Steganografi LSB 3 Bit pada Gambar Digital dengan Key Terenkripsi *Vigenere Chiper*

Helda Yenni
STMIK-AMIK Riau
helda@stmik-amik-riau.ac.id

Abstrak

Komunikasi antar komputer saat ini merupakan hal yang umum dilakukan para pengguna komputer. Komunikasi ini dapat memperpendek jarak dan waktu terutama pada posisi geografis yang berjauhan. Bentuk komunikasi tersebut dapat salah satunya berupa transfer data. Dalam hal transfer data tersebut,mutlak diperlukannya aspek keamanan data baik pada saat pengiriman data sehingga data diterima oleh pihak penerima dalam keadaan utuh. Hal tersebut mencegah terjadinya kemungkinan kerusakan ataupun manipulasi data oleh pihak yang tidak memiliki otoritas terhadapnya.Steganografi merupakan teknik untuk melindungi file digital dalam hal ini file gambar digital dengan prinsip kerja menyisipkan "suatu pesan" didalam file digital tersebut. Metode LSB (Least Significant Bit dapat menyisipkan 3 bit pada setiap file sumber (carrier). Selain itu dalam penelitian digunakan juga metode enkripsi pesan berupa Vigenere Chiper yang nantinya dapat mengubah bentuk pesan yang disisipkan ke dalam gambar digital ke dalam bentuk chipertext sehingga meningkatkan keamanan data gambar digital tersebut. Pengujian aplikasi ini dibuat dengan bahasa pemograman Borland Delphi 2007. Sistem ini mampu menyisipkan teks sebanyak ± 37,5% dari jumlah pixel pesan pada setiap file carrier.

Kata Kunci : keamanan data, file gambar,enkripsi pesan

Abstract

Currently, internal computer communication is a common thing done by computer user. This communication can shorten the distance and time, especially on geographical positions that are far apart. One form of communication can include data transfer. In transferring data, security data in sending and receiving process is needed. It avoids the possibility of damage or manipulation of data by unauthorized user. Steganography is a technique to protect digital file, in this case digital image file with the working principle insert a message in the digital file. LSB method (Least Significant Bit) can insert 3 bits in every file carrier. Besides, in the research also used the message encryption method as Vigenere Chiper in which can change the message form inserted to the digital image in the form of chipertext so it can raise the data security. This system is able to insert text around ± 37,5% of the total message pixels in file carrier.

Keywords : data security, image file, message encryption

1. Pendahuluan

Perkembangan teknologi informasi yang semakin pesat mampu memperluas fungsi dari sebuah komputer. Dengan teknologi informasi dapat mempermudah aktivitas manusia dalam menyelesaikan suatu pekerjaan. aaaaapenggunaan teknologi informasi dalam hal transfer data seperti transfer file, electronic mail

dan sebagainya rentan terhadap kerusakan yang salah satunya bisa diakibatkan oleh tindakan yang tidak bertanggung jawab oleh pihak yang tidak memiliki otoritas terhadap data tersebut. Untuk itulah diterapkan metode keamanan data, salah satunya adalah steganografi.

*Menurut Ana Sapta Rindi, Sihar N.M.P. Simamora,dan Isa Puncuna dalam jurnalnya Teknik steganography LSB (*Least Significant Bit*), metode ini banyak digunakan karena metode ini paling sederhana dan mudah diimplementasikan. Media penampungnya berupa gambar digital karena jumlahnya yang besar di internet. Kehandalan penggunaan citra dibandingkan dengan media lain adalah kualitas citra yang telah disisipi pesan rahasia tidak berbeda jauh dengan kualitas citra aslinya. [7]*

Pada dasarnya setiap pixel citra digital dengan format bitmap (*.bmp) memiliki 3 elemen warna, yang jika dikombinasikan akan menghasilkan 16 juta lebih warna. Berdasarkan hal-hal tersebut, maka penulis tertarik untuk melakukan penelitian dengan modifikasi pada setiap LSB dari 3 elemen warna yang ada pada setiap pixel sehingga setiap pixel dapat disisipkan 3 bit pesan.

2. Citra Digital

Citra digital adalah sebuah fungsi 2D, f(x,y), yang merupakan fungsi intensitas cahaya, dimana nilai x dan y merupakan koordinat spasial dan nilai fungsi di setiap titik (x,y) merupakan tingkat keabuan citra pada titik tersebut. Di dalam komputer, citra digital disimpan sebagai suatu file dengan format tertentu. Format citra tersebut menunjukan cara sebuah citra digital disimpan, misalnya apakah dengan suatu kompresi atau tidak. Contoh format citra digital adalah .bmp, .jpg, .png, .tif dan sebagainya. Ukuran citra digital dinyatakan dalam pixel (picture element) [5].

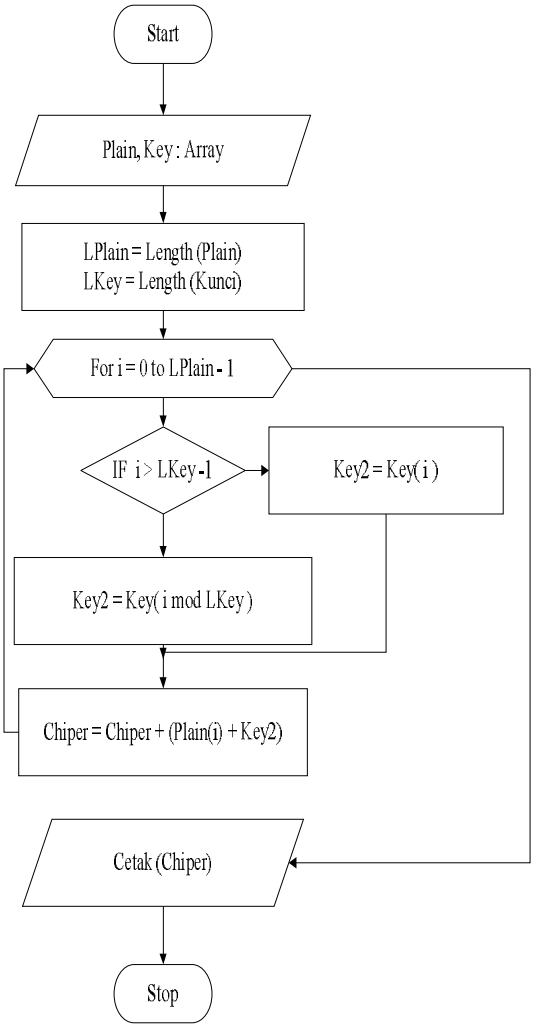
3. LSB

Pada susunan *bit* di dalam sebuah *byte* (1 *byte* = 8 *bit*), terdapat *bit* yang paling berarti, yaitu *Most Significant Bit* (MSB) dan *bit* yang kurang berarti, yakni *Least Significant Bit* (LSB). Sebagai ilustrasi, pada huruf A yang memiliki nilai biner 01000001, terdapat MSB dan LSB. Untuk 0 (0 yang digarisbawahi) adalah MSB, sedangkan 1 (1 yang digarisbawahi) adalah LSB.

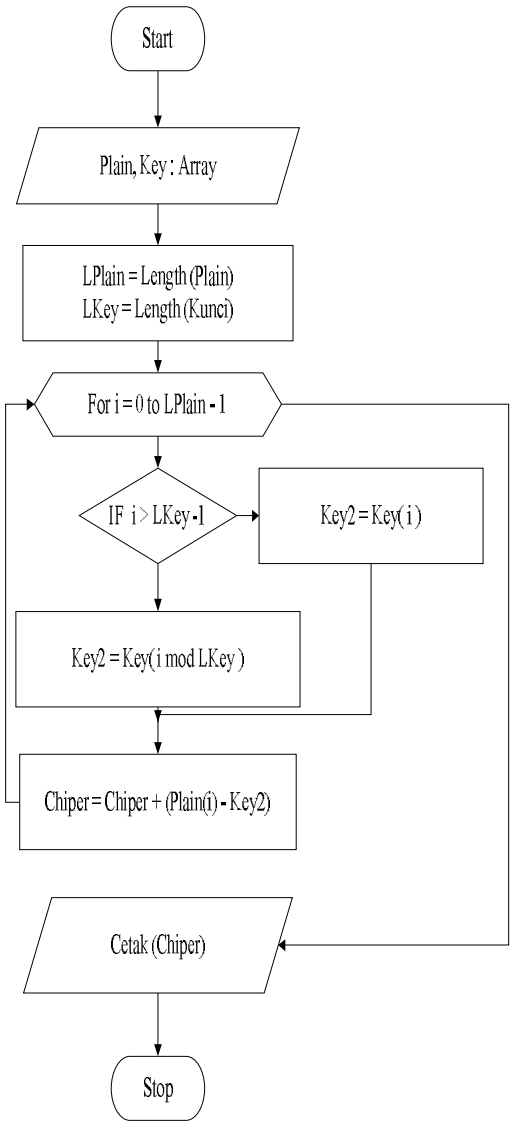
Karena LSB merupakan nilai bit terakhir atau paling rendah dari setiap *byte* data, maka *bit* yang dianggap cocok untuk diganti dengan bit pesan adalah LSB, sebab penggantian hanya mengubah *byte* tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya.

4. Enkripsi dan Dekripsi

Berikut ini adalah Flowchart Enkripsi dan Dekripsi dari aplikasi yang dibangun :



Gambar 1. Flowchart enkripsi pesan



Gambar 2. Flowchart dekripsi pesan

Enkripsi dan dekripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli (plaintext) diubah menjadi kode-kode yang tidak dapat dimengerti (Ciphertext). Sedangkan Dekripsi merupakan proses pengembalian Chipertext menjadi Plaintext kembali sehingga data yang dikirimkan dapat dibaca dengan baik dan dapat dimengerti maknanya.

Kode Vigenere (Vigenere Cipher) termasuk kode abjad majemuk (Polyalphabetic Substitution Cipher). Untuk mengenkripsi pesan dengan kode Vigenere digunakan tabula recta(disebut juga dengan bujursangkar Vigenere).

Secara matematis enkripsi dengan kode vigenere dapat dinyatakan sebagai :

E(pi) = V (pi, k(i mod m))

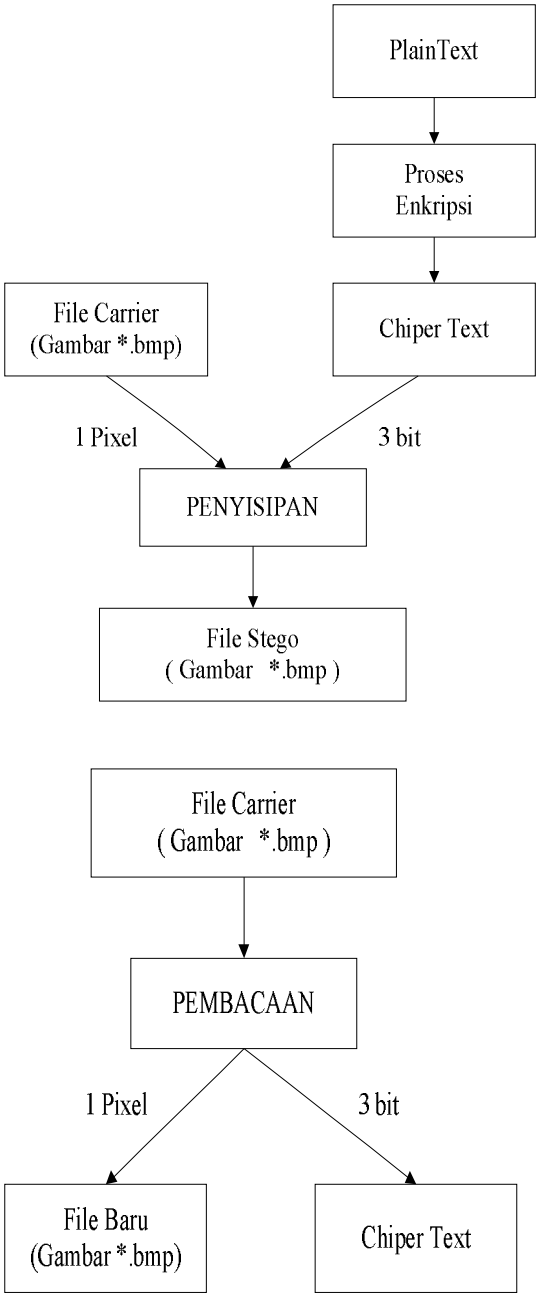
Dengan :
Pi = huruf ke-i dalam plaintext
Kn = huruf ke-n dalam kunci
M = panjang kunci
V(x,y)= huruf yang tersimpan pada baris x dan kolom y pada tabula recta. [6]

5. Penyisipan dan Pembacaan Pesan

Sesuai dengan fungsinya, untuk melakukan penyisipan atau penyembunyian informasi, maka teknik ini akan melakukan perubahan pada LSB untuk setiap byte data, yaitu dengan cara mengganti bit terakhir atau bit sebelah kanan pada setiap byte yang dimiliki oleh file carrier dengan satu bit data yang terdapat pada pesan atau informasi yang akan disembunyikan. Sedangkan untuk membaca pesan atau informasi yang tersembunyi pada file carrier, kita dapat menggunakan teknik yang sama pada saat penyembunyian pesan, yaitu menggunakan Least Significant Bit (LSB).

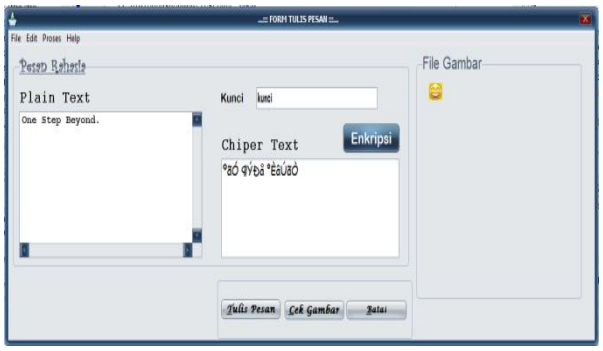
Adapun yang membedakan antara proses penyisipan dan pembacaan yakni pada proses penyembunyian pesan, setiap bit pesan diletakkan dan disusun tepat pada LSB dari masing-masing byte file carrier, kemudian LSB yang dimiliki oleh file carrier tersebut diganti dengan setiap bit pesan, sehingga diperoleh sebuah nilai binary yang baru. Sedangkan pada proses pembacaan pesan, maka semua LSB dari file yang sudah memiliki pesan (file stego) disusun kembali sesuai dengan proses peletakannya, kemudian dilakukan pembacaan, sehingga diperoleh informasi atau pesan yang disembunyikan tersebut.

Berikut ini diagram Penyisipan dan Pembacaan Pesan pada gambar digital berformat *.bmp :

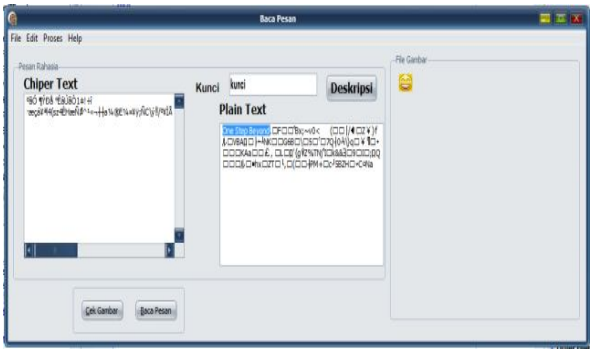


6. Hasil Pengujian

Pada tahapan implementasi dan pengujian diperoleh hasil bahwa file stego yang merupakan file hasil dari proses steganografi tidak memberikan perubahan yang sangat berarti jika dilihat secara kasat mata. Hasil tersebut dapat dilihat pada perbandingan informasi secara detail untuk file carrier dan file stego berikut :



Gambar 3. Form tulis pesan



Gambar 4. Form baca pesan

Gambar 5. Gambar yang akan dienkripsi (Smile.bmp)

Name	smile.bmp
Item type	Bitmap Image
Folder path	F:\
Date created	29/12/2012 15:34
Date modified	08/10/2012 8:30
Size	1,46 KB
Size:	1,46 KB (1.496 bytes)
Size on disk:	4,00 KB (4.096 bytes)

Gambar 6. Hasil Enkripsi

Name	111.bmp
Item type	Bitmap Image
Folder path	F:\carrier
Date created	29/12/2012 15:27
Date modified	29/12/2012 15:23
Size	1,45 KB
Size:	1,45 KB (1.494 bytes)
Size on disk:	4,00 KB (4.096 bytes)

7. Kesimpulan

Berdasarkan pengujian terhadap aplikasi yang dibangun maka dapat disimpulkan bahwasanya teknik Steganografi didukung oleh pesan yang terenkripsi juga dapat dijadikan suatu solusi untuk mengamankan file berupa gambar digital dari adanya intervensi dari pihak-pihak yang tidak memiliki otoritas terhadap file tersebut. Di tahapan imlementasi, gambar digital yang digunakan berformat bitmap(*.bmp). Aplikasi ini mampu menyisipkan pesan pada gambar sejumlah 37,5% dari jumlah pixel pesan pada file carrier yang sudah terenkripsi kemudian dapat didekripsi untuk dapat dibaca kembali oleh penerima pesan yang terotorisasi terhadapnya.

Referensi

[1] Achmad Balza, 2011. Pemograman Delphi Untuk Aplikasi Mesin Visi Menggunakan Webcam, Gava Media, Yogyakarta.

[2] Fadlisyah, 2007, Computer Vision dan Pengolahan Citra, Andi, Yogyakarta.

[3] Kusnassriyanto, 2011, Belajar Pemrograman Delphi, Modula, Bandung.

[4] Munir, Rinaldi, 2004, Pengolahan Citra Digital dengan Pendekatan Algoritmik, Informatika, Bandung.

[5] Sutoyo, T., Edy Mulyanto, Vincent Suhartono, Oky Dwi Nurhayati, Wijanarto,2009, Teori Pengolahan Citra Digital, ANDI, Yogyakarta.

[6] Doni Ariyus,2008. Pengantar Ilmu Kriptografi Teori,Analisis,danImplementasi,ANDI, Yogyakarta

[7] Ana Sapta Rindi, Sihar N.M.P. Simamora, ST., MT., Isa Puncuna, ST., 2010,Politeknik Telkom.