

BAB I PENDAHULUAN

1.1. Latar Belakang Masalah

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. *DES* 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 *DES* ke dalam sebuah citra dengan metode penyisipan *LSB*.

Berdasarkan latar belakang masalah diatas maka tema penulisan skripsi ini, adalah "Meningkatkan Keamanan Pesan Pada Gambar ber-*Watermark* Dengan Alogritma Kriptografi *DES*".

1.2. Rumusan Masalah

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

1. Bagaimana mengimplementasikan teknik kriptografi *DES(Data Encryption Standard)* dan *Watermarking* metode *LSB(Least Significant Bit)* pada data citra RGB?
2. Bagaimana kualitas dan perbedaan citra sebelum dan sesudah disisipkan teks?
3. Bagaimana performa teknik kriptografi *DES* dan *watermark* dengan metode *LSB*?

1.3. Batasan Masalah

Pembatasan masalah pada penulisan skripsi ini sebagai berikut :

1. Data rahasia yang akan disisipkan berupa data teks.
2. Citra masukan berupa citra berwarna format RGB yang akan disisipi oleh data rahasia.
3. Penelitian ini hanya sebatas pengimplementasian algoritma *DES* ke dalam teknik *Watermark LSB* dan tidak membahas tentang distribusi kunci.
4. Diimplementasikan ke dalam bahasa pemrograman java J2SE dan dijalankan di sistem operasi Windows.
5. Tipe *Watermark* yang digunakan adalah *invisible*.
6. Tidak membahas masalah keamanan pada algoritma *DES* dan metode *LSB*.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah untuk menawarkan alternatif dalam hal penyisipan pesan maupun penyandian pesan. Selain itu, penelitian ini juga bertujuan untuk menganalisis kinerja dan performa algoritma *DES* dan *Watermark* metode *LSB (Least Significant Bit)* dengan data terbatas.

1.5. Manfaat Penelitian

Manfaat yang diharapkan adalah alternatif enkripsi data menggunakan algoritma *DES* dan *Watermark* metode *LSB* 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

Metode pengumpulan data adalah cara atau teknik yang dilakukan peneliti untuk menyusun karya tulis dan mengumpulkan data-data yang dibutuhkan. Dalam kasus ini penulis menggunakan beberapa metode pengumpulan data, yaitu:

1. Metode Kepustakaan

Metode kepustakaan merupakan studi literatur untuk mengumpulkan data atau informasi yang berhubungan dengan objek penelitian yang dilakukan. Penulis melakukan studi literatur dari berbagai tulisan ilmiah dan melakukan *download* data dari berbagai macam sumber dari internet.

2. Metode Eksperimental

Metode eksperimental dilakukan dengan cara mengimplementasikan perancangan yang telah dibuat ke dalam komputer. Objek dalam hal ini penulis menyajikan simulasi enkripsi dan dekripsi data serta hasil dan analisisnya.



