BAB I

PENDAHULUAN

I.I. Latar Belakang

Perkembangan teknologi yang semakin maju berdampak juga terhadap teknologi yang digunakan oleh masyarakat, dimana pada era *modern* ini kebutuhan masyarakat akan informasi meningkat, dengan adanya teknologi seperti sekarang ini sangat membantu masyarakat dalam berkomunikasi dan bertukar informasi. Namun teknologi yang berkembang tidak selalu menghasilkan dampak *positif*. Salah satu dampak *negatif* dari teknologi adalah maraknya pencurian data pribadi seperti gambar yang dilakukan oleh pihak–pihak yang tidak bertanggung jawab, sehingga jika data pribadi diberitakan ke publik oleh orang yang tidak bertanggung jawab tersebut, akan menimbulkan dampak yang kurang etis bahkan dapat menjadi bahan *pornografi*. Hal ini terjadi karena belum banyak aplikasi yang mudah digunakan publik untuk mengamankan data pribadi khususnya gambar.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. *Kriptografi* menggunakan berbagai macam teknik dalam upaya untuk mengamankan data termasuk gambar. Pengamanan gambar melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan gambar tersebut. Gambar tersebut harus tetap rahasia dengan bertujuan untuk menjaga karahasiaannya terhadap akses orang-orang yang tidak berhak. (Simatupang, 2017)

AES merupakan sistem penyandian blok yang bersifat non-feistel kerena *AES* menggunakan komponen yang selalu memiliki invers dengan panjang blok 128. Penyandian *AES* menggunakan proses yang berulang disebut

dengan ronde. jumlah ronde yang digunakan oleh *AES* tergantung panjang kunci yang digunakan. Enkripsi pesan teks pada *AES* adalah transformasi terhadap state secara berulang dalam beberapa ronde. *State* menjadi keluaran ronde, k masukan untuk ronde untuk ronde k-k+1. (Hasibuan, 2017)

Peneliti menggunakan AES dikarenakan AES sebagai salah satu algoritma yang penting tentu memiliki berbagai kegunaan yang sudah diaplikasikan atau diimplementasikan di kehidupan sehari-hari yang tentu saja membutuhkan suatu perlindungan atau penyembunyian informasi di dalam prosesnya. Salah satu contoh penggunaan AES adalah pada kompresi 7-Zip dan WinZip.

Fenomena yang ditemukan dalam penelitian ini yaitu jika data gambar tidak diamankan, data gambar bisa saja diakses oleh orang yang tidak bertanggung jawab dan pentingnya pengamanan untuk melindungi *privasi* atau kerahasiaan data. Penelitian ini difokuskan pada perancangan sistem untuk mengamankan gambar dengan menggunakan algoritma *AES (Advanced Encryption Standart)* untuk mengenkripsi dan mendekirpsi gambar. Sistem dibangun berbasis *web* yang bertujuan untuk membantu pengguna agar mudah mengakses aplikasi yang dibuat karena bersifat *online* dan *multiuser*. Dengan demikian, hasil penelitian ini dapat memberikan kontribusi kepada publik dalam hal sarana pengamanan gambar, yaitu untuk melindungi gambar yang bersifat pribadi dan tidak seharusnya menjadi konsumsi masyarakat luas serta kemudahan akses aplikasi.

Berdasarkan permasalahan tersebut, penulis mengangkat sebuah judul **"Aplikasi Pengamanan *Image* Menggunakan Metode Algoritma *AES (Advanced Encryption Standard)* Berbasis Web".**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Sehubungan dengan permasalahan yang ada maka penulis mencoba untuk mengidentifikasi masalah adalah :

1. Jika data gambar tidak diamankan, data gambar bisa saja diakses oleh orang yang tidak bertanggung jawab.
2. Pentingnya pengamanan untuk melindungi *privasi* atau kerahasiaan data.
3. Belum adanya aplikasi dengan mengimplentasikan keamanan data berupa *image* menggunakan algoritma *AES*.

I.2.2. Perumusan Masalah

Rumusan masalah pada penelitian ini yaitu :

1. Bagaimana merancang dan membangun sistem keamanan gambar menggunakan algoritma *AES*?
2. Bagaimana mengimplementasikan metode *AES (Advanced Encryption Standard)* untuk mengamankan gambar?
3. Bagaimana mengimplementasikan sistem keamanan gambar menggunakan bahasa pemograman *PHP*?

I.2.3. Batasan Masalah

Adapun batasan masalah dari penelitian ini yaitu :

1. Panjang kunci yang digunakan pada algoritma *AES* adalah 128 bit.
2. Format gambar yang digunakan adalah JPEG, JPG, dan PNG.
3. Besar ukuran gambar maksimal 3 MB.

1.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini yaitu :

1. Mengetahui cara pengamanan gambar menggunakan algoritma *AES (Advanced Encryption Standard).*
2. Mengimplementasikan algoritma *AES (Advanced Encryption Standard)* untuk keamanan gambar.
3. Menerapkan algoritma *AES (Advanced Encryption Standard)* pada aplikasi berbasis web.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini yaitu :

1. Meningkatkan pengetahuan tentang prosedur pengamanan gambar menggunakan algoritma *AES.*
2. Meningkatkan keamanan gambar dari orang-orang yang tidak bertanggung jawab
3. Meningkatkan efesiensi waktu dan keakuratan proses pengamanan gambar melalui sebuah aplikasi.

I.4. Metodologi Penelitian

I.4.1. Pengumpulan data

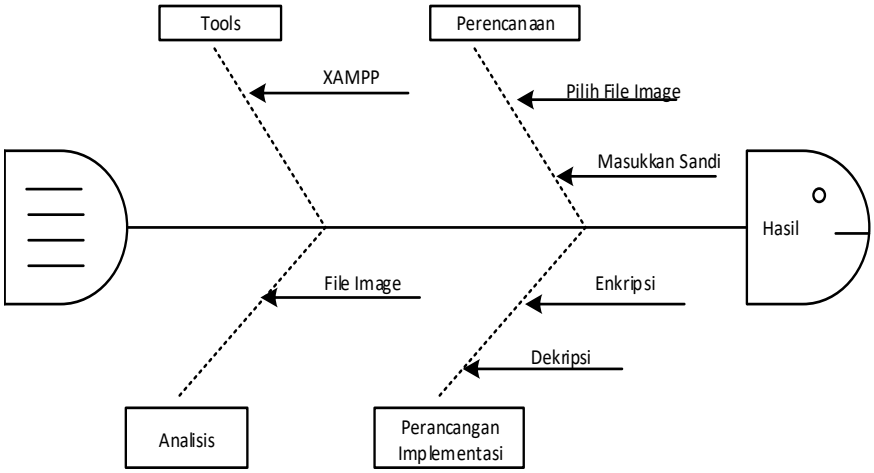
Berikut ini adalah beberapa teknik pengumpulan data yang peneliti lakukan untuk melengkapi bahan penelitian :

1. Tinjauan Pustaka (*Library Research*)

Pada tahapan ini peneliti menggunakan buku, jurnal dan karya ilmiah sebagai referensi dan landasan teori pada penelitian.

I.4.2. Metode Perancangan Sistem

Tahapan dalam penelitian ini dapat di modelkan dengan *Waterfall* metodologi penelitian. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar I. 1. Prosedur Perancangan

Keterangan :

1. **Analisa Kebutuhan**

   Peneliti menganalisis kebutuhan untuk perancangan sistem berupa *hardware* dan *software* yang nantinya akan digunakan untuk penelitian ini.

2. **Perancangan Sistem**

   Pada tahap ini peneliti merancang sebuah desain aplikasi pengamanan gambar dengan menggunakan algoritma AES Serta menggunakan pemodelan UML yaitu *use case diagram, class diagram, activity diagram, dan sequence* diagram untuk perancangan system.

3. **Penulisan Kode Program**

   Pada proses pengamanan gambar peneliti menggunakan bahasa pemrograman PHP dan menggunakan database MySQL dalam pembuatan system.

4. **Pengujian**

   Pada tahap ini peneliti melakukan pengujian aplikasi pengamanan gambar apakah sudah dapat mengamankan gambar dengan baik dan benar.

5. **Hasil**

   Pada tahapan ini peneliti telah menyelesaikan seluruh penelitian baik teori maupun aplikasi yaitu Aplikasi Pengamanan Gambar Menggunakan Metode Algoritma *AES (Advanced Encryption Standard)* Berbasis *web.*

I.5. Kontribusi Penelitian

Adapun kontribusi penelitian ini adalah :

Berdasarkan penelitian yang dilakukan oleh (Simatupang, "Aplikasi Pengamanan Data Gambar Dengan Menerapkan Algoritma Vigenere Cipher", 2017) dengan judul "Aplikasi Pengamanan Data Gambar Dengan Menerapkan Algoritma Vigenere Cipher" Tujuan penelitian ini yaitu penyandian gambar dengan

cara menginput gambar asli, lalu mengambil nilai decimal dari setiap pixel lalu menambahkan kunci. Sedangkan pada proses dekripsinya jumlah nilai elemen warna terenskripsi dikurang nilai kunci lalu di moduluskan 256. Perancangan aplikasi dengan *visual basic* 2008 akan memberikan penyelesaian permasalahan dengan mengoperasikan aplikasi yang telah dibuat seperti *form* login, *form* menu utama, *form* menu enkripsi dan *form* menu dekripsi.

Adapun perbedaan penelitian yang dilakukan penulis dengan penelitian terkait sebelumnya yaitu pada penelitian ini penulis menggunakan aplikasi berbasis *Web* untuk mengamankan data gambar. Dengan menggunakan bahasa pemrograman PHP dan algoritma *AES (Advanced Encryption Standard)* Sehingga dengan adanya aplikasi ini, dapat memberikan rasa aman lebih kepada *user* dalam menyimpan data gambar.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penelitian ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang

sedang dihadapi yaitu berupa pembahasan mengenai sistem wireless, UML dan normalisasi.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk system