Kajian Penyimpanan Data Pada Media Citra (*Steganografi*) Menggunakan Metode DCT (*Discrete Cosine Transform)*

Sri Murwantini
(Dosen Prodi Pendidikan Teknik Mesin FKIP UNPAR)

Abstrak*:* Steganografi merupakan teknik menyembunyikan informasi digital dibalik informasi digital lainnya sehingga informasi digital yang sesungguhnya tidak kelihatan. Metode steganografi yang digunakan adalah DCT (*Discrete Cosine Transform*) untuk menyisipkan pesan rahasia. Citra yang telah disisipi pesan disebut citra stego. Pengolahan citra berupa kompresi pada citra stego untuk menguji ketahanannya.Penggunaan steganografi dengan metode DCT mempunyai keuntungan yaitu dapat menggunakan citra terkompresi JPEG. Citra yang telah dinormalisasi menjadi 256x256 piksel dipilih sebagai medium stego. Kemudian setelah disisipi pesan ditentukan nilai D (distance) yaitu perbedaan nilai koefisien dari 2 lokasi piksel yang dipilih untuk penyisipan. Setelah itu pesan rahasia kembali disisipkan pada medium stego yang tidak dinormalisasi dengan nilai D yang telah ditentukan kemudian dilakukan ekstraksi pesan dan dilakukan kompresi.Teknik steganografi dengan Metode DCT menghasilkan citra stego dalam ukuran kecil, mempunyai tingkat kesamaan yang tinggi dengan citra aslinya, selain itu pesan yang disembunyikan dalam citra stego tidak mudah terdeteksi. Nilai D paling baik yang dihasilkan pada penelitian ini adalah 21. Pada D = 21, citra stego masih belum tahan terhadap kompresi tetapi tingkat kesamaannya terhadap citra asli sangat tinggi.
Kata-kata Kunci : *Steganografi, DCT, JPEG, nilai D, citra stego, citra asli*

PENDAHULUAN

Steganografi merupakan salah satu cara untuk mengamankan data atau informasi rahasia dengan menyembunyikan informasi dan data digital dibalik informasi digital lainnya, sehingga informasi digital yang sesungguhnya tidak kelihatan. Secara teori, semua berkas umum yang ada di dalam komputer dapat digunakan sebagai media, seperti berkas citra berformat JPEG, GIF, BMP, musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Penelitian ini menggunakan media citra (disebut juga citra sampul) JPEG untuk menyimpan data digital atau disebut juga pesan rahasia.

Ada sejumlah teknik untuk melakukan steganografi, diantaranya penyisipan *least significant bit* (LSB), *masking*/ *filtering*, dan transformasi/alihragam. Penelitian ini menggunakan metode DCT yang merupakan teknik alihragam dan mempunyai kelebihan mampu menggunakan citra sampul berupa citra JPEG.

Algoritma penyimpanan dan pengambilan pesan rahasia dinyatakan dengan (Katzenbeisser& Petitcolas, 1998; Zhao & Koch, 1995),

```
for i = 1,...,l(M) do
    choose one cover-block b_i
    B_i= D{b_i}
    if m_i= 0 then
        if B_i(u_1, v_1) >B_i(u_2, v_2)then
            swap Bi(u1, v1) and Bi(u2, v2)
        end if
    else
        if B_i(u_1, v_1) <B_i(u_2, v_2) then
            swap B_i(u_1, v_1) and B_i(u_2, v_2)
        end if
    end if
    adjust both values so that |B_i(u_1, v_1) - B_i(u_2, v_2)| >x
    b_i'= D^-1{B_i}
end for
create stego-image out of all b''
```

Gambar 1 Proses penyimpanan pesan

```
for i = 1,...,l(M) do
   get cover-block bi associated
with bit i
   B_i= D{b_i}
   if B_i(u_1, v_1) ≤ B_i(u_2, v_2) then
     m_i= 0
   elsem_i= 1
   end if
end for
```

Gambar 2 Proses pengambilan pesan

Penyisipan pesan dilakukan blok per blok, tiap blok berukuran 8x8 piksel. Simbol (u,v) menunjukkan lokasi piksel pada baris u dan kolom v dalam blok tersebut. Berdasarkan tabel kuantisasi, koefisien (4,1) dan (2,3) atau (1,2) dan (3,0) merupakan kandidat yang baik (Katzenbeisser and Petitcolas, 1998); sedang Zhao & Koch memilih berbeda berdasarkan penelitiannya adalah (1,3), (1,4), (2,2, (2,3), (2,4), (3,1), (3,2) dan (3,3). Nilai x pada Gambar 1 merupakan nilai D dalam penelitian ini. Semakin besar nilai D maka ketahanan citra terhadap perubahan semakin bagus tetapi kualitas citra yang dihasilkan akan semakin jelek.

Untuk menentukan nilai D, digunakan nilai PSNR dan korelasi antara citra sampul (A) dan citra stego (B). Dengan matlab dirumuskan sebagai berikut.

PSNR = 20*log10(1/(sqrt(mean(mean((A-B).^2))))) (1)

r = corr2 (A,B) (2)

Selanjutnya juga dihitung MSE untuk menunjukkan perbedaan kedua citra, bila nilainya semakin mendekati 0 maka semakin kecil perbedaannya.

MSE = sum(A.^2 - B.^2) (:))/prod(size(clama)) (3)

METODE

Bahan dari penelitian ini adalah 2 citra foto yang didapat dari hasil pemotretan dengan telepon genggam NOKIA 7610 yaitu berkas *foto(151).jpg* dengan resolusi 1152 x 864 piksel dan berkas *foto(169).jpg* dengan resolusi 1152 x 864 piksel. Dan ditambah berkas-berkas citra *wallpaper* komputer yaitu *flowers0411280.jpg*, *cube11280.jpg*, *cube31280.jpg*, *people.jpg*, dan *spongebob.jpg*. Berkas-berkas citra ini dinormalisasi dengan perangkat lunak Adobe Photoshop 7.0 sehingga diperoleh citra berukuran 256x256 piksel. Citra-citra lain yang digunakan untuk pengujian program steganografi akan diambil dari internet dan tanpa dilakukan pengolahan atau perubahan.citra-citra tersebut adalah:

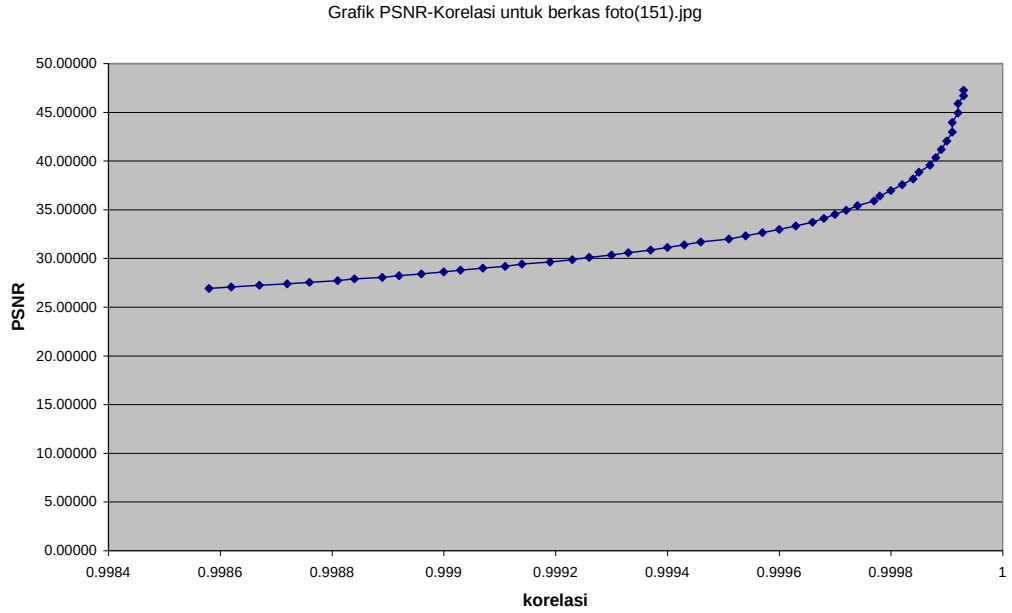
- Berkas *bunga_pagoda.jpg* ukuran 256x243 piksel,
  sumber: http://www.iptek.net.id/ind/pd_tanobat/gambar/bunga_pagoda.jpg
- Berkas *normal_Lund - Building 2.jpg* ukuran 535x400,
  sumber: http://www.pbd.gov.bn/Tcp%2520building2.jpg
- Berkas *tcp building2. jpg* ukuran 475x368 piksel,
  sumber: http://www.pbd.gov.bn/Tcp%2520building2.jpg
- Berkas *tcp building2. jpg* ukuran 475x368 piksel,
  sumber: http://www.pbd.gov.bn/Tcp%2520building2.jpg
- Berkas *rhs-chelsea-flower-show.jpg* ukuran 350x316 piksel,
  sumber:http://www.mooseyscountrygarden.com/chelsea-flower-show/chelsea-flower show.html
- Berkas *06062006dweb.jpg* ukuran 577x576 piksel,
  sumber: http://www.homeofourfathers.com/lisbeth/phpimages/06062006dweb.jpg
- Berkas *building.jpg* ukuran 480x640 piksel,
  sumber: http://www.psy.ritsumei.ac.jp/~akitaoka/building.jpg

Sedangkan data/pesan rahasia yang akan disisipkan adalah berkas *pesan.txt* yang berisi : “Kajian Penyimpanan Data pada Media Citra (Steganografi) Menggunakan Metode DCT (*Discrete Cosine Transform*)”.

Kegiatan penelitian diawali dengan menentukan pesan/data rahasia. Setelah itu citra yang telah dinormalisasi dipilih sebagai medium stego. Masing-masing dari tujuh buah berkas citra dicoba untuk menentukan nilai D (*distance*) atau perbedaan nilai koefisien dari 2 lokasi piksel yang dipilih untuk penyisipan. Lokasi piksel yang digunakan adalah (2,3) dan (4,1). Tiap citra dicoba dengan variasi nilai D dari 1 sampai dengan 50. Kemudian dianalisa sehingga diperoleh rerata nilai D yang akan digunakan untuk proses selanjutnya. Data pada medium stego kembali disisipkan dengan memakai nilai D yang telah ditentukan dengan bantuan perangkat lunak Matlab kemudian dilakukan ekstraksi data/pesan dari citra stego. Citra stego diuji ketahanannya dengan kompresi, tingkat kompresi yang diberikan untuk masing-masing citra adalah 90, 80, 70, 60, 50, 40, 30, 20, 10. Melalui tingkat kompresi yang berbeda pada citra stego diteliti apakah data/pesan rahasia masih dapat diekstrak dan sampai tingkatan mana kompresi masih bisa ditolerir oleh citra stego tersebut

HASIL

Hasil analisa penggunaan nilai D yang bervariasi dari 1 sampai dengan 50 menunjukkan hubungan antara PSNR dan korelasi seperti yang ditunjukkan Gambar 3.



Gambar 3. Grafik PSNR-Korelasi untuk berkas foto(151).jpg

Sedangkan nilai rerata D untuk tiap citra sampul yang diujikan ditunjukkan oleh Tabel 1.

Tabel 1. Nilai D rerata untuk berkas-berkas citra sampul

Nama berkas	D rerata
foto(151).jpg	20
foto(169).jpg	21
cube11280.jpg	20
cube31280.jpg	20
flowers0411280.jpg	22
people.jpg	21
spongebob.jpg	22
Rerata keseluruhan	20.857

Berdasarkan Tabel 1, nilai D yang digunakan dalam penelitian ini adalah 21. Citra stego yang dihasilkan disimpan dalam berkas citra format TIFF.

Pengujian untuk citra sampul yang tanpa mengalami pengolahan sebelumnya (tidak dinormalisasi) menghasilkan nilai PSNR, korelasi dan MSE seperti yang ditunjukkan dalam Tabel 2.

Tabel 2. Hasil pengukuran PSNR, Korelasi dan MSE pada penyisipan pesan

Nama berkas	Ukuran (piksel)	Citra Stego		
		PSNR	Korelasi	MSE
bunga_pagoda.jpg	256x243	39.611	0.99893	0.0003089
normal_Lund - Building 2.jpg	535x400	47.264	0.99968	0.0000671
tcp building2. jpg	475x368	53.2	0.99995	0.0002612
rhs-chelsea-flower-show.jpg	350x316	45.589	0.99959	0.0001033
06062006dweb.jpg	577x576	48.405	0.99984	0.0000526
building.jpg	480x640	53.221	0.99997	0.0000761

Citra stego yang dihasilkan pada proses di atas, secara keseluruhan pesan dapat direkonstruksi. Pesan hasil ekstraksi disimpan dalam berkas *ekstrak.txt* dan juga ditampilkan dalam kotak dialog seperti pada Gambar 4. Apabila proses pengambilan bit tidak dibatasi (secara otomatis memproses seluruh blok citra) maka pesan yang dihasilkan adalah pesan yang disembunyikan ditambah karakter-karakter lain yang berasal dari blok-blok citra bukan penyimpan bit pesan.

Gambar 4. Hasil ekstraksi dari citra sampul *building.jpg*

Pada proses pengambilan bit yang dibatasi untuk sejumlah n karakter maka jumlah blok yang diproses adalah n x 8 blok. Sedangkan jumlah karakter maksimum yang bisa dimasukkan adalah jumlah blok total dibagi 8. Misal untuk berkas sampul *building.jpg*, maka pada saat ekstraksi dengan pembatasan karakter yang digunakan akan muncul kotak dialog seperti Gambar 5.

Gambar 5 Kotak dialog ekstraksi pesan dengan pembatasan karakter

Pada kotak dialog diatas, untuk citra sampul *building.jpg* jumlah blok totalnya adalah 4800 blok sehingga karakter yang bisa disembunyikan pada proses penyisipan sebelumnya maksimum 4800/8 = 600 karakter. Dengan demikian, ekstraksi pesan bisa dibatasi sampai dengan 600 karakter. Dalam hal ini, digunakan angka 106 karakter, hasilnya diperlihatkan Gambar 6.

Gambar 6 Hasil ekstraksi dengan pembatasan sebanyak 106 karakter

Digunakan 106 karakter karena ingin mengetahui secara pasti jumlah karakter yang disembunyikan. Apabila pembatasan karakter yang dimasukkan kurang dari angka tersebut maka pesan ekstraksi akan terpotong. Bila melebihi dari angka 106 tersebut maka pesan ekstraksi adalah pesan yang disembunyikan ditambah karakter lain yang diwakili oleh blok-blok tambahan yang ikut diproses.

Citra stego dalam format TIFF dikompres untuk disimpan dalam citra JPEG dengan tingkat kompresi 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80% dan 90%. Mode yang disediakan oleh Matlab adalah *lossless* dan *lossy*. Pada mode *lossless* hasil pengukuran menunjukkan tidak ada perubahan pada citra. Proses kompresi juga dilakukan untuk mengubah ke format TIF dengan mode kompresi *packbits*. Hasil kompresi ini dilihat dari segi ukuran berkasnya ditunjukkan Tabel 3 dan dilihat dari segi tingkat kesamaannya ditunjukkan Tabel 4.

Tabel 3. Ukuran berkas citra stego terkompresi

Citra Sampul Ukuran citra asal, ukuran citra stego	Kompresi JPEG (KB)									Kompresi TIF (KB)
	10	20	30	40	50	60	70	80	90	Packbits
bunga_pagoda.jpg 19 KB, 185 KB	36	27	24	19	19	18	17	10	7	185
normal_Lund - Building 2.jpg 60 KB, 633KB	82	60	53	44	34	32	26	20	13	633
tcp building2. jpg 30 KB, 457 KB	40	29	26	23	22	15	14	11	8	457
rhs-chelsea-flower-show.jpg 35 KB, 328 KB	47	34	29	24	21	19	16	13	8	328
06062006dweb.jpg 90 KB, 983 KB	136	104	90	85	80	46	41	30	19	983
building.jpg 253 KB, 901 KB	129	86	69	59	52	45	39	31	21	901

Tabel 4 Korelasi berkas citra stego terkompresi

Citra Sampul	Kompresi JPEG									Kompresi TIF
	10	20	30	40	50	60	70	80	90	Packbits
bunga_pagoda.jpg	0.9995	0.9969	0.9956	0.9958	0.9995	0.9924	0.9716	0.9043	0.8622	1
normal_Lund - Building 2.jpg	0.9999	0.9999	0.9968	0.9898	0.9887	0.9868	0.9808	0.9728	0.9538	1
Tcp building2. jpg	0.9999	0.9996	0.9997	0.9986	0.9964	0.9947	0.9938	0.9909	0.9847	1
rhs-chelsea-flower-show.jpg	0.9996	0.9984	0.9955	0.9928	0.9901	0.9871	0.9829	0.9750	0.9548	1
06062006dweb.jpg	0.9998	0.9975	0.9999	0.9965	0.9896	0.9741	0.9729	0.9668	0.9547	1
building.jpg	0.9992	0.9974	0.9958	0.9943	0.9928	0.9911	0.9883	0.9832	0.9713	1

Ekstraksi pesan terhadap citra stego yang dikompresi JPEG pada mode *lossless* dan TIF pada mode *packbits* dapat dilakukan dengan baik. Sedangkan pada mode *lossy* tidak dapat dilakukan dengan baik, walaupun antara citra stego asal dan citra stego terkompresi mempunyai korelasi besar. Hal ini berarti pesan yang disembunyikan tidak dapat diekstrak pada nilai D = 21, walau tingkat kompresinya hanya 10%.

PENUTUP

Dari penelitian yang dilakukan maka diperoleh kesimpulan sebagai berikut:

1. Teknik steganografi dengan metode DCT dapat menggunakan citra sampul berupa berkas JPEG, yang berukuran relatif kecil dan umum digunakan/dipertukarkan dalam hubungan internet, sehingga citra stego yang dihasilkan juga masih kecil dan mudah dipertukarkan lewat komunikasi internet.
2. Algoritma penyisipan pesan dengan metode DCT menghasilkan citra stego yang mempunyai tingkat kesamaan yang tinggi terhadap citra aslinya, sehingga pesan yang disembunyikan dalam citra stego tidak mudah dideteksi.
3. Ekstraksi pesan dilakukan dengan algoritma yang sama, perbedaannya kalau pada penyisipan pesan berpatokan pada bit pesan sedangkan pada ekstraksi pesan berpatokan pada perbandingan koefisien DCT dari piksel (2,3) dan (4,1).
4. Nilai D yang merupakan nilai mutlak dari nilai minimum selisih koefisien DCT dari piksel (2,3) dan (4,1) menentukan tingkat ketahanan citra stego. Nilai D secara default adalah 1. Dalam penelitian ini dihasilkan bahwa nilai D yang paling baik adalah 21.

5. Citra stego yang dihasilkan menggunakan D = 21 apabila dikompres pada mode *lossy* tidak dapat diekstrak, sebaliknya semua citra stego yang dikompres pada mode *lossless* dapat diekstrak dengan baik. Kompresi TIF semua pesan dapat diekstrak. Karena kompresi umumnya bersifat *lossy*, sehingga pada algoritma ini dengan nilai D = 21 dapat dikatakan citra stego tidak tahan terhadap kompresi.
6. Kekurangan dari algoritma ini adalah kapasitas pesan yang disembunyikan kurang besar karena pada proses penyisipannya hanya menyimpan 1 bit pesan pada 1 blok citra.

DAFTAR RUJUKAN

Amin, M.S., S. Ibrahim, M.R. Katmin, and M.Z.I. Shamsudins, *Information Hiding Using Steganography*. 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia. 2003

Artz, Donovan, *Digital Steganography: Hiding Data within Data*. IEEE Internet Computing.May-Juni. 2001. pp 75-80
Available: http://www.isi.edu/~dono/pdf/artz01digital.pdf [2006, April 24]

Cachin, Christian, *Digital Steganography*.Zurich Research Laboratory CH-8803 Rüschlikon. Switzerland. 2004
Available: http://citeseer.ist.psu.edu/cachin04digital.html [2006, April 24]

Cole, Eric, *Hiding in Plain Sight : Steganography and the Art of Covert Communication*. Wiley Publishing, Inc. 2003

Dwiandiyanta, B. Y., *Watermarking Citra Digital Menggunakan Alihragam Wavelet*. Tesis. Program Pascasarjana Univeritas Gadjah Mada. Yogyakarta. 2004

Fridrich, *Applications of Data Hiding in Digital Images*. Tutorial for the ISPACS'98. Melbourne. 1998
Available: http://citeseer.ist.psu.edu/fridrich98application.html [2006, April 24]

Gonzalez, R.C. and P.Wintz, *Digital Image Procesing Second Edition*. Addison-Wesley Publishing Company. United States of America. 1987

Irianto, *Embedding Pesan Rahasia dalam Gambar*. Tugas Akhir. Departemen Teknik Elektro Bidang Khusus Kendali dan Sistem Cerdas, Institut Teknologi Bandung. Bandung. 2004
Available: http://budi.insan.co.id/courses/el7010/2004-2005/irianto-report.pdf [2006, April 22]

Johnson, N. and S. Jajodia, *Exploring Steganography: Seeing the Unseen*. IEEE Comp. Vol. 31, No.2 (Feb. 1998), pp 26–34

Katzenbeisser, Stefan and F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House. Boston. 1999

Khayam, S.A., *The Discrete Cosine Transform (DCT):Theory and Application*. Department of Electrical & Computer Engineering.Michigan State University. Michigan. 2003
Available: http://www.egr.msu.edu/Ali_files/DCT_TR802.pdf [2006, April 24]

Kipper, Gregory, *Investigator's Guide Steganography*.Aurbach Publications. Florida. 2004

Munir, Rinaldi, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Penerbit Informatika. Bandung. 2004

Pitas, I., *Digital Image Procesing Algorithms*.Prentice Hall International (UK) Ltd. Cambridge. 1993

Reyzin, Leonid and Scott Russell, *More Efficient Provably Secure Steganography*. Department of Computer Science Boston University. 2003
Available http://citeseer.ist.psu.edu/reyzin03more.html [2006, April 24]

The International Telegraph and Telephone Consultative Committee (CCITT), *Recommendation T.81*. 1992

Vanda, Y., *Digital Image Watermarking (DIW) yang Tahan Terhadap Transformasi Geometris*. Tesis. Program Pascasarjana Univeritas Gadjah Mada. Yogyakarta. 2004

Zhao, Jian & Koch, Echkard, *Embedding Robust Labels into Images for Copyright Protection*.Fraunhofer Institute for Computer Graphics. Germany. 1995.