APLIKASI PENYISIPAN TEKS PADA GAMBAR DENGAN ALGORITMA *BLOWFISH* DAN *LEAST SIGNIFICANT BIT*

Angga Aditya Permana[1]
Universitas Muhammadiyah Tangerang / Fakultas Teknik,
Program Studi Informatika
Jl. Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang TLP. 55793251, 55772949, 55793802, 55736926
Email: anggaumt@yahoo.com

ABSTRAK

Aplikasi komputer pada berbagai bidang kehidupan menimbulkan beberapa kekhawatiran, salah satunya berkaitan dengan keamanan bertransaksi melalui media ini. Belakangan ini, steganografi menjadi metode yang sangat menarik perhatian sebagai salah satu jalan keluar yang menjanjikan. Steganografi dilakukan dengan tujuan mencegah penyalahgunaan informasi (hacking), sehingga informasi tersebut terlindung dari hal-hal yang tidak diinginkan. Kriptografi dan steganografi saat ini telah menjadi kebutuhan bagi mereka yang membutuhkan privacy dan security dalam hal pengiriman data teks, suara, image, serta video. Untuk menghindari pesan informasi bisa dibaca oleh orang yang tidak berhak mendapatkan informasi tersebut, bahkan tidak diketahui atau disadari oleh pihak ketiga, bahwa data ataupun file image yang dilihat tersebut mengandung informasi rahasia, terkecuali bagi mereka yang mengerti kuncinya. Implementasi menggabungkan dua teknik kriptografi dan steganografi yang disisipkan pada sebuah file gambar untuk menjamin lebih kuat dan aman informasi yang ada didalam file gambar tersebut. Metode yang digunakan adalah melakukan teknik kriptografi terlebih dahulu menggunakan algoritma Blowfish “OpenPGP.Cipher.4”. Teks informasi yang telah terenkripsi tersebut kemudian dimasukkan pada pixel yang diambil dengan menggunakan metode *Least Significant Bit Insertion* (LSB).

Kata kunci *: Kriptografi, Steganografi, Blowfish, Least Significant Bit Insertion (LSB).*

ABSTRACT

Computer applications in various fields of life raises some concerns, one of which relates to the security of transactions through this medium. Lately, steganography be the method is very interesting as one promising way out. Steganography is done with the aim of preventing the misuse of information (hacking), so that the information is protected from things that are not desirable. Cryptography and steganography has now become a necessity for those who need privacy and security in terms of data transmission of text, voice, image, and video. To avoid the message information can be read by people who are not entitled to the information, is not even known or recognized by a third party, that data or image file that contains confidential information visible, except for those who know the key. Implementation combines two techniques of cryptography and steganography is pasted on an image file to ensure more robust and secure information in the image file. The method used is to first perform cryptographic technique using the Blowfish algorithm "OpenPGP.Cipher.4". Text information that has been encrypted are then put on a pixel taken using the method Insertion Least Significant Bit (LSB).

Keywords*: Kriptografi, Steganografi, Blowfish, Least Significant Bit Insertion (LSB).*

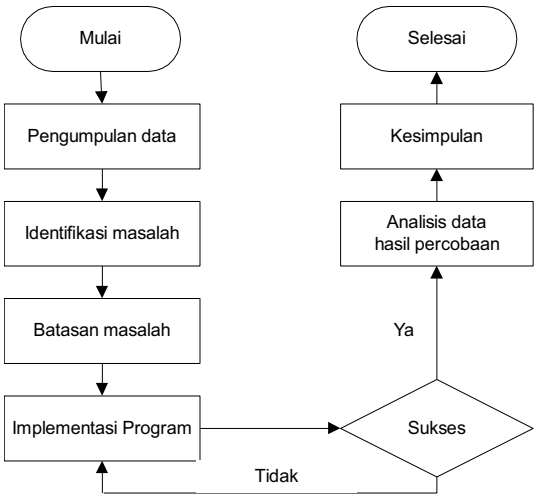
1. Pendahuluan

Kemajuan teknologi memungkinkan kita untuk berkomunikasi dan bertukar informasi melalui media digital. Namun penggunaan media digital meningkatkan resiko penyadapan terhadap informasi/pesan. Hal ini merupakan permasalahan penting dalam menjaga kerahasiaan informasi/pesan. Salah satu cara untuk mencegah penyadapan informasi/pesan adalah dengan melakukan penyandian yang dikenal dengan proses enkripsi. Dalam proses enkripsi, pesan/informasi akan diubah menggunakan algoritma tertentu untuk menyembunyikan makna sebenarnya.

Banyak cara untuk melakukan teknik kriptografi seperti menggunakan teknik AES yang merupakan teknik yang sangat powerful. Metode kriptografi merupakan sebuah metode untuk mengolah informasi dengan algoritma tertentu sehingga informasi menjadi samar dan sulit untuk dimengerti maknanya. Dengan menggunakan metode ini akan menimbulkan kecurigaan bagi pihak ketiga, sebab pesan yang sulit dimengerti sudah bisa dipastikan mengandung informasi yang penting. Kriptografi akan merahasiakan informasi dengan menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Saat ini banyak bermunculan algoritma kriptografi yang terus dianalisis, dicoba dan disempurnakan untuk mencari algoritma yang dianggap memenuhi standar keamanan. Beberapa algoritma kriptografi yang dikenal antara lain DES, Rijndael, Blowfish, RC4, Vigenere Cipher, Enigma, IDEA dan lainnya.

2. Metodologi

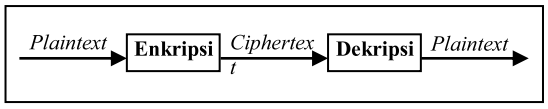
Subjek dari penelitian ini adalah kriptografi algoritma Blowfish dan steganografi algoritma Least Significant Bit insertion (LSB) untuk proses enkripsi dan dekripsi teks kedalam file image. Penelitian ini akan diimplementasikan dalam bentuk program aplikasi dengan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0. Adapun metode pengumpulan data yang dilakukan dalam proses penelitian ini yaitu dengan menggunakan metode kepustakaan, metode ini dilakukan dengan cara mengumpulkan data, mempelajari dan memahami buku-buku literatur serta beberapa jurnal dan paper yang berhubungan dengan penelitian ini.



Gambar 2.1 Diagram alir penelitian

3. Landasan Teori

Bentuk asli dari sebuah pesan atau data disebut dengan *plaintext* dan bentuk asli dari pesan atau data yang terenkripsi di sebut *ciphertext.*



Gambar 3.1 Enkripsi dan Dekripsi

Data atau *Plaintext* dinotasikan dengan M *(Message)*, yang dapat berupa *bit stream, file text, digital video image*, dan sebagainya atau lebih singkatnya M adalah data ***binary.*** Fungsi Enkripsi **E**, berfungsi untuk mengubah **M** menjadi **C** atau *Ciphertext*, dalam matematika dinotasikan dengan:

E(M) = C.

Fungsi Dekripsi **D**, berfungsi untuk mengubah **C** menjadi **M**, dalam matematika dinotasikan dengan :

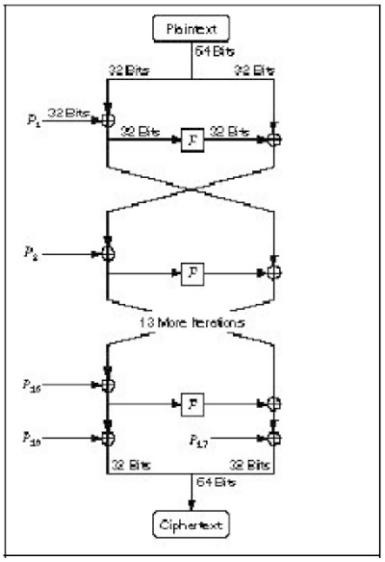
D(C) = M.

3.1. Blowfish

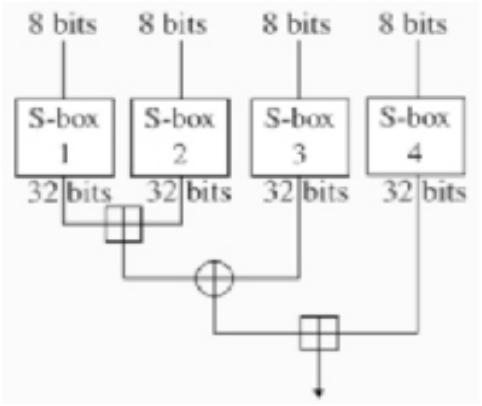
Blowfish merupakan metode enkripsi yang mirip dengan DES (DES-

like Cipher) dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroprosessor besar (32 bit ke atas dengan cache data yang besar).
Blowfish dikembangkan untuk memenuhi criteria desain sebagai berikut:

1. Cepat, pada implementasi yang optimal Blowfish dapat mencapai kecepatan 26 clock cycle per byte.
2. Kompak, Blowfish dapat berjalan pada memori kurang dari 5 KB.
3. Sederhana, Blowfish hanya menggunakan operasi yang simple: penambahan (addition), XOR, dan penelusuran table (table lookup) pada operand 32 bit. Desainnya mudah untuk dianalisa yang membuatnya resisten terhadap kesalahan implementasi.
4. Keamanan yang variable, panjang kunci Blowfish dapat bervariasi da dapat mencapai 448 bit (56 byte).



Gambar 3.2 Struktur Blowfish Cipher



Gambar 3.3. F-function Blowfish Cipher

3.2. Least Significant Bit Insertion (LSB)

Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya pada file image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada *file stego*,harus digunakan format *lossless compression*. Hal itu dikarenakan metode inimenggunakan bit-bit pada setiap piksel pada *image*. Jika digunakan format *lossycompression*, pesan rahasia yang disembunyikan dapat hilang. Contoh penggunaan *LSB*, sebuah susunan bit pada sebuah *byte:*

Untuk memperkuat teknik penyembunyian data, bit–bit data rahasia tidak digunakan mengganti *byte* yang berurutan namun dipilih susunan *byte* yang acak. Misalnya, jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan maka *byte* yang diganti bit *LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49. Bilangan acak dibangkitkan dengan *pseudo-random-number-generator*

(*PRNG*)*cryptography. PRNG cryptography* merupakan algoritma *cryptography* yang digunakan untuk enkripsi dan dibangun dengan menggunakan algoritma *DES* (*Data EncryptionStandard*). Misalkan segmen dari data sebelum ditukar adalah:

00110011 10100010 11100010

01101111

Setelah data '0110' disembunyikan,

segmen menjadi:

0011001**0** 10100001**1** 11100011

0110111**0**

Jika digunakan *image* 24 bit *color* sebagai *cover,* sebuah bit dari masing-masing komponen *Red, Green*, dan *Blue* (RGB) dapat digunakan, sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 *bytes*) data rahasia. Misalnya, terdapat 3 piksel dari *image* 24 bit *color* :

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Jika diinginkan untuk menyembunyikan karakter A dengan nilai biner 10000001 maka dihasilkan:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

4. Pembahasan

4.1. Analisa Kebutuhan Sistem

Pada sub bab berikut ini akan membahas tentang analisa kebutuhan-kebutuhan dalam pembuatan sistem. Sistem yang dibuat adalah Kriptografi menggunakan algoritma Blowfish terhadap teks dan steganografi *Least Significant Bit Insertion* (LSB) yang disisipkan pada media gambar yang berekstensi *.JPG. setelah melalui proses penelitian yang lebih mendalam dan merujuk pada beberapa pustaka yang ada dapat dinyatakan bahwa sistem ini akan terdiri dari enam unsur penting antara lain:

a. Terdapat fasilitas untuk melakukan proses enkripsi *plaintext* berupa Teks.
b. Terdapat fasilitas untuk melakukan proses *chipertext* terhadap teks.
c. Terdapat fasilitas untuk melakukan proses Steganografi menggunakan metode *Least Significant Bit Insertion* (LSB) terhadap sebuah image.
d. Proses enkripsi dan dekripsi membutuhkan kunci yang diinputkan oleh user.
e. Terdapat proses untuk penyimpanan file gambar yang telah disisipkan *chipertext.*
f. Terdapat proses login untuk menyaring menyeleksi penggunaan aplikasi program.

4.2. Flowchart Program

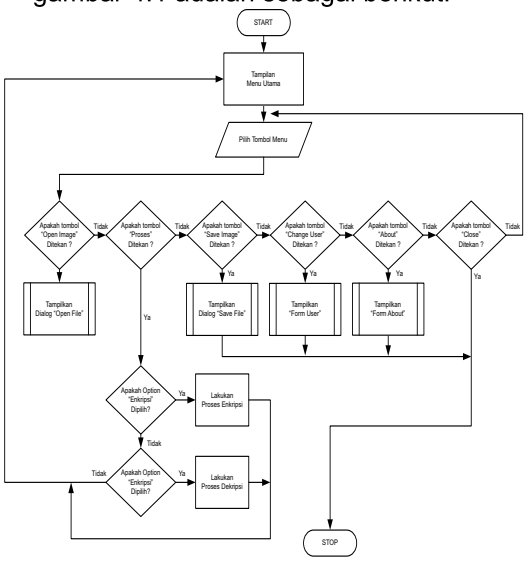
Flowchart program akan menggambarkan alur proses penggunaan program sehingga dapat berfungsi sebagai sarana untuk melakukan proses enkripsi dan dekripsi menggunakan algoritma *Blowfish* dan proses steganografi menggunakan metode *Least Significant Bit Insertion* (LSB). Adapun langkah-langkah dari flowchart tersebut adalah sebagai berikut :

a. User memulai proses dengan melakukan pemilihan pada tombol menu.
b. Menampilkan masing-masing proses sesuai menu yang dipilih.
c. Jika user memilih tombol menu "Open Image" maka aplikasi akan menampilkan dialog open file, dan menampilkannya pada image box yang telah disediakan sesuai dengan file gambar yang dipilih.
d. Jika user memilih tombol menu "Proses" akan melakukan proses sesuai dengan pilihan yang dipilih pada option "Enkripsi" atau "Dekripsi" dan checkbox "show Pixels" akan menampilkan hasil penyisipan pada gambar yang ada pada image box, sehingga akan terlihat bintik-bintik warna merah. Sedangkan jika

checkbox tidak dicentang maka bintik-bintik merah pada gambar tidak akan terlihat pada hasil proses enkripsi.

e. Jika user memilih tombol menu “Save Image” maka akan dilakukan proses penyimpan file gambar yang merupakan hasil dari proses penyisipan *chipertext*.
f. Jika user memilih tombol menu “Change User” maka aplikasi akan menampilkan form untuk melakukan proses penggantian dan penambahan username dan kode password untuk menjalankan aplikasi.
g. Jika user memilih tombol menu “About” maka aplikasi akan menampilkan form about, yang digunakan sebagai informasi pembuat program kepada pengguna.
h. Jika user meilih tombol close maka aplikasi akan menutup program tersebut dan akan mengkonfirmasi ulang pada pengguna untuk memastikan bahwa pengguna akan benar-benar melakuka proses penutupan aplikasi.

Adapun gambaran dari proses algoritma diatas akan terlihat pada gambar 4.1 adalah sebagai berikut:



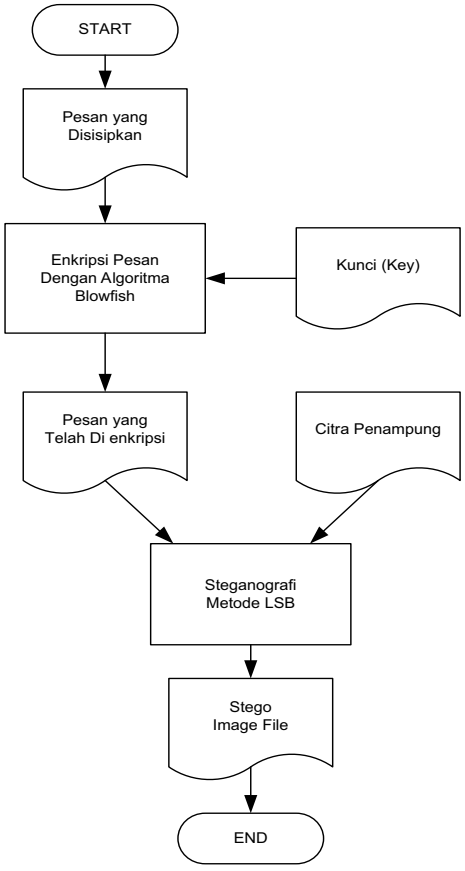
Gambar 4.1. Gambar Flowchart Program

4.3. Perancangan Sistem

Prosedur perancangan sistem secara umum untuk pembangunan aplikasi kriptografi dan steganografi pada file gambar ini terdiri atas beberapa tahapan, antara lain meliputi perancangan :

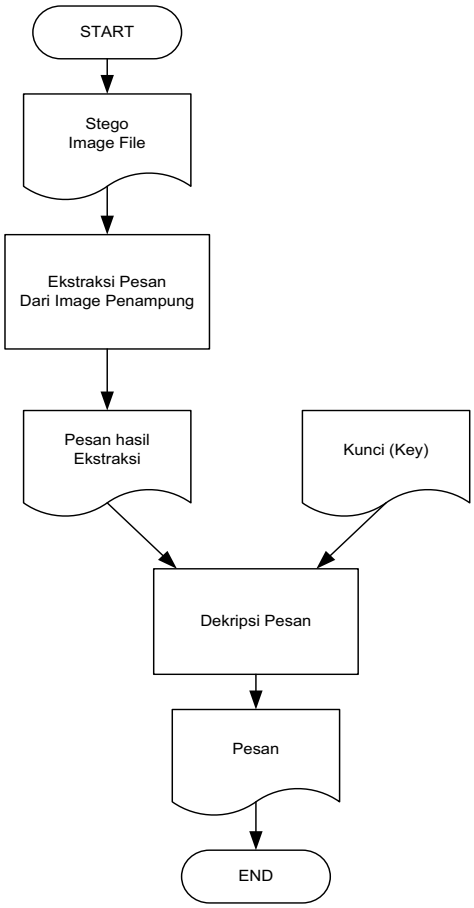
a. Proses

Perancangan proses yang dimaksudkan adalah bagaimana sistem akan bekerja, proses-proses yang digunakan, mulai dari user melakukan input *chipertext* kemudian melalui proses kriptografi hingga aplikasi mengeluarkan output berupa stego file pada proses penyisipan (*hiding*). Pada gambar 4.2 berikut ini merupakan diagram alur proses tersebut.



Gambar 4.2. Diagram Alur Proses Enkripsi Penyisipan Pesan

Dan juga saat user melakukan input stego file dan key file hingga aplikasi memberikan output berupa informasi rahasia dan carrier file pada proses penguraian (*extracting*).



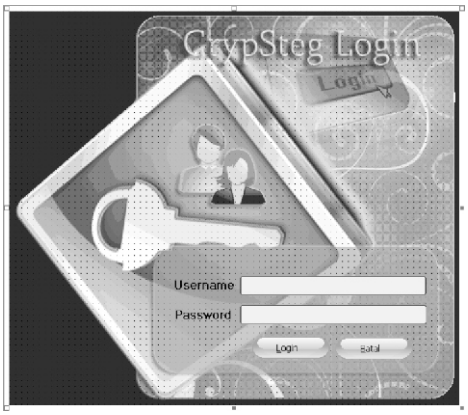
Gambar 4.3. Diagram Alur Proses Ekstraksi dan Dekripsi Pesan

b. Antar Muka

Perancangan antarmuka mengandung penjelasan tentang desain dan implementasi sistem yang digunakan dalam sistem yang dibuat dan diwujudkan dalam tampilan antarmuka sang menghubungkan user dengan aplikasi.

1. Perancangan antarmuka Form Login

Pada perancangan form login ini digunakan untuk memfilter hak akses dalam menggunakan program aplikasi yang dibuat. Pada proses penyimpanan username dan kode password ini akan disimpan pada database yang sebelumnya kode password tersebut dilakukan proses enkripsi dengan menggunakan algoritma MD5, sehingga kode yang tersimpan dalam database tidak sesuai dengan teks kode yang dimasukkan pada Txt_Pass pada form Login. Ada rancangan Form Login yang dibuat adalah sebagai berikut:



Gambar 4.4. Rancangan Form Login

2. Perancangan antarmuka Form Utama

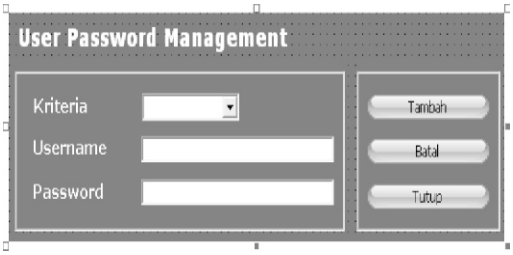
Pada perancangan Form Utama digunakan untuk aplikasi melakukan proses utama pada aplikasi ini, yang didalamnya berisi proses untuk melakukan pengambilan file image untuk disisipkan teks hasil enkripsi yang kemudian file image hasil penyisipan tersebut akan disimpan menjadi sebuah file image yang mengandung informasi rahasia. Pada gambar 4.5 berikut merupakan rancangan tampilan antarmuka Form Utama.

Gambar 4.5. Rancangan Form Utama

Selain aplikasi ini dapat melakukan proses penyisipan teks rahasia yang telah terenkripsi, dapat juga digunakan untuk menampilkan kembali (ekstraksi) teks informasi yang disisipkan pada image file (stego file) sehingga file informasi yang telah disisipkan dapat di kenali dan dimengerti maksud dan tujuan dari pesan tersebut.

3. Perancangan antarmuka Form User

Perancangan Form User digunakan untuk melakukan proses memasukkan dan mengubah username dan kode password yang telah tersimpan dalam database, sehingga pengguna dari aplikasi ini dapat di tambah sesuai dengan kebutuhan penggunaan. Pada gambar 4.6 merupakan gambar Form User.



Gambar 4.6. Rancangan Form User

5. Kesimpulan

Steganografi dengan menggunakan metode *Least Significant Bit Insertion* (LSB) merupakan teknik yang relatif mudah untuk dimengerti, walupun pesan yang terdapat dalam file stego dapat dengan mudah diekstrak oleh orang-orang yang tidak bertanggung jawab menggunakan software steganalysis yang dapat dengan mudah mendapatkannya dan penggunaanya, sehingga siapapun dapat melakukan proses ekstraksi informasi pada file stego. Selain itu, ukuran file yang mengandung stego akan semakin besar sesuai dengan kandungan teks informasi yang disisipkan. Tetapi dengan cara melakukan proses enkripsi teks informasi yang akan disisipkan terlebih dahulu, keamanan pesan informasi yang terkandung didalamnya akan semakin terjaga kerahasiaannya.

Daftar pustaka

[1] Aditya, Yogie, dkk, 2010, *Studi Pustaka untuk steganografi dengan beberapa metode*, Prosiding Seminar Nasional Aplikasi Teknologi Informasi Yogyakarta 9 Juni 2010.

[2] Alatas, Putri, 2009, *Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital*, Jakarta, Universitas Gunadarma.

[3] Krisnawati, 2008, *Metode Least Significant Bit (LSB) dan End Of File (EOF) untuk menyisipkan Teks ke Dalam Citra Grayscale*, Prosiding Seminar Nasional Informatika @ UPN Veteran Yogyakarta 24 Mei 2008.