Penulis menyajikan simulasi enkripsi dan dekripsi data serta hasil dan analisanya.

1.7 Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan diuraikan dalam bentuk bab, dan masing-masing bab akan dipaparkan dalam beberapa sub bab, diantaranya :

BAB I. Pendahuluan

Dalam bab ini akan menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metode pengumpulan data dan sistematika penulisan.

BAB II. Landasan Teori

Dalam bab ini akan membahas dan menjelaskan mengenai dasar teoritis yang menjadi landasan dan mendukung pelaksanaan penulisan scripsi.

BAB III. Analisis dan Perancangan Sistem

Dalam bab ini akan membahas tentang analisis kebutuhan sistem dan perancangan sistem antara lain use case diagram, class diagram, flowchart sistem dan flowchart program.

BAB IV. Implementasi dan Pembahasan

Dalam bab ini akan membahas tentang hasil pengujian kecepatan berdasarkan proses, pembahasan kode program, dan petunjuk penggunaan aplikasi.

BAB V. Penutup

Dalam bab ini akan disampaikan kesimpulan dan saran dari keseluruhan bahasa.