Jurnal Nasional Informatika dan Teknologi Jaringan
E-ISSN : 2540-7600
P-ISSN : 2540-7597

KONSEP PENYANDIAN FILE JPEG DENGAN MENGGUNAKAN METODE LSB

Haikal Nando Winata[1], Raja Nasrul Fuad[2]
Institut Teknologi Medan - Fakultas Teknologi Industri, Prodi Teknik Informatika
ekalnata@itm.ac.id

Abstrak— Steganography is a technique to hide text or messages that other people do not know the contents of the text or the secret message. Steganography technique is often used to avoid suspicion and to avoid other people desire to know the contents of the text or the secret message. Digital image is one of the most well-known media and the public by the author. Digital image acts as a medium or a text container you want to hide a secret message. Methods LSB (Least Significant Bit) that hides the bytes of text or message you want to hide into the last byte in the digital image. LSB method has the advantage of not changing the size and shape of the digital image by naked eye, text data or messages hidden can be restored without any change in size and shape.

Keywords— Steganography, Digital Image, LSB Method.

I. PENDAHULUAN

Steganografi salah satu pengembangan sistem keamanan data atau pesan yang ada pada saat ini. Steganografi merupakan seni atau praktik menyembunyikan pesan, citra, atau file kedalam pesan, citra atau file yang lain. Keuntungan steganografi dibandingkan dengan kriptografi adalah pesan rahasia tidak menarik perhatian karena bersifat tersembunyi pada media lain. Steganografi meliputi penyembunyian informasi dalam file komputer. Dalam steganografi digital, komunikasi elektronik dapat mencakup steganografi coding dalam lapisan transport, seperti file dokumen, file gambar, program atau protokol . File media yang ideal untuk transmisi steganografi karena ukurannya yang besar.

Steganografi pada saat ini telah banyak diterapkan memanfaatkan citra digital. Berbagai teknik dan algoritma telah berkembang dan digunakan dalam implementasi steganografi pada citra digital. LSB atau Least Significant Bit merupakan salah satu teknik atau algoritma yang banyak digunakan pada bidang steganografi. Teknik LSB adalah teknik dimana tiap bit dari pesan akan menggantikan bit terendah dari piksel warna pada citra digital. Proses penggantian bit terus dilakukan secara berulang pada tiap urutan piksel warna pada citra digital.

Penyembunyian pesan atau steganografi banyak diterapkan pada komunikasi publik, dimana pesan atau informasi mengalir pada jaringan yang digunakan oleh banyak orang ke penerima. Luasnya jaringan komunikasi publik menyebabkan sulitnya menjaga atau mengamankan informasi dari pihak – pihak luar seperti penyadap atau peretas selama informasi tersebut mengalir ke penerima Steganografi dapat diterapkan untuk mengatasi masalah keamanan informasi pada komunikasi. Informasi ditanamkan pada media lain sehingga seolah-olah informasi yang dikomunikasikan adalah media tersebut yang mana media penampung tidak lebih berharga dari informasi yang ditanamkan pada media tersebut. Selain steganografi, bidang lain yang digunakan untuk mengamankan informasi adalah kriptografi. Kriptografi memiliki tingkat keamanan yang cukup tinggi namun terlalu menarik perhatian pihak – pihak lain seperti penyadap atau peretas dibandingkan dengan steganografi karena yang terlihat oleh pihak lain adalah media penampung yang terkesan tidak bernilai.

II. LANDASAN TEORI

A. Teori Dasar Citra Digital

Pengolahan citra digital menunjuk pada pemrosesan gambar 2 dimensi menggunakan komputer. Dalam konteks yang lebih luas, pengolahan citra digital mengacu pada pemrosesan setiap data 2 dimensi. Citra digital merupakan sebuah larik (array) yang direpresentasikan dengan deretan bit tertentu[1].

Berdasarkan cara penyimpanan atau pembentukannya, citra digital dapat

dibagi menjadi dua jenis. Jenis pertama adalah citra digital yang dibentuk oleh

kumpulan pixel dalam array dua dimensi. Citra jenis ini disebut citra bitmap (bitmap image) atau citra raster (raster image). Jenis citra yang kedua adalah citra yang dibentuk oleh fungsi-fungsi geometri dan matematika. Jenis citra ini disebut grafik vektor (vector graphics). Dalam pembahasan skripsi ini, yang dimaksud citra digital adalah citra image.

Citra digital (diskrit) dihasilkan dari citra analog (kontinu) melalui digitalisasi . Digitalisasi citra analog terdiri atas sampling dan kuantisasi (quantization) Penerokan adalah pembagian citra ke dalam elemenelemen diskrit (pixel).

Berdasarkan warna-warna penyusunnya, citra digital dapat dibagi menjadi tiga macam[2] yaitu:

1) Citra biner, yaitu citra yang hanya terdiri atas dua warna, yaitu hitam dan putih. Oleh karena itu, setiap *pixel* pada citra biner cukup direpresentasikan dengan 1 bit. Citra biner sering kali muncul sebagai hasil dari proses pengolahan seperti segmentasi, pengembangan, morfologi, ataupun *dithering*.
2) Citra *grayscale*, yaitu citra yang nilai *pixel*-nya merepresentasikan derajat keabuan atau intensitas warna putih. Nilai intensitas paling rendah merepresentasikan warna hitam dan nilai intensitas paling tinggi merepresentasikan warna putih. Pada umumnya citra *grayscale* memiliki kedalaman *pixel* 8 bit (256 derajat keabuan), tetapi ada juga citra *grayscale* yang kedalaman *pixel*-nya bukan 8 bit, misalnya 16 bit untuk penggunaan yang memerlukan ketelitian tinggi .
3) Citra berwarna, yaitu citra yang nilai *pixel*-nya merepresentasikan warna tertentu. Banyaknya warna yang mungkin digunakan bergantung kepada kedalaman *pixel* citra yang bersangkutan. Citra berwarna direpresentasikan dalam beberapa kanal (*channel)* yang menyatakan komponen-komponen warna penyusunnya. Banyaknya kanal yang digunakan bergantung pada model warna yang digunakan pada citra tersebut.

B. Steganografi

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi "rahasia" di dalam suatu informasi lainnya[3]. Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi (steganography) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung". Teknik ini meliputi banyak sekali metoda komunikasi untuk menyembunyikan pesan rahasia. Meliputi penggunaan tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Seperti perangkat keamanan lainnya, steganografi dapat digunakan untuk berbagai macam alasan, beberapa diantaranya untuk alasan yang baik, namun dapat juga untuk alasan yang tidak baik. Untuk tujuan legitimasi dapat digunakan pengamanan seperti citra dengan watermarking dengan alasan untuk perlindungan copyright. Digital watermark (yang juga dikenal dengan fingerprinting, yang dikhususkan untuk hal-hal yang menyangkut copyright) sangat mirip dengan Steganography karena menggunakan metode penyembunyian dalam arsip, yang muncul sebagai bagian asli dari arsip tersebut dan tidak mudah dideteksi oleh kebanyakan orang.

C. Metode Least Significant Bit

Penyembunyian data dilakukan dengan mengganti bit-bit data yang tidak terlalu berpengaruh di dalam segmen citra dengan bit-bit data rahasia[3]. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Berikut contoh sebuah susunan bit pada sebuah byte:

MSB = Most Siginificant Bit LSB = Least Significant Bit

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil .

III. METODE PENELITIAN

Tempat penelitian dilakukan dirumah penulis sendiri . Waktu yang dibutuhkan penulis untuk melakukan penelitian dan mengerjakan skripsi adalah 3 bulan.

A. Metode Pengumpulan Data

Studi Literatur : Penulis mengkaji teori dan referensi dari teknik yang penulis gunakan dalam penulisan tugas akhir ini yaitu Steganografi, Algoritma LSB dan referensi tambahan lain . Bahan referensi yang penulis dapatkan yaitu dari beberapa karya ilmiah seperti jurnal, skripsi dan dari buku.

B. Analisis Algoritma Metode LSB

Metode penyisipan LSB (Least Significant Bit) pada media citra digital (foto) adalah dengan mengganti bit terakhir pada foto dengan bit-bit pada teks . Contoh:

Misalkan segmen data citra sebelum perubahan:

00110011 10100010 11100010 10101011
00100110
10010110 11001001 11111001 10001000
10100011

Segmen data citra setelah pesan '1110010111' disembunyikan:

00110011 10100011 11100011 10101010
00100110
10010111 11001000 11111001 10001001
10100011

Contoh lain misalkan karakter "a" yang memiliki bilangan biner "01100001" yang akan disispi ke image dengan ukuran 3 piksel sebagai berikut:

10010010 10100010 10010110
11111001 11001000 11100010
10101010 01010101 00100110

Maka biner yang akan dihasilkan dari proses metode LSB adalah sebagai berikut:

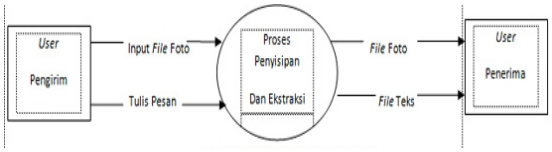
10010010 10100011 10010111

11111000	11001000	11100010
10101010	01010101	00100110

Jadi bit-bit pesan yang disisipi ke bit-bit image (foto) hanya bit ke-8, ke-16, ke-24, dan bit ke-32 (cetak tebal) yang berubah . Sehingga tidak terlihat perubahan signifikan warna foto pada penglihatan mata manusia atau sangat mustahil manusia dapat membedakan warna foto sebelum disisipi teks maupun yang sudah disisipi teks .

C. Data Flow Diagram

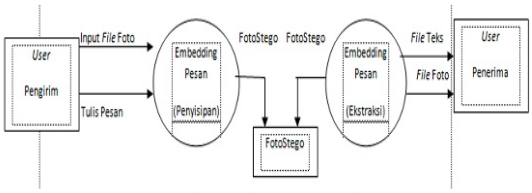
DFD merupakan suatu network yang menggambarkan ssuatu sistem automata, manual atau gabungan yang penggambarannya disusun dalam bentuk kumpulan komponen sistem yang saling berhubungan sesuai dengan aturan mainnya .
DFD (Data Flow Diagram) level 0 cara kerja aplikasi Steganografi adalah sebagai berikut:



Gbr.1 Diagram Level 0

D. Data Flow Diagram (DFD) Level 1

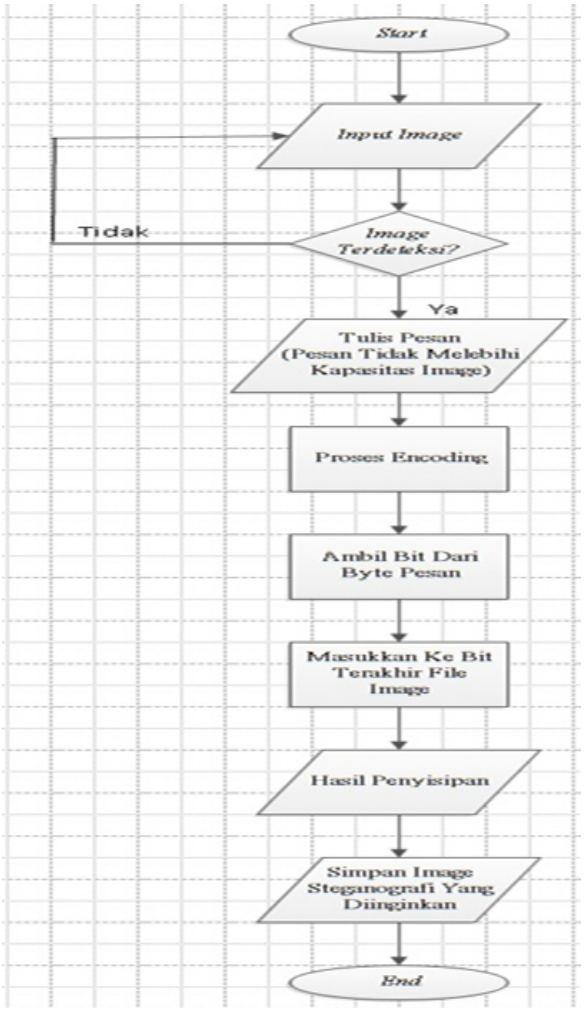
DFD (Data Flow Diagram) level 1 dari pengembangan aplikasi Steganografi adalah sebagai berikut:



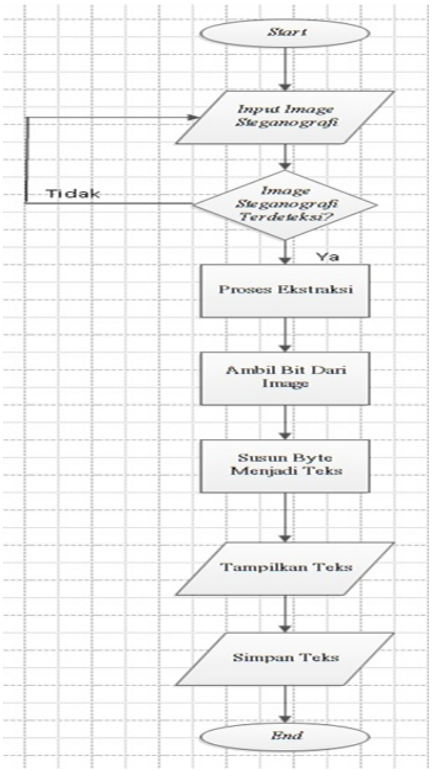
Gbr.2 Diagram Level 1

E. Flowchart

Flowchart atau diagram alir memodelkan alir kerja sebuah proses dan urutan aktivitas dalam suatu proses . Diagram alir ini akan menjelaskan proses dari prosedur yang terjadi pada aplikasi dengan simbol-simbol tertentu . Dengan penggunaan flowchart memungkinkan penggambaran keseluruhan dari pengambilan data awal hingga dihasilkan keluaran (output).



Gbr.3 *Flowchart* Penyisipan



Gbr.4 *Flowchart* Ekstraksi

IV. HASIL DAN PEMBAHASAN

A. Tampilan Aplikasi

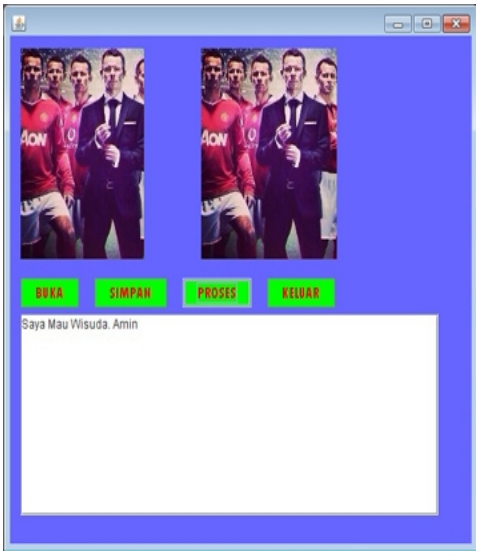
Tampilan program Steganografi yang dibuat penulis terdiri dari beberapa form . Dimana form-form tersebut memiliki tampilan-tampilan yang berbeda sesuai dengan fungsinya .
Berikut tampilan program yang terdiri dari beberapa form:

1) Tampilan Utama
Tampilan utama pada program Steganografi yang penulis buat terdapat tombol petunjuk, tombol tentang, tombol keluar dan 2 buah tombol proses yaitu tombol proses penyisipan dan tombol proses ekstraksi seperti yang akan terlihat pada gambar

Gbr.5 Tampilan Utama Program Steganografi

2) Tampilan Penyisipan Pesan
Untuk memasuki tampilan program Steganografi penyisipan pesan, terlebih dahulu harus mengklik tombol "PENYISIPAN" pada tampilan utama program Steganografi tersebut . Dan untuk melakukan penyisipan pesan (teks) yang ingin disisipkan pengguna harus memiliki foto sebagai media penampung pesan .
Berikut contoh gambar-gambar dari program Steganografi pada tampilan penyisipan pesan .

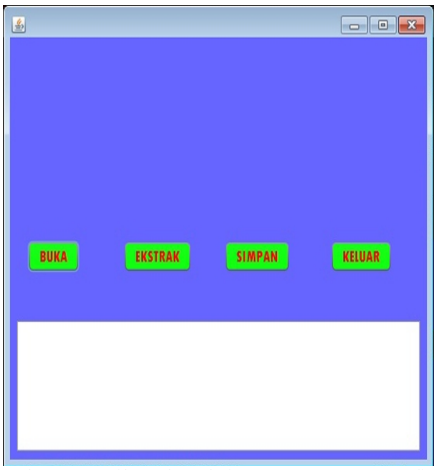
Gbr.6 Tampilan Penyisipan Program Steganografi



Gbr.7 Proses Penyisipan Program Steganografi

Penyisipan pesan telah dilakukan, untuk itu maka foto yang sudah disisipkan pesan tersebut akan disimpan agar dapat dikirim ke pihak atau ke seseorang yang dituju . Adapun cara melakukan penyimpanan foto dengan cara mengklik tombol "SIMPAN".

3) Tampilan Ekstraksi Pesan
Untuk memasuki tampilan program Steganografi ekstraksi pesan, terlebih dahulu harus mengklik tombol "EKSTRAKSI" pada tampilan utama program Steganografi tersebut . Pada proses ekstraksi pesan merupakan kebalikan dari proses penyisipan di mana yang menjadi masukan (*Input*) adalah foto yang telah tersisipi pesan.



Gbr.8 Tampilan Ekstraksi Program Steganografi

Ekstraksi digunakan untuk melakukan pengekstrakan pesan terhadap fotostego (foto yang sudah disisipi pesan) yang sudah disimpan sebelumnya.

Gbr.9 Ekstraksi Pesan Program Steganografi

Fotostego yang sudah diupload maka selanjutnya adalah melakukan ekstraksi dengan cara mengklik tombol "EKSTRAK" maka akan terlihat teks yang tersisipi oleh foto tersebut, seperti pada gambar diatas.

B. Proses Pelaporan Data

Pengujian yang dilakukan setiap pemprosesan pada aplikasi Steganografi yang dibuat oleh penulis dengan menggunakan tabel dalam melakukan pengujiannya adalah sebagai berikut:

1) Data pengujian proses penyisipan

TABEL I
PENGUJIAN PENYISIPAN (NORMAL)

INPUT FILE	PESAN (TEKS)	PEMPROSESAN (PENYISIPAN)	PENGAMATAN	KESIMPULAN
FILE IMAGE (FOTO) .	PESAN (TEKS) YANG INGIN DISISIPI .	JIKA FILE PENAMPUNG TEKS SUDAH DI INPUT DAN TEKSNYA SUDAH DIKETIK, TEKAN TOMBOL PROSES MAKA AKAN TERJADI PENYISIPAN DENGAN METODE LSB .	TOMBOL PROSES UNTUK MENYISIPI PESAN (TEKS) DAPAT BERFUNGSI DAN MENGHASILKAN FILE IMAGE (FOTO) YANG SUDAH DISISIPI PESAN (TEKS) .	DAPAT DIPROSES .

2) Data pengujian proses ekstraksi

TABEL II
PENGUJIAN PROSES EKSTRAKSI

INPUT FILE	PEMPROSEAN (EKSTRAKSI)	PESAN (TEKS)	PENGAMATAN	KESIMPULAN
FILE IMAGE (FOTO) YANG SUDAH DISISIPI PESAN (TEKS) .	JIKA MENEKAN TOMBOL EKSTRAK MAKA FILE PENAMPUNG TEKS AKAN MENGELUARKAN (MENGEKSTRAK) TEKS YANG SUDAH DISISPI.	PESAN (TEKS) YANG SUDAH DIEKSTRAK .	TOMBOL EKSTRAK UNTUK MENGEKSTRAK PESAN (TEKS) DAPAT BERFUNGSI DAN MENGEKSTRAK FILE IMAGE (FOTO) YANG SUDAH DISISPI PESAN (TEKS) .	DAPAT DIPROSES .

3) Data Pengujian Proses Penyisipan Salah (*Error*)

TABEL III
PENGUJIAN PENYISIPAN (ERROR)

INPUT FILE	PESAN (TEKS)	PEMPROSESAN (PENYISIPAN)	PENGAMATAN	KESIMPULAN
FILE IMAGE (FOTO) .	TIDAK ADA PENULISAN PESAN (TEKS) .	JIKA FILE PENAMPUNG TEKS SUDAH DI INPUT DAN TEKS TIDAK DITULIS, TEKAN TOMBOL PROSES MAKA TIDAK AKAN TERJADI PENYISIPAN TEKS (*ERROR*) .	TOMBOL PROSES UNTUK MENYISIPI PESAN (TEKS) TIDAK DAPAT MELAKUKAN PEMPROSESAN PENYISIPAN TEKS .	TIDAK DAPAT DIPROSES (*ERROR*) .
FILE IMAGE (FOTO) TIDAK DI INPUT	PESAN (TEKS) YANG INGIN DISISIPI .	JIKA FILE PENAMPUNG TEKS TIDAK DI INPUT SEDANGKAN TEKS SUDAH DITULIS, TEKAN TOMBOL PROSES MAKA TIDAKA AKAN TERJADI PENYISIPAN TEKS (*ERROR*) .	TOMBOL PROSES UNTUK MENYISIPI PESAN (TEKS) TIDAK DAPAT MELAKUKAN PEMPROSESAN PENYISIPAN TEKS .	TIDAK DAPAT DIPROSES (*ERROR*) .

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari pengujian bab-bab sebelumnya maka penulis dapat memberikan kesimpulan bahwa:

1. Aplikasi Steganografi menggunakan objek image (foto) dapat dikerjakan dengan bahasa pemograman berbasis Java.
2. Aplikasi Steganografi dari hasil implementasi metode LSB dapat digunakan dengan baik dalam melakukan penyembunyian pesan (teks)
3. Aplikasi Steganografi dapat digunakan dengan mudah karena ada tombol-tombol yang mengarahkan baik untuk melakukan penyisipan pesan (teks) maupun ekstraksi pesan .
4. Image (foto) sebagai media penyimpanan pesan tidak merubah foto tersebut secara signifikan atau tidak terlihat secara kasat mata sehingga orang lain tidak menyadari bahwa didalam foto tersebut

5. Aplikasi Steganografi untuk melakukan ekstraksi pesan (teks), pesan yang telah disisipi dan di ekstrak akan memiliki jumlah byte yang sama .
6. Aplikasi Steganografi ini menyadarkan kita bahwa data atau pesan rahasia itu harus benar-benar dijaga kerahasiannya.

B. Saran

1. Aplikasi Steganografi yang telah dibuat oleh penulis media penampung pesannya (teks) hanya file image (foto), diharapkan ada pengembangan media penampungnya yang menggunakan seperti file teks, audio, video dan lain-lain .
2. Aplikasi Steganografi yang telah dibuat oleh penulis hanya dapat digunakan di komputer atau di desktop . Akan lebih canggih lagi apabila dapat digunakan di handphone disemua sistem operasi .
3. Aplikasi Steganografi yang telah dibuat oleh penulis diharapkan digunakan dan dimanfaatkan sebagai keamanan data .
4. Image (foto) yang disisipi pesan (teks) kapasitasnya akan bertambah tersisipi pesan (teks).

REFERENCE

[1] Darma Putra. 2010. Pengolahan Citra Digital. Yogyakarta: Andi Publisher.
[2] Marvin Wijaya. 2007. Pengolahan Gambar Digital. Menggunakan MATLAB. Bandung: Informatika.
[3] Cummins, Jonathan. 2004. Steganography And Digital Watermarking. Birmingham. School of Computer Science, The University of Birmingham.