

BAB I

PENDAHULUAN

Pada bab ini, dijelaskan pendahuluan dari pengerjaan Tugas Akhir meliputi latar belakang topik Tugas Akhir, rumusan masalah, tujuan penelitian, batasan masalah, sistematika pembahasan dari pengerjaan Tugas Akhir.

1.1 Latar Belakang

Dalam memudahkan berkomunikasi atau bertukar informasi dapat digunakan salah satu sarana yaitu internet. Pencurian data dapat terjadi dengan adanya kemajuan teknologi yang dapat merugikan pihak-pihak yang memiliki dokumen rahasia. Oleh karena itu, salah satu cara untuk mengamankan informasi rahasia tersebut yaitu dengan kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.

Kriptografi itu sendiri terdiri dari dua proses yakni proses enkripsi dan proses dekripsi. Enkripsi merupakan proses penggunaan algoritma yang kompleks untuk mengkonversi pesan tertentu (*plaintext* atau *cleartext*) ke suatu pesan terenkripsi (*chipertext*). Hal ini dimaksudkan untuk mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Sedangkan dekripsi merupakan proses penggunaan algoritma yang kompleks untuk mengkonversi pesan terenkripsi (*chipertext*) ke suatu pesan tertentu (*plaintext* atau *cleartext*).

Kriptografi visual adalah sebuah teknik kriptografi yang memungkinkan penyembunyian informasi visual atau citra (enkripsi) sehingga tidak bermakna. Teknik ini diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam jurnal *Eurocrypt'94*. Teknik ini dilakukan dengan membagi citra plaintext menjadi beberapa share yang merupakan hasil enkripsinya. Dari beberapa hasil

enkripsi tadi, proses dekripsi dilakukan dengan menumpuk share yang ada dengan benar sehingga terlihat makna dari citra tersebut. Ekspansi piksel merupakan istilah untuk perbesaran atau perluasan suatu piksel. Perbesaran yang dimaksud disini adalah setiap piksel pada citra awal diekspansi atau direpresentasikan menjadi m buah piksel untuk citra baru. Hal ini mengakibatkan citra baru tersebut akan mengalami perbesaran sesuai dengan perbesaran tiap pikselnya. Oleh karena itu, dibutuhkan kriptografi visual tanpa ekspansi piksel agar tidak terjadi perbesaran jumlah piksel dari citra semula maupun setelah proses enkripsi dan dekripsi (jumlah piksel tetap sama). Sedangkan kompresi RLE (*Run Length Encoding*) bertujuan untuk mengkodekan matriks citra hasil enkripsi atau *share*.

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas, masalah utama yang akan diangkat pada Tugas Akhir ini adalah merancang perangkat lunak untuk proses kriptografi visual tanpa ekspansi piksel kemudian dikompresi dengan metode RLE menggunakan program MATLAB.

1.3 Rumusan Masalah

Rumusan masalah pada Tugas Akhir ini adalah:

1. Bagaimana merancang kriptografi visual tanpa ekspansi piksel dan dikodekan dengan algoritma RLE pada program MATLAB?
2. Bagaimana performansi citra hasil dekripsi setelah melalui proses kriptografi visual tanpa ekspansi piksel dan dikodekan dengan algoritma RLE?
3. Bagaimana perbandingan antara citra hasil dekripsi tanpa *additional basis* dan dengan *additional basis* pada program MATLAB?

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari Tugas Akhir ini adalah merancang dan merealisasikan perangkat lunak untuk proses kriptografi visual tanpa ekspansi piksel dan dikodekan dengan algoritma RLE menggunakan MATLAB.

1.5 Batasan Masalah

Pembatasan masalah pada Tugas Akhir ini meliputi :

1. Citra yang diproses hitam putih.
2. Jumlah *share* yang akan digunakan adalah sebanyak 3 *share*.
3. Matriks citra hasil enkripsi akan dikodekan dengan algoritma RLE.
4. Implementasi dilakukan dengan bahasa pemrograman MATLAB R2012a.

1.6 Sistematika Pembahasan

Sistematika penulisan yang akan digunakan untuk menyusun laporan Tugas Akhir ini adalah sebagai berikut:

1. Bab I Pendahuluan

Pada bab ini akan dibahas mengenai latar belakang, perumusan masalah, identifikasi masalah, tujuan, pembatasan masalah, dan sistematika penulisan dari Tugas Akhir ini.

2. Bab II Landasan Teori

Pada bab ini akan dibahas mengenai teori-teori penunjang yang akan digunakan untuk merancang perangkat lunak untuk proses kriptografi visual tanpa ekspansi piksel dan dikodekan dengan algoritma RLE.

3. Bab III Perancangan Perangkat Lunak

Bab ini berisi penjelasan desain yang akan dilakukan dalam membuat perangkat lunak untuk proses kriptografi visual tanpa ekspansi piksel dan dikodekan dengan algoritma RLE.

4. Bab IV Data Pengamatan dan Analisa Data

Bab ini berisikan percobaan-percobaan yang dilakukan terhadap perangkat lunak dan menampilkan data pengamatan serta analisis hasil percobaan.

5. Bab VI Simpulan dan Saran

Bab ini berisikan kesimpulan dari hasil percobaan yang telah didapatkan dari Tugas Akhir serta saran-saran yang dapat digunakan untuk membantu dalam pengembangan Tugas Akhir ini.