ANALISIS STEGANOGRAFI GANDA PADA CITRA DIGITAL MENGGUNAKAN METODE DISCRETE WAVELET TRANSFORM DAN SINGULAR VALUE DECOMPOSITION DENGAN PENYISIPAN SPREAD SPECTRUM IMAGE STEGANOGRAPHY

ANALYSIS OF DOUBLE DIGITAL IMAGE STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM AND SINGULAR VALUE DECOMPOSITION METHOD WITH SPREAD SPECTRUM IMAGE STEGANOGRAPHY INSERTION

Reza Ahmad Nurfauzan[1], Bambang Hidayat[2], Sofia Saidah[3]
Fakultas Teknik Elektro, Universitas Telkom, Bandung, Jawa Barat 40257[123]
rezaahmadn@gmail.com[1], bhidayat@telkomuniversity.ac.id [2]

Abstrak - Steganografi adalah sebuah ilmu atau seni menyamarkan keberadaan informasi. Terdapat beragam metode dalam melakukan steganografi, di era digital ini steganografi banyak digunakan pada media seperti citra, audio dan video. Pada umumnya steganografi dilakukan dengan satu kali proses penyisipan dan menggunakan satu buah cover untuk menyembunyikan informasi, namun pada penelitian ini digunakan dua buah cover berupa citra digital dan dua kali proses penyisipan untuk mengelabui pihak yang tidak memiliki hak dalam mengakses informasi tersebut. Metode Spread Spectrum Image Steganography digunakan untuk metode penyisipan pertama pada domain spasial, sedangkan pada penyisipan kedua digunakan metode Discrete Wavelet Transform digunakan untuk mentransformasi cover citra kedua ke domain frekuensi dan pesan disisipkan dengan memodifikasi singular value dengan menggunakan metode Singular Value Decomposition. Hasil penelitian menunjukan stego-file yang dihasilkan memiliki imperceptibility dan robustness yang cukup baik. Hal ini diukur berdasarkan nilai PSNR dan SNR pada kedua proses penyisipan, SSIM pada penyisipan kedua dan BER pada saat proses ekstraksi.

Kata kunci: Steganografi, Double Steganography, Discrete Wavelet Transform, Singular Value Decomposition, Spread Spectrum Image Steganography

Abstract - Steganography is the science or art of disguising the existence of information. There are various methods in steganography, in this digital era steganography is widely used on media such as image, audio and video. In general, steganography is done with a single insertion process and uses one cover to hide information, but in this research I used two digital cover image and two insertion process to trick the one who has no right in accessing the information. Spread Spectrum Image Steganography is used for the first insertion method in the spatial domain, whereas in the second insertion the Discrete Wavelet Transform method is used to transform the second cover image into frequency domain and the message is inserted by modifying the singular value using the Singular Value Decomposition method. The results show that the resulting stego-file has good imperceptibility and robustness. It is measured based on PSNR and SNR values on both insertion processes, SSIM on second insertion and BER at the extraction process.

Keywords: Steganography, Double Steganography, Discrete Wavelet Transform, Singular Value Decomposition, Spread Spectrum Image Steganography

1. Pendahuluan

Steganografi merupakan seni dan ilmu dalam penyembunyian pesan ke dalam suatu media atau *cover*, dimana keberadaan pesan tersebut hanya dapat diketahui oleh orang-orang tertentu [1] [2]. Dibanding kriptografi yang keberadaan pesannya dapat diketahui dengan jelas, steganografi memanfaatkan kelemahan indera manusia agar pesan rahasia tidak dapat diidentifikasi [1]. Pada kondisi tertentu hal tersebut menjadi alasan untuk menggunakan steganografi. Selain itu juga membuat steganografi menarik untuk dikembangkan. Saat ini banyak sekali penelitian tentang steganografi citra, tetapi sebagian besar dari penelitian tersebut, pada umumnya melakukan satu kali penyisipan. Sistem tersebut sangat rentan terdeteksi oleh pihak yang tidak memiliki hak [1]. Oleh karenanya pada penelitian ini dilakukan dua kali steganografi atau *double steganography* (steganografi ganda) untuk mengelabui atau menyulitkan pencurian dan pendeteksian informasi.

Secara teknis steganografi ganda ini hampir sama dengan steganografi pada umumnya yaitu terdapat proses *embedding* (penyisipan) dan ekstraksi. Namun yang membedakannya adalah terdapat dua kali proses penyisipan dan juga dua kali proses ekstraksi. Oleh karena itu apabila steganografi biasa memerlukan satu buah *cover* maka steganografi ganda memerlukan dua buah *cover*.

Dua proses penyisipan pada steganografi ganda ini dilakukan pada domain spasial dan domain frekuensi. Proses penyisipan terluar atau penyisipan kedua dilakukan pada domain frekuensi dengan menggunakan metode transformasi atau DWT. DWT adalah suatu metode untuk mengubah suatu informasi pada domain *spasial* ke domain frekuensi. Sebelum DWT, metode yang paling terkenal untuk transformasi dari domain spasial ke domain frekuensi adalah Transformasi Fourier atau *Fourier Transform* (FT). Kelebihan DWT dibanding FT yaitu dalam hal analisis yang mana DWT menampilkan aspek sinyal seperti diskontinyuitas, *breakdown point* dan lain lain dengan lebih jelas dibanding FT [3].

Selain metode transformasi DWT, pada penyisipan kedua juga digunakan metode dekomposisi *Singular Value Decomposition* atau SVD. SVD adalah salah satu *tools* dasar yang sangat penting untuk melakukan faktorisasi matriks dengan bilangan real ataupun kompleks [4]. SVD juga sering digunakan dalam steganografi dan watermarking terutama pada citra, karena teknik ini merupakan teknik yang cukup efektif [5].

Pada penyisipan pertama dilakukan penyisipan pada domain spasial. Metode yang digunakan adalah *Spread Spectrum Image Steganography* (SSIS) atau biasa disebut *Spread Spectrum* (SS). SSIS atau SS adalah salah satu metode penyisipan yang banyak digunakan dalam steganografi. Prinsip dari metode ini adalah menumpangkan sinyal informasi ke sebuah noise kemudian menambahkannya ke dalam *cover image* [6]. Noise yang ditambahkan memiliki intensitas yang relatif rendah sehingga tidak menimbulkan kecurigaan pada citra yang telah disisipi [6].

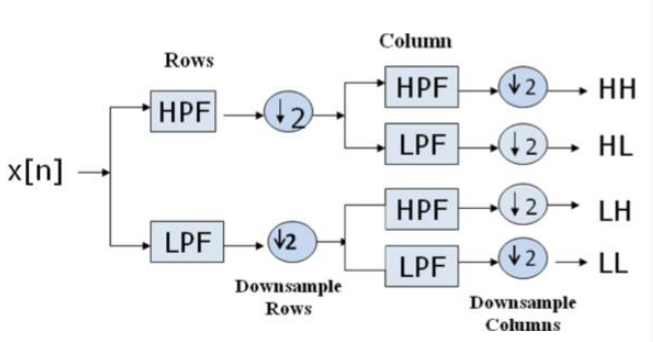
Dengan metode SS yang memiliki robustness yang cukup baik dan kombinasi DWT-SVD yang menyisipkan pesan rahasia pada domain frekuensi agar pesan rahasia semakin tidak mudah dideteksi oleh indera manusia, skema steganografi ganda ini diarahkan pada peningkatan keamanan dan robustness dari steganografi itu sendiri.

2. Metode Penelitian

Penelitian ini menggabungkan beberapa metode diantanya:

2.1 Discrete Wavelet Transform (DWT) [3] [7] [8]

DWT menggunakan filter untuk menganalisis dan merekonstruksi sinyal. Prosedur ini disampaikan oleh S. Mallat pada tahun 1989 yang memanfaatkan dekomposisi *wavelet transform filter low pass* (*averaging*) dan *filter high pass* (*differencing*). Sebuah *filter* memisahkan sinyal pada frekuensi yang berbeda. DWT dari sinyal domain spasial didapat dengan cara memfilter sinyal menggunakan LPF dan HPF seperti yang ditunjukkan pada gambar di bawah, prosedur ini dikenal dengan *Mallat Tree decomposition*. Suatu sinyal input yang dinotasikan dengan x[n], di mana n adalah bilangan bulat. Pada setiap *level*, HPF menghasilkan *detailed information* atau *detailed coefficient*, d[n], sedangkan LPF menghasilkan *approximate coefficient*, a[n]. *Input* data dilewatkan melalui set LPF dan HPF. *Output* dari *high pass* dan *low pass filter* mengalami *downsample* sebesar 2. DWT dari sebuah citra merepresentasikan penjumlahan dari beberapa wavelet. Mata manusia kurang begitu sensitif terhadap detil frekuensi tinggi. Pada DWT 2 level, dibutuhkan dua kali operasi.



Gambar 1. Blok Diagram DWT 2 Dimensi [3]

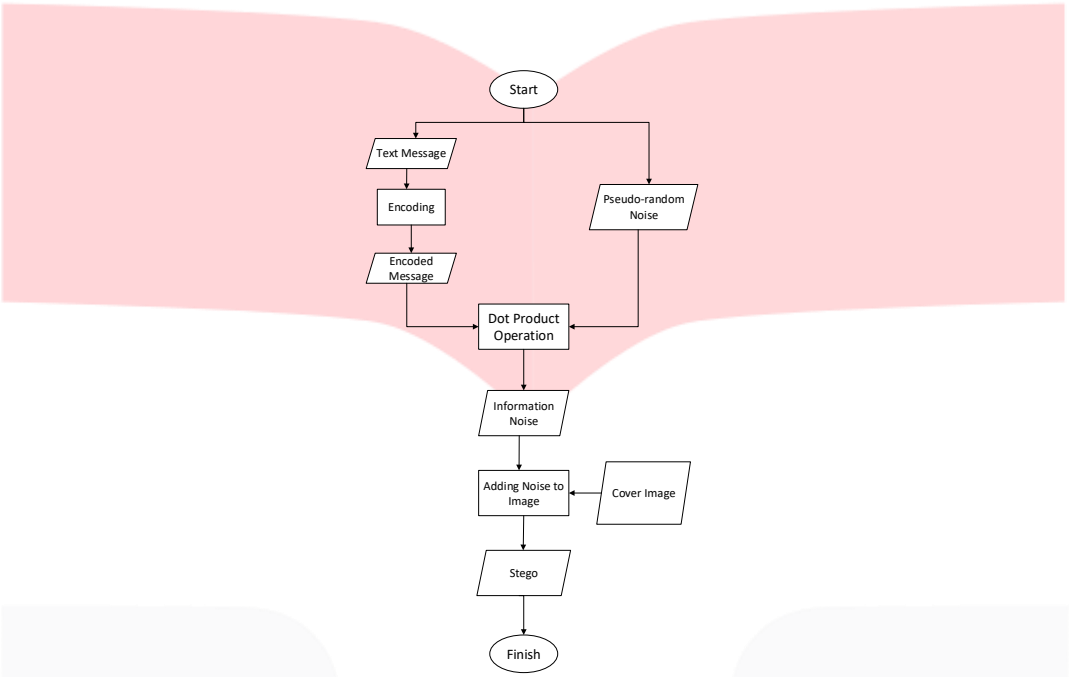
Mirip seperti DWT yang dapat dijelaskan dengan menggunakan teori *filter*, rekonstruksi juga dapat dilakukan menggunakan IDWT. Prosesnya sebenarnya hanya merupakan kebalikan dari DWT. Koefisien DWT dilakukan *upsample* yang secara otomatis akan menggandakan panjang masing-masing sinyal dekomposisi. Kemudian sinyal tersebut dikonvolusikan dengan *filter* skala rekonstruksi (*filter* skala rekonstruksi hanya *filter* skala asli yang telah dibalik menjadi kiri ke kanan). Hasil ini kemudian ditambahkan bersama-sama untuk sampai pada sinyal asli

2.2 Spread Spectrum Image Steganography [6]

Konsep mendasar dari metode penyisipan ini adalah dengan menyisipkan sinyal informasi *narrowband* ke dalam *noise wideband* lalu menambahkan *noise* tersebut ke dalam *cover image*. *Noise* yang ditambahkan tersebut seperti

noise yang terjadi pada saat proses akuisisi citra dan jika pada *level* rendah, tidak akan mudah terdeteksi oleh indera penglihatan manusia maupun analisis komputer tanpa menggunakan citra aslinya.

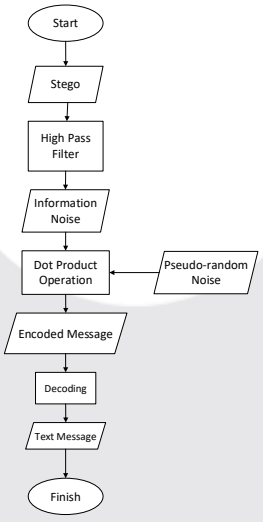
Secara umum proses *spread spectrum* ini digambarkan pada gambar di bawah. Pada sistem ini, pesan teks diubah ke dalam bentuk biner kemudian pesan dikalikan dengan *pseudorandom noise* sehingga menghasilkan *noise* informasi.



Gambar 2. Proses Penyisipan Menggunakan Spread Spectrum

Setelah itu *noise* informasi tersebut ditambahkan ke *cover image* dalam intensitas yang rendah agar tidak terdeteksi oleh mata manusia.

Di sisi penerima, stegoimage diterima oleh penerima yang mempunyai kunci yang sama yaitu *pseudorandom-noise* yang sama untuk mengekstrak pesan yang diterima.



Gambar 3. Proses Ekstraksi Pesan

Pertama, *stegoimage* melewati *High Pass Filter* untuk mendapatkan *noise* informasi kembali. Setelah itu noise informasi dikalikan dengan *pseudorandom-noise* yang sama seperti pada saat disisipkan. Kemudian pesan rahasia dapat direkonstruksi kembali.

2.3 Singular Value Decomposition [4] [5] [9] [10]

Singular Value Decomposition (SVD) dari sebuah matriks A adalah faktorisasi dari A menjadi tiga matriks A = USV^T dimana kolom U dan V adalah ortogonal dan matriks S adalah matriks diagonal dengan bilangan real positif.

Matrik U,S dan V dapat dicari menggunakan persamaan:

$$A^T A = VS^T U^T USV^T \quad (1)$$

Karena U merupakan matriks yang orthogonal maka U U^T=1, sehingga persamaannya menjadi:

$$A^T A = VS^T SV^T \quad (2)$$

Lalu persamaan dibawah ini juga disederhanakan seperti persamaan diatas:

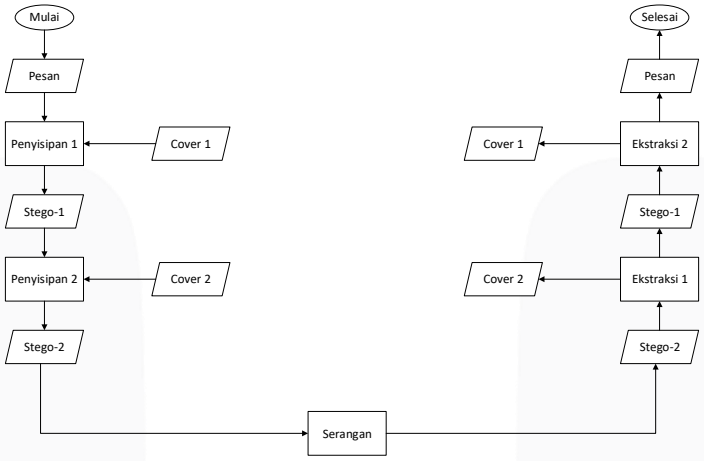
$$AA^T = USV^T VS^T U^T \quad (3)$$

$$AA^T = USS^T U^T \quad (4)$$

Dapat dilihat bahwa persamaan $A^TA=VS^TSV^T$ merupakan persamaan diagonalisasi, begitu juga dengan $AA^T=USS^TU^T$, maka S^TS dan SS^T merupakan nilai-nilai eigen untuk setiap vektor eigen V dan U. Sehingga untuk mendapatkan matrik U, S dan V perlu dicari nilai eigen dan vektor eigen dari A^TA dan AA^T.

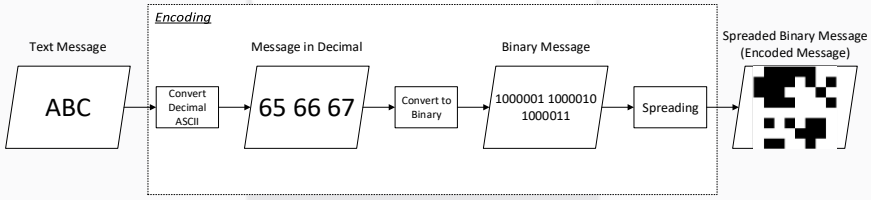
3. Desain Model Sistem

Secara umum steganografi terdiri dari proses penyisipan (*embedding*) dan ekstraksi. Pada tugas akhir ini diimplementasikan steganografi ganda menggunakan dua buah *cover* berupa citra sehingga pada sistem ini terdapat dua kali proses penyisipan dan juga dua kali proses ekstraksi. Model sistem yang diajukan secara umum digambarkan pada diagram berikut:



Gambar 4. Desain Umum Model Sistem Steganografi Ganda

Pada proses penyisipan di diagram sebelah kiri, terdapat dua kali penyisipan. Penyisipan pertama dilakukan dengan menyisipkan pesan rahasia berupa teks ke dalam sebuah *cover* citra menggunakan metode *Spread Spectrum*. Dengan metode *spread spectrum*, pesan teks diubah ke dalam kode biner. Setelah itu dilakukan *encoding* pada pesan rahasia tersebut sehingga pesan rahasia dapat dimodulasi dengan *pseudo-random noise*.



Gambar 5. Proses Encoding Pesan

Setelah melalui proses *encoding*, pesan tersebut dikalikan dengan *noise*. Lalu ditambahkan ke dalam *cover image* dengan intensitas yang tidak terdeteksi oleh mata manusia. Penyisipan pertama selesai dan dihasilkan *stego-1*.

Pada proses penyisipan kedua, pesan rahasia yang disisipkan adalah citra keluaran dari penyisipan pertama yaitu *stego-1*. Cover yang digunakan berupa citra, sedangkan metode yang digunakan adalah metode DWT *(Discrete Wavelet Transform)* dan SVD *(Singular Value Decomposition). Cover* terlebih dahulu ditranformasi ke dalam domain frekuensi menggunakan metode DWT kemudian salah satu *subband* DWT diambil dan dilakukan SVD. Di sisi lain pesan yang akan disisipkan juga dilakukan proses SVD. *Singular value* dari *subband* dimodifikasi dengan menggunakan *singular value* dari pesan. *Left-singular value* dari pesan, *right-singular value* dari pesan dan *singular value* asli dari cover dikirim ke penerima melalui kanal terpisah. Setelah itu subband termodifikasi direkonstruksi kembali dan dilakukan *invers* DWT menjadi *stego-2. Stego-2* atau *final stego* siap dikirimkan.

Di sisi penerima terdapat dua kali proses ekstraksi. Ekstraksi pertama merupakan kebalikan dari proses penyisipan kedua. Stego-2 yang diterima ditransformasi ke dalam domain frekuensi menggunakan DWT, kemudian diambil subband yang disisipi pesan. Lalu dilakukan proses SVD untuk mengambil singular value dari subband tersebut, setelah itu dilakukan rekonstruksi pesan kembali menjadi *stego-1* dengan menggunakan informasi tambahan berupa *left-singular value* dari pesan, *right-singular value* dari pesan dan *singular value* asli dari cover. Setelah *stego-1* berhasil diekstrak, barulah masuk ke proses ekstraksi terakhir. *Stego-1* dilewatkan kepada *filter* HPF untuk diambil frekuensi tingginya dimana noise informasi tadi ditambahkan. Kemudian noise informasi tersebut dikalikan dengan pseudo-random noise yang sama dengan penyisipan pertama, sehingga didapat pesan yang ter-*encoding*. Dilakukan proses *decoding* kembali sehingga didapatkan pesan biner, setelah itu pesan biner diubah kembali ke bentuk teks yang bisa dipahami oleh manusia.

4. Hasil dan Analisis

Hasil optimal yang dapat dicapai sistem steganografi ganda ini adalah sebagai berikut:

Tabel 1. Nilai Parameter Hasil Pengujian

	Hiroshima		Kyoto		Okinawa		Osaka		Tokyo	
	PSNR	SNR	PSNR	SNR	PSNR	SNR	PSNR	SNR	PSNR	SNR
Cat	43.178	35.752	43.182	37.673	43.18	39.179	43.18	36.777	43.179	38.374
Jaguar	48.074	40.648	48.06	42.551	48.07	44.067	48.072	41.669	48.072	43.266
Lion	42.291	34.864	42.29	36.781	42.285	38.284	42.286	35.884	42.286	37.481
Panther	47.75	40.324	47.756	42.247	47.748	43.747	47.753	41.35	47.755	42.949
Tiger	42.055	34.628	42.056	36.548	42.055	38.054	42.053	35.65	42.056	37.251
	SSIM	BER	SSIM	BER	SSIM	BER	SSIM	BER	SSIM	BER
Cat	0.9966	0	0.9994	0	0.9985	0	0.9989	0	0.9993	0
Jaguar	0.9991	0	0.9998	0	0.9995	0	0.9996	0	0.9998	0
Lion	0.9958	0	0.9993	0.0011	0.9981	0	0.9987	0	0.9991	0
Panther	0.9988	0	0.9998	0	0.9995	0	0.9996	0	0.9997	0
Tiger	0.9957	0	0.9993	0	0.998	0.0011	0.9986	0	0.9991	0

Diatas adalah tabel hasil pengujian sistem tanpa serangan. Kualitas *final stego* yang dihasilkan cukup baik, dengan nilai PSNR diatas 40 dB, SNR diatas 30 dB dan SSIM diatas 0.9900. Meskipun diuji tanpa serangan nilai BER tidak 0% karena pada proses penyisipan pertama menggunakan metode *Spread Spectrum* dengan *noise* yang bersifat *random* sehingga memunculkan kemungkinan *error* pada saat penyisipan. Akan tetapi nilai BER pada sistem ini mendekati 0% sehingga dapat dikatakan sistem ini memiliki tingkat error yang rendah. Sistem ini juga memiliki rata-rata waktu komputasi yang cepat yaitu 0.754 detik. Kapasitas pesan yang dapat disisipkan adalah 78 karakter.

Pada pengujian menggunakan serangan, sistem ini cukup tahan terhadap *noise Gaussian* dalam intensitas yang kecil (0.4 pada MATLAB) dan tahan terhadap serangan *noise Salt & Pepper*. Sedangkan untuk serangan *filter*, sistem ini tidak tahan terhadap *filter* LPF, tetapi tahan terhadap *filter* HPF karena pada sistem ini informasi disisipkan pada frekuensi tinggi.

5. Kesimpulan

Sistem steganografi ganda menggunakan metode *Discrete Wavelet Transform* dan *Singular Value Decomposition* dengan penyisipan *Spread Spectrum Image Steganography* ini dapat bekerja dengan baik dan memiliki ketahanan yang cukup baik terhadap *noise*, namun karena sistem ini termasuk *semi-blinded steganography* maka sistem ini memerlukan beberapa informasi dari pesan dan *cover* untuk dapat mengekstrak pesan rahasia. Sistem ini tahan terhadap *noise salt & pepper* dan *noise Gaussian* dengan intensitas 0,6. Sistem ini juga tahan terhadap *filter* HPF namun tidak tahan terhadap *filter* LPF. Sistem ini memiliki nilai rata-rata PSNR 44 dB, SNR 39 dB, SSIM 0,9988 pada penyisipan kedua dan BER mendekati 0%.

Referensi

[1] A. Zakaria dan R. Munir, “Steganografi Citra Digital Menggunakan Teknik Discrete Wavelet Transform pada Ruang Warna CIELab,” 2015.

[2] J. Makwana and S. Chudasama, "Dual Steganography: A New Hidiing Technique for Digital Communication," *International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering*, vol. V, no. 4, pp. 3184-3188, 2016.

[3] B. Gupta Banik and S. K. Bandyopadhyay, "A DWT Method for Image Steganography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. III, no. 6, pp. 983-989, 2013.

[4] E. Biglieri and K. Yao, "Some Properties of Singular Value Decomposition and Their Applications to Digital Signal Processing," *Signal Processing 18,* pp. 277-289, 1989.

[5] H. A. Abdallah, M. M. Hadhoud and A. A. Shaalan, "An Efficient SVD Image Steganographic Approach," *Computer Engineering & Systems*, pp. 257-262, 2009.

[6] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," *IEEE Transactions on Image Processing*, vol. VIII, no. 8, pp. 1075-1083, 1999.

[7] P.-Y. Chen and H.-J. Lin, "A DWT Based Approach for Image Steganography," *International Journal ofApplied Science and Engineering* , vol. IV, no. 5, pp. 275-290, 2006.

[8] H. Olkkonen , Discrete Wavelet Transforms: Algorithms and Applications, Rijeka: InTech, 2011.

[9] Y. Zeng and Y.-C. Liang, "Eigenvalue-Based Spectrum Sensing Algorithms for Cognitive Radio," *IEEE TRANSACTIONS ON COMMUNICATIONS*, vol. 57, no. 6, pp. 1784-1793, 2009.

[10] K. S. Babu, K. B. Raja, U. M. Rao, R. K. A, V. K. R and L. M. Patnaik, "Robust and High Capacity Image Steganography using SVD," *IET-UK International Conference on Information and Communication Technology in Electrical Sciences* , pp. 718-723, 2007.