IMPLEMENTASI *STEGANOGRAPHY* MENGGUNAKAN ALGORITMA *DISCRETE COSINE TRANSFORM*

Ahmad Adil Faruqi[1], Imam Fahrur Rozi[2]

[1,2] Teknik Informatika, Teknologi Informasi, Politeknik Negeri Malang
[1] ahmadadilf@gmail.com, [2] imam.rozi@polinema.ac.id

Abstrak

Steganography merupakan metode yang berbeda dengan metode kriptografi yang mengubah sebuah informasi kedalam sebuah sandi sehingga tidak dapat dibaca tanpa mengetahui kunci atau sandi yang digunakan, namun keberadaannya tetap diketahui dan tidak disembunyikan. Sedangkan pada *steganography* informasi akan disembunyikan didalam suatu media pembawa sehingga tak seorangpun yang menyadari bahwa terdapat suatu informasi.

Algoritma yang digunakan dalam *steganography* ini adalah algoritma *discrete cosine transform*. *Steganography* menggunakan algoritma *discrete cosine transform* menghasilkan gambar *steganography* dengan memiliki kualitas yang tidak jauh berbeda dari gambar aslinya hal ini ditunjukkan dengan besarnya nilai rata-rata hasil *peak signal to noise ratio* (*PSNR*) dari tiga gambar yang berbeda yaitu sebesar 37.44 db. Hasil pengujian kompresi gambar *steganography*, menyimpulkan bahwa pesan dalam gambar hasil *steganography* menggunakan algoritma *discrete cosine transform* tahan terhadap kompresi gambar.

Kata kunci : *steganography*, penyisipan informasi, algoritma *discrete cosinus transform* (DCT)

1. Pendahuluan

Perkembangan media digital yang pesat dan penggunaannya yang semakin banyak menimbulkan banyak keresahan dalam mengirim suatu informasi. Salah satu cara untuk mengamankan informasi dengan cara *steganography*. *Steganography* merupakan seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.

Metode ini berbeda dengan metode kriptografi yang mengubah sebuah informasi kedalam sebuah sandi sehingga tidak dapat dibaca tanpa mengetahui kunci atau sandi yang digunakan, namun keberadaannya tetap diketahui dan tidak disembunyikan. Sedangkan pada *steganography* informasi akan disembunyikan didalam suatu media pembawa sehingga tak seorangpun yang menyadari bahwa terdapat suatu informasi.

Salah satu metode yang digunakan dalam penyembunyian pesan ke dalam media gambar adalah *Discrete Cosine Transform* (DCT). Pada makalah ini, diimplementasikan sistem steganography menggunakan DCT dimana informasi yang disisipkan berupa teks sedangkan media pembawanya berupa gambar. Kelebihan *steganography* menggunakan algoritma DCT yakni pesan rahasia pada gambar akan tetap terjaga terhadap kompresi pada gambar. Setelah diimplemenasikan, sistem akan diuji dengan menggunakan parameter uji berupa nilai *Peak Signal to Noise Ratio* (PSNR) untuk mengevaluasi perbedaan antara citra hasil dan citra aslinya.

2. Landasan Teori

2.1 *Steganography*

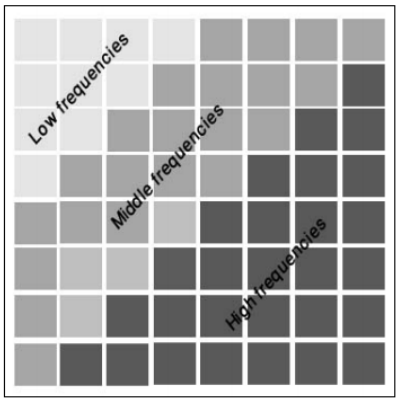
Steganography adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehinga keberadaan pesan rahasia tersebut tidak diketahui. *Steganography* berasal dari bahasa Yunani yaitu *steganos* yang artinya tulisan tersembunyi (*covered writing*). *Steganography* sangat kontras dengan *cryptography*. *Steganography* membutuhkan dua properti yaitu media penampung dan pesan rahasia berupa karakter atau tulisan.

2.2 *Discrete Cosine Transform* (DCT)

Discrete Cosine Transform adalah sebuah teknik untuk mengubah sebuah sinyal ke dalam komponen frekuensi dasar. *Discrete Cosine Transform* merepresentasikan sebuah citra dari penjumlahan sinusoida dari magnitude dan frekuensi yang berubah-ubah. Sifat dari DCT adalah mengubah informasi citra yang signifikan dikonsentrasikan hanya pada beberapa koefisien DCT.

Discrete Cosine Transform merupakan skema *lossy compression* yang digunakan dalam JPEG kompresi gambar NxN block ditransformasikan dari domain spasial ke domain DCT. DCT menyusun sinyal tersebut ke frekuensi spasial yang disebut

dengan koefisien DCT. Frekuensi DCT yang lebih rendah muncul pada kiri atas dari sebuah matriks DCT, dan frekuensi koefisien DCT yang lebih tinggi berada pada kanan bawah dari matriks DCT. Sistem penglihatan menusia tidak begitu sensitive dengan error-error yang ada pada frekuensi tinggi dibanding dengan yang ada pada frekuensi rendah. Karena itu, maka frekuensi yang lebih tinggi tersebut dapat dikuantisasi.



Gambar 1 Distribusi frekuensi pada block DCT

Discrete Cosine Transform (DCT) untuk suatu citra merupakan sinyal dua dimensi, *Discrete Cosine Transform* dua dimensi dapat diperoleh dengan rumus berikut:

$$C(u,v)=\frac{2}{\sqrt{MN}}\propto(u)\propto(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}f(x,y)\cos\left(\frac{\pi(2x+1)u}{2N}\right)\cos\left(\frac{\pi(2y+1)u}{2M}\right) \quad (1)$$

C : koefisien pada index ke-u
M : ukuran tinggi matriks
N : ukuran lebar matriks
x, y : indeks yang dicari nilainya

3. Proses *Steganography*

$$\alpha(k) = \begin{cases} \frac{1}{\sqrt{2}} & \text{untuk } k = 0 \\ 1 & \text{untuk } k \neq 0 \end{cases} \quad (2)$$

2.3 *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau atau *noise* yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (db). Pada makalah ini PSNR digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus menentukan nilai *Mean Square Error* (MSE). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi. Dalam steganography, MSE adalah nilai error kuadrat rata-rata antara citra asli (*cover-image*) dengan citra hasil penyisipan (*stegano-image*).

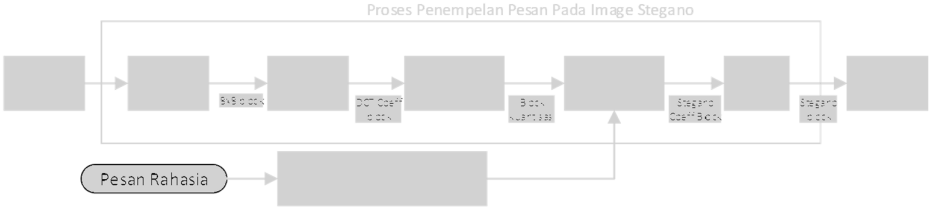
Perhitungan untuk menentukan PSNR adalah sebagai berikut:

$$PSNR = 10log_{10}(\frac{b^2}{MSE}) \quad (3)$$

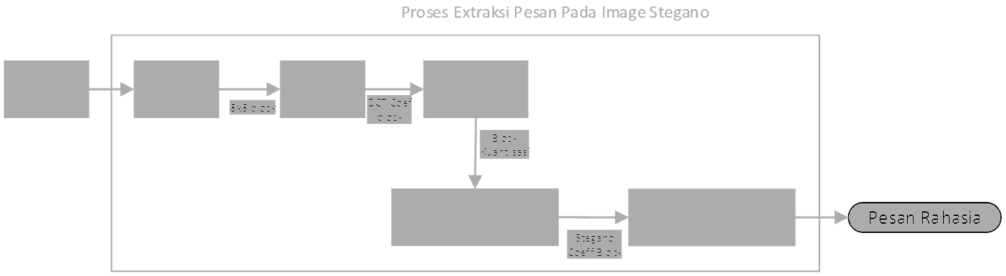
Nilai b merupakan nilai maksimum dari piksel citra yang digunakan. Nilai b pada makalah ini adalah 255. Dengan perhitungan MSE sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2 \quad (4)$$

Dimana x dan y adalah koordinat dari gambar, M dan N merupakan dimensi citra. I(x,y) merupakan nilai piksel pada citra asli, sedangkan I'(x,y) merupakan nilai piksel pada citra hasil *steganography*.



Gambar 2 Proses Encrypt Steganography



Gambar 3 Proses Decrypt Steganography

Untuk mendapatkan nilai matriks DCT dari rumus (1), kita akan menggunakan rumus berikut:

$$T(i,j) = \begin{cases} \frac{1}{\sqrt{N}} & \text{if } i = 0 \\ \sqrt{\frac{2}{N}} \cos \frac{(2j+1)i\pi}{2N} & \text{if } i \neq 0 \end{cases} \quad (5)$$

Dimana nilai N adalah panjang matriks yaitu 8. Untuk menghitung nilai koefisien DCT digunakan rumus berikut:

$$D = T.M.T^t \quad (6)$$

Lakukan kuantisasi pada matriks dengan matriks Q50.

Gambar 4 Matriks Q50

$$Q_{50} = \begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix} \quad (7)$$

Invers hasil matriks kuantisasi untuk mengembalikan nilai matriks kebentuk piksel seperti semula.

$$R_{i,j} = Q_{i,j} \circ C_{i,j} \quad (8)$$

$$N = \text{round}(T' RT) + 128 \quad (9)$$

3.1 Proses *Encrypt Steganography*

Langkah-langkah untuk menyisipkan pesan atau *encrypt steganography*:

1. Input gambar
2. Kurangi nilai piksel gambar dengan 128
3. Cari nilai matriks DCT
4. Hitung nilai matriks koefisien DCT
5. Kuantisasi matriks koefisien DCT
6. *Zigzag scanning* menjadi matriks satu dimensi
7. Ubah pesan menjadi *binner*
8. Ganti nilai matriks *zigzag* dengan nilai binner
9. Kembalikan matriks *zigzag* menjadi 8x8
10. Lakukan *invers* DCT disetiap bloknya

3.2 Proses *Decrypt Steganography*

Langkah-langkah untuk membaca kembali pesan pada gambar *steganography*:

1. Input gambar *steganography*
2. Kurangi nilai piksel gambar dengan 128
3. Cari nilai matriks DCT
4. Hitung nilai matriks koefisien DCT
5. Kuantisasi matriks koefisien DCT
6. *Zigzag scanning* menjadi matriks satu dimensi
7. Ambil nilai matriks berupa *binner*
8. Ubah *binner* ke *ASCII*

4. Implemantasi dan Pembahasan

4.1 Implementasi

Dengan menggunakan perhitungan dari PSNR dapat diketahui kualitas hasil gambar *steganography* dengan membandingkan antara gambar original dengan gambar hasil *steganography*.

Tabel 1 Pengaruh Banyaknya Pesan Terhadap PSNR

Gambar	einstein.jpg	pkl.jpg	lena.jpg
Ukuran File	154 KB	258 KB	251 KB
Ukuran Piksel	600 x 551	600 x 800	1024 x 1024
Pesan	"hello"		
Nilai *PSNR*	38,26 db	37,28 db	36,8 db
Pesan	"steganography joss"		
Nilai *PSNR*	38,25 db	37,27 db	36,79 db
Pesan	"polinema tetap jaya selalu"		
Nilai *PSNR*	38,24 db	37,27 db	36,79 db

Hasil pada tabel 1 menunjukkan bahwa semakin banyaknya pesan yang disisipkan maka akan mengurangi kualitas gambar yang ditunjukkan semakin berkurangnya nilai PSNR.

Pengujian kompresi gambar dilakukan terhadap gambar *steganography* untuk mengetahui apakah pesan tahan terhadap kompresi gambar.

Tabel 2 Ketahanan Pesan Terhadap Kompresi Dengan Quality 50 %

Nama Gambar	Ukuran File Stegano	Ukuran File Compress	Pesan yang Tersisip	Pesan Hasil Kompresi
baboon.jpg	20,8 KB	15,4 KB	"hello"	"hello"
eintein.jpg	24,2 KB	18,5 KB	"hello"	"hello"
hamilton.jpg	86 KB	65,6 KB	"hello"	"hello"
pkl.jpg	39,1 KB	30,7 KB	"hello"	"hello"
lena.jpg	96,7 KB	71,9 KB	"hello"	"hello"

Dari table 2 dapat dilihat bahwa pesan dari hasil dari kompresi dengan quality 50% pada gambar *steganography* masih tetap sama.

Tabel 3 Ketahanan Pesan Terhadap Kompresi Dengan Quality 30 %

Nama Gambar	Ukuran File Stegano	Ukuran File Compress	Pesan yang Tersisip	Pesan Hasil Kompresi
baboon.jpg	20,8 KB	15,4 KB	"hello"	"h"
eintein.jpg	24,2 KB	18,5 KB	"hello"	-
hamilton.jpg	86 KB	65,6 KB	"hello"	-
pkl.jpg	39,1 KB	30,7 KB	"hello"	-
lena.jpg	96,7 KB	71,9 KB	"hello"	-

Dari table 3 dapat dilihat bahwa pesan dari hasil dari kompresi dengan quality 30% pada gambar *steganography* masih tetap sama.

Tabel 4 Pengaruh Letak Pneyisipan Pada Tingkatan Frekuensi

Nama File Gambar	lena.jpg	eintein.jpg	pkl.jpg
Pesan	"qwerty"		
	Nilai *PSNR*		
Frekuensi Rendah	36,8046	38,2576	37,2804
Frekuensi Tengah Index 16	36,7881	38,2308	37,2696
Frekuensi Tengah Index 22	36,7775	38,1839	37,244
Frekuensi Tinggi Index 37	36,7551	38,0883	37,191
Frekuensi Tinggi Index 57	36,6971	37,8678	37,0536

Table 4 menunjukkan bahwa letak penyisipan pada tingkatan frekuensi berpengaruh terhadap besarnya nilai PSNR.

Pesan rahasia pada gambar *steganography* akan diuji ketahanannya terhadap perubahan *brightness* dan *contrast* sebesar +40. Sehingga gambar *steganography* akan lebih terang dibandingkan dengan sebelumnya.

Tabel 5 Tabel Ketahanan Pesan Terhadap Perubahan *Brightness* dan *Contrast*

Nama File Gambar	Pesan yang Tersisip	Pesan Hasil Kompresi	Kesimpulan
baboon.jpg	"hello"	"h`)tn"	Pesan Rusak
eintein.jpg	"hello"	"hdllo"	Pesan Rusak
hamilton.jpg	"hello"	"l¼g"	Pesan Rusak
pkl.jpg	"hello"	"hello"	Pesan Utuh
lena.jpg	"hello"	"hello"	Pesan Utuh

Dari table 5 dapat dilihat bahwa pesan dari hasil dari perubahan *brightness* dan *contrast* sebesar +40 pada gambar *steganography* mengalami kerusakan pesan tetapi terdapat dua pesan yang utuh dari dua gambar yang memiliki tingkat awal *brightness* dan *contrast* yang gelap.

4.2 Pembahasan

1. **Pengaruh Banyaknya Karakter yang Disisipkan**

   Semakin banyak katakter yang disisipkan pada gambar akan semakin turun nilai PSNR yang didapatkan atau kualitas gambarnya semakin menurun.

   Hal ini disebabkan karena binner pada karakter disisipkan dengan cara mengganti nilai matriks kuantisasi dengan nilai binner. Semakin banyak karakter yang disisipkan maka semakin banyak nilai matriks kuantisasi yang diganti. Sehingga error yang didapat semakin banyak dan kualitasnya menurun.

2. **Pengaruh Letak Penyisipan Karakter**

   Peletakan penyisipan binner pada tingkatan frekuensi berpengaruh terhadap nilai *PSNR*. Penyisipan pada frekuensi rendah, memiliki nilai *PSNR* yang lebih tinggi dibandingkan penyisipan pada frekuensi tengah dan frekuensi tinggi.

   Hal ini disebabkan nilai koefisien *DCT* pada frekuensi tinggi akan dibagi dengan matriks Q50 yang nilainya dominan lebih besar dari nilai matriks koefisien *DCT* sehingga nilai kuantisasi pada frekuensi tinggi akan bernilai nol (0). Ketika nilai matriks pada frekuensi tinggi yang bernilai nol (0) diganti dengan nilai binner yang bernilai satu (1), dan dilakukan *invers* dimana langkah awal *invers* adalah melakukan perkalian *Hadamard Product* pada matriks kuantisasi hasil penyisipan dengan Q50. Maka nilai matriks hasil perkalian pada frekuensi tinggi akan memiliki nilai yang

jauh lebih besar dibandingkan nilai matriks koefisien *DCT* sebelumnya. Hal inilah yang mengakibatkan error yang lebih banyak pada nilai piksel sehingga nilai *PSNR* lebih kecil dibandingkan dengan karakter yang disisipkan pada frekuensi rendah.

3. **Ketahanan Pesan Terhadap Kompresi Gambar**

   Pada pengujian kompresi gambar *steganography*, pesan yang tersisipkan di dalam gambar *steganography* masih tetap utuh terhadap kompresi gambar. Format gambar *steganography* yang dihasilkan pada algoritma *DCT* adalah *JPEG* dan kompresi gambar dengan format *JPEG* menggunakan algoritma yang sama yaitu *DCT* dimana ketika melakukan kompresi, informasi pada frekuensi tinggi dihilangkan dengan cara melakukan kuantisasi. Sedangkan pada frekuensi rendah tidak memiliki terlalu banyak perubahan. Sehingga pesan rahasia yang disisipkan pada frekuensi rendah akan tetap ada sejauh besarnya kompresi yang dilakukan. Semakin banyak melakukan kompresi maka pesan yang tersisipkan akan rusak bahkan hilang.

4. **Ketahanan Pesan Terhadap Perubahan *Brightness* dan *Contrast***

   Gambar *steganography* yang ditambah nilai *brightness* dan *contrast* sebesar +40 akan menjadi lebih terang hal ini akan menyebabkan perubahan setiap nilai piksel pada gambar. Sehingga tidak menutup kemungkinan bahwa pesan rahasia akan rusak bahkan hilang. Tetapi pesan rahasia yang terdapat pada gambar *steganography* yang awalnya gelap kemudian ditambahkan nilai *brightness* dan *contrast* sebesar +40 maka nilai piksel mengalami sedikit perubahan. Sehingga terdapat kemungkinan bahwa pesan rahasia masih tetap utuh.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil pengujian dapat diambil kesimpulan antara lain:

1. Dengan algoritma *discrete cosine transform*, pesan text dapat disisipkan ke dalam media berupa gambar.
2. Dengan algoritma *discrete cosine transform*, pesan text yang terisisip pada gambar dapat dibaca kembali.
3. Kualitas gambar *steganography* menggunakan metode *discrete cosine transform* tergolong baik. Hal ini dapat dilihat dari hasil nilai PSNR yang lebih besar dai 30 db.
4. Peletakan informasi yang akan disisipkan pada tingkatan frekuensi sangat berpengaruh terhadap besarnya nilai PSNR.
5. Semakin banyak karakter pada pesan yang disisipkan maka nilai PSNR semakin kecil.
6. Pesan rahasia pada gambar *steganography* tahan terhadap kompresi gambar.
7. Pesan rahasia pada gambar *steganography* rusak terhadap perubahan *brightness* dan *contrast* sebesar +40.

5.2 Saran

Pada aplikasi ini hanya dapat menyisipkan pesan rahasia pada gambar yang memiliki mode warna *grayscale* saja. Aplikasi ini dapat dikembangkan sehingga tidak hanya gambar *grayscale* saja tetapi gambar dengan mode warna RGB.

Steganography dapat dirancang dengan metode yang berbeda dan setiap metode pasti memiliki kelebihan masing-masing. Diharapkan untuk penelitian kedepannya dapat mengetahui perbedaan dari kelebihan dan kekurangan setiap metode.

Daftar Pustaka:

Agustian, Indra, M.Eng. 2013. *Definisi Citra.* [Online] Tersedia: http://te.unib.ac.id/lecturer/indraagustian/2013/06/defnisi-citra/ [23 Desember 2014]

Al-Momen, S, M, A and George, L. 2010. *Image Hiding Using Magnitude Modulation on the DCT Coefficients.* Iraq: Information Technology Unit University of Baghdad

Andrian, Yudhi. *Perbandingan Metode Lsb, Lsb+1, dan Msb pada Steganografi Citra Digital.* Medan: STMIK Potensi Utama

Hermawati, F, A. 2013. *Pengolahan Citra Digital Konsep dan Teori.* Yogyakarta: CV. Andi Offset

Nugroho dan Aulia, Febri. 2011. *Implementasi Kompresi Video dengan Algoritma Discrete Cosine Transform Pada Perangkat Bergerak*. Sumatra Utara: University of Sumatra Utara Institutional Repository

Sitorus, Ahmad Ramadoni. 2014. *Perancangan Perangkat Lunak Steganography Menggunakan Algoritma Outguess.* Medan: STMIK Budi Darma Medan