

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi komputer yang semakin canggih, hal ini juga diikuti dengan peningkatan kebutuhan akan teknologi baik perangkat keras ataupun perangkat lunak, karena banyak pekerjaan dapat diselesaikan dengan cepat, akurat, dan efisien. Sejalan dengan perkembangan teknologi tersebut, semakin mengubah cara masyarakat dalam berkomunikasi. Dahulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti email, SMS (*Short Messaging Service*) dan internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan.

Internet telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat melewati batas-batas negara dan budaya. Selain itu juga pengembangan perangkat baru misalnya ponsel, *notebook*, *computer screen*, *MP4*, dan *digital camera* menyebabkan konsumsi konten media yang terus bertambah. Namun tidak semua perkembangan teknologi komunikasi memberikan dampak yang positif dan menguntungkan. Salah satu dampak negatif dalam perkembangan teknologi adalah penyalahgunaan informasi dari konten multimedia (dalam hal ini citra digital atau foto). Sebagai contoh adalah tindak kejahatan penyebaran citra digital yang bersifat pribadi ke media jaringan internet, dengan tujuan untuk pemerasan atau merusak nama baik. Hal tersebut bisa terjadi karena dalam penyajiannya, citra digital tidak mengalami proses enkripsi atau pengamanan terhadap informasi yang dimilikinya. Sehingga pengguna bisa melihat jelas informasi apa yang terkandung dalam citra digital tersebut. Oleh sebab itu, diperlukan pengamanan terhadap informasi dari citra digital. Hal tersebut bertujuan agar dalam penyajiannya, informasi dari citra digital hanya bisa dilihat oleh pemiliknya atau pihak yang mempunyai kunci akses pada citra digital

tersebut. Sedangkan pengguna lain hanya bisa melihat citra digital dengan informasi piksel citra yang bersifat acak.

Pada penelitian sebelumnya oleh K. Loukhaoukha, telah dilakukan pengamanan informasi pada citra digital dengan pengacakan piksel pada citra hitam putih menggunakan prinsip kerja kubus permainan rubik. Pada penelitian tersebut dilakukan pengujian dengan menggunakan serangan penambahan *noise salt and pepper* dan diperoleh nilai MSE 3.42×10^3 untuk citra dengan dimensi 64x64 piksel. Pada penelitian K. Loukhaoukhan, untuk melakukan pengacakan pada piksel citra asli, digunakan prinsip kubus rubik, yakni dengan cara memindah posisi piksel pada citra. Pada penelitian tersebut digunakan dua buah kunci, kunci yang pertama digunakan untuk proses operasi xor dengan piksel citra asli, sehingga dihasilkan piksel baru yang terenkripsi. Sedangkan kunci yang kedua digunakan untuk melakukan proses rotasi atau pergeseran piksel pada citra (Loukhaoukha. K, 2012). Sehingga dengan teknik tersebut memungkinkan informasi bisa kembali. Selain itu, teknik tersebut memiliki tingkat error yang kecil terhadap pengujian dengan serangan. Berdasarkan latar belakang yang telah dikemukakan, penulis mencoba mengembangkan dari algoritma *rubic's cube* yang telah diajukan sebelumnya menggunakan citra hitam putih, disini penulis melakukan pengembangan dengan menggunakan ruang warna *RGB (Red Green Blue)*, sehingga judul yang diambil dalam skripsi ini adalah **“Enkripsi Citra Digital Dengan Menggunakan Algoritma Rubic's Cube”**.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang permasalahan yang ada, maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana mengimplementasikan teknik pengamanan pada citra digital menggunakan algoritma *Rubic's Cube*.
2. Bagaimana kualitas citra digital setelah dilakukan proses enkripsi menggunakan algoritma *Rubic's Cube*.
3. Bagaimana ketahanan citra digital terhadap manipulasi citra yang umum dilakukan yakni penambahan *noise*, *blur* dan *center cropping*.

1.3 Tujuan

Berdasarkan pada masalah yang telah diidentifikasi, maka tujuan yang hendak dicapai skripsi ini adalah:

1. Menghasilkan perangkat lunak untuk pengamanan citra digital yang mengimplementasikan algoritma *rubic's cube*.
2. Mengetahui perubahan kualitas citra digital setelah dilakukan proses enkripsi menggunakan algoritma *rubic's cube*.
3. Mengetahui ketahanan citra digital terhadap manipulasi citra yang umum dilakukan yakni penambahan *noise*, *blur* dan *center cropping*.

1.4 Batasan Masalah

Batasan masalah bertujuan agar penelitian yang dilakukan tetap mengacu pada topik penelitian. Batasan masalah dalam penelitian ini adalah:

1. Citra masukan yang digunakan dan citra keluaran yang dihasilkan dalam proses enkripsi dan dekripsi hanya citra dengan *format bitmap* 24 bit dengan ruang warna *RGB* dengan dimensi citra 512x512 piksel.
2. Menggunakan algoritma *rubic's cube* dalam proses enkripsi dan dekripsi.
3. Pengujian serangan pada citra hanya menggunakan teknik penambahan *noise* dengan *amount* 10%, 20% dan 30% untuk *gaussian noise*. *Blur* dengan *radius* 1, 1.5 dan 2 piksel *gaussian blur*. *Center cropping* sebesar 10%, 20%, dan 30% dari dimensi citra.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Menyediakan aplikasi untuk melakukan enkripsi dan dekripsi pada citra digital, sehingga diharapkan informasi rahasia yang akan dipertukarkan melalui media citra hanya dapat diketahui dan diakses oleh orang yang memiliki wewenang saja.
2. Menyediakan referensi mengenai kriptografi terhadap citra digital menggunakan algoritma *Rubic's Cube*.

1.6 Metode Penelitian

Untuk mencapai tujuan yang dirumuskan sebelumnya, maka penyusunan skripsi ini menggunakan metodologi sebagai berikut :

1. Studi Literatur

Mempelajari teori – teori dari literatur dan artikel yang berhubungan dengan konsep Kriptografi, algoritma *Rubic's Cube*, citri-ciri citra digital serta metode-metode pengujian.

2. Perancangan dan Implementasi Sistem

Mengumpulkan data yang diperlukan, melakukan analisis dan membuat rancangan model perangkat lunak dengan analisis terstruktur dan mengimplementasikan hasil rancangan tersebut yaitu membuat piranti lunak enkripsi dan dekripsi citra digital menggunakan algoritma *Rubic's Cube*.

3. Uji Coba dan Analisis Hasil Implementasi

Melakukan pengujian perangkat lunak yang telah dibangun pada tahap implementasi.

4. Pembuatan Laporan

Membuat laporan tertulis mengenai skripsi ini berdasarkan sistematika penulisan skripsi yang telah ditetapkan.

1.7 Sistematika Penulisan

Pembuatan skripsi ini disusun berdasarkan sistematika penulisan sebagai berikut:

1. BAB I PENDAHULUAN

Berisi latar belakang masalah dari pembuatan perangkat lunak, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

2. BAB II KAJIAN PUSTAKA DAN DASAR TEORI

Menguraikan teori – teori yang erat hubungannya dengan kriptografi, algoritma *Rubic's Cube* dan citra digital.

3. BAB III METODOLOGI PERANCANGAN

Pada bab ini akan dijelaskan mengenai metode – metode yang digunakan dalam melakukan enkripsi dan dekripsi citra digital menggunakan algoritma *Rubic's Cube*.

4. BAB IV IMPLEMENTASI

Dalam bab ini akan dijelaskan mengenai implementasi sistem model sistem perangkat lunak untuk melakukan enkripsi dan dekripsi citra digital menggunakan algoritma *Rubic's Cube*.

5. BAB V ANALISIS DAN PEMBAHASAN

Dalam bab ini akan dijelaskan mengenai pembahasan dan analisis model sistem perangkat lunak pada proses enkripsi dan dekripsi citra digital menggunakan algoritma *Rubic's Cube*.

6. BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari seluruh rangkaian penelitian serta saran kemungkinan pengembangannya.

