BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini teknologi informasi sudah merambah tiap sendi kehidupan. Mulai dari hal-hal yang kecil hingga hal-hal besar sekalipun. Kemajuan teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia. Tetapi keuntungan yang ditawarkan oleh teknologi informasi juga menimbulkan kejahatan seperti pencurian data. Padahal saat ini tiap saat terjadi berbagai jenis transaksi dalam proses penyebaran informasi. Oleh karena itu dibutuhkan perkembangan ilmu untuk Mengamankan data agar pengguna teknologi selalu merasa aman (Zelviana dkk 2012).

Data terdiri dari berbagai macam jenis, yaitu berupa Gambar/citra, tulisan, suara, dan video. Berkat kemajuan teknologi, berbagai jenis data tersebut dapat dinikmati secara digital dan dapat disebarluaskan secara bebas. Namun tidak bisa dipungkiri, data yang penyebarluasannya dapat dilakukan dengan bebas tersebut akan rentan terhadap keamanannya, karena dapat diubah, dihapus, ataupun dimanipulasi oleh orang yang tidak bertanggungjawab. Salah satu jenis data yang sering dimanipulasi adalah data citra atau Gambar. (Hanifah, 2012)

Saat ini citra banyak digunakan dalam berbagai bidang seperti bisnis, iklan, pendidikan, medis, dan lain-lain. Dengan semakin banyaknya penggunaan citra dalam lini masa kehidupan, tentu saja perlu diperhatikan kerahasian, keutuhan dan keaslian datanya. Karena kerahasian sebuah informasi bersifat penting dan sangat pribadi (Hafidz dkk 2011). Oleh karena itu, perlu diterapkan pengamanan data dalam sebuah data. Salah satu teknik untuk mengamankan data adalah teknik penyandiaan data.

Teknik penyandian data atau yang biasa disebut dengan teknik kriptogafi adalah teknik dalam menyembunyikan data agar tidak dapat dibaca oleh orang yang tidak berkepentingan. Dalam bukunya, Setyaningsih menjelaskan bahwa “Sebelum tahun 1970-an, teknologi kriptografi digunakan hanya untuk tujuan miter dan diplomasi. Namun kemudian, bidang bisnis dan perorangan pun mulai

menyadari pentingnya untuk melindungi informasi berharga" (Setyaningsih, 2015).

Dalam penggunaan kriptografi sebagai pengamanan data, diperlukan sebuah algoritma kriptografi sebagai pendukung utama dalam peningkatan kerahasian masing-masing sistem kriptografi. Saat ini terdapat banyak algoritma yang dapat dipergunakan dengan kelebihan dan kekurangannya masing-masing. Jenis algoritma yang biasa dipergunakan dalam kriptografi adalah jenis algoritma simetris dan algoritma asimetris. Algoritma simetri adalah jenis algoritma yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsinya. Sementara algoritma asimetri menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsinya. Masalah yang rentan terjadi pada algoritma simetri adalah bahwa agar orang yang ingin mengenkripsi ataupun mendekripsi data harus memiliki kunci yang sama dimana jalan satu-satunya adalah dengan menyebarluaskan kunci tersebut. Sehingga dalam penyebarluasan kunci tersebut diperlukan kepercayaan lebih oleh masing-masing individu. Selain itu juga dibutuhkan jalur yang aman dalam penyebarluasan kuncinya (O 'keeffe, 2008). Oleh karena itu, pada penelitian ini, peneliti akan menggunakan algoritma asimetri, karena dalam proses penyebarluasan kuncinya tidak memerlukan jalur khusus, karena proses enkripsi dan dekripsinya menggunakan kunci yang berbeda. Saat ini terdapat berbagai jenis algoritma kunci publik, diantaranya adalah *Digital Signature Algorithm* (DSA), algoritma RSA, dan algoritma *Paillier Cryptosystem.* Beberapa karakteristik dari algoritma *Paillier Cryptosystem* adalah proses enkripsinya dilakukan perkarakter sehingga algoritma ini disebut sebagai algoritma probabilistik yang efisien. Selain itu, salah satu kelebihan dari algoritma *Paillier Cryptosystem* adalah adanya sifat homormofisme dan *self-blinding*. Beberapa sifat inilah yang membuat algoritma *Paillier Cryptosystem* dapat dipergunakan untuk berbagai keperluan.

Didalam laporan tugas akhir ini, penulisan akan menggunakan salah satu jenis algoritma kunci publik. Algoritma yang akan dipergunakan adalah *Paillier cryptosystem*. Jenis algoritma ini akan digunakan dalam pengamanan data citra digital yang bertipe RGB dan *grayscale*. Oleh karena itu, penulis akan membuat

Tugas Akhir dengan judul "Algoritma *Paillier Cryptosystem* untuk Mengamankan Citra Digital"

1.2 Perumusan Masalah

1. Bagaimana menggunakan Algoritma *Paillier cryptosystem* untuk mengamankan Citra Digital ?
2. Bagaimana proses enkripsi dan dekripsi pada *Paillier cryptosystem*?
3. Bagaimana tingkat keamanan dari data citra digital yang sudah dienkripsi?

1.3 Pembatasan Masalah

1. Data yang akan dienkripsi adalah data citra / Gambar dengan format *.bmp, *jpg atau *png.
2. Algoritma yang akan dipergunakan adalah *Paillier cryptosystem.*
3. Pembuatan aplikasi pengamanan citra digital ini dilakukan menggunakan software MATLAB.

1.4 Tujuan Penelitian

1. Menggunakan algoritma *Paillier cryptosystem* untuk pengamanan citra digital.
2. Membangun aplikasi pengamanan citra digital berbasis *Paillier cryptosystem.*
3. Menguji tingkat keamanan hasil enkripsi data citra melalui analisis histogram dan analisis koefisien korelasi.

1.5 Manfaat Penelitian

1. Aplikasi ini dapat membantu untuk mengamankan data citra digital.
2. Laporan Tugas Akhir ini dapat membantu menjelaskan konsep dari *Paillier cryptosystem* dalam mengenkripsi dan mendekripsi citra.

1.6 Metode Penelitian

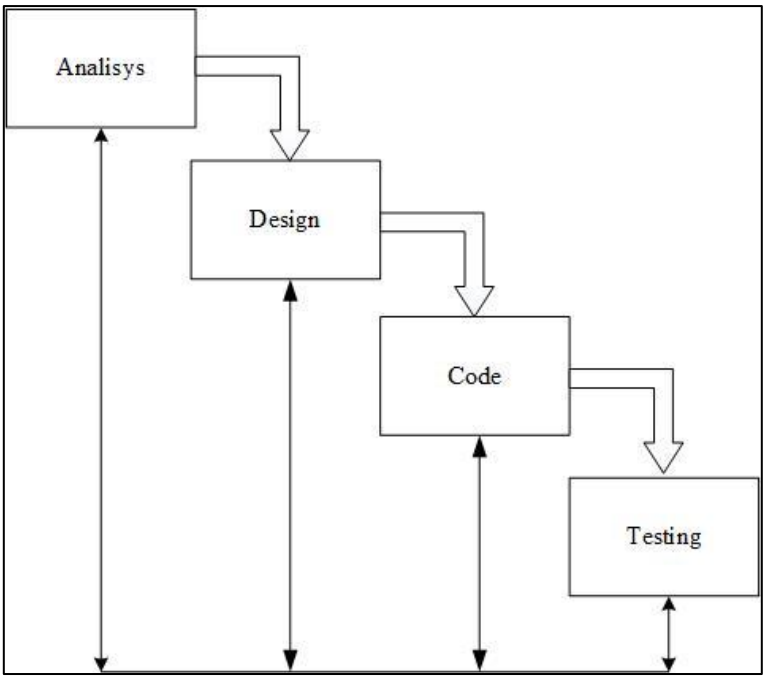
Metodologi penelitian pada laporan tugas akhir ini adalah sebagai berikut :

1. Metode Pengumpulan Data

   Sumber data dalam penelitian ini adalah data sekunder. Jadi pengumpulan data diperoleh peneliti secara tidak langsung melalui media perantara dalam hal ini yaitu internet. Data yang dibutuhkan dalam penelitian ini adalah citra digital RGB atau *grayscale* yang berformat bitmap, JPEG, atau PNG.

2. Model Proses Pengembangan Sistem

Proses dalam pengembangan sistem ini menggunakan model *modified waterfall* menurut referensi Pressman. Dibawah ini model *modified waterfall* yang akan diterapkan pada sistem (Nur dkk 2015).



Gambar 1. 1 Langkah-langkah penelitian (Nur dkk 2015)

Berdasarkan model *waterfall* pada Gambar 1.1, maka tahapan prosedur penelitian yang akan dilakukan adalah sebagai berikut:

a. Analisys

Pada tahap ini akan dilakukan analisa kebutuhan atas apa saja yang akan dibutuhkan dalam pembangunan sistem, dalam hal ini peneliti telah membaginya kedalam 2 analisa kebutuhan. Yaitu analisa kebutuhan fungsional dan analisa kebutuhan non-fungsional

b. Design

Pada tahap ini akan dilakukan tahap desain terhadap sistem. Adapun tahap desain yang dilakukan peneliti adalah tahap desain pemodelan sistem yang berbasis *structural programming* yang menggunakan program Ms. Visio 2016 dan dilanjutkan dengan tahap desain *interface* menggunakan program CorelDraw.

c. Code

Pada tahap ini akan dilakukan proses mewujudkan atau menerjemahkan desain yang telah dibuat sebelumnya ke dalam program perangkat lunak melalui proses *coding.* Proses *coding* ini dilakukan program per program. Proses *coding* ini akan dilakukan melalui *software* MATLAB.

d. Testing

Pada tahap ini akan dilakukan proses untuk menyatukan unit-unit program yang telah dibuat sebelumnya kedalam sistem yang utuh. Pada tahap ini juga akan dilakukan pengujian secara keseluruhan pada sistem. Pengujian dilakukan untuk mengetahui kesesuaian hasil ouput dari sistem dengan kebutuhan yang telah dirancang sebelumnya pada tahap *analisys.*

1.7 Sistematika Laporan

BAB I Pendahuluan

Menjelaskan tentang latar belakang, perumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan laporan tugas akhir.

BAB II Landasan Teori

Menjelaskan tentang beberapa penelitian terdahulu, prinsip dasar dan konsep dari teori-teori yang akan menjadi referensi yang dipergunakan dalam penyelesaian laporan Tugas Akhir ini.

BAB III Analisa dan Perancangan Sistem

Menjelaskan tentang tahap analisa dan perancangan dari aplikasi Algoritma *Paillier cryptosystem* yang akan dibuat.

BAB IV Implementasi dan Pengujian Sistem

Bab ini membahas mengenai penggunaan algoritma *Paillier cryptosystem* dalam melakukan enkripsi dan dekripsi terhadap *file* citra, selain itu juga membahas pengujian keamanan terhadap *file* citra yang telah dienkripsi.

BAB V Kesimpulan dan Saran

Bab ini berisikan kesimpulan akhir mengenai hasil perancangan dan analisa yang diperoleh serta saran dan harapan untuk pengembangan lebih lanjut.