



**PENGEMBANGAN APLIKASI PENYEMBUNYIAN PESAN (STEGANOGRAFI)
PADA CITRA DIGITAL DENGAN TRANSFORMASI WAVELET HAAR**

Oleh

Putu Erik Pratama, NIM 0915057135
Jurusan Pendidikan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Email : bhuerik@gmail.com

ABSTRAK

Steganografi merupakan teknik dan seni bagaimana menyembunyikan data digital dibalik data digital lain sehingga keberadaannya tidak mengundang kecurigaan dari persepsi pengamatan manusia. Dengan memanfaatkan kekurangan dari mata manusia, maka dipilih citra digital sebagai *carrier*. Penerapan teknik steganografi pada citra digital dikatakan memiliki kinerja baik jika citra *carrier* tidak mengalami penurunan kualitas yang signifikan. Untuk menghasilkan citra steganografi dengan kualitas yang baik maka dikembangkanlah aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar*.

Perangkat lunak ini hanya menangani proses *embedding* dan *extraction*. Proses *embedding* merupakan proses untuk menyisipkan pesan teks pada citra digital yang telah melalui proses transformasi *wavelet haar* 1 level. Untuk menambah tingkat keamanan, ditambahkan beberapa algoritma pengolahan terhadap *password*. Algoritma *blum blum shub* juga digunakan untuk menentukan posisi pesan pada citra digital secara acak. Proses *extraction* merupakan proses untuk memisahkan pesan teks dari citra steganografi. Agar didapatkan pesan teks yang telah disisipkan diperlukan *password* yang sama dengan *password* yang digunakan pada saat proses *embedding*. Untuk mengetahui kualitas citra steganografi, maka dilakukan perhitungan nilai PSNR dengan membandingkan antara citra asli dengan citra steganografi.

Perangkat lunak ini dibuat dengan bahasa pemrograman *Borland Delphi 7.0*. Perangkat lunak ini juga diimplementasikan dan telah diujicobakan pada sistem operasi berbasis *Windows*.

Kata-kata kunci: citra digital, Steganografi, embedding, extraction, Wavelet Haar, blum blum shub, PSNR



ABSTRACT

Steganography is a technique of concealing digital data under the presence of other digital data so that its existence does not attract humans attention. Upon making use of man's sight weakness, digital image is chosen to serve this purpose. Steganography is considered to work well provided that the carrier image does not undergo a significant decrease of quality. This research aims at designing and implementing steganography software so as to produce high quality digital image with a method known as wavelet haar.

This software in discussion only works on embedding and extraction. Embedding is defined as a process to insert a text message on a digital image that has been through 1 level of the process of waveler haar transformation. For the sake of increasing the security level, the author adds several algorithms for processing password. Blum blum shub algorithm is also used to determine the position of messages on the digital image at random. Extraction process is a process to separate the message text from the image steganography. For the text embedded text message to be taken out, a password during the extraction has to be the same as the one used during the embedding, In order to figure out the quality of steganography image, PSNR calculation is done by comparing the original image and the steganography image.

The results of this study is an application of message hiding (steganography) on digital images with haar wavelet transform. This software is created with Borland Delphi 7.0 programming language. The software is also implemented and has been tested on Windows-based operating system.

Key words: digital image, Steganography, embedding, extraction, Wavelet Haar, blum blum shub, PSNR

1. PENDAHULUAN

Steganografi merupakan teknik dan seni bagaimana menyembunyikan data digital dibalik data digital lain yang berperan sebagai medium pembawa (*carrier*) sehingga keberadaannya tidak mengundang kecurigaan dari persepsi pengamatan manusia. Dengan memanfaatkan kekurangan dari mata manusia, maka dipilih citra digital sebagai *carrier* selama data yang disisipkan tersebut tidak mengubah secara signifikan kualitas informasi citra *carrier*. Penerapan teknik steganografi pada citra digital dikatakan memiliki kinerja baik jika citra *carrier* tidak mengalami penurunan kualitas yang signifikan (Eddy Muntina Dharma , 2004).



Penelitian ini juga dilatarbelakangi oleh 2 penelitian yang sebelumnya telah dilakukan. Penelitian yang pertama dilakukan oleh Eddy Muntina Dharma (2004) yaitu penelitian tentang teknik steganografi pada citra digital dengan transformasi *wavelet*. Pada penelitian tersebut menyimpulkan bahwa metode *wavelet* menunjukkan kinerja yang baik dalam teknik *steganography* walaupun disisipkan data sebesar kapasitas maksimal yang dapat ditampung oleh citra *carrier*. Perbedaan kualitas antara citra steganografi dengan citra sebelum disisipkan juga tidak begitu besar. Penelitian yang kedua dilakukan oleh Prima Imam (2009) tentang komparasi algoritma *blum blum shub* (BBS) dan *linear congruential generator* (LCG) pada aplikasi *digital watermarking* dengan metode *least significant bit* (LSB). Hasil penelitian tersebut menyebutkan bahwa penyisipan *watermark* dengan algoritma LCG lebih unggul. Penyisipan *watermark* dengan algoritma BBS kurang maksimal, akan tetapi apabila dilihat dari segi keamanan BBS sulit ditebak penempatan *bit-bit* dari *watermark* yang dimasukkan.

Melihat hasil penelitian tersebut, maka peneliti mencoba untuk melakukan penelitian tentang steganografi dengan transformasi *wavelet haar* yang digabungkan dengan algoritma *blum blum shub* pada proses penyisipan pesan. Penelitian ini diharapkan akan didapatkan citra steganografi dengan kualitas bagus dengan tingkat keamanan yang tinggi.

2. TINJAUAN PUSTAKA

2.1. Steganografi

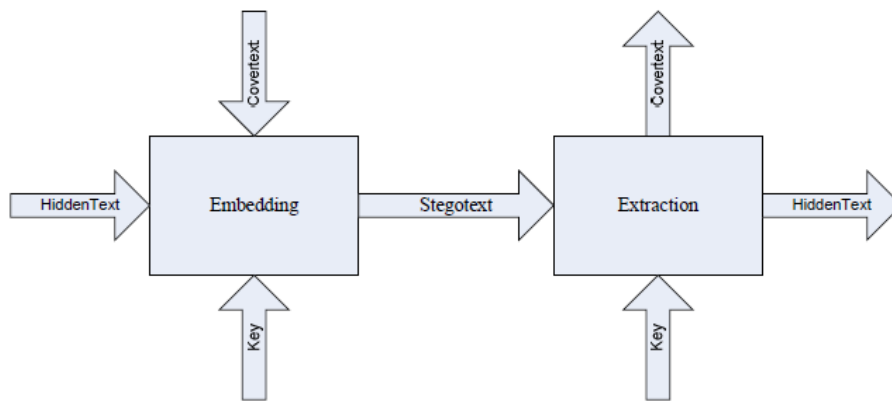
Kata steganografi berasal dari bahasa Yunani, yaitu dari kata *steganos* (tersembunyi atau terselubung) dan *graphien* (tulisan) yang berarti tulisan tersembunyi (Rinaldi Munir, 2006). Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Terdapat beberapa istilah yang berkaitan dengan steganografi antara lain.

- a) *Hiddentext* atau *hidden object* merupakan informasi yang akan disembunyikan.
- b) *Coverttext* atau *cover object*, merupakan media penampung pesan.

- c) *Stegotext* atau *stego object*, media yang sudah disisipkan pesan.
- d) *Stegokey*, merupakan kunci untuk menyisipkan pesan atau membaca pesan.

Penyisipan pesan ke dalam media *cover object* dinamakan *embedding*, sedangkan pemisahan pesan dari *stego object* dinamakan *extraction*. Kedua proses ini memerlukan kunci (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan pemisahan pesan. Untuk lebih jelasnya tentang proses steganografi dapat dilihat pada gambar 2.1.



Gambar 2.1 : Skema Proses Steganografi
(Sumber : Prima Iman, 2009)

Proses steganografi sedikit atau banyak akan mengubah kualitas dari media tersebut. Ada beberapa kriteria dalam steganografi yaitu:

a) *Imperceptibility*

Keberadaan pesan tidak diketahui oleh indera manusia.

b) *Fidelity*

Mutu dari media penampung tidak berubah banyak setelah dilakukan proses penyisipan sehingga orang akan sulit mengetahui bahwa sebenarnya didalamnya terdapat pesan.

c) *Robustness*

Data yang disembunyikan harus tahan terhadap manipulasi pada *cover object*. Bila pada *cover object* dilakukan operasi pengolahan gambar, maka data yang disembunyikan tidak rusak.

d) *Recovery*

Pesan yang disisipkan harus dapat diungkapkan kembali, karena tujuan dari steganografi adalah hanya untuk menyembunyikan data.

Untuk hasil steganografi dapat dikatakan baik cukup dengan memenuhi tiga kriteria, yaitu *imperceptibility*, *fidelity* dan *recovery*. Kriteria *robustness* hanya dipenuhi oleh *copyright marking*.

2.2. Transformasi *Wavelet Haar*

Salah satu metode transformasi *wavelet haar* adalah dengan dekomposisi *averages* dan *differences*. Seperti telah dijelaskan sebelumnya dimana h_0 (tapis *low pass*) yang berkaitan dengan proses perataan akan melauai proses dekomposisi *averages* sedangkan h_1 (tapis *high pass*) yang berkaitan dengan proses pengurangan akan melauai proses *differences* (Darma Putra, 2010). Untuk dapat lebih dipahami, berikut merupakan contoh transformasi *wavelet* untuk citra 1 dimensi menggunakan *averages* dan *differences*.

37	35	28	28	58	18	21	15
----	----	----	----	----	----	----	----

Gambar 2.2 : Contoh Citra 1 Dimensi

Hasil proses perataan untuk citra 1 dimensi pada gambar 2.2 adalah:

$\frac{37 \quad 35}{36}$	$\frac{28 \quad 28}{28}$	$\frac{58 \quad 18}{38}$	$\frac{21 \quad 15}{18}$
--------------------------	--------------------------	--------------------------	--------------------------

Sedangkan hasil proses pengurangannya adalah:

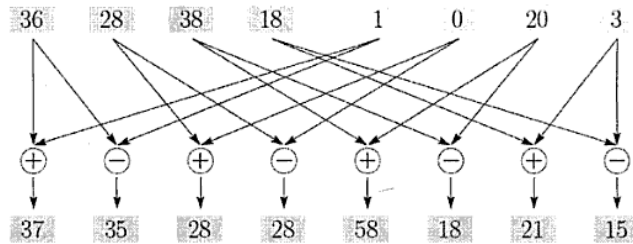
$\frac{37 \quad 35}{1}$	$\frac{28 \quad 28}{0}$	$\frac{58 \quad 18}{20}$	$\frac{21 \quad 15}{3}$
-------------------------	-------------------------	--------------------------	-------------------------

Sehingga hasil proses dekomposisi perataan dan pengurangan 1 *level* adalah:

36	28	38	18	1	0	20	3
----	----	----	----	---	---	----	---

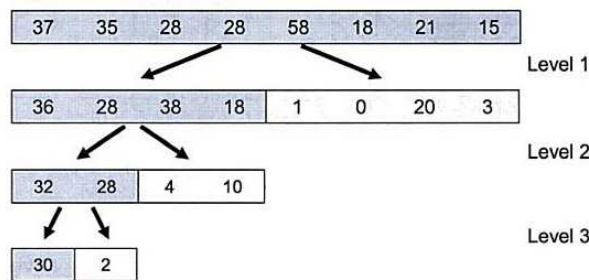
Gambar 2.3 : Hasil Transformasi *Wavelet Haar* dengan Proses Perataan dan Pengurangan

Untuk mendapatkan citra semula dari citra hasil dekomposisi maka dapat dilakukan proses rekonstruksi atau sintesis seperti ditunjukkan pada gambar 2.5.



Gambar 2.4 : Proses Rekonstruksi Terhadap Gambar 2.3

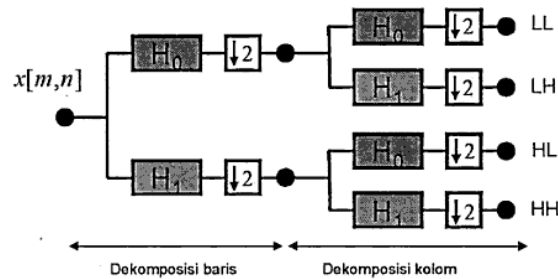
Proses dekomposisi yang dilakukan hanya 1 level saja. Gambar 2.5 menunjukkan proses transformasi penuh dan berhenti setelah tersisa 1 pixel saja.



Gambar 2.5 : Proses Dekomposisi Perataan dan Pengurangan Penuh (3 level)

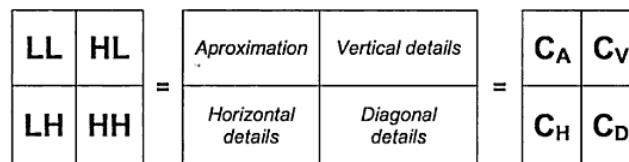
Pada setiap level, proses dekomposisi hanya dilakukan pada bagian hasil proses perataan dan hasil proses dekomposisi adalah gabungan dari proses perataan dengan seluruh hasil proses pengurangan.

Suatu citra dapat dianggap sebagai matrik 2 dimensi sehingga diperlukan transformasi *wavelet haar* 2 dimensi. Pada citra 2D proses transformasi dilakukan pada baris terlebih dahulu, kemudian dilanjutkan dengan transformasi pada kolom (Darma Putra, 2010), seperti ditunjukkan pada gambar 2.6.



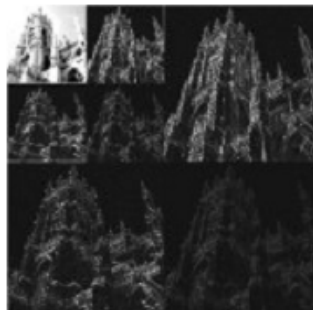
Gambar 2.6 : Transformasi *Wavelet Haar* 2 Dimensi 1 Level
 (Sumber : Darma Putra , 2010)

Hasil transformasi *wavelet haar* 2D 1 level, sering dibuat dalam bentuk skema seperti pada gambar 2.7.



Gambar 2.7 : Skema Hasil Transformasi *Wavelet Haar* 2D 1 Level
 (Sumber : Darma Putra , 2010)

Transformasi *wavelet haar* pada gambar 2.7 merupakan transformasi *wavelet haar* 1 level, transformasi *wavelet haar* dengan level yang lebih tinggi didapatkan dengan membagi kembali koefisien aproksimasi (LL) menjadi *subband-subband* yang lebih kecil. Jika proses transformasi *wavelet haar* dilakukan pada sebuah citra akan menghasilkan citra seperti pada gambar 2.12.



Gambar 2.12 : Citra Cathedral Hasil Transformasi *Wavelet Haar* 2 Level
 (Sumber : Mohammed F. Al Hunaity, 2007)



Pada pengembangan aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* peneliti akan menyisipkan pesan teks pada bagian HH (detail diagonal). Alasannya karena pada bagian ini melalui proses tapis *high pass* dan dilanjutkan lagi dengan tapis *high pass* sehingga menyebabkan bagian ini menjadi bagian yg paling *less visible* dibandingkan dengan 3 bagian lainnya.

2.3. Blum Blum Shub (BBS)

BBS ditemukan pada tahun 1986 oleh *Lenore Blum, Manuel Blum, dan Michael Shub*. BBS merupakan CSPNRG yang dirancang dengan dasar teori bilangan. Pada dasarnya algoritma BBS ini memiliki 2 *generator engine* dalam proses pengacakan bilangan, yaitu:

- a) $1/P$ generator
- b) $x^2 \bmod n$ generator

BBS memerlukan 2 *seed* yaitu *seed n* yang sebaiknya didapat dari perkalian 2 buah bilangan prima yang berbeda agar dapat menghasilkan periode yang panjang, dan *seed x* dimana $2 \leq x < n$. Untuk dapat lebih dipahami, berikut merupakan perhitungan BBS.

$$\begin{aligned}n &= 7 \times 13 = 133 & x &= 100 \\x_0 &= 100^2 \bmod 133 = 25 & x_1 &= 25^2 \bmod 133 = 93 \\x_2 &= 93^2 \bmod 133 = 4 & x_3 &= 4^2 \bmod 133 = 16 \\x_4 &= 16^2 \bmod 133 = 123\end{aligned}$$

2.4. Peak Signal to Noise Ratio (PSNR)

Meskipun banyak parameter untuk mengukur kualitas citra, PSNR dianggap merupakan salah satu parameter yang sangat bagus digunakan. Nilai PSNR ini didapat dengan mengkomparasikan citra asli dengan citra steganografi. Satuan untuk nilai PSNR adalah *decibel* (dB), semakin besar nilai PSNR semakin baik pula *image watermark* (Prima Imam, 2009). Secara matematis PSNR didefinisikan:



$$\text{PSNR} = 20 \log_{10} \frac{R}{\text{MSE}}, \quad \text{MSE} = \sqrt{\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |f(x, y) - g(x, y)|^2}$$

R = sinyal terbesar (pada citra hitam putih, $b = 255$)

MSE = akar pangkat dua dari selisih antara citra semula dengan citra hasil

M = panjang gambar

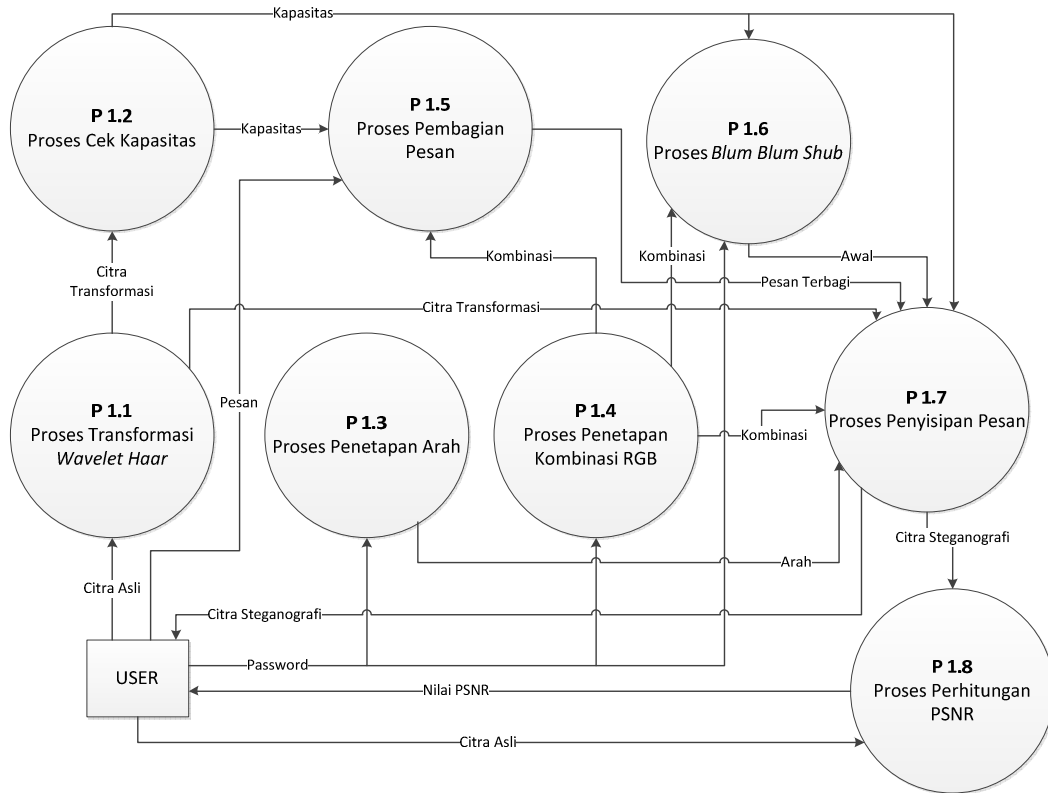
N = lebar gambar

f = nilai piksel citra semula

g = nilai piksel citra hasil

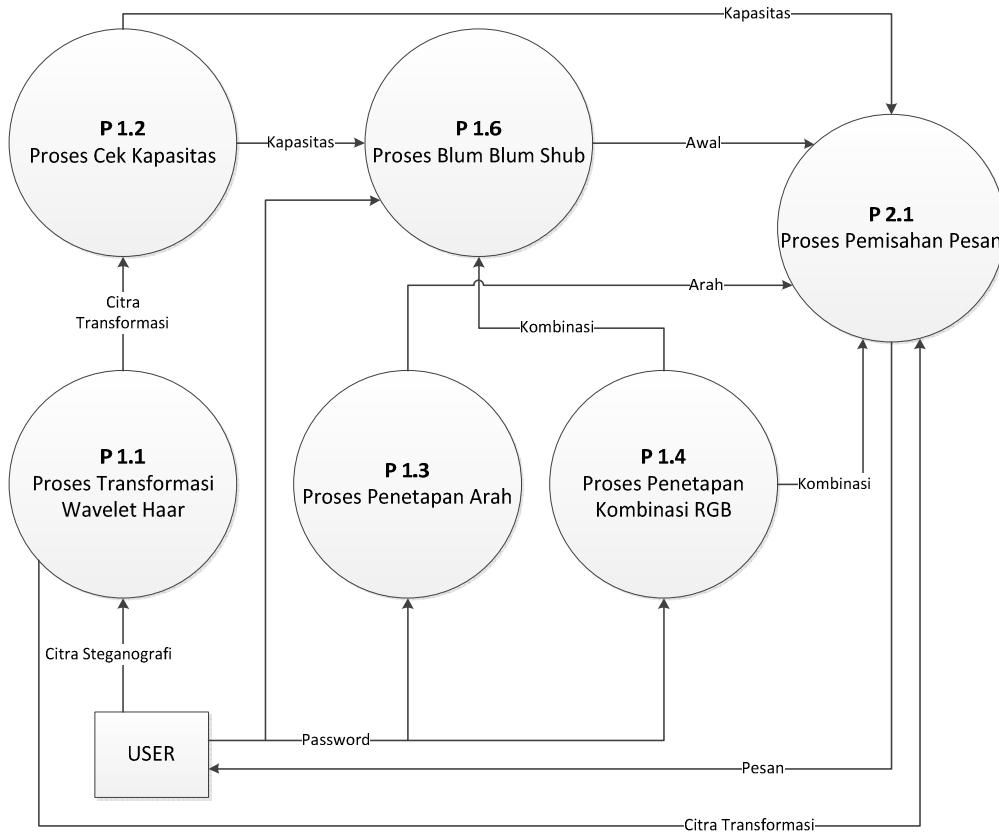
3. ANALISIS DAN PERANCANGAN

Model fungsional perang lunak akan digambarkan dalam bentuk DFD (*Data Flow Diagram*). DFD merupakan suatu model logika data atau proses yang dibuat untuk menggambarkan dari mana asal data, kemana tujuan data yang keluar dari sistem, dimana data disimpan, proses apa yang menghasilkan data tersebut, bagaimana interaksi antara data yang tersimpan, serta proses apa yang dikenakan pada data tersebut. Perangkat lunak penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* yang akan dikembangkan akan menangani 2 proses yaitu proses *embedding* dan *ectraction*. Untuk lebih jelasnya berikat digambarkan DFD kedua proses tersebut.



Gambar 3.1 : DFD Level 2 Untuk Proses 1 (*Embedding*)

Pada DFD *level 2* untuk proses 1 yaitu proses *embedding user* akan melakukan 8 proses yang saling berhubungan yaitu proses transformasi *wavelet haar*, cek kapasitas, penetapan arah, penetapan kombinasi RGB, pembagian pesan, *blum blum shub*, penyisipan pesan, dan perhitungan PSNR.



Gambar 3.4 : DFD Level 2 Untuk Proses 2 (*Extraction*)

Pada DFD *level 2* untuk proses 2 yaitu proses *extraction*. Beberapa proses pada proses *extraction* merupakan proses yang sama dengan proses yang dilakukan pada saat proses *embedding* dengan bentuk keluaran dan masukan yang sama. Pada proses *extraction* ini *user* akan melakukan 6 proses yang saling berhubungan yaitu proses transformasi *wavelet haar*, cek kapasitas, penetapan arah, penetapan kombinasi RGB, *blum blum shub*, dan pemisahan pesan yang akan dijabarkan sebagai berikut.



4. IMPLEMENTASI DAN PENGUJIAN

4.1. Batasan Implementasi Perangkat Lunak

Batasan implementasi dari aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* dapat dipaparkan sebagai berikut.

1. Aplikasi hanya menerima masukan citra digital dengan jenis citra warna (*true color*) 24 bit.
2. Aplikasi hanya menerima masukan citra warna dengan format bitmap (*.bmp).
3. Aplikasi hanya menerima masukan citra digital dengan ukuran panjang dan lebar yang bernilai genap.
4. Aplikasi tidak membatasi besar maksimum ukuran citra digital, sebaiknya nanti *user* memilih ukuran citra dengan mempertimbangkan kemampuan perangkat keras yang digunakan.

4.2. Tata Ancang dan Teknik Pengujian Perangkat Lunak

Berikut akan dijabarkan tata ancaang dan teknik pengujian aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar*.

1. Dalam pengujian kebenaran proses *embedding* dan *extraction* pada aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar*, akan dilakukan pada 3 variabel yang terdapat pada proses *embedding*. Variable tersebut adalah citra digital, *password*, dan pesan *text*. Teknik yang digunakan adalah memvariasikan variable yang ingin diuji dan menyeragamkan variable lainnya. Karena terdapat 3 variabel yang akan diuji maka akan dilakukan 3 jenis pengujian.
2. Untuk pengujian ketahanan citra steganografi hasil dari proses *embedding* pada aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* terhadap serangan-serangan yang mungkin terjadi, akan dilakukan dengan memanipulasi citra steganografi yang merupakan hasil dari proses *embedding*. Akan dilakukan 3 jenis manipulasi yaitu manipulasi geometri, manipulasi warna, dan manipulasi bentuk dan ukuran. Teknik yang digunakan adalah mengubah citra steganografi kedalam beberapa



jenis sesuai dengan jenis manipulasi yang akan dilakukan. Kerena terdapat 3 jenis manipulasi yang akan dilakukan maka akan dilakukan 3 jenis pengujian.

3. Dalam pengujian penggunaan aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* pada 10 orang dengan menggunakan *hardware* mereka masing-masing, akan dilakukan dengan memberikan angket. Teknik yang dilakukan adalah memberikan kesempatan ke 10 orang tersebut untuk melakukan proses *embedding* dan *extraction* dengan memberikan kebebasan kepada mereka untuk memilih masukan seperti citra digital, *password*, dan pesan. Proses juga akan dilakukan pada perangkat keras mereka masing-masing tetapi tetap mendampingiya sehingga jika terdapat kesulitan dapat langsung ditanyakan. Setelah mencoba aplikasi mereka akan diberikan kesempatan untuk mengisi angket yang telah diberikan sesuai dengan pendapat mereka masing-masing.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian pengembangan aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* yang telah dilakukan adapun simpulan yang didapat antara lain.

1. Rancangan sistem aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* digambarkan menggunakan DFD (*Data Flow Diagram*). DFD yang telah dibuat meliputi DFD *level 0*, DFD *level 1*, DFD *level 2* untuk proses 1 (*embedding*), dan DFD *level 2* untuk proses 2 (*extraction*).
2. Rancangan antarmuka yang telah dibuat pada pengembangan aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* yaitu rancangan antarmuka *form* utama, rancangan antarmuka *form embedding*, dan rancangan antarmuka *form extraction*.



3. Implementasi aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar* menghasilkan suatu program aplikasi yang menangani proses *embedding* dan *extraction*.
4. Perangkat lunak yang dibangun dapat dijadikan sebagai salah satu pengamanan pesan teks dan alternatif pengiriman pesan teks. Dilihat dari nilai PSNR yang besar yang menunjukkan citra steganografi yang dihasilkan tidak mengalami penurunan kualitas secara signifikan walaupun telah disisipkan pesan.
5. Masukan citra digital, *password*, dan pesan sangat berpengaruh terhadap kualitas proses *embedding* dan *extraction* pada aplikasi penyembunyian pesan (steganografi) pada citra digital dengan transformasi *wavelet haar*.
6. Citra steganografi hasil dari proses *embedding* sangat rentan terhadap serangan yang mengubah nilai *pixel*, komposisi *pixel*, atau ukuran *pixel* karena akan mempengaruhi pesan yang disembunyikan didalamnya.
7. Perubahan bentuk citra steganografi aman dilakukan selama perubahan bentuk tersebut tidak mengubah nilai, komposisi, dan ukuran *pixel* citra steganografi.
8. Kecepatan proses *embedding* dan *extraction* sangat dipengaruhi oleh besarnya citra digital dan perangkat keras yang digunakan.
9. Karena belum pernah diuji coba pada sistem operasi selain *Windows*, mengakibatkan tidak diketahui apakah perangkat lunak berjalan dengan baik pada sistem operasi lain.

DAFTAR PUSTAKA

- Belza Achmad, Kartika Firdausy. 2005. *Teknik Pengolahan Citra Digital Menggunakan Delphi*. Yogyakarta : Ardi PubliShing
- Darma Putra. 2010. *Pengolahan Citra Digital*. Yogyakarta : Penerbit Andi.
- Dina Cahyati. 2003. "Draf Tesis II *Wavelet*". <http://www.cs.ui.ac.id/WebKuliah/citra/2003/Wavelet1.doc>. (diakses tanggal 23 Maret 2011)
- Eddy Muntina Dharma. 2004. "Teknik *Steganography* Pada Citra Digital Dengan Transformasi *Wavelet*". <http://wahyudisetiawan.wordpress.com/2009/10/16/steganography-pada-citra-digital-dengan-transformasi-wavelet/>. (diakses tanggal 7 April 2011)



- Isma Fahdiani. 2008. "Transformasi *Wavelet*". http://digilib.itelkom.ac.id/index.php?option=com_content&view=article&id=356:transformasi-wavelet&catid=15:pemrosesan-sinyal&Itemid=14. (diakses tanggal 23 Maret 2011)
- Maryam Qonita. 2009. "Pertemuan Pertama *Study Club Flowchart Algoritma*". <http://studyclubtik.blogspot.com/2009/12/pertemuan-pertama-study-club-flowchart.html>. (diakses tanggal 20 Mei 2011)
- Mohammed F. Al Hunaity, dkk. 2007 "*Colored Digital Image Watermarking using the Wavelet Technique*". <http://www.scipub.org/fulltext/ajas/ajas49658-662.pdf>. (diakses tanggal 23 Maret 2011)
- Prima Imam. 2009. *Komparasi Algoritma Blum Blum Shub (BBS) dan Linear Congruential Generator (LCG) Pada Aplikasi Digital Watermarking dengan Metode Least Significant Bit (LSB)*. Bandung : Program Pendidikan Ilmu Komputer FPMIPA UPI
- Rinaldi Munir. 2006. *Kriptografi*. Bandung : Informatika
- Rinaldi Munir. 2006. "Bahan Kuliah 7, IF 5054 Steganografi dan Watermaking". http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/bahankuliah_2006.htm. (diakses tanggal 21 Juli 2010)
- Rinaldi Munir. 2006. "Bahan Kuliah 1, IF 5054 Kriptografi Pengantar Kriptografi". <http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/kripto2006.htm>. (diakses tanggal 21 Juli 2010)
- Sutoyo, T., dkk. 2009. *Teori Pengolahan Citra Digital*. Yogyakarta : Penerbit Andi
- Trajianto. 2010. "Pemrograman Lanjutan Delphi 7.0". <http://tarjianto.files.wordpress.com/2010/03/perulangan-if-then-else-pada-delphi.pdf>. (diakses 23 Maret 2011)
- Umi Probeykti. 2008. "Bahan Ajar Rekaya Perangkat Lunak Software Process Model I". <http://lecturer.ukdw.ac.id/othie/softwareprocess.pdf>. (diakses tanggal 4 Oktober 2010)
- Yudi Hariwibowo. 2007. "Kriptanalisis terhadap Pembangkit Bilangan Acak Semu". <http://scriptkiddy394.blogspot.com/Makalah-082.pdf>. (diakses tanggal 12 September 2010)