PEMBUKTIAN KEPEMILIKAN CITRA DIGITAL DENGAN TEKNIK STEGANOGRAFI MENGGUNAKAN MATLAB

Veronica Lusiana
Dosen Fakultas Teknik Universitas Stikubank Semarang

DINAMIKA TEKNIK
Vol. II, No. 2
Juli 2008
150 – 160

Abstract

Steganography is the art of hiding information in ways that prevent the detection of hiding messages. Digital technology gives us new ways to apply steganographic techniques, including hiding information in digital images. Steganography encompasses methods of transmitting secret messages through innocuous cover carries in such a manner that the very existence of the embedded messages is undetectable. The purpose of steganography is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed. Digital watermarking is described as a possibility to interface and close the gap between copyright and digital distribution. It is based on steganographic techniques and enables useful rights protection mechanisms.

Keyword: Steganography, Watermarking, Hiding Messages

PENDAHULUAN

Internet merupakan salah satu aplikasi dari jaringan komputer yang telah mengalami perkembangan sangat cepat, dimana pertukaran bentuk informasi dapat berupa data teks, gambar atau citra, gambar bergerak dan suara. Seiring dengan perkembangan tersebut, secara langsung ikut mempengaruhi cara kita berkomunikasi. Dahulu untuk berkomunikasi menggunakan surat yang dikirim melalui kantor pos, sekarang telah banyak layanan surat elektronik (*e-mail)* di Internet yang dapat mengirimkan pesan secara lebih cepat. Tetapi sebagai suatu jaringan publik, Internet rawan terhadap pencurian data.

Steganografi (*steganography*) adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang. Aplikasi yang banyak diapakai dari teknik steganografi adalah digunakan sebagai alat pembuktian kepemilikan data oleh seseorang. Data rahasia yang disembunyikan adalah berukuran relatif kecil apabila dibandingkan dengan data

yang disisipinya, sehingga data yang disembunyikan ini dapat digunakan sebagai penanda siapa pemilik yang sah dari data yang telah disisipi atau ditambah. Oleh karena itu steganografi dapat dimanfaatkan pada saat mengirim data melalui jaringan Internet.

DASAR TEORI

Sejarah steganografi

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". Catatan pertama tentang steganografi ditulis oleh seorang sejarawan Yunani bernama Herodotus, yaitu ketika Histaeus seorang raja kejam Yunani dipenjarakan oleh Raja Darius di Susa pada abad ke 5 SM. Histaeus harus mengirim pesan rahasia kepada anak laki-lakinya Aristagoras di Militus. Histaeus menulis pesan dengan cara mentato pesan pada kulit kepala seorang budak dan ketika rambut budak itu mulai tumbuh, Histaeus mengutus budak itu ke Militus untuk mengirim pesan di kulit kepalanya tersebut kepada Aristagoras.

Cerita lain tentang steganografi datang juga dari sejarawan Yunani Herodotus, yaitu dengan cara menulis pesan pada papan kayu yang ditutup dengan lilin. Demeratus, seorang Yunani yang akan mengabarkan berita kepada Sparta bahwa Xerxes bermaksud menyerbu Yunani. Agar tidak diketahui pihak Xerxes, Demaratus menulis pesan dengan cara mengisi tabung kayu dengan lilin dan menulis pesan dengan cara mengukirnya pada bagian bawah kayu, lalu papan kayu tersebut dimasukkan ke dalam tabung kayu, kemudian tabung kayu ditutup kembali dengan lilin. Selain bangsa Yunani, bangsa Romawi kuno juga telah mengenal steganografi yaitu menggunakan tinta yang tidak terlihat, yang ditulis menggunakan air sari buah jeruk, urine atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas nyala lilin, tinta yang sebelumnya tidak terlihat ketika terkena panas akan berangsur-angsur menjadi gelap sehingga pesan dapat dibaca.

Pada abad 20, steganografi benar-benar mengalami perkembangan. Selama berlangsung perang Boer, Lord Boden Powell (pendiri gerakan kepanduan) yang bertugas untuk membuat tanda posisi sasaran dari basis artileri tentara Boer, untuk alasan keamanan, Boden Powell menggambar peta-peta posisi musuh pada sayap kupu-kupu agar gambar-gambar peta sasaran tersebut terkamuflase. Perang Dunia II adalah periode pengembangan teknik-teknik baru steganografi. Pada awal Perang Dunia II walaupun masih digunakan teknik tinta yang tak terlihat, namun teknik-teknik baru mulai dikembangkan seperti menulis pesan rahasia ke dalam kalimat lain yang tidak berhubungan langsung dengan isi pesan rahasia tersebut, kemudian teknik menulis pesan rahasia ke dalam pita koreksi karbon mesin ketik, dan juga teknik menggunakan pin berlubang untuk menandai kalimat terpilih yang digunakan dalam pesan, teknik terakhir adalah microdots yang dikembangkan oleh tentara Jerman pada akhir Perang Dunia II.

Dari contoh-contoh steganografi konvensional tersebut dapat dilihat bahwa semua teknik

steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasian komunikasinya bukan pada datannya. Seiring dengan perkembangan teknologi terutama teknologi komputasi, steganografi merambah juga ke media digital.

Pengertian Steganografi

Teknik menyembunyikan data rahasia di dalam media digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain.

1. Seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut.

2. *Stegranography* merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi "rahasia" di dalam suatu informasi lainnya

Steganografi memerlukan dua property yaitu wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan wadah penampung citra, audio, teks dan video. Sedangkan data rahasia yang disembunyikan dapat berupa citra, suara, teks atau video. Kriteria steganografi yang baik memiliki beberapa parameter berikut ini :

1. Fidelity

Mutu citra penampung tidak jauh berubah. Artinya setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik, tetapi pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia yang disembunyikan.

2. Robustness

Data yang disembunyikan harus tahan terhadap berbagai operasi manipulasi(pengubahan kontras, penajaman, rotasi, pembesaran dsb) yang dilakukan pada ctra penampung.Data yang disembunyikan tetap valid atau tidak rusak setelah dilakukan operasi manipulasi tersebut.

3. Recovery

Data yang disembunyikan harus dapat diungkap kembali, karena tujuan steganografi adalah data hiding, jika sewaktu-waktu data rahasia di dalam citra penampung harus daapt diambil kembali untuk digunakan lebih lanjut.

4. Security

Data yang disembunyikan harus tahan terhadap usaha memindahkan dari satu multimedia data ke multimedia lainnya.

IMPLEMENTASI

Untuk implementasi ,penulis membuat sebuah program menggunakan Matlab yaitu wm02.m yang berfungsi untuk menyisipkan citra kecil ke dalam sebuah citra yang berukuran lebih besar. Dalam program ini citra disisipkan secara rahasia,

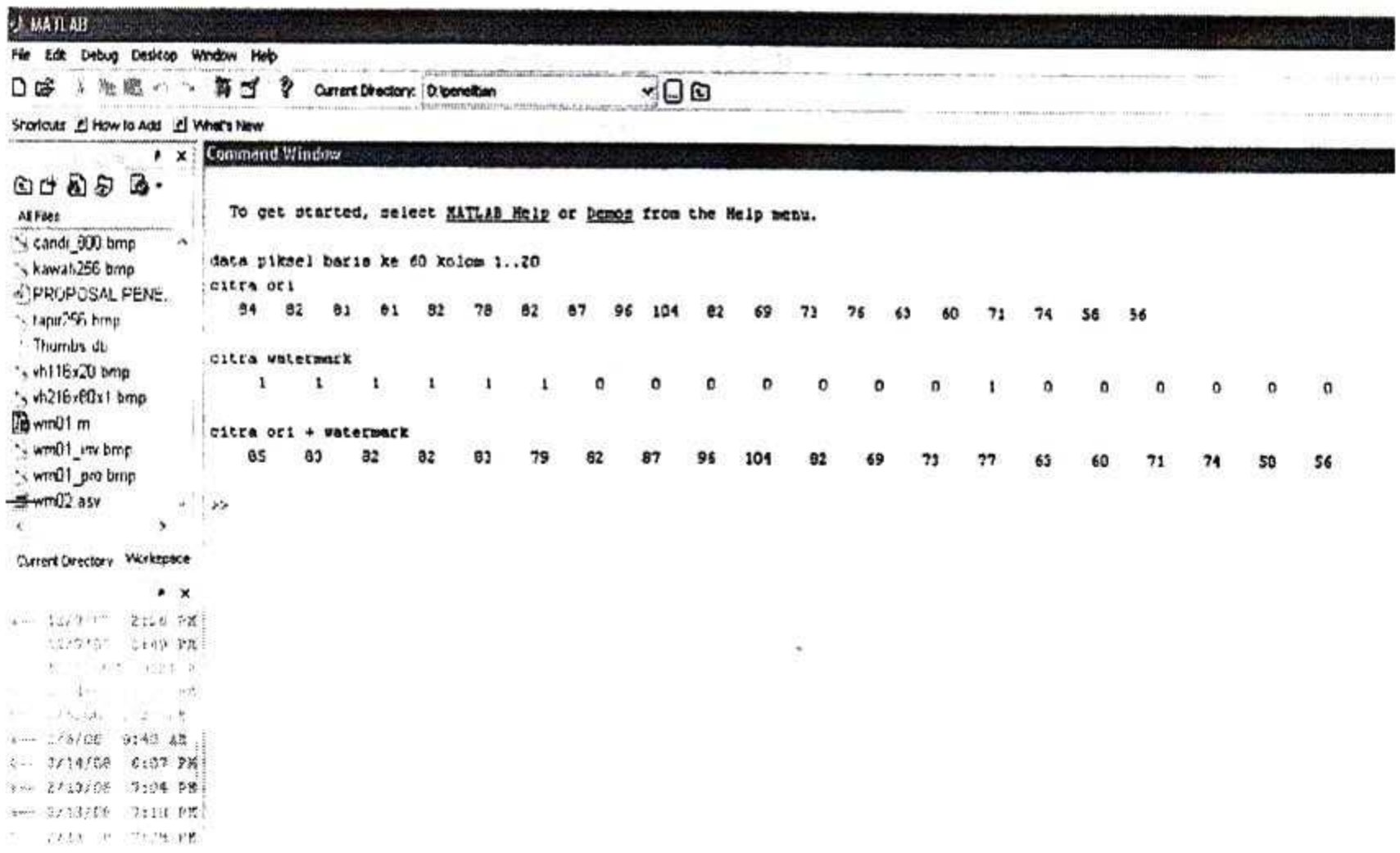
dengan tingkat ketersembunyiannya dapat diatur prosentasenya. Kedalaman warna citra yang akan disisipi adalah 24 bit RGB, dengan citra watermark yang disisipkan memilki kedalaman 1 bit (citra biner). Ukuran citra yang akan disisipi adalah 256 x 256 piksel dan ukuran citra watermark 216 x 80 piksel. Pada penelitian ini ukuran citra watermark dibuat cukup besar dengan tujuan agar dapat diamati proses penyembunyiannya. Di dalam aplikasi citra watermark berukuran lebih kecil. Untuk keperluan pengaturan tingkat ketersembunyian citra watermark terhadap citra data dapat dilakukan dengan mengubah nilai *ampilified* mulai dari 0 sampai dengan 100. Nilai amplified = 0 adalah citra watermark tidak terlihat oleh mata manusia, tetapi bisa dideteksi oleh program. Sebaliknya untuk amplified = 100 citra watermark akan terlihat secara jelas.

Sedangkan fungsi-fungsi Matlab yang dipergunakan adalah :

1. Imread ( ) : sebuah fungsi yang digunakan untuk membaca sebuah file citra
2. Imshow( ) : sebuah fungsi yang digunakan untuk menampilkan citra
3. Subplot ( ) : sebuah fungsi yang digunakan untuk mengatur tampilan citra
4. Disp ( ): sebuah fungsi yang digunakan untuk menampilkan string

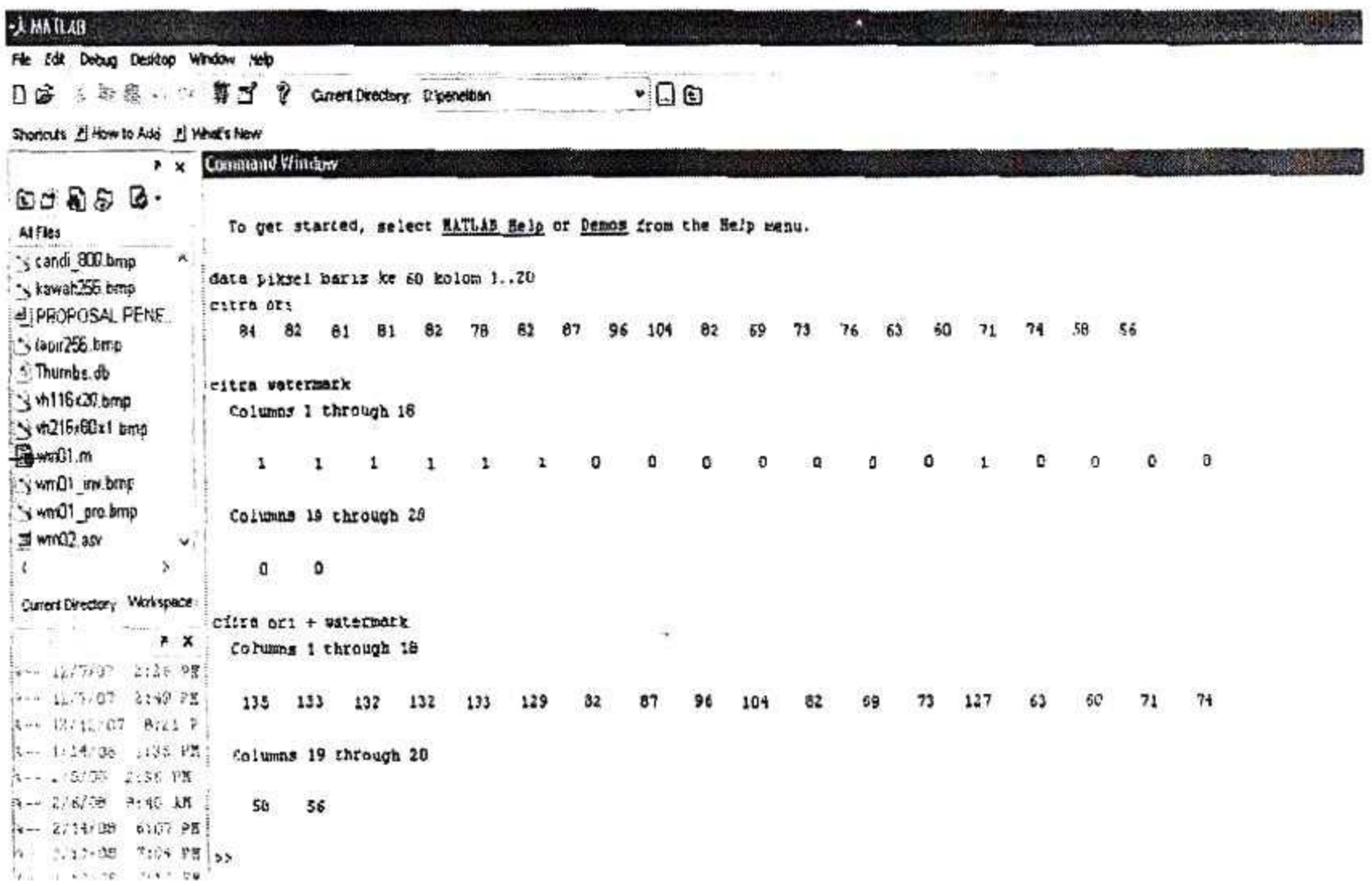
```
1. amplified=0; %memperkuat citra watermark
```

VEROHARTONO



amplified=50; %memperkuat citra watermark

VEROHARTONO



Listing program

```
function wm02
% kedalaman warna citra: original 24 bit, watermark 1 bit
% ukuran citra: original 256x256 piksel, watermark 216x80 piksel
% membaca citra original
rgb_line=3;  %memilih komponen yang akan ditambahkan citra watermark
amplified=50; %memperkuat citra watermark
file_ori=imread('d:\penelitian\candi_800.bmp');
file_pro=file_ori;
file_inv=file_ori;
sizefile_ori=size(file_ori);
sizefile_pro=sizefile_ori;
baris_ori=sizefile_ori(1,1); kolom_ori=sizefile_ori(1,2);
ori=zeros(sizefile_ori);
%menduplikasi data citra original ke variabel ori dan pro
for i=1:baris_ori;
  for j=1:kolom_ori;
    for k=1:3;
      ori(i,j,k)=file_ori(i,j,k);
    end
  end
end
pro=ori;
inv_ori;
% membaca citra watermark
file_wm=imread('d:\penelitian\vh216x80x1.bmp');
sizefile_wm=size(file_wm);
baris_wm=sizefile_wm(1,1); kolom_wm=sizefile_wm(1,2);
wm=zeros(sizefile_wm);
%menduplikasi data citra original ke variabel wm
for i=1:baris_wm;
```

```
  for j=1:kolom_wm;
      wm(i,j)=file_wm(i,j);
    end
end
% memproses citra original + citra watermark (pada salah satu komponen R/G/B)
% file_pro = (citra ori + citra watermark)
for i=1:baris_ori;
   for j=1:kolom_ori;
      if ((i<=baris_wm)&(j<=kolom_wm))
         if (wm(i,j)~=0)
            wm(i,j) = wm(i,j) + amplified;
         end
         pro(i,j,rgb_line)=ori(i,j,rgb_line) + wm(i,j);
         file_pro(i,j,rgb_line)=pro(i,j,rgb_line);
      end
   end
end
% proses invers (menampilkan kembali citra ori dengan mengeluarkan citra
watermark)
% file_inv = (citra ori + citra watermark) - citra watermark
for i=1:baris_ori;
   for j=1:kolom_ori;
      if ((i<=baris_wm)&(j<=kolom_wm))
         inv(i,j,rgb_line)=pro(i,j,rgb_line) - wm(i,j);
         file_inv(i,j,rgb_line) = inv(i,j,rgb_line);
      end
   end
end
%menampilkan citra: original, watermark, hasil proses watermarking, dan invers
imwrite(file_pro,'wm01_pro.bmp');
```

```
imwrite(file_inv,'wm01_inv.bmp');
file_wm01_pro=imread('d:\penelitian\wm01_pro.bmp');
file_wm01_inv=imread('d:\penelitian\wm01_inv.bmp');
subplot (1,4,1),imshow(file_ori);
subplot (1,4,2),imshow(file_wm);
subplot (1,4,3),imshow(file_wm01_pro);
subplot (1,4,4),imshow(file_wm01_inv);
%melihat data citra, untuk proses checking,
%contoh untuk data citra pada baris ke 60 kolom ke 1..20
%komponen yang dipilih untuk ditambahkan citra watermark sesuai dengan
pilih_rgb
for j=1:20;
   a(1,j)= file_ori(60,j,rgb_line);
   b(1,j)=file_wm(60,j);
   c(1,j)=pro(60,j,rgb_line);
end
disp('data piksel baris ke 60 kolom 1..20');
disp('citra ori'); disp(a);
disp('citra watermark'); disp(b);
disp('citra ori + watermark'); disp(c);
```

KESIMPULAN

1. Teknik steganografi dapat digunakan untuk pembuktian kepemilikan citra digital.
2. Citra watermark yang disisipkan menggunakan citra biner, sehingga citra yang dihasilkan citra watermarknya tidak terlihat dengan mata.
3. Program wm02.m dapat dipergunakan untuk mengiplementasikan teknik steganograpy dengan cara menyisipkan citra watermark ke citra data.

DAFTAR PUSTAKA

1. Andino Masaleno,Pengantar Steganografi, Kuliah Umum Ilmu computer.com, 2003-2006
2. Aris Sugiarto, Pemrograman GUI Dengan Matlab, Andi Yogyakarta, 2006.
3. Donovan Artz,Digital Steganography, Hiding data within data,los Alamos national laboratory,IEEE internet computing 1089-7801/01/2001, may.june 2001,http://computer.org/internet/may.june 2001.
4. Frank Hartung, Student member IEEE, and Martin Kutter, Multimedia Watermarking Techniques,Proceeding of the IEEE, vol 87 No 7, July 1999.
5. Rohit Agaewalla,Shradha ,Steganography Exploring the unseen.
6. Rinaldi Munir, Pengolahan Citra Digital dengan pendekatan algoritmik,Penerbit Informatika Bandung, 2004.