Penyembunyian Pesan dalam Gambar dengan Teknik Steganografi menggunakan Matlab 7.7.0

Endang Pujiastuti

Abstract*—Steganography technique is the concealment of a secret message by putting the message in a picture in general. The Secret message hidden in the image here is complemented by using steganographic techniques that the author limits to images in the TIFF format. Least Significant Bit (LSB) is one of the methods in steganography that is used for embedded messages. This method performs insertion of binary messages in the binary file of the media used. This method produces images that visually look exactly like the initial image media. In the past, the recovered tattoo was used to convey the contents of steganographic messages, now using computer and network technology, it also develops steganographic techniques. This discussion in computational technology encourages the development of steganography for plumbing in engineering techniques, the message filtering technique in the drawing has become an application of important areas, such as the concealment of copyright notes or serial numbers and also the prevention of direct copying of people which is not eligible.

***Intisari*—Teknik steganografi merupakan penyembunyian suatu pesan rahasia dengan cara menyatukan pesan tersebut dalam suatu gambar secara umum. Pesan Rahasia yang disembunyikan dalam gambar disini dilakukan dengan menggunakan teknik steganografi yang penulis batasi untuk gambar dalam format TIFF. Least Significant Bit (LSB) merupakan salah satu metode dalam Steganografi yang digunakan untuk menyembunyikan pesan. Metode ini melakukan penyisipan binary pesan kedalam binary file media yang digunakan. Metode ini menghasilkan gambar yang secara visual terlihat sama persis dengan media gambar awal. Dahulu, tattoo tersembunyi digunakan untuk menyampaikan isi pesan steganografi, sekarang ini dengan menggunakan teknologi komputer dan jaringan, maka berkembang pula teknik-teknik steganografi. Pertumbuhan akhir-akhir ini dalam teknologi komputasional tersebut mendorong perkembangan steganografi untuk menyembunyikan pesan rahasia diterapkan dalam teknik-teknik keamanan sistem, dimana penyembunyian pesan rahasia dalam gambar telah menjadi suatu aplikasi bidang-bidang yang penting, seperti penyembunyian catatan copyright atau nomor serial dan juga pencegahan pengcopyan secara langsung dari orang-orang yang tidak berhak.**

Kata Kunci— Steganografi, LSB, Penyembunyian Pesan, Gambar.

I. PENDAHULUAN

Penyembunyian pesan rahasia dalam gambar merupakan Salah satu teknik pada pengolahan citra digital yang dikenal dengan istilah Steganografi**,** yaitu teknik penyembunyian pesan rahasia sehingga keberadaan data tersebut tidak diketahui oleh pihak asing. Adapun cara penyembunyian pesan tersebut yaitu dengan menggunakan teknik steganografi.

Data atau informasi tidak hanya disajikan dalam bentuk teks, tetapi juga dapat berupa gambar, audio (bunyi, suara, musik), dan video. Beberapa macam data atau informasi ini sering disebut multimedia. Citra (*Image*) sebagai salah satu komponen multimedia memegang peranan sangat penting sebagai bentuk informasi visual. Dengan menggunakan bahasa pemograman Matlab 7 dimana Matlab merupakan salah satu bahasa pemograman yang dikembangkan oleh MathWorks yang memiliki fungsi dan karakteristik berbeda dengan bahasa pemrograman lain. Matlab merupakan bahasa pemrograman level tinggi yang dikhususkan untuk kebutuhan komputasi teknis, visualisasi dan pemrograman.

Teknologi digital memberikan kontribusi yang besar pada penerapan teknologi steganografi karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan antara lain: bmp, gif, jpeg, file teks, html, pdf, mp3, wav atau voc. contohnya pada file gambar, pesan dapat disembunyikan dengan menyisipkan pada bit rendah di dalam data pixel yang menyusun file gambar.

Adapun tujuan dari penulisan yaitu sebagai pembelajaran dan pengenalan bagaimana cara penyamaran serta penyembunyian pesan ke dalam data citra dengan menggunakan bahasa pemograman tingkat tinggi Matlab 7 serta untuk menjaga kerahasiaan pesan yang disisipkan sehingga tidak mengizinkan orang lain untuk mendeteksi keberadaan pesan rahasia tersebut.

Dalam pembuatan *Aplikasi ini*, penulis membatasi permasalah pada proses bagaimana data citra dan teks diambil dan disajikan untuk proses steganografi dengan teknik LSB (*Least Significant Bit*) dimana proses steganografi ini menyisipkan dan mengungkapkan kembali pesan tersebut dalam citra yang terseleksi dengan menggunakan Matlab 7.

II. KAJIAN LITERATUR

A. *Matlab*

MATLAB (*Matrix Laboratory*) adalah sebuah program untuk analisis dan komputasi numeric, merupakan suatu bahasa pemrograman matematika lanjutan yang dibentuk dengan dasar pemikiran menggunakan sifat dan bentuk matriks[3]. Pada awalnya, program ini merupakan *interface* untuk koleksi rutin-rutin numeric proyek LINKPACK dan EISPACK, dikembangkan menggunakan bahasa FORTRAN. Namun sekarang, program ini merupakan produk komersial dari perusahaan Mathwork, Inc. yang dalam perkembangan selanjutnya dikembangkan

[1] *Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta, Jl. Damai No.8 Warung JAti Barat (Margasatwa) Jakarta Selatan 12510 INDONESIA (tlp: 021-78839513; fax: 021-78839421; e-mail: endangpuji20@gmail.com)*

menggunakan bahasa C++ dan assembler (terutama fungsi-fungsi dasar MATLAB). Selain itu, MATLAB merupakan bahasa pemrograman tingkat tinggi berbasis pada matriks sering digunakan untuk teknik komputasi numeric, digunakan untuk menyelesaikan masalah-masalah yang melibatkan operasi matematika elemen,matrik, optimasi, aproksimasi, dan lain-lain. MATLAB banyak juga digunakan pada :

a. Matematika dan Komputasi,
b. Pengembangan Algoritma,
c. Pemrograman modeling, simulasi dan pembuatan prototype,
d. Analisis data, eksplorasi, dan visualisasi,
e. Analisis numeric dan statistic,
f. Pengembangan aplikasi teknik.

B. *Steganografi*

Steganografi adalah seni atau ilmu untuk menyamarkan sebuah pesan/data rahasia di dalam data atau media yang tampaknya biasa saja, sehingga keberadaan pesan rahasia itu sulit diketahui [1]. Steganografi adalah seni menyamarkan data. Jika kriptografi adalah ilmu yang menjaga isi data atau pesan agar tetap aman dengan cara menyandikan isi pesan, maka steganografi lebih berfokus agar keberadaan pesan rahasia tersamar.

C. Teknik *Steganografi*

Untuk memperkuat penyembunyian data, bit-bit data tidak digunakan untuk mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Bilangan acak dibangkitkan dengan *pseudo-random-number-generator* (PNRG). PNRG menggunakan kunci rahasia untuk membangkitkan posisi pixel yang akan digunakan untuk menyembunyikan bit-bit. PNRG dibagun dalam sejumlah cara, salah satunya dengan menggunakan algoritma kriptografi DES (*Data Encription Standart*), algoritma *hash* MD5, dan metode kriptografi CFB (*Chiper-Feedback Mode*). Tujuan dari ekripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi

D. Kriteria Steganografi yang baik

Seperti yang sudah disebutkan pada bagian awal bab, data yang disembunyikan tidak hanya berupa teks, tetapi juga berupa citra, audio, atau video. Selain citra digital, media penampung data rahasia juga bisa berupa teks, audio, atau video.

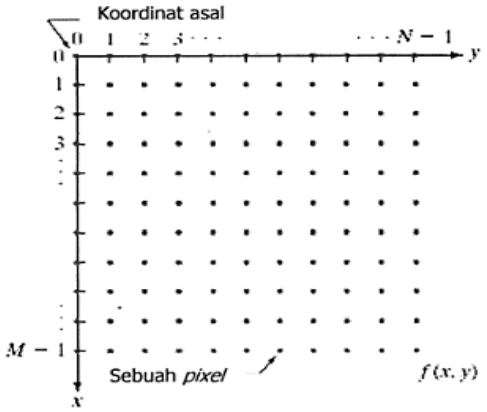
Penyembuyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. *Fidelity.* Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui jika di dalam citra tersebut terdapat data rahasia.
2. *Robustness.* Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi menipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, pembesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya. Bila pada citra penampung dilakukan operasi-operasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak.

Recovery. Data yang disembunyikan harus diungkapkan kembali (*Reveal*). Karena tujuan dari steganografi adalah penyembunyian data, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk dapat digunakan lebih lanjut.

E. *Citra Digital*

Suatu citra dapat di definisikan sebagai fungsi f(x,y)berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial, dan amplitude f di titik koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut [4]. Apabila nilai x, y, dan nilai amplitude f secara keseluruhan berhingga (finite) dan bernilai diskrit maka dapat dikatakan bahwa citra tersebut adalah citra digital.



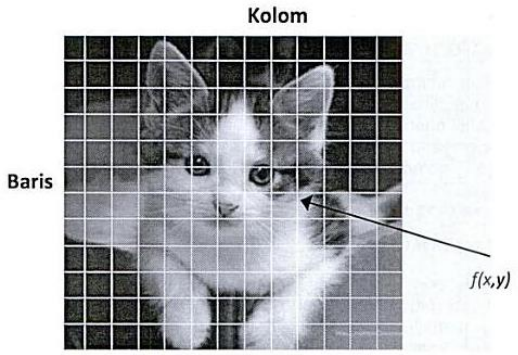
Sumber : [4]

Gbr. 1 Koordinat citra digital

Berikut merupakan citra digital dalam bentuk matrik:

$$f(x,y)=\begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix} \quad \text{..... (2.1)}$$

Nilai pada suatu irisan antara baris dan kolom (pada bposisi x,y) disebut dengan *picture elements, image elements, pels,* atau pixels. Istilah terakhir (pixel) paling sering digunakan pada citra digital. Berikut ilustrasi digitalisasi citra dengan M=16 baris dan N=16 kolom.



Gbr. 2 Ilustrasi digitalisasi citra (pixel pada koordinat x = 10, y = 3 memiliki nilai 110)

Secara harafiah, citra (*image*) adalah gambar pada bidang dwimatra (dua dimensi). ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. pantulan cahaya ini ditangkap oleh alat-alat optik, Seperti mata pada manusia, kamera, pemindai (*scanner*), dan sebagainya sehingga bayangan objek yang disebut citra tersebut terekam.

Citra yang dimaksudkan dalam keseluruhan penulisan ini adalah citra diam (*still images*). Citra diam adalah citra tunggal yang tidak bergerak sedangkan citra bergerak (*moving images*) adalah rangkaian citra diam yang ditampilkan secara beruntun (*sequensial*) sehingga memberi kesan pada mata sebagai gambar-gambar yang bergerak.

Meskipun sebuah citra kaya informasi, namun seringkali citra yang dimiliki mengalami penurunan mutu (degradasi), misalnya mengandung cacat atau derau (*noise*), warnanya terlalu kontras, kurang tajam, kabur (*blurring*), dan sebagainya. maka tentu saja citra semacam ini menjadi lebih sulit diinterpretasikan karena informasi yang disampaikan oleh citra tersebut menjadi berkurang. Agar citra yang mengalami gangguan tersebut mudah diinterpretasikan (baik oleh manusia maupun mesin), maka citra tersebut perlu dimanipulasi menjadi citra lain yang kualitasnya lebih baik. Bidang studi yang menyangkut hal ini adalah Pengolahan Citra (*Image Processing*)

III. METODE PENELITIAN

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. Dengan demikian pada setiap pixel file bitmap 24 bit kita dapat menyisipkan 3 bit data.

Contoh 8 bit pixel:

1 pixel : (00 01 10 11)
white red green blue

Insert 0011 : (00 **00** **11** 11)
white white blue blue

Contoh 24 bit pixel :
Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut :

(00100111 11101001 11001000)
red blue green

(00100111 11001000 11101001)
red green blue

(11001000 00100111 11101001)
green red blue

Sedangkan representasi biner huruf A adalah 100000111. Dengan menyisipkan-nya pada data pixel diatas maka akan dihasilkan:

(00100111 **11101000** 11001000)
red green blue

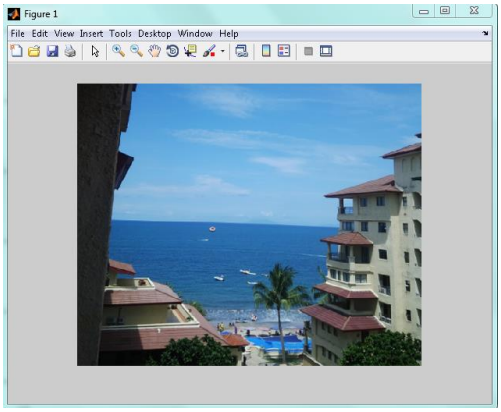
(**00100110** 11001000 **11101000**)
white green green

(**11001001** 00100111 11101001)
blue red blue

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metode ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga.

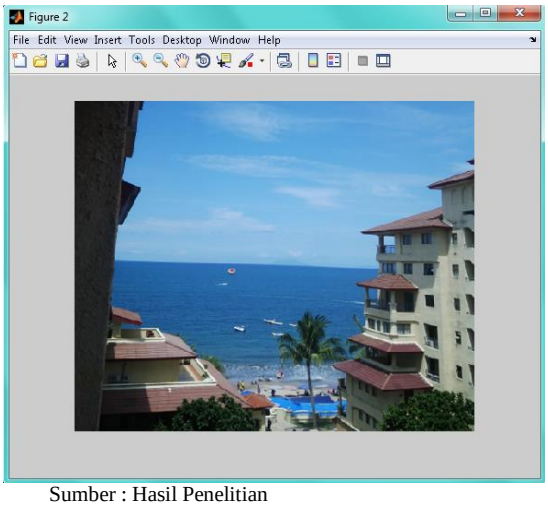
IV. HASIL DAN PEMBAHASAN

Contoh kasus pada gambar citra asli gambar1.tif dengan ukuran 500 x 410 Pixel yang disisipi pesan rahasia yaitu "P" maka hasilnya adalah sebagai berikut.



Sumber : Hasil Penelitian

Gbr. 3 Hasil sebelum penyisipan



Sumber : Hasil Penelitian

Gbr. 4 Hasil setelah penyisipan

TABEL I
KETERANGAN PROSES PENYISIPAN HURUF 'P'

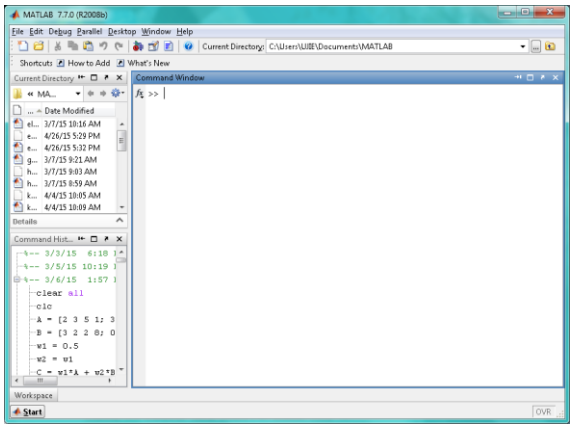
Pixel	Gambar Asli RGB (red)	Raster data	Bit rendah	Bit pesan (huruf 'P')	Hasil	Gambar Stego RGB (red)
[1,1]	46	00101110	0	**0**	00101110	**46**
[2,1]	39	00100111	1	**1**	00100111	**39**
[3,1]	36	00100100	0	**0**	00100100	**36**
[4,1]	29	00011101	1	**1**	00011101	**29**
[5,1]	21	00010101	1	**0**	00010100	**20**
[6,1]	30	00011110	0	**0**	00011110	**30**
[7,1]	46	00101110	0	**0**	00101110	**46**
[8,1]	47	00101111	1	**0**	00101110	**46**

Sumber : Hasil Penelitian

Pada contoh kasus di atas setiap byte di dalam data bitmap diganti satu bit LSB-nya dengan bit data huruf 'P' yang akan disembunyikan. Jika byte tersebut merupakan komponen pembentuk warna hijau, maka penggantian 1 bit LSB-nya hanya mengubah sedikit tingkat kecerahan warna hijau, dan perubahan warna yang terjadi pada pixel 5.1, dan 8.1 tidak terdeteksi oleh mata manusia.

Window pada Matlab 7.0 terdiri dari Current Directory, Command History, Command Window, Workspace. Penjelasannya adalah sebagai berikut :

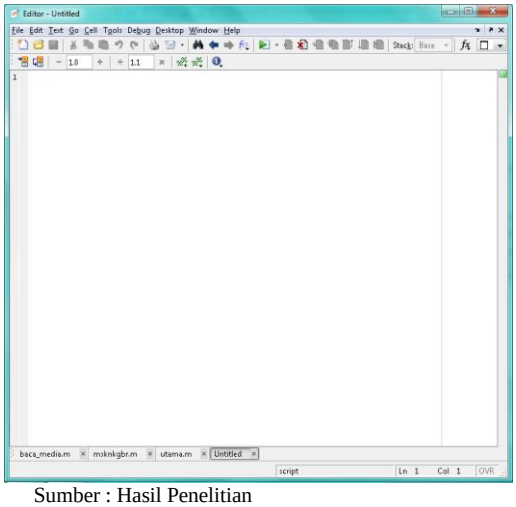
1. Current Directory.
   Window ini menampilkan isi dari direktori kerja saat menggunakan matlab. Kita dapat mengganti direktori ini sesuai dengan tempat direktori kerja yang diinginkan. Default dari alamat direktori berada dalam folder works tempat program files Matlab berada.
2. Command History.
   Window ini berfungsi untuk menyimpan perintah-perintah apa saja yang sebelumnya dilakukan oleh pengguna terhadap Matlab.
3. Command Window.
   Window ini adalah window utama dari Matlab. Disini adalah tempat untuk menjalankan fungsi, mendeklarasikan variabel, menjalankan proses-proses, serta melihat isi variabel.
4. Workspace.
   Workspace berfungsi untuk menampilkan seluruh variabel-variabel yang sedang aktif pada saat pemakaian matlab. Apabila variabel berupa data matriks berukuran besar maka user dapat melihat isi dari seluruh data dengan melakukan double klik pada variabel tersebut. Matlab secara otomatis akan menampilkan window "array editor" yang berisikan data pada setiap variabel yang dipilih user.



Sumber : Hasil Penelitian

Gbr. 5 Tampilan Antar Muka Dari Matlab Versi 7.0

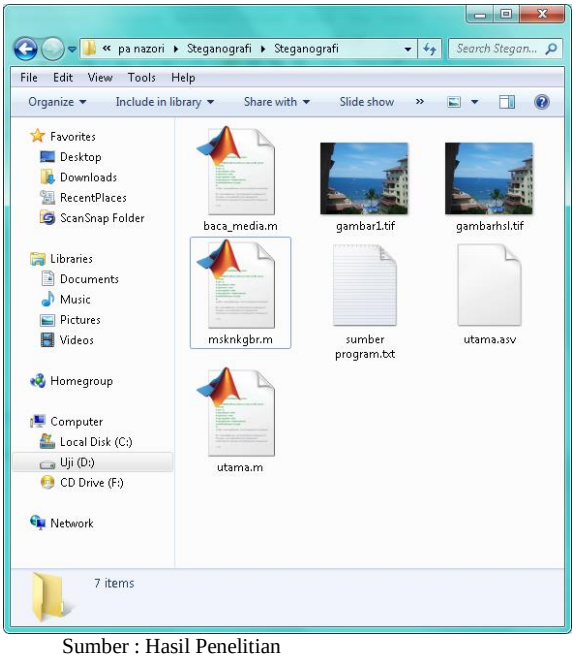
Di dalam matlab, kita dapat menyimpan semua script yang akan digunakan dalam file pada matlab dengan ekstensi .M. M-File dapat dipanggil dengan memilih menu file->new->M-File. Di dalam M-File, kita dapat menyimpan semua perintah dan menjalankan dengan menekan tombol atau mengetikan nama M-File yang kita buat pada command window.



Sumber : Hasil Penelitian

Gbr. 6 M-File Workspace.

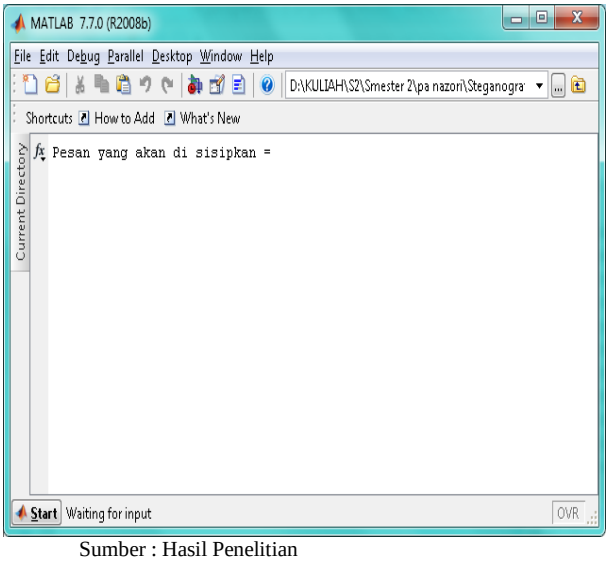
Lokasi penyimpanan gambar yang dimasukan kedalam script di simpan di dalam satu folder yang sama. Pada script penyembunyian pesan dalam gambar format gambar berupa TIFF.



Sumber : Hasil Penelitian

Gbr. 7 Penyimpanan File MATLAB

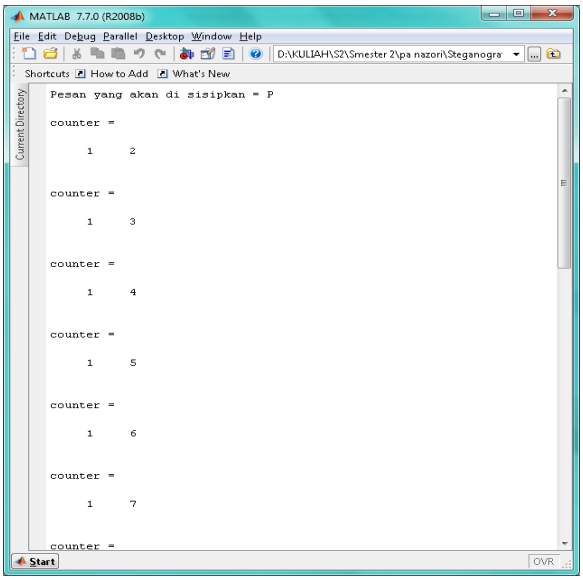
Pada saat compile program jalankan melalui file utama, setelah program berhasil dijalankan maka tampil dialog "Pesan yang akan disisipkan" seperti pada gambar dibawah ini:



Sumber : Hasil Penelitian

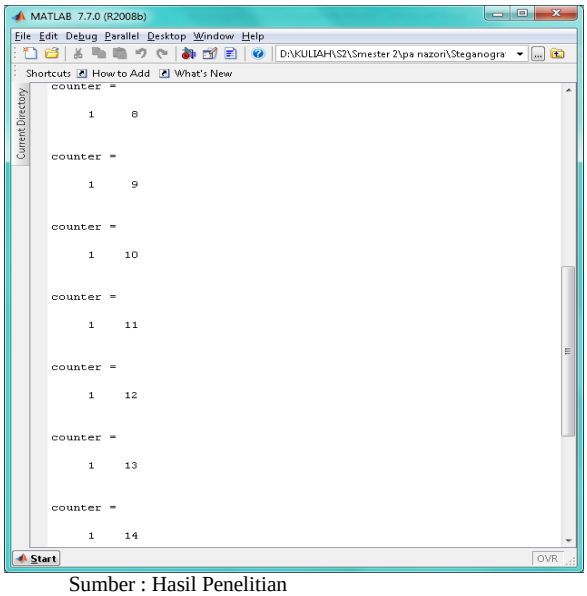
Gbr. 8 Hasil sebelum dan setelah penyisipan

Seperti pesan yang sudah dicontohkan sebelumnya, pesan yang akan disisipkan adalah huruf "P".



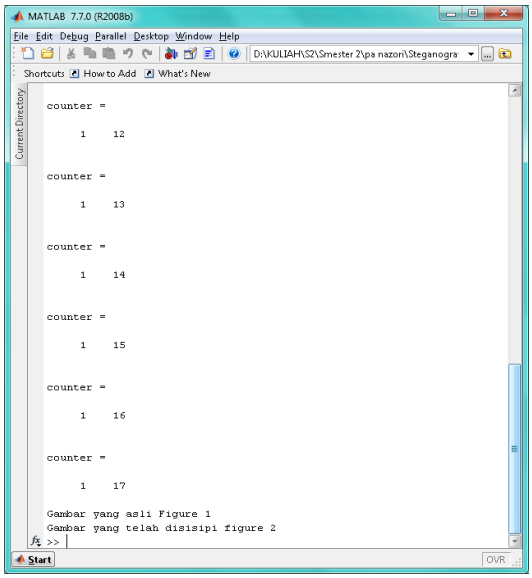
Sumber : Hasil Penelitian

Gbr. 9 Hasil setelah penyisipan pesan



Sumber : Hasil Penelitian

Gbr. 10 Hasil setelah penyisipan pesan



Sumber : Hasil Penelitian

Gbr. 11 Hasil setelah penyisipan pesan

Gambar asli sebelum disisipi pesan rahasia adalah figure 1, sedangkan figure 2 adalah contoh gambar yang telah disisipi pesan rahasia.

Sumber : Hasil Penelitian

Gbr. 12 Hasil figure 1

Sumber : Hasil Penelitian

Gbr. 13 Hasil figure 2

V. KESIMPULAN

Pesan berhasil disisipkan kedalam media gambar dengan menggunakan *software* MATLAB versi 7. Perubahan warna yang dialami citra tidak terlihat jelas, sangat berguna dalam menjaga kerahasiaan data sehingga tidak banyak orang yang menyadarinya. Citra yang digunakan penulis dengan ukuran 500 x 410 pixel.

Jika proses penyisipan pesan menggunakan 3 komponen warna (R, G, B) akan menambah daya tampung pesan sebanyak 3 kali lipat. Penyisipan ini masih menggunakan 1 komponen warna. Semakin banyak pesan rahasia yang digunakan mengakibatkan lamanya proses penyisipan dan ekstraksi.

Jika menggunakan format lain, maka pesan yang tersembunyi akan hancur. Jadi citra stego ini hanya bisa menggunakan tiff, maka metode steganosistem yang digunakan harus bebas dari karakteristik kompresi. Metode yang digunakan sederhana namun jika terjadi kompresi pada citra stegano maka pesan rahasia akan hancur, metode MSB (Most Significant Bit) dapat digunakan sehingga pixel-pixel yang mengalami kompresi hanya pixel dengan bit yang kurang.

UCAPAN TERIMA KASIH

Terimakasih kepada Tim JTI yang yang telah meluangkan waktu untuk membuat template ini, sehingga penulis dapat dengan mudah menulis sesuai dengan informasi dan arahan yang tertuang pada template Jurnal Teknik Informatika. Selain itu, penulis juga mengucapkan terimakasih atas kesempatannya untuk dapat publikasi pada Jurnal Teknik Informatika ini.

REFERENSI

[1] Arryawan, Eko dan Community, Smitdev. Mengatasi Investigasi Komputer Forensik. Jakarta: Elex Media Komputindo. 2010.
[2] Prasetyo, Fahri Perdana. Steganografi Menggunakan Metode LSB dengan menggunakan MATLAB. Jakarta. 2010.
[3] Pusadan, Mohammad Yazdi. Pemrograman MATLAB pada Sistem Pakar Fuzzy. Yogyakarta: Deepublish. 2014.
[4] Putra, Darma. Pengolahan Citra Digital. Yogyakarta: Andi Offset. 2010.
[5] Setiani, Yeni. Pembuatan aplikasi steganografi menggunakan matlab 7. Jakarta: Gunadarma. 2008.

Endang Pujiastuti. Jakarta, 05 Januari 1990. Lulus dari Program Diploma Tiga (D.III) Program Studi Komputerisasi Akuntansi AMIK BSI Jakarta Tahun 2012, Lulus dari Program Strata Satu (S1) Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta Tahun 2014, Lulus dari Program Strata Dua (S2) Program Studi Magister Ilmu Komputer Universitas Budi Luhur Tahun 2016. Bekerja pada Yayasan Indonesia Nusa Mandiri, sebagai Tenaga Pengajar sejak tahun 2015. Publikasi Paper Jurnal pada Tahun 2015 di IJSE dengan judul "Prototipe Peningkatan Pelayanan Rawat Jalan dengan Pengujian FGD dan ISO 9126 pada Klinik Eka Anugerah", Publikasi Paper Jurnal pada Tahun 2016 di IJSE dengan judul "Perancangan Aplikasi Mobile Berbasis Android untuk Pemeliharaan Mesin Produksi pada PT. Temprint".