BAB I

PENDAHULUAN

I.1 Latar Belakang Masalah

Saat ini komunikasi data melalui media internet merupakan hal yang umum. Kendala keamanan informasi dari data yang dikirimkan merupakan masalah yang dihadapi dalam komunikasi data. Berikut ini merupakan salah satu cara untuk meningkatkan keamanan informasi data yang berbentuk citra hitam putih.

Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali dengan istilah sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi atau data awal.

Kriptografi visual diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994 yang mengubah gambar rahasia (*hidden image*) menjadi n buah transparansi (*share*) dan kemudian gambar rahasia tersebut hanya bisa dibaca jika n buah transparansi tersebut diletakkan bertumpuk secara bersamaan. Skema kriptografi yang diperkenalkan oleh mereka disebut dengan *Visual Secret Sharing Scheme* (VSSS).

Sistem Kriptografi visual adalah salah satu teknik dalam kriptografi yang memungkinkan informasi yang bersifat visual untuk dienkripsi dengan metode tertentu untuk mendekripsinya dapat dilakukan dengan penglihatan manusia. Pada kriptografi visual, gambar diurai menjadi n-bagian yang disebut *share* (yang tidak dapat dikenali). Kerahasiaan ini dapat terjadi karena citra dapat dideskripsikan apabila terdapat n buah *share*, sedangkan n-1 *share* tidak akan memberikan informasi visual.

Keamanan skema ini dianggap baik dan hampir tidak dapat dipecahkan. Cara untuk mendeskripsikan pesan tersebut juga sangat mudah. Untuk proses dekripsi kriptografi visual tanpa perluasan piksel cukup dengan menumpukkan *share* 1 dan

share 2. Setelah digabungkan, maka dapat melihat informasi yang terkandung di dalamnya. Perbedaan antara kriptografi visual biasa dengan kriptografi visual tanpa perluasan piksel adalah pada kriptografi visual biasa menggunakan pola yang sudah ada (*pattern book*) dan adanya perluasan piksel, sedangkan pada kriptografi tanpa perluasan piksel tidak adanya perluasan piksel pada *secret image* yang akan dienkripsi dan tidak menggunakan pola (*pattern book*).

I.2 Perumusan Masalah

Permasalahan yang akan dibahas dalam Tugas Akhir ini meliputi :

1. Bagaimana membuat sistem yang dapat membuat suatu citra asli menjadi tidak dikenali informasinya?
2. Bagaimana cara mengembalikan citra yang tidak dikenal informasinya, menjadi citra asal yang dikenali?

I.3 Tujuan

Tujuan yang ingin dicapai dari Tugas Akhir ini adalah merancang dan merealisasikan perangkat lunak yang mampu melakukan proses kriptografi visual dengan melakukan pengkodean citra hitam putih menjadi dua buah citra bayang dengan menggunakan metoda tanpa perluasan piksel dan pendekodean menjadi citra asal dengan menggunakan MATLAB.

I.4 Pembatasan Masalah

1. Dimensi citra yang digunakan adalah 64x64, 128x128, 256x256 dan 200x360 piksel.
2. Penggabungan citra berupa citra hitam, putih.
3. Terdapat 2 (dua) *secret image* sebagai citra input (*Multiple Secret*).
4. Tidak adanya perluasan piksel pada setiap *secret image* yang akan dienkripsi.

I.5 Sistematika Penulisan

Sistematika pembahasan laporan Tugas Akhir ini disusun menjadi lima bab, yaitu sebagai berikut :

- Bab I PENDAHULUAN

  Pada bab pendahuluan ini dibahas tentang latar belakang, identifikasi masalah, perumusan masalah, tujuan, pembatasan masalah, metodologi, dan sistematika penulisan.

- Bab II LANDASAN TEORI

  Untuk memudahkan pembahasan tentang Tugas Akhir ini, disertakan teori pendahuluan yang dibahas pada Tugas Akhir ini adalah definisi kriptografi, tujuan kriptografi, pengenalan kriptografi visual, cara kerja kriptografi visual, serta model kriptografi.

- Bab III PERANCANGAN DAN REALISASI

  Untuk merealisasikan Tugas Akhir, perancangan perangkat lunak dibuat dengan menggunakan perangkat lunak Matlab. Pada bab ini akan dijelaskan cara kerja dan proses enkripsi serta dekripsi untuk perangkat lunak kriptografi visual.

- Bab IV DATA PENGAMATAN DAN ANALISA DATA

  Untuk melihat hasil rancangan perangkat lunak, maka dibuat pengujian perangkat lunak. Analisa data pengamatan dipaparkan pada bab ini.

- Bab V SIMPULAN DAN SARAN

  Simpulan dan saran disusun untuk memberikan gambaran tentang Tugas Akhir yang dilakukan.