**BAB 2**

**LANDASAN TEORI**

**2.1 Tinjauan Pustaka**

Tinjauan pustaka ini merupakan rangkuman dari beberapa jurnal yang berkaitan dengan Tugas Akhir yang dibuat oleh penulis. Bagian ini berisi tentang penelitian yang telah dilakukan oleh penulis sebelumnya, yaitu steganografi pada citra.

Steganografi pada citra pernah digunakan pada beberapa penelitian, seperti pada penelitian Archana, et.al (2013) menawarkan teknik steganografi menempatkan pesan tersembunyi dalam domain frekuensi. Tidak seperti pendekatan domain ruang, pesan tersembunyi ditanamkan dalam koefisien frekuensi yang dihasilkan oleh *Discrete Wavelet Transform* (DWT). Algoritma kriptografi digunakan untuk mengubah pesan tersembunyi dalam format yang tak dapat dibaca sebelum ditanamkan. Algoritma ini memungkinkan pesan terhindar dari pencurian maupun hancur akibat ketidaksengajaan pengguna internet sehingga dapat memberikan jaminan kepuasan keamanan yang diharapkan. Algoritma Blowfish digunakan untuk melakukan enkripsi dan dekripsi pesan teks menggunakan *secret-key block cipher*. Algoritma blowfish merupakan evolusi pengembangan dari DES, 3DES, dan lain-lain yang didesain untuk meningkatkan kemanan dan performa. Adapun algoritma ini menggunakan *variable key* hingga ukuran 448 bit.

Penelitian lain yang dilakukan oleh Chen dan Lin (2006) adalah mengenai penelitian terhadap teknik steganografi baru yang mengintegrasikan pesan rahasia ke dalam *frequency domain*. Merujuk pada permintaan *user* terhadap kapasitas integrasi pesan rahasia dan kualitas citra, algoritma yang mereka ajukan dibagi kedalam dua mode dan lima kasus. Namun idak seperti pendekatan *space domain*, pesan rahasia diintegrasikan ke dalam *high frequency* *coefficients* yang dihasilkan dari *Discrete Wavelet Transform*. *Coefficients* di dalam *low frequency subband* tidak akan diubah untuk meningkatkan kualitas citra. Sebelum pesan rahasia diintegrasikan ke dalam citra, akan dilakukan beberapa proses matematika dasar. Operasi matematika tersebut dan juga *table-mapping* akan melindungi pesan rahasia tersebut dari *user* yang berniat untuk mencuri atau menghancurkan enkripsi, sehingga tujuan akhir dapat tercapai, yakni perasaan aman dan terlindungi dari serangan hacker.

Penelitian Bhattacharyya & Sanyal (2012) yang berjudul “A Robust Image Steganography using DWT Difference Modulation (DWTDM)” menggunakan DWT, metode baru dalam teknik mengubah domain citra stenografi DWT *Difference Modulation* (DWTDM) disajikan dimana data rahasia tertanam dalam perbedaan koefisien DWT yang berdekatan. Rentang dinamis dari perbedaan DWT dipertimbangkan, sementara ekstraksi data yang menghasilkan teknik *stegano* yang efisien dan kuat yang dapat menghindari berbagai serangan terhadap *cover-image* dan bekerja dengan baik.

Penelitian lain juga dilakukan oleh Chawla dan Sukla (2014), dalam penelitiannya, mereka menawarkan modifikasi skema steganografi yang aman dan berkapasitas tinggi dalam menyembunyikan citra rahasia berukuran besar dalam citra pelindung berukuran kecil. Rotasi matriks diterapkan untuk mengacak citra rahasia. Adapun DWT diterapkan pada kedua citra dan diikuti oleh operasi *alpha blending*. Kemudian teknik *Inverse* DWT (IDWT) akan diterapkan untuk mendapatkan citra stego. Mereka telah meneliti performa dari skema yang digunakan dengan membandingkan berbagai kualitas citra stego dan citra pelindung serta membandingkannya dengan metode lama seperti *Arnold Transform*. Hasilnya menunjukkan bahwa algoritma modifikasi steganografi yang mereka tawarkan memiliki tingkat keamanan lebih tinggi serta memiliki *perceptual invisibility* yang lebih baik.

Penelitian lain juga dilakukan oleh Banik dan Bandyopadhyay (2013) yaitu sebuah *wavelet* merupakan gelombang kecil yang berosilasi dan meluruh dalam domain waktu. Analisis wavelet menguntungkan karena melakukan analisis lokal dan analisis multi-resolusi. Untuk menganalisis sinyal pada frekuensi yang berbeda dengan resolusi yang berbeda disebut analisis multi-resolusi (MRA). Analisis *wavelet* dapat dari dua jenis: kontinyu dan diskrit. Dalam penelitian mereka, teknik diskrit transformasi *wavelet* telah digunakan untuk citra steganografi. Metode ini mengubah objek dalam domain *wavelet*, memproses koefisien dan kemudian melakukan transformasi *wavelet* balik untuk mewakili format asli dari objek *stego*.

Penelitian lain juga dilakukan oleh Barve, Nagaraj dan Gulaban (2011), pada penelitiannya mereka menawarkan metode *Biometric*. Fitur *biometrik* yang digunakan untuk mengimplementasikan Steganografi adalah kulit wilayah nada citra. Metode yang diusulkan memperkenalkan metode embedding yang baru. Data rahasia dalam bagian kulit citra seseorang, karena tidak banyak sensitif terhadap HVS (*Human Visual System*). Daerah kulit ini menyediakan lokasi yang aman baik untuk data bersembunyi. Jadi, pertama deteksi kulit dilakukan dalam citra sampul dan kemudian embedding data rahasia akan dilakukan di *domain* DWT yang memberikan kinerja lebih baik daripada metode DCT ketika dikompresi. Metode biometrik dari steganografi ini meningkatkan ketahanan dari metode yang ada.

Dalam penelitian Shah, Kaul,dan Dhande (2012) menyajikan steganografi citra yang menggabungkan *Discrete Wavelet Transform* (DWT), *Least significant bit* (LSB) dan teknik enkripsi citra mentah untuk meningkatkan keamanan pesan rahasia. Awalnya, algoritma DWT digunakan untuk mengubah citra dari domain spasial ke domain frekuensi. Kemudian kita mengenkripsi pesan kita menggunakan *Data Encryption Standard* (DES). Terakhir mereka menanamkan bit rahasia ke dalam citra *cover* untuk mendapatkan citra *stegano* menggunakan LSB.

Penelitian mengenai steganografi dilakukan juga oleh Parul, Manju dan Rohil (2014), dimana mereka menyajikan pendekatan baru untuk steganografi pada citra menggunakan DWT. Citra *cover* dibagi menjadi frekuensi tinggi dan rendah. Data tertanam ke frekuensi *sub-band* tinggi. *Transformasi Arnold* digunakan untuk meningkatkan keamanan.

Penelitian yang lain juga dilakukan oleh Kumar dan Padmajam (2014), mereka menyajikan cara terbaru untuk mengambil data rahasia terenkripsi yang tertanam dalam citra *grayscale* guna menghasilkan tingkat keamanan data berita yang lebih baik pada ruang lingkup komunikasi yang tidak aman. Kriptografi dan steganografi merupakan dua teknik yang saling terkait erat dan digunakan dalam sistem yang ditawarkan pada penelitian mereka. Kriptografi diterapkan dengan mengubah suatu catatan rahasia menjadi *cipher* yang tidak dapat dikenali. Steganografi kemudian diterapkan dengan implementasi metode *double-stegging* untuk mereprarasi data yang telah dienskripsi tadi menjadi citra *cover* yang kerahasiannya masih tetap terjaga.

Menurut Pathil dan Chandel (2014), steganografi adalah ilmu komunikasi yang aman yang telah menerima banyak perhatian dari masyarakat ilmiah baru-baru ini. Empat tujuan utama steganografi adalah: *indefectibility*, keamanan, *embedding payload*, dan *robustness*. Namun tidak menjamin keamanan total. Steganografi merupakan ilmu embedding ke dalam citra *cover* berupa teks, video, dan citra (*payload*) tanpa menyebabkan perubahan signifikan secara statistik dengan citra *cover*.

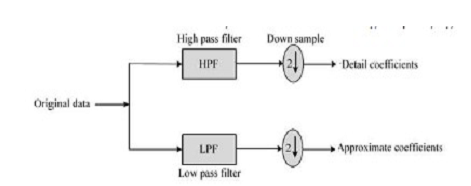
* 1. **Landasan Teori**
     1. **Steganografi**

Steganografi merupakan teknik dalam keamanan informasi yang digunakan untuk menyembunyikan informasi tersembunyi dalam media penyedia (*carrier*) normal seperti citra digital, audio, video, dan lain-lain. Steganografi berasal dari kata Yunani dan secara literal berarti “tulisan rahasia atau tersembunyi”. (Suchitra 2013) steganografi adalah teknik memanfaatkan celah kelemahan sistem visual manusia sebagai keunggulannya. Pihak lain tak dapat dengan mudah menemukan pesan yang tersimpan dalam citra. Tujuan utama dari steganografi adalah menyembunyikan data dari pandangan penyerang dan mengamankan transmisi data melalui citra dari sumber menuju tujuan. Steganografi terbentuk dari dua macam yaitu pesan digital atau sering disebut dengan pesan (*message*) yang akan disisipkan dan media tempat penyisipan. Media tempat penyisipan dapat berupa teks, citra, audio, dan video. Penyembunyian pesan yang berupa teks maupun citra ke dalam citra digital akan mempengaruhi kualitas citra tersebut.

* + 1. **Discrete Wavelet Transform (DWT)**

Menurut Dinesh (2012)*Discrete Wavelet Transform* (DWT) merupakan metode yang dapat membagi informasi dari suatu citra menjadi pendekatan dan detail sinyal. Adapun LL *band*meliputi koefisien *low pass* dan pendekatan terhadap suatu citra serta detail sub signal lainnya yang menunjukkan rincian vertikal, horisontal, atau diagonal atau perubahan di dalam suatu citra**.**

Metode DWT merepresentasikan citra sebagai jumlah dari fungsi wavelet, yang dikenal sebagai wavelets, dengan lokasi dan skala yang berbeda. Metode DWT merepresentasikan data dalam himpunan koefisien *high pass* (detil) dan *low pass* (pendekatan). Data masukan diteruskan melalui himpunan filter *low pass* dan *high pass*. Hasil keluaran filter high pass dan low pass diperkecil sampelnya menjadi dua. Hasil keluaran filter *low pass* merupakan koefisien pendekatan dan hasil keluaran filter *high pass* merupakan koefisien detil. Adapun mata manusia kurang sensitif terhadap sinyal frekuensi tinggi.



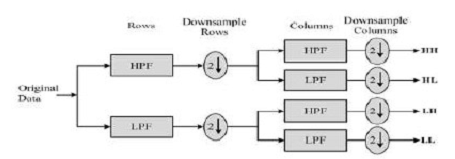
Gambar 2.1.Blok diagram terusan 1-D DWT

(Archana., et al2013)

Mata manusia pada umumnya menemukan detil secara lebih baik pada area lebih kecil dan hanya mengingat keseluruhan area yang diperbesar. Prosedur satu dimensi (1-D) ditunjukkan pada gambar 2.1.

Pada kasus 2-D DWT, data masukan diteruskan melalui himpunan filter low pass dan high pass pada dua arah, yaitu baris dan kolom. Hasil keluarannya kemudian diperkecil menjadi 2 sampel pada masing-masing arah sebagaimana dalam kasus 1-D DWT. Sebagaimana yang ditunjukkan pada gambar 2.2, hasil keluaran didapatkan dari himpunan 4 koefisien LL, HL, LH, dan HH. Huruf pertama merepresentasikan transformasi pada baris, sedangkan huruf kedua merepresentasikan transformasi pada kolom.

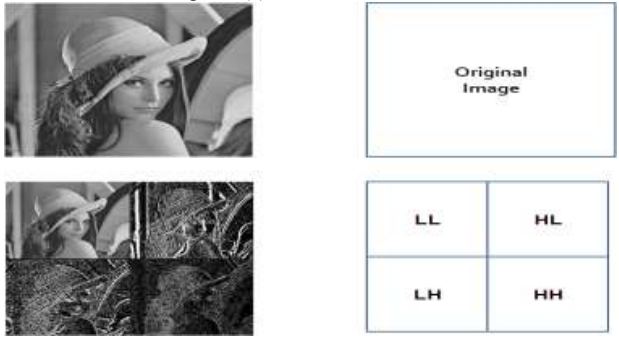
Alfabet L berarti *low pass signal* dan H berarti *high pass signal*. Sinyal LH berarti *low pass* *signal* pada baris dan *high pass* pada kolom. Oleh karena itu, sinyal LH memuat elemen horisontal. Demikian halnya dengan HL dan HH, dimana masing-masing sinyal tersebut memuat elemen vertikal dan diagonal.



Gambar 2.2.Blok diagram terusan 2-D DWT

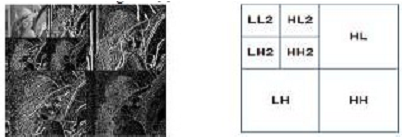
(Archana., et al 2013)

Berikut ini adalah gambar ilustrasi hasil keluaran 1D DWT dan 2D DWT:



Gambar 2.3.Ilustrasi 1D DWT

(Archana., et al 2013)



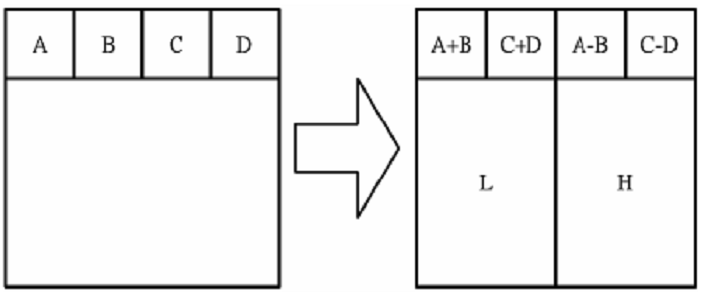
Gambar 2.4. Ilustrasi 2D DWT

(Archana., et al 2013)

**2.2.2.1 Haar DWT**

Transformasi Haar-DWT merupakan bentuk DWT paling sederhana dan terdiri dari dua operasi utama : operasi horisontal serta operasi vertikal. Prosedur detil dari 2D Haar DWT dapat dijabarkan sebagai berikut :

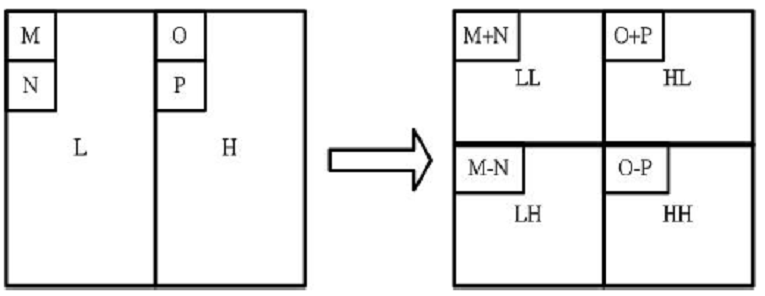
**Tahap 1** : Pertama, melakukan proses scan terhadap *pixel* dari kiri ke kanan secara horisontal. Kemudian lakukan operasi penjumlahan dan pengurangan pada *pixel* disebelahnya (*neighbouring pixel*). Simpan hasil penjumlahan disebelah kiri dan hasil pengurangan disebelah kanan seperti yang ditunjukkan pada gambar 2.5. Ulangi kembali operasi tersebut hingga seluruh baris berhasil diproses. Hasil penjumlahan *pixel* merepresentasikan bagian berfrekuensi rendah (disimbolkan dengan L) dan hasil pengurangan merepresentasikan bagian berfrekuensi tinggi dari citra asli (disimbolkan dengan H).



Gambar 2.5.Operasi Horisontal pada metode DWT

(Archana., et al 2013)

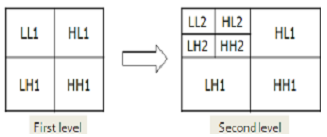
**Tahap 2** : Kedua, lakukan proses *scan* *pixel* dari atas ke bawah secara vertikal. Kemudian lakukan operasi penjumlahan dan pengurangan pada *pixel* disebelahnya (*neighboouring* *pixel*) dan simpan hasil penjumlahan pada bagian atas dan hasil pengurangan pada bagian bawah seperti yang ditunjukkan pada gambar 2.6



Gambar 2.6.Operasi Vertikal pada metode DWT

(Archana., et al 2013)

Ulangi kembali operasi tersebut hingga seluruh kolom berhasil diproses. Terakhir akan didapatkan 4-sub-himpunan yang disimbolkan dengan LL, HL, LH, dan HH. Adapun sub-himpunan LL merupakan bagian berfrekuensi rendah karena itu memiliki kemiripan dengan citra asli. Keseluruhan prosedur yang dijabarkan diatas tersebut disebut 1D Haar-DWT. Proses 2D DWT dengan mengaplikasikan Haar DWT pada bagian LL. Gambar 2.7 menunjukkan proses 2D DWT.



Gambar 2.7. Proses 2D DWT

(Archana., et al 2013)

* + 1. ***Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR)**

*Peak Signal to Noise Ratio* (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan decibel (dB). Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan *Mean Square Error* (MSE). Adapun MSE adalah nilai error kuadrat rata-rata antara citra *cover* dengan citra steganografi, secara matematis dapat dirumuskan sebagai berikut:

 [2.1]

Diketahui:

MSE = Nilai Mean Square Error citra steganografi

M = Panjang citra stego (dalam *pixel*)

N = Lebar citra stego (dalam *pixel*)

I (x,y) = nilai *pixel* dari citra *cover*

K(x,y) = nilai *pixel* pada citra stego

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan sebagai berikut :

[2.2]

Diketahui:

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 acuan PSNR bisa dikatakan baik adalah bernilai ≥ 30.

* + 1. ***Joint Photographic Experts Group* (JPEG)**

*Joint Photographic Experts Group* merupakan skema kompresi citra bitmap. Adapun Kusrianto (2008) mengemukakan bahwa jpeg adalah format untuk menyimpan *image* atau citra digital *full color* 24 bit atau biasa disebut dengan istilah *true color*. Format ini dipakai dikalangan fotografer maupun desainer webpage karena bobot filenya relative kecil sehingga mudah ditampilkan pada halaman web.

Keuntungan lain dari format JPEG adalah dapat diterima pada hampir semua program-program komputer, baik yang berbasis Windows maupun Apple Macintosh. Adapun kelemahan dari format JPEG ini adalah kompresi citra pada format ini mempengaruhi kualitas citra itu sendiri. Apabila di edit dan di simpan kualitas citra berkurang dan semakin sering melakukan edit, kualitas citra akan menurun terus. Citra JPEG ini mengorbankan kualitas demi ukuran citra yang kecil.

* + 1. **Bitmap**

Bitmap adalah representasi dari citra grafis yang terdiri dari susunan titik (*pixel*) yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu bit data (untuk citra hitam putih) atau lebih (untuk citra berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam citra ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 800×600).

Citra bitmap sangat bergantung pada resolusi. Jika citra diperbesar maka citra akan tampak kurang halus atau pecah, sehingga mengurangi detailnya. Selain itu citra bitmap akan mempunyai ukuran file yang lebih besar. Semakin besar resolusi citra akan semakin besar pula ukuran filenya.

Untuk menampilkan citra bitmap pada monitor atau mencetaknya pada printer, komputer menterjemahkan bitmap ini menjadi *pixel* (pada layar) atau titik tinta (pada printer). Beberapa format file bitmap yang populer adalah BMP, PCX dan TIFF.

Pada penelitian ini penulis menggunakan bitmap berformat BMP yang memiliki karakteristrik yang berlawanan dengan format JPEG. Jika pada citra JPEG setiap di edit mengalami penurunan kualitas, lain halnya dengan citra berformat BMP apabila di edit tidak mengalami penurunan kualitas citra. Beda dengan JPEG, citra berformat BMP memiliki ukuran citra yang lebih besar dan memiliki kualitas citra lebih baik.

.

* + 1. ***Portable Netwok Graphics* (PNG)**

*Portable Netwok Graphics* merupakan format standar terbuka yang didukung oleh W3C dan IETF. Mulyanta (2006) mengemukakan bahwa PNG bukan merupakan format baru karena telah dikembangkan pada tahun 1995 untuk mengganti format GIF (*Graphics Interchange Format*) dan format TIFF (*Tagged Image File Format*).

PNG adalah format citra yang sangat baik untuk grafis internet, karena mendukung transparansi didalam perambah (*browser*) dan memiliki keindahan tersendiri yang tidak bisa diberikan GIF atau bahkan JPG. Bisa disebut sebagai salah satu format yang merupakan gabungan dari format JPG dan GIF. Untuk tipe ini mampu untuk gradiasi warna.

Tipe file PNG merupakan solusi kompresi yang powerful dengan warna yang lebih banyak (24 bit RGB + *alpha*). Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (*lossles compression*). Kelebihan file PNG adalah adanya warna transparan dan *alpha*. Warna *alpha* memungkinkan sebuah citra transparan, tetapi citra tersebut masih dapat dilihat mata seperti samar-samar atau bening.

File PNG dapat diatur jumlah warnanya hingga 64 bit (*true color* + *alpha*) sampai *indexed color* 1 bit. Dengan jumlah warna yang sama, kompresi file PNG lebih baik daripada GIF, tetapi memiliki ukuran file yang lebih besar daripada JPG.

Kekurangan tipe PNG adalah belum populer sehingga sebagian browser tidak mendukungnya. Format PNG ini diperkenalkan untuk menggantikan format GIF. PNG mempunyai faktor kompresi yang lebih baik dibandingkan dengan GIF. Tetapi ada satu fasilitas dari GIF yang tidak terdapat pada PNG format yaitu dukungan terhadap penyimpanan multi format untuk keperluan animasi. Untuk keperluan pengolahan citra, meskipun format PNG bisa dijadikan alternatif selama proses pengolahan grafis namun format JPEG masih menjadi pilihan yang lebih baik.

**DAFTAR PUSTAKA**

Archana.,Vaidya., Pooja, N., Rita, K., Fegade., Madhuri, A., Bhavsar., dan Raut, P.V. (2013).” Image Steganography using DWT and Blowfish Algorithms”.IOSR Journal of Computer Engineering. Volume 8, Issue 6, PP 15-1.

Banik,B.G., dan Bandyopadhyay, S.K. (2013).” A DWT Method for Image Steganography”. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 6.

Barve,S., Nagaraj, U., dan Gulaban,R. (2011).” Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform”. International Journal of Computer Science & Communication Networks.Vol 1.

Bhattacharyya, S., dan Sanyal, G. (2012).” A Robust Image Steganography using DWT Difference Modulation (DWTDM)”. International Journal Computer Network and Information Security.Vol 7, page 27-40.

Chawla, A., dan Shukla, P. (2014).” Comparison of Arnold and Matrix Rotation Using DWT Image Steganography”. International Journal of Scientific & Engineering Research. Volume 5, Issue 2.

Chen,P.Y., dan Lin, H.J. (2006).”A DWT Based Approach for Image Steganography”. International Journal of Applied Science and Engineering. 4, 3: 275-290.

Dinesh, Y., dan Ramesh, A.P. (2012). “Efficient Capacity Image Steganography by Using Wavelets”. International Journal of Engineering Research and Applications (IJERA). Vol. 2, Issue 1, Jan-Feb 2012, pp.251-259.

Kumar, E.Y., dan Padmajam, P. (2014).” RSA Based Secured Image Steganography Using DWT Approach”. International Journal of Engineering Research and Applications. Vol. 4, Issue 8( Version 1), pp.01-04.

Kusrianto, A., (2008). ”Berkreasi Membuat Album Foto dengan PowerPoint 2007”. Elex Media Komputindo.

Mulyanta, E.S. (2005). “Menjadi Desainer Layout Andal dengan Adobe InDesign”. ANDI. hlm. 175.

Patil, S, dan Chandel, G.S. (2014).” Literature Survey on DWT Based Image Steganography”. International Journal of Computer Science and Mobile Computing. Vol.3, Issue.2, pg. 904-909. Diakses November 2014 dari

http://www.academia.edu/6772257/Literature\_Survey\_on\_DWT\_Based\_Image\_Steganography\_

Parul, Manju, dan Rohil, H. (2014).”Optimized Image Steganography using Discrete Wavelet Transform (DWT)”. International Journal of Recent Development in Engineering and Technology. Volume 2, Issue 2.

Shah, K., Kaul S, dan Dhande,M.J. (2012)” Image Steganography using DWT and Data Encryption Standard (DES)”. International Journal of Science and Research. Impact Factor.3.358.

Suchitra., M,P., dan J,R. (2013).” Image Steganography Based On DCT Algorithm for Data Hiding”. International Journal of Advanced Research in Computer Engineering & Technology. Volume 2, Issue 11.