

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi di era digitalisasi sekarang ini sangat berkembang pesat. Hal ini berpengaruh terhadap kebutuhan manusia yang semakin bergantung terhadap penggunaan teknologi. Dimulai dari kebutuhan pekerjaan, hiburan, dan menjadi kebutuhan demi kelancaran komunikasi dengan keluarga, kerabat, maupun teman.

Kemajuan teknologi ini juga diikuti dengan semakin mudahnya memperoleh data atau informasi. Pengiriman dan penyimpanan data bisa dilakukan dengan cepat, mudah, dan praktis. Proses penyimpanan data atau informasi ini perlu untuk diperhatikan dari aspek keutuhan, kerahasiaan, dan keamanannya. Informasi yang diperoleh dapat berupa *file* teks, citra, audio maupun video yang dikemas secara digital.

Pada zaman teknologi saat ini, citra menjadi salah satu dari sekian banyaknya bentuk informasi yang digunakan dalam pertukaran data atau informasi. Namun tidak jarang informasi tersebut disalah-gunakan oleh pihak-pihak yang tidak memiliki otoritas dan tidak bertanggung jawab, seperti manipulasi ataupun rekayasa citra. Sehingga data citra ini yang bersifat pribadi atau rahasia perlu untuk diamankan agar menghindari hal-hal yang dapat merugikan pribadi, organisasi, kelompok, maupun perusahaan. Hal seperti inilah yang menyebabkan pentingnya untuk mengamankan citra digital. Salah satu

metode yang dapat memecahkan masalah yang disebutkan di atas adalah dengan menggunakan teknik pengamanan data atau teknik kriptografi (*cryptography*).

Kriptografi adalah ilmu mengenai teknik enkripsi yang mengacak suatu data menggunakan kunci publik (*public key*) sehingga sulit dibaca oleh orang yang tidak memiliki kunci privat (*private key*) (Kromodimoeljo, 2010). Penggunaan kriptografi digunakan untuk mencegah adanya penyadapan data pada pengiriman dengan cara penyandian data (Kusumaningtyas, 2018). Penyandian data dengan cara mengubah teks asli (*plaintext*) menjadi teks yang tersandi (*ciphertext*) yang tidak mempunyai makna dan tidak dapat dibaca. Metode yang digunakan dengan menggunakan enkripsi untuk penyandian dan dekripsi untuk membuka penyandian tersebut. Proses enkripsi merubah data asli (*plaintext*) menjadi teks sandi (*ciphertext*). Sedangkan proses dekripsi merubah data tersandikan (*ciphertext*) menjadi data asli (*plaintext*) ketika data diterima.

Pada proses enkripsi dan dekripsi memerlukan algoritma, yang disebut algoritma kriptografi (*cipher*). Algoritma kriptografi sangat beragam, tujuannya membuat serumit mungkin pesan yang dikirim sehingga data didalamnya aman kemudian hanya orang yang berhak saja yang dapat menggunakan data tersebut.

Secara umum ada 2 jenis kriptografi yaitu kriptografi klasik dan kriptografi modern. Algoritma *route cipher* merupakan salah satu teknik kriptografi klasik yang menggunakan transposisi dalam melakukan enkripsi. (Bangun, 2019).

Berdasarkan latar belakang di atas, penulis hendak melakukan penelitian mengenai pengamanan citra digital dengan menggunakan algoritma *route cipher*. Kelebihan *route cipher* mempunyai kelebihan penentuan kunci yang paling kuat

karena mempunyai proses enkripsi yang rumit. Hal ini dikarenakan *key* yang lebih membuat proses enkripsi dan dekripsi menjadi fleksibel (Kusumaningtyas, 2018).

Proses yang akan dilakukan di dalam penelitian ini adalah menganalisa proses enkripsi dan dekripsi menggunakan algoritma *route cipher* kemudian merancang sistem keamanan *file* citra menggunakan alat bantu perancangan seperti *Unified Modelling Language* dan dengan *tools SharpDevelop*, sehingga menghasilkan sistem yang dapat mengamankan *file* citra dengan cara menyandikan *file* tersebut menggunakan algoritma *route cipher*. Setelah selesai perancangan, kemudian *file* citra akan dienkripsi dan didekripsi menggunakan sistem keamanan tersebut. Hasil dari proses enkripsi dan dekripsi berupa citra yang sulit dilihat oleh manusia.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana penggunaan algoritma *route cipher* dalam mengamankan citra digital.
2. Bagaimana perbedaan waktu proses enkripsi dan dekripsi antara citra yang memiliki resolusi berbeda pada aplikasi pengamanan citra digital menggunakan algoritma *route cipher*.

1.3 Batasan Basalah

Batasan masalah yang menjadi acuan dalam pengerjaan skripsi ini adalah:

1. Citra yang digunakan dengan ekstensi *.jpeg

2. Mencari perbedaan waktu saat proses enkripsi dan dekripsi *file* citra dalam satuan milisekon (Ms) berdasarkan ukuran *file* citra <2000 pixel.
3. Menggunakan alat bantu perancangan seperti Unified Modelling Language (UML) dan pengembangan sistem menggunakan tools SharpDevelop dengan bahasa pemrograman Visual C#.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk membangun sebuah aplikasi pengamanan citra digital dengan menggunakan algoritma *route cipher* berbasis *desktop*.
2. Untuk menganalisa proses waktu eksekusi (*running time*) enkripsi dan dekripsi pada pengaman file citra dalam satuan milisekon (ms).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Memberikan pengetahuan kepada penulis dalam merancang sebuah kriptosistem dalam pengamanan citra digital dengan menggunakan algoritma *route cipher*.
2. Menghasilkan aplikasi yang mampu menjaga keamanan data dalam bentuk *file* citra.
3. Membantu para pengguna dalam melindungi citra digital yang bersifat rahasia.
4. Menjadi bahan referensi bagi penelitian lain yang serupa.

1.6 Sistematika Penulisan

Dalam penulisan skripsi ini disajikan beberapa kelompok uraian dan pembahasan yang tersusun dalam penelitian ini.

BAB I : PENDAHULUAN

Bab ini membahas tentang latar belakang, tujuan, manfaat penelitian, rumusan masalah, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas teori-teori mengenai file citra, algoritma *route cipher*, dan beberapa penelitian yang berhubungan pada skripsi ini.

BAB III : METODE PENELITIAN

Bab ini berisi analisa permasalahan, pemecahan masalah, metode penelitian, metode pengembangan perangkat lunak, analisa dan perancangan sistem.

BAB IV : HASIL DAN PEMBAHASAN

Berisi tentang hasil dan pembahasan dari aplikasi pengaman citra digital yang telah dibuat.

BAB V

: KESIMPULAN DAN SARAN

Berisi kesimpulan dari keseluruhan bab-bab penulisan skripsi dan saran yang telah diajukan untuk pengembangan lebih lanjut.