PERBANDINGAN METODE DALAM TEKNIK STEGANOGRAFI

Patrisius Batarius[1], Martinus Maslim[2]

[1] *Jurusan Teknik Informatika Universitas Widya Mandira Kupang*
patrisbatarius@gmail.com

[2]*Program Pasca Sarjana Magister Teknik Informatika*
Universitas Atma Jaya Yogyakarta
tinusaja@yahoo.co.id

ABSTRAK

Pesan digital dapat berbentuk teks, gambar, suara, atau video. Keamanan dari suatu pengiriman pesan digital terutama pesan digital rahasia sangatlah dibutuhkan. Dengan terus berkembangnya bidang pengolahan citra digital, maka teknik keamanan bagi pesan digital pun dapat diselesaikan. Pesan rahasia digital dapat disisipkan ke dalam sebuah citra digital menggunakan sebuah teknik yang dinamakan dengan steganografi. Banyak metode yang dapat digunakan dalam teknik steganografi seperti Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) dan metode yang lainnya. Di dalam karya tulis ini akan dianalisis tentang perbandingan metode-metode yang dapat digunakan dalam teknik steganografi. Yang akan dianalisis adalah nilai dari Peak Signal to Noise Ratio (PSNR) dan waktu yang dibutuhkan oleh setiap metode terhadap proses steganografi yang dilakukan. Kesimpulan yang didapatkan dari analisis yang dilakukan adalah metode DWT mempunyai nilai PSNR yang paling besar dibandingkan kedua metode lainnya dan metode DCT memiliki waktu yang paling singkat dalam proses steganografi.

Kata Kunci : steganografi, LSB, DCT, DWT

1. PENDAHULUAN

Pesan digital dapat berbentuk teks, gambar, suara, atau video. Keamanan dari suatu pengiriman pesan digital terutama pesan digital rahasia sangatlah dibutuhkan. Hal ini ditujukan agar orang lain tidak dapat mengetahui pesan digital rahasia yang ingin disampaikan pengirim kepada penerima. Dengan terus berkembangnya bidang pengolahan citra digital, maka teknik keamanan bagi pesan digital pun dapat diselesaikan. Pesan rahasia digital dapat disisipkan ke dalam sebuah citra digital menggunakan sebuah teknik. Teknik penyisipan pesan rahasia digital ini dinamakan dengan steganografi. Steganografi merupakan teknik untuk menyisipkan atau menyembunyikan pesan rahasia digital ke dalam sebuah citra digital. Banyak metode yang dapat digunakan dalam teknik steganografi ini misalnya *Least Significant Bit* (LSB), *Discrete Wavelet Transform* (DWT), atau *Discrete Cosine Transform* (DCT). *Least Significant Bit* (LSB) merupakan metode yang digunakan dalam domain spasial sedangkan *Discrete Wavelet Transform* (DWT) dan *Discrete Cosine Transform* (DCT) merupakan metode yang digunakan dalam domain transformasi.

Dalam penelitian ini akan dianalisis perbandingan metode-metode yang dapat digunakan dalam teknik steganografi. Analisis perbandingan yang dilakukan berdasarkan nilai *Peak Signal to Signal Ratio* (PSNR) dan waktu yang dihasilkan dalam proses steganografi. PSNR merupakan nilai untuk membandingkan citra asli dengan citra hasil dari pengolahan citra digital dalam hal ini citra hasil proses steganografi. Semakin besar nilai PSNR maka nilai dari citra hasil steganografi mendekati nilai dari citra aslinya dan sebaliknya semakin kecil nilai PSNR maka nilai dari citra hasil steganografi jauh dengan nilai dari citra aslinya. Untuk waktu yang digunakan dalam proses analisis adalah waktu yang diperlukan dalam proses penyisipan pesan dan waktu yang diperlukan untuk mengekstraksi pesan yang ada di citra hasil steganografi. Tujuan dilakukan analisis ini adalah untuk mengetahui kualitas hasil yang dihasilkan dari ketiga metode ini serta untuk menghitung waktu yang dibutuhkan ketiga metode ini untuk melakukan proses steganografi.

2. TINJAUAN PUSTAKA

Teknik steganografi merupakan penelitian yang cukup menarik untuk dikembangkan. Keamanan dari suatu pesan yang ingin disampaikan oleh pengguna telah menjadi sebuah kebutuhan penting yang harus diselesaikan. Penyembunyian data telah menjadi peran penting dalam perkembangan teknologi yang ada [3]. Teknik steganografi merupakan teknik yang paling aman dibandingkan dengan teknik kriptografi tradisional yang bertujuan tidak hanya untuk menyembunyikan informasi tetapi juga untuk aktivitas komunikasi [17]. Steganografi membutuhkan dua properti, yaitu pesan dan media penampung [16]. Media penampung yang umumnya digunakan sekarang dapat berupa teks, suara, gambar, atau video. Sedangkan pesan yang disembunyikan dapat berupa teks, gambar, atau pesan lainnya. Keuntungan penggunaan

steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan [16].

Banyak penelitian yang telah dilakukan telah membahas tentang metode-metode yang dapat diterapkan di dalam teknik steganografi terutama di dalam citra digital. Pada dasarnya teknik steganografi di dalam citra digital dibagi ke dalam 2 bagian yaitu *spatial domain* dan *transform domain* [11]. *Spatial domain* mencakup metode *bitwise* yang mengaplikasikan metode penyisipan bit sedangkan untuk *transform domain* memanipulasi algoritma dan mentransformasi citra [4]. Salah satu metode transformasi yang digunakan adalah *Discrete Cosine Transform* (DCT) dalam teknik steganografi [8]. Salah satu teknik steganografi yang digunakan adalah dengan menggunakan *Discrete Cosine Transform* (DCT) [13]. Metode *Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT) digunakan dalam teknik steganografi [1]. Dari penelitian yang telah banyak dilakukan, peneliti ingin menganalisis perbandingan setiap metode yang telah dijelaskan. Analisis perbandingan akan dilakukan dengan menggunakan dua buah komponen yaitu waktu yang dibutuhkan untuk proses steganografi dan nilai PSNR.

3. STEGANOGRAFI

Steganografi berasal dari bahasa Yunani yaitu kata *stegos* yang berarti sembunyi dan *graphia* yang berarti tulisan. Steganografi secara umum memiliki arti ilmu dan seni menyembunyikan suatu fakta untuk berkomunikasi. Dengan menggunakan steganografi, pesan rahasia dapat disisipkan ke dalam sebuah informasi yang tidak mencurigakan dan mengirimkannya tanpa ada yang mengetahui keberadaan dari pesan rahasia tersebut [7]. Dalam era digital ini, steganografi berarti penyisipan pesan dalam bentuk digital ke dalam media digital yang ada. Untuk steganografi terbentuk dari dua macam yaitu pesan digital atau sering disebut dengan *message* yang akan disisipkan dan media tempat penyisipan akan dilakukan. Media tempat penyisipan dapat berupa teks, gambar, suara, dan video. Untuk media gambar, gambar yang dijadikan sebagai citra penampung disebut dengan cover *image*. Penyembunyian pesan yang berupa teks maupun gambar ke dalam citra digital akan mempengaruhi kualitas citra tersebut. Terdapat kriteria-kriteria yang harus diperhatikan dalam penyembunyian data [18] yaitu :

1. Bitrate yaitu jumlah data yang akan disembunyikan haruslah sesuai
2. Fidelity yaitu mutu citra penampung tidak jauh berubah
3. Robustness yaitu data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan, enkripsi, dan sebagainya)
4. Recovery yaitu data yang disembunyikan harus dapat diungkapkan kembali

Beberapa istilah dalam steganografi yaitu [12]:

1. *Hiddentext* atau *embedded message* yaitu pesan atau informasi yang disembunyikan.
2. *Covertext* atau *cover-object* yaitu pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stegotext* atau *stego-object* yaitu pesan yang sudah berisi *embedded message*.

4. LEAST SIGNIFICANT BIT (LSB)

LSB adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil [18]. Letaknya adalah paling kanan dari barisan bit Metode LSB menambahkan bit pesan di bit yang terakhir dalam bit suatu pixel *host image*. Proses algoritma LSB untuk kasus penyembunyian suatu citra ke dalam citra lain yaitu [18] :

1. Untuk *host image* dan pesan diubah dalam bentuk matriks.
2. Untuk matriks *host* diubah ke dalam bentuk biner
3. Nilai biner dari matriks pesan kemudian disisipkan ke dalam bit terakhir dari nilai dalam suatu pixel
4. Untuk ukuran dari citra pesan (*message*) akan ikut diubah dalam bentuk biner 8 bit dan akan ikut disisipkan ke dalam *host image.*

5. DISCRETE COSINE TRANSFORM (DCT)

DCT merupakan sebuah metode yang telah diterapkan di berbagai bidang pengetahuan. DCT merupakan metode yang mentransfrormasikan sebuah informasi dari domain ruang atau waktu ke dalam domain frekuensi dengan tujuan untuk mempercepat transmisi, mengurangi penyimpanan di dalam memori, menyediakan representasi *compact*, dan sebagainya [15]. Metode DCT adalah perubahan basis yang mengambil fungsi yang bernilai riil dan mengubahnya dalam bentuk basis

ortonomal kosinus [2]. Metode DCT yang banyak digunakan dalam aplikasi adalah DCT 2D. Persamaan untuk transformasi DCT 2D (citra berukuran m x n) ditunjukkan pada persamaaan di bawah ini:

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

dimana $\propto(u) = \sqrt{\frac{1}{N}}$, untuk u = 0,

$\propto(u) = \sqrt{\frac{2}{N}}$, untuk u = 1,2,3,…, n-1

Untuk invers dari transformasi 2D DCT dapat dilihat pada persamaan di bawah ini:

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

6. DISCRETE WAVELET TRANSFORM (DWT)

DWT merupakan metode yang dapat membagi informasi dari suatu citra menjadi pendekatan dan detail sinyal. *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 [3]. Persamaan umum untuk DWT dapat dilihat pada persamaan di bawah ini [14].

$$DWT\{f(t)\} = W_\phi(j_0,k) + W_\varphi(j,k) \quad (3)$$

dimana: $W_\phi(j_0,k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x|n| \phi_{j_0,k}|n|$

$W_\varphi(j,k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x|n| \varphi_{j,k}|n|, \varphi \qquad j \geq j_0$

Di dalam penelitian ini akan menggunakan transformasi *wavelet haar*. *Wavelet haar* dapat digunakan untuk merepresentasikan suatu citra dengan proses perhitungan *wavelet*. Persamaan transformasi *wavelet haar* ditunjukkan dalam persamaan di bawah ini [14]:

$$X[2k] = 1/2(x[2k] + x[2k+1]) \quad (4)$$
$$X[2k+1] = 1/2(x[2k] - x[2k-1]) \quad (5)$$

7. PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR merupakan sebuah parameter yang penting untuk mengukur kualitas dari proses pengolahan citra. PSNR adalah rasio antara intesitas maksimum citra dengan Mean Square Error (MSE) dari citra [10]. Persamaan untuk menghitung nilai PSNR adalah:

$$PSNR = 20\ 20_{log} \frac{MAX(1)}{\sqrt{MSE}} \quad (6)$$

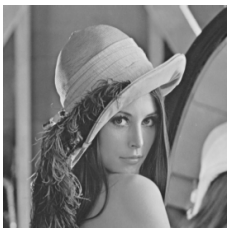
dimana persamaan MSE adalah :

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} [I(i,j) - K(i,j)]^2 \quad (7)$$

8. PEMBAHASAN

Dalam pembahasan kali ini akan membandingkan tiga buah metode yaitu *Least Significant Bit* (LSB), *Discrete Wavelet Transform* (DWT), atau *Discrete Cosine Transform* (DCT) dalam proses steganografi. Dalam pembahasan proses

steganografi kali ini akan menggunakan 2 buah citra digital. Yang pertama citra yang akan dijadikan sebagai *host image* sedangkan yang kedua merupakan citra yang akan dijadikan sebagai pesan (*message*) seperti yang dapat dilihat dalam gambar 1 dan 2. Proses steganografi kali ini akan menggunakan *tools* Matlab.

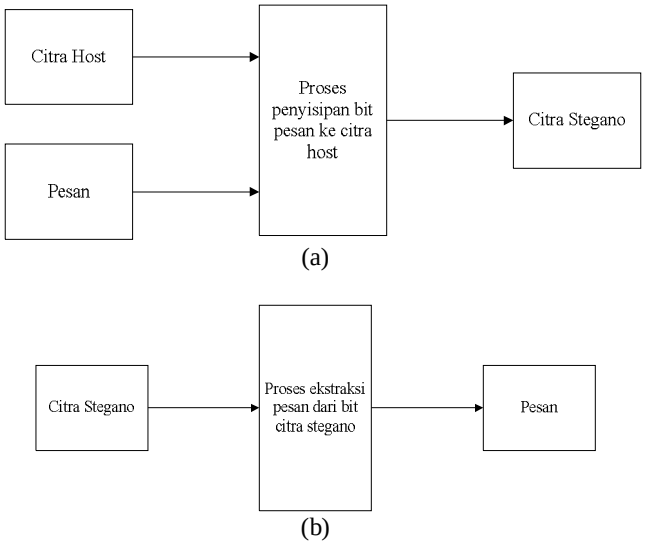


Gambar 1: Gambar citra *host image*

Gambar 2: Gambar citra *message*

8.1. STEGANOGRAFI DENGAN LSB

Aliran proses steganografi baik proses penyisipan maupun proses ekstraksi dengan menggunakan metode LSB dapat dilihat dalam diagram pada gambar 3.



Gambar 3: (a) Proses penyisipan dengan metode LSB (b) Proses ekstraksi dengan metode LSB

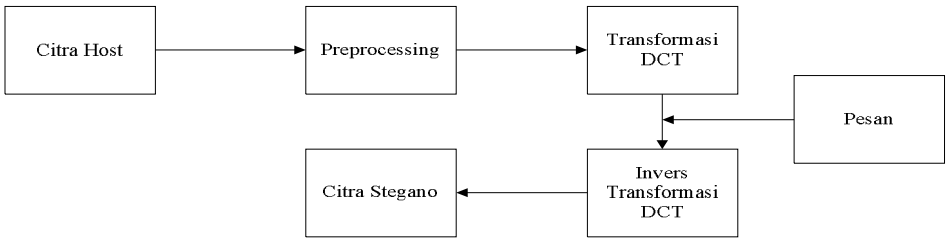
Dengan menggunakan metode LSB proses steganografi dari kedua gambar yang telah dibahas sebelumnya akan menghasilkan hasil yang dapat dilihat pada gambar 4

Gambar 4: Hasil steganografi dengan metode LSB

Dapat dilihat dari gambar di atas bahwa di dalam hasil dari proses steganografi menggunakan metode LSB tidak terlihat citra yang menjadi pesan rahasia. Seperti pada algoritma yang telah dijelaskan di bagian LSB, proses penyisipan pesan akan dilakukan dalam bit terakhir pada nilai dari *host image*.

8.2. STEGANOGRAFI DENGAN DCT

Aliran proses steganografi baik proses penyisipan maupun proses ekstraksi dengan menggunakan metode DCT dapat dilihat dalam diagram alir pada gambar 5.

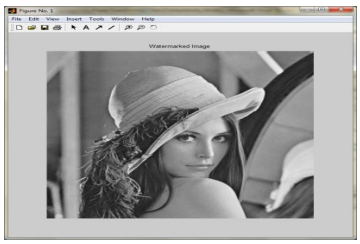


(a)

(b)

Gambar 5: (a) Proses penyisipan dengan metode DCT (b) Proses ekstraksi dengan metode DCT

Dengan menggunakan metode DCT proses steganografi dari kedua gambar yang telah dibahas sebelumnya akan menghasilkan hasil yang dapat dilihat pada gambar 6

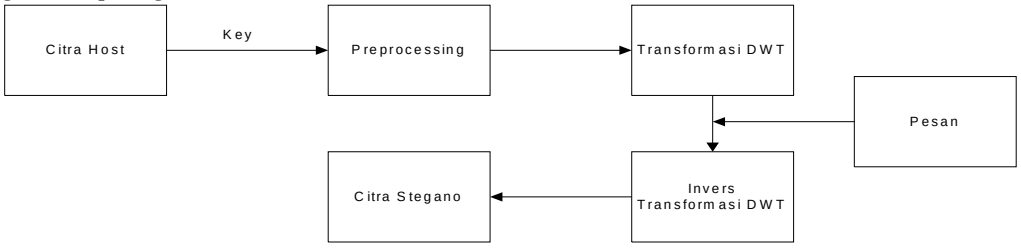


Gambar 6: Hasil steganografi dengan metode DCT

Dapat dilihat dari gambar di atas bahwa di dalam hasil dari proses steganografi dengan menggunakan metode DCT tidak terlihat citra yang menjadi pesan rahasia. Dalam proses DCT akan menggunakan nilai minimun koefisien perbedaan sebesar 50 dan menggunakan *blocksize* sebesar 8.

8.3. STEGANOGRAFI DENGAN DWT

Aliran proses steganografi baik proses penyisipan maupun proses ekstraksi dengan menggunakan metode DWT dapat dilihat dalam diagram alir pada gambar 7.



(a)

(b)

Gambar 7: (a) Proses penyisipan dengan metode DWT (b) Proses ekstraksi dengan metode DWT

Dengan menggunakan metode DWT proses steganografi dari kedua gambar yang telah dibahas sebelumnya akan menghasilkan hasil yang dapat dilihat pada gambar 8

Gambar 8: Hasil steganografi dengan metode DWT

Dapat dilihat dari gambar di atas bahwa di dalam hasil dari proses steganografi dengan menggunakan metode DWT tidak terlihat citra yang menjadi pesan rahasia. Dalam proses DWT akan menggunakan faktor *gain* sebesar 2. Proses steganografi dengan metode DWT akan menggunakan sebuah kunci (*key*) yang berupa sebuah citra. Lalu wavelet yang digunakan adalah wavelet haar.

8.4. ANALISIS PERBANDINGAN METODE

Dengan menggunakan ketiga metode di atas terdapat nilai PSNR serta waktu yang dibutuhkan untuk proses penyisipan dan ekstraksi. Nilai PSNR dan waktu yang diperlukan dapat dilihat dalam tabel 1 di bawah ini.

Tabel 1. Analisis perbandingan metode steganografi

No	Metode	PSNR	Waktu Penyisipan	Waktu Ekstraksi
1	*Least Significant Bit* (LSB)	181.1242	4.3100	2.4190
2	*Discrete Cosine Transform* (DCT)	48.3278	2.7230	2.3260
3	*Discrete Wavelet Transform* (DWT)	574.9269	21.4780	27.4580

Dilihat dari tabel di atas nilai PSNR yang paling besar adalah hasil proses steganografi dengan menggunakan metode *Discrete Wavelet Transform* (DWT) dengan nilai 574.9269. Ini membuktikan bahwa citra hasil dari proses steganografi hampir menyerupai citra aslinya. Tetapi dengan resiko waktu yang dibutuhkan untuk proses penyisipan dan ekstraksi yang paling lama dibandingkan dengan metode yang lainnya. Dengan menggunakan metode *Discrete Cosine Transform* (DCT) proses steganografi akan dilakukan dengan lebih cepat dibandingkan dengan metode lainnya tetapi citra hasil steganografi mempunyai nilai PSNR yang paling kecil dibandingkan dengan metode yang lainnya yang berarti citra hasil steganografi yang dihasilkan kurang menyerupai dengan citra aslinya. Metode LSB menghasilkan citra steganografi lebih baik dibandingkan dengan metode DCT tetapi metode LSB merupakan metode yang telah lama dipakai sehingga mudah untuk diserang. Alasannya adalah metode LSB hanya menyisipkan bit pesan ke dalam *host image* sehingga dapat dideteksi dengan mudah. Dapat dilihat juga dari waktu yang diperlukan untuk melakukan ekstraksi lebih cepat daripada waktu yang diperlukan untuk penyisipan pesan dengan menggunakan metode LSB. Ini menandakan begitu mudahnya proses ekstraksi citra hasil steganografi dengan menggunakan metode LSB.

9. KESIMPULAN

Steganografi dapat digunakan sebagai salah satu teknik dalam keamanan suatu data serta dalam penyampaian suatu pesan. Banyak metode yang dapat digunakan dalam teknik steganografi. Metode yang digunakan dapat dibagi menjadi dua

yaitu *spatial domain* dan *transform domain*. Setiap metode yang digunakan memiliki keunggulan serta kelemahan tersendiri. Keunggulan dan kelemahan tersebut dapat menjadi sebuah pertimbangan untuk memutuskan metode yang akan dipakai dalam teknik steganografi.

Perbandingan yang dilakukan dalam penelitian ini menunjukkan bahwa dengan menggunakan metode *Discrete Wavelet Transform* (DWT) memiliki nilai PSNR yang besar yang mencerminkan bahwa citra hasil steganografi hampir menyerupai citra aslinya tetapi membutuhkan waktu yang lama dalam pemrosesannya. Dengan menggunakan metode *Discrete Cosine Transform* (DCT) waktu prosesnya relatif lebih singkat dibandingkan ketiga metode lainnya tetapi nilai PSNR yang dihasilkan paling kecil yang menunjukkan citra stegano kurang menyerupai citra aslinya. Untuk metode LSB, terdapat kelemahan yaitu mudah untuk diserang terlihat juga dari waktu proses ekstraksinya lebih cepat dibandingkan dengan waktu penyisipannya.

10. DAFTAR PUSTAKA

[1] Bhattacharya, Tanmay, Dey, Nilanjan, Chaudhuri, S.R. Bhadra, 2012, *A Session based Multiple Image Hiding Technique using DWT and DCT*, International Journal of Computer Applications, Vol. 38, No. 5, pp. 18-21.

[2] Cuddy, Aileen, Walden, Elisabeth, Zalewski, Sarah, 2001, *The Discrete Cosine Transform*.

[3] Dinesh, Yedla, Ramesh, Addanki Purna, 2012, *Efficient Capacity Image Steganography by Using Wavelets*, International Journal of Engineering Research and Applications, Vol. 2, No. 2, pp. 251-259 .

[4] Johnson, N.F. & Jajodia, S., 1998, *Steganalysis of Images Created Using Current Steganography Software*, *Proceedings of the 2nd Information Hiding Workshop*.

[5] Katharotiya, Anilkumar, Patel, Swati, Goyani, Mahesh, 2011, *Comparative Analysis Between DCT & DWT Techniquesof Image Compression*, Journal of Information Engineering and Applications, Vol. 1, No. 2, pp. 9-17.

[6] Kaur, Blossom, Kaur, Amandeep, Singh, Jasdeep, 2011, *Steganographic Approach for Hiding Image in DCT Domain*, International Journal in Engineering and Technology, Vol. 1, No. 3, pp. 72-78.

[7] Krenn, J.R., 2004, *Steganography and Steganalysis*, www.krenn.nl/univ/cry/steg/article.pdf

[8] Kumar, K.B. Shiva, Raja, K B, Chhotaray, R K, Pattanaik, Sabyasachi, 2010, *Bit Length Replacement Steganography Based on DCT Coefficients*, International Journal of Engineering Science and Technology, Vol. 2, No. 8, pp. 3561-3570.

[9] Lecompte, Jonathan, Legoff, Olivier, Hascoet, Jean-Yves, 2010, *Technological Form Defects Identification Using Discrete Cosine Transform Method*, International Journal Advance Manufacturing Technology, Vol. 51, pp. 1033-1044.

[10] Modalavalasa, Nagamani, Prasad, K. Satya, Rani, S. Swapna, Rao, G. Sasi Bhushana, Goswami, Rajkumar, 2012, *Quantitive Evaluation of Various Spatial Filters for Underwater Sonar Images Denoising Application*, International Journal of Engineering, Vol. 10, No. 1, pp. 47-51.

[11] Morkel, T., Eloff, J.H.P., Olivier, M.S., 2005, *An Overview of Image Steganography*, Proceedings of the Fifth Annual Information Security South Africa Conference, Sandton, South Africa.

[12] Munir, Rinaldi, 2006, *Diktat Kuliah IF5054 Kriptografi*, Institut Teknologi Bandung, Bandung.

[13] Patel, Hardik, Dave, Preeti, 2012, *Steganography Technique Based on DCT Coefficients*, International Journal of Engineering Research and Applications, Vol. 2, No. 1, pp. 713-717.

[14] Thyagarajan, K.S, 2011, *Still Image and Video Compression with Matlab*, A John Wiley & Sons, Inc. New Jersey, Canada.

[15] Uma, R., 2011, *FPGA Implementation of 2-D DCT for JPEG Image Compression*, International Journal of Advanced Engineering Sciences and Technologies, Vol. 7, No. 1, pp. 1-9

[16] Vembrina, Yus Gias, *Spread Spectrum Steganography*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung.

[17] Wang, Shen, Song, Xianhua, Niu, Xiamu, 2012, *An Affine Transformation Based Image Steganography Approach*, International Journal of Digital Content Technology and its Applications, Vol. 6, No. 1, pp. 8-14.

[18] Yusuf, Yesrani Helyda, 2011, *Implementasi Aplikasi Steganografi dengan Menggunakan Eureka Steganograher, JPHide, and Seek, Steganog, dan Stegomagic*, Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM", Yogyakarta