Rancang Bangun Perangkat Lunak Transformasi Wavelet Haar Level 3 Pada *Least Significant Bit* (Lsb) *Steganography*

Abdul Haris[1], Febi Yanto[2]
[1,2] Teknik Informatika, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau
Jl. H.R. Soebrantas No. 155 KM. 18 Simpang Baru, Pekanbaru 28293
email: haris7233@gmail.com[1], febiyanto@uin-suska.ac.id[2]

Abstrak

Least Significant Bit Steganography bekerja dengan menyisipkan beberapa bit teks informasi ke beberapa bit terakhir citra *carrier* dan hanya menyebabkan perubahan beberapa bit pada citra *carrier* tersebut sehingga tidak berbeda jauh dari sebelumnya, minimal tidak dapat dibedakan oleh indra *visual* manusia. Dalam steganografi, setiap informasi yang disisipkan harus dapat di-*retrieve* kembali untuk dibaca. *Retrieving* informasi dilakukan dengan cara mengumpulkan kembali bit-bit rahasia pada citra *carrier* yang telah ditanami bit-bit informasi tersebut. Untuk mengumpulkan bit-bit rahasia ini maka diperlukan informasi dimana persisnya letak bit-bit tersebut. Dalam transformasi wavelet haar, citra *carrier* akan didekomposisi menjadi 4 *subband* baru untuk menggantikan citra semula. Pengembangan penelitian ini, transformasi akan dilakukan 3 level sehingga *subband* area penyisipan akan berukuran 1/64 kali *carrier* asli dan keseluruhan *subband* atau kombinasi s*ubband* level 3 akan digunakan sebagai area *embedding.* Penelitian ini bertujuan untuk melihat pengaruh pemilihan kombinasi *subband* terhadap kualitas citra steganografi dan informasi yang telah disisipkan. Dari hasil pengujian, nilai PSNR yang berbeda membuktikan bahwa pemilihan kombinasi s*ubband* terbukti berpengaruh terhadap citra steganografi dan terhadap informasi yang telah disisip, dengan hasil pengujian kombinasi *subband* LL sebagai s*ubband* terbaik untuk penyisipan informasi dan menghasilkan citra steganografi yang berkualitas tinggi yaitu 72.2628 dB untuk penyisipan maksimal informasi yang dapat disisip pada kombinasi tunggal *subband* citra *carrier*.

Kata kunci : *Carrier, Least Significant Bit,* PSNR, Steganografi, *Subband,* Transformasi Wavelet Haar

1. Pendahuluan

Perlu adanya antisipasi untuk meminimalisir pencurian informasi oleh pihak ketiga yang tidak berkepentingan terhadap infomasi tersebut. Salah satu caranya adalah dengan menggunakan teknik steganografi. Steganografi adalah seni menyembunyikan keberadaan suatu informasi pada media yang tampaknya tidak berbahaya[1].

Dalam steganografi, setiap informasi yang disisipkan harus dapat di-*retrieve* (diambil) kembali untuk dibaca. *Retrieving* informasi dilakukan dengan cara mengumpulkan bit-bit rahasia pada citra *carrier* yang telah ditanami bit-bit informasi. Untuk mengumpulkan bit-bit rahasia ini maka diperlukan informasi dimana persisnya area peletakan bit-bit tersebut. Pada metode *Least Significant Bit* (LSB) Steganografi konvensional, bit-bit informasi akan disisip berurutan sesuai dengan urutan nilai piksel citra *carrier*. Sehingga informasi rahasia yang telah disisip tidak terjamin keamanannya. Dengan alasan inilah citra *carrier* pada penelitian ini akan ditransformasi terlebih dahulu menggunakan Transformasi Wavelet Haar sebelum proses penyisipan informasi dilakukan.

Pada Transformasi Wavelet Haar, citra *carrier* akan didekomposisi menjadi 4 *subband (sub-image)* baru untuk menggantikan citra semula. Proses demikian dapat diulang seterusnya, sesuai dengan level (tingkatan) transformasi yang diinginkan [2]. Dalam penelitian ini, transformasi citra *carrier* akan dilakukan 3 level. Transformasi pertama dan kedua akan dilakukan pada *subband* LL (aproksimasi). Transformasi 3 level ini akan meningkatkan keamanan informasi yang disembunyikan karena informasi tersebut "ditanam" lebih dalam dibandingkan dengan hanya ditransformasi satu level. Namun, proses transformasi yang berulang kali mengakibatkan berkurangnya kapasitas informasi yang akan disisip apabila *subband* yang digunakan hanya satu dari 4 *subband* hasil transformasi yang nantinya akan berukuran 1/64 kali dari citra asli. Hal ini menjadi permasalahan tersendiri, yaitu bagaimana agar kapasitas penyembunyian informasi bisa lebih besar tanpa mengorbankan keamanan informasi seperti yang telah dijelaskan sebelumnya. Solusi yang tepat menurut peneliti adalah

dengan memberikan fleksibilitas kombinasi *subband* peletakan informasi yang akan disisipkan pada 4 *subband* hasil transformasi ketiga. Kemungkinan terjadinya peletakan informasi pada keempat *subband level* 3 adalah sebanyak 64 kombinasi *subband* (urutan *subband* diperhatikan). Sehingga secara tidak langsung, selain memberikan solusi terhadap masalah kapasitas informasi yang akan disisip, fleksibilitas pemilihan kombinasi *subband* yang akan digunakan sebagai area penyisipan informasi ini juga dapat lebih meningkatkan keamanan informasi selain dengan "ditanam" lebih dalam pada citra *carrier*-nya tersebut. Sehingga dapat disimpulkan bahwa penelitian ini bertujuan untuk mengetahui apakah pengaruh kombinasi subband terhadap citra *carrier* dan informasi yang telah disisip dan berapa maksimal informasi teks yang dapat disembunyikan pada citra *carrier* yang telah didekomposisi tiga level. Tentunya yang diharapkan ukuran dan kualitas citra tidak berubah banyak dan informasi yang disembunyikan dapat di-*retrieve* kembali.

Untuk itu, diangkatlah sebuah penelitian yaitu "Rancang Bangun Perangkat Lunak Transformasi Wavelet Haar Level 3 Pada *Least Significant Bit* (LSB) *Steganography* " dimana Wavelet Haar digunakan sebagai metode untuk mentransformasikan citra *carrier* dan metode LSB untuk menyisipkan informasi kedalam bit citra *carrier.*

2. Landasan Teori

2.1 Format Citra PNG

Format citra yang akan digunakan pada penelitian ini adalah format citra PNG. Format ini digunakan sebagai Citra C*arrier* yaitu citra tampung yang akan digunakan untuk menyisipkan informasi rahasia, dan Citra Steganografi yaitu citra hasil penyisipan informasi juga akan berformat PNG untuk meminimalisir kecurigaan pihak ketiga akan adanya informasi yang terdapat didalamnya.

Format PNG adalah format penyimpanan citra terkompresi. Format ini dapat digunakan pada citra *grayscale,* citra dengan palet warna, dan citra *fullcolor*. Format png juga mampu menyimpan informasi hingga kanal *alpha* (kanal yang mengatur transparansi citra) dengan penyimpanan sebesar 1 hingga 16 bit perkanal.

2.2 Format Citra TIFF

Sebuah file TIFF dimulai dengan file 8 *byte header* gambar yang menunjuk ke direktori file gambar (IFD) [3]. Direktori file gambar berisi informasi tentang gambar, seperti petunjuk ke data gambar yang sebenarnya. Urutan 8-*byte* file *header* gambar tersebut adalah sebagai berikut:

1. *Bytes* 0-1: Urutan *byte* digunakan di dalam file. Nilai legalnya adalah "II" (4949.H) dan "MM" (4D4D.H).
2. *Bytes* 2-3 : Sembarang tapi dipilih nomor (42) yang selanjutnya mengenali file sebagai file TIFF. Urutan *byte* tergantung pada nilai Bytes 0-1.
3. *Bytes* 4-7 : Nilai offset (dalam *bytes*) dari IFD pertama.

Format citra TIFF pada penelitian ini digunakan sebagai format untuk Citra Key, yaitu citra yang harus ada (sebagai kunci) saat informasi yang telah disisipkan pada Citra Steganografi yang berformat PNG akan di-*retrieve* kembali. Apabila Citra Key ini tidak terdapat pada folder yang sama dengan Citra Steganografi, maka informasi yang terdapat didalamnya tidak akan dapat diambil kembali untuk dibaca.

2.3 Transformasi Wavelet Haar

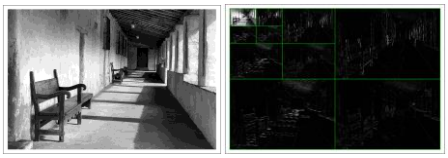
Transformasi *Wavelet* merupakan sebuah fungsi konversi yang dapat membagi fungsi atau sinyal ke dalam komponen frekuensi atau skala yang berbeda, dan selanjutnya dapat dipelajari setiap komponennya tersebut dengan resolusi tertentu sesuai dengan skalanya [2]. Fungsi skala (*scaling function*) disebut juga dengan *Lowpass Filter* maksudnya skala ini yang akan mengambil citra dengan gradiasi intensitas yang halus dan perbedaan intensitas yang tinggi akan dikurangi atau dibuang. Sedangkan fungsi *wavelet* (*wavelet function*) disebut juga dengan *Highpass Filter* maksudnya fungsi ini yang mengambil citra dengan gradiasi intensitas yang tinggi dan perbedaan intensitas yang rendah akan dikurangi atau dibuang. Kedua fungsi ini digunakan pada saat Transformasi *Wavelet.*

Jenis *Wavelet* yang digunakan dalam penelitian ini adalah Wavelet Haar yang berfungsi untuk membagi subband peletakan atau penyisipan informasi menjadi subband yang lebih spesifik sehingga tingkat keamanan steganografi LSB dapat lebih ditingkatkan. Koefisien transformasi tapis *low-pass* dan tapis *high-pass* fungsi basis wavelet haar:

Tapis *Lowpass:* h0 = (1/√2 , 1/√2)
Tapis *Highpass:* h1 = (1/√2 , - 1/√2)

Maka cara untuk memperoleh nilai LL, LH, HL dan HH adalah :

1. LL (*Aproksimasi*) : filter *lowpass* terhadap baris kemudian filter *lowpass* terhadap kolom
2. LH (Detil *Horizontal*) : filter *lowpass* terhadap baris kemudian filter *highpass* terhadap kolom
3. HL (Detil *Vertikel*) : filter *highpass* terhadap baris kemudian filter *lowpass* terhadap kolom
4. HH (Detil *Diagonal)* : filter *highpass* terhadap baris kemudian filter *highpass* terhadap kolom.



Gambar 1. Perbandingan Citra Asli dan Citra Hasil Transformasi Wavelet Haar 3 level (*sumber : whydomath.org/node/wavlets*)

2.4 Steganografi

Steganografi adalah teknik menyembunyikan data rahasia didalam sebuah media digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain [4]. Pada penyembunyian data rahasia dengan media *carrier* citra tentu akan membuat kualitas citra berubah, untuk itu perlu adanya kriteria apabila ingin melakukan penyembunyian data. kriteria penyembunyian data rahasia pada citra haruslah memperhatikan hal-hal berikut:

1. *Fidelity*, yaitu kualitas citra yang tidak terlalu jauh berubah.
2. *Robustness*, yaitu data yang disembunyikan harus tahan (*robust)* terhadap berbagai operasi manipulasi citra.
3. *Recovery*, yaitu data yang disembunyikan harus dapat diungkapkan kembali (*reveal*).

Metode dan teknik steganografi pada file digital yang telah dikenal, antara lain [5]:

1. *Least Significant Bit* (LSB).
2. *Masking and Filtering.*
3. *Dynamic Cell Spreading.*
4. *Algorithm and Transformations.*
5. *Spread Spectrum Method.*

2.4.1 Least Significant Bit

Least significant bit merupakan metode standar yang banyak digunakan untuk melakukan steganografi terutama pada media citra digital perubahan satu bit pada *least significant bit* tidak akan mengakibatkan perubahan warna yang cukup besar sehingga tidak dapat terlihat secara kasat mata oleh orang lain [6].

Konsep dasar dari subtitusi LSB adalah dengan menggantikan data rahasia di paling kanan bit (bit dengan bobot terkecil) sehingga prosedur *embedding* tidak signifikan mempengaruhi nilai pixel aslinya [7]. Representasi matematika pada metode LSB adalah:

$$Xi' = Xi - Xi \bmod 2^k + Mi$$

Dimana:

Xi' = Mewakili i nilai piksel dari citra stego
Xi = Mewakili i nilai piksel dari citra *carrier*
k = Jumlah bit LSB yang akan digantikan
Mi = Nilai desimal dari i blok teks informasi

Untuk proses *retrieving* informasi, dapat dilakukan dengan rumus matematis berikut:

$$M_i = X_i \bmod 2^k$$

2.5 PSNR

Untuk mengevaluasi kualitas citra hasil steganografi adalah dengan penilaian secara *obyektif* yaitu menghitung nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR), secara matematis dapat dirumuskan sebagai berikut:

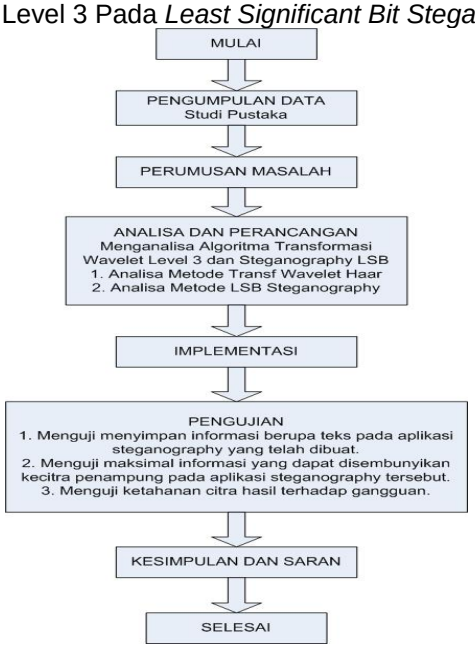
$$MSE = \frac{1}{mn} \sum_{i}^{m} \sum_{j}^{n} ||I(i,j) - K(i,j)||^2$$

$$PSNR = 10 \cdot \log\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Semakin besar PSNR, semakin baik pula kualitas gambar yang dihasilkan (Alatas, 2009)[8]

3. Metodologi Penelitian

Metodologi penelitian adalah acuan dan tahapan yang diterapkan pada sebuah penelitian untuk mencapai tujuan penelitian. Gambar 2 berikut adalah tahapan metodologi yang digunakan dalam penelitian tugas akhir yang berjudul "Rancang Bangun Perangkat Lunak Transformasi Wavelet Haar Level 3 Pada *Least Significant Bit Steganography*".

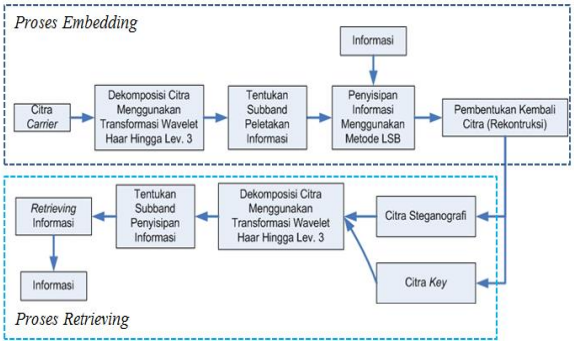


Gambar 2. Tahapan Metodologi Penelitian

4. Analisa Dan Perancangan

4.1 Gambaran Umum Sistem

Gambaran umum tahapan yang dilakukan dalam proses *embedding* dan *retrieving* informasi menggunakan Transformasi Wavelet Haar dan *Least Significant Bit* Steganografi pada penelitian ini dapat dilihat pada gambar 3 berikut.



Gambar 3. Gambaran Umum Tahapan Proses *Embedding* dan *Retrieving* Transformasi Wavelet Haar Pada *Least Significant Bit* Steganografi

1. Citra *Carrier*
   Citra yang digunakan dalam penelitian ini adalah citra warna RGB 24-bit berformat png.
2. Dekomposisi Citra *Carrier*
   Citra *carrier* akan didekomposisi dengan mentransformasikan citra *carrier* menjadi 4 *subband* baru hingga 3 level.

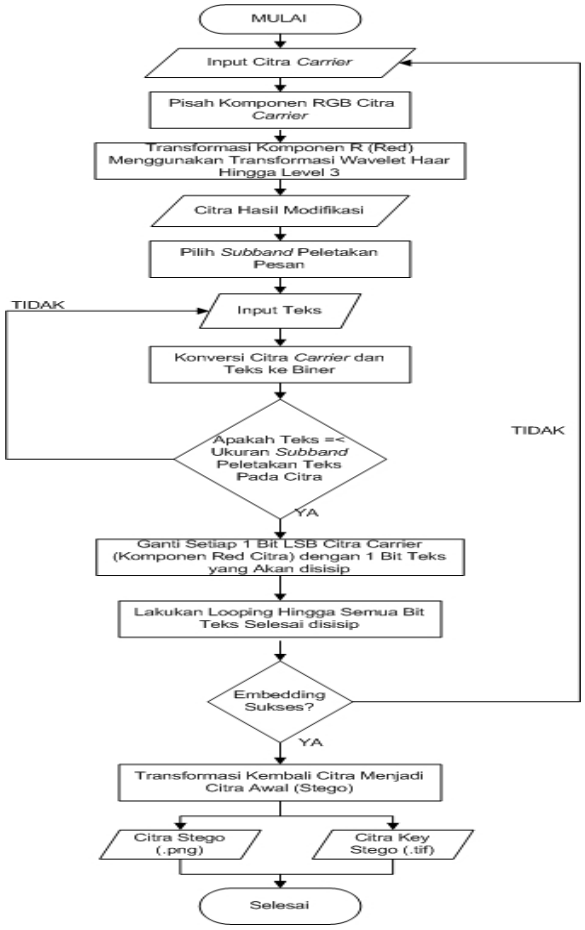
3. Subband Peletakan / Penyisipan Informasi.
   Pengembangan penelitian pada LSB steganografi menggunakan Transformasi Wavelet Haar pada penelitian ini adalah dengan memberikan fleksibilitas *subband* peletakan informasi yang ingin disisipkan pada 4 kombinasi *subband* (LL, HL, LH dan HH) hasil transformasi ketiga.
4. Informasi
   Informasi yang akan disisipkan pada penelitian ini adalah informasi berbasis teks.
5. Penyisipan / *Embedding* Informasi
   Least Significant Bit, teknik ini merupakan teknik dengan cara melakukan perubahan atau modifikasi pada *bit-bit* yang tidak terlalu berpengaruh *(unsignificant)* yang pada penelitian ini modifikasi dilakukan pada 1 bit pada komponen *Red* citra *carrier*.
6. Rekontruksi Citra
   Rekontruksi citra adalah proses pembentukan kembali (*inverse*) citra kebentuk semula. Pada penelitian ini rekontruksi citra menghasilkan 2 output citra, yaitu citra steganografi dan key citra steganografi.
7. Citra Steganografi
   Citra stego berformat sama dengan citra aslinya yaitu citra berformat png.
8. Citra *Key*
   Citra *key* adalah citra hasil pengurangan dari citra FullRecovere.tif dengan citra steganografi berformat png, sehingga nilai pikselnya berupa bilangan berkoma kurang dari 1 dan bilangan nol. Citra *key* akan berformat tiff dan beratribut hidden sehingga filenya akan tersembunyi.
9. *Retrieving* Informasi
   Data yang disembunyikan didalam citra dapat dibaca kembali dengan me-*retrieve* kembali untuk dibaca.

4.2 Perancangan *Flowchart Embedding*

Proses *embedding* adalah proses penyembunyian teks informasi pada citra *carrier*. Secara umum, proses *embedding* rancang bangun perangkat lunak steganografi yang akan dibangun dapat dilihat pada gambar 4. *flowchart* berikut:

Berdasarkan gambar 4. *flowchart* proses *embedding* dapat dijelaskan bahwa:

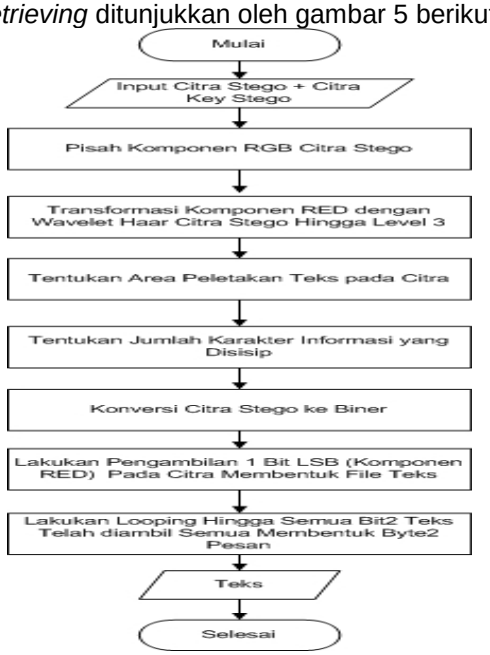
1. Proses dimulai dengan menginput citra *carrier* berformat png kesistem.
2. Komponen RGB citra *carrier* yang telah diinputkan akan dipisah sesuai komponennya masing-masing.
3. Komponen *Red* citra *carrier* yang telah dipisah akan ditransformasikan menggunakan Transformasi Wavelet Haar hingga level 3.
4. Kemudian *user* akan memilih *subband* atau kombinasi *subband* mana yang menjadi tempat peletakan teks informasi.
5. *User* lalu akan menginput teks informasi yang akan disisipkan.
6. Sistem akan mengkonversikan citra dan teks ke biner. Lalu dibandingkan kapasitas ukuran teks dan kapasitas subband citra *carrier* apakah sesuai.
7. Lakukan proses *embedding* dengan mengganti setiap 1 bit LSB komponen *Red* pada citra *carrier* dengan bit-bit teks informasi yang diinputkan *user* sebelumnya.
8. Apabila proses *embedding* sukses maka dilakukan proses rekontruksi kembali citra dengan menggunakan Transformasi Wavelet Haar oleh sistem membentuk citra semula yang kemudian dikenal dengan nama citra_stego.png dan keynya berupa key_citra_stego.tif.
9. Selesai.



Gambar 4. Flowchart *Proses* Embedding

4.3 Perancangan *Flowchart Retrieving*

Flowchart proses *retrieving* ditunjukkan oleh gambar 5 berikut:



Gambar 5. Flowchart *Proses* Retrieving

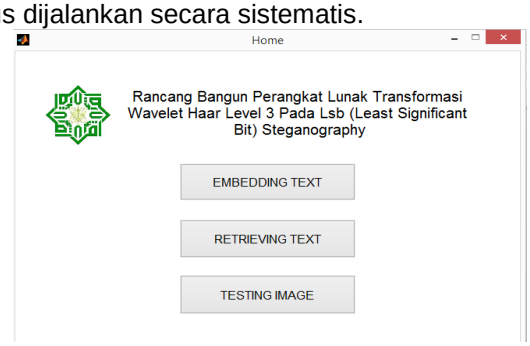
Berdasarkan gambar 5 *flowchart* proses *retrieving* diatas dapat dijelaskan bahwa:

1. Proses dimulai dengan menginput citra_stego.png dan key_citra_stego.tif kesistem.
2. Hasil penjumlahan kedua nilai piksel citra_stego.png dan key_citra_stego.tif yang telah diinputkan akan dipisahkan sesuai dengan komponen RGB nya.
3. Komponen *Red* pada citra tersebut akan ditransformasikan menggunakan Transformasi Wavelet Haar hingga level 3.
4. Kemudian *user* akan memilih *subband* mana yang menjadi tempat peletakan teks informasi yang nantinya akan di-*retrieve* kembali.
5. Sistem akan mengkonversi barisan nilai piksel komponen *Red* citra ke biner.
6. Ambil setiap 1 bit LSB citra_stego dan lakukan perulangan hingga proses selesai dimana 1 bit yang diambil disusun membentuk teks kembali.
7. Selesai.

5. Implementasi dan Pengujian

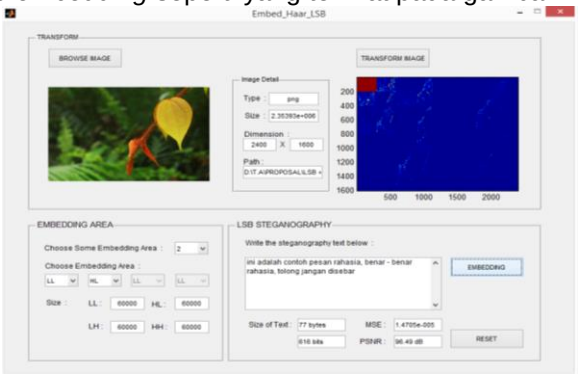
5.1 *Interface* Perangkat Lunak

Gambar 6 berikut merupakan menu utama ketika sistem dijalankan, terdiri dari beberapa form yang harus dijalankan secara sistematis.



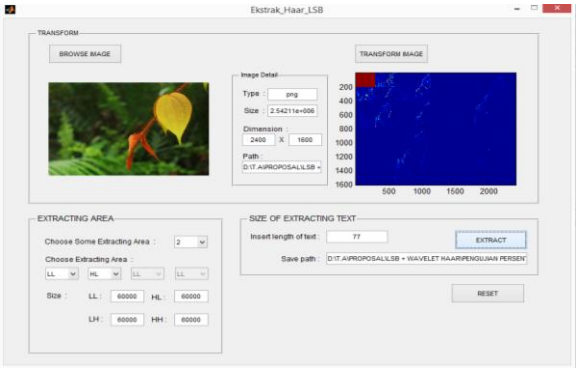
Gambar 6. Tampilan Menu Utama (Home) Sistem Steganografi

Menu berikutnya merupakan menu *embedding* teks, yaitu menu untuk proses penyisipan teks ke citra carrier yang akan ditransformasikan menggunakan Transformasi Wavelet Haar, bertujuan untuk membagi per-area citra carrier sehingga penyisipan informasi dapat lebih aman. Menu *embedding* seperti yang terlihat pada gambar 7 berikut.



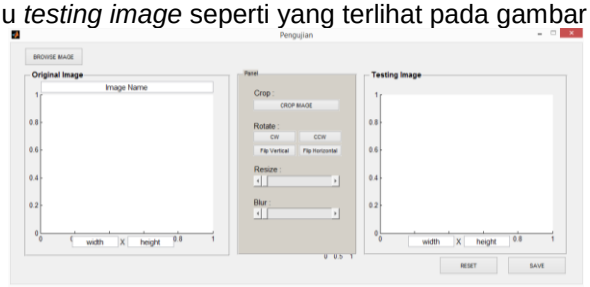
Gambar 7. Tampilan Sistem Steganografi Menu Embeding Teks

Menu berikutnya merupakan menu *retrieving* teks, yaitu menu untuk pengambilan kembali informasi yang telah disisip sebelumnya. Gambar 8 berikut merupakan menu *retrieving* teks.



Gambar 8. Tampilan Sistem Steganografi Menu Retrieving Teks

Menu berikutnya adalah menu *testing image*, menu ini digunakan untuk menguji citra steganografi apakah cukup *robust* terhadap serangan manipulasi yang dilakukan terhadap citra steganografi. Serangan serangan tersebut adalah proses *cropping, resizing, blurring*, dan *rotating*. Tampilan menu *testing image* seperti yang terlihat pada gambar 9 berikut.



Gambar 9. Tampilan Sistem Steganografi Menu Testing Image (Pengujian Robustness)

5.2 Pengujian Terhadap Fidelity Citra Steganografi

Pengujian dilakukan pada satu citra *carrier* dengan menggunakan seluruh *subband* atau kombinasi *subband* yang mungkin dilakukannya penyisipan informasi pada *subband* tersebut. Tentunya dengan ukuran informasi yang berbeda.

Tabel 1. Pengujian terhadap kualitas citra steganografi

No	CITRA CARRIER (PNG)	SIZE CARRIER		UKURAN KEY_CITRA_STEGO.TIFF	SUBBAND PELETAKAN / PENYISIPAN INFORMASI				SIZE INFORMASI/ PESAN	MSE	PNSR
		SEBELUM	SESUDAH		LL	HL	LH	HH			
1		143,071 bytes	150,148 bytes	1,331,762 bytes	1				5176 bytes	0.0038923	72.2628 dB
2		143,071 bytes	157,032 bytes	1,331,762 bytes		1			5176 bytes	50.9829	31.0906 dB
3	Wikinewslogo.png	143,071 bytes	156,859 bytes	1,331,762 bytes			1		5176 bytes	94.2057	28.424 dB
4		143,071 bytes	160,189 bytes	1,331,762 bytes				1	5176 bytes	14.8081	36.4598 dB
5		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2			5176 bytes	0.0036683	72.5201 dB
6		143,071 bytes	150,148 bytes	1,331,762 bytes	1		2		5176 bytes	0.0036023	72.599 dB
7		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2	3		5176 bytes	0.004372	71.758 dB
8		143,071 bytes	150,404 bytes	1,331,762 bytes	1	2	3	4	5176 bytes	0.0049188	71.2462 dB
1		143,071 bytes	150,148 bytes	1,331,762 bytes	1				2568 bytes	0.0018615	75.4662 dB
2		143,071 bytes	154,337 bytes	1,331,762 bytes		1			2568 bytes	26.3379	33.95898 dB
3	Wikinewslogo.png	143,071 bytes	153,616 bytes	1,331,762 bytes			1		2568 bytes	44.4175	31.6893 dB
4		143,071 bytes	154,878 bytes	1,331,762 bytes				1	2568 bytes	6.3382	40.1452 dB
5		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2			2568 bytes	0.0024806	74.2192 dB
6		143,071 bytes	150,148 bytes	1,331,762 bytes	1		2		2568 bytes	0.0024805	74.2194 dB
7		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2	3		2568 bytes	0.0027063	73.841 dB
8		143,071 bytes	150,249 bytes	1,331,762 bytes	1	2	3	4	2568 bytes	0.0027781	73.7273 dB
1		143,071 bytes	150,148 bytes	1,331,762 bytes	1				1256 bytes	0.0012448	77.2139 dB
2	Wikinewslogo.png	143,071 bytes	151,908 bytes	1,331,762 bytes		1			1256 bytes	17.2552	35.7956 dB
3		143,071 bytes	152,111 bytes	1,331,762 bytes			1		1256 bytes	4.7059	41.4383 dB
4		143,071 bytes	151,916 bytes	1,331,762 bytes				1	1256 bytes	1.759	45.7121 dB
5		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2			1256 bytes	0.001353	76.8517 dB
6		143,071 bytes	150,148 bytes	1,331,762 bytes	1		3		1256 bytes	0.001362	76.823 dB
7		143,071 bytes	150,148 bytes	1,331,762 bytes	1	2	3		1256 bytes	0.0014554	76.535 dB

5.3 Pengujian Terhadap Kapasitas Citra Steganografi

Pengujian dilakukan dengan menggunakan 3 sampel citra *carrier* yang berbeda ukuran maupun dimensi. 3 sampel ini akan dijadikan acuan untuk citra *carrier* yang akan digunakan selanjutnya.

Tabel 2 Pengujian terhadap kapasitas citra steganografi

CITRA CARRIER (PNG)	DIMENSI CITRA	UKURAN CARRIER		UKURAN KEY_CITRA_STEGO.TIFF	*SUBBAND* PELETAKAN / PENYISIPAN INFORMASI				UKURAN TEKS YANG DISISIP
		SEBELUM	SESUDAH		LL	HL	LH	HH	
Yellow.png	85 x 142	22,161 bytes	19,471 bytes	49,250 byte					24 bytes
Yellow.png	85 x 142	22,161 bytes	19,929 bytes	49,250 byte					24 bytes
Yellow.png	85 x 142	22,161 bytes	20,290 bytes	49,250 byte					24 bytes
Yellow.png	85 x 142	22,161 bytes	20,196 bytes	49,250 byte					24 bytes
Wikinewslogo.png	800 x 415	143,071 bytes	150,148 bytes	1,331,762 bytes					647 bytes
Wikinewslogo.png	800 x 415	143,071 bytes	157,032 bytes	1,331,762 bytes					647 bytes
Wikinewslogo.png	800 x 415	143,071 bytes	156,859 bytes	1,331,762 bytes					647 bytes
Wikinewslogo.png	800 x 415	143,071 bytes	160,189 bytes	1,331,762 bytes					647 bytes
Multifruits1.png	976 x 1044	938,719 bytes	927,479 bytes	4,092,586 bytes					1799 bytes
Multifruits1.png	976 x 1044	938,719 bytes	941,080 bytes	4,092,586 bytes					1799 bytes
Multifruits1.png	976 x 1044	938,719 bytes	945,043 bytes	4,092,586 bytes					1799 bytes
Multifruits1.png	976 x 1044	938,719 bytes	943,971 bytes	4,092,586 bytes					1799 bytes

Keterangan:
Stego baik (file informasi dapat ditampilkan sempurna)
Stego rusak (file informasi dapat ditampilkan namun maksimal setengah informasi rusak)
Stego rusak sekali (file informasi Sama Sekali Tidak Dapat Ditampilkan)

Dari hasil pengujian pada tabel 2 dapat diambil kesimpulan berupa perbandingan ukuran dimensi citra *carrier* dan ukuran informasi maksimal yang dapat disisipkan pada komponen *Red* hasil Transformasi Wavelet Haar level 3 adalah seperti pada tabel 3 berikut:

Tabel 3. Perbandingan Ukuran Citra Carrier Terhadap Ukuran Teks Informasi

Citra *Carrier*	**Dimensi Citra**	**Perbandingan *Carrier* Dan Informasi**
Yellow.png	85 x 142	12070 : 24 atau 503 : 1
Wikinewslogo.png	800 x 415	332000 : 647 atau 514 : 1
Multifruits1.png	976 x 1044	10018944 : 1799 atau 567 :1
Rata – rata perbandingan		**454338 : 824** atau **528 : 1**

Sehingga untuk setiap citra carrier yang berukuran 528 *bytes* sebelum ditransformasi hanya dapat menyisipkan 1 karakter atau 1 *bytes* informasi setelah ditransformasi hingga 3 level pada komponen *Red* citra carrier.

5.4 Pengujian Terhadap Recovery Teks Steganografi

Agar informasi dapat diambil kembali maka syaratnya yaitu citra kunci key_citra_stego.tif yang dihasilkan saat penyisipan informasi harus berada satu *folder* dan bernama sama dengan citra stego nya.

Tabel 4 Pengujian terhadap recovery teks steganografi

No	CITRA CARRIER (PNG)	SIZE CARRIER	SUBBAND PELETAKAN / PENYISIPAN INFORMASI				SIZE INFORMASI/ PESAN	MSE	PNSR
			LL	HL	LH	HH			
1	Wikinewslogo.png	143071 bytes	1				2568 bytes	0.0018615	75.4662 dB
2		143071 bytes		1			2568 bytes	26.3379	33.95898 dB
3		143071 bytes			1		2568 bytes	44.4175	31.6893 dB
4		143071 bytes				1	2568 bytes	6.3382	40.1452 dB
5		143071 bytes	1	2			2568 bytes	0.0024806	74.2192 dB
6		143071 bytes	1	2	3		2568 bytes	0.0027063	73.841 dB
7		143071 bytes	1	2	3	4	2568 bytes	0.0027781	73.7273 dB
1	Wikinewslogo.png	143071 bytes	1				1256 bytes	0.0012448	77.2139 dB
2		143071 bytes		1			1256 bytes	17.2552	35.7956 dB
3		143071 bytes			1		1256 bytes	4.7059	41.4383 dB
4		143071 bytes				1	1256 bytes	1.759	45.7121 dB
5		143071 bytes	1	2			1256 bytes	0.001353	76.8517 dB
6		143071 bytes	1	2	3		1256 bytes	0.0014554	76.535 dB
7		143071 bytes	1	2	3	4	1256 bytes	0.0014612	76.5177 dB
1	Wikinewslogo.png	143071 bytes	1				576 bytes	0.00063296	80.1511 dB
2		143071 bytes		1			576 bytes	13.1041	36.9907 dB
3		143071 bytes			1		576 bytes	1.0674	47.8814 dB
4		143071 bytes				1	576 bytes	0.52287	50.9809 dB
5		143071 bytes	1	2			576 bytes	0.00067501	79.8717 dB
6		143071 bytes	1	2	3		576 bytes	0.00070193	79.7018 dB

Keterangan:
Stego baik (file informasi dapat ditampilkan sempurna)
Stego rusak (file informasi dapat ditampilkan namun maksimal setengah informasi rusak)
Stego rusak sekali (file informasi Sama Sekali Tidak Dapat Ditampilkan)

6. Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkan analisa, perancangan dan implementasi pada perangkat lunak steganografi diatas, dapat diambil kesimpulan sebagai berikut:

1. Perangkat lunak sistem steganografi untuk menyembunyikan informasi berupa teks menggunakan metode *Least Significant Bit* dan Transformasi Wavelet Haar berhasil diimplementasikan dengan pengembangan penelitian pada fleksibilitas pemilihan area *subband* penyisipan informasi pada level 3 Transformasi Wavelet Haar.
2. Secara *visual*, tidak terlihat pengaruh apapun pada citra *carrier* kecuali perubahan ukuran *carrier* yang bertambah maupun berkurang beberapa *byte*. Sedangkan pada informasi yang disisip, kecuali penyisipan pada *subband* LL, tidak terlihat konsistensi informasi terambil sempurna saat proses *retrieving* informasi dilakukan.
3. Fleksibilitas pemilihan kombinasi *subband* dapat digunakan sebagai tempat penyisipan informasi hanya jika ukuran informasi tersebut tidak terlalu besar.
4. Perhitungan PSNR yang dilakukan pada citra hasil steganografi membuktikan bahwa kualitas citra steganografi tergantung pada pemilihan *subband* atau kombinasi *subband* yang dipilih untuk penyisipan informasi. Nilai PSNR yang tinggi tidak menjamin selalu bahwa informasi akan dapat di-*retriving* kembali secara sempurna.
5. Citra key_citra_stego.tif yang digunakan sebagai *key* keamanan citra stego saat me-*retrieving* kembali informasi terbukti dapat dijadikan sebagai bentuk keamanan citra stego.
6. Citra steganografi tidak tahan terhadap manipulasi citra seperti *cropping, rotating, resizing* dan *blurring*.

6.2 Saran

Beberapa hal yang disarankan untuk pengembangan penelitian selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya tidak menutup kemungkinan dikembangkan menggunakan media digital dan citra digital dengan format yang lain. Untuk melihat perbandingan media digital dan citra digital dengan format apakah yang ideal digunakan sebagai media *carrier* menggunakan metode *Least Significant Bit Steganography* dengan fleksibilitas subband penyisipan informasi menggunakan Transformasi Wavelet Haar ini.
2. Dalam penyisipan informasi, sistem ini menggunakan metode *Least Significant Bit*. Sehingga disarankan untuk mengembangkannya dengan metode steganografi lainnya untuk membandingkan metode yang tepat untuk penyisipan informasi dengan fleksibilitas subband penyisipan Transformasi Wavelet Haar ini.
3. Kendala pada penelitian ini terletak pada adanya beberapa nilai piksel hasil rekontruksi citra *carrier* yang berkoma, menyebabkan informasi yang disisipkan sebelumnya tidak dapat di-*retrieving* kembali karena nilai piksel yang berkoma ini melakukan pembulatan saat proses *creating* citra. sehingga pada pengembangan penelitian selanjutnya peneliti menyarankan untuk dapat memperhatikan nilai piksel yang berkoma ini agar didapat solusi penyelesaian yang dianggap tepat.

Referensi

[1] N. F. Johnson, "Steganography," JJTC, 1995.

[2] D. Putra, Pengolahan Citra Digital, Yogyakarta: Andi, 2010.

[3] A. D. Association, TIFF Revision 6.0, Mountain View, CA: Adobe Systems Incorporated., 1992.

[4] R. Munir, Pengolahan Citra Digital, ebook, 2004.

[5] F. Rahmat, Steganografi Menggunakan Metode Least Significant Bit (Lsb) Dengan Modifikasi 4 Bit Pada Media File Gambar Dan File Suara, Riau: Teknik Informatika UIN Suska Pekanbaru, 2012.

[6] S. Jamasoka, "Perbandingan Steganografi pada Citra Gambar Graphics Interchange Format dengan Algoritma Gifshuffle dan Metode Least Significant Bit," *Makalah IF3058 Kriptografi,* 2011.

[7] P.-Y. Chen and H.-J. Lin, "A DWT Based Approach for Image Steganography," *International Journal of Applied Science and Engineering ISSN 1727-2394 ,* pp. 275-290, 2006.

[8] Handayaningtyas, T. *Sistem Penyembunyian File Document dengan Menggunakan Metode Least Significant Bit (LSB) pada Citra Bitmap.* Riau: Teknik Informatika UIN Suska Pekanbaru, 2011.