

BAB 1 PENDAHULUAN

1.1. Latar Belakang

Pada masa sekarang ini data merupakan aspek yang sangat penting dan berharga. Karena penting dan berharganya sebuah data maka, data – data ini harus diamankan agar tidak bisa jatuh ke orang yang salah. Apalagi banyak data – data yang disimpan dalam bentuk file citra yang sangat bersifat rahasia. Banyak gambar maupun citra yang bersifat rahasia ini biasanya memiliki informasi yang sangat penting dan tidak mungkin hanya dilihat oleh satu orang. Apabila terdapat lebih dari satu orang dan tidak berada di tempat yang sama, maka gambar tersebut harus dikirim melalui internet. Karena gambar tersebut yang bersifat rahasia maka sangat terlalu berbahaya apabila hanya dikirmkan dalam format biasa dan dikirimkan melalui internet biasa tanpa citra atau gambar tersebut dilakukan proses pengamanan data. Apabila hanya mengirim citra digital tersebut tanpa dilakukan pengaman data maka bisa saja ada yang menyadap file citra tersebut dan informasi yang ingin disampaikan menjadi tersebar ke masyarakat luas. Dengan adanya pengaman data tersebut bisa meminimalisir terjadinya hal itu. Agar data – data yang berisi dalam citra tersebut aman, maka harus dilakukan tindakan pengamanan tersebut. Salah satu bentuk untuk mengamankan data citra tersebut adalah dengan melakukan kriptografi. Salah satu contoh kasus penggunaan pengamanan citra adalah untuk dokumen yang dalam berbentuk citra.

Dalam dunia kriptografi ada dua tipe algoritma yang digunakan dan dilihat dari persamaan kuncinya, yaitu algoritma simetrik (symmetric algorithm) dan algoritma asimetrik (asymmetric algorithm). Salah satu contoh algoritma kriptografi yang digunakan disini adalah Advanced Encryption System (AES) yang bersifat simetrik. Dalam algoritma ini terdapat persamaan yaitu dimana kunci dekripsi dan kunci enkripsinya sama dengan terdapat tiga pilihan panjang kunci yaitu, 128bit, 192bit, dan 256bit.

Apabila citra digital yang telah dienkrpsi menggunakan algoritma Advanced Encryption System (AES) maka sudah dipastikan atau ada kemungkinan ukuran file yang sudah dienkrpsi akan melebihi dari ukuran awalnya, mungkin kalo hanya jumlah citra digitalnya hanya sedikit tidak akan menjadi masalah, namun apabila

citra digital yang dienkripsi dalam jumlah banyak maka tentu saja akan memberatkan media penyimpanan dimana seharusnya datanya sudah aman namun memiliki ukuran citra digital yang masih besar. Oleh karena itu dengan adanya teknik kompresi data ini, maka dapat menyusutkan ukuran data yang sudah dienkripsi. Sehingga data aman dan tidak memakan banyak ruang untuk disimpan ke dalam media penyimpanan tersebut. Teknik kompresi yang digunakan adalah dengan menggunakan algoritma kompresi Lempel-Ziv-Welch (LZW).

1.2. Rumusan Masalah

Dari latar belakang di atas yang telah dijelaskan, maka permasalahan yang akan di bahas adalah:

1. Berapa ukuran file sebelum dan sesudah untuk proses enkripsi dengan menggunakan algoritma kriptografi AES dan algoritma kompresi LZW?
2. Mengapa perlu digabungkan antar enkripsi dengan algoritma AES dan algoritma kompresi *Lempel-Ziv-Welch* (LZW)?
3. Bagaimana kondisi setelah citra digital di enkripsi dengan algoritma AES dan di kompresi dengan algoritma *Lempel-Ziv-Welch* (LZW)?

1.3. Batasan Masalah

Sedangkan batasan masalah yang dibahas penulis hanya terbatas pada pembahasan sebagai berikut:

1. File citra digital yang digunakan hanya berupa file yang memiliki format JPG dan PNG.
2. Algoritma AES yang digunakan untuk melakukan enkripsi dan dekripsi file citra digital tersebut.
3. Algoritma *Lempel-Ziv-Welch* (LZW) yang digunakan untuk melakukan proses pengkompresan file citra digital yang telah dienkripsi dengan algoritma AES.

1.4. Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah untuk meneliti suatu sistem untuk mengamankan file citra digital dengan menggabungkan algoritma AES untuk proses enkripsi dan dekripsi citra digital dengan algoritma Lempel-Ziv-Welch (LZW) untuk proses pengkompresan file citra digital yang telah dienkripsi.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Untuk individu dan organisasi

Merupakan sebuah solusi untuk pengamanan file citra dengan menggunakan kombinasi algoritma AES dan algoritma LZW sehingga memenuhi kebutuhan dalam konteks kerahasiaan dan keamanan citra digital.

2. Untuk penulis

Meningkatkan kemampuan dan pengetahuan dengan implementasi dalam bidang kriptografi dan kompresi mengenai algoritma AES dan algoritma LZW.

1.6. Ruang Lingkup

Ruang Lingkup yang terdapat pada penelitian yang dilakukan ini adalah mengenai kombinasi antara algoritma enkripsi dekripsi AES (Advanced Encryption System) dan algoritma kompresi dekompresi LZW (Lempel-Ziv-Welch) dalam proses pengamanan yang lebih efisien untuk file citra gambar yang memiliki tipe jpg dan png.

1.7. Luaran yang Diharapkan

Luaran yang diharapkan adalah dari penelitian ini adalah program dapat melakukan pengamanan data file citra digital dan pemampatan (kompresi) pada file citra digital. Dengan metode penggabungan antara algoritma enkripsi yang menggunakan AES dan algoritma kompresi dengan menggunakan LZW.

1.8. Sistematika Penulisan

Berikut merupakan sistematika penulisan penelitian ini:

BAB 1 PENDAHULUAN

Bab ini berisi tentang Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Ruang Lingkup, dan Sistematika Penulisan dari penelitian ini.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi tentang teori dasar yang berhubungan dengan penelitian ini dan juga digunakan dalam penelitian ini

BAB 3 METODE PENELITIAN

Bab ini menjelaskan tentang beberapa metode yang digunakan oleh penulis dan proses tahapan dalam melakukan penelitian yang dilakukan secara menyeluruh.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi hasil dari luaran dari program yang telah dibuat dan dibahas sesuai penelitian untuk menjawab permasalahan yang ada.

BAB 5 PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil penelitian yang telah dilakukan pada di bab 4 dalam proses penelitian ini sebagai suatu referensi dan acuan untuk penelitian yang dilakukna kedepannya.

DAFTAR PUSTAKA

RIWAYAT HIDUP