JIMT
Vol. 9 No. 1 Juni 2012 (Hal. 89 – 100)

Jurnal Ilmiah Matematika dan Terapan

ISSN : 2450 – 766X

ENKRIPSI *AFFINE CIPHER* UNTUK STEGANOGRAFI PADA ANIMASI CITRA *GIF*

S. Hardiyanti[1], S. Musdalifah[2], A. Hendra[3]

[1,2]Prodi Matematika Jurusan Matematika FMIPA UNTAD
[3]Jurusan Tekhnik Informatika Fakultas Tekhnik UNTAD
Kampus Bumi Tadulako Tondo
Jl.Soekarno Hatta Km.9, Palu, 94118, Indonesia
[1]siti.hardiyanti90@gmail.com, [2]selvymusdalifah@yahoo.com, [3]a_for_andie@icloud.com

Abstrak

Perkembangan teknologi informasi saat ini membuat para pelaku kejahatan semakin mudah.oleh karena itu dibutuhkan proses penyandian agar pengiriman dan penyimpanan pesan aman dari para pelaku kejahatan komputer. Adapun metode yang digunakan untuk mengamankan pesan yakni *Kriptografi* dan *Steganografi*. *Kriptografi* diimplementasikan melalui *algoritma affine cipher*, menggunakan bentuk penyadian dan kunci pesan. Sedangkan *Steganografi* diimplementasikan melalui *gifshuffle* yang dimana proses sistem penyisipan dan pengekstrakan. Adapun proses *enkripsi affine cipher* untuk *Steganografi* pada animasi citra *gif* yakni atur kunci *enkripsi* dan *dekripsi*, input animasi *gif*, input pesan, dan menyisipkan kedalam animasi citra *gif*. Hasil dari penelitian menunjukkan bahwa *enkripsi affine cipher* untuk *Steganografi* pada animasi citra *gif* cukup aman, tidak mudah dilihat dan tidak mengubah media animasi citra *gif*.

Kata Kunci : Affine Cipher, Steganografi, Animasi GIF, Gifshuffle.

I. Pendahuluan

Perkembangan jaringan internet yang memungkinkan orang untuk saling bertukar data melalui jaringan internet tersebut. Seiring dengan perkembangan tersebut, kejahatan teknologi komunikasi dan informasi juga turut berkembang, seperti yang sering kita dengar adalah *hacker, cracker, carder, phreaker* dan sebagainya. Oleh karena itu diperlukan sebuah sistem atau aplikasi yang aman sehingga dapat mempersulit para pelaku kejahatan computer untuk melakukan aktivitasnya, dan membantu para pengguna teknologi dalam hal pengamanan data yang diakses tersebut.

Perkembangan steganografi ini menjadi salah satu alternative pengamanan dalam komunikasi data di jaringan internet. Berbeda dengan teknik kriptografi, kalau kriptografi, kecurigaan

terhadap pesan yang disamarkan mudah dikenali karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca. Sedangkan steganografi lebih mengurangi kecurigaan karena pesan yang disamarkan disembunyikan dalam file.

II. Tinjauan Pustaka

2.1. Kriptografi

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data/informasi tersebut.

Secara umum, Kriptografi terdiri dua proses utama, yaitu enkripsi dan dekripsi. Proses enkripsi akan mengubah pesan asli (*plainteks*) menjadi pesan terenkripsi dengan menggunakan algoritma dan kunci tertentu yang tidak dapat dibaca secara langsung (*cipherteks*).

2.1.1. Tujuan Kriptografi

Tujuan utama dari suatu sistem Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan 4 (empat) aspek keamanan dari suatu informasi yakni kerahasiaan, yaitu :

1. Kerahasiaan (*confidentiality*)
   Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.
2. Integritas data (*data integrity*)
   Integritas data bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut.
3. Otentikasi (*authentication*)
   Otentikasi merupakan identifikasi yang dilakukan oleh masing–masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya.
4. *Nir penyangkalan (Non-repudiation)*
   Non-repudiation berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang telah dilakukan oleh pelaku aksi itu sendiri.

2.2. *Affine Cipher*

Affine cipher adalah perluasan dari *Caesar cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Secara matematis *enkripsi plainteks* menghasilkan *cipherteks* dinyatakan dengan fungsi kongruen:

$C(P) \equiv mP + b \,(mod\ n)$ ..... (1)

Untuk memperoleh kembali plaintext maka kita harus memperoleh fungsi dekripsi terlebih dahulu.

$C(P) \equiv m^{-1}(C - b)(mod\ n)$ ..... (2)

dimana:

n : ukuran alfabet

P : plainteks yang dikonversi menjadi bilangan bulat dari 0 sampai *n* – 1 sesuai dengan urutan dalam alfabet

C : cipherteks yang dikonversi menjadi bilangan bulat dari 0 sampai *n* – 1 sesuai dengan urutan dalam alfabet

m : bilangan bulat yang harus relatif prima dengan *n* (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan)

b : jumlah pergeseran.

2.3. Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata steganografi berasal dari Bahasa Yunani yang berarti "tulisan tersembunyi" (*covered writing*).

Steganografi terdapat konsep pesan yang akan disampaikan kepada orang lain, tentunya ada beberapa pesan yang penting sehingga hanya orang yang berhak saja yang dapat menerimanya, sehingga dalam bidang Steganografi ini pesan tersebut akan disembunyikan, artinya ini berhubungan dengan keamanan pesan. Jadi, terdapat dua hal yang penting disini yaitu penyampaian pesan dan keamanannya.

2.3.1. Tujuan Steganografi

Tujuan dari Steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial.

2.3.2. Kriteria Steganografi

Penyembunyian pesan rahasia ke dalam media penampung pasti mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian pesan adalah (Sitompul, 2010) :

1. *Imperceptibility*.

   Keberadaan pesan dalam media penampung tidak dapat dideteksi.

2. *Fidelity*.

   Mutu media penampung setelah ditambahkan pesan rahasia tidak jauh berbeda dengan mutu media penampung sebelum ditambahkan pesan.

   n rahasia yang telah disisipkan dalam media penampung harus dapat diungkap kembali. Hal ini merupakan syarat mutlak dalam sebuah *algoritma Steganografi*, kerena ada banyak cara penyisipan pesan yang tidak terdeteksi namun sulit dalam pembacaan kembali.

2.4. Steganografi pada Media Digital File Gambar

Pada komputer, gambar yang tampil di layar monitor merupakan kumpulan array yang merepresentasikan intensitas cahaya yang bervariasi pada pixel. Pixel adalah titik di layar monitor yang dapat diatur untuk menampilkan warna tertentu. Melalui pixel inilah suatu gambar dapat dimanipulasi untuk menyimpan informasi yang akan digunakan sebagai salah satu pengimplementasian Steganografi.

Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia.

2.5. *Gifshuffle*

Gifshuffle yang dikembangkan oleh Matthew Kwan adalah salah satu algoritma Steganografi yang menggunakan berkas citra dengan format GIF. Akan dibahas bagaimana proses *encoding* dan *decoding* pesan dalam citra dengan menggunakan *gifshuffle*. Algoritma ini melakukan penyisipan pesan dengan cara mengganti susunan palet warna yang ada dalam sebuah berkas citra dengan format GIF. Dalam algoritma ini tidak terjadi perubahan apapun dalam data berkas dengan format GIF.

Sesuai dengan namanya *gifshuffle* akan melakukan *"Shuffle"* terhadap palet warna dari sebuah berkas gif. *"Shuffle"* jika diterjemahkan ke dalam bahasa Indonesia berari memutar. Sehingga dapat diartikan bahwa *gifshuffle* adalah algoritma yang memanfaatkan penukaran posisi ke 256 palet warna dalam berkas citra berformat GIF. Hal tersebut aman dilakukan karena dua buah berkas GIF dengan palet warna yang berbeda akan ditampilkan secara sama persis.

Algoritma *gifshuffle* memiliki dua macam aktifitas yang berbeda namun saling berkaitan, yaitu:

1. *Encoding*

Pada *encoding* terjadi proses penyisipan pesan teks ke media. Masukannya adalah pesan teks dan citra berformat GIF sebagai media menyembunyikan pesan teks tersebut. Keluarannya adalah citra berformat GIF yang telah disisipkan pesan atau biasa disebut *stego image*.

2. *Decoding*

Pada *decoding* terjadi proses pengekstrakan pesan teks dari gambar. Masukannya adalah citra berformat GIF tempat pesan disembunyikan (*stego image*) dan keluarannya adalah pesan teks. Atau dapat dikatakan bahwa *decoding* adalah proses pembalikan dari *encoding*.

2.6. GIF (*Graphics Interchange Format*)

Graphics Interchange Format (GIF) adalah sebuah format yang sering digunakan dalam dunia web maupun dalam dunia citra digital. Format gambar GIF memiliki dua versi, yaitu GIF87a dan GIF89a. GIF87a adalah versi pertama dari format GIF yang berupa gambar statis. *Compu Serve* kemudian memperkenalkan versi lanjutan, yaitu GIF89a. GIF89a dapat menampilkan gambar dinamis (animasi) dan latar belakang transparan.

Format ini terkompresi *lossless*, maksimum 256 warna. Format ini banyak digunakan sebagai grafik animasi dan mempunyai ukuran file yang kecil. Karena ukuran file yang cukup kecil maka GIF ini sering digunakan dalam pembuatan image dan animasi di internet sehingga waktu untuk mentransfer data dapat lebih cepat. GIF berukuran kecil karena membatasi jumlah warnanya sebanyak 256 warna sehingga tentunya ukuran file akan lebih kecil. Namun 256 palet warna tersebut tidak mutlak hanya 256 warna tertentu. Warna tersebut dapat dipilih dari 8-bit palet warna RGB atau dapat disimpulkan bahwa berkas dengan format GIF akan membuang palet warna yang tidak diperlukan dan mengambil hanya 256 palet warna yang diperlukan.

2.7. Animasi

Animasi merupakan serangkaian citra yang bergerak. Animasi mensimulasikan pergerakan dengan menampilkan serangkaian frame ke layar. Frame adalah sebuah gambar tunggal pada serangkaian gambar yang membentuk animasi.

III. Metode Penelitian

Berikut adalah penjelasan dari tahapan penelitian yang akan dilakukan penyusun dalam proses penelitian :

1. Melakukan studi literatur dengan mengumpulkan materi dari buku-buku, artikel dan jurnal yang didapat dari perpustakaan dan perpustakaan online.

2. Menerapkan proses enkripsi dan dekripsi *Affine Cipher*.
3. Menyisipkan pesan teks ke dalam animasi citra *gif* menggunakan *gifshuffle.*
4. Melakukan pengujian program terhadap data baru yang sudah didapat.
5. Membuat pembahasan tentang hasil yang diperoleh.
6. Menyimpulkan hasil penelitian.

IV. Hasil dan Pembahasan

4.1. Hasil

4.1.1. Input Citra

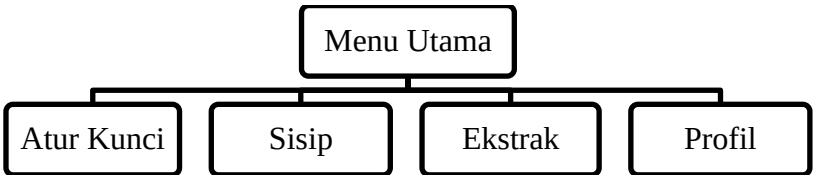
Pada pengujian penelitian ini menentukan cover atau media penyimpanan yang akan disisipkan pesan berupa media animasi citra *gif* pada gambar 1, proses penyisipan file akan dilakukan penyisipan pesan teks kedalam animasi citra *gif*. Kemudian proses penginputan yang dilakukan berupa citra digital dengan format *gif* adalah sebagai berikut :

```
//input animasi citra gif

FileNameExtensionFilter gif;
final JFileChooser ffile = new JFileChooser(new File("c:/"));
gif = new FileNameExtensionFilter("GIF", "gif");

ffile.addChoosableFileFilter(gif);
try{
int y = ffile.showOpenDialog(this);
if (y == JFileChooser.APPROVE_OPTION){
      File f =ffile.getSelectedFile();
      curdir = new File(f.getAbsolutePath());
      src.setText(f.getAbsolutePath());
}else{
     return;
}
```

Gambar 1 : Media penyimpanan animasi gif

4.1.2. Perancangan Struktur Menu

Struktur menu merupakan penggambaran fungsi-fungsi atau link yang ada pada sebuah program. Perancangan struktur menu berfungsi untuk mengetahui alur-alur rancangan program. Dalam pembuatan program aplikasi ini menggunakan alat bantu berupa struktur. Perancangan struktur menu adalah sebagai berikut :



Gambar 2 : Struktur Menu Aplikasi Steganografi.

4.1.3. Enkripsi dan Dekripsi

a. Proses Enkripsi

Pada penelitian ini dilakukan pengujian program yang berupa penyisipan pesan teks "MOSQUE" ke dalam animasi gif. Menggunakan Modulo 256 karakter berupa angkah, huruf dan simbol, maka $n = 256$. Pesan MOSQUE akan di ubah menjadi ciphertext menggunakan *Affine Cipher* dengan ketentuan $m = 137$ (137 relatif prima dengan 256) dan $b = 79$. Enkripsi plainteks dihitung dengan kekongruenan:

$C(P) \equiv 137P + 79 \ (mod\ 256)$

Plaintext	M	O	S	Q	U	E
P	77	79	83	81	85	69
$137P + 79$	10628	10902	11450	11176	11724	9532
$137P + 79 \ (mod\ 256)$	132	150	186	168	204	60
Ciphertext	ä	û	‖	ċ	╠	<

Maka menghasilkan Cipherteks sebagai berikut : ä û ‖ ċ╠ <

b. Proses Dekripsi

Untuk mengembalikan teks yang telah dienskripsi menjadi pesan rahasia dapat dilakukan pendekripsian, pertama-tama dapat dihitung $185^{-1}(mod\ 256)$, yang dapat dihitung dengan memecahkan kekongruenan lanjar

$$137P \equiv 1 \ (mod\ 256)$$

Untuk deskripsi dengan hasil 1 maka solusinya adalah $P = 185 \ (mod\ 256)$ dikarenakan $137 \times 185 = 25345\ mod\ 256$ menghasilkan $= 1$.

$$P\ (C) \equiv 185\ (C - 79)\ (mod\ 256)$$

Ciphertext	ä	û	‖	ċ	╠	<
C	132	150	186	168	204	60
$y - 79$	53	71	107	89	125	-19

$185\ (y\ -79)$	9805	13135	19795	16465	23125	-3515
$185\ (y-79)(mod\ 256)$	77	79	83	81	85	60
Plaintext	M	O	S	Q	U	E

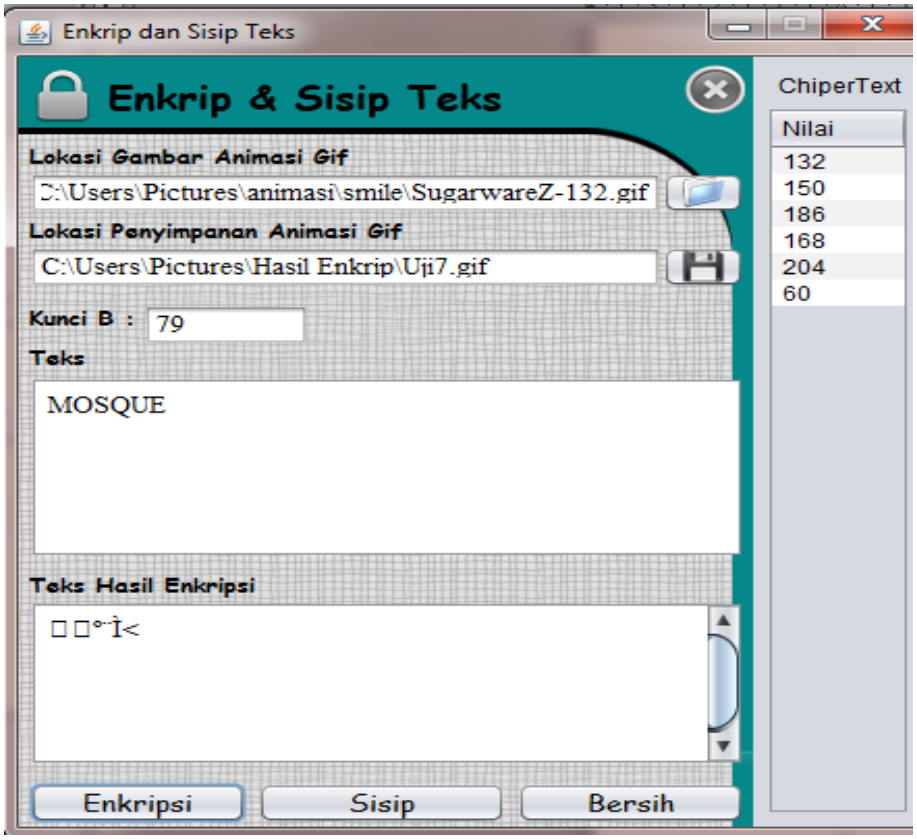
Maka menghasilkan Plainteks sebagai berikut : MOSQUE

4.1.4. *Encoding* dan *Decoding*

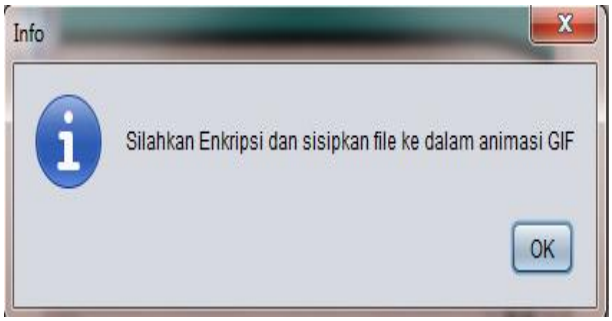
a. Encoding

Proses *encoding* yaitu proses untuk menyisipkan pesan kedalam media citra animasi *gif* yang telah diinputkan. Animasi *gif* sebagai media menyembunyikan pesan test atau biasa disebut *stego image*.

Proses *encoding* mengunakan *library gifshuffle* digunakan untuk menyisipkan teks ke dalam animasi *gif* dengan memanggil *lib* tersebut dan menginputkan parameter. Dengan menggunakan bahasa pemrograman java.

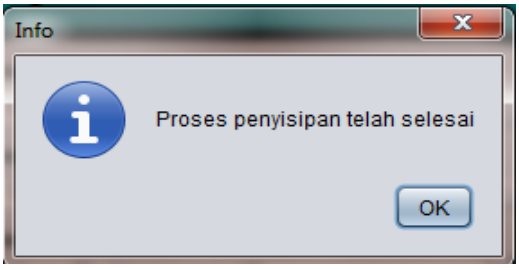


Gambar 3 : Layar Sisip yang telah disisi



Gambar 4 : Layar info penyisipan

Jika proses penyisipan pesan berhasil, maka akan muncul tampilan seperti di bawah ini:



Gambar 5 : Layar info telah selesai

Citra yang telah disisipkan pesan diberi nama "RAHASIA".gif yang akan berada pada direktori yang sama dengan citra asli. Berikut merupakan tampilan kedua gambar tersebut:

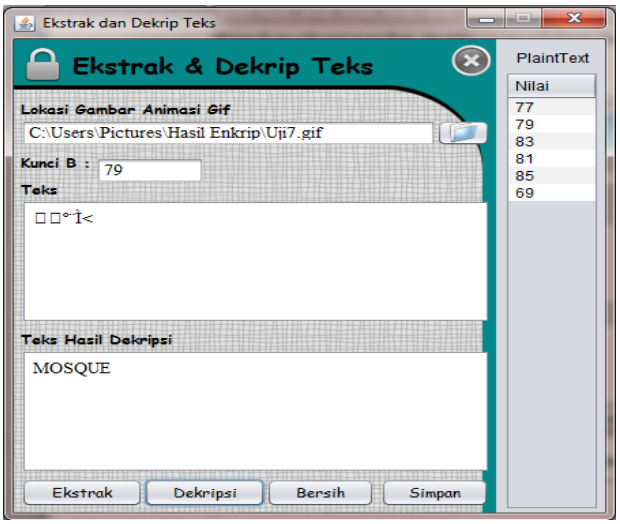
Gambar 6 : Animasi GIF asli.

Gambar 7 : Animasi GIF yang telah disisipkan teks.

Dari kedua gambar di atas dapat kita lihat bahwa perbedaan antara gambar asli dengan stego image tidak dapat terlihat oleh mata. Perbedaan antra keduanya hanya berupa ukurannya yang animasi asli 35,7 Kb sedangkan animasi yang sudah terisi pesan 35,9 Kb. Hal ini disebabkan perbedaan susunan palet warna di antara kedua gambar tersebut tidak menyebabkan perubahan pada bagaimana gambar tersebut terlihat oleh mata. Dengan demikian, algoritma *gifshuffle* telah memenuhi *imperceptibility*.

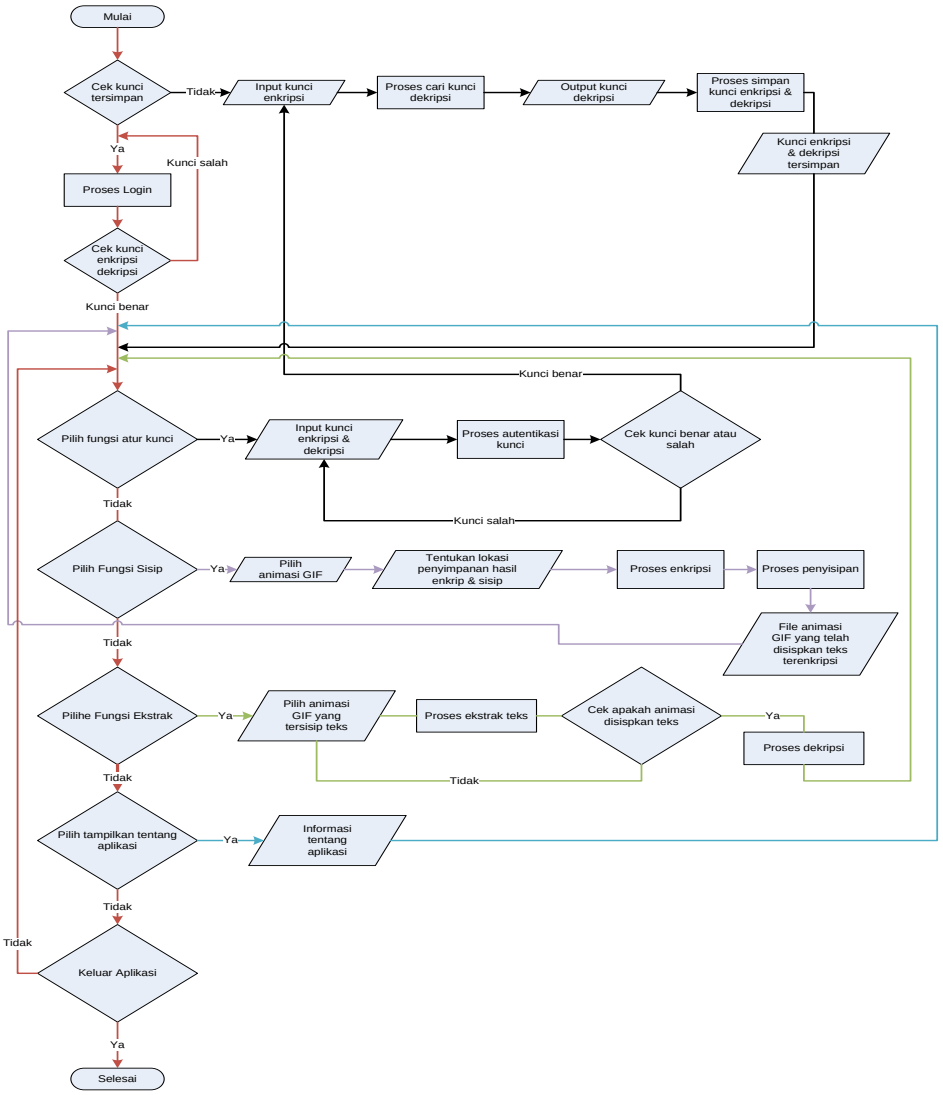
b. *Decoding*

Proses *decoding* yaitu proses pengekstrakan pesan dari citra animasi *gif* yang telah disisipkan pesan (*stego image*). Atau dapat dikatakan *decoding* adalah proses pembalikan dari *encoding* , yang dimana *library gifsuffle* dapat juga digunakan untuk mengekstrak teks dari dalam animasi *gif* yang telah disisipkan. Pertama file bat akan dibuat dengan nama “decompression.bat” agar dapat menjalankan GZ_unzip (*library* untuk melakukan ekstrak).



Gambar 8 : Layar ekstrak yang akan diekstrak

4.1.5. Flowchart



Gambar 9 : Flowchart

4.2. Pembahasan

Enkripsi *affine cipher* untuk *Steganografi* pada animasi citra *gif.* Diuji dengan menggunakan file citra dengan tipe *gif* dimana file-file tersebut akan disisipkan pesan dengan menggunakan teknik algoritma *affine cipher* dan *gifshuffle* file citra dengan tipe file *gif,* kemudian kita akan mengenkripsi pesan yang akan disisipi setelah enkripsi maka pesan akan sisipkan kedalam media atau disebut *stego-image*.

Untuk melakukan pengujian terhadap citra GIF dilakukan implementasi sistem ke dalam komputer dengan menggunakan bahasa pemrograman yang digunakan adalah bahasa Java dengan menggunakan NetBeans IDE 7.1.2 dan untuk memudahkan pemakaian program dibuat dalam bentu GUI (*Graphic User Interface)*. Aplikasi ini berjalan di komputer dengan sistem operasi *Windows XP.*

Dalam program ini tidak di batasi karakter yang akan disisipkan sehingga penggunaanya bisa lebih umum dan memiliki kunci ekripsi dan dekripsi yang berbeda sehingga sangat sulit untuk melakukan steganalisis.

V. Kesimpulan

Hasil pengujian program diperoleh bahwa aplikasi ini dapat mengacak dan menyembunyikan pesan dengan aman dan tidak menimbulkan kecurigaan. Pada file hasil, tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya.

Daftar Pustaka

[1]. Sitompul, R Putri, 2010, *Analisis Dan Implementasi Steganografi Pada Citra Gif Menggunakan Algoritma Gifshuffle,* Skripsi*,* Medan.