1. Pendahuluan

1.1 Latar Belakang

Citra adalah suatu media yang biasa digunakan oleh banyak orang untuk mengabadikan suatu kejadian yang dianggap penting, berkesan atau bersejarah. Kita dapat mengingat atau mengenang kejadian-kejadian yang pernah terjadi di masa lalu hanya dengan melihat suatu citra. Selain itu dengan adanya citra kita dapat melihat suatu kejadian seperti fenomena alam yang jarang terjadi di suatu daerah tanpa kita harus berkujung ke daerah tersebut untuk melihatnya. Terdapat dua jenis citra, yaitu citra *analog* dan citra *digital* . Citra *analog* adalah citra yang telah tercetak pada media lain seperti kertas atau sejenisnya, sedangkan citra *digital* adalah citra yang dapat disimpan dalam format *digital* (dalam bentuk file).

Dengan adanya citra, kita dapat menggunakannya sebagai suatu media yang dapat menceritakan pengalaman pribadi. Terkadang, kita tidak ingin orang lain melihat suatu citra yang kita miliki dengan alasan *privacy*, malu, atau hanya rahasia pribadi segelintir orang saja. Namun, jika kita ingin menghapus citra tersebut sayang sekali, karena bisa jadi citra tersebut sangat berarti bagi kita sendiri.

Dengan adanya permasalahan diatas, maka dibutuhkan suatu program yang dapat melindungi kerahasiaan pada citra tersebut. Salah satu cara yang digunakan untuk pengamanan data adalah dengan menggunakan teknik kriptografi yaitu dengan menyandikan isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi, disertai dengan menggunakan kunci yang benar.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, integritas data, autentikasi data, serta non-repudasi. Banyak algoritma enkripsi yang ada saat ini, antara lain *Rijndael*, *Serpent*, *Twofish*, *MARS*, *RC6*, *MRC6*, *RSA*, dll.

Pada tahun 1998 diadakan suatu kompetisi untuk menetapkan metode algoritma enkripsi standar di Amerika. Pada kompetisi itu diperoleh lima finalis yaitu algoritma *Rijndael*, *Serpent*, *Twofish*, *MARS*, dan *RC6*. Pada kompetisi itu ditetapkan algoritma *Rijndael* sebagai algoritma standar untuk enkripsi di Amerika. Sedangkan *Serpent* dan *Twofish* sebagai juara kedua dan ketiga. *Rijndael* dipilih karena kecepatan proses enkripsinya dan kemudahan dalam pembentukannya. Sedangkan Serpent tidak menjadi juara satu karena algoritmanya yang sulit dan waktu enkripsinya yang relatif lama. Namun diantara semua metode tersebut algoritma *Twofish* dianggap sebagai algoritma yang memiliki tingkat keamanan yang tinggi dan metode ini bebas digunakan[2].

Algoritma *Twofish* menggunakan desain yang mudah dan tidak memiliki kunci lemah[8]. Desain yang mudah akan mempengaruhi kecepatan proses enkripsi dan dekripsi sehingga algoritma ini cocok untuk penyandian citra *digital* yang membutuhkan proses yang cepat . Sementara itu, dengan tidak adanya kunci

lemah maka kunci apapun yang menjadi masukkan oleh pengguna, tingkat keamanannya akan tetap sama. Berdasarkan latar belakang diatas, pada tugas akhir ini diajukan suatu proses penyandian citra *digital* menggunakan algoritma *Twofish* yang akan melakukan proses enkripsi dan dekripsi.

1.2 Perumusan Masalah

Pada penelitian Tugas Akhir ini, penelitian difokuskan pada analisis dan implementasi penyandian citra *digital* menggunakan algoritma *Twofish*. Berdasarkan latar belakang masalah, maka beberapa permasalahan utama yang akan dirumuskan antara lain:

a. Bagaimana mengimlementasikan algoritma *Twofish* dalam penyandian citra *digital*.
b. Mengetahui bagaimana performansi algoritma *Twofish* dalam mengenkripsi citra *digital* berdasarkan parameter waktu enkripsi/dekripsi, *avalanche effect*, besar file input/output setelah di enkripsi/dekripsi dan *brute force attack*.

1.3 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan Tugas Akhir ini adalah sebagai berikut:

a. Mengimplementasikan algoritma *Twofish* pada data berupa citra *digital* .
b. Menganalisis performansi seperti *avalanche effect*, kecepatan proses enkripsi/dekripsi, besar file input/output setelah di enkripsi-dekripsi menggunakan algoritma Twofish dan kemungkinan waktu yang dibutuhkan untuk memecahkan kunci menggunakan *brute force attack*.

1.4 Batasan Masalah

Yang menjadi batasan masalah dalam tugas akhir ini adalah :

a. File masukan yang digunakan adalah citra *digital* dengan format *jpg. atau *jpeg.
b. Menggunakan Algoritma Twofish sebagai algoritma enkripsi dan dekripsi.
c. Kunci yang digunakan berukuran 16 byte atau 128bit.
d. Masukan pada proses enkripsi berupa cita *digital* dan keluaran berupa file biner, sedangkan pada proses dekripsi masukan berupa file biner hasil enkripsi dan keluaran berupa citra *digital.*

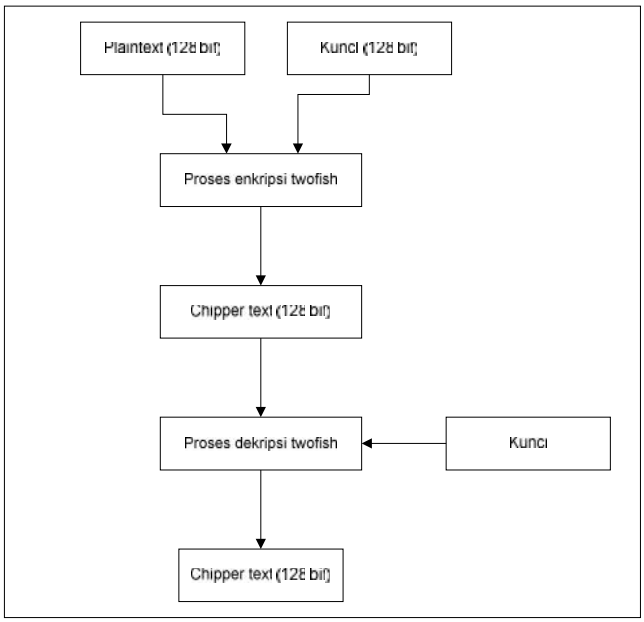
1.5 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan untuk penyelesaian permasalahan diatas adalah dengan menggunakan langkah-langkah sebagai berikut :

1. Studi literatur
   Pada tahap ini dilakukan pencarian sumber-sumber bacaan atau referensi dari buku, artikel maupun paper-paper yang terdapat pada internet serta memahami dan mempelajarinya sehingga dapat digunakan sebagai dasar teori dalam penyusunan Tugas Akhir ini. Literatur yang dicari adalah yang terkait dengan algoritma *Twofish*, penyandian data, enkripsi citra *digital* , serta informasi lain yang menunjang pembuatan tugas akhir ini.

2. Perancangan program yang akan dibuat.
   Pada tahap ini dilakukan perancangan perangkat lunak dalam membangun aplikasi desktop yang dapat melakukan enkripsi dan dekripsi citra *digital* menggunakan algoritma *Twofish*.
3. Implementasi
   Mengimplementasikan perancangan dengan menggunakan blok diagram dan diagram alir (*flowchart)* yang telah dibuat untuk membangun aplikasi ini menggunakan java.
4. Pengujian dan analisa hasil
   Menguji perangkat lunak yang telah di implementasikan, yaitu :
   1. Menguji avalanche effect pada citra *digital* yang telah di dekripsi.
   2. Menguji kecepatan proses enkripsi algoritma *Twofis*h pada penyandian citra *digital* .
   3. Menguji apakah terjadi perubahan besar file setelah proses enkripsi dan dekripsi.
   4. Menguji tingkat keamanan dalam proses penyandian citra *digital* pada algoritma Twofish.

5. Penarikan kesimpulan dan penyusunan laporan tugas akhir
   Tahap ini merupakan tahap penarikan kesimpulan terhadap pengujian yang telah dilakukan dan pembuatan laporan.



Gambar 1-1 : Gambaran Umum Proses Penyandian Citra Digital

Berdasarkan gambar 1-1, masukan dari proses enkripsi merupakan file plaintext berukuran dan kunci yang berukuran 128 bit dan keluaran setelah proses enkripsi berupa chipertext berukura 128 bit. Sedangkan untuk proses dekripsi, masukan berupa file chipertext dan kunci berukuran 128 bit dan keluaran berupa file plaintext berukuran 128 bit.