BAB III

METODE PENELITIAN

3.1 Perancangan Sistem

Sistem enkripsi karakter ke sebuah file gambar adalah sebuah sistem yang mampu untuk mengkodekan sebuah karakter ke dalam pixel – pixel untuk menjadikan sebuah file gambar. Sedangkan sistem dekripsi gambar ke beberapa karakter adalah sebuah sistem yang mampu decode beberapa pixel dalam satu gambar menjadi beberapa karakter.

Oleh karena itu, penulis mencoba untuk membuat sebuah alat bantu atau aplikasi yang berjalan di Sistem Operasi Microsoft windows, dimana alat bantu tersebut dapat merubah beberapa karakter sampai dengan ribuan karakter. Yang dimaksud merupakan karakter inputan yang berasal dari keyboarb (papan ketik), hasil dari inputan keyboard akan diubah menjadi sebuah file gambar yang terenkripsi dalam angka 0 (nol) sampai dengan 9 (sembilan). Jika karakter menempati posisi ganjil maka nilai bytenya akan ditambahkan 69 dan jika menempati posisi genap maka nilai bytenya akan ditambahkan 71. nilai 69 dan 71 didapatkan karena merupakan ambang batas bawah dan atas antara nilai 100 sampai dengan 199. Karena nilai hasil akan diambil dua karakter dari belakang. Sebagai contoh : huruf “A” (nilai byte sama dengan 65). Yang terdapat dalam sebuah kalimat atau kata menempati posisi ganjil, maka 65+69 = 134 dan jika menempati posisi genap maka 65+71 = 136. dari hasil tersebut diambil dua angka yang terakhir. Jika ganjil maka hasil enkripsi huruf “A” = 34, jika genap maka

hasil enkripsi huruf “A” = 36. Jadi setiap karakter akan diwakili / di-enkripsi 2 (dua) karakter angka. Hasil tersebut disimpan dalam bentuk Circulant Matrik (M x M) / matrik bujur sangkar. Dalam hal ini jika terdapat 32 karakter hasil enkripsi maka disimpan dalam matrik ordo 6 x 6, dan jika terdapat 37 karakter hasil enkripsi maka disimpan dalam ordo matrik 7 x 7, karena 37 karakter tidak memungkinkan untuk disimpan dalam ordo matrik 6 x 6. Ordo matrik 6 x 6 hanya mampu menampung 36 karakter. Begitu juga untuk kasus jumlah karakter 26, tidak memungkinkan disimpan dalam bentuk ordo matrik 5 x 5. Dari enkripsi angka 0 sampai dengan 9, pengertiannya adalah bahwa angka 0 diwakili oleh sebuah warna pixel, angka 1 diwakili oleh sebuah warna pixel yang lain dan seterusnya sampai angka 9.

Begitu juga untuk enkripsi ke file text. Alur atau proses sama dengan proses ekripsi ke file gambar, tetapi tidak menjadikan hasil enkripsi ke sebuah pixel – pixel. Sehingga hasil enkripsi murni tersimpan dalam bentuk angka 0 sampai dengan 9 dalam sebuah file text.

3.2 Perancangan Proses

Proses yang menjadi skenario / arus proses pengaplikasian sistem ini dijelaskan sebagai berikut :

1. Inisialisasi sistem.

Sistem aplikasi pada saat awal dijalankan akan melakukan inisialisasi antara lain :

a. Inisialisasi koneksi dengan Microsoft Access, dilakukan dengan melakukan setting tipe koneksi “*Connection String*” yang

menggunakan ADO Connection. Dimana ADO Conection merupakan komponen dari Delphi. Dimana dalam membangun sistem tersebut menggunakan Delphi 5. String yang dihasilkan untuk tipe koneksi ini adalah :

"Provider" = Microsoft.Jet.OLEDB.4.0, *"DataSource"* = tabel.mdb, Persist Security Info=False.

b. Inisialisasi atau starting Microsoft Access sebagai awal siap dipakainya untuk melakukan manipulasi data. Baik itu perintah *select,delete,insert,update* serta perintah SQL lainnya. Terutama untuk Login sistem.

2. Login sistem.

Setiap user yang bergabung atau terdaftar bisa menggunakan sistem tersebut. Dengan syarat tidak semua user dapat melakukan deskripsi maupun enkripsi suatu obyek atau data. Tergantung siapa yang diberikan hak akses dari obyek tersebut. Dan user siapa yang memiliki hak atau *granted previleges* terhadap obyek atau data tersebut atas kehendak dari operator aktif aplikasi tersebut. Jadi yang berhak untuk melakukan dekripsi baik itu dari gambar atau dari karakter,tergantung pemberian hak akses oleh operator aktif. Jika operator lain tidak diberikan hak akses, maka operator tersebut tidak akan pernah bisa melihat isi dari gambar atau file text tersebut. Secara garis besar pengguna dalam sistem ini terbagi dua kelompok berdasarkan hak akses, yaitu :

A. Operator Aktif.

Operator Aktif adalah operator yang mengunakan aplikasi saat itu juga. Jadi operator aktif yang melakukan login aplikasi. Operator aktif mempunyai wewenang besar dalam menentukan siap yang berhak untuk membuka hasil enkripsinya. Seorang operator administrator pun tidak berhak untuk membuka hasil enkripsinya, kecuali diberikan hak akses kepada operator administrator. Jadi operator administrator belum tentu dapat membuka semua hasil enkripsi dari semua operator(pemakai). Jadi keamanan data hasil enkripsi dari seorang operator terjamin keamanannya.

B. Operator Tidak Aktif.

Operator tidak aktif adalah operator yang tidak melakukan login saat itu juga atau operator yang tidak mengunakan aplikasi tersebut. Operator tidak aktif tersebut merupakan *list*(daftar) bagi operator aktif untuk diberikan hak akses. Operator tidak aktif dibagi dua, yaitu :

1. Memiliki Hak Akses.

Operator tidak aktif yang memiliki hak akses adalah operator yang diberikan hak akses / *granted* oleh operator aktif. Jadi statusnya memiliki hak atas yang dienkripsi oleh operator aktif.

2. Tidak Memiliki Hak Akses.

Operator tidak aktif yang tidak memiliki hak akses adalah operator yang tidak diberikan hak akses sedikitpun oleh operator aktif. Jadi statusnya tidak memiliki hak atas yang dienkripsi oleh operator aktif. Operator tersebut disebut juga sebagai operator pasif.

3. Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses mengkodekan sebuah pesan menjadi sesuatu yang tidak mempunyai arti. Sebuah enkripsi terhadap sebuah pesan atau data dilakukan untuk mencegah dari pembacaan data oleh orang yang tidak berhak membacanya. Sedangkan dekripsi mengadung arti sebagai kebalikan dari proses enkripsi yaitu proses transformasi dari sebuah pesan yang terenkripsi dan dikembalikan ke bentuk normal dengan menggunakan algoritma terbalik.

4. Dokumentasi.

Dokumentasi yang dimaksud disini adalah tampilan dari sebuah record set yang merupakan proses seleksi record atas data yang telah di enkripsi oleh seorang yang sedang aktif menggunakan sistem ini. Dokumentasi juga memiliki utility selain menampilkan record juga dapat menampilkan data record seperti proses enkripsi yang telah dilakukan terhadap record tersebut. Informasi yang didapat dari dokumentasi antara lain :

a. EcryptID, menampilkan identitas sebuah record yang merupakan autoincrement (penambahan otomatis) terhadap record enkripsi dan merupakan primary key (kunci utama) yang membedakan antar record.
b. Username menampilkan nama user yang melakukan proses enkripsi terhadap sebuah data atau obyek.
c. TglEncrypt, menginformasikan tanggal dari proses enkripsi sebuah obyek atau data dilakukan.

5. Administering User.

Aplikasi kewenangan bagi administrator aplikasi untuk melakukan pendaftaran bagi seorang user baru. Memilihkan menu – menu dari hak

akses yang dapat dilakukan. User yang dapat menjadi pengguna sistem aplikasi ini tentunya adalah user – user yang tergantung atau yang menjadi anggota dalam suatu domain.

6. Kompresi File.

Menjadi salah satu kelebihan dari sistem aplikasi ini, untuk sebuah file yang telah terenkripsi selain melakukan proses pengubahan data proses enkripsi juga melakukan proses pemadatan ukuran file. Hal ini didasarkan pada pemikiran yang berdasarkan pada dua segi yaitu efektifitas dan securitas.

Efektifitas, proses enkripsi akan menghasilkan sebuah file yang sama untuk ukuran filenya sehingga perlu memperkecil ukuran filenya. Hal ini dmaksudkan apapun yang dilakukan untuk proses enkripsi

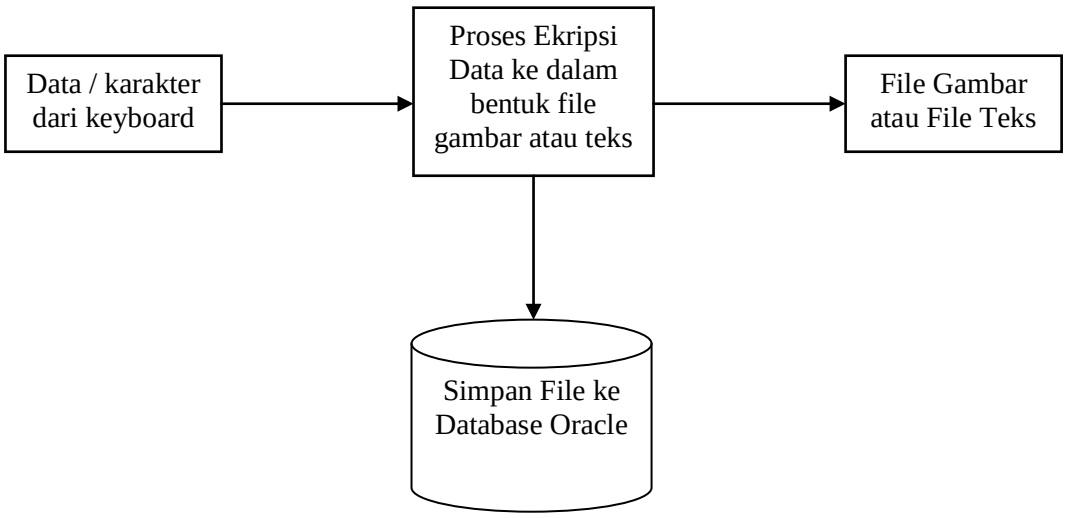
7. Backup Data.

Sistem aplikasi ini dilengkapi dengan kemampuan untuk backup data. Dimana data yang tersimpan mampu untuk di duplikasi atau disimpan ke dalam sekunder disk yang lain. Jadi jika data dalam primary disk rusak atau tidak terbaca, maka data masih dapat diselamatkan atau masih ada dalam sekunder disk. Sekunder disk dapat berupa : hard disk, disket, Compact Disk, Memory Card dan lain sebagainya.

3.3 Algoritma atau Prosedur Penelitian

Langkah – langkah / algoritma dalam melakukan penelitian pada sistem tersebut sebagai berikut :

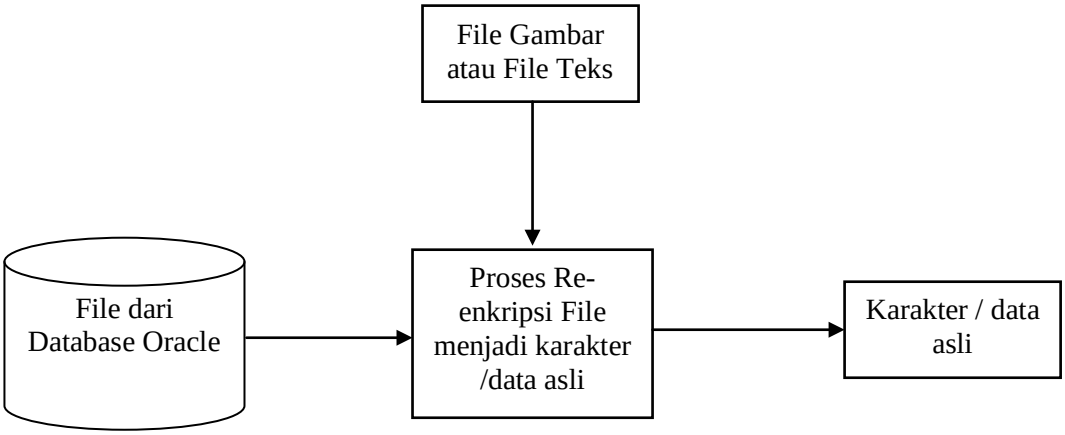
3.3.1 Proses Enkripsi data / karakter menjadi file gambar atau file teks



Gambar 3.1. Proses ekripsi data / karakter menjadi file gambar atau file teks

Enkripsi data / karakter menjadi file gambar atau file teks terdiri dari 3 tahap secara umum yaitu : Input, proses dan output. Inputan berupa karakter yan diketikan dari papan ketik / keyboard. Semua karakter yang ada pada papan ketik dapat dienkripsi. Termasuk papan ketik yang mendukung operating sistem windows. Proses merupakan proses enkripsi karakter ke bilangan antara 0 sampai dengan 9, kemudian menjadi beberapa pixel – pixel yang membentuk sebuah gambar atau tetap dijadikan sebuah karakter yang ter-enkripsi. Kemudian output berupa file gambar / file teks. Bisa juga file gambar / file teks tersebut disimpan dalam database oracle.

3.3.2 Proses Dekripsi file gambar atau file teks menjadi data / karakter



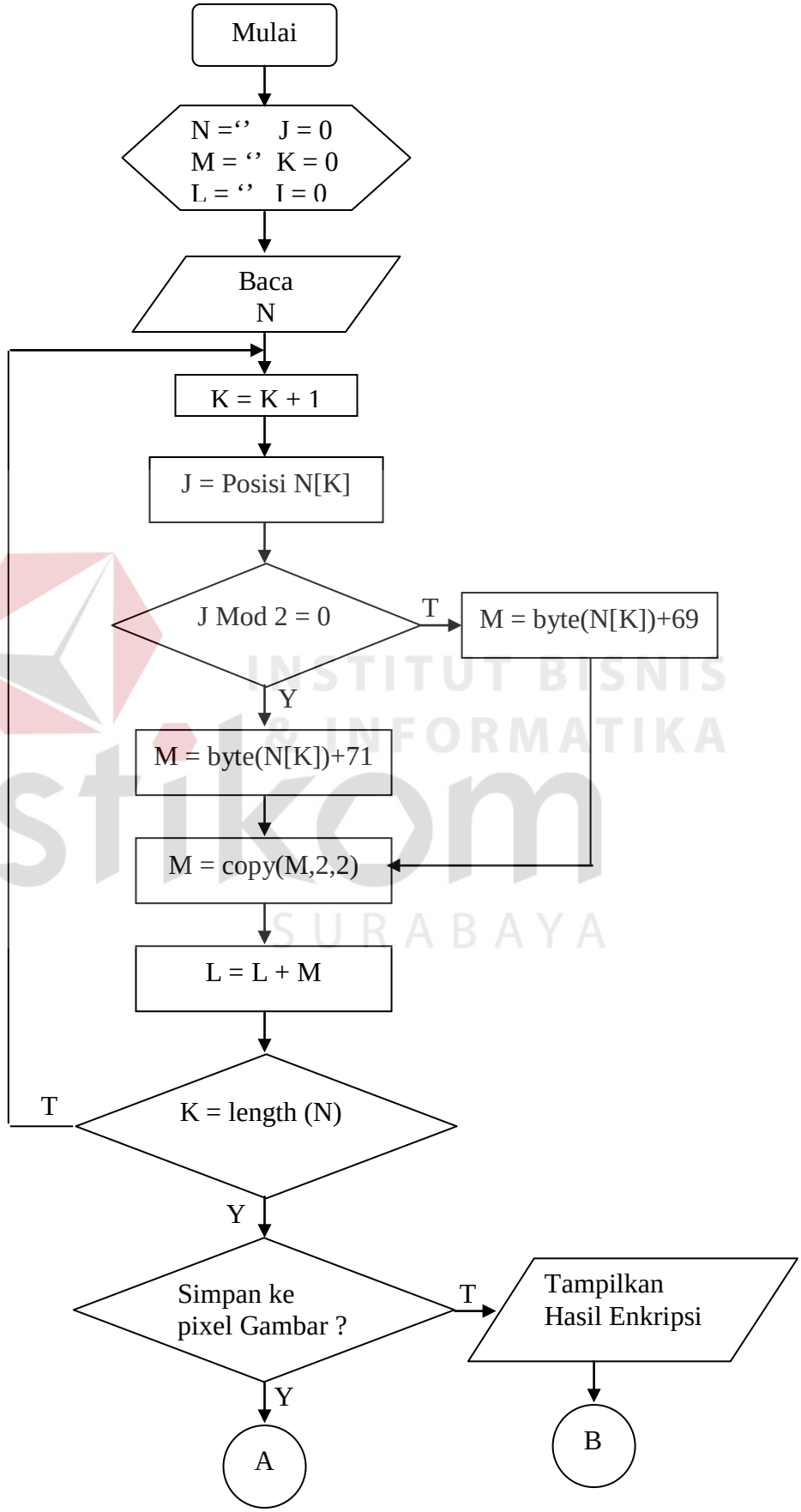
Gambar 3.2. Proses dekripsi file gambar atau file teks menjadi data asli

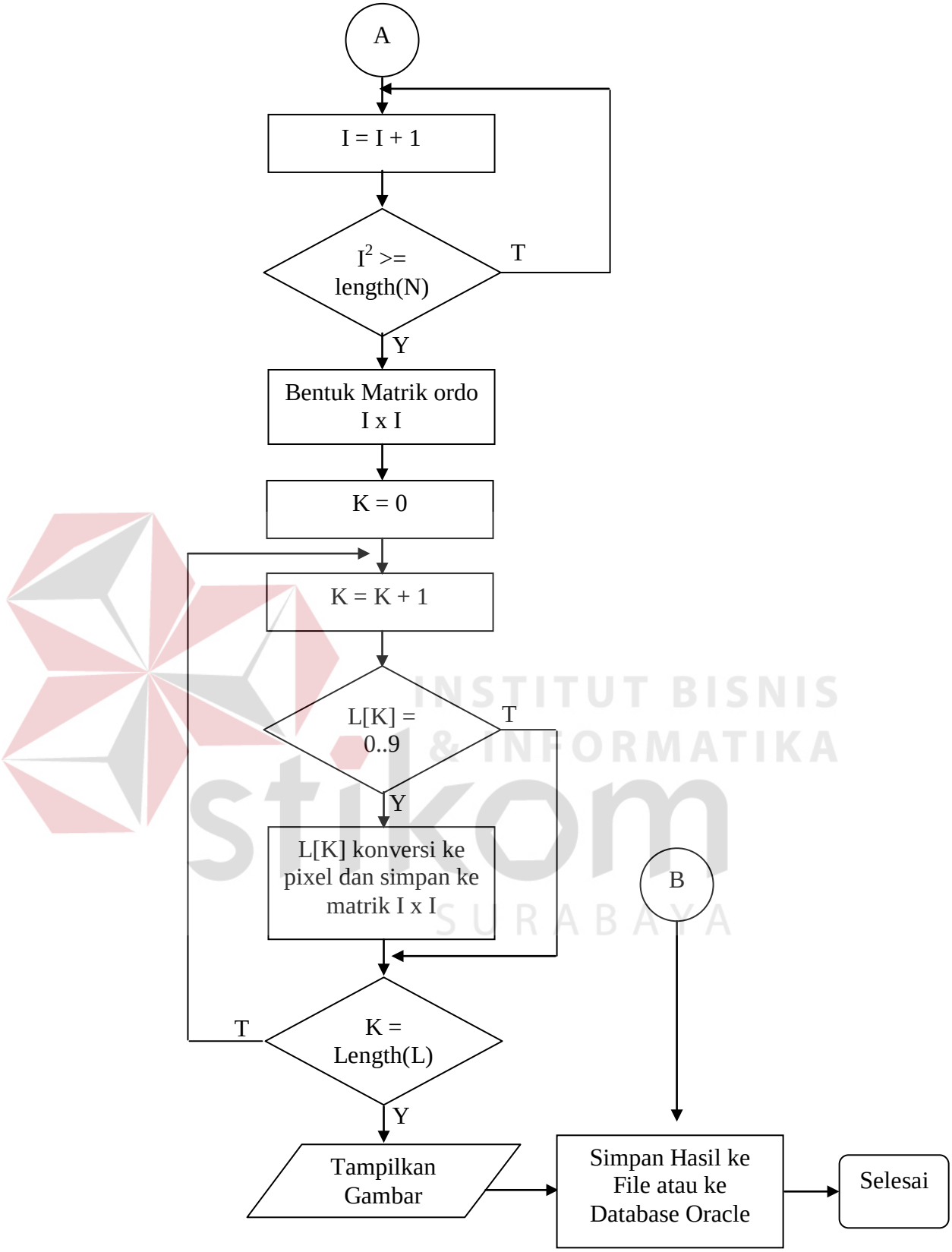
Dekripsi file gambar atau file teks menjadi data asli, juga terdiri dari 3 tahapan. Yaitu input, proses dan output. Input bisa berupa file gambar atau file teks, atau juga dari file yang tersimpan dalam database oracle. Proses merupakan proses untuk re-enkripsi atau dekripsi, dimana akan dikembalikan ke nilai yang sesunguhnya. Output berupa karakter atau data dokumen aslinya.

3.3.3 Desain system

Membuat rancangan yang diperlukan dalam pembuatan system yang baru. Dimana system tersebut harus mudah dipahami dan digunakan oleh semua penguna komputer.

3.3.4 Algoritma / flowchart enkripsi karakter ke gambar atau teks



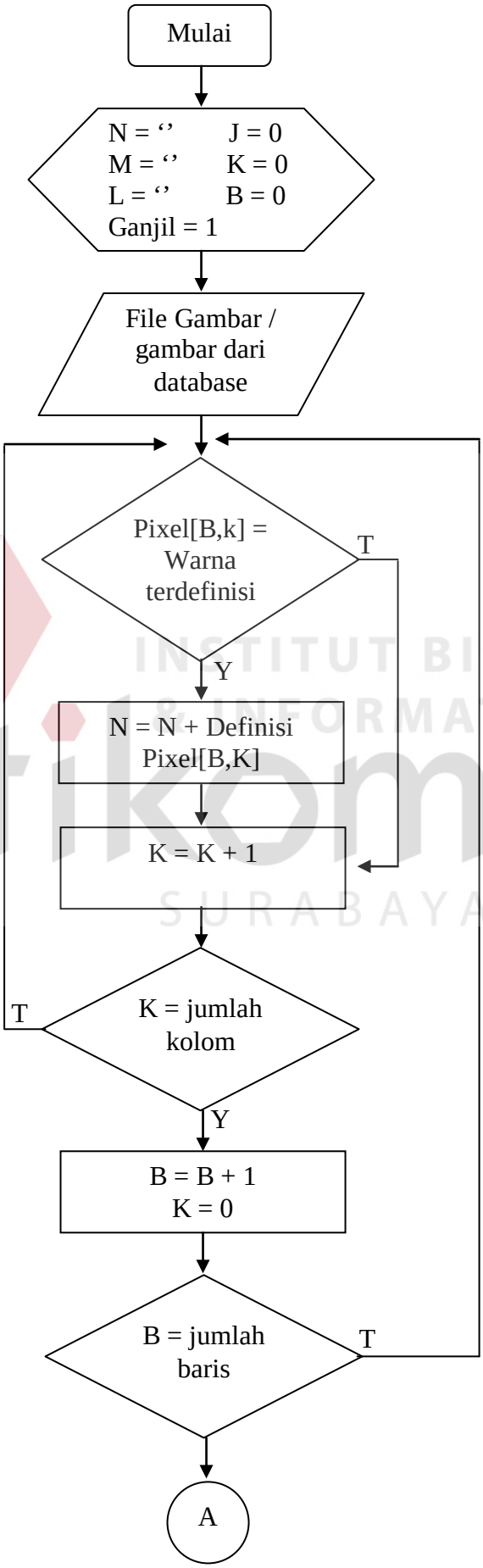


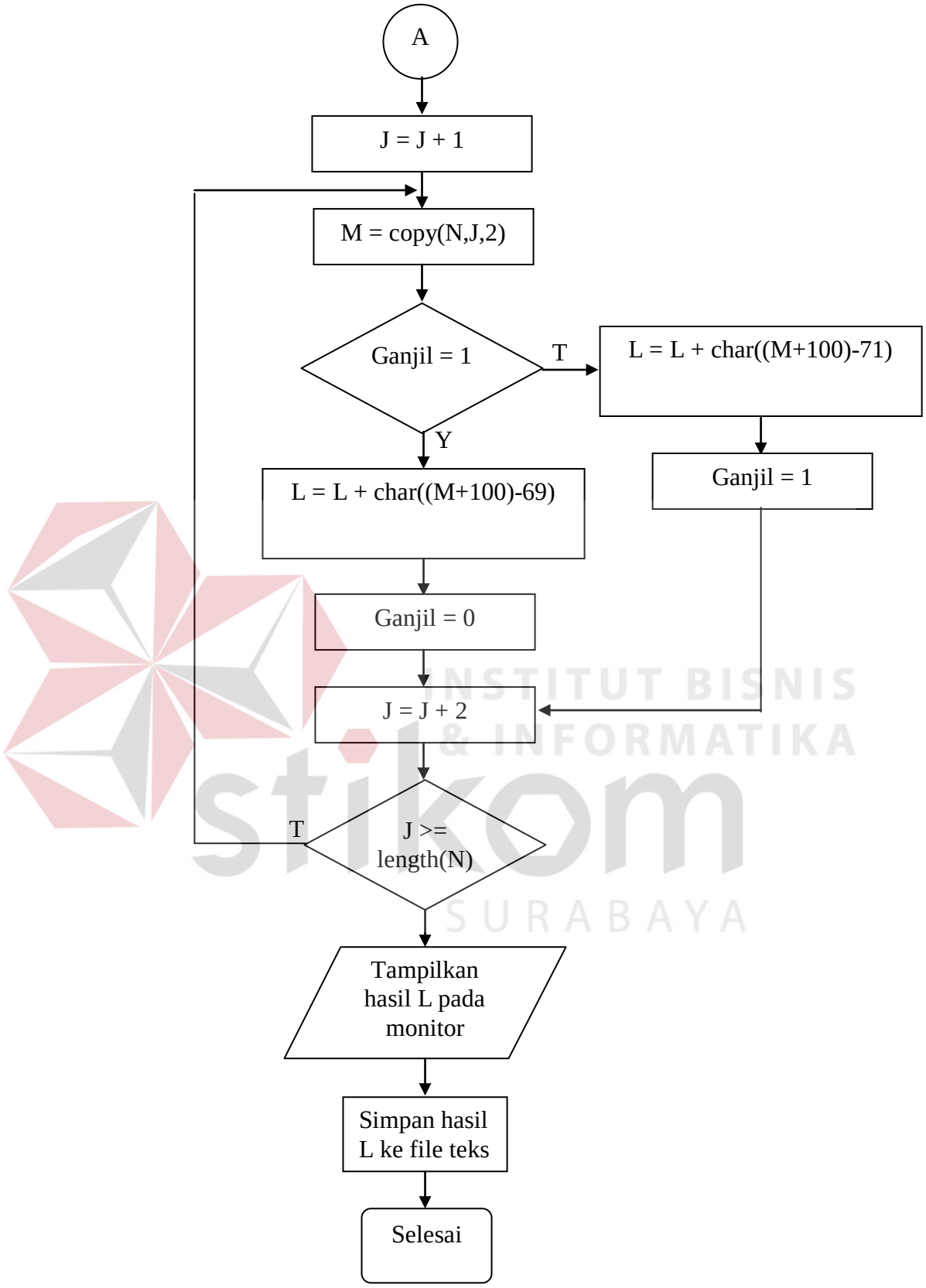
Gambar 3.3. Algoritma / flowchart enkripsi karakter ke gambar atau teks

Inputan dari algoritma diatas berupa karaker yang diketikan dari papan ketik (keyboard). Dan inisialisasi variabel pertama yaitu : N, M, J dan K. Hasil inputan dari papan ketik disimpan pada variabel N.

Selanjutnya isi dari variabel N, diproses satu persatu. Dengan melakukan looping (perputaran) berdasarkan dari panjang / banyaknya karakter pada variabel N. atau dalam algoritma diatas disebut length(N). Jika posisi karakter terletak pada posisi ganjil, maka hasil konversi ke byte pada karakter akan ditambahkan 69, selanjutnya akan diambil dua karakter terakhir saja. Sedangkan kalau posisi karakter terletak pada posisi genap, maka hasil konversi ke byte pada karakter akan ditambahkan 71 dan juga akan diambil dua karakter terakhir saja. Setiap hasilnya akan di simpan kedalam pixel – pixel gambar. Dimana hanya diwakili 10 warna saja, karena hasil konversi hanya terdiri angka 0 sampai dengan 9. Dimana setiap pixel akan disimpan pada ordo matrik bujur sangkar. Ordo matrik didapat berdasarkan jumlah karakter hasil enkripsi.

3.3.5 Algoritma / flowchart re-enkripsi dari gambar atau teks ke karakter





Gambar 3.4. Algoritma / flowchart re-enkripsi dari gambar atau teks ke karakter

Inputan dari algoritma tersebut berupa file gambar. Inisialiasi variabel pertama yaitu : N, M, L, J, K dan Flag.

Proses pertama yaitu looping / perputaran dimana berdasarkan jumlah pixels. Dalam proses tersebut selalu diadakan pengecekan, apakah pixels sesuai dengan angka hexadecimal yang didifinisikan. Jika ya berarti sesuai dengan nilai yang ada. Misal : jika warna red (merah) = hexadecimal red, maka nilai yang didefinisikan semisal 9. Proses tersebut berjalan sampai pixel terakhir. Hasil tersebut kemudian di-dekripsi.

Proses dekripsi sebagai berikut :

Proses looping, dimana berdasarkan panjang dari hasil tersebut. Didalam proses tersebut ada logika program, dimana angka diambil dua karakter dua karakter. Dua karakter pertama disebut posisi ganjil, sedangkan dua karakter berikutnya disebut posisi genap. Jika posisi genap maka angka tersebut akan ditambahkan 100 dikurangi 69, lalu dikonversi menjadi sebuah karakter. Proses berlanjut sampai semua di-dekripsi. Lalu hasilnya ditampilkan pada monitor.

3.4 Evaluasi Penelitian

Program yang sudah jadi dilakukan evaluasi dan uji coba kepada setiap pengguna komputer yang kebanyakan masih awam tentang komputer. Dengan menggunakan user yang masih awam tersebut kemungkinan error program akan muncul. Sehingga program yang dihasilkan akan benar – benar baik. Bila masih ada kesalahan yang terjadi, maka penulis memperbaiki kesalahan yang ada.

3.5 Tabel – Tabel Database

Ada beberapa tabel yang dipakai. Dimana tabel tersebut mengunakan dua database yaitu *Microsoft Access* dan *Oracle*. Pada *Microsoft Access* hanya sebuah tabel yaitu : tabel pemakai. Sedangkan pada *Oracle* ada dua tabel yaitu : tabel foto dan tabel teks. Berikut penjelasnya :

3.5.1 Tabel Pemakai

Tabel 3.1. Pemakai

NO	FIELD	DATA TYPE	LENGTH
1	Nama	Text	50
2	Sandi	Text	16
3	Nama_Login	Text	8
4	Nama_Entry	Text	50

Fungsi : Untuk menyimpan, menampilkan, mengubah serta menghapus nama – nama pemakai. Yang kemudian digunakan untuk menentukan hak akses. Tabel tersebut dibuat dengan *Microsoft Access*, karena tabel tersebut sangatlah perlu dan juga penulis memperhitungkan bahwa setiap komputer dominan memiliki *Microsoft Access*, jika dibanding memiliki *Oracle*.

3.5.2 Tabel Foto

Tabel 3.2. Foto

NO	FIELD	DATA TYPE	LENGTH
1	Nama	Varchar2	30
2	Photo	Long Raw	~
3	Tgl_Modifikasi	Date	Format Date
4	Jam_Modifikasi	Varchar2	8

Fungsi : Untuk menyimpan, menampilkan, mengubah serta menghapus file foto yang tersimpan dalam database. Jika tidak memiliki database *Oracle*, hal tersebut bersifat optional / tidak harus.

3.5.3 Tabel Teks

Tabel 3.3. Teks

NO	FIELD	DATA TYPE	LENGTH
1	Nama	Varchar2	30
2	Teks	Long Raw	~
3	Tgl_Modifikasi	Date	Format Date
4	Jam_Modifikasi	Varchar2	8

Fungsi : Untuk menyimpan, menampilkan, mengubah serta menghapus file teks yang tersimpan dalam database. Jika tidak memiliki database *Oracle*, hal tersebut bersifat optional / tidak harus.