JURNAL ILMIAH INFORMATIKA GLOBAL Volume 09 No. 2 Desember 2018
ISSN PRINT : 2303-500X
ISSN ONLINE : 2477-3786

Keamanan Pesan Rahasia Menggunakan Steganografi DCT (*Discrete Cosine Transform*) pada Citra JPEG

Dian Hafidh Zulfikar[1)]

[1)]*Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang*
Jl. Prof. K.H. Zainal Abidin Fikry KM 3.5 Palembang 30126
Email : dianhafidhzulfikar_uin@radenfatah.ac.id[1)]

Abstract

The least significant-bit (LSB) based techniques are very popular for steganography in spatial domain. The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In Discrete Cosine Transform (DCT) based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information.

Keywords : *Discrete Cosine Transform (DCT), steganography, secret message*

Abstrak

Pada steganografi domain spasial, teknik least significant-bit (LSB) merupakan teknik yang paling banyak digunakan pada steganografi. Teknik yang sederhana yang hanya mengubah nilai LSB pada cover image dengan nilai bit pesan rahasia, atau dengan teknik yang lebih baik lagi yaitu dengan menentukan bit-bit LSB mana yang akan dilakukan pergantian nilai bit. Lain halnya dengan metode Discrete Cosine Transform (DCT), teknik steganografi ini akan menyembunyikan informasi rahasia tergantung dari nilai Koefisien DCT.

Kata Kunci : *Steganografi, DCT, Citra, JPEG, Pesan Rahasia*

ISSN PRINT : 2303-500X
ISSN ONLINE : 2477-3786

1. Pendahuluan

Upaya penyembunyian informasi (*message*) tidak hanya dapat dilakukan dengan mengubah pesan tersebut menjadi pesan yang tidak bisa dipahami, tapi dapat dilakukan juga dengan menyisipkan pesan tersebut ke dalam media lain (Morkel dkk,2005). Sehingga orang tidak akan curiga terhadap pesan yang dikirimkan, karena pesan tersebut tidak terlihat. Yang terlihat hanyalah media penampung pesan tersebut. Teknik penyisipan pesan dalam media lain ini dinamakan Steganografi (Roy dkk, 2013).

Terdapat beberapa penelitian pada metode steganografi yang dalam teknik penyisipanya menggunakan transformasi *Discrete Cosine Tranform* DCT (Walia dkk, 2010), secara umum proses penyisipan pesan pada kawasan dct dilakukan dengan menyisipkan pesan rahasia pada LSB diarea koefisien DCT hasil kuantisasi secara sekuensial (Reddy dkk, 2011). Berbeda pada kebanyakan proses steganografi pada kawasan dct, pada steganografi dct dengan metode F5 menggunakan metode baru dalam cara penggantian LSB pada koefisien DCT dengan data pesan, dimana F5 tidak mengganti koefisien DCT namun mengurangi bit koefisien DCT dengan data pesan (Fridrich dkk, 2002).

Konsep penyisipan pesan pada citra sebenarnya adalah proses mengganti nilai bit pesan dengan nilai pixel yang ada pada citra sedemikian sehingga pesan yang disisipkan mampu tersamarkan dalam nilai pixel citra, sehingga dapat memanipulasi keterbatasan visual manusia (Patel dan Dave, 2012), secara umum proses penyisipan pesan pada kawasan dct dilakukan dengan menyisispkan pesan rahasia pada LSB diarea koefisien DCT hasil kuantisasi (Westfeld, 2001).

Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor salah satunya yaitu kualitas (fidelity) yaitu dimana mutu atau kualitas citra penampung setelah ditambahkan pesan tidak jauh berbeda dengan kualitas citra penampung sebelum ditambahkan pesan dan yang kedua adalah ketahanan (robustness) yaitu data yang disembunyikan harus tahan terhadap berbagai operasi manipulasi atau penambahan image distortion yang dilakukan pada citra stego (Murwantini, 2007).

Masalah yang timbul adalah apakah algoritma dct baik atau layak untuk digunakan dalam steganografi. Oleh karena itu selain akan dilakukan penerapan proses steganografi pada kawasan dct juga akan dilakukan pengujian. Pengujian tersebut meliputi pengujian terhadap kualitas citra apakah setelah disisipkan pesan mengalami penurunan kualitas atau tidak dan ketahanan citra stego untuk melihat apakah pesan yang disisipkan masih dapat diekstrak meskipun gambar mengalami beberapa perubahan.

2. Pembahasan

Pada format gambar JPEG, masing-masing komponen warna menggunakan transformasi DCT (*discrete cosine transform*) untuk mentransformasi blok-blok gambar 8x8 pixel kedalam 64 masing-masing koefisien DCT (Huang dkk,2012). Koefisien-koefisien DCT tersebut adalah F(u,v) dari suatu blok 8x8 dari citra pixel f(x,y) dinyatakan pada Persamaan (1):

$$\left[F(u,v) = \frac{1}{4} C(u)C(v) \left[\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \right] \right]$$

…… (1)

Pada persamaan 1 F(u,.v) berbentuk matriks 2-dimensi 8x8 dengan keterangan:
$u,v,x,y = 0,1,2,\ldots,7$
x,y adalah koordinat spatial dari domain asal.
u,v adalah koordinat frekuensi pada domain transformasi atau koefisien-koefisien DCT.
$C(u),C(v) = 1/\sqrt{2}$ Untuk u,v = 0
C(u), C(v) = 1, untuk nilai lainya.

Selanjutnya adalah kuantisasi, proses kuantisasi diterapkan pada keluaran proses DCT. Kuantisasi dilakukan dengan cara membagi keluaran proses DCT dengan suatu nilai yang ditetapkan dalam matriks kuantisasi (Westfeld, 2001). Proses kuantisasi dilakukan dengan Persamaan (2) :

$$F_Q(u,v) = Round\left(\frac{F[u,v]}{q[u,v]} \right)$$ ……(2)

Dimana:
(q[u,v]) = tabel kuantisasi.
Gambar 1 merupakan nilai kuantisasi komponen luminance dan chrominance standar JPEG.

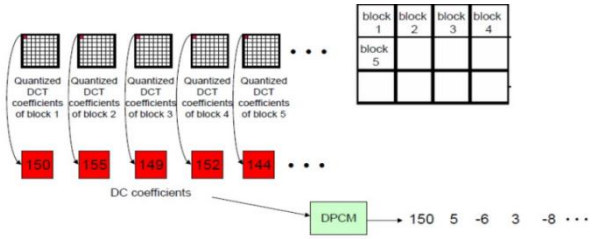
16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Gambar 1. Kuantisasi *luminance* dan *chrominance*

LSB dari koefisien DCT yang terkuantisasi digunakan sebagai bit-bit redundant untuk menyisipkan pesan rahasia (Walia dkk, 2010). Pada tahap ini, koefisien DC dari tiap blok disatukan untuk memasuki tahap entropy coding, teknik DPCM (differential pulse code modulation) digunakan karena nilai-nilai koefisien DC antar blok tidak berbeda jauh (Morkel dkk, 2005). Gambar 2 menjelaskan proses DPCM yang diterapkan pada koefisien DC.

ISSN PRINT : 2303-500X
ISSN ONLINE : 2477-3786



Gambar 2. *Differential Pulse Code modulation*

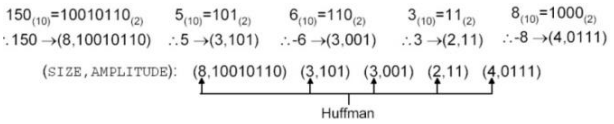
A. Entropy Coding pada Koefisien DC

Koefisien DC yang sudah melalui tahap DPCM kemudian dikompresi menggunakan metode huffman, tetapi sebelumnya deretan angka tersebut akan dirubah bentuknya menjadi pasangan-pasangan (size,amplitude) dimana size menyatakan jumlah bit yang diperlukan untuk merepresentasikan jumlah angka DPCM dan amplitude menyatakan angka tersebut dalam bit (Reddy dan Reddy, 2011). Berikut Tabel 1 yang menyatakan hubungan antara size dan amplitude-nya:

Tabel 1 Hubungan Nilai size dan amplitude-nya

Size	Amplitude Number	Number
1	0,1	-1,1
2	00,01,10,11	-3-2,2,3
3	000,...,011,100,...,111	-7,...,-4,4,...,7
4	0000,...,0111,1000,...,1111	-15,...,-8,8,...,15
....	....	...
10	0000000000,...,0111111111,1000000000,...,1111111111	-1023,...,-512,512,...,1023

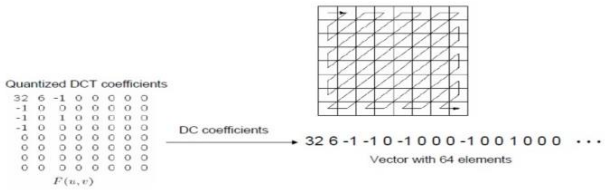
Pada Gambar 3 merupakan contoh proses *huffman* pada koefisien DC.



Gambar 3. Proses *entropy encoding* pada koefisien DC

B. Zig-zag Scanning

Pada proses *zig-zag scanning* ini koefisien DCT terkuantisasi yang bernilai nol cenderung terbaca secara berurutan. Gambar 4 merupakan contoh proses zig-zag scan.



Gambar 4. Proses *zig-zag scan*

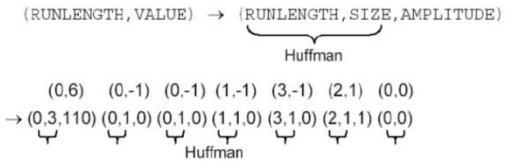
C. Run Length Code

RLC (*Run Length Code*) yaitu proses serangkaian simbol yang berurutan dikodekan menjadi suatu kode yang terdiri dari simbol tersebut dan jumlah pengulanganya. RLC mempunyai dua simbol yaitu:

Symbol 1	Symbol 2
(RUNLENGTH, SIZE)	(AMPLITUDE)

D. Entropy Coding pada Koefisien AC

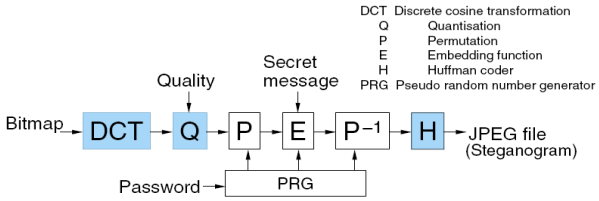
AC yang sudah melalui tahap RLC juga dikompresi menggunakan kompresi *huffman*, pasangan-pasangan sebelumnya diubah lagi menjadi pasangan-pasangan (runlength, size, amplitude). Dalam hal ini yang mengalami kompresi huffman hanya runlength dan size-nya seperti pada koefisien DC. Lebih lanjut dijelaskan dalam Gambar 5 (Morkel dkk, 2005)



Gambar 5. Proses *Entropy Encoding* pada koefisien AC

E. Steganografi pada domain DCT

Proses penyisipan pesan dalam citra dapat dilihat dalam Gambar 6



Gambar 6. Proses penyisipan pesan .(Westfeld, 2001)

Dalam proses embedding pesan dalam citra ini pertama-tama dimasukkan (input) file citra. Setelah itu masukkan password atau shared secret sebagai kunci steganografi. Setelah itu ambil pixel dari citra tersebut, kemudian lakukan perhitungan DCT sesuai dengan Persamaan (1) untuk memperoleh koefisien DCT atau domain frekuensinya serta hasil tabel kuantisasinya. Inisialisasi PRNG dengan password yang telah dimasukkan. Setelah itu dilakukan permutasi pada koefisien DCT, lalu dilakukan proses embedding bit data pesan ke dalam koefisien DCT yang telah dipermutasikan. Setelah proses embedding selesai, lakukan invers permutasi terhadap koefisien DCT yang telah disisipkan pesan. Sehingga didapatkan hasil berupa stego image. Selanjutnya dilakukan huffman coding untuk mengkompresi citra sehingga output citra atau stego image merupakan citra dengan format JPEG (*.jpg).

F. Kapasitas Pesan pada steganografi dct

Perhitungan kapasitas pesan yang dapat disisipkan pada steganografi F5 dilakukan dengan menghitung nilai total koefisien DCT dikurangi dengan koefisien DC, koefisien DCT bernilai nol, serta koefisien DCT bernilai nol hasil proses shrinked. Shrinked terjadi ketika dalam

proses pengurangan atau penambahan koefisien DCT dengan data pesan, nilai koefisien DCT menjadi nol, proses Shrinked terjadi akan terjadi tergantung dari pesan yang akan disisipkan, sehingga dalam hal ini kapasitas pesan yang dihitung adalah perkiraan kapasitasnya. Formula untuk menghitung kapasitas pesan pada steganografi kawasn dct menurut (Sajedi dan Zamjad, 2012) yaitu:

$$Kapasitas=\#DCT_{(total)}-\#DCT_{(-1)}-\#DCT_{(1)}-DCT_{(0)}-\#DCT_{(dc)}$$

Dimana #DCT(total) =Jumlah total koefisien dct
#DCT(-1) =Jumlah koefisien dct bernilai -1
#DCT(1) =Jumlah koefisien dct bernilai 1
#DCT(0) =Jumlah koefisien dct bernilai 0
#DCT(dc) =Jumlah koefisien dct bernilai dc

G. Entropi Citra

Entropi citra merupakan salah satu fitur yang dapat dihitung pada matrik GLCM (*Gray Level Co-occurrence matrix*). Matrix GLCM dihitung dari nilai pixel yang berpasangan dan memiliki nilai intensitas tertentu. Misalkan *d* adalah jarak antara dua pixel yaitu (x1,y1) dan (x2,y2) dan Θ tetha didefinisikan sebagai sudut antara keduanya, maka matrix GLCM merupakan distribusi spasial dari $P_{d\ \Theta}$ (i,j). Fitur Entropi sendiri merupakan salah satu fitur yang digunakan untuk mengukur kompleksitas atau keacakan suatu citra. Nilai entropi akan bernilai tinggi ketika citra tidak seragam, sebaliknya akan bernilai rendah ketika kompleksitas citra semakin seragam (Sajedi dan Jamzad, 2012).

H. Pengujian Kualitas Fidelity (Stego Image)

Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE (Mean Square Error). MSE adalah nilai error kuadrat rata-rata antara citra cover dengan stego image, secara matematis dapat dirumuskan seperti pada Persamaan (3)

$$MSE = \frac{1}{M\,N}\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(x,y)-I'(x,y)]^2 \quad \ldots\ldots\ldots\ldots(3)$$

Dimana :
MSE = Nilai Mean Square Error citra steganografi
M = Panjang citra stego (dalam pixel)
N = Lebar citra stego (dalam pixel)
I(x,y) = nilai piksel dari citra cover
I'(x,y) = nilai piksel pada citra stego

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan Persamaan (4) :

$$PSNR = 10\log_{10}\left(\frac{MAXi^2}{MSE}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Dimana:
MSE = nilai MSE.
MAXi= nilai maksimum dari pixel citra yang digunakan Semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi. Nilai PSNR yang wajar pada perbandingan dua berkas citra adalah 30-50 dB (Fridrich, 2001).

I. Hasil dan Pembahasan

Berikut adalah hasil perhitungan kapasitas pesan dari algoritma steganografi DCT F5 pada citra dengan dimensi 128 x 128 pixel.

1. Hubungan antara kompleksitas Citra dengan Kapasistas Pesan

Tabel 2 menunjukkan perbandingan kapasitas penyisipan citra asli berdasarkan kompleksitas citra, terlihat kapasitas citra cenderung meningkat seiring meningkatnya kompleksitas citra.

Tabel 2. Hubungan antara kompleksitas Citra dengan kapasitas Pesan

No	Nama Citra Ori	Nilai *Entropy*	Kapasitas Penyisipan (bits)
1	Low1.jpg	5.297	6814
2	Low2.jpg	5.359	6897
3	Low3.jpg	6.018	7816
4	Middle1.jpg	7.450	6284
5	Middle2.jpg	7.685	6834
6	Middle3.jpg	7.893	6463
7	High1.jpg	8.102	8380
8	High2.jpg	8.494	8252
9	High3.jpg	8.701	9264
10	Veryhigh1.jpg	8.809	8978
11	Veryhigh2.jpg	8.928	11049
12	Veryhigh3.jpg	9.265	12047
Rata-rata			**8256.5**

2. Hubungan antara kompleksitas citra dengan kualitas citra

Tabel 3 menunjukkan perbandingan nilai PSNR dan MSE pada steganografi DCT, nilai yang didapatkan merupakan perbandingan antara citra asli dengan citra stego.

Tabel 3. Perbandingan Nilai PSNR dan MSE citra asli dengan citra stego

No	Nama Citra Asli	PSNR (db)	MSE
1	Low1.jpg	32.81	104.41
2	Low2.jpg	34.36	91.79
3	Low3.jpg	34.78	94.83
4	Middle1.jpg	35.31	96.58
5	Middle2.jpg	35.40	105.79
6	Middle3.jpg	36.12	99.72
7	High1.jpg	36.61	99.40
8	High2.jpg	37.04	99.71
9	High3.jpg	37.37	102.94

10	Veryhigh1.jpg	38.52	82.13
11	Veryhigh2.jpg	38.52	82.28
Rata-Rata		**36.07**	**96.32**

Berdasarkan kompleksitas citra pada steganografi dct diketahui semakin tinggi kompleksitas citra maka semakin baik nilai PSNR dan MSE yang didapatkan.

3. Hubungan antara Ukuran Pesan dengan Kualitas Citra

Tabel 4 menunjukan data nilai PSNR dan MSE pada citra Middle, terlihat nilai PSNR semakin menurun saat ukuran pesan yang disisipkan semakin tinggi, begitu sebaliknya dengan nilai MSE semakin naik saat ukuran pesan semakin besar.

Tabel 4. Perbandingan kualitas citra berdasarkan ukuran pesan

No	Nama Citra Asli	Ukuran Pesan(bytes)	PSNR (db)	MSE
1	Middle1.jpg	2	42.846	30.383
2	Middle2.jpg	4	42.840	30.430
3	Middle3.jpg	6	42.827	30.520
4	Middle4.jpg	8	42.809	30.647
5	Middle5.jpg	10	42.805	30.671
6	Middle6.jpg	12	42.784	30.819
7	Middle7.jpg	14	42.761	30.988
8	Middle8.jpg	16	42.745	31.100
9	Middle9.jpg	18	42.748	31.076
10	Middle10.jpg	20	42.743	31.115
Rata-Rata			**42.79**	**30.77**

4. Uji Ketahanan

Berikut adalah hasil pengujian berdasarkan ketahanan citra pada proses steganografi DCT pada 10 citra digital berukuran 128 x 128 piksel dengan format jpg.

a. Efek Rotasi

Pada Tabel 5 merupakan data hasil proses ektraksi pesan pada steganografi DCT setelah pemberian efek rotasi vertikal. Dari hasil yang didapatkan tidak ada satupun file pesan yang mampu dibaca kembali.

Tabel 5. Hasil Ektraksi DCT setelah efek rotasi

No	Nama Citra Asli	Hasil ektraksi (bit)
1	Low1stegoRotation.jpg	Null
2	Low2stegoRotation.jpg	Null
3	Low3stegoRotation.jpg	Null
4	Middle1stegoRotation.jpg	Null
5	Middle2stegoRotation.jpg	Null
6	Middle3stegoRotation.jpg	Null
7	High1stegoRotation.jpg	Null
8	High2stegoRotation.jpg	Null
9	Veryhigh1stegoRotation.jpg	Null
10	Veryhigh2stegoRotation.jpg	Null

b. Efek Penskalaan

Tabel 6 merupakan data hasil proses ektraksi pesan pada steganografi DCT setelah pemberian efek penskalaan menjadi 150 pixel pada sisi panjang dan sisi lebar . Dari hasil yang didapatkan tidak ada satupun file pesan yang mampu dibaca kembali.

Tabel 6. Hasil Ektraksi DCT setelah efek penskalaan

No	Nama Citra Asli	Hasil ektraksi(bit)
1	Low1stegostegoScalling.jpg	Null
2	Low2stegScalling.jpg	Null
3	Low3stegoScalling.jpg	Null
4	Middle1stegScalling.jpg	Null
5	Middle2stegoScalling.jpg	Null
6	Middle3stegoScalling.jpg	Null
7	High1stegoScalling.jpg	Null
8	High2stegoScalling.jpg	Null
9	Veryhigh1stegoScalling.jpg	Null
10.	Veryhigh2stegoScalling.jpg	Null

3. Kesimpulan

a) Steganografi dapat digunakan untuk komunikasi rahasia tanpa mencurigakan karena media penyimpanannya berupa gambar digital yang masih dapat dilihat dengan mata tanpa ada suatu kejanggalan.
b) Kualitas citra stego yang dihasilkan oleh metode steganografi dct tidak jauh berbeda dengan citra aslinya, terlihat dari hasil pengujian rata-rata nilai PSNR yang didapatkan berkisar diatas nilai 30 db.
c) Steganografi pada kawasan DCT ini memiliki kelemahan yaitu citra yang telah disisipi pesan tidak tahan terhadap perubahan. Karena setelah dilakukan beberapa perubahan terhadap citra diperoleh hasil bahwa pesan tidak dapat lagi diekstrak. Hal ini disebabkan adanya perubahan warna tiap-tiap piksel citra

DaftarPustaka

Fridrich, J.,Goljan, M dan Hogea, D., 2002, *Steganalysis of JPEG Images Breaking The Algorithm*, http://www.ws.binghamton.edu/fridrich/Research/f5.pdf, diakses 13 Januari 2013.

Huang,F., Huang, J., dan Shi,Y.Q., 2012, New Channel Selection Rule for JPEG Steganography, *IEEE Transaction On Information Forensics and Security.,* Vol. 7, No. 4, pp. 1181-1191.

Morkel, T.,Eloff, J.H.P dan Olivier, M.S., 2005, An Overview of Image Steganography, *Proceedings of the Fifth Annual Information SecuritySouth Africa Conference*, Vol 2, No 3, June, pp.103-112.

Murwantini, S., 2007, Kajian Penyimpanan Data pada Media Citra (Steganografi) menggunakan Metode DCT, *Tesis*, Program Studi Teknik Elektro UGM,Yogyakarta.

ISSN PRINT : 2303-500X
ISSN ONLINE : 2477-3786

Patel,H., dan Dave, P., 2012, Steganography Technique Based on DCT Coefficients , *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, Issue 1, Jan-Feb 2012, pp.713-717.

Reddy,V.L., Subramanyam, A., dan Reddy,C.P., 2011, Steganography + JPEG, *International Journal of Computer Graphics.*, Vol. 2, no. 1, pp. 31-42.

Roy,R., Changder,S. Sarkar, A. dan Debnath,N.C, 2013, Evaluating Image Steganography Techniques: Future Research Challenges, *Jurnal of IEEE*, pp 309-314.

Sajedi, H dan Jamzad, M., 2012, BSS: Boosted steganography scheme with cover image preprocessing, *International Journal of Expert Systems with Applications available at ScienceDirect*, pp. 7703-7710.

Walia, E., Jain, P. dan Navdeep., 2010, An Analysis of LSB & DCT based Steganography, *Global Journal of Computer Science and Technology*, Vol 10, Issue 1 (Ver 1.0), 4-8.

Westfeld, A., 2001, F5-A Steganographic Algorithm: High capacity despite better steganalysis, *Proc. 4th International Workshop on Information Hiding* , Springer, vol. 2137, pp. 289-302.