BAB III
METODE PENELITIAN

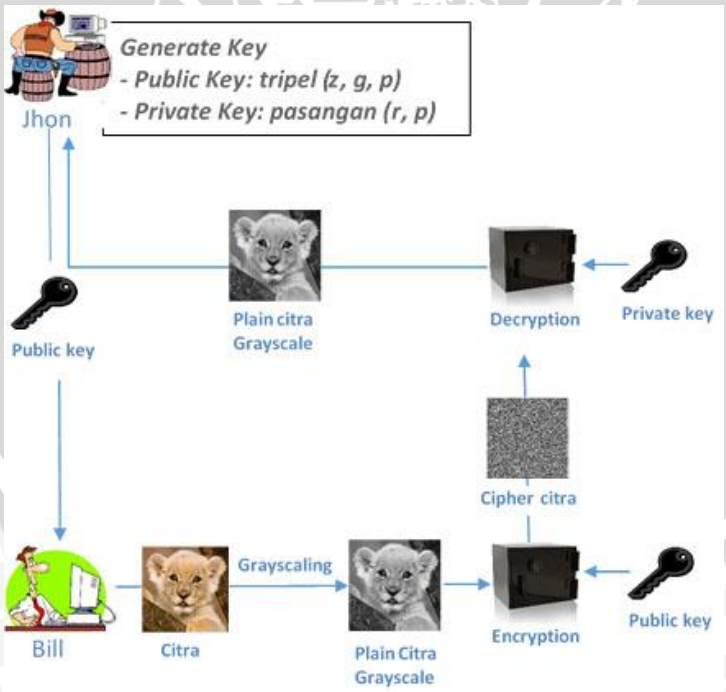
Dalam penyusunan skripsi ini, dirancang suatu aplikasi sistem enkripsi *file* citra 2 dimensi menggunakan algoritma kriptografi ElGamal. Metode penelitian yang digunakan pada penyusunan skripsi ini adalah :

3.1 Studi Literatur

Studi literatur menjelaskan dasar teori yang digunakan untuk menunjang penulisan skripsi. Teori-teori pendukung tersebut meliputi:

1. Membaca dan mempelajari buku – buku yang berhubungan dengan Algoritma ElGamal dan *image processing.*
2. Mempelajari teknik – teknik dasar pemrograman dengan menggunakan *Microsoft Visual C#.*

3.2 Blok Diagram Sistem



Gambar 3.1 Blok Diagram

Keterangan :

Bill akan mengirim citra kepada Jhon. Jhon membuat 2 buah kunci yaitu kunci publik dan kunci privat dan akan memberikan kunci publiknya kepada Bill. Kemudian Bill mengubah citra berwarna menjadi citra abu-abu *(grayscale)*. Setelah itu Bill mengenkripsi menggunakan kunci publik algoritma ElGamal menjadi *cipher*citra dan mengirim kepada Jhon.

Jhon menerima *cipher*citra dan akan mendekripsi menggunakan kunci privat algoritma ElGamal sehingga Jhon mendapatkan *plain* citra *grayscale* dari Bill.

3.3 Perancangan dan Implementasi Sistem

3.3.1 Algoritma *generate key*

Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima *p* dan dua buah bilangan acak (random) *g* dan *r*dengan syarat $g<p$ dan $1 \leq r \leq p-2$ yang memenuhi persamaan.

$$z = g^r \bmod p$$

Dari persamaan tersebut nilai z, g dan p merupakan pasangan kunci public sedangkan r, p merupakan pasangan kunci pribadi.

Properti algoritma ElGamal sebagai berikut:

1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, g (g < p, *grayscale*) (tidak rahasia)
3. Bilangan acak, r (r < p, kunci privat) (rahasia)
4. z = g^r mod p (kunci publik,RRGGBB) (tidak rahasia)
5. m atau f(x,y) (*plain*citra, *grayscale*) (rahasia)
6. a dan b (a dan b adalah *cipher* citra,RRGGBB) (tidak rahasia)

Misalkan m adalah *plain* citra *grayscale f(x,y)*=$\begin{bmatrix} \mathbf{65} & \mathbf{30} \\ \mathbf{100} & \mathbf{165} \end{bmatrix}$, p = 317, g = $\begin{bmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{4} \end{bmatrix}$, r = 7. Kemudian p, g, dan r digunakan untuk menghitung z :

z = g^r mod p

z = $\begin{bmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{4} \end{bmatrix}^7$ mod 317

$\mathbf{z} = \begin{bmatrix} \mathbf{1} & \mathbf{128} \\ \mathbf{285} & \mathbf{217} \end{bmatrix}$

Maka di dapat :

- Kunci publik: tripel ($\begin{bmatrix} \mathbf{1} & \mathbf{128} \\ \mathbf{285} & \mathbf{217} \end{bmatrix}$, $\begin{bmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{4} \end{bmatrix}$,317)
- Kunci privat: pasangan (7, 317)

3.3.2 Algoritma Proses Enkripsi

Pada proses enkripsi dilakukan dengan menyusun nilai-nilai intensitas sesuai blok-blok pada pixel citra. Nilai-nilai ini yang disebut nilai m (*plain*citra). nilai m harus masih berada didalam range 0 sampai p – 1. Kemudian memilih bilangan acak *k*, yang dalam hal ini $1 \leq k \leq p - 2$. Setiap blok dienkripsi dengan rumus.

$$\mathbf{a = g^k \bmod p}$$

$$\mathbf{b = z^k m \bmod p}$$

Misalkan m adalah *plain* citra *grayscale* $f(x,y)=\begin{bmatrix} \mathbf{65} & \mathbf{30} \\ \mathbf{100} & \mathbf{165} \end{bmatrix}$. Kemudian pilih bilangan acak k = 10 dengan ketentuan $1 \leq k \leq p - 2$. Hitung a dan b.

$a = g^k \bmod p$

$a = \begin{bmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{4} \end{bmatrix}^{10} \bmod 317$

$\mathbf{a} = \begin{bmatrix} \mathbf{1} & \mathbf{73} \\ \mathbf{87} & \mathbf{257} \end{bmatrix}$

$b = z^k m \bmod p$

$b = \begin{bmatrix} \mathbf{1} & \mathbf{128} \\ \mathbf{285} & \mathbf{217} \end{bmatrix}^{10} \begin{bmatrix} 65 & 30 \\ 100 & 165 \end{bmatrix} \bmod 317$

$\mathbf{b} = \begin{bmatrix} \mathbf{65} & \mathbf{80} \\ \mathbf{66} & \mathbf{11} \end{bmatrix}$

maka nilai pixel yang dihasilkan *cipher* citra adalah $\begin{bmatrix} \mathbf{1} & \mathbf{73} \\ \mathbf{87} & \mathbf{257} \end{bmatrix}$ **dan** $\begin{bmatrix} \mathbf{65} & \mathbf{80} \\ \mathbf{66} & \mathbf{11} \end{bmatrix}$

3.3.3 Algoritma Proses Dekripsi

Pada porses dekripsi digunakan kunci pribadi r dan p untuk mendekripsi a dan b menjadi *plain* citra m dengan persamaan.

$$(a^r)^{-1} = a^{p-1-r} \bmod p$$

$$m = b/a^r \bmod p = b(a^r)^{-1} \bmod p$$

Seperti pada proses enkripsi *cipher*citra didapatkan $\begin{bmatrix} \mathbf{1} & \mathbf{73} \\ \mathbf{87} & \mathbf{257} \end{bmatrix}$ **dan** $\begin{bmatrix} \mathbf{65} & \mathbf{80} \\ \mathbf{66} & \mathbf{11} \end{bmatrix}$ maka untuk mendekripsikannya adalah dengan menggunakan pasangan a dan b.

$m = b\,(a^r)^{-1} \bmod 17$

$(a^r)^{-1} = a^{p-1-r} \bmod p$

$= \begin{bmatrix} \mathbf{1} & \mathbf{73} \\ \mathbf{87} & \mathbf{257} \end{bmatrix}^{317-1-7} \bmod 317$

$= \begin{bmatrix} \mathbf{1} & \mathbf{73} \\ \mathbf{87} & \mathbf{257} \end{bmatrix}^{309} \bmod 317$

$= \begin{bmatrix} \mathbf{1} & \mathbf{40} \\ \mathbf{136} & \mathbf{15} \end{bmatrix}$

$m = \begin{bmatrix} \mathbf{65} & \mathbf{80} \\ \mathbf{66} & \mathbf{11} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{40} \\ \mathbf{136} & \mathbf{15} \end{bmatrix} \bmod 317$

$\mathbf{m} = \begin{bmatrix} \mathbf{65} & \mathbf{30} \\ \mathbf{100} & \mathbf{165} \end{bmatrix}$

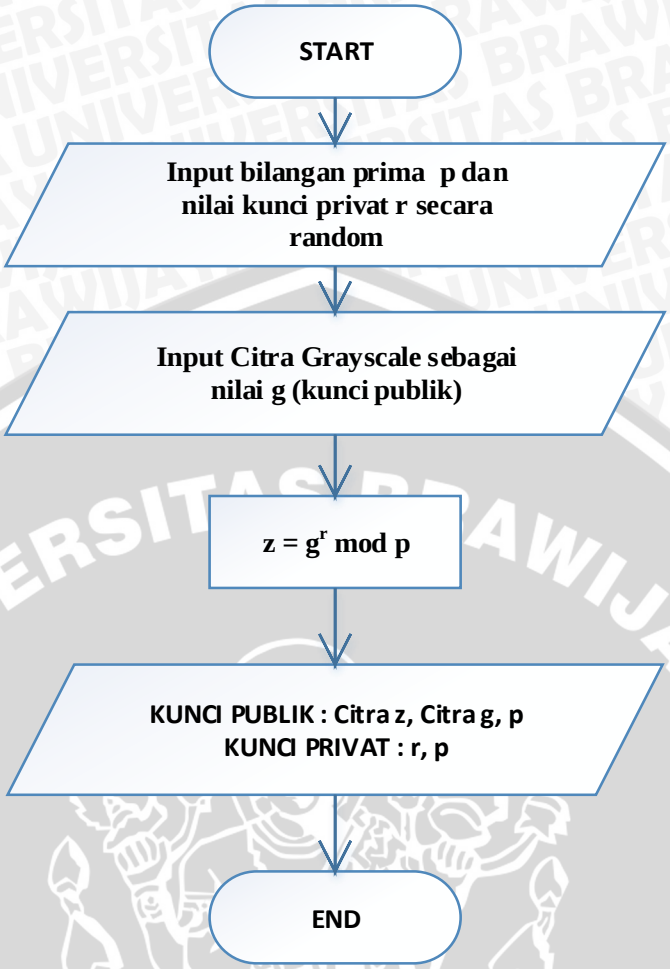
Sehingga *plain* citra dapat ditemukan kembali.

3.3.4 Diagram Alir

Untuk membantu memahami abstraksi sistem, Berikut ini merupakan diagram alir dari proses *generate key*, enkripsi dan dekripsi citra dengan algoritma ElGamal.

A. Proses *Generate Key*

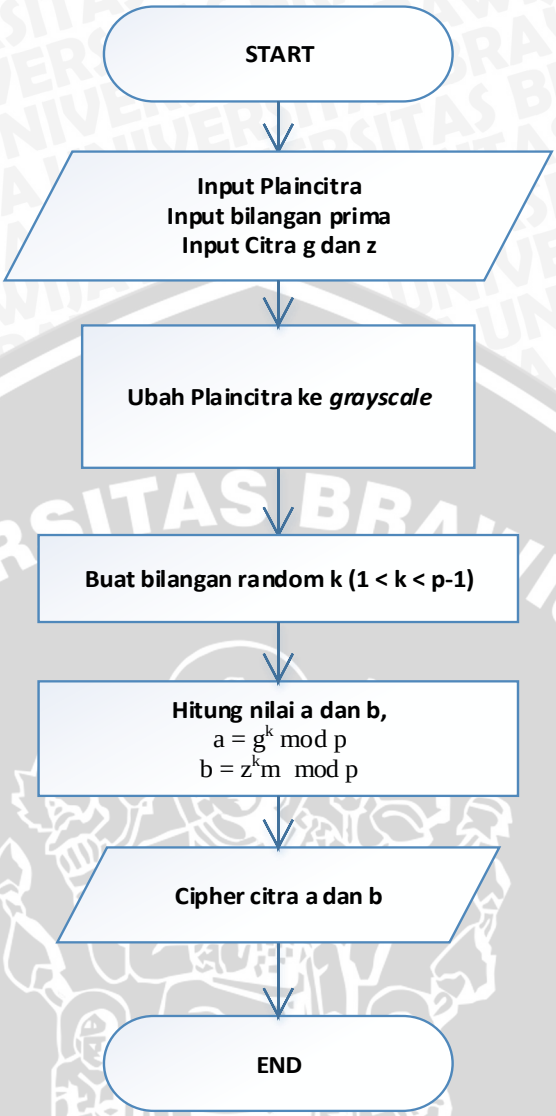
Proses *Generate Key* adalah proses untuk membangkitkan kunci yang digunakan untuk proses enkripsi maupun dekripsi. Rancangan proses *generate key* dapat dilihat pada Gambar 3.2.



Gambar 3.2 *Flowchart* Proses *Generate Key*

B. Proses Enkripsi

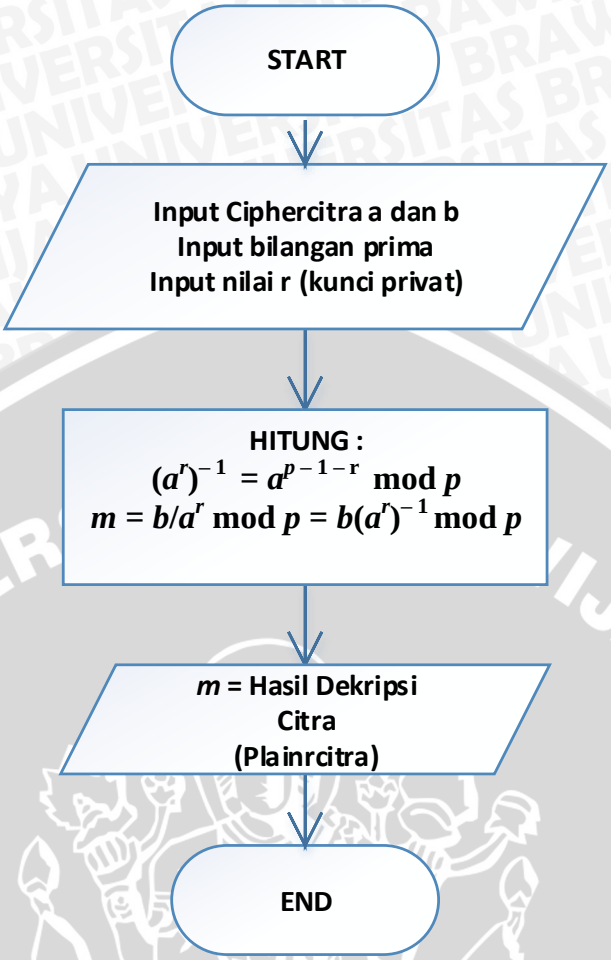
Proses enkripsi merupakan proses untuk mengubah data sumber menjadi *fileciphertext* dengan menggunakan nilai-nilai kunci publik yang dihasilkan dari proses *generate key*. Rancangan proses enkripsi dapat dilihat pada Gambar 3.3.



Gambar 3.3 *Flowchart* Proses Enkripsi

C. Proses Dekripsi

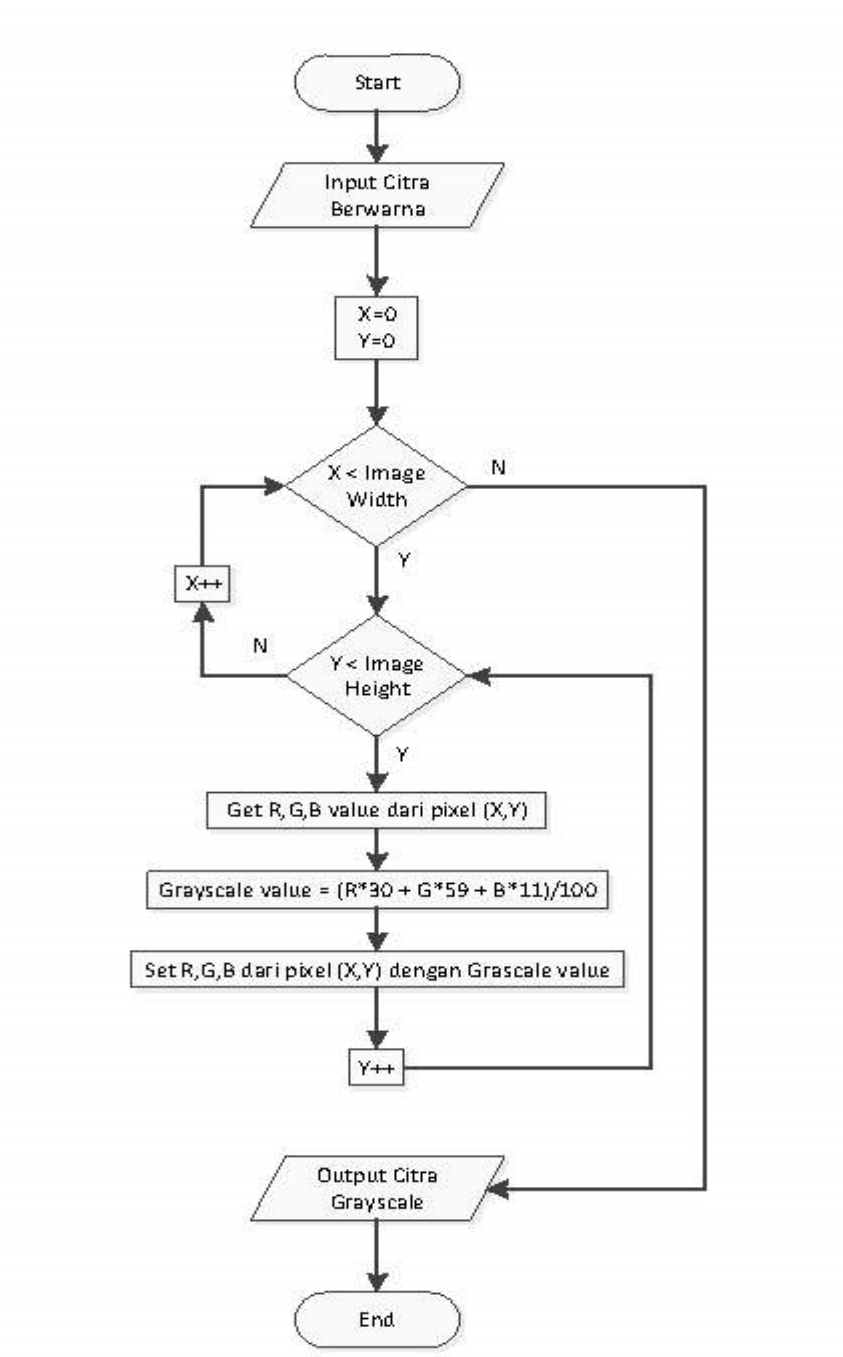
Proses dekripsi adalah proses untuk mengembalikan *ciphertext* kedalam bentuk *plaintext*, dengan menggunakan kunci privat (r,p). Rancangan proses dekripsi dapat dilihat pada Gambar 3.4.



Gambar 3.4 *Flowchart* Proses Dekripsi

3.3.5 *Grayscale*

Fungsi *grayscale* yang digunakan berpegang pada konsep RGB, dimana porsi *grayscale value* dari suatu *pixel* adalah *value* dari R * 0.30 + G * 0.59 + B * 0.11. Pada *grayscale image*, nilai *R,G*, dan *B* bernilai sama. Proses *grayscale* seperti ditunjukkan pada gambar 3.5.



Gambar 3.5 *Flowchart Grayscale*

3.4 Pengujian Sistem

Pengujian dilakukan untuk menjamin dan memastikan bahwa aplikasi yang telah dirancang memiliki tingkat kesalahan yang kecil. Untuk mengetahui apakah aplikasi bekerja dengan baik dan sesuai dengan perancangan, maka diperlukan serangkaian pengujian. Pengujian aplikasi sistem enkripsi *file* citra 2 dimensi menggunakan algoritma kriptografi ElGamal dilakukan terhadap beberapa sample

citra yang berasal dari *file*.

Hasil pengujian dari proses enkripsi citra nantinya akan dibandingkan dengan citra awal yang belum diproses. Parameter yang menjadi tolak ukur antara lain : keacakan citra (dengan menggunakan analisis korelasi), waktu yang dibutuhkan untuk memproses suatu citra (dengan melakukan pengujian terhadap citra yang memiliki resolusi dan besar kapasitas *file* nya), serta hasil *cipher* citra dari proses enkripsi.

3.5 Lingkungan Implementasi

Untuk mengimplementasikan aplikasi sistem enkripsi *file* citra 2 dimensi menggunakan algoritma kriptografi ElGamal, dibutuhkan suatu perangkat pendukung antara lain:

a. Perangkat Keras :
    1. PC atau Laptop.
b. Perangkat Lunak :
    1. *Operating System Windows* 7.
    2. *Software Microsoft Visual C#* 2010.

3.6 Kesimpulan dan Saran

Pada tahap ini, diambil dari hasil pengujian dan analisa terhadap Aplikasi Sistem Enkripsi *File* Citra 2 Dimensi Menggunakan Algoritma Kriptografi ElGamal. Tahap Selanjutnya adalah membuat saran untuk perbaikan terhadap penelitian selanjutnya sehinga dapat menyempurnakan kekurangan-kekurangan yang ada.