PERBANDINGAN ALGORITMA LSB DAN DCT PADA STEGANOGRAFI

Nizar Arif Amrullah A11.2008.04309
Program Studi Teknik Informatika – S1
Fakultas Ilmu Komputer
Universitas Dian Nuswantoro, Jl. Nakula I No. 5-11, Semarang
ijankbae89@gmail.com

ABSTRAK

Seiring semakin canggihnya dunia teknologi informasi semakin tinggi tingkat kejahatan pada data-data teknologi informasi, salah satu cara yang dapat digunakan untuk mengamankan data-data itu dengan metode kriptografi. Steganografi merupakan salah satu metode kriptografi yang menggunakan metode watermaking yaitu menyamarkan data pada sebuah gambar. banyak algoritma yang di terapkan pada kriptografi diantarnya LSB (*Least Significant Bit Insertion*) dan DCT (*Discrete Cosine Transformation*). Pada kesempatan ini penulis akan membandingkan metode yang digunakan pada steganografi yaitu metode LSB dan DCT. Proses Perbandingan metode ini akan diukur dari *fidelity* (kualitas citra digital tidak berubah), *robustness* (tahan terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung) dan recovery (dokumen yang disembunyikan dalam citra digital harus dapat dibaca kembali).

Kata kunci : perbandingan algoritma, dct, lsb, fidelity, robustness, recovery

I. PENDAHULUAN

1.1 Latar Belakang

Takdir manusia menjadi mahluk social menjadikan manusia tidak terlepas dari komunikasi baik secara langsung ataupun tidak langsung.Salah satu media yang digunkan dalam komunikasi tidak langsung yaitu internet. Internet menjadi salah satu media yang paling populer di dunia. Fasilitas dan kemudahan yang dimiliki oleh internet menjadikan internetsebagai bagian media komunikasi yang tidak bisa terpisahkan dan menjadi barang yang tidak asing lagi. Banyak komunikasi yang dilakukan dengan menggunakan internet diantaranya bertukar*e-mail, video call*, betukar gambar, adan juga berutukar file-file yang lain. Seiring dengan perkembanganinternet dan aplikasi yang semakin banyak, semakin berkembang pula kejahatan sistem pada lalulintas di internet. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya kemudian memafaatkan dengan tidak semestinya baikmenggandakan, dan memanfaatkan untuk tindak kejahatan. Salah satu alternatif solusiyang dapat dipakai yaitumenggunakan sistem keamanan termasuk didalamnya penggunaan ilmu kriptografi.Dengan menggunakan kriptografi pesan yang akan disampaikan dapat disimpan pada media yang dipakai untuk penyisipan atau memberikan legalitas kepemilkan dengan menggunakan *digital watermaking*.

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi.Teknik steganografi sudah dipakai lebih dari 2500 tahun yang lalu untuk menyembunyikan pesan rahasia.Berbeda dengan teknik kriptografi, steganografi menyembunyikan pesan rahasia agar bagi orang awam tidak menyadari keberadaan dari pesan yang disembunyikan.Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut.Dalam steganografi modern media yang digunakan adalah file-file multimedia baik berupa gambar seperti png, bmp,jpg atau menggunakan format audio atau video. Lalu lintas file-file multimedia di internet sudah lumrah sehingga akan mengurangi kecurigaan akan adanya pesan rahasia.Kegunaan file multimedia pada steganografi adalah kedok untuk menyembunyikan pesan, teknik ini dikenal dengan sebutan *digital watermarking*.

Terdapat banyak metode *digital watermaking* untuk citra digital diantaranya yaitu *LSB (Least Significant Bit)* coding, berbeda dengan metode *MSB(Most Significant Bit)*, Metode penyisipan *LSB (Least Significant Bit)* ini adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Proses penyisipi pesan dilakukan dengan cara menggantikan bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap pixel file gambar citra 24 bit dapat disisipkan

3 bit pesan,sedankan MSB yaitu penggunaan angka yang paling berarti/paling besar yang letaknya disebelah paling kiri. Selain metode LSB dan MSB ada juga metode tarnsform yaitu DCT(*Discrete Cosine Transform*). MetodeDCTmerupakan sebuah proses digital pada citra klasik dan metode domain populer yang paling banyak digunakan. Dengan metode ini. Proses dari DCT sendiri yaitu memecahsebuah citra kedalam bentuk kelompok frekuensi yang berbeda-beda, dan membuat penyembunyian informasi watermark ke bagian tengah dari kelompok frekuensi dari citra. Tujuan terpilihnya bagian tengah dari kelompok frekuensi yang dimaksudkan yaitu untuk menghindari bagian visual yang paling penting dari sebuah gambar melalui sebuah kompresi maupun gangguan noise.

Tingkat keamanan dari pertukaran pesan harus dijaga supaya tidak disalah gunakan oleh orang lain. Salah satu cara untuk menyamarkan pesan rahasia pada file multimedia adalah digital watermaking baik memakai LSB atau DCT. Untuk mengetahui tingkat kesamaran dari penggunaan LSB dan DCT penulis tertarik untuk melakukan perbandingan LSB dan DCT pada steganografi dengan melihat beberapa kriteria teknik watermark yang baik yaitu Fidelity, Robustnessdan Recovery.

1.2 Tujuan

Membandingkan metode LSB dan DCT berdasarkan kriteria Fidelity, Robustnessdan Recovery

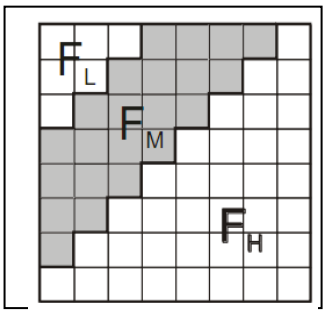
1.3 Batasan Masalah

Pada penelitian ini citra penampung yang digunakan untuk menyimpan pesan adalah citra grayscale berukuran 512x512 piksel. Sedangkan citra pesan yang digunakan adalah citra biner berukuran 64x64 piksel. Kriteria watermark yang digunakan adalah Fidelity, Robustness (mengubah-ubah brigthness dan kontras dari citra watermark) dan Recovery yang diukur menggunakan Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) dan Corelation (C).

II. TINJAUAN PUSTAKA

2.1 DCT

DCT merupakan sebuah proses citra klasik dan metode domain populer yang paling banyak digunakan. Dengan metode ini, sebuah citra dipecah kedalam bentuk kelompok frekuensi yang berbeda-beda, dan membuat penyembunyian informasi watermark ke bagian tengah dari kelompok frekuensi dari citra menjadi lebih mudah. Terpilihnya bagian tengah dari kelompok frekuensi dimaksudkan untuk menghindari bagian visual yang paling penting dari sebuah gambar melalui sebuah kompresi maupun gangguan noise. Salah satu teknik yang digunakan yaitu dengan menerapkan perbandingan antara koefisien DCT untuk pengkodean bit tunggal kedalam blok DCT. Sebagai permulaan, dinyatakan middle-band frequencies (FM) dari 8x8 blok DCT seperti pada gambar 2.6 dibawah ini.



Gambar 2.1 : Daerah Gambar DCT

FL digunakan untuk menyatakan komponen frekuensi terendah dari blok, sementara FH menyatakan komponen tertinggi dari blok. FM dipilih sebagai daerah ketahanan tambahan terhadap teknik pengurangan pemampatan, yang bertujuan untuk mencegah perubahan yang berarti pada citra cover.

2.2 LSB

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri.

Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 1111 1111b). Bilangan tersebut dapat berarti :

$$1*2^7+1*2^6+1*2^5+1*2^4+1*2^3+1*2^2+1*2^1+1*2^0=128+64+32+16+8+4+2+1=255$$

Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, danitu adalah yang paling kecil. Bagian tersebut disebut dengan leastsignificant bit (bit yang paling tidak berarti), sedangkan bagian paling kiribernilai 128 dan disebut dengan mostsignificant bit (bit yang paling berarti). Least significant bit sering kali digunakan untuk kepentingan penyisipan

data ke dalam suatu media digital lain.salah satu yang memanfaatkan least significant bit sebagai metode penyembunyian adalah steganografi audio dan gambar. Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam bit rendah (least significant bit) pada data pixel yang menyusun file gambar BMP 24 bit tersebut. Pada file gambar BMP 24 bit setiap pixel pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1byte) dari 0 sampai 255 atau denganformat biner 00000000 sampai 11111111. Sebagai contoh file gambar BMP 24 bit dengan warna merah murni dalam format biner akan terlihat sebagai berikut :

00000000 00000000 11111111
00000000 00000000 11111111

Sedangkan untuk warna hijau murni dalam format biner akan terlihat sebagai berikut :

00000000 11111111 00000000
00000000 11111111 00000000

Sedangkan untuk warna biru murni dalam format biner akan terlihat sebagai berikut :

11111111 00000000 00000000
11111111 00000000 00000000

Dari uraian di atas dapat dilihat bahwa informasi dari warna biru berada pada bit pertama sampai bit delapan, dan informasi warna hijau berada pada bit sembilan sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24. Metode penyisipan LSB (least significant bit) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap pixel file gambar BMP 24 bit dapat disisipkan 3 bit pesan, misalnya terdapat data raster original file gambar adalah sebagai berikut :

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka akan dihasilkan

0010011**0** 11101001 11001000
00100110 1100100**0** 1110100**0**
11001000 00100111 11101001

Terlihat pada bit kedelapan, enambelas dan 24 diganti dengan representasi biner huruf A, dan hanya tiga bit rendah yang berubah (cetak tebal), untuk penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada file gambar yang sudah diisi pesan rahasia jika dibandingkan dengan file gambar asli sebelum disisipi dengan pesan rahasia.

2.3 Mean Squared Error (MSE)

MSE (*Mean Squared Error*) adalah alat ukur kuantitatif yang digunakan mengukur rata-rata kesalahan pada suatu gambar sebagai prosedur perbaikan citra (*pre-prosesing*). Dinyatakan dengan :

$$MSE=\frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_a(i,j)^2 - f_b(i,j)^2)\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Ket :

M dan N = ukuran panjang dan lebar citra

$f_a(i,j)$ = intensitas citra di titik (i,j) sebelum dilakukan proses

$f_b(i,j)$ = intensitas citra di titik (i,j) setelah dilakukan proses

Semakinkecil nilai MSE semakin bagus nilai proses yang dilakukan pada citra.

2.4 Peak Signal Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besaran derau yang berpengaruh pada sinyal tersebut. PNSR biasanya diukur dalam satuan desible citra yang dikatakan baik adalah citra yang memiliki PSNR antara 20 dB hingga 40 dB. Untuk menentukan nilai PSNR digunakan rumus:

$$PNSR= 10 \log(\frac{MAXi^2}{\sqrt{MSE}})$$

$$= 20 \log(\frac{MAXi}{\sqrt{MSE}})$$

20 log (MAX) – 10 .log (MSE)

PNSR = nilai PSNR citra (dalam dB)

MAXi = nilai maksimum piksel i

MSE = nilai MSE

Dengan $MSE = \frac{\sum_{y=1}^{m}\sum_{x=1}^{n}[I(x,y)-I'(x,y)]2}{mn}$

m dan n adalah baris dan kolom citra. I dan I‟ adalah citra asli dan citra rekonstruksi. Untuk menentukan PSNR, terlebih dahulu harus diketahui nilai rata-rata kuadrat dari error

(Mean Square Error - MSE). MSE menyatakan tingkat kesalahan kuadrat rata-rata dari perubahan citra yang dihasilkan terhadap citra asli.Semakin kecil nilai MSE menunjukkan semakin sesuai dengan citra asli.Parameter PSNR bernilai sebaliknya, semakin besar parameter PSNR semakin mirip dengan citra asli.

2.5 Corelasi (C)

Tingkat kemiripan antara dua buah citra diukur dengan Corelation (C), yang didefinisikan sebagai berikut:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}$$

nilai r berada diantara -1 s/d 1.

A_{mn} = intensitas piksel di posisi (m,n) pada citra A

A bar = rata-rata intensitas pada citra A

B_{mn} = intensitas piksel di posisi (m,n) pada citra B

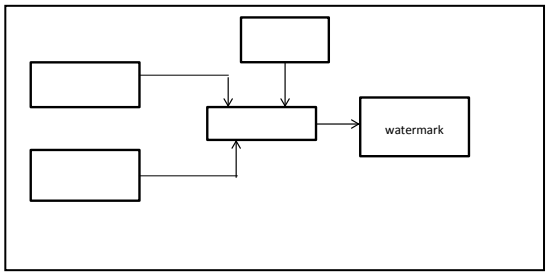
B bar = rata-rata intensitas pada citra B

III. METODE PENELITIAN

3.1 Arsitektur Utama LSB dan DCT

3.1.1 LSB

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Proses enkripsi pada LSB adalah sebagai berikut :

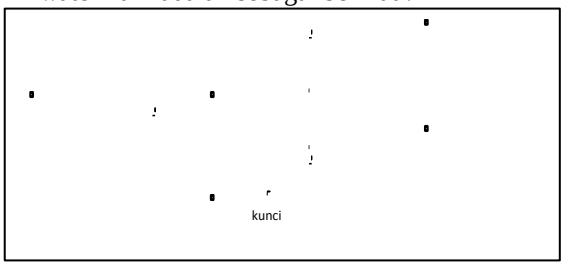


Gambar 3.1 : Proses Watermaking Pada Gambar MenggunakanLSB

Penjelasan :

1. Input gambar adalah proses proses input gambar yang akan digunakan sebagai gambar pesan.
2. Input gambar cover adalah prose input gambar yang digunakan sebagai gambar pembawa pesan.
3. Embed gambar adalah prose menjadikan satu antara gambara pesan dengan gambar cover. Pada proses inilah gambar pesan disisipkan menggunakan LSB.
4. Hasil gambar watermar adalah gambar hasil dari proses embed antara gambar pesan dengan gambar cover.
5. Kunci digunakan sebagai verifikasi enkripsi atau penyisipan pesan dan cover.

Proses ektraksi gambar yang sudah ter-watermark adalah sebagai berikut :



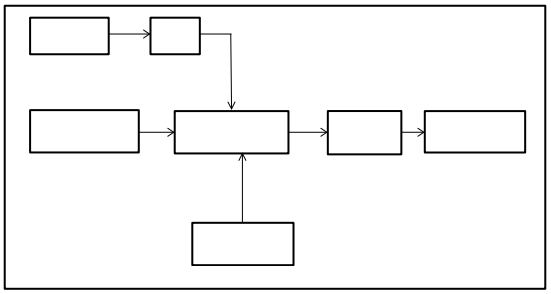
Gambar 3.2 : Proses Ekstraksi Pada Gambar Hasil

Proses ektraksi merupakan proses kebalikan dari proses enkripsi Penjelasan :

1. Input gambar adalah proses proses input gambar yang akan digunakan sebagai gambar pesan.
2. Input gambar cover adalah prose input gambar yang digunakan sebagai gambar pembawa pesan.
3. Ektraksi gambar adalah prose menjadikan satu antara gambar pesan dengan gambar cover. Pada proses ini dilakukan proses kebalikan dari proses embed pada enkripsi.
4. Hasil gabar watermar adalah gambar hasil dari proses embed antara gambar pesan dengan gambar cover.
5. Kunci digunakan sebagai verifikasi dekripsi atau ektrakasi pesan dan cover

3.1.2 DCT

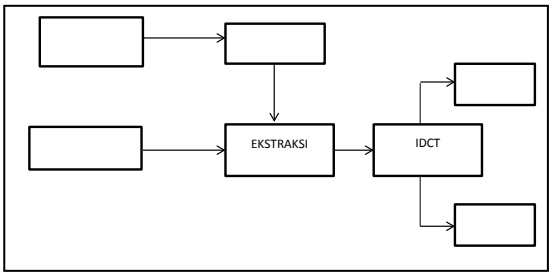
Proses penyisipan gambar dengan DCT adalah sebagai berikut :



Gambar 3.3 : Proses Enkripsi Pada Gambar Menggunakan DCT

1. Gambar merupakan gmbar cover yang digunakan untuk cover untuk pesan rahasia
2. Proses DCT yang bertujuan untuk memperoleh koefisien-koefisien DCT
3. Embed proses penyatuan gambar cover, pesan rahasia, dan kunci sebagai verivikasi untuk enkripsi.
4. Pesan rahasia merupakan pesan yang akan dismpaikan
5. Kunci digunakan sebagai kode verifikasi
6. IDCT merupakan transformasi balikan untuk memperoleh citra berwatermark
7. Gambar waterwark yaitu gambar hasil dari enkripsi menggunakanDCT.

Proses ekstraksi pada gambar watermarking menggunakan DCT pada citra dua dimensi



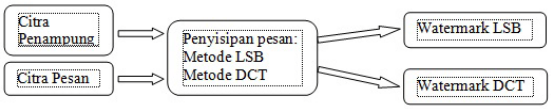
Gambar 3.4 : Proses Ekstraksi Pada Gambar Hasil Enkripsi Menggunakan DCT

1. Gambar merupakan gmbar cover yang digunakan untuk cover untuk pesan rahasia
2. Proses DCT yang bertujuan untuk memperoleh koefisien-koefisien DCT
3. Ekstraksi proses pembandngan bit-bit dengan kunci gambar cover, pesan rahasia, dan kunci sebagai verivikasi untuk enkripsi.
4. Pesan rahasia merupakan pesan yang akan dismpaikan
5. Kunci digunakan sebagai kode verifikasi
6. IDCT merupakan transformasi balikan untuk memperoleh citra berwatermark
7. Gambar waterwark yaitu gambar hasil dari enkripsi menggunakan DCT.

3.2 Rancangan Peneliian

Berikut adalah rancangan penelitian dari awal sampai akhir. Adapun proses penelitian yang dilakukan adalah sebagai berikut :

1. Proses Penyisipan Pesan
   Citra penampung disisipi citra pesan menggunakan metode LSB dan DCT menghasilkan citra watermark LSB dan citra watermark DCT .

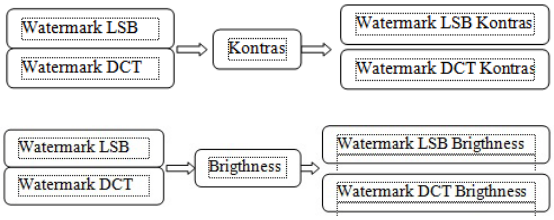


2. Pengujian Kriteria Fidelity
   Citra watermark LSB dan Citra watermark DCT dibandingkan dengan citra penampung menggunakan alat ukur MSE, PSNR dan C. Semakin kecil nilai MSE dan semakin besar nilai PSNR dan C, menunjukkan bahwa citra watermark dan citra penampung semakin mirip, artinya tingkat Fidelity-nya semakin bagus. Hal ini bisa juga dibuktikan secara visual (secara kasad mata).

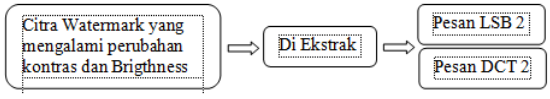
3. Pengujian Kriteria Recovery
   Citra watermark LSB dan Citra watermark DCT diekstrak menghasilkan citra pesan LSB dan citra pesan DCT.

citra pesan LSB dan citra pesan DCT dibandingkan dengan citra pesan secara visual dan diukur menggunakan MSE, PSNR dan Corelasi.

4. Pengujian Kriteria Robustness
   Pada Citra watermark LSB dan Citra watermark DCT dilakukan perubahan kontras dan perubahan brigthness menghasilkan Citra watermark LSB kontras, Citra watermark LSB Brigthness dan Citra watermark DCT kontras, Citra watermark DCT Brigthness.



Kemudian citra watermark yang telah mengalami perubahan kontras dan brigthness diekstrak sehingga menghasilkan citra pesan LSB2 dan citra pesan DCT2.



Citra pesan LSB2 dan citra pesan DCT2 dibandingkan secara visual dan diukur menggunakan MSE, PSNR dan C.

IV. HASIL PENELITIAN DAN PEMBAHASAN

4.1 Teknik Percobaan Perubahan Brigthness

Berikut adalah hasil uji dari pengujian Robustness dengan mengubah brigthness dari kosntanta kelipatan dari 5. Hasil uji ini untuk membuktikan seberapa kuatnya penyimpanan pesan gambar antara DCT (Discrete Cosine Transform) dan LSB (Least Significant Bit).

4.1.1 Uji Robustness Pada Brigthness

Tabel 4.1 : Hasil Uji Robustness Pada Brithness

Berikut adalah hasil dari uji robustness pada brigthnes dari kelipatan 5 konstanta brigthness.

Konstanta Brigthness	LSB			DCT		
	MSE	PSNR	Korelasi	MSE	PSNR	Korelasi
5	1	110,8253	-1	0,34937	121,3416	0,33608
10	0	Inf	1	0.34937	121.3416	0.33608
15	1	110.8253	-1	0.34912	121.3486	0.33681
20	0.0063477	161.422	0.9855	0.34985	121.3277	0.33464
25	0.99951	110.8302	-0.99887	0.34937	121.3416	0.33648
30	0.023926	148.1533	0.94717	0.39795	120.0396	0.26786
35	0.97095	111.1201	-0.93333	0.50879	117.5825	0.13364
40	0.028809	146.2961	0.93695	0.54248	116.9413	0.095809
45	0.9707	111.1226	-0.93277	0.59277	116.0547	0.038895
50	0.029785	145.9627	0.93493	0.60205	115.8994	0.032498

4.1.2 Uji Fidelity Pada Brigthness

Tabel 4.2 : Hasil Uji Fidelity Pada Brithness

Berikut adalah hasil dari uji fidelity pada brigthnes dari kelipatan 5 konstanta brigthness.

Konstanta Brigthness	LSB			DCT		
	MSE	PSNR	Korelasi	MSE	PSNR	Korelasi
5	24.9791	78.6449	1	26.9478	77.8863	0.99966
10	99.9486	64.7787	1	101.9114	64.5842	0.99966
15	224.8905	56.6691	1	226.8108	56.5841	0.99966
20	0.0063477	161.422	0.9855	0.34985	121.3277	0.33464
25	0.33464	54.1671	1	290.7067	54.1021	0.99966
30	864.1429	43.2079	0.99948	865.592	43.1911	0.99917
35	1077.4156	41.0021	0.99834	1078.8049	40.9892	0.99805
40	1244.5031	39.5604	0.99695	1245.9374	39.5488	0.99667
45	1397.4512	38.4012	0.99572	1398.987	38.3902	0.99544
50	1556.3512	37.3243	0.99436	1557.9986	37.3137	0.99407

4.1.3 Uji Robustness Pada Kontras

Tabel 4.3 : Hasil Uji Robustness Pada Kontras

Berikut adalah hasil dari uji fidelity pada kontras dari kelipatan 5 konstanta kontras.

Konstanta Kontras	LSB			DCT		
	MSE	PSNR	Korelasi	MSE	PSNR	Korelasi
5	0.48877	117.9839	0.0328448	0.61035	115.7625	0.0318
10	0.52075	117.3501	-0.0106693	0.61304	115.7186	0.0169006
15	0.51221	117.5155	0.0141669	0.60962	115.7745	0.03197
20	0.48047	118.1552	0.0572978	0.61157	115.7425	0.0194456
25	0.48877	117.9839	0.0328448	0.60913	115.7825	0.0328144
30	0.5542	116.7276	0.0258666	0.64966	115.1384	-0.034626
35	0.51196	117.5203	0.0145022	0.6084	115.7945	0.034627
40	0.48047	118.1552	0.0572978	0.61157	115.7425	0.0194456
45	0.48877	117.9839	0.0328448	0.60962	115.7745	0.0325199
50	0.52002	117.3642	-0.0096916	0.61475	115.6907	0.01391

4.1.4 Uji Fidelity Pada Kontras

Tabel 4.4 : Hasil Uji Fidelity Pada Kontras

Berikut adalah hasil dari uji fidelity pada kontras dari kelipatan 5 konstanta kontras.

Konstanta Kontras	LSB			DCT		
	MSE	PSNR	Korelasi	MSE	PSNR	Korelasi
5	1791.2551	35.91	0.96682	1794.4755	35.9006	0.96634
10	1708.5547	36.3912	0.96963	1711.9964	36.3711	0.96918
15	1630.5101	36.8588	0.97218	1633.5605	36.8401	0.97174
20	1555.1906	37.3317	0.97455	1558.4306	37.3109	0.97412
25	1484.4997	37.7969	0.97668	1487.3975	37.7774	0.97627
30	3802.5689	28.3909	0.80128	3807.5296	28.3779	0.80025
35	1353.2495	38.7226	0.9805	1355.9924	38.7024	0.98012
40	1292.8964	39.1789	0.98227	1295.7527	39.1568	0.98191
45	1237.0508	39.6204	0.98396	1239.6016	39.5998	0.98363
50	1184.4805	40.0547	0.98561	1187.0961	40.0326	0.98529

V. KESIMPULAN DAN SARAN

5. 1 Kesimpulan

Kesimpulan yang diambil dari tugas akhir perancangan dan implementasi steganografi adalah sebagai berikut :

a. Teknik steganografi yang dibuat telah memenuhi 3 Kriteria penyembunyian dokumen pada citra digital yang baik antara lain memenuhi syarat – syarat seperti *fidelity*, *robustness*, dan *recovery*.

Penulis telah menyimpulkan, bahwa dari perbandingan algoritma LSB dan algoritma DCT. Algoritma LSB yang lebih baik dari penyembunyian pesan. Karena LSB lebih memenuhi syarat *fidelity*, *robustness* dan *recovery.*Dan LSB juga lebih kuat ketahan gangguannya dari *brigthness* dan *kontras*.

b. Dengan penyisipan pesan citra, diharapkan dokumen yang ada didalam citra digital akan semakin sulit untuk dibaca oleh orang lain.

c. Teknik Steganografi dapat digunakan untuk menghindari kecurigaan pada pengiriman data rahasia melaui media internet sehingga dapat mengurangi tingkat pencurian data.

5. 2 Saran

a. Dalam penelitian ini penulis hanya membahas teknik *fidelity, robustness* dan recovery.Operasi pengolahan citra seperti pembesaran, pemotongan, dll pada stegoimage dapat mengakibatkan dokumen yang ada pada stegoimage tidak dapat dibaca, sehingga untuk kedepannya diharapkan steganografi yang dibuat tahan terhadap segala manipulasi citra.
b. Dalam penelitian kali ini hanya menggunakan citra bertype bmp untuk menyimpan dokumen hasil penyisipan, oleh karena itu, untuk penelitian selanjutnya akan mengembangkan penggunaan type lain untuk penyimpanan citra digital hasil penyisipan

Daftar Pustaka

1. Maradilla, Temmy. (2010) Aplikasi Steganografi Untuk Penyisipan Data teks Ke Dalam Citra Digital, Universitas Gunadarma
2. http://id.wikipedia.org/wiki/Steganografi, Tuesday, October 17, 2012
3. Sutoyo, S.Si., Mkom, Mulyanto, Edy., S.Si.,Mkom., Suhartono ,Vincent., Nurhayati., MT., Wijanarto, Mkom., Pengolahan Citra Digital, 2009, Yogyakarta,andioffset
4. Dharmaputra (2010). *PENGOLAHAN CITRA DIGITAL* . Yogyakarta. andioffset.
5. Fitri,sulidar. "IMPLEMENTASI ALGORITMA KRIPTOGRAFI DES DAN WATERMARK DENGAN METODE LSB PADA DATA CITRA" Yogyakarta. Amikom. 2010
6. Hasibuan A. Zainal, Ph.D. (2007). Metode Penelitian Dalam Bidang Ilmu Komputer dan Teknoogi Informasi. Depok. Universitas Indonesia.