STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN TEKNIK DISCRETE WAVELET TRANSFORM PADA RUANG WARNA CIELab

Alfian Zakaria[1], Rinaldi Munir[2]

Program Studi Magister Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jalan Ganesha No. 10, Bandung, Jawa Barat, 40132
[1] alfian.zakaria@students.itb.ac.id, [2] rinaldi-m@stei.itb.ac.id

Abstrak

Saat ini berbagai macam teknik dalam meningkatkan keamanan informasi telah banyak dikembangkan seperti kriptografi, steganografi dan *watermarking*. Steganografi merupakan teknik yang paling banyak dipakai untuk untuk menyamarkan keberadaan dari informasi, sehingga informasi tersebut menjadi sulit untuk dideteksi. Selain itu steganografi dapat diimplementasikan pada berbagai media seperti teks, gambar, audio dan video. Umumnya steganografi pada citra digital dilakukan pada ruang warna RGB, namun pada penelitian ini disajikan penerapan steganografi pada citra digital dengan ruang warna yang berbeda, yakni pada ruang warna CIELab dengan menggunakan teknik steganografi *Discrete Wavelet Transform* atau lebih tepatnya menggunakan Haar *wavelet*, ruang warna ini dipilih karena belum pernah digunakan pada penelitian steganografi dengan teknik DWT. Teknik DWT digunakan untuk mentransformasi citra asli (*original image*) dari domain *spatial* ke dalam domain *frequency* pada ruang warna CIELab. Penyisipan pesan rahasia dilakukan pada koefisien *wavelet* dari *sub band* LL dan HL menggunakan *Least Significant Bit,* dimana pemilihan koefisien tersebut dilakukan secara acak menggunakan *Pseudo Random Number Generator* dengan *key* tertentu. Hasil penelitian ini menunjukkan *stego image* yang dihasilkan memiliki *imperceptibility*, *fidelity* dan *recovery* yang cukup baik. Hal tersebut diukur berdasarkan nilai PSNR terhadap citra yang telah disisipi pesan, serta proses ektraksi yang menghasilkan pesan yang utuh seperti saat sebelum disisipkan.

Kata kunci : steganografi*, discrete wavelet transform, CIELab, least significant bit, PRNG.*

1. Pendahuluan

Seiring dengan perkembangan teknologi saat ini, pertukaran informasi menjadi sangat mudah dan cepat. Hal ini terjadi karena setiap informasi yang dipertukarkan telah dikemas kedalam bentuk digital, sehingga dapat dengan mudah dipertukarkan melalui berbagai macam media transmisi yang telah tersedia di era digital saat ini. Oleh karenanya keamanan informasi yang dipertukarkan turut menjadi hal yang sangat penting untuk dijaga, agar informasi tersebut hanya dapat diakses oleh orang-orang yang berhak. Berdasarkan isu-isu keamanan seperti ini telah banyak dikembangkan berbagai macam metode dan teknik untuk dapat mengamankan informasi, salah satunya seperti teknik pengenkripsian pesan (kriptografi). Namun teknik ini dapat menimbulkan kecurigaan karena menghasilkan sebuah pesan acak yang tidak memiliki makna secara kasat mata, sehingga mudah dicurigai. Untuk menjawab masalah dari kriptografi digunakan teknik penyembunyian pesan atau yang dikenal dengan steganografi.

Kata steganografi berasal dari bahasa Yunani, "*steganos*" yang berarti tersembunyi/tertutup dan "*graphein*" yang berarti tulisan. Sehingga kata steganografi dapat diartikan sebagai "tulisan tersembunyi" [2][3]. Secara umum steganografi juga dapat didefinisikan sebagai seni dan ilmu menyembunyikan pesan dengan cara apa pun sehingga orang lain selain penerima pesan tidak mencurigai adanya pesan tersembunyi. Terdapat beragam metode yang dapat digunakan dalam steganografi, antara lain penggunaan tinta yang tidak terlihat, penyusunan ulang huruf-huruf penyusun pesan, dan *microdots*. Pada steganografi ada 3 hal penting yang perlu diperhatikan yakni (1) *imperceptibility*, yaitu keberadaan pesan tidak dapat dipersepsi oleh indrawi manusia, (2) *fidelity*, yaitu mutu dari media steganografi tidak mengalami perubahan signifikan akibat proses penyisipan, dan (3) *recovery*, yaitu pesan dapat diekstraksi sewaktu-waktu saat dibutuhkan [11]. Pada umumnya steganografi dapat diterapkan pada hampir semua jenis file multimedia, namun yang paling sering digunakan adalah pada citra digital, karena pertukaran data dalam bentuk citra digital pada jaringan internet saat ini cukup tinggi, sehingga dapat mengurangi kecurigaan akan adanya pesan rahasia yang telah disisipkan.

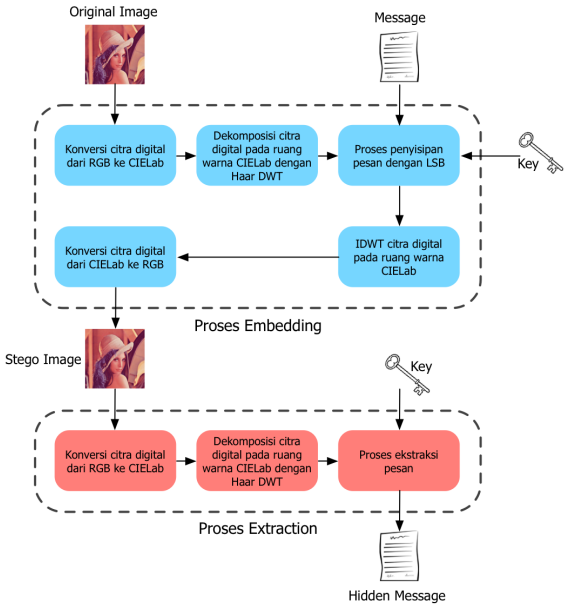
Ada dua macam skema yang populer digunakan untuk penarapan steganografi pada citra digital yakni penyisipan pada *spatial* domain dan pada *transform* domain [7]. *Transform* domain juga dikenal dengan sebutan *frequency* domain. *Discrete Wavelet Transform* (DWT) dan *Continuos Wavelet Transform* (CWT) merupakan teknik-teknik steganografi yang digunakan pada domain *transform* [1]. Ide dasar DWT sama seperti CWT. Di dalam CWT, sinyal dianalisis menggunakan seperangkat fungsi dasar yang saling berhubungan dengan penskalaan dan transisi sederhana. Sedangkan di dalam DWT, penggambaran sebuah skala waktu sinyal digital didapatkan menggunakan teknik filterisasi digital [6][12][15]. Secara garis besar proses yang dilakukan dalam teknik ini adalah melewatkan sinyal yang akan dianalisis pada *filter* dengan frekuensi dan skala yang berbeda.

Saat ini banyak penelitian di bidang steganografi yang telah dilakukan baik pada domain *spatial* maupun domain *transform*, begitu pula dengan penggunaan teknik DWT ini. Sebagian besar dari penelitian tersebut, pada umumnya menggunakan citra dengan ruang warna RGB atau dengan mode warna *grayscale* [14]. Hal ini dikarenakan RGB mampu menghasilkan *stegoimage* dengan kualitas yang cukup baik, namun waktu yang dibutuhkan untuk proses *embedding* dan *extracting* pada RGB jauh lebih lama dibandingkan dengan ruang warna lainnya [5]. Begitu pula dengan *grayscale*, karena mode warna ini lebih tahan terhadap serangan *steganalysis* [4], namun memiliki kualitas visual yang lebih rendah dibandingkan dengan citra yang berwarna [10]. Oleh karenanya pada penelitian ini metode yang diusulkan yakni penggunaan teknik DWT pada citra berwarna dengan ruang warna yang berbeda yakni CIELab. CIELab diperkenalkan oleh CIE (*Commission internationale de l'éclairage*) pada tahun 1976 yang merupakan perbaikan dari sistem CIEXYZ yang berfokus pada pendekatan dan keseragaman angka dengan persepsi visual. CIELab terdiri dari 3 *channel* utama yakni L* (*lightness*), a* (merah dan hijau) dan b* (kuning dan biru). Pada penelitian ini, CIELab dipilih berdasarkan beberapa alasan yakni: 1) karena CIELab belum pernah digunakan untuk penelitian dibidang steganografi dengan menggunakan teknik DWT, 2) CIELab mampu menghasilkan *image* dengan rentang kompresi yang cukup baik dan memiliki penyimpangan warna yang kecil pada tranformasi berbasis *wavelet* [9], selain itu CIELab merupakan ruang warna yang memiliki ketahanan (*robustness*) paling baik pada teknik watermarking dalam domain *wavelet* dibandingkan dengan ruang warna lainnya seperti YUV, YCbCr, YIQ, JPEG-YcbCr dan RGB [8].

Adapun penelitian ini memiliki 3 tujuan utama yakni (1) mengkaji penggunaan teknik *Discrete Wavelet Transform* pada ruang warna CIELab, (2) menerapkan teknik *Discrete Wavelet Transform* pada ruang warna CIELab untuk meningkatkan keamanan dan kerahasiaan informasi yang disisipkan serta mutu dari *stegoimage* yang dihasilkan, dan yang terakhir (3) melakukan pengukuran terhadap *imperceptibility*, *fidelity* dan *recovery* dari informasi rahasia yang telah disisipkan.

2. Usulan Metode

Secara umum metode yang diusulkan pada penelitian ini, mulai dari tahap penyisipan (*embedding*) pesan sampai pada tahap ekstraksi (*extracting*) pesan dapat dilihat pada Gambar 1. Misalkan *I* adalah citra asli (*original image*) dengan ukuran *N* x *N* (citra harus berukuran persegi yang merupakan hasil perpangkatan dengan 2).



Gambar 1. Metode yang diusulkan

2.1 Proses Penyisipan (*Embedding*)

Rincian proses penyisipan pesan ke dalam original image dalam penelitian ini adalah sebagai berikut :

Step 1 : Konversi *I* dari ruang warna RGB ke ruang warna CIELab dengan formula berikut ini :

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.412 & 0.358 & 0.180 \\ 0.213 & 0.715 & 0.072 \\ 0.019 & 0.119 & 0.950 \end{bmatrix} . \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

$$L^* \begin{cases} 116(Y/Y_n)^{1/3} - 16 & (Y/Y_n) > 0.008856 \\ 903(Y/Y_n)^{1/3} & (Y/Y_n) \le 0.008856 \end{cases} \quad (2)$$

$$\begin{cases} a^* = 500[f(X/X_n) - f(Y/Y_n)] \\ b^* = 200[f(Y/Y_n) - f(Z/Z_n)] \end{cases} \quad (3)$$

$$f(q) = \begin{cases} q^{1/3} & (q > 0.008856) \\ 7.787q + 16/116 & (q \le 0.008856) \end{cases} \quad (4)$$

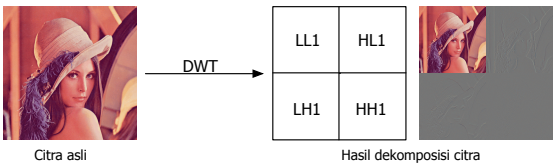
dimana $X_n = 95.047$, $Y_n = 100$, $Z_n = 108.883$

Step 2 : Dekomposisi *I* pada ruang warna CIELab untuk mentransformasi *I* dari domain *spatial* ke domain *frequency* dengan persamaan Haar DWT berikut ini :

$$H0 : f(n) = \frac{X_n + X_{n+1}}{2} \quad (5)$$

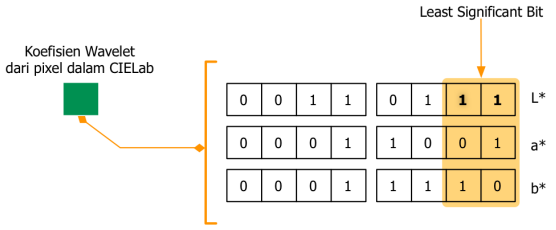
$$H1 : f(n) = \frac{X_n - X_{n+1}}{2} \quad (6)$$

dimana H_0 merupakan *low pass filter*, H_1 merupakan *high pass filter* dan X = $\{X_n\}$, n = 1, 2, ..., N merupakan *pixel-pixel* dari *I.* Proses ini dilakukan sebanyak 1 *level,* yang kemudian akan menghasilkan *sub band* LL1, LH1, HL1 dan HH1 untuk masing-masing *channel* pada ruang warna CIELab (Gambar 2).



Gambar 2. Dekomposisi *I*

Step 3 : Penyisipan pesan (*message*) pada koefisien DWT (f_{HL}(m,n) dan f_{LH}(m,n)) dari salah satu *channel* CIELab dari *I* menggunakan LSB (*Least Significant Bit*). Penyisipan ini dilakukan dengan cara mengganti 2 bit terakhir dari koefisien-koefisien DWT tersebut dengan bit-bit pesan (*message*) sehingga menghasilkan koefisien baru yang telah dimodifikasi (f'_{HL}(m,n) dan f'_{LH}(m,n)) (Gambar 3). Sedangkan *channel* yang dipilih adalah *channel L*, channel* ini dipilih agar dapat memudahkan proses penyisipan dengan LSB karena *channel* ini memiliki rentang nilai dari 0 – 100 (tidak bernilai negatif dan tidak lebih dari 255) yang jika dikonversi kedalam biner hanya akan menghasilkan deretan angka biner dengan panjang 8 bit, yang sama dengan panjang dari bit pesan (*message*) yang akan disisipkan.



Gambar 3. LSB pada koefisien *wavelet* dari *channel* CIELab

Acuan yang digunakan dalam pemilihan posisi koefisien *wavelet* (m,n) tersebut adalah dengan berdasarkan angka *random* yang yang dibangkitkan dengan *pseudo random number generator* (PRNG) dengan kunci tertentu (*k*), yang memiliki rentang dari 1 – *N*. *Sub band* LH_1 dan HL_1 dipilih dengan alasan untuk menjaga keseimbangan antara *imperceptibility* dan *robustness* dari *stego-image* yang akan dihasilkan.

Step 4 : Terapkan *Inverse Discrete Wavelet Transform* (IDWT) 1 *level* pada *I* hasil Step 3 untuk mentransformasi *I* kembali ke domain *spatial* dengan persamaan berikut :

$$Y_n = X_n + X_{n+m} \quad (7)$$

$$Y_{n+1} = X_n - X_{n+m} \quad (8)$$

dimana m = N / 2,

Step 5 : Konversi *I* hasil step sebelumnya dari CIELab kembali ke RGB untuk menghasilkan *stego-image* (*I'*), dengan persaman berikut ini :

$$X = Xn * (P + a^* / 500)^3 \quad (9)$$

$$Y = Yn * P^3 \quad (10)$$

$$Z = Zn * (P - b^* / 200)^3 \quad (11)$$

dimana P = (L* + 16) / 116

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 3.240 & -1.537 & -0.498 \\ -0.969 & 1.875 & 0.041 \\ 0.055 & -0.204 & 1.057 \end{bmatrix} . \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \quad (12)$$

2.2 Proses Ekstraksi (*Extraction*)

Pada penelitian ini proses ekstrasi dapat dilakukan tanpa memerlukan citra asli (*original image*) melainkan hanya menggunakan *stego-image* (*I'*) saja atau yang dikenal dengan istilah *blind steganography*. Adapun rincian proses yang dilakukan pada tahap ini adalah sebagai berikut :

Step 1 : Konversi *I'* dari ruang warna RGB ke ruang warna CIELab seperti pada proses *embedding* dengan persamaan (1), (2), (3) dan (4).

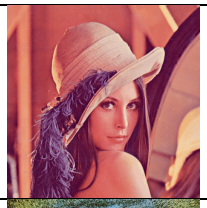
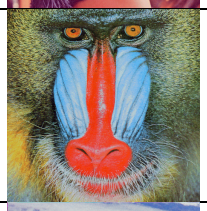
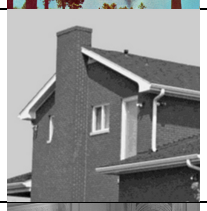
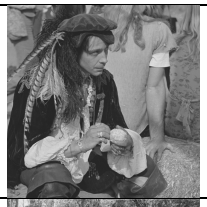
Step 2 : Dekomposisi *I'* pada ruang warna CIELab untuk mentransformasi *I'* dari domain *spatial* ke domain *frequency* seperti pada proses *embedding* dengan persamaan (5) dan (6).

Step 3 : Ektraksi pesan dari f'_{HL}(m,n) dan f'_{LH}(m,n), dimana posisi koefisien (m,n) kembali dibangkitkan menggunakan PRNG dengan kunci *k* yang sama, seperti yang digunakan pada saat penyisipan. Proses ekstraksi ini dilakukan dengan mengumpulkan 2 bit terakhir dari masing-masing koefisien dan kemudian disimpan per 8 bit sebagai bit-bit dari pesan yang nantinya akan dibentuk menjadi sebuah *file*.

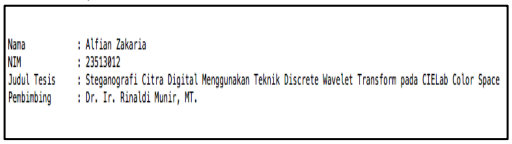
3. Eksperimen dan Pembahasan

Metode usulan diatas diprogram menggunakan bahasa pemrograman C#. Sepuluh buah citra uji standard yang digunakan dalam eksperimen ini, yakni 5 buah citra berwarna dan 5 buah citra *grayscale* yang masing-masing berukuran 512 x 512 *pixex,* yang diperlihatkan pada Tabel 1. Kunci yang digunakan untuk membangkitkan bilangan *random* pada eksperimen ini adalah "1".

Tabel 1. Citra uji standar yang digunakan

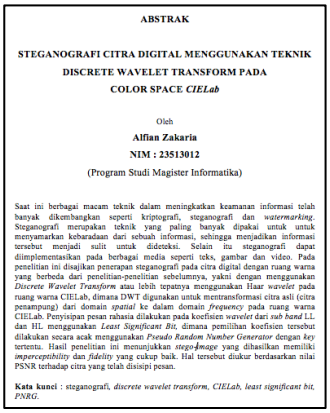
No.	Citra Asli	
1.	lena.png (526 kb)	
2.	baboon.png (654 kb)	
3.	jetplane.png (476 kb)	
4.	peppers.png (502 kb)	
5.	lake.png (587 kb)	
6.	house.png (122 kb)	
7.	couple.png (181 kb)	
8.	pirate.png (182 kb)	
9.	walkbridge.png (253 kb)	
10.	woman.png (147 kb)	

Sedangkan pesan (*message*) yang akan disisipkan dalam eksperimen ini yakni berupa 4 jenis *file* yang berbeda, masing-masing 1 buah *file* teks 'info.txt' dengan ukuran 193 *bytes* (Gambar 4), 1 buah *file* citra *grayscale* 'cameraman.jpg' dengan ukuran 21 kb (Gambar 5), 1 buah *file* dokumen 'abstrak.doc' dengan ukuran 27 kb (Gambar 6), dan 1 buah *file audio* 'match.mp3' dengan ukuran 26 kb (Gambar 7).


Nama : Alfian Zakaria
NIM : 23513012
Judul Tesis : Steganografi Citra Digital Menggunakan Teknik Discrete Wavelet Transform pada CIELab Color Space
Pembimbing : Dr. Ir. Rinaldi Munir, MT.

Gambar 4. *File* teks 'info.txt (*message*)

Gambar 5. *File* citra *grayscale* 'cameraman.jpg' (*message*)


ABSTRAK

STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN TEKNIK DISCRETE WAVELET TRANSFORM PADA COLOR SPACE *CIELab*

Oleh

Alfian Zakaria

NIM : 23513012

(Program Studi Magister Informatika)

Saat ini berbagai macam teknik dalam meningkatkan keamanan informasi telah banyak dikembangkan seperti kriptografi, steganografi dan *watermarking*. Steganografi merupakan teknik yang paling banyak dipakai untuk untuk menyamarkan kebaradaan dari sebuah informasi, sehingga menjadikan informasi tersebut menjadi sulit untuk dideteksi. Selain itu steganografi dapat diimplementasikan pada berbagai media seperti teks, gambar dan video. Pada penelitian ini disajikan penerapan steganografi pada citra digital dengan ruang warna yang berbeda dari penelitian-penelitian sebelumnya, yakni dengan menggunakan *Discrete Wavelet Transform* atau lebih tepatnya menggunakan Haar *wavelet* pada ruang warna CIELab, dimana DWT digunakan untuk mentransformasi citra asli (citra penampung) dari domain *spatial* ke dalam domain *frequency* pada ruang warna CIELab. Penyisipan pesan rahasia dilakukan pada koefisien *wavelet* dari *sub band* LL dan HL menggunakan *Least Significant Bit*, dimana pemilihan koefisien tersebut dilakukan secara acak menggunakan *Pseudo Random Number Generator* dengan *key* tertentu. Hasil penelitian ini menunjukkan *stego-image* yang dihasilkan memiliki *imperceptibility* dan *fidelity* yang cukup baik. Hal tersebut diukur berdasarkan nilai PSNR terhadap citra yang telah disisipi pesan.

Kata kunci : steganografi, *discrete wavelet transform, CIELab, least significant bit, PNRG.*

Gambar 6. *File* dokumen 'abstrak.doc' (*message*)

Gambar 7. *File* audio ‘match.mp3’ (*message*)

Hasil-hasil eksperimen terhadap beberapa citra yang dipilih pada Tabel 1 dituliskan pada bagian di bawah ini.

3.1 Hasil Proses *Embedding*

Gambar 8 menunjukkan *stego-image* dari citra ‘lena’ hasil proses penyisipan *file* ‘info.txt’, sedangkan Gambar 9 menunjukkan *stego-image* dari citra ‘peppers’ hasil proses penyisipan *file* ‘cameraman.jpg’.

Gambar 8. *Stego-image* dari *message* ‘cameraman.jpg’

Stego-image hasil penyisipan file ‘info.txt’ (Gambar 8) memiliki nilai PSNR = 35.01 dB. PSNR (*peak signal to noise ratio*) dihitung dengan rumus $PSNR = 10log_{10}\left[\frac{255^2}{MSE}\right]$, yang dalam hal ini MSE adalah singkatan dari *mean squared error*.

Gambar 9. *Stego-image* dari *message* ‘cameraman.jpg’

Gambar 9 menunjukkan *stego-image* dari pesan ‘cameraman.jpg’, dimana *stego-image* tersebut memiliki nilai PSNR = 31.48 dB.

Gambar 10. *Stego-image* dari *message* ‘abstrak.doc’ untuk citra *grayscale*

Gambar 10 menunjukkan *stego-image* dari pesan ‘abstrak.doc’ pada citra *grayscale* ‘pirate.png’, dimana *stego-image* tersebut memiliki nilai PSNR = 32.07 dB.

Gambar 11. *Stego-image* dari *message* ‘match.mp3’ untuk citra *grayscale*

Gambar 11 menunjukkan *stego-image* dari pesan ‘abstrak.doc’ pada citra *grayscale* ‘woman.png’, dimana *stego-image* tersebut memiliki nilai PSNR = 31.52 dB.

3.2 Hasil Proses *Extracting*

Secara umum proses ektraksi pesan pada eksperimen ini dapat dilakukan secara baik, selain itu hasil ekstraksi pesan dari seluruh *stego-image* yang dihasilkan dalam eksperimen ini adalah utuh sama persis seperti *file* pesan sebelum proses penyisipan dilakukan. Untuk lebih lengkapnya, keseluruhan dari hasil eksperimen pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Hasil eksperimen

Citra Asli	Pesan (*Message*)	PSNR (dB)	Eks-traksi
lena.png	info.txt	35.01	Baik
	cameraman.jpg	32.73	Baik
	abstrak.doc	31.71	Baik
	match.mp3	32.3	Baik
baboon.png	info.txt	35.98	Baik
	cameraman.jpg	32.8	Baik
	abstrak.doc	31.69	Baik
	match.mp3	32.29	Baik
jetplane.png	info.txt	30.78	Baik
	cameraman.jpg	29.78	Baik
	abstrak.doc	29.23	Baik
	match.mp3	29.59	Baik
peppers.png	info.txt	33.38	Baik
	cameraman.jpg	31.48	Baik

	abstrak.doc	30.64	Baik
	match.mp3	31.14	Baik
lake.png	info.txt	32.09	Baik
	cameraman.jpg	30.68	Baik
	abstrak.doc	30.03	Baik
	match.mp3	30.42	Baik
house.png	info.txt	33.24	Baik
	cameraman.jpg	31.69	Baik
	abstrak.doc	31.01	Baik
	match.mp3	31.47	Baik
couple.png	info.txt	35.81	Baik
	cameraman.jpg	33.09	Baik
	abstrak.doc	32.04	Baik
	match.mp3	32.65	Baik
pirate.png	info.txt	35.57	Baik
	cameraman.jpg	33.09	Baik
	abstrak.doc	32.07	Baik
	match.mp3	32.66	Baik
walkbridge.png	info.txt	34.21	Baik
	cameraman.jpg	32.02	Baik
	abstrak.doc	31.16	Baik
	match.mp3	31.64	Baik
woman.png	info.txt	33.13	Baik
	cameraman.jpg	31.77	Baik
	abstrak.doc	31.08	Baik
	match.mp3	31.52	Baik

4. Kesimpulan

Sebuah usulan metode dalam steganografi citra digital pada domain frekuensi telah dipresentasikan. Hasil eksperimen ini menujukkan bahwa ruang warna CIELab dapat digunakan dalam steganografi dengan menggunakan *Discrete Wavelet Transform* serta dapat menghasilkan *stego-image* dengan *imperceptibility* dan *fidelity* yang cukup baik yang didasarkan pada hasil pengukuran PSNR yang masih berada di atas dari 30 dB dan *stego-image* yang sama persis dengan citra aslinya, selain itu tingkat *recovery* pesan dari *stego-image* yang dihasilkan sangat baik karena pesan yang disisipkan dapat diekstraksi secara utuh seperti semula.

Daftar Pustaka :

[1] Cheddad, A. (2007) : *Strengthening Steganography in Digital Images*, Disertasi Program Doktor, University of Ulster, Magee.

[2] Conrad, E., Misenar, S., Feldman J. (2013) : *CISSP Study Guide*, Elsevier, Waltham.

[3] Cox I. J., Miller, M. L., Bloom, J. A., Fridrich, J., Kalker T. (2007) : *Digital Watermarking And Steganography Second Edition*. Morgan Kaufmann Publishers, USA

[4] Harmsen, J. dan Pearlman, W. (2003) : *High-Order Statistical of Palette Images*, in Proc. SPIE Security Watermarking Multimedia Contents, 5020, 131-142.

[5] Hemalatha, S., Acharya, U. D., Renuka, A. (2013) : *Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB And YCbCr Domains, International Journal of Advanced Information Technology*, 3, 1-9.

[6] Iza, D. R. (2013) : *Steganografi pada Citra Digital Menggunakan Metode rDiscrete Wavelet Transform*, Universitas Brawijaya, Malang.

[7] Joshi, S. V., Bokil A. A., Jain, N. A., Koshti, D. (2012) : *Image Steganography Combination of Spatial and Frequency Domain*, International Journal of Computer Applications, 53, 25 - 29.

[8] Khalili, M. dan Asatryan D. (2013) *: Colour Spaces Effects on Improved Discrete Wavelet Transform-Based Digital Image Watermarking using Arnold Transform Map*, IET Signal Processing, 7, 177 – 187.

[9] Li-na, H., Guo-hua, G., Jie, X., Zheng-long, X. (2009) : *Real-color Image Denoised and Enhanced Synchronously Based on Wavelet Transform*, IEEE International Conference on Intelligent Computation Technology and Automation, 658 – 661.

[10] Mandal, J. K. dan Das, D. (2012) : *Color Image Steganography Based on Pixel Value Differencing in Spatial Domain*, International Journal of Information Sciences and Technique, 2, 83 - 93.

[11] Munir, R. (2004) : *Pengolahan Citra Digital, Informatika*, Bandung.

[12] Polikar, R. (1998) : *Multi Resolution Analysis: The Discrete Wavelet Transform*, Iowa State University, Iowa.

[13] Rahardjo, B. (2005) : *Keamanan Sistem Informasi Berbasis Internet*, PT Indocisc, Bandung.

[14] Roy, R., Changder, S., Sarkar, A., Debnath, N. C., (2013) : *Evaluating image Steganography Techniques: Future Research Challanges*, IEEE Conference on Computing, Management and Telecomunications, 309 - 314.

[15] Sripathi, D. (2003) : *Effiicient Implementations of Discrete Wavelet Transform Using FPGAs*, Florida State University, Florida.