



**IMPLEMENTASI METODE STEGANOGRAFI SLT-DCT PADA CITRA UNTUK  
MENINGKATKAN KUALITAS CITRA STEGANOGRAFI**

**Lilik Widyawati**

**16917109**

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*

*Konsentrasi Forensika Digital*

*Program Studi Magister Teknik Informatika*

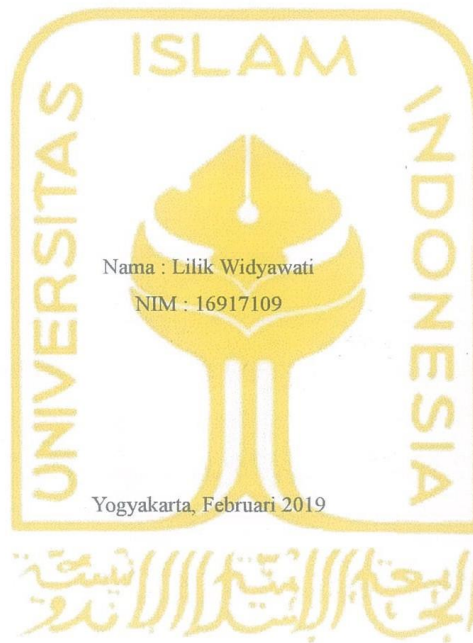
*Program Pascasarjana Fakultas Teknologi Industri*

*Universitas Islam Indonesia*

2019

Lembar Pengesahan Pembimbing

Implementasi Metode Steganografi SLT-DCT pada Citra untuk Meningkatkan  
Kualitas Citra Steganografi



Pembimbing I,

  
Dr. Imam Riadi, M.Kom

Lembar Pengesahan Penguji

Implementasi Metode Steganografi SLT-DCT pada Citra untuk Meningkatkan Kualitas Citra Steganografi

Nama : Lilik Widyawati  
NIM : 16917109

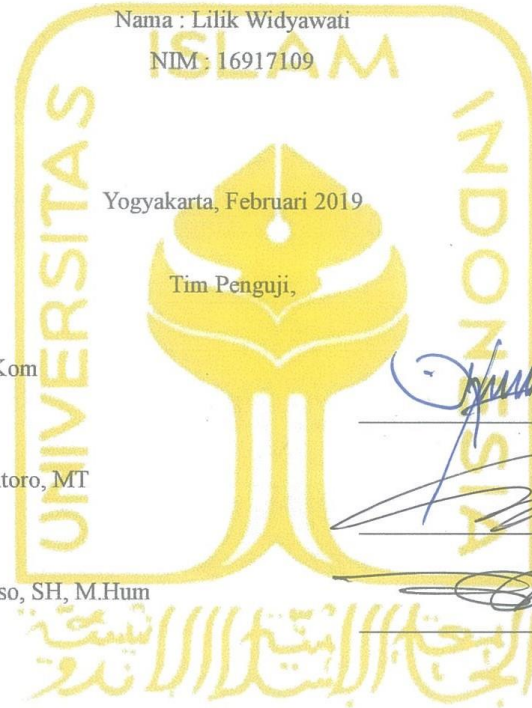
Yogyakarta, Februari 2019

Tim Penguji,

Dr. Imam Riadi, M.Kom  
Ketua

Dr. Bambang Sugiantoro, MT  
Anggota I

Dr. Bambang Sutyoso, SH, M.Hum  
Anggota II



*(Handwritten signatures of the examiners)*

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia



*(Handwritten signature of the Dean)*

Suzati Muhiyomah, ST., M.Sc., Ph.D

## Abstrak

Teknologi informasi saat ini sudah sangat berkembang terutama dalam keamanan informasi, mudahnya akses pertukaran data membuat informasi tersebut rentan dicuri dan dimanipulasi, untuk menjaga keamanan informasi dapat dilakukan dengan cara data dan informasi tersebut disembunyikan pada media digital lain yang disebut steganografi, yang perlu diperhatikan dalam steganografi yaitu kualitas dari hasil citra steganografi. Penelitian ini bertujuan untuk membuat aplikasi steganografi dengan algoritma Slantlet Transform (SLT) dan Discrete Cosine Transform (DCT). SLT memiliki kualitas citra lebih baik dibanding algoritma lainnya, sedangkan DCT memiliki kelebihan tahan terhadap serangan akan tetapi memiliki kelemahan yaitu pada kualitas citra yang kurang baik dibanding algoritma lainnya, perhitungan kualitas didasari oleh perhitungan nilai PSNR dan MSE citra, nilai PSNR ditentukan oleh besarnya nilai MSE, semakin tinggi nilai MSE dari citra steganografi, maka semakin terlihat perbedaan citra asli dengan citra hasil steganografi sehingga hal ini dapat menyebabkan citra steganografi rentan diketahui keberadaannya dari sini lah peneliti bertujuan menggabungkan algoritma SLT dan DCT untuk menutupi kelemahan masing-masing algoritma. Hasil penelitian membuktikan bahwa citra steganografi SLT-DCT yang dihasilkan sangat baik terbukti dengan nilai PSNR citra stego lebih tinggi dibandingkan dengan citra stego algoritma SLT dan DCT, dan nilai PSNR yang dihasilkan  $> 40$  db yang berarti kualitas citra steganografi sangat baik. Untuk hasil ketahanan terbukti algoritma SLT-DCT tahan terhadap beberapa serangan seperti *contrast stretching* dan *histogram equalization*.

Kata kunci: *Slantlet transform*; *Discrete Cosine Transform*; PSNR; MSE;

## ***Abstract***

*Information technology is currently very developed, especially in information security, easy access to data exchange makes the information vulnerable to being stolen and manipulated, to maintain the security of information can be done by means of data and information hidden in other digital media called steganography, which needs to be considered in steganography namely the quality of the results of steganographic images. This study aims to make the application of steganography with the Slantlet Transform (SLT) and Discrete Cosine Transform (DCT) algorithms. SLT has better image quality than the other algorithms [2], while DCT has the advantage of being resistant to attacks but has a disadvantage that is in poor image quality compared to other algorithms, quality calculations are based on calculation of PSNR and MSE images, PSNR values are determined by the value of MSE, the higher the value of MSE from steganographic images, the more visible differences in the original image with the results of steganography images so that this can cause susceptible steganographic images to be known from here. The results showed that the resulting SLT-DCT steganographic image was very well proven by the PSNR value of the stego image compared to the stego image of the SLT and DCT algorithms, and the resulting PSNR value was > 40 db which meant that the quality of steganographic images was very good. For the results of durability, it is proven that the SLT-DCT algorithm is resistant to several attacks such as contrast stretching and histogram equalization.*

*Keywords: Slantlet transform; Discrete Cosine Transform; PSNR; MSE;*

### Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, 9 Februari 2019



Lilik Widyawati

## Publikasi Selama Studi

### *Sitasi publikasi 1*

Kontributor	Jenis Kontribusi
Author Lilik Widyawati	Mendesain eksperimen (60%) Menulis <i>paper</i> (70%)
Author Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit <i>paper</i> (15%)
Author Imam Riadi	Mendesain eksperimen (20%) Menulis dan mengedit <i>paper</i> (15%)

## **Kontribusi Pihak Lain Yang Diberikan Dalam Tesis Ini**

Tidak ada kontribusi dari pihak lain



## Halaman Persembahan



Karya ini saya persembahkan kepada:

1. Kedua orang tua saya yang telah menginspirasi untuk tetap belajar dan belajar dalam kehidupan ini.
2. Kedua mertua saya yang telah memberikan doa dan semangat sehingga karya tulis ini dapat terselesaikan.
3. Suami tercinta yang telah memberikan segalanya selama menempuh pendidikan pascasarjana.
4. Buah hati tercinta (Nizam) yang telah menginspirasi dan sebagai motivasiku dalam menempuh pendidikan pascasarjana.

Pada akhirnya saya persembahkan karya saya ini kepada semua pembaca, untuk ditelusuri dan menjadi inspirasi yang akhirnya bisa ditarik hikmahnya.

## Kata Pengantar



*Assalamualaikum Wr. Wb.*

Segala puji bagi Allah SWT, Tuhan seru sekalian alam yang setia membimbing hamba-hamba-Nya. Atas bantuan dan tuntunan-Nya, penulisan tesis dengan judul **“Implementasi Metode Steganografi SLT-DCT pada Citra untuk Meningkatkan Kualitas Citra Steganografi “** dapat diselesaikan.

Adapun tesis ini ditulis dengan maksud untuk memenuhi persyaratan menyelesaikan pendidikan Magister Teknik Informatika Konsentrasi Forensik Digital pada Program Pascasarjana Universitas Islam Indonesia Yogyakarta.

Penulis menyadari dalam penulisan proposal tesis ini masih sangat jauh dari sempurna, karena keterbatasan yang penulis miliki. Walaupun demikian penulis telah berusaha semaksimal mungkin agar inti dari pembahasan di dalam tesis ini dapat bermanfaat bagi penulis maupun para pembaca.

Penulis telah berusaha menyajikan penelitian dalam tesis ini dengan kondisi yang terbaik dan setepat mungkin, namun karena keterbatasan dan kelemahan yang ada, pasti terbuka kemungkinan kesalahan. Untuk itu penulis mengharap kritikan, saran dan masukan dari semua pihak dalam rangka meningkatkan kualitas tesis ini dan di masa yang akan datang.

Dengan penuh kerendahan hati, penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang langsung maupun tidak langsung, turut andil dan memotivasi penyelesaian tesis ini, antara lain kepada :

1. Rektor Universitas Islam Indonesia Yogyakarta, Fathul Wahid, S.T., M.Sc., Ph.D yang telah memberi kesempatan kepada penulis untuk dapat belajar dan menggali ilmu pada institusi pendidikan yang beliau pimpin;
2. Dr. R. Teduh Dirgahayu, ST., MSc., selaku Direktur Program Pasca Sarjana Fakultas Teknik Industri Universitas Islam Indonesia Yogyakarta yang semenjak semester pertama telah memotivasi untuk belajar dan memberikan wacana penelitiannya;
3. Bapak Dr. Imam Riadi, M.Kom selaku Dosen Pembimbing yang telah memberikan motivasi dan bimbingan sehingga penulis menyelesaikan tesis ini.
4. Yudi Prayudi, S.Si, M.Kom sebagai Dosen Pembimbing yang telah mendorong dan membimbing penulis menyelesaikan tesis ini;

5. Dr. Bambang Sugiantoro, MT sebagai Dosen Penguji yang telah memberikan motivasi dan bimbingan sehingga penulis menyelesaikan tesis ini;
6. Seluruh Dosen Studi Program Magister Teknik Informatika Universitas Islam Indonesia Yogyakarta yang telah berkenan memberikan dan membuka cakrawala ilmu pengetahuan kepada penulis;
7. Seluruh staff dan karyawan Studi Program Pasca Sarjana yang dengan ramah dan baik dalam memberikan pelayanannya kepada mahasiswa;
8. Teman-teman Mahasiswa Program Magister Teknik Informatika Universitas Islam Indonesia Yogyakarta angkatan XIV yang sering berbagi wacana dan masukannya;

Semoga Allah SWT senantiasa memberikan berkat dan anugrah-Nya berlimpah bagi beliau-beliau yang tersebut di atas. Sangat disadari dalam tesis ini terdapat banyak kekurangan oleh karena itu semua saran dan kritik penulis terima dengan lapang dada demi kesempurnaan penulisan tesis ini. Akhirnya harapan penulis semoga tesis ini bermanfaat bagi kita semua.

Aamiin ya Robbal ‘Aalamiin

*Wassalamualaikum Wr. Wb.*

Yogyakarta, 9 Februari 2019

Lilik Widyawati

## Daftar Isi

Lembar Pengesahan Pembimbing .....	<b>Error! Bookmark not defined.</b>
Lembar Pengesahan Penguji.....	<b>Error! Bookmark not defined.</b>
Abstrak .....	iii
<i>Abstract</i> .....	iv
Pernyataan Keaslian Tulisan.....	<b>Error! Bookmark not defined.</b>
Publikasi Selama Studi .....	v
Kontribusi Pihak Lain Yang Diberikan Dalam Tesis Ini .....	vii
Halaman Persembahan .....	viii
Kata Pengantar.....	ix
Daftar Isi.....	xi
Daftar Tabel .....	xiv
Daftar Gambar .....	xv
BAB 1 Pendahuluan .....	1
1.1 Latar belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	5
1.5 Manfaat Penelitian .....	5
1.6 Metode Penelitian .....	5
1.7 Sistematika Penulisan .....	6
BAB II Tinjauan Pustaka.....	8
2.1 Literatur Riview .....	8
2.2 Tinjauan Pustaka .....	10
2.2.1 Steganografi.....	10
2.2.2 Algoritma DCT.....	11
2.2.3 Algoritma SLT .....	12
2.2.4 Matlab.....	13
2.2.5 Metode Contrast Stretching Dan Histogram Equalization .....	15
2.2.6 Citra Digital .....	16
2.2.7 Peak Signal to Noise Ratio (PSNR) .....	18
2.2.8 Mean Square Error (MSE).....	18
BAB III Metodologi Penelitian .....	19

3.1	Perancangan Umum Sistem .....	19
3.2	Metode Steganografi yang digunakan .....	20
3.2.1	Steganografi SLT .....	20
3.2.2	Steganografi DCT.....	22
3.2.3	Steganografi SLT-DCT.....	23
3.3	Parameter Pengujian .....	24
3.3.1	Parameter <i>Imperceptibility</i> .....	24
3.3.2	Parameter Kapasitas Pesan .....	25
3.3.3	Parameter Ketahanan Citra.....	25
3.4	Data yang Digunakan.....	25
3.5	Rancangan Pengujian Sistem.....	26
3.5.1	Pengujian Kualitas Citra stego .....	26
3.5.2	Pengujian Kapasitas Pesan .....	26
3.5.3	Pengujian Ketahanan citra steganografi .....	27
3.6	Rancangan Hasil Analisa .....	28
3.6.1	Rancangan Tampilan .....	28
3.6.2	Rancangan hasil analisa kualitas citra .....	29
3.6.3	Hasil analisa kapasitas pesan.....	29
3.6.4	Hasil analisa ketahanan stego image .....	30
BAB IV Hasil dan Pembahasan.....		31
4.1	Implementasi system.....	31
4.1.1	Steganografi SLT .....	31
4.1.2	Steganografi DCT .....	32
4.1.3	Steganografi SLT-DCT.....	32
4.2	Tampilan GUI Aplikasi teganografi SLT-DCT.....	34
4.2.1	Contoh Gambar .....	35
4.3	Analisis Output .....	36
4.4	Hasil Pengujian .....	41
4.4.1	Pengujian Kualitas Image.....	42
4.4.2	Pengujian kapasitas pesan .....	46
4.4.3	Pengujian Ketahanan Stego Image .....	47
4.4.4	Analisa .....	52
BAB V Kesimpulan Dan Saran .....		54
A.	Kesimpulan .....	54

B. Saran .....	54
Daftar Pustaka .....	55

## Daftar Tabel

Tabel 2. 1 Literatur Review .....	8
Tabel 3. 1 Rancangan hasil analisa kualitas citra .....	29
Tabel 3. 2 Hasil persentase kapasitas pesan pada steganografi SLT, DCT, SLT-DCT .....	29
Tabel 3. 3 Rancangan Hasil analisa Ketahanan citra steganografi SLT .....	30
Tabel 3. 4 Rancangan Hasil analisa Ketahanan citra steganografi DCT .....	30
Tabel 3. 5 Rancangan Hasil analisa Ketahanan citra steganografi SLT dan DCT.....	30
Tabel 4. 1 tabel Contoh Gambar .....	35
Tabel 4. 2 Kualitas Citra Steganografi berdasarkan PSNR .....	42
Tabel 4. 3 Perbandingan nilai PSNR dan MSE berdasarkan Ukuran Pesan.....	43
Tabel 4. 4 Hasil perbandingan kualitas citra yang disisipi pesan 30 karakter .....	44
Tabel 4. 5 Perbandingan nilai PSNR dan MSE berdasarkan ukuran cover image .....	45
Tabel 4. 6 Hasil kapasitas pesan pada steganografi SLT, DCT, SLT-DCT.....	47
Tabel 4. 7 Ketahanan Citra Steganografi SLT-DCT pada Tree .....	48
Tabel 4. 8 Ketahanan Citra Steganografi SLT-DCT pada Airpalne .....	49
Tabel 4. 9 Ketahanan Citra Steganografi SLT-DCT pada San Diego .....	50
Tabel 4. 10 Perbandingan Ketahanan Citra Steganografi SLT, DCT, dan SLT-DCT.....	51

## Daftar Gambar

Gambar 2. 1 Distribusi Frekuensi pada Blok DCT (Faruqi & Rozi, 2015).....	12
Gambar 2. 2 Iterasi FilterBank menggunakan DWT.....	13
Gambar 2. 3 Iterasi FilterBank Menggunakan SLT.....	13
Gambar 3. 1 Perancangan Umum Sistem.....	19
Gambar 3. 2 Perancangan Algoritma SLT.....	20
Gambar 3. 3 Perancangan Algoritma DCT.....	22
Gambar 3. 4 Perancangan Algoritma SLT-DCT.....	23
Gambar 3. 5 Perancangan pengujian kualitas citra.....	26
Gambar 3. 6 Perancangan pengujian kapasitas pesan.....	26
Gambar 3. 7 Perancangan pengujian ketahanan citra.....	27
Gambar 4. 1 Perbandingan Hasil pada Algoritma SLT.....	36
Gambar 4. 2 Perbandingan hasil pada Algoritma SLT-DCT.....	37
Gambar 4. 3 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT.....	37
Gambar 4. 4 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT-DCT.....	37
Gambar 4. 5 Perbandingan hasil penyisipan pesan menggunakan Algoritma DCT.....	38
Gambar 4. 6 Perbandingan hasil penyisipan menggunakan Algoritma SLT-DCT.....	39
Gambar 4. 7 Histogram perbedaan citra pada Tree menggunakan Algoritma DCT.....	40
Gambar 4. 8 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT-DCT.....	40
Gambar 4. 9 Tampilan Aplikasi.....	34
Gambar 4. 10 Grafik Perbandingan nilai PSNR dengan jumlah pesan yang sama.....	45



# BAB 1

## Pendahuluan

### 1.1 Latar belakang

Perkembangan teknologi informasi dan komunikasi membuat kegiatan pertukaran data dan informasi menjadi semakin mudah dan cepat, akan tetapi keamanan data dan informasi agar sampai tepat kepada tujuan harus diperhatikan, karena data dan informasi tersebut rentan dicuri dan dimanipulasi oleh pihak yang tidak berkepentingan sehingga keamanan dan kerahasiaan data dan informasi tersebut sangat penting untuk dijaga.

Menjaga keamanan data dan informasi dapat dilakukan dengan cara data dan informasi tersebut disandikan atau disembunyikan pada media digital lain, teknik menyembunyikan pesan pada media digital lain disebut Steganografi. Steganografi adalah seni menyembunyikan atau menyamarkan keberadaan informasi dalam media lain (Morkel, Eloff, & Oliver, 2005) sehingga informasi digital yang asli tidak dapat diketahui oleh pihak yang tidak berkepentingan.

Implementasi steganografi saat ini telah menggunakan media digital sebagai media penampung atau penyembunyi pesan, salah satu mediana adalah media gambar (citra digital). Steganografi bertujuan menyisipkan atau menyembunyikan pesan didalam sebuah gambar (cover image), agar pihak lain tidak menyadari keberadaan informasi yang ada didalam gambar tersebut. Steganografi menjadikan citra stego (cover image) dalam bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut sebatas kemampuan indra manusia secara visual, artinya mata manusia tidak dapat membedakan gambar stego dengan gambar asli yang tidak memiliki pesan didalamnya. Steganografi memiliki dua proses yaitu *encoding* dan *decoding*. *Encoding* merupakan proses penyisipan pesan kedalam media penampung (*cover image*) dalam hal ini adalah citra/gambar, sedangkan *decoding* adalah proses ekstraksi pesan dari citra stego (stego image) atau proses pengembalian pesan dari citra stego (Aji & Wijanarto, 2014).

Sebuah teknik steganografi citra dikatakan baik jika memenuhi 3 kriteria yaitu kualitas citra hasil steganografi masih cukup baik (imperceptibility), tahan terhadap operasi citra dasar seperti penambahan kontras dan perubahan ukuran citra (robustness), dan pesan yang disisipi dapat dikembalikan atau ekstraksi (recoverable) (Munir, 2004). Kualitas citra hasil steganografi dapat ditentukan dengan beberapa metode, salah satu metode yang

paling banyak digunakan adalah dengan mengukur nilai MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*) (Solichin, 2015). MSE dan PSNR merupakan sebuah nilai yang memiliki satuan dB (desibels), semakin rendah nilai MSE maka nilai PSNR semakin tinggi yang berarti kualitas citra semakin baik, sementara itu, kualitas citra steganografi dikatakan baik jika nilai PSNR 40 dB atau lebih (Cheddad, 2010).

Pada citra teknik steganografi dibagi menjadi dua yaitu domain spasial dan domain transformasi (Morkel, Eloff, & Oliver, 2005), Teknik domain spasial menyisipkan bit rahasia secara langsung di file cover. Teknik domain spasial yang umum digunakan adalah Least Significant Bit Insertion (LSB). Dalam LSB, bit-bit rahasia dimasukkan ke dalam bit penutup gambar yang paling tidak signifikan. Transform domain menyembunyikan bit rahasia di bagian penting dari file cover. Teknik Transform Domain mencoba untuk menyandikan bit pesan dalam mengubah koefisien domain dari gambar. Teknik serupa juga dapat mewujudkan kapasitas *embedding* besar untuk steganografi (Bansal & Chhikara, 2014). Teknik transformasi domain yang paling sering digunakan yaitu Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) dan Slantlet Transform (SLT). SLT merupakan penyempurnaan dari kelemahan-kelemahan yang terdapat pada DWT. Dalam penerapannya, SLT membagi komponen sinyal ke dalam sub band horisontal dan vertikal rendah (LL), horisontal rendah dan vertikal tinggi (LH), horisontal tinggi dan vertikal rendah (HL) dan horisontal dan vertikal tinggi (HH), SLT juga menerapkan konsep yang hampir sama dengan DWT namun SLT memiliki waktu lokalisasi yang lebih baik dibandingkan DWT karena dukungan komponen filter yang lebih pendek (Imamah, 2015). Sushil Kumar dan S.K. Muttoo (2013), mengemukakan Slantlet Transform (SLT) lebih baik dari DWT, Haar Wavelet dan Contourlet transform dalam hal kualitas gambar, payload terbaik, mendapatkan hasil yang lebih baik untuk mengekstraksi dan embedding gambar asli, meningkatkan kapasitas embedding, dan mendapatkan imperceptibility (Rachmawanto & Sari, 2014).

*Discrete Cosine Transform* (DCT) adalah sebuah teknik untuk mengubah sebuah sinyal ke dalam komponen frekuensi dasar, metode *Discrete Cosine Transform* (DCT) memiliki kelebihan yakni pesan rahasia pada gambar akan tetap terjaga terhadap kompresi pada gambar akan tetapi memiliki kelemahan yaitu penurunan kualitas citra stego jika dibandingkan dengan citra aslinya, semakin banyak katakter yang disisipkan pada gambar akan semakin turun nilai PSNR yang didapatkan atau kualitas gambarnya semakin menurun (Faruqi & Rozi, 2015) dan Herlinawati (2016) juga mengungkapkan Kualitas

video yang dihasilkan bergantung dari besarnya ukuran pesan, semakin besar pesan yang disisipkan maka kualitas video akan semakin buruk, dari kelemahan algoritma DCT tersebut dibutuhkan sebuah proses perbaikan kualitas citra sehingga kualitas citra lebih baik dan mendekati citra aslinya. Sejauh ini pengembangan metode steganografi masih terus dilakukan untuk meningkatkan keamanan dan kualitas *stego-image*. Beberapa hal yang umum dilakukan adalah dengan menggabungkan beberapa metode dan peningkatan algoritma.

Penelitian sebelumnya pernah dilakukan oleh Wissarto (2016) dengan menerapkan Steganografi menggunakan algoritma SLT dan peningkatan kualitas citra menggunakan Huffman Coding pada Citra *GreyScale* mengungkapkan bahwa ukuran *Secret-Image* berpengaruh terhadap ratio PSNR yang diperoleh dimana semakin besar *secret image* yang digunakan semakin kecil ratio PSNR yang diperoleh. Garno & Solehudin (2017) juga melakukan penelitian dengan menggabungkan teknik steganografi dengan model penyisipannya menggunakan teori matematik discrete cosine transform(DCT) yang dipadukan dengan model teori matematik interpolasi bilinear sehingga dapat menampung pesan dalam ukuran besar, akan tetapi ukuran *stego image* yang dihasilkan jauh lebih besar dibandingkan *cover image*, dan nilai PSNR yang dihasilkan kurang < 30 db, nilai PSNR jatuh dibawah 30 db mengindikasikan kualitas yang relative rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas.

Batarius & Maslim (2012) juga melakukan penelitian dengan Analisis perbandingan yang dilakukan berdasarkan nilai Peak Signal to Signal Ratio (PSNR) dan waktu yang dihasilkan dalam proses steganografi dan mengungkapkan bahwa metode Discrete Cosine Transform (DCT) proses steganografi akan dilakukan dengan lebih cepat dibandingkan dengan metode lainnya tetapi citra hasil steganografi mempunyai nilai PSNR yang paling kecil dibandingkan dengan metode yang lainnya yang berarti citra hasil steganografi yang dihasilkan kurang menyerupai citra aslinya. Semakin besar nilai MSE yang dihasilkan, maka semakin terlihat perbedaan citra asli dengan citra hasil steganografi sehingga hal ini dapat menyebabkan citra steganografi rentan diketahui keberadaannya. Secara kasat mata, nilai terbaik pada citra menunjukkan bahwa mata kita hampir tidak mengenali citra yang asli dan citra hasil steganografi, dalam artian citra asli dan citra steganografi hampir tidak terdapat perubahan (Wirayasa, 2015).

Dari latar belakang permasalahan diatas, peneliti mencoba melakukan penelitian untuk menutupi kelemahan steganografi DCT terkait masalah kualitas citra stego dengan cara menggabungkan dua algoritma yaitu *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT), dengan tujuan untuk meningkatkan kualitas citra stego. Pengujian kualitas Citra dilakukan dengan mengukur nilai MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*). MSE dan PSNR merupakan nilai untuk membandingkan citra asli dengan citra hasil dari pengolahan citra digital dalam hal ini citra hasil proses steganografi, dengan harapan nilai MSE semakin rendah dan nilai PSNR menjadi semakin tinggi sehingga citra steganografi yang dihasilkan semakin baik dan mendekati citra aslinya.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang diatas, dirumuskan permasalahan dalam penelitian ini yaitu :

1. Bagaimana mengimplementasikan metode gabungan algoritma *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT) pada citra ?
2. Bagaimana hasil implementasi steganografi *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT) terhadap kualitas citra ?

## **1.3 Batasan Masalah**

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Data yang digunakan pada proses steganografi adalah bentuk citra digital (\*.tiff) offline, yaitu gambar sudah dalam bentuk file.
2. Ukuran citra digital yang dijadikan cover image adalah 256x256, 512x512 dan 1024x1024 piksels.
3. File rahasia yang akan disisipkan berupa file teks dengan format text (.txt).
4. Parameter yang digunakan dalam uji kualitas adalah nilai PSNR dan MSE citra.
5. Aplikasi dibuat dengan Matlab R2018a.

#### **1.4 Tujuan Penelitian**

Tujuan yang ingin dicapai dari penelitian ini adalah

1. Mengimplementasikan metode gabungan algoritma *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT) pada citra.
2. Mendapatkan hasil implementasi steganografi *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT) terhadap kualitas citra.

#### **1.5 Manfaat Penelitian**

Berdasarkan tujuan dari penelitian, diharapkan peneliti dapat mengetahui hasil perbandingan antara algoritma SLT, algoritma DCT dan gabungan algoritma *Stantlet Transform* (SLT) dan *Discrete Cosine Transform* (DCT) terhadap hasil kualitas citra.

#### **1.6 Metode Penelitian**

Dalam menyelesaikan penelitian ini perlu disusun langkah-langkah penyelesaian penelitian secara sistematis yang disebut dengan metodologi penelitian. Metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

1. Melakukan Identifikasi Masalah  
Tahap awal dalam penelitian ini adalah merumuskan masalah yang akan menjadi titik focus pada penelitian yang akan dilakukan.
2. Tinjauan Pustaka  
Tinjauan pustaka dilakukan guna mencari literatur pendukung yang terkait dalam penelitian ini.
3. Metode Pengumpulan Data  
Metode yang digunakan untuk mengumpulkan data pada penelitian ini yaitu dengan melakukan studi literatur. Studi literatur dilakukan untuk mencari semua informasi yang berkaitan tentang Steganografi SLT dan DCT pada citra serta informasi tentang contrast stretching dan histogram equalization seperti membaca buku-buku, paper atau jurnal-jurnal dan mengunjungi situs-situs yang ada di internet yang berhubungan dengan Steganografi.
4. Perancangan Sistem  
Metode yang digunakan untuk membangun sebuah sistem atau yaitu dengan menggunakan metode perancangan terstruktur serta menggunakan *Workflow* (Bagan Kerja). Perancangan ini dimulai dari perancangan secara umum yang disebut dengan

desain konseptual (*conceptuai design*) atau desain logikal (*logical design*). Dilanjutkan dengan perancangan masing-masing poin pembahasan.

#### 5. Implementasi Sistem

Implementasi adalah proses untuk memastikan bahwa sistem atau metode algoritma yang dibangun bebas dari kesalahan dan mudah digunakan oleh pengguna.

#### 6. Pengujian Metode

Pada tahapan ini dilakukan pengujian system sesuai dengan parameter yang telah ditentukan.

#### 7. Kesimpulan

Penyusunan laporan akhir penelitian ini.

### **1.7 Sistematika Penulisan**

Tahapan ini memberikan gambaran secara umum tentang penyusunan penelitian yang dilakukan, dalam sistematika penulisan terbagi dalam beberapa BAB yaitu :

#### **Bab I Pendahuluan**

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan diteliti. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

#### **Bab II Landasan Teori**

Pada Bab ini menjelaskan teori-teori yang terkait untuk memecahkan masalah dalam penelitian yang dilakukan.

#### **Bab III Metodologi Penelitian**

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang akan digunakan, desain dan perancangan antarmuka aplikasi yang akan dibuat, serta pengujian terhadap parameter yang telah ditentukan.

#### **Bab IV Hasil dan Pembahasan**

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diteliti dengan membangun sebuah aplikasi dan cara pengujian yang dilakukan untuk menjawab permasalahan yang di usulkan.

## **Bab V Kesimpulan dan Saran**

kesimpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

## BAB II

### Tinjauan Pustaka

#### 2.1 Literatur Riview

Beberapa penelitian yang pernah membahas tentang steganografi terkait penelitian yang akan dilakukan yaitu penelitian yang dilakukan oleh Wissarto (2016) dan Abduljabar (2016) yaitu melakukan Steganografi menggunakan algoritma SLT pada citra /Image dan peningkatan kualitas citra menggunakan Huffman Coding, mengungkapkan bahwa ukuran Secret-Image berpengaruh terhadap ratio PSNR yang diperoleh dimana semakin besar secret image yang digunakan semakin kecil ratio PSNR yang diperoleh, dan penerapan SLT-Huffman Coding pada steganografi citra grayscale menghasilkan PSNR yang lebih baik dari penerapan metode SLT maupun SLT-DCT tanpa Huffman Coding dengan dapat meningkatkan ratio PSNR lebih dari 10 db.

Garno & Solehun (2017) melakukan steganografi dengan metode DCT dengan *interpolasi bilinear* untuk keamanan pesan, teknik *interpolasi bilinear* pada penelitiannya digunakan untuk memperbesar media yang akan digunakan menjadi wadah dalam penyisipan, sehingga didapatkan kapasitas pesan yang besar akan tetapi kelemahan dari metode ini adalah ukuran file menjadi lebih besar dan kualitas dari citra menjadi kurang baik.

Faruqi & Rozi (2015) melakukan penelitian tentang steganografi pada citra atau image menggunakan algoritma DCT dan mengungkapkan semakin banyak katakter yang disisipkan pada gambar akan semakin turun nilai PSNR yang didapatkan atau kualitas gambarnya semakin menurun, Herlinawati (2016) melakukan Steganografi pada Video H263 menggunakan algoritma DCT mengungkapkan Kualitas video yang dihasilkan bergantung dari besarnya ukuran pesan, semakin besar pesan yang disisipkan maka kualitas video akan semakin buruk. (Zulfikar & Harjoko, 2016) melakukan perbandingan steganografi antara DCT Sekuensial dan DCT F5, dan melakukan penerapan *Point Operation Image Enhancement* mengungkapkan kualitas citra stego pada steganografi DCT F5 lebih baik dibandingkan dengan steganografi DCT sekuensial baik sebelum penerapan POIE maupun setelah penerapan POIE dan Kapasitas pesan pada steganografi DCT sekuensial lebih besar dibandingkan dengan steganografi DCT F5 baik sebelum penerapan POIE maupun setelah penerapan POIE.



Penerapan steganografi DCT menggunakan aplikasi Matlab juga pernah dilakukan oleh Ardiansyah, Susilo, & Erlansari (2017) mengungkapkan Metode DCT (Discrete Cosine Transform) dapat menyisipkan pesan kedalam gambar baik itu berupa huruf, angka dan simbol. Penelitian selanjutnya dilakukan (Aji & Wijanarto, p. 2016) tentang pengimplementasian metode Huffman untuk kompresi citra hasil dari steganografi DCT dan menjelaskan bahwa Kompresi algoritma huffman tidak merubah ukuran citra dikarenakan hasil stego DCT sudah melakukan kuantisasi citra sampai piksel yang paling minimum. Jadi tidak perlu digunakan kompresi algoritma huffman untuk citra hasil stego DCT.

Penelitian tentang peningkatan kualitas citra steganografi juga pernah dilakukan oleh Vyas & Pal (2014) dan Kumar (2013) dengan memodifikasi algoritma LSB, Vyas & Pal melakukan modifikasi algoritma SLB dengan menyembunyikan dua bit ke dua bit dengan mengambil nilai yang sama, hamper sama dengan Vyas & Pal, Kumar melakukan modifikasi algoritma dengan mencari nilai2 yang sama antara pesan rahasia dan gambar kemudian menyisipkan dua bit ke dua bit pesan rahasia kedalam pixel gambar.

Hadi dan mahmood (2017) juga melakukan penelitian tentang kompresi dengan algoritma DCT-DWT dan DCT-SLT dan membanding nilai PNSR dari masing2 algoritma, SLT adalah DWT ortogonal dan menyediakan lokalisasi waktu yang lebih baik daripada DWT. Hasil yang didapatkan yaitu algoritma *hybrid* SLT-DCT untuk kompresi gambar memiliki kinerja yang lebih baik dalam kualitas dan kinerja dibandingkan dengan DWT-DCT. Teknik DCT-SLT meningkatkan nilai CR, PSNR, SSIM dan UQI dibandingkan teknik DWT-DCT. Hasil penelitian menunjukkan bahwa nilai PSNR yang didapatkan rata-rata lebih dari 43dB, yang dianggap sangat tinggi, ukuran file berkurang dari (786432 byte) menjadi (29494 byte) dalam teknik DCT-SLT dan dikurangi menjadi (46917 byte) pada teknik DWT-DCT. Dan waktu yang diperlukan untuk menghitung SLT-DCT adalah 16,085 detik sementara pada teknik DWT-DCT adalah 33,624 detik, ini berarti bahwa teknik DCT-SLT lebih baik daripada teknik DWT-DCT.

Tabel 2. 1 Literatur Review

No	Paper Utama	Judul	Metode Pendekatan	Objek Digital	Tujuan
1	Wissarto (2016)	Implementasi Slantlet Transform (SLT) Dan Huffman Coding pada Steganografi Citra Grayscale	SLT dan Huffman Coding	Cover : Gambar Pesan : Gambar	Menerapkan Huffman Coding pada pesan rahasia dan selanjutnya melakukan penyisipan menggunakan algoritma SLT
2	Anuradha Goswami, Sarika Khandelwal(2016)	Hybrid DCT-DWT Digital Image Steganography	Algoritma DWT-DCT	Cover : Gambar Pesan : Gambar	Mengembangkan algoritma steganografi DWT dan DCT pada gambar, kemudian menghitung nilai PNSR dari stego image dan membandingkannya dengan metode vivek.
3	Herlinawati (2016)	Steganografi Video H263 dengan Metode Discrete Cosine Transform	Discrete Cosine Transform (DCT)	Cover: Video H2 63 Pesan : Text	Mengimplementasi steganografi dengan metode DCT <i>Modification</i> pada video dan menghasilkan perangkat lunak yang disebut XGP Dekstop
4	Zulfikar & Harjoko (2016)	Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement	DCT Sekuensial dan DCT F5	Cover : Gambar Pesan : Text	Melakukan perbandingan steganografi antara DCT Sekuensial daan DCT F5, dan melakukan penarapan <i>Point Operation Image Enhancement</i> .

No	Paper Utama	Judul	Metode Pendekatan	Objek Digital	Tujuan
5	Dr.Ismael Hadi challoob Rasha Riyadh Mahmood (2017)	Suggested hybrid Transform Technique for image compression	DCT, DWT, SLT and Hybrid DCT-SLT	Gambar	Melakukan kompresi dengan algoritma DCT-DWT dan DCT-SLT dan membanding nilai PNSR dari masing2 algoritma.
6	R. K. Nithya(2013)	The Image Steganography Techniques to Improve the Security and the Stego Image Quality	Reversible steganography dan Least Significant Bit	Cover : Gambar Pesan : Text	Mengembangkan algoritma reversible steganography untuk mengamankan dan meningkatkan kualitas citra steganografi.
7	Abduljabar (2016)	Steganography System Using Slantlet Transform	Algoritma Stantlet Transform dan Huffman Coding	Cover : Gambar Pesan : Gambar	Menerapkan Huffman Coding pada pesan rahasia dan selanjutnya melakukan penyisipan menggunakan algoritma SLT
8	Garno & Solehudin (2017)	Teknik Steganografi dengan Metode Discrete Cosine Transform (DCT) pada Citra Interpolasi Bilinier untuk Pengamanan Pesan	Discrete Cosine Transform (DCT) dan Interpolasi Bilinier	Cover : Gambar Pesan : Text	Menggabungkan teknik steganografi dengan model penyisipannya menggunakan teori matematik discrete cosine transform(DCT) yang dipadukan dengan model teori matematik interpolasi bilinear sahingg dapat menampung pesan dalam ukuran besar.

No	Paper Utama	Judul	Metode Pendekatan	Objek Digital	Tujuan
9	Imamah (2015)	Enkripsi Data Menggunakan Steganografi Untuk Keamanan Data Pada Cloud	Algoritma Stantlet Transform (SLT)	Cover : Gambar Pesan : Text	Melakukan penyisipan pesan menggunakan algoritma SLT dan menghitung nilai PNSR dari masing2 stego image.
10	Aji & Wijanarto (2014)	Implementasi Metode Huffman Untuk Kompresi Citra Hasil Dari Steganografi Discrete Cosine Transform (Dct)	Discrete Cosine Transform (DCT) dan Metode Huffman	Cover : Gambar Pesan : Gambar	Melakukan proses steganografi dengan algoritma DCT kemudian membandingkan <i>stego image</i> hasil Steganografi DCT dengan stego image yang kemudian di kompresi dengan Huffman coding
11	Usulan Penelitian	Implementasi Metode Steganografi SLT-DCT pada Citra untuk Meningkatkan Kualitas Citra Steganografi	SLT, DCT, Gabungan SLT-DCT	Cover : Gambar Pesan : Text	Meningkatkan Kualitas Stego image dengan menerapkan algoritma SLT dan DCT

## 2.2 Tinjauan Pustaka

### 2.2.1 Steganografi

Steganografi adalah kata Yunani yang berarti tulisan tersembunyi. Kata "steganos" berarti "tertutup" dan "grafis" berarti "tulisan". Dengan demikian, steganografi tidak hanya seni menyembunyikan data tapi juga menyembunyikan fakta transmisi data rahasia. Steganografi menyembunyikan data rahasia di file lain sedemikian rupa sehingga hanya penerima yang tahu adanya pesan. Dahulu kala, data itu dilindungi dengan menyembunyikannya di belakang lilin, menulis meja, perut kelinci atau di kulit kepala para budak. Tapi hari ini sebagian besar orang mengirimkan data berupa teks, gambar, video, dan audio di atas medium. Agar transmisi data rahasia aman, objek multimedia seperti audio, video, gambar digunakan sebagai sumber cover untuk menyembunyikan data.

Steganografi merupakan teknik menyembunyikan pesan rahasia kedalam pesan lainnya sebagai wadah (media) sedemikian rupa sehingga keberadaan pesan rahasia tersebut tidak diketahui atau disadari keberadaannya oleh orang lain. Steganografi membutuhkan dua properti: pesan sebagai wadah penampung dan pesan rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital baik sebagai wadah penampung maupun data rahasia, misalnya citra, suara (audio), teks, dan video (Prabowo, Hidayatno, & Christyono, 2011).

Steganografi merupakan proses keamanan atau perlindungan data multimedia dengan cara menyisipkan pesan rahasia pada media digital lain dengan tujuan menyembunyikan pesan rahasia (data hiding), sedangkan watermarking merupakan cabang ilmu dari steganografi, yang membedakan steganografi dengan watermark yaitu pada konten yang dilindungi, pada steganografi yang dilindungi adalah pesan rahasianya sedangkan watermark yang dilindungi adalah multimedianya sedangkan pesan rahasianya dijadikan sebagai identitas kepemilikan file untuk proteksi dan perlindungan kepemilikan file multimedia tersebut (Innuddun, 2016).

Penyembunyian data dan informasi rahasia ke dalam citra digital akan mempengaruhi kualitas suatu citra. Kriteria yang harus diperhatikan dalam penyembunyian data tersebut adalah:

#### 1. Imperceptibility.

Kualitas cover citra tidak berbeda jauh dari citra steganografi, setelah melakukan penambahan data dan informasi rahasia, citra hasil steganografi masih terlihat dengan

baik. Jika dilihat dengan kasat mata, tidak dapat dibedakan antara citra asli dan citra steganografi dan keberadaan data rahasia yang ada didalam citra steganografi sulit diketahui.

## 2. Robustness.

Data yang disembunyikan harus tahan (robust) terhadap berbagai serangan (attack) atau manipulasi data citra yang dilakukan pada citra cover, seperti pemotongan (cropping), pengubahan ukuran, pengubahan kontras, pengubahan format, dll. Bila pada citra cover dilakukan manipulasi data citra tersebut, maka data yang disembunyikan seharusnya tetap utuh atau tidak rusak jika diekstraksi kembali.

## 3. Recovery.

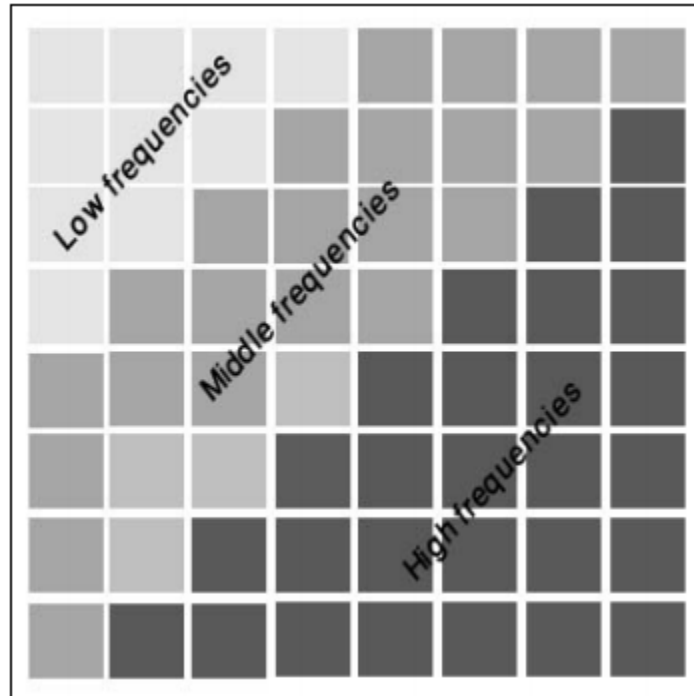
Data dan informasi yang disembunyikan harus dapat dikembalikan (reveal). Karena steganografi bertujuan untuk *data hiding*, maka suatu saat data dan informasi rahasia yang berada di dalam citra cover harus dapat diambil kembali untuk digunakan lebih lanjut.

Steganografi memiliki dua proses, yaitu encoding dan decoding. Encoding merupakan proses penyisipan data dan informasi rahasia kedalam media penampung (coverttext) dalam hal ini adalah gambar/citra digital, sedangkan decoding adalah proses ekstraksi data dan informasi rahasia tersebut dari citra steganografi (stego image) (Aji & Wijanarto, 2015).

### 2.2.2 Algoritma DCT

Discrete Cosine Transform adalah sebuah teknik untuk mengubah sebuah sinyal ke dalam bentuk komponen frekuensi dasar. Discrete Cosine Transform merepresentasikan sebuah citra dari penjumlahan sinusoida dari magnitude dan frekuensi yang berubah-ubah. Sifat dari DCT adalah mengubah informasi citra yang signifikan dikonsentrasikan hanya pada beberapa koefisien DCT (Faruqi & Rozi, 2015).

Discrete Cosine Transform merupakan skema lossy compression yang digunakan dalam JPEG kompresi gambar NxN block ditransformasikan dari domain spasial ke domain DCT. DCT menyusun sinyal tersebut ke frekuensi spasial yang disebut dengan koefisien DCT. Frekuensi DCT yang lebih rendah muncul pada kiri atas dari sebuah matriks DCT, dan frekuensi koefisien DCT yang lebih tinggi berada pada kanan bawah dari matriks DCT. Sistem penglihatan manusia tidak begitu sensitive dengan error-error yang ada pada frekuensi tinggi dibanding dengan yang ada pada frekuensi rendah. Karena itu, maka frekuensi yang lebih tinggi tersebut dapat dikuantisasi. (Faruqi & Rozi, 2015).



Gambar 2. 1 Distribusi Frekuensi pada Blok DCT (Faruqi & Rozi, 2015)

Discrete Cosine Transform (DCT) untuk suatu citra merupakan sinyal dua dimensi, Discrete Cosine Transform dua dimensi dapat diperoleh dengan rumus berikut:

$$C(u,v) = \frac{2}{\sqrt{MN}} \alpha(u) \alpha(v) \sum_{X=0}^{N-1} \sum_{Y=0}^{M-1} f(x,y) \cos\left(\frac{\pi(2Y+1)u}{2N}\right) \cos\left(\frac{\pi(2X+1)v}{2M}\right) \quad (2.1)$$

C : koefisien pada index ke-u

M : ukuran tinggi matriks

N : ukuran lebar matriks

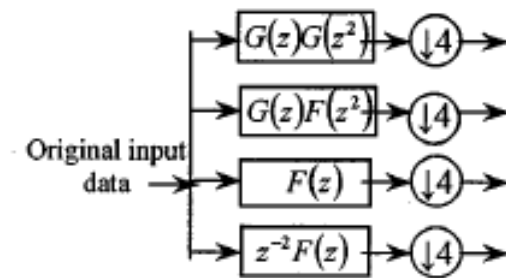
x,y : indek yang dicari nilainya

### 2.2.3 Algoritma SLT

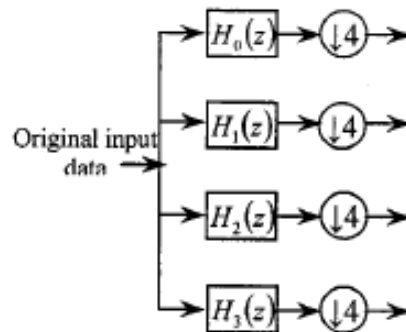
Algoritma SLT adalah pengembangan metode dari DWT dimana SLT mempunyai waktu lokalisasi yang lebih baik dari DWT karena dukungan komponen filter yang lebih pendek. DWT biasanya diimplementasikan dalam bentuk bank iterasi dengan struktur pohon, tapi SLT terinspirasi dari bentuk struktur paralel dengan cabang paralel (Wissarto, 2014).

Output turun sampel dengan faktor 4 yang merupakan transformasi koefisien kemudian thresholding menggunakan parameter yang sesuai. Invers Slantlet Transform (ISLT) adalah metode untuk merekonstruksi hasil embedding SLT (Wissarto, 2014). Sushil Kumar dan S.K. Muttoo menjelaskan keuntungan Slantlet Transform (SLT) yang lebih baik dari DWT, Haar Wavelet dan Contourlet transform dalam kualitas gambar, payload terbaik,

mendapatkan hasil yang lebih baik untuk mengekstraksi dan embedding gambar asli, meningkatkan kapasitas embedding, dan mendapatkan imperceptibility (Rachmawanto & Sari, 2014).



Gambar 2. 2 Iterasi FilterBank menggunakan DWT (Kumar & Muttoo, 2013)



Gambar 2. 3 Iterasi FilterBank Menggunakan SLT (Kumar & Muttoo, 2013)

Teknik kompresi berbasis SLT menghasilkan kinerja yang lebih baik dibandingkan dengan DCT dan DWT. Dalam skema kompresi menggunakan SLT, data pertama kali diterapkan pada struktur filter dua tingkat  $H_0(z)$ ,  $H_1(z)$ ,  $H_2(z)$ , dan  $H_3(z)$ . Output dari filter ini turun sampel dengan faktor 4, yang merupakan koefisien transformasi dari data input yang diperoleh setelah operasi konvolusi dari data asli dengan koefisien filter (Kumar & Muttoo, 2013).

#### 2.2.4 Matlab

Matlab merupakan sebuah singkatan dari Matrix Laboratory, yang pertama kali dikenalkan oleh University of New Mexico dan University of Stanford pada tahun 1970. software ini pertama kali memang digunakan untuk keperluan analisis numerik, aljabar linier dan teori tentang matriks. Saat ini, kemampuan dan fitur yang dimiliki oleh Matlab sudah jauh lebih lengkap dengan ditambahkannya toolbox toolbox yang sangat luar biasa. (NS, 2015). Beberapa manfaat yang didapatkan dari Matlab (NS, 2015) antara lain:

- a. Perhitungan Matematika



- b. Komputasi numeric
- c. Simulasi dan pemodelan
- d. Visualisasi dan analisis data
- e. Pembuatan grafik untuk keperluan sains dan teknik
- f. Pengembangan aplikasi, misalnya dengan memanfaatkan GUI.

Matlab dapat dipadang sebagai sebuah kalkulator dengan fitur yang lengkap. Kita pernah menggunakan kalkulator dengan degan fasilitas minimal, misalnya hanya terdapat fasilitas penambahan, pengurangan perkalian dan pembagian. Kalkulator yang lebih lengkap lagi adalah kalkulator scientific dimana fasilitas yang diberikan tidak hanya yang disebutkan di atas, melainkan sudah ada fungsi-fungsi trigonometri, bilangan kompleks, akar kuadrat dan logaritma. Matlab mirip dengan kalkulator tersebut, tetapi dengan fitur-fitur yang lengkap diantaranya dapat digunakan untuk memprogram, aplikasi berbasis GUI dan lengkap dengan toolbox yang dapat dimanfaatkan untuk memecahkan masalah sains dan teknik.

Matlab memberikan kemudahan bagi para pengguna untuk menemukan bantuan sehubungan dengan semua fasilitas yang diberikan oleh Matlab. Misalnya, bantuan tentang bagaimana memulai Matlab pertama kali, trik pemrograman, membuat grafik 2 dan 3 dimensi, menggunakan tool akuisisi data, pengolahan sinyal, penyelesaian persamaan diferensial parsial. Untuk memperoleh bantuan tersebut, kita dapat memilih MATLAB Menu dari menu Help (NS, 2015). Untuk bantuan tentang Matlab sendiri, dibagi atas beberapa bagian (NS, 2015) antara lain:

- a. Development Environment, bagian ini akan memberikan informasi yang lengkap mengenai desktop dari Matlab.
- b. Mathematics, bagian yang menjelaskan bagaimana menggunakan fitur yang dimiliki oleh Matlab untuk dalam mengolah data matematis dan statistik. Isi dalam bantuan ini dicakup antara lain: Matrks dan aljabar linier, polinomial dan interpolasi, analisis data dan statistik, fungsi function, matriks jarang (sparse matrix).
- c. Programming and data type, bagian ini menjelaskan bagaimana membuat script dan fungsi dengan menggunakan Matlab. Bantuan ini mencakup pemrograman M-File, larik, larik multidimensi, optimalisasi performance Matlab, tip pemrograman Matlab.

- d. Graphics, bagian ini menjelaskan tentang bagaimana membuat atau mengplot grafik dari data yang kita miliki. Yang termasuk dalam bagian ini antara lain, dasar-dasar pengeplotan, format grafik, membuat grafik khusus misalnya grafik dalam bentuk bar, histogram, contour dan lain-lain
- e. 3-D Visualization, bagian ini menjelaskan dengan tuntas bagaimana menampilkan data yang kita miliki dalam grafik 3 dimensi, termasuk didalamnya membuat grafik 3D, menentukan tampilan objek, transparansi objek, lighting dan lain-lain.
- f. Creating Graphical User Interfaces, bagian ini menjelaskan bagaimana kita dapat membuat GUI (Graphical User Interface) berbasis Matlab.

Disamping bagian-bagian yang sudah disebutkan di atas, disini juga disertakan beberapa bagian tambahan yang ikut melengkapi dokumentasi penjelasan tentang Matlab, diantaranya *function-By category*, *function-Alphabetical List*, *handle graphic property browser*, *external interfaces/API*, *external interfaces/API references* dan lain-lain (NS, 2015).

## **2.2.5 Metode Contrast Stretching Dan Histogram Equalization**

Peningkatan kualitas citra dibagi menjadi dua jenis yaitu contrast stretching dan histogram equalization. Contrast stretching merupakan metode perbaikan kualitas citra yang bertujuan untuk meningkatkan atau menurunkan kontras suatu citra dengan memperlebar atau mempersempit range nilai intensitas piksel citra, sedangkan histogram equalization merupakan metode perbaikan kualitas citra yang bertujuan untuk meratakan perebaran nilai intensitas piksel suatu citra (Pamungkas, 2012).

### **A. Contrast Stretching**

Kualitas citra dengan kontras-rendah dapat diperbaiki dengan operasi peregangan kontras (contrast stretching). Melalui operasi ini, nilai-nilai keabuan pikselakan menjangkau dari 0 sampai 255 (pada citra 8bit), dengan kata lain seluruh nilai keabuan piksel terpakai secara merata (Kurniawan, 2013). Proses peregangan kontras (contrast stretching) pada citra 8 bit dapat dilakukan dengan cara sebagai berikut :

Yang pertama yaitu mengelompokkan dan menghitung jumlah piksel berdasarkan nilai keabuannya (membuat histogram), yang kedua dengan cara memindai histogram dari nilai keabuan terkecil ke nilai keabuan terbesar (0 sampai 255) sehingga ditemukan batas nilai keabuan terendah dan batas nilai keabuan tertinggi dari kelompok piksel (citra). Yang

ketiga yaitu memetakan (menskalakan) piksel – piksel yang berada di antara batas terendah dan batas tertinggi untuk memenuhi rentang nilai – nilai keabuan yang lengkap (0 sampai 255) (Kurniawan, 2013) .

## B. Histogram Equalization

Histogram citra memberikan informasi tentang penyebaran intensitas piksel-piksel di dalam citra. Misalnya, citra yang terlalu terang atau terlalu gelap memiliki histogram yang sempit. Agar kita memperoleh citra yang baik, maka penyebaran nilai intensitas harus diubah. Teknik yang lazim dipakai adalah perataan histogram(histogram equalization). Tujuan dari perataan histogram adalah untuk mendistribusikan histogram secara merata, sehingga setiap nilai keabuan memiliki jumlah piksel yang relatif sama (Kurniawan, 2013).

Menurut Marvin Ch. Wijaya dan Agus Priyono (2007), tahapan untuk melakukan histogram equalization adalah sebagai berikut. Tahapan dalam melakukan peregangan histogram (histogram equalization) yang pertama yaitu mengelompokkan dan menghitung jumlah piksel berdasarkan nilai keabuannya (membuat histogram), lalu memindai (scan) histogram dari nilai keabuan 0 sampai 255 untuk menemukan batas nilai keabuan terendah dan batas nilai keabuan tertinggi dari kelompok piksel (citra), yang ketiga yaitu menghitung peluang kemunculan setiap intensitas piksel ( $P_r$ ) dan menghitung distribusi kumulatifnya ( $S_k$ ) (proses normalisasi), selanjutnya yaitu membulatkan hasil perkalian distribusi kumulatif ( $S_k$ ) dengan jumlah variansi nilai keabuan terbesar yang muncul(L-1). Yang terakhir yaitu memetakan (menskalakan) piksel-piksel hasil dengan cara mengkalikan hasil pembulatan dengan skala keabuan yang digunakan (255 untuk citra 8bit) (transformasi balik).

### 2.2.6 Citra Digital

Citra adalah representasi dua dimensi untuk bentuk fisik nyata tiga dimensi. Citra dalam perwujudannya dapat bermacam-macam, mulai dari gambar hitam-putih pada sebuah foto (yang tidak bergerak) sampai pada gambar berwarna yang bergerak pada pesawat televisi. Proses transformasi dari bentuk tiga dimensi ke bentuk dua dimensi untuk menghasilkan citra akan dipengaruhi oleh bermacam-macam factor yang mengakibatkan penampilan citra suatu benda tidak sama persis dengan bentuk fisik nyatanya. Faktor-faktor tersebut merupakan efek degradasi atau penurunan kualitas yang dapat berupa rentang kontras benda yang terlalu sempit atau terlalu lebar, distorsi geometrik, keaburan (blur), keaburan akibat obyek yang bergerak (motion blur), noise atau gangguan yang

disebabkan oleh interferensi peralatan pembuat citra, baik berupa transduser, peralatan elektronik ataupun peralatan optic (Putri, 2016).

Pengolahan citra dilakukan dengan komputer digital maka citra yang akan diolah terlebih dahulu ditransformasikan ke dalam bentuk besaran-besaran diskrit dari nilai tingkat keabuan pada titik-titik elemen citra. Bentuk citra ini disebut citra digital. Setiap citra digital memiliki beberapa karakteristik, antara lain ukuran citra, resolusi dan format lainnya. Umumnya citra digital berbentuk persegi panjang yang memiliki lebar dan tinggi tertentu, yang biasanya dinyatakan dalam banyaknya titik atau piksel (picture elemen/pixel) (Putri, 2016).

Ukuran citra dapat juga dinyatakan secara fisik dalam satuan panjang (misalnya mm atau inch). Dalam hal ini tentu saja harus ada hubungan antara ukurn titik penyusun citra dengan satuan panjang. Hal tersebut dinyatakan dengan resolusi yang merupakan ukuran banyaknya titik untuk setiap satuan panjang. Biasanya satuan yang digunakan adalah dpi (dot per inch). Makin besar resolusi makin banyak titik yang terkandung dalam citra dengan ukuran fisik yang sama. Hal ini memberikan efek penampakan citra menjadi semakin halus. Format citra digital ada bermacam- macam. Karena sebenarnya citra merepresentasikan informasi tertentu, sedangkan informasi tersebut dapat dinyatakan secara bervariasi, maka citra yang mewakilinya dapat muncul dalam berbagai format. Citra yang merepresentasikan informasi yang hanya bersifat biner untuk membedakan 2 keadaan tentu tidak sama citra dengan informasi yang lebih kompleks sehingga memerlukan lebih banyak keadaan yang diwakilinya. Pada citra digital semua informasi tadi disimpan dalam bentuk angka, sedangkan penampilan angka tersebut biasanya dikaitkan dengan warna (Utama, 2012).

Citra digital (digital image) adalah citra kontinyu  $f(x,y)$  yang sudah didiskritkan baik koordinat spasial maupun tingkat kecerahannya. Setiap titik biasanya memiliki koordinat sesuai dengan posisinya dalam citra. Koordinat ini biasanya dinyatakan indeks  $x$  dan  $y$  hanya bernilai bilangan bulat positif, yang dapat dimulai dari 0 atau 1. Citra digital adalah gambaran dari suatu objek yang bersifat analog berupa sinyal-sinyal video pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan seperti harddisk, flashdisk, memory card dan berbagai macam media penyimpanan lainnya (Utama, 2012).

### 2.2.7 Peak Signal to Noise Ratio (PSNR)

*Peak Signal to Noise Ratio* adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau atau noise yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (db). Pada makalah ini PSNR digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus menentukan nilai *Mean Square Error* (MSE).

Perhitungan untuk menentukan PSNR adalah sebagai berikut:

$$\text{PSNR} = 10 \log_{10} \left( \frac{b^2}{\text{MSE}} \right) \quad (2.2)$$

Nilai PSNR yang tinggi menunjukkan bahwa mata kita hampir tidak mengenali citra yang asli dan citra hasil steganografi, dalam artian citra asli dan citra steganografi hampir tidak terdapat perubahan.

### 2.2.8 Mean Square Error (MSE)

MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi. Dalam steganografi, MSE adalah nilai error kuadrat rata-rata antara citra asli (cover-image) dengan citra hasil penyisipan (stegano-image). Dengan perhitungan MSE sebagai berikut:

$$\text{MSE} = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N [I(x,y) - I'(x,y)]^2 \quad (2.3)$$

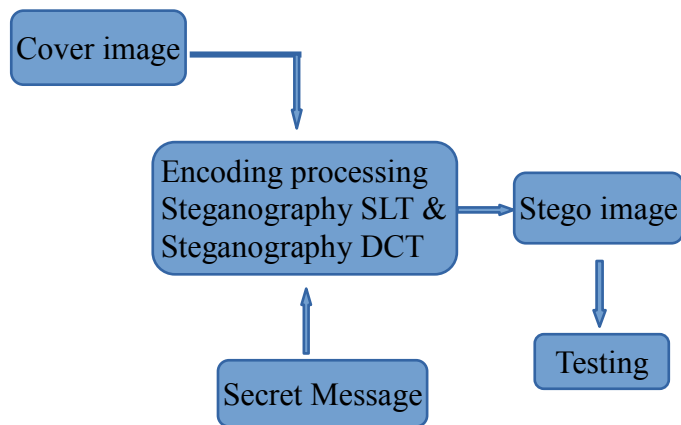
Dimana  $x$  dan  $y$  adalah koordinat dari gambar,  $M$  dan  $N$  merupakan dimensi citra.  $I(x,y)$  merupakan nilai piksel pada citra asli, sedangkan  $I'(x,y)$  merupakan nilai piksel pada citra hasil steganografi.

## BAB III

### Metodologi Penelitian

#### 3.1 Perancangan Umum Sistem

Berdasarkan permasalahan yang telah dipaparkan pada BAB I maka akan dibangun sebuah aplikasi steganografi yang akan digunakan untuk melakukan penyisipan pesan dan akan dilakukan beberapa pengujian. Aplikasi ini diharapkan dapat menganalisa kualitas citra, kapasitas pesan dan ketahanan pesan pada algoritma SLT-DCT



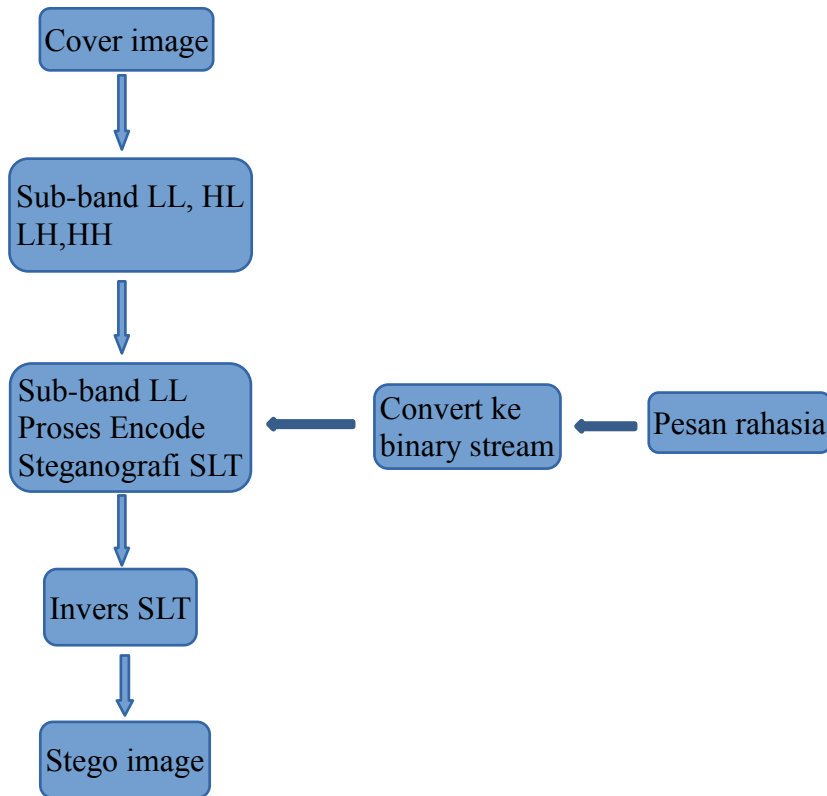
Gambar 3. 1 Perancangan Umum Sistem

Pada gambar diatas dijelaskan proses perancangan pengujian secara umum, akan dilakukan pengujian pada Citra Steganografi hasil dari algoritma SLT dan DCT. Pada proses penyisipan pesan, proses yang pertama yaitu Citra Cover akan disisipi pesan menggunakan metode steganografi SLT dan DCT, sehingga menghasilkan Citra Stego, selanjutnya masing-masing Citra Stego tersebut akan dilakukan pengujian terhadap kualitas citra, kapasitas pesan, serta ketahanannya, dan selanjutnya akan dilakukan uji coba perbandingan steganografi SLT-DCT dengan steganografi SLT dan steganografi DCT.

### 3.2 Metode Steganografi yang digunakan

#### 3.2.1 Steganografi SLT

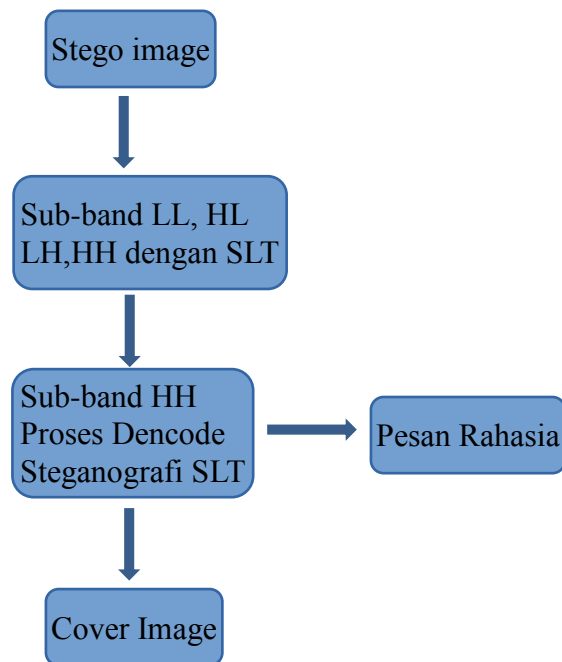
Metode steganografi yang pertama adalah SLT, dalam penerapannya, SLT membagi komponen sinyal ke dalam sub band horisontal dan vertikal rendah (LL), horisontal rendah dan vertikal tinggi (LH), horisontal tinggi dan vertikal rendah (HL) dan horisontal dan vertikal tinggi (HH).



Gambar 3. 2 Perancangan Algoritma SLT

Pada gambar diatas dijelaskan alur proses pada algoritma SLT dimana pada pesan yang akan disisipkan akan di *convert* ke bentuk *binary stream* kemudian baru dilakukan penyisipan pesan. Pada proses penyisipan pesan, *Cover image* akan diuraikan menjadi empat sub-band LL, HL, LH dan HH, kemudian Sub band LL akan digunakan untuk menyisipkan pesan. Kemudian sub band akan dikembalikan atau proses invers SLT sehingga menghasilkan stego image.

Tahapan selanjutnya yaitu proses ekstraksi, proses ekstraksi pesan yang ada didalam citra steganografi akan dilakakn melalui tahapan berikut:



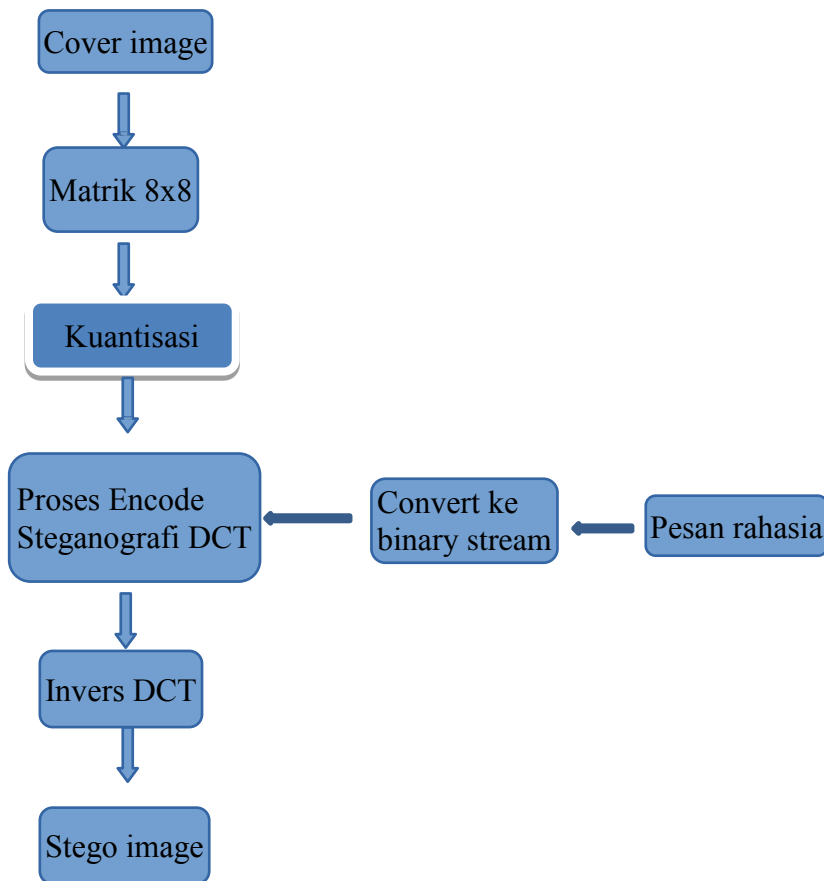
*Gambar 3. 3 Proses Ekstraksi menggunakan algoritma SLT*

Proses ekstraksi pada algoritma SLT dilakukan dengan tahapan yang pertama yaitu itra setganografi akan diuraikan menggunakan algoritma SLT untuk mendapatkan sub band LL, HL, HH dan LH kemudian pilih sub band LL kemudian ekstrak bit pesan selanjutnya bit pesan yang dihasilkan digabungkan dan selanjutnya diubah kedalam bentuk pesan semula.



### 3.2.2 Steganografi DCT

Metode steganografi selanjutnya adalah steganografi DCT, metode steganografi DCT dilakukan transformasi yang mengubah suatu sinyal menjadi unsur komponen frekuensi dasar.

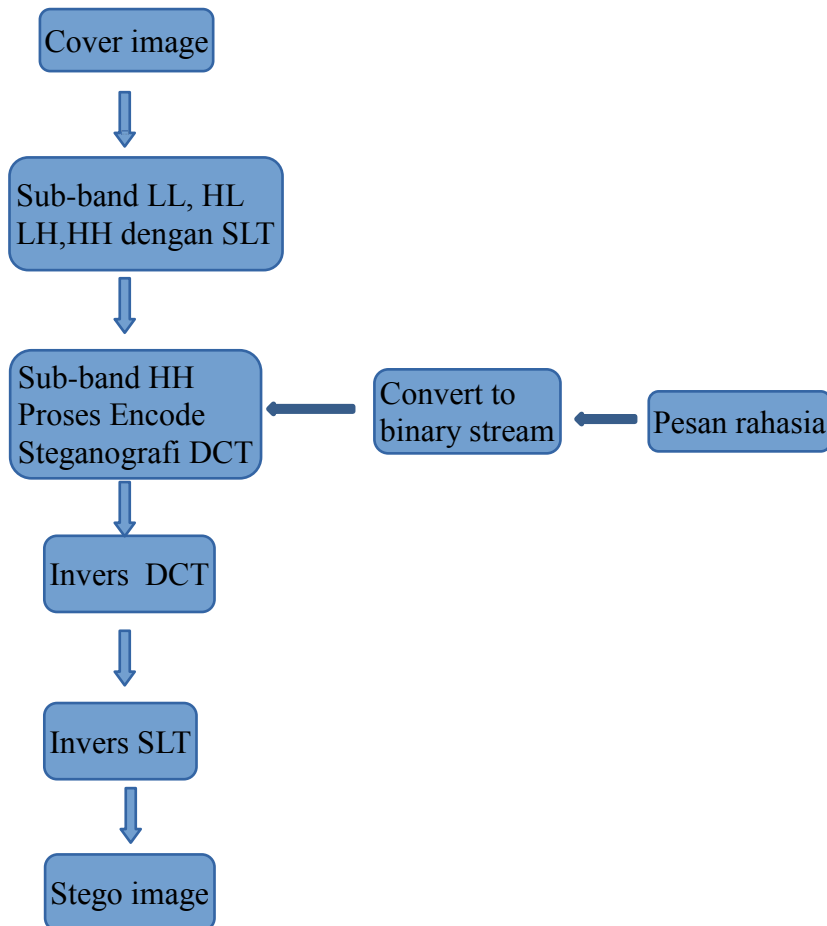


Gambar 3. 4 Perancangan Algoritma DCT

Pada proses penyembunyian pesan hal pertama yang dilakukan adalah merubah media menjadi matrik 8x8 dengan dilanjutkan proses kuantisasi , dari hasil tersebut didapatkan perubahan frekuensi yang memiliki nilai tinggi dari kiri atas sampai bawah dengan ukuran sama. Dari bentuk itulah penyisipan pesan dapat dilakukan pada bagian frekuensi yang memiliki nilai 0 dan 1. sedangkan pada pesan yang akan disisipkan akan di ubah dulu ke bentuk binary stream kemudian baru dilakukan penyisipan pesan.

### 3.2.3 Steganografi SLT-DCT

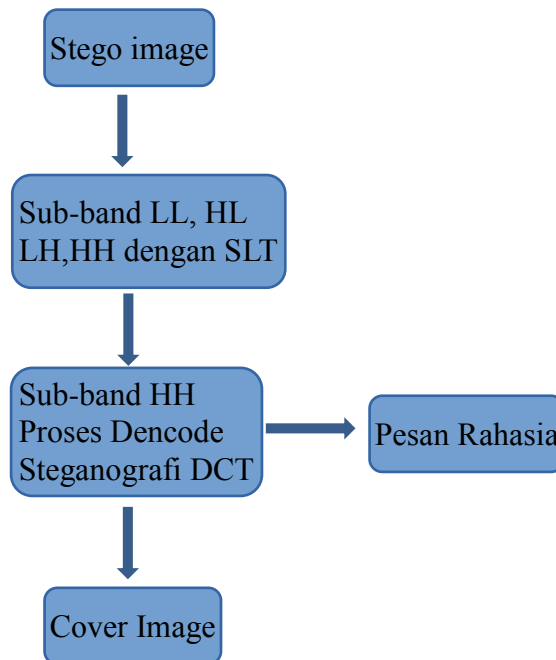
Metode steganografi selanjutnya yaitu metode gabungan algoritma SLT dan DCT, algoritma SLT disini berperan dalam menguraikan *Cover image* menjadi subband LL,LH,HL dan HH, selanjutnya untuk proses embeddingnya menggunakan algoritma DCT pada Sub band tinggi yaitu HH.



Gambar 3. 5 Perancangan Algoritma SLT-DCT

Pada proses penyisipan steganografi SLT-DCT, hal pertama yang dilakukan yaitu menerapkan algoritma SLT pada cover image untuk menguraikannya menjadi empat sub band: LL, HL, LH dan HH. Selanjutnya Terapkan DCT pada sub-band (HH) sehingga didapatkan koefisien DCT, kemudian lakukan penyisipan bit pesan pada koefisien DCT, setelah itu lakukan invers DCT lalu invers SLT sehingga menghasilkan citra stego.

Tahapan selanjutnya yaitu proses ekstraksi, proses ekstraksi pesan yang ada didalam citra steganografi akan dilakakn melalui tahapan berikut:



Gambar 3. 6 Perancangan Proses Ekstraksi Steganografi SLT-DCT.

Proses ekstraksi pada algoritma SLT-DCT dilakukan dengan tahapan yang pertama yaitu itra setganografi akan diuraikan menggunakan algoritma SLT untuk mendapatkan sub band LL, HL, HH dan LH Kemudian terapkan algoritma DCT ke setiap blok di sub-band yang dipilih (HH), dan ekstrak koefisien blok DCT Kemudian bit pesan yang dihasilkan digabungkan dan selanjutnya diubah kedalam bentuk pesan semula.

### 3.3 Parameter Pengujian

Secara umum, pengukuran kualitas citra yang sudah disisipi pesan melalui teknik steganografi tertentu (sering disebut sebagai stego-image) dapat dilakukan melalui 3 (tiga) aspek (Munir, 2004) yaitu:

#### 3.3.1 Parameter *Imperceptibility*

Pengujian terhadap aspek Kualitas (*Imperceptibility*) citra hasil steganografi dapat dilakukan dengan beberapa metode. Salah satu metode yang paling banyak digunakan adalah dengan mengukur nilai MSE (Mean Square Error) dan PSNR (Peak Signal to Noise Ratio). Keduanya merupakan sebuah nilai yang memiliki satuan dB (desibels). Semakin rendah nilai MSE maka kualitas citra semakin baik. Sementara itu, mutu stego-image dikatakan baik jika nilai PSNR 40 dB atau lebih.

### **3.3.2 Parameter Kapasitas Pesan**

Pengujian kapasitas bertujuan untuk mengetahui daya tampung sebuah *cover image*. Proses pengukuran kapasitas pesan dapat dilakukan dengan menghitung jumlah karakter yang berhasil disisipkan pada *cover image*, dan ukuran pesan yang akan digunakan berupa bits.

### **3.3.3 Parameter Ketahanan Citra**

Proses pengukuran ketahanan citra dilakukan dengan cara memanipulasi data citra pada *Stego Image* sehingga tahap proses uji tersebut dapat membuktikan bahwa pesan yang terkandung dalam *Stego Image* dapat diekstraksi sehingga pesan tersebut didapatkan secara utuh atau proses tersebut mengalami kegagalan.

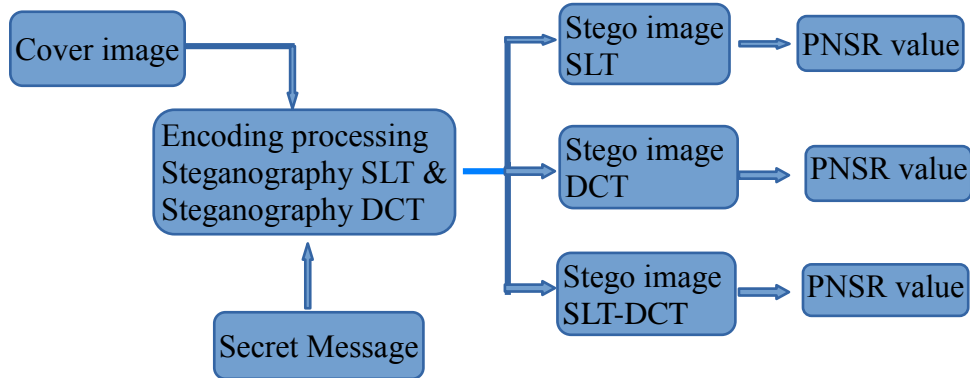
## **3.4 Data yang Digunakan**

Data yang digunakan pada penelitian ini adalah file citra digital gambar yang diambil dari situs <http://sipi.usc.edu/database/database.php>, database laboratorium SIPI (*Signal and Image Processing Institute*) USC (*University of Southern California*). USC-SIPI merupakan koleksi gambar digital untuk mendukung penelitian pengolahan gambar dan analisis citra. Pada penelitian ini jenis citra yang digunakan yaitu *color image*, dengan format tiff (\*.tiff) dan ukuran citra yang bersifat square yaitu panjang dan lebar citra sama, yaitu 256x256, 512x512 dan 1024x1024 piksel. Sedangkan file pesan rahasia yang akan digunakan berupa file dengan format text (\*.txt).

### 3.5 Rancangan Pengujian Sistem

#### 3.5.1 Pengujian Kualitas Citra stego

Pengujian kualitas citra dilakukan dengan membandingkan nilai PSNR dari citra stego yang belum dan yang sudah diberi efek contrast stretching dan histogram equalization.

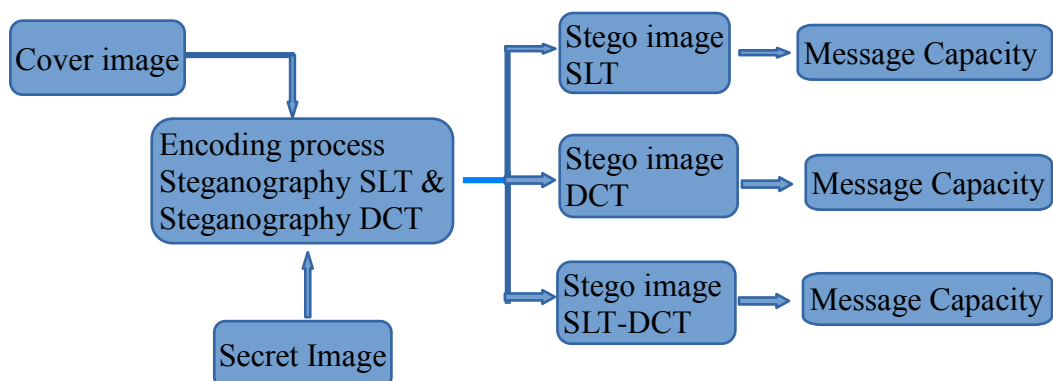


Gambar 3. 7 Perancangan pengujian kualitas citra

Dari gambar diatas dijelaskan alur proses pengujian kapasitas pesan, *cover image* akan disisipi pesan menggunakan steganografi SLT dan DCT, lalu akan menghasilkan *stego image* yang kemudian akan dihitung nilai PSNR dari masing-masing *stego image* tersebut.

#### 3.5.2 Pengujian Kapasitas Pesan

Pengujian kapasitas pesan dilakukan dengan menghitung jumlah kapasitas maximum pesan yang dapat disisipi pada *cover image*, penghitungan dilakukan pada algoritma SLT, DCT dan SLT-DCT

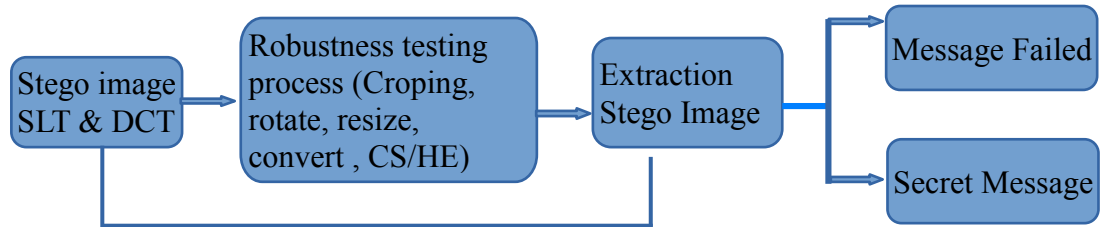


Gambar 3. 8 Perancangan pengujian kapasitas pesan

Dari gambar diatas dijelaskan alur proses pengujian kapasitas pesan, *cover image* akan disisipi pesan menggunakan steganografi SLT , DCT dan SLT-DCT, lalu akan menghasilkan *stego image* yang kemudian akan dihitung kapasitas maximum pesan dari masing-masing *stego image* tersebut.

### 3.5.3 Pengujian Ketahanan citra steganografi

Pengujian Ketahanan citra dilakukan dengan cara memanipulasi data citra pada Stego Image sehingga prose uji ketahanan akan membuktikan bahwa pesan yang ada pada Stego Image berhasil diektraks atau tidak.



Gambar 3. 9 Perancangan pengujian ketahanan citra

Dari gambar diatas dijelaskan alur proses pengujian ketahanan citra, dimana *stego image* hasil steganografi SLT dan DCT akan dilakukan manipulasi data citra seperti :

a. Cropping

Cropping merupakan proses menghilangkan sebagian image yang ada sehingga nilai parameter-parameter dari LSB yang ada menjadi berubah atau termodifikasi menyebabkan konten digital yang didalamnya mengalami kerusakan stuktur.

b. Rotate (Rotasi)

Rotate (Rotasi) adalah suatu proses untuk mengubah posisi gambar sesuai dengan derajat kemiringan yang akan ditentukan. Proses ini menimbulkan kerusakan pada konten digital didalamnya.

c. Resize

Resize merupakan proses merubah luas bidang image menjadi lebih besar atau lebih kecil dari ukuran aslinya, dalam hal ini dengan mengubah ukuran dapat mengakibatkan pergeseran nilai warna dan LSB yang ada sehingga dengan berubahnya nilai parameter tersebut juga mengubah konten digital yang ada didalamnya.

d. Convert (konversi)

Convert (konversi) adalah proses perubahan data dari format tif ke PNG maupun sebaliknya. Pada proses tersebut jika dilakukan maka dapat mengakibatkan perubahan parameter nilai warna yang terkandung pada gambar karena adanya proses kompresi.

e. Contrast Stretching

Contrast stretching (peregangan kontras) salah satunya dengan cara Memindai (scan) histogram dari nilai keabuan terkecil ke nilai keabuan terbesar (0 sampai 255) untuk menemukan batas nilai keabuan terendah dan batas nilai keabuan tertinggi dari kelompok piksel (citra).

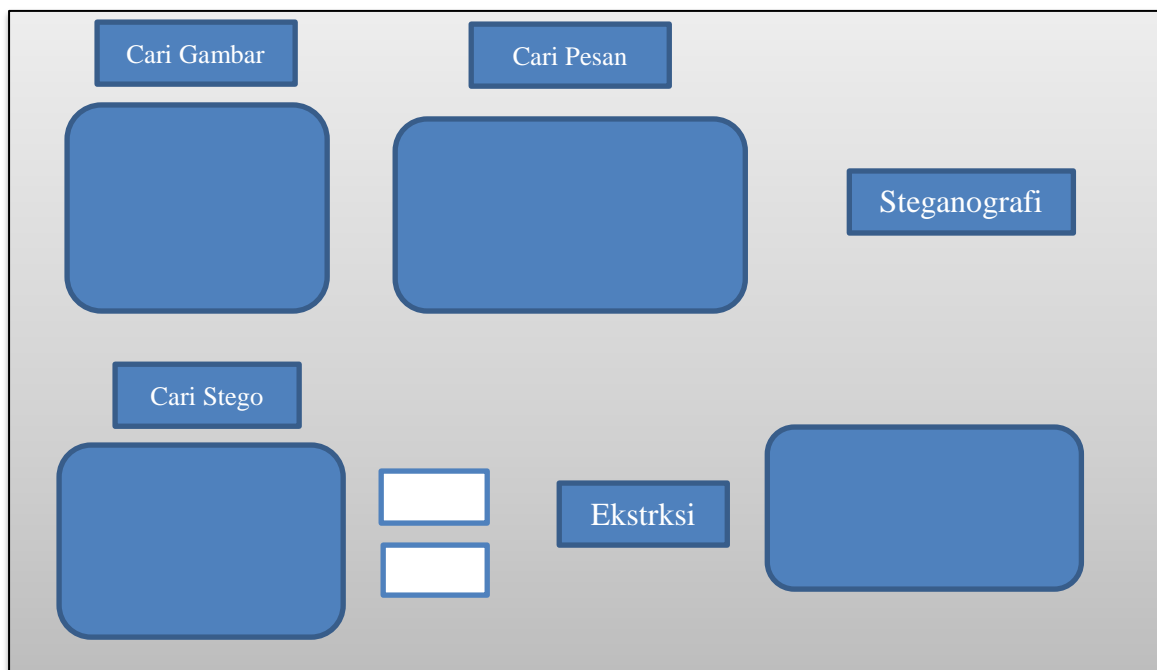
f. Histogram Equalization

Histogram equalization (perataan histogram) bertujuan untuk mendistribusikan histogram secara merata, sehingga setiap nilai keabuan memiliki jumlah piksel yang relatif sama.

### 3.6 Rancangan Hasil Analisa

#### 3.6.1 Rancangan Tampilan

Rancangan antarmuka pengguna adalah tahap akhir dari proses pembuatan suatu aplikasi, Berikut rancangan tampilan aplikasi steganografi SLT-DCT yang akan dibuat, aplikasi dibuat menggunakan Matlab R2018a.



Gambar 3. 10 Rancangan Tampilan Aplikasi

Gambar diatas merupakan rancangan tampilan aplikasi Steganografi SLT-DCT, dimana terdapat 5 tombol penting yaitu Cari Gambar yang berfungsi untuk mengambil gambar yang akan dijadikan sebagai Cover Image, Cari Pesan yang digunakan untuk mengambil pesan yang akan disisipkan, kemudian tombol Steganografi untuk melakukan proses penyisipan menggunakan algoritma SLT-DCT. Kemudian tombol Cari Stego

berfungsi untuk mencari citra steganografi yang telah disimpan dan yang terakhir yaitu tombol ekstraksi digunakan untuk melakukan proses ekstraksi dari citra steganografi yang telah dipilih.

### 3.6.2 Rancangan hasil analisa kualitas citra

Rancangan hasil analisa kualitas citra dimana kualitas ditentukan oleh nilai PSNR dan MSE dari masing-masing citra steganografi.

*Tabel 3. 1 Rancangan hasil analisa kualitas citra*

Nama Citra	PSNR(Db)			MSE		
	SLT	DCT	SLT-DCT	SLT	DCT	SLT-DCT
Citra 1						
Citra 2						
Citra 3						

Dari tabel diatas akan diketahui perbandingan nilai PNSR dan MSE pada steganografi SLT, DCT dan SLT-DCT.

### 3.6.3 Hasil analisa kapasitas pesan

Rancangan hasil analisa kapasitas pesan dari masing-masing citra berdasarkan penyisipan dari masing-masing algoritma.

*Tabel 3. 2 Hasil kapasitas pesan pada steganografi SLT, DCT, SLT-DCT*

Citra	SLT	DCT	SLT-DCT
Citra 1			
Citra 2			
Citra 3			

Dari tabel diatas akan diketahui kapasitas maksimal dari masing-masing citra berdasarkan penyisipan masing-masing algoritma yaitu algoritma SLT, algoritma DCT dan algoritma SLT-DCT.



### 3.6.4 Hasil analisa ketahanan stego image

#### a. Ketahanan citra pada Steganografi SLT

Tabel 3. 3 Rancangan Hasil analisa Ketahanan citra steganografi SLT

Uji Proses	Proses Restore	Proses Ekstraksi	Keterangan
Croping			
Rotate			
Resize			
Convert			
CS			
HE			

#### b. Ketahanan citra pada Steganografi DCT

Tabel 3. 4 Rancangan Hasil analisa Ketahanan citra steganografi DCT

Uji Proses	Proses Restore	Proses Ekstraksi	Keterangan
Croping			
Rotate			
Resize			
Convert			
CS			
HE			

#### c. Ketahanan citra pada Steganografi SLT-DCT

Tabel 3. 5 Rancangan Hasil analisa Ketahanan citra steganografi SLT dan DCT

Uji Proses	Proses Restore	Proses Ekstraksi	Keterangan
Croping			
Rotate			
Resize			
Convert			
CS			
HE			

Dari pengujian ketahanan citra akan didapatkan hasil uji proses mana yang masih bisa diekstraksi dan pesan tersebut dapat dikembalikan secara utuh atau tidak.

## **BAB IV**

### **Hasil dan Pembahasan**

#### **4.1 Implementasi system**

Pada tahap ini akan dilakukan implementasi system yaitu pembuatan aplikasi gabungan steganografi SLT dan DCT menggunakan Matlab versi R2018a. Hasil yang diharapkan berupa sebuah aplikasi steganografi menggunakan gabungan algoritma SLT dan DCT yang memiliki hasil citra steganografi dengan kualitas yang baik serta memiliki *imperceptibility* yang tinggi. Implementasi dan proses analisa pada penelitian ini menggunakan computer dengan spesifikasi hardware dan software sebagai berikut.

1. Processor Intel(R) Core (TM) i5-5200U CPU@ 2.20GHz 2.20GHz
2. RAM 4 GB;
3. System Type 64-bit Windows 7 Ultimate
4. Hardisk 500 GB
5. Matlab R2018a

##### **4.1.1 Steganografi SLT**

###### **a. Proses Penyisipan**

Pada proses penyisipan dengan menggunakan algoritma SLT, cover image akan diuraikan menjadi 4 subband yaitu LL,HL,LH,HH, dan kemudian akan dipilih subband LL sebagai lokasi penyisipan,  $l(x,y)$  adalah koefisien data gambar yang akan dimodifikasi,  $\alpha$  adalah faktor *embedding strength*, pada proses penyisipan bit menggunakan algoritma :

1. Jika bit sama dengan “1” maka koefisien  $l(x,y)$  sama dengan koefisien  $l(x,y)$  ditambah dengan  $\alpha$ .
2. Jika bit sama dengan “0” maka koefisien  $l(x,y)$  sama dengan koefisien  $l(x,y)$  dikurangi dengan  $\alpha$ .

Setelah algoritma tersebut dijalankan, kemudian koefisien tersebut dikembalikan ke semula dengan invers SLT.

###### **b. Proses Ekstraksi**

Proses ekstraksi dilakukan dengan cara melihat jika koefisien  $l(x,y)$  lebih dari “0” maka bit pesan sama dengan “1”, jika koefisien  $l(x,y)$  kurang dari “0” maka bit pesan sama dengan “0”. Kemudian bit pesan yang dihasilkan digabungkan dan selanjutnya diubah kedalam bentuk pesan semula.

### 4.1.2 Steganografi DCT

#### a. Proses penyisipan

Algoritma steganografi yang digunakan adalah algoritma DCT, pesan yang disisipkan adalah pesan yang telah diubah kedalam bentuk biner, proses penyisipan menggunakan perbedaan nilai piksel ( $c_1$ ) dan ( $c_2$ ) pada tiap blok citra, program akan terlebih dahulu membaca satu blok dan mengalihragamkannya dengan DCT, selanjutnya berdasarkan bit pesan digunakan algoritma berikut:

1. Untuk bit pesan "0", apabila nilai pada lokasi piksel ( $c_1 > c_2$ ) lebih besar maka kedua piksel ditukar.
2. Untuk bit pesan "1", apabila nilai pada lokasi piksel ( $c_1 < c_2$ ) lebih kecil maka kedua piksel ditukar.

Setelah algoritma tersebut dijalankan, kemudian blok tersebut dikembalikan ke semula dengan invers DCT.

#### b. Proses ekstraksi

Proses ekstraksi pesan hampir mirip dengan proses penyisipan pesan yaitu tiap blok di alihragamkan dengan DCT, tetapi pada proses ekstraksi hanya memeriksa yang lebih besar antara nilai piksel ( $c_1$ ) dan ( $c_2$ ), hal ini untuk menentukan nilai bit 0 dan 1, seperti pada algoritma dibawah ini :

1. Bila nilai piksel ( $c_1 < c_2$ ) maka bit pesan diwakili adalah "0"
2. Bila nilai piksel ( $c_1 > c_2$ ) maka bit pesan diwakili adalah "1"

Kemudian bit pesan yang dihasilkan digabungkan dan selanjutnya diubah kedalam bentuk pesan semula.

### 4.1.3 Steganografi SLT-DCT

#### a. Proses Penyisipan

Pada proses penyisipan steganografi SLT-DCT, hal pertama yang dilakukan yaitu terapkan algoritma SLT pada cover image untuk menguraikannya menjadi empat sub band: LL, HL, LH dan HH.

```
[ll, lh, hl hh] = slantlt(im, Lo_D, Hi_D);
```

*Im* merupakan cover image yang akan diuraikan menggunakan algoritma SLT (*slantlt*), dan proses *Lo\_D* dan *Hi\_D* yang dilakukan terhadap baris dan terhadap kolom. Setelah proses penguraian cover image menjadi empat subband, selanjutnya terapkan DCT pada sub-band (HH) sehingga didapatkan koefisien DCT.

```
hh = steg_encode_dct(secret_msg_bin, hh, frequency_coefficients, persistence);
```

```

block = dct2(carrier(posx, posy));
c1 = block(s1x, s1y);
c2 = block(s2x, s2y);

```

Kemudian lakukan penyisipan dengan algoritma :

1. Untuk bit pesan “0”, apabila nilai pada lokasi piksel ( $c1 < c2$ ) lebih besar maka kedua piksel ditukar.
2. Untuk bit pesan “1”, apabila nilai pada lokasi piksel ( $c1 > c2$ ) lebih besar maka kedua piksel ditukar.

```

if (secret_bit == 0)
    if (c1 > c2)
        % swap
        t = c1;
        c1 = c2;
        c2 = t;
    end
else
    if (c1 < c2)
        % swap
        t = c1;
        c1 = c2;
        c2 = t;
    end
end

```

Setelah algoritma tersebut dijalankan, kemudian blok tersebut dikembalikan ke semula dengan invers DCT,

```

stego(posx, posy) = idct2(block);

```

kemudian yang terakhir lakukan invres SLT (ISLT) sehingga menghasilkan stego image.

```

im_stego = islantlt(ll, lh, hl, hh, Lo_R, Hi_R);

```

## b. Proses Ekstraksi

Pada proses ekstraksi terapkan SLT untuk menguraikan gambar stego menjadi empat sub-band: LL, HL, LH dan HH.

```

[ll,hl,lh,hh] = slantlt(im, mode);

```

Kemudian terapkan DCT ke setiap blok di sub-band yang dipilih (HH),

```

extracted_msg_bin = steg_decode_dct(hh, frequency_coefficients);

```

selanjutnya ekstrak koefisien blok DCT Kemudian bit pesan yang dihasilkan digabungkan dan selanjutnya diubah kedalam bentuk pesan semula.

```

block = dct2(stego(posx, posy));
c1 = block(s1x, s1y);
c2 = block(s2x, s2y);
if (c1 > c2)
    stego_bin(stego_bin_i) = 1;
else
    stego_bin(stego_bin_i) = 0;
end

```

```

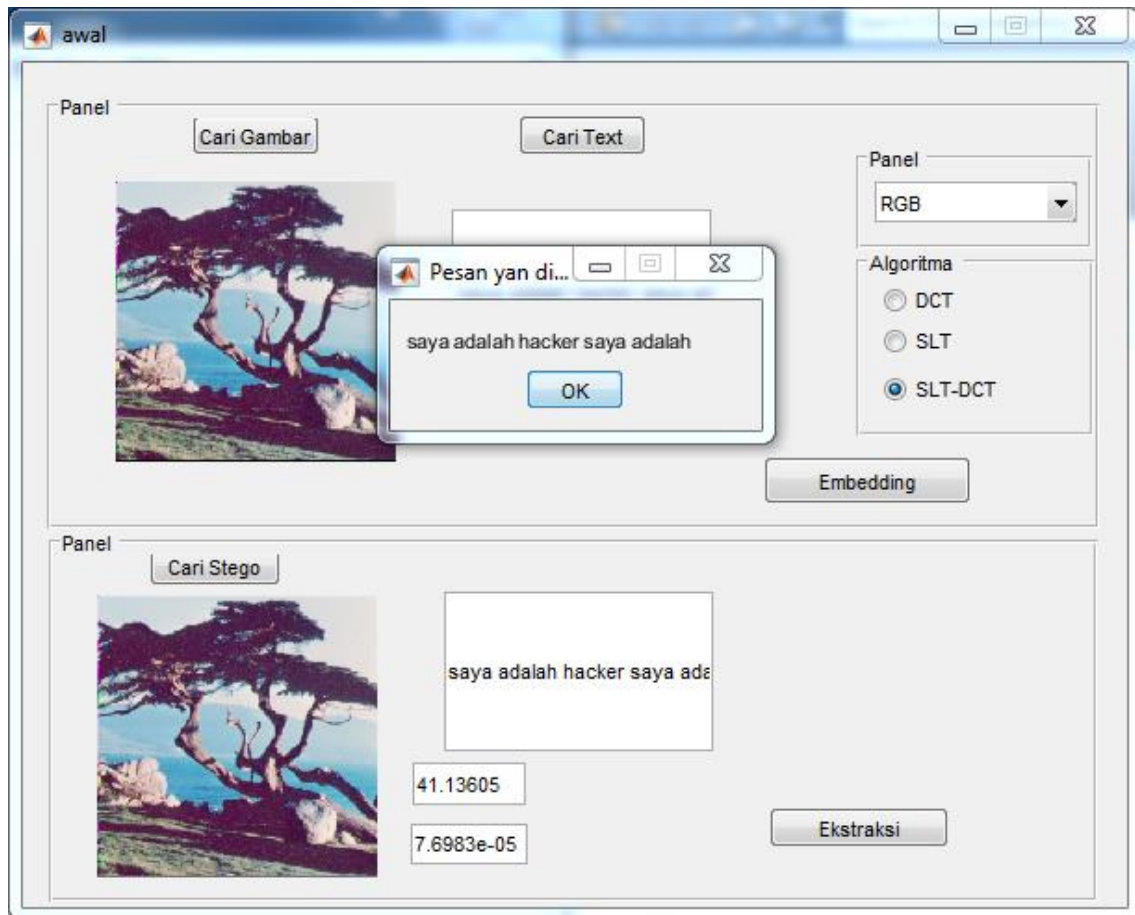
secret = stego_bin;

```

Sehingga didapatkan pesan yang sama seperti yang telah disisipkan sebelumnya.

#### 4.2 Tampilan GUI Aplikasi teanografi SLT-DCT

Grafical User Interface (GUI) merupakan tampilan yang berfungsi sebagai penghubung pengguna dengan aplikasi sehingga pengguna dapat menjalankan aplikasi steganografi SLT-DCT, berikut adalah tampilan aplikasi steganografi SLT-DCT.






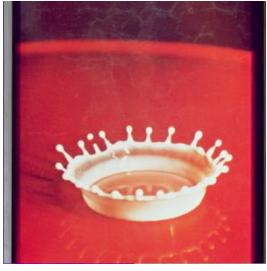

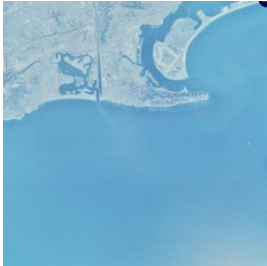
*Gambar 4. 1 Tampilan Aplikasi*

Gambar diatas adalah tampilan dari aplikasi steganografi SLT-DCT yang telah berhasil melakukan proses steganografi dan berhasil mengekstraksi pesan yang ada dalam citra steganografi. Terdapat 5 tombol penting yaitu Cari Gambar yang berfungsi untuk mengambil gambar yang akan dijadikan sebagai Cover Image, Cari Pesan yang digunakan untuk mengambil pesan yang akan disisipkan, kemudian tombol Steganografi untuk melakukan proses penyisipan menggunakan algoritma SLT-DCT. Kemudian tombol Cari Stego berfungsi untuk mencari citra steganografi yang telah disimpan dan yang terakhir yaitu tombol ekstraksi digunakan untuk melakukakn proses ekstraksi dari citra steganografi yang telah dipilih

#### 4.2.1 Contoh Gambar

Gambar yang digunakan dalam penelitian ini adalah jenis gambar yaitu *Color Image (RGB)*. Database dibagi menjadi beberapa volume berdasarkan karakter dasar gambar. Gambar dalam setiap volume memiliki berbagai ukuran seperti 256x256 piksel, 512x512 piksel, atau 1024x1024 piksel. Sehingga didapatkan Sample untuk *Cover Image* yaitu *Tree* dan *Female* dengan resolusi gambar sebesar 256x256 piksel, serta ukuran file sebesar 193 kb dan *Airplane(F-16)* dan *Splash* dengan resolusi gambar sebesar 512x512 piksel, serta ukuran file sebesar 769 kb dan *San Diego* yang mempunyai resolusi 1024x1024 piksel dengan ukuran file sebesar 3 Mb.

Tabel 4. 1 tabel Contoh Gambar

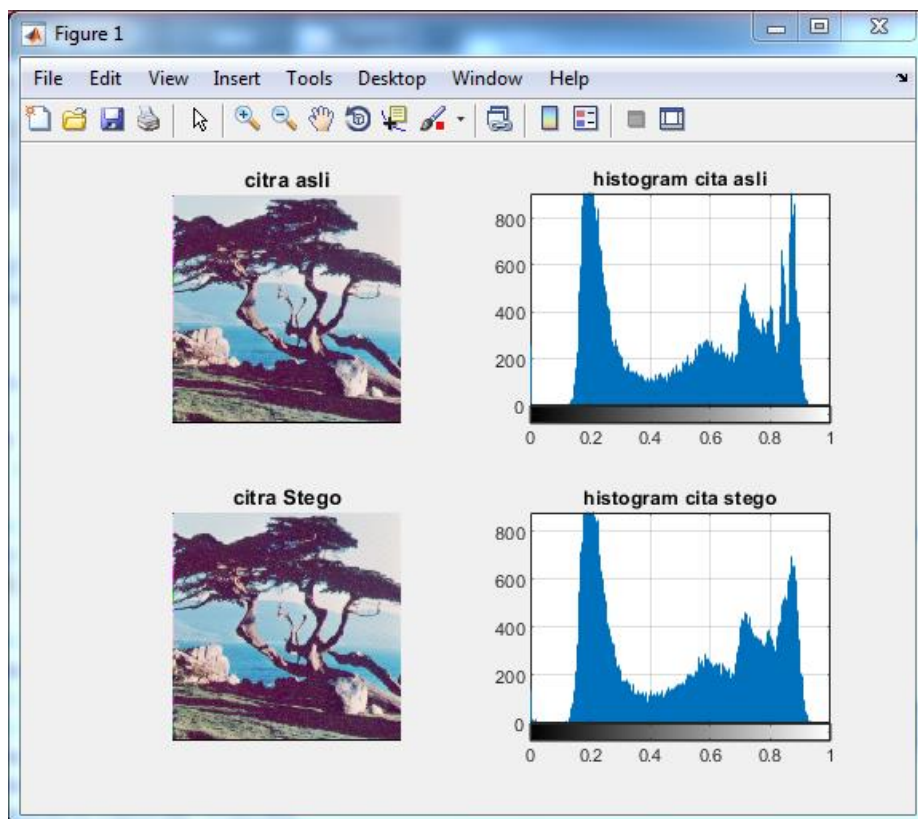
Ukuran	Ukuran (Bytes)	Gambar	
256x256	196,748 bytes	Tree	Female
			
512x512	786,572 bytes	Airplane	Splash
			
1024x1024 4	3,145,868 bytes	San Diego	San Diego
			

### 4.3 Analisis Output

Informasi penting tentang isi gambar digital dapat dilihat dengan membuat histogram gambar. Histogram juga dapat menunjukkan banyak informasi tentang kecerahan dan kontras gambar, histogram dapat mengubah gambar RGB menjadi grayscale. Oleh karena itu, histogram adalah alat yang berharga dalam pengolahan gambar baik secara kualitatif dan kuantitatif (Riadi, Fadhil, & Sari, 2017). Proses analisis output yang telah dihasilkan dari aplikasi Steganografi SLT, DCT dan SLT-DCT sebagai berikut :

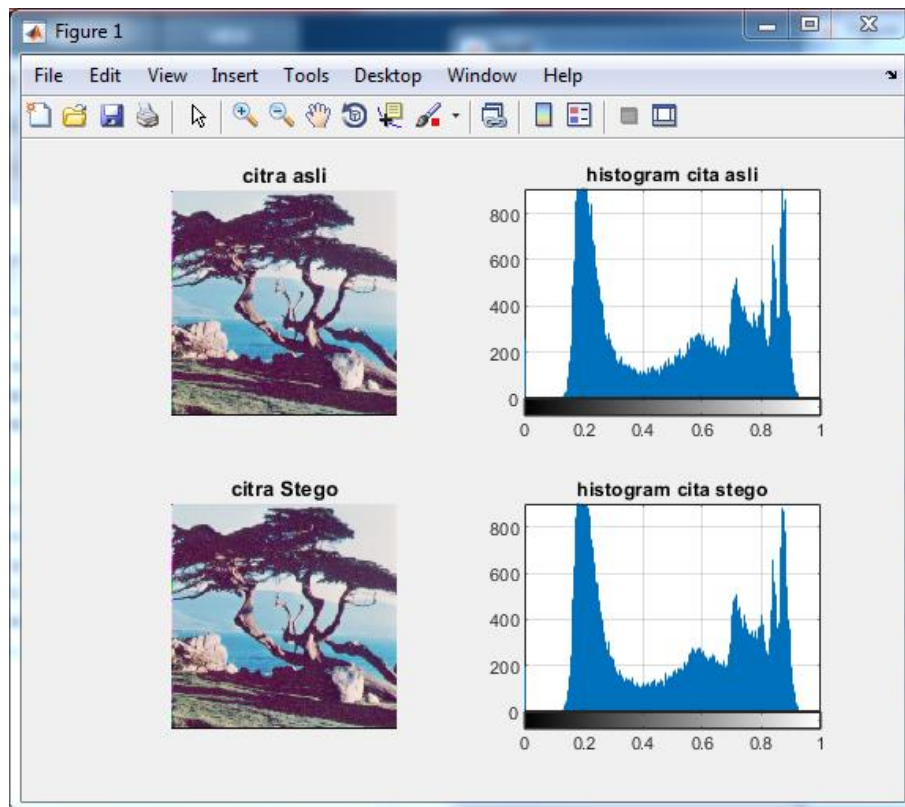
a. Algoritma SLT dan SLT-DCT

Hasil output histogram dari steganografi SLT dan SLT-DCT dengan ukuran pesan yang sama yaitu 30 karakter pada citra Tree, sebagai berikut :



*Gambar 4. 2 Perbandingan Hasil pada Algoritma SLT*

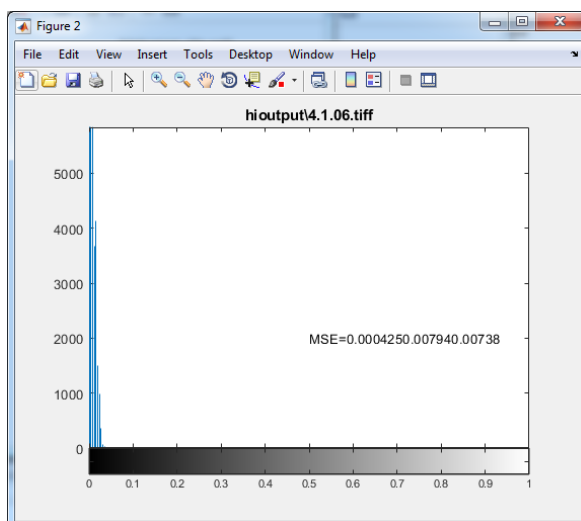
Gambar diatas menunjukkan perbandingan hasil histogram citra asli dan citra steganografi SLT, dapat dilihat perbedaan histogram antara citra asli dan citra steganografi, secara kasat mata tidak terlihat jelas perbedaan citra asli dan citra steganografi akan tetapi pada histogram terlihat ada perbedaan antara histogram citra asli dan histogram citra steganografi.



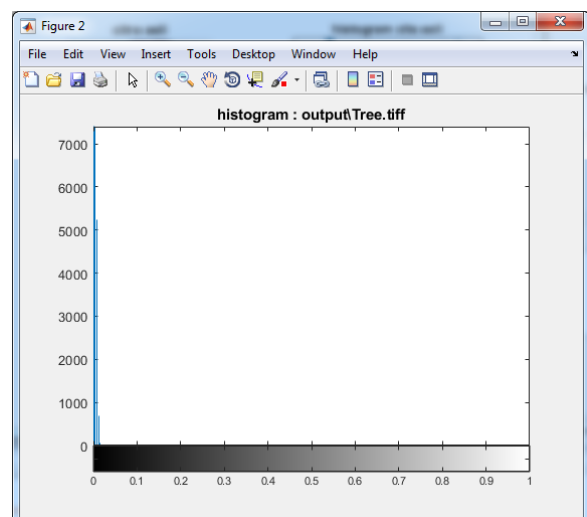
*Gambar 4. 3 Perbandingan hasil pada Algoritma SLT-DCT*

Sama halnya dengan gambar 4.4, gambar 4.5 juga menunjukkan perbandingan hasil histogram citra asli dan citra steganografi SLT, dapat dilihat perbedaan histogram antara citra asli dan citra steganografi SLT-DCT.

Perbandingan histogram error pada citra Tree pada algoritma SLT dan SLT-DCT sebagai berikut:



*Gambar 4. 4 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT*



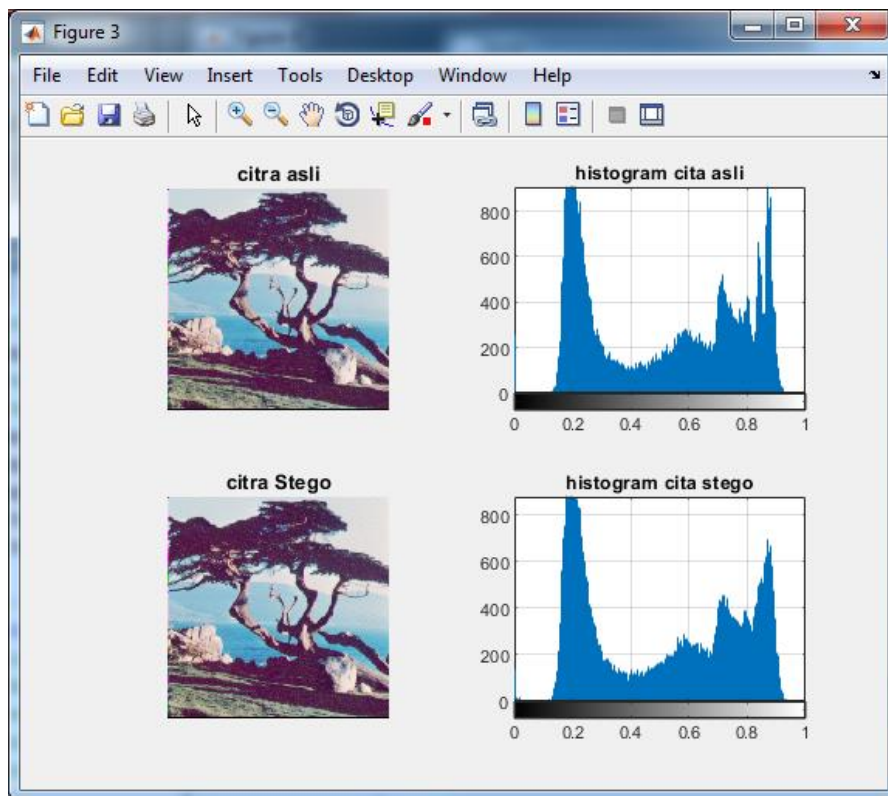
*Gambar 4. 5 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT-DCT*



Gambar diatas menunjukkan hasil perbedaan histogram citra tree menggunakan algoritma SLT dan SLT-DCT. Dari gambar diatas terlihat jelas perbedaan histogram antara Steganografi menggunakan algoritma SLT dan steganografi menggunakan algoritma SLT-DCT, histogram error yang dihasilkan algoritma SLT-DCT lebih sedikit dibandingkan algoritma SLT yang berarti perbedaan antara citra asli dan citra steganografi lebih sedikit pula.

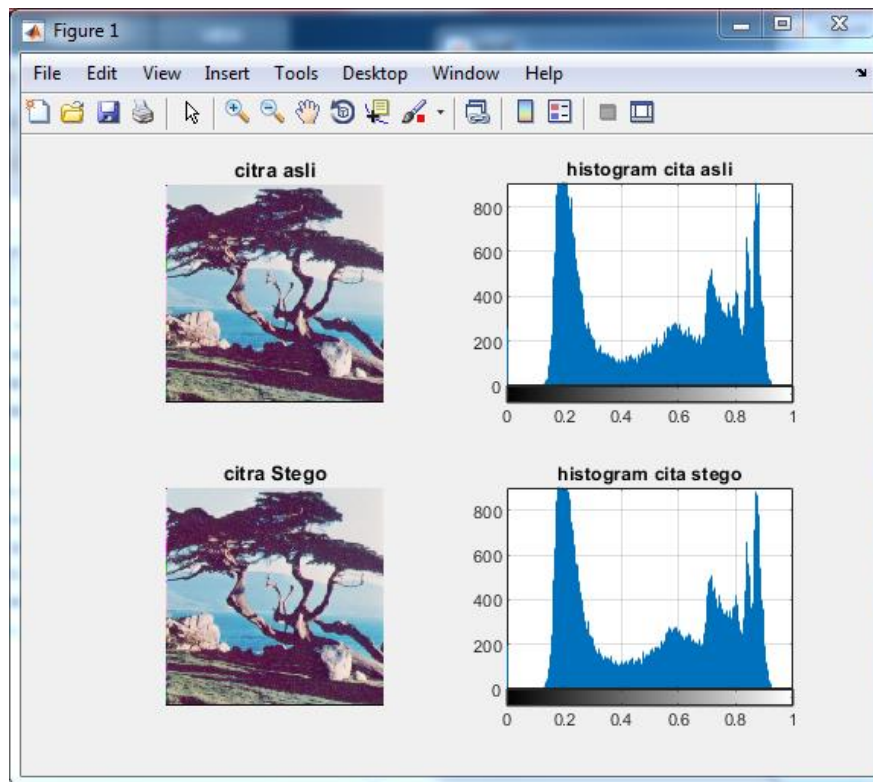
b. Algoritma DCT dan SLT-DCT

Hasil output histogram dari steganografi DCT dan steganografi SLT-DCT dengan ukuran pesan yang sama yaitu 30 karakter pada citra Tree, sebagai berikut :



*Gambar 4. 6 Perbandingan hasil penyisipan pesan menggunakan Algoritma DCT*

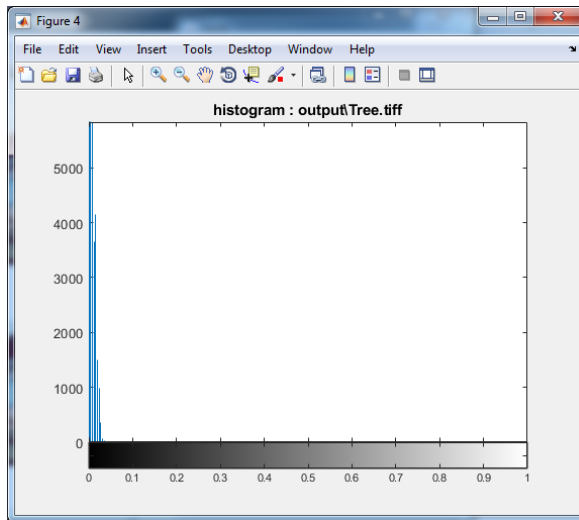
Gambar diatas menunjukkan perbandingan hasil histogram citra asli dan citra steganografi DCT, dapat dilihat perbedaan histogram antara citra asli dan citra steganografi, secara kasat mata tidak terlihat jelas perbedaan citra asli dan citra steganografi akan tetapi pada histogram terlihat ada perbedaan antara histogram citra asli dan histogram citra steganografi.



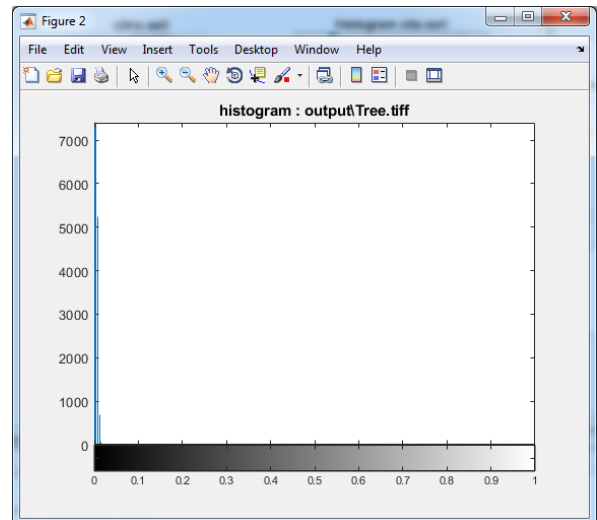
*Gambar 4. 7 Perbandingan hasil penyisipan menggunakan Algoritma SLT-DCT*

Gambar diatas menunjukkan perbandingan hasil histogram citra asli dan citra steganografi SLT-DCT, dapat dilihat perbedaan histogram antara citra asli dan citra steganografi, secara kasat mata tidak terlihat jelas perbedaan citra asli dan citra steganografi akan tetapi pada histogram terlihat ada perbedaan antara histogram citra asli dan histogram citra steganografi walaupun sangat sedikit.

Perbandingan histogram error pada citra Tree pada steganografi menggunakan algoritma DCT dan algoritma SLT-DCT sebagai berikut:



*Gambar 4. 8 Histogram perbedaan citra pada Tree menggunakan Algoritma DCT*








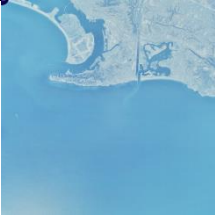
*Gambar 4. 9 Histogram perbedaan citra pada Tree menggunakan Algoritma SLT-DCT*

Gambar diatas menunjukkan hasil perbandingan histogram citra tree menggunakan algoritma SLT dan SLT-DCT. Dari gambar diatas terlihat jelas perbedaan histogram antara Steganografi menggunakan algoritma DCT dan steganografi menggunakan algoritma SLT-DCT, histogram error yang dihasilkan algoritma SLT-DCT lebih sedikit dibandingkan algoritma DCT yang berarti perbedaan antara citra asli dan citra steganografi lebih sedikit pula.

#### 4.4 Hasil Pengujian

Pengujian terhadap aplikasi steganografi SLT-DCT berdasarkan system yang telah dibuat, pengujian ini bertujuan untuk mengetahui tingkat keberhasilan system.

Tabel 4. 2 Pengujian Keberhasilan System

Cover Image	Secret Message	Citra Steganografi	Hasil Ekstraksi
Tree	30 karakter		Berhasil
Female	30 karakter		Berhasil
Airplane	30 karakter		Berhasil
Splash	30 karakter		Berhasil
San Diego 1	30 karakter		Berhasil
San Diego 2	30 karakter		Berhasil

Dari table diatas dapat dilihat dari semua sampel yang telah diuji, pesan yang telah disisipkan berhasil dikembalikan atau diekstraksi.

#### 4.4.1 Pengujian Kualitas Image

Penentuan kualitas citra steganografi ditentukan berdasarkan table berikut (Imamah, 2015):

Tabel 4. 3 Kualitas Citra Steganografi berdasarkan PSNR

Nilai PSNR	Keterangan
<20	Memuaskan, tingkat degradasi tidak dapat diterima dan hampir tidak terlihat oleh kasat mata
$\geq 20$ dan $\leq 40$	Diterima kasat mata, kualitas gambar yang baik direkonstruksi
>40	Selalu terlihat kasat mata, kualitas gambar yang baik, dan dapat menutupi sebagian besar serangan

##### A. Pengujian Kualitas Citra Steganografi

Pengujian kualitas citra steganografi dapat ditentukan dengan beberapa metode, salah satu metode yang paling banyak digunakan adalah dengan mengukur nilai MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*). Kualitas citra steganografi dikatakan baik jika nilai PSNR 40 dB atau lebih (Cheddad, 2010).

Tabel 4. 4 Nilai PSNR dan MSE algoritma SLT-DCT

Ukuran	Gambar	PSNR	MSE
256x256	Tree	41.13605	0.0007698
	Female	42.63572	0.00054504
512x512	Airplane	42.6226	0,00054669
	Splash	42.83999	0.00052005
1024x1024	San Diego	40.75013	0,00084140
	San Diego	41.25671	0.00074874

Dari table diatas terdapat 3 kelompok gambar berdasarkan ukuran diantaranya 256x256, 512x512 dan 1024x1024 piksel merupakan ukuran standar dalam penelitian tentang *image* analisis. Dari setiap ukuran diambil dua gambar sebagai sampel dalam menerapkan algoritma SLT-DCT. Berdasarkan nilai PSNR didapatkan, Rata-rata nilai PSNR diatas 40 db yang berarti citra steganografi yang dihasilkan oleh aplikasi steganografi SLT-DCT sangat baik.

## B. Pengujian Pengaruh Besarnya Citra Cover

Dari hasil pengujian yang telah dilakukan perbandingan kualitas citra yang disisipi pesan 30 karakter dan pesan maksimum yang dapat ditampung oleh masing-masing citra cover dengan ukuran 256x256, 512x512, dan 1024x1024 menggunakan algoritma SLT-DCT.

*Tabel 4. 5 Perbandingan nilai PSNR dan MSE berdasarkan Ukuran Pesan*

Cover Image	Ukuran pesan	PSNR	MSE
Tree(256x256)	30 karakter	41.13605	0.0007698
	32 karakter	41.13472	0.00077007
Airplane(512x512)	30 karakter	42.6226	0,00054669
	128 karakter	42.61077	0,0005481
San	30 karakter	40.75013	0,0008414
Diego(1024x1024)	512 karakter	40.74333	0,00084269

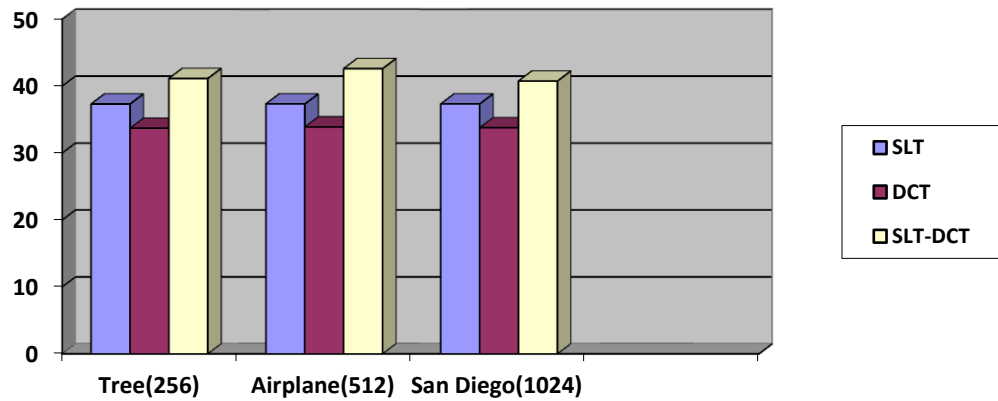
Dari tabel diatas dapat dilihat nilai PSNR dan MSE dari masing-masing citra cover yang telah diuji cobakan, citra cover Tree disisipi pesan 30 karakter memiliki nilai PSNR 41.13605 db dengan nilai MSE sebesar 0.0007698, dan disisipi pesan 32 karakter memiliki nilai PSNR sebesar 41.13472 db dengan nilai MSE sebesar 0.00077007, nilai MSE mengalami peningkatan dan menghasil nilai PSNR mengalami penurunan, pada citra Airplane disisipi pesan 30 karakter memiliki nilai PSNR sebesar 42.6226 db dengan nilai MSE sebesar 0.00054669, dan di sisipi pesan 128 karakter memiliki nilai PSNR sebesar 42.61077 db dengan nilai MSE sebesar 0,0005481, pada citra San Diego disisipi pesan 30 karakter memiliki nilai PSNR sebesar 40.75013 db dengan nilai MSE sebesar 0.0008414, dan di sisipi pesan 512 karakter memiliki nilai PSNR sebesar 40.74333 db dengan nilai MSE sebesar 0.00084269, dari hasil yang telah didapat dari masing-masing citra cover, dapat diambil kesimpulan semakin banyak jumlah karakter pesan yang disisipkan, maka nilai MSE mengalami peningkatan nilai error yang menyebabkan nilai PSNR menjadi semakin rendah.

Hasil pengujian selanjutnya yaitu perbandingan nilai PSNR pada citra cover yang disisipi pesan pada algoritma SLT, DCT dan SLT-DCT, citra cover yang disisipi memiliki ukuran 256x256, 512x512 dan 1024x1024 dengan jumlah karakter yang disisipi adalah 30 karakter.

*Tabel 4. 6 Hasil perbandingan kualitas citra yang disisipi pesan 30 karakter*

Ukuran Cover image	Algoritma	PSNR(db)	MSE
Tree(256x256)	SLT	37,3313	0,0001849
	DCT	33,7112	0,0004254
	SLT-DCT	41.13605	0.0007698
Airplane(512x512)	SLT	37,3392	0.00018454
	DCT	33,9062	0.00040689
	SLT-DCT	42.61077	0,0005481
San Diego (1024x1024)	SLT	37,3392	0.00018454
	DCT	33,7955	0,0004173
	SLT-DCT	40.75013	0,0008414

Dari tabel diatas diketahui perbandingan nilai PNSR dan MSE dengan citra format tiff yaitu citra Tree yang mempunyai resolusi 256x256 piksel, Airplane dengan resolusi 512x512 piksel, dan citra San Diego dengan resolusi 1024x1024 piksel yang telah disisipkan pesan sejumlah 30 karakter, pada citra Tree, nilai PSNR citra steganografi pada algoritma SLT yaitu 37,3313 db, pada algoritma DCT yaitu 33,7112 dan pada algoritma SLT-DCT yaitu 41.13605 db, sehingga PNSR tertinggi dari setiap citra steganografi terlihat pada penyisipan menggunakan Algoritma SLT-DCT yaitu sebesar 41.13605 db. pada citra Airplane, nilai PSNR citra steganografi pada algoritma SLT yaitu 37,3392 db, pada algoritma DCT yaitu 33,9062 db dan pada algoritma SLT-DCT yaitu 42.61077db, sehingga PNSR tertinggi dari setiap citra steganografi terlihat pada penyisipan menggunakan Algoritma SLT-DCT yaitu sebesar 42.61077, dan pada citra San Diego, nilai PSNR citra steganografi pada algoritma SLT yaitu 37,3392 db, pada algoritma DCT yaitu 33,7955 db dan pada algoritma SLT-DCT yaitu 40.75013 db, sehingga PNSR tertinggi dari setiap citra steganografi terlihat pada penyisipan menggunakan Algoritma SLT-DCT yaitu sebesar 40.75013 db.



Gambar 4. 10 Grafik Perbandingan nilai PSNR dengan jumlah pesan yang sama

Dari grafik diatas dapat dilihat nilai PNSR dari masing-masing algoritma diatas 30 db dan nilai PSNR tertinggi pada setiap citra yang disisipkan menggunakan algoritma SLT-DCT dengan nilai PNSR > 40 db. Apabila nilai PSNR jatuh dibawah 30 dB, mengindikasikan kualitas citra relatif rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas. Akan tetapi kualitas image stego yang tinggi berada pada nilai 40 dB dan diatasnya (Cheddad, 2010).

#### C. Pengujian Pengaruh Besarnya Citra Cover pada pesan karakter maksimal

Pada pengujian ini system diuji dengan menyisipkan jumlah karakter pesan yang berbeda-beda yaitu karakter maksimal yang dapat ditampung masing-masing cover image seperti Tree 256x256, Airplane 512x512 dan San Diego 1024x1024 menggunakan algoritma SLT, DCT dan SLT-DCT untuk mengetahui pengaruh nilai PSNR dan MSE pada stego image.

Tabel 4. 7 Perbandingan nilai PSNR dan MSE berdasarkan ukuran cover image

Ukuran Cover image	Algoritma	Karakter maksimal	PSNR	MSE
Tree(256x256)	SLT	2048 karakter	37.2584	0.0001880
	DCT	128 karakter	33.8337	0.00041365
	SLT-DCT	32 karakter	41.13472	0.00077007
Airplane(512x512)	SLT	8192 karakter	37.3390	0.00018454
	DCT	512 karakter	33.9053	0.00040689
	SLT-DCT	128 karakter	42.6226	0,00054669
San Diego (1024x1024)	SLT	32.768 karakter	37.3390	0.00018454
	DCT	2048 karakter	33.7710	0.00041966
	SLT-DCT	512 karakter	40.74333	0,00084269



Dari table diatas dapat dilihat pada algoritma SLT, penyisipan karakter yang dengan jumlah 2024 pada cover image tree 256x256 memiliki nilai MSE yaitu 0.0001880 dan nilai PSNR adalah 37.2584 db, dan karakter yang dengan jumlah 8192 pada cover image Airplane 512x512 memiliki nilai MSE=0.00018454 dan nilai PSNR=37.3390, hal ini menunjukkan semakin besar cover image maka nilai MSE semakin kecil dan nilai PSNR semakin besar, pada algoritma DCT penyisipan karakter yang dengan jumlah 128 karakter pada cover image tree 256x256 memiliki nilai MSE yaitu 0.00041365 dan nilai PSNR adalah 33.8337 db, dan karakter yang dengan jumlah 512 pada cover image Airplane 512x512 memiliki nilai MSE=0.00040689 dan nilai PSNR=33.9053 db dan pada algoritma SLT-DCT penyisipan karakter yang dengan jumlah 32 karakter pada cover image tree 256x256 memiliki nilai MSE yaitu 0.00077007 dan nilai PSNR adalah 41.13472 db, dan karakter yang dengan jumlah 128 pada cover image Airplane 512x512 memiliki nilai MSE=0,00054669 dan nilai PSNR=42.6226 db, untuk cover image San Diego 1024x1024 yang disisipi karakter maksimal mengalami peningkatan nilai MSE yang berarti nilai PSNR menurun.

#### **4.4.2 Pengujian kapasitas pesan**

Pada steganografi SLT, pengujian kapasitas pesan dilakukan dengan cara membagi piksel-piksel citra kedalam blok 2x2, kemudian hasil bit yang didapatkan dibagi 8, sehingga didapatkan jumlah karakter maksimum dari sebuah citra.

Pada steganografi DCT, pengujian kapasitas dilakukan dengan cara menghitung nilai kapasitas maksimal dari sebuah citra, hal tersebut dilakukan dengan cara membagi piksel-piksel citra kedalam blok 8x8, kemudian hasil bit yang didapatkan dibagi 8, sehingga didapatkan jumlah karakter maksimum yang dapat ditampung oleh sebuah citra.

Pada steganografi SLT-DCT, pengujian kapasitas pesan dilakukan dengan membagi piksel-piksel citra dedalam blok 2x2, kemudian dibagi ke dalam blok 8x8 dan hasil bit yang didapatkan dibagi 8 sehingga didapatkan jumlah karakter maksimum yang dapat ditampung oleh sebuah citra.

Tabel 4. 8 Hasil kapasitas pesan pada steganografi SLT, DCT, SLT-DCT







Citra	Ukuran	SLT	DCT	SLT-DCT
Tree	256x256	2048 karakter	128 karakter	32 karakter
Airplane	512x512	8192 karakter	512 karakter	128 karakter
San Diego	1024x1024	32.768 karakter	2048 karakter	512 karakter

Dari table diatas diketahui algoritma SLT memiliki kapasitas penyimpanan pesan pada citra tree dengan ukuran 256x256 sebanyak 2048 karakter, algoritma DCT sebanyak 128 karakter dan algoritma SLT-DCT sebanyak 32 karakter. Pada citra Airplane dengan ukuran 512x512, penyisipan menggunakan algoritma SLT dapat menyimpan sebanyak 8192 karakter, algoritma DCT sebanyak 512 karakter dan algoritma SLT-DCT sebanyak 128 karakter. Pada citra San Diego dengan ukuran 1024x1024, penyisipan menggunakan algoritma SLT dapat menyimpan pesan sebanyak 32.768 karakter, algoritma DCT sebanyak 2048 karakter dan algoritma SLT-DCT sebanyak 512 karakter. Dari table tersebut dapat dilihat kapasitas penyimpanan pesan terbanyak pada setiap citra adalah penyisipan menggunakan algoritma SLT dan kapasitas terendah pada algoritma SLT-DCT.

#### 4.4.3 Pengujian Ketahanan Stego Image

Pengujian ketahanan stego image dilakukan dengan manipulasi data pada citra, seperti *cropping* yaitu menghilangkan sebagian data citra, *Rotasi* yaitu memutar arah citra, *Resize* yaitu merubah ukuran citra, *convert* yaitu merubah format citra, *CS* yaitu melakukan *contrast stretching* pada citra dan yang terakhir yaitu menambahkan Histogram pada citra. Berikut akan dijelaskan hasil analisa ketahanan citra steganografi SLT-DCT dengan contoh data yaitu Tree dengan ukuran citra asli yaitu 196,748 bytes dengan format file yaitu tiff.







Tabel 4. 9 Ketahanan Citra Steganografi SLT-DCT pada Tree

Uji Proses	Gambar	Ukuran (byte)	Proses Ekstraksi	Keterangan
Cropi Ng		122,534 bytes	Gagal	Menghilangkan bagian citra yang lain
Rotate		194,058 bytes	Gagal	Memutar citra kearah 180 derajat
Resize		49,742 bytes	Gagal	Rezise 256x256 piksel menjadi 128x128 piksel
Convert		136,711 bytes	Berhasil	Merubah format dari tiff ke PNG
CS		197,708 bytes	Berhasil	Menambahkan contrast stratching pada citra
HE		197,686 bytes	Berhasil	Menambahkan histogram pada citra

Dari table diatas dapat dilihat dari enam percobaan manipulasi yang dilakukan, hanya 3 percobaan yang tidak merusak pesan yaitu perubahan format ke bentuk PNG, penambahan Contrast stretching dan histogram.

Berikut akan dijelaskan hasil analisa ketahanan citra steganografi SLT-DCT dengan contoh data yaitu Airplane dengan ukuran citra asli yaitu 786,572 bytes dengan format file yaitu tiff .







*Tabel 4. 10 Ketahanan Citra Steganografi SLT-DCT pada Airpalne*

Uji Proses	Gambar	Ukuran (byte)	Proses Ekstraksi	Keterangan
Cropping		122,534 bytes	Gagal	Menghilangkan bagian citra yang lain
Rotate		617,194 bytes	Gagal	Memutar citra kearah 180 derajat
Resize		198,584 bytes	Gagal	Rezise 256x256 piksel menjadi 128x128 piksel
Convert		15,998 bytes	Berhasil	Merubah format dari tiff ke PNG
CS		793,404 bytes	Berhasil	Menambahkan contrast strtching pada citra
HE		793,092 bytes	Berhasil	Menambahkan histogram pada citra

Dari table diatas dapat dilihat dari enam percobaan manipulasi yang dilakukan, hanya 3 percobaan yang tidak merusak pesan yaitu perubahan format ke bentuk PNG, penambahan Contrast stretching dan histogram.

Berikut akan dijelaskan hasil analisa ketahanan citra steganografi SLT-DCT dengan contoh data yaitu Airplane dengan ukuran citra asli yaitu 786,572 bytes dengan format file yaitu tiff .

Tabel 4. 11 Ketahanan Citra Steganografi SLT-DCT pada San Diego

Uji Proses	Gambar	Ukuran (byte)	Proses Ekstraksi	Keterangan
Cropping		122,534 bytes	Gagal	Menghilangkan bagian citra yang lain
Rotate		2,976,520 bytes	Gagal	Memutar citra kearah 180 derajat
Resize		793,294 bytes	Gagal	Rezise 256x256 piksel menjadi 128x128 piksel
Convert		2,194,723 bytes	Berhasil	Merubah format dari tiff ke PNG
CS		3,171,052 bytes	Berhasil	Menambahkan contrast stratching pada citra
HE		3,170,032 bytes	Berhasil	Menambahkan histogram pada citra

Kemudian ketahanan citra steganografi SLT-DCT akan dibandingkan dengan algoritma lain yaitu algoritma SLT dan algoritma DCT.

Tabel 4. 12 Perbandingan Ketahanan Citra Steganografi SLT, DCT, dan SLT-DCT

Uji Proses	Ukuran (byte)	Proses Ekstraksi SLT	Proses Ekstraksi DCT	Proses Ekstraksi SLT-DCT	Keterangan
<b>Cropping</b>	122,534 bytes	Gagal	Gagal	Gagal	Menghilangkan bagian citra yang lain
<b>Rotate</b>	617,194 bytes	Gagal	Gagal	Gagal	Memutar arah citra dari 0 derajat ke 180 derajat
<b>Resize</b>	198,584 bytes	Gagal	Gagal	Gagal	Rezise 256x256 piksel menjadi 128x128 piksel
<b>Convert</b>	15,998 bytes	Gagal	Berhasil	Berhasil	Merubah format dari tiff ke PNG
<b>CS</b>	793,404 bytes	Gagal	Berhasil	Berhasil	Menambahkan contrast stratching pada citra
<b>HE</b>	793,092 bytes	Gagal	Berhasil	Berhasil	Menambahkan histogram pada citra

Dari table diatas dapat dilihat dari enam percobaan manipulasi yang dilakukan, pada citra steganografi SLT semua serangan atau manipulasi data citra yang dilakukan dapat merusak pesan yang ada didalam citra steganografi sehingga pesan yang ada di dalam citra tersebut tidak bisa dikembalikan ke bentuk aslinya, sedangkan uji proses pada citra steganografi DCT, dari 6 uji proses terdapat 3 uji proses yang berhasil atau citra steganografi tahan terhadap 3 serangan diantaranya yaitu proses *Convert*, penambahan *Contrast Stretching*, dan *Histogram Equalization*. Sedangkan uji proses pada citra steganografi SLT-DCT sama dengan steganografi DCT mampu menahan 3 serangan yaitu *Convert*, *Contrast Stretching* dan *Histogram Equalization*.

#### 4.4.4 Analisa

Dari hasil percobaan yang telah dilakukan terhadap aplikasi steganografi SLT-DCT yang telah dibangun membuktikan bahwa steganografi SLT-DCT berjalan dengan baik, pesan yang telah disisipkan pada citra mampu dikembalikan atau diekstrak dalam bentuk semula dan aplikasi steganografi SLT-DCT mampu meningkatkan nilai PSNR dari citra steganografi jika dibandingkan dengan Steganografi SLT dan steganografi DCT dengan adanya peningkatan nilai PSNR tersebut, citra steganografi semakin sulit dibedakan dengan citra aslinya sehingga kemungkinan pesan yang ada di dalam citra steganografi tersebut semakin sulit diketahui keberadaannya dan nilai PSNR yang dihasilkan lebih dari 40 db membuktikan kualitas citra steganografi yang dihasilkan sangat baik, dengan nilai PSNR lebih dari 40 db, kualitas citra steganografi berada pada kategori bagus dan lebih tahan terhadap beberapa serangan, sehingga dari segi ketahanan steganografi SLT-DCT mampu menahan 3 serangan yang berarti ada peningkatan ketahanan citra. Serangan yang mampu di tahan yaitu :

1. Convert (konversi) adalah proses perubahan data dari format tif ke PNG maupun sebaliknya. Pada proses tersebut data yang ada dalam citra steganografi mampu dikembalikan karena format PNG adalah format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut.
2. Contrast Stretching adalah Memindai (scan) histogram dari nilai keabuan terkecil ke nilai keabuan terbesar (0 sampai 255) untuk menemukan batas nilai keabuan terendah dan batas nilai keabuan tertinggi dari kelompok piksel (citra). Pada proses tersebut data yang ada dalam citra steganografi mampu dikembalikan karena tidak menghilangkan bagian dari citra atau tidak merubah parameter dari LSB citra tersebut.
3. Histogram Equalization bertujuan untuk mendistribusikan histogram secara merata, sehingga setiap nilai keabuan memiliki jumlah piksel yang relatif sama. Pada proses tersebut data yang ada dalam citra steganografi mampu dikembalikan karena tidak menghilangkan bagian dari citra atau tidak merubah parameter dari LSB citra tersebut.

Proses yang mengalami kegagalan dalam proses ekstraksi yaitu

4. Cropping yaitu proses menghilangkan sebagian citra sehingga nilai parameter-parameter dari LSB yang ada dalam citra tersebut mengalami perubahan sehingga menyebabkan konten digital yang didalamnya mengalami kerusakan struktur.
5. Resize merupakan proses merubah ukuran citra menjadi lebih besar atau lebih kecil dari ukuran aslinya, dalam hal ini dengan mengubah ukuran dapat mengakibatkan pergeseran nilai warna dan LSB yang ada sehingga dengan nilai parameter tersebut membuat konten digital yang ada didalamnya mengalami perubahan juga.
6. Rotate (rotasi) adalah suatu proses untuk mengubah posisi gambar sesuai dengan derajat kemiringan yang akan ditentukan. Proses ini menimbulkan kerusakan pada konten digital didalamnya karena derajat kemiringannya 180 sehingga membuat posisi gambar berubah.

Akan tetapi aplikasi steganografi SLT-DCT memiliki kelemahan terkait masalah kapasitas pesan yang mampu ditampung oleh citra, kapasitas maksimal yang mampu ditampung untuk ukuran 256x256 hanya 32 karakter berbeda dengan steganografi SLT atau DCT yang mampu menampung kapasitas maksimum yang lebih besar yaitu 128 karakter untuk steganografi DCT, 2048 karakter untuk steganografi SLT.



## **BAB V**

### **Kesimpulan Dan Saran**

#### **A. Kesimpulan**

Dari hasil penelitian yang telah dilakukan dapat diambil kesimpulan :

1. Pengimplementasian metode steganografi SLT-DCT pada sebuah aplikasi dapat dilakukan dengan baik, aplikasi steganografi SLT-DCT yang telah dibangun dapat berjalan sesuai harapan dibuktikan dengan pesan yang telah disisipkan pada citra mampu dikembalikan atau diekstrak dalam bentuk semula.
2. Kualitas citra steganografi yang dihasilkan sangat baik, terbukti dengan nilai PSNR yang dihasilkan lebih tinggi dibandingkan dengan algoritma SLT dan DCT dan nilai PSNR yang didapat rata rata lebih dari 40 db. Dengan nilai PSNR yang tinggi maka perbedaan antara citra asli dan citra steganografi semakin sedikit sehingga keberadaan dari pesan yang ada pada citra steganografi semakin sulit untuk terlihat. Dari segi ketahanan citra, citra steganografi yang dihasilkan algoritma SLT-DCT tahan terhadap proses *convert*, penambahan contrast dan histogram, dan memiliki ketahanan yang sama dengan algoritma DCT yang mampu menahan 3 proses serangan yaitu perubahan format, penambahan contrast dan penambahan histogram, akan tetapi algoritma SLT tidak tahan terhadap serangan apapun yang telah diuji cobakan.

#### **B. Saran**

Saran untuk penelitian selanjutnya tentang *Image Analisis* yaitu

1. Untuk pengujian kualitas dapat dilakukan dengan beberapa metode, sehingga disarankan untuk penelitian kedepannya bisa melakukan percobaan pengujian kualitas citra steganografi dengan parameter pengujian yang berbeda.
2. Pada aplikasi steganografi SLT-DCT tersebut kapasitas maksimum pesan yang ditampung masih sedikit, sehingga disarankan mencoba menambahkan metode algoritma lainnya sehingga kapasitas maksimum yang dapat ditampung lebih banyak.

## Daftar Pustaka

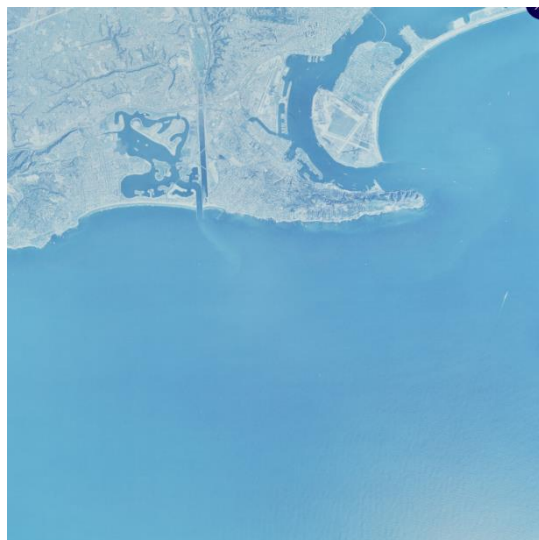
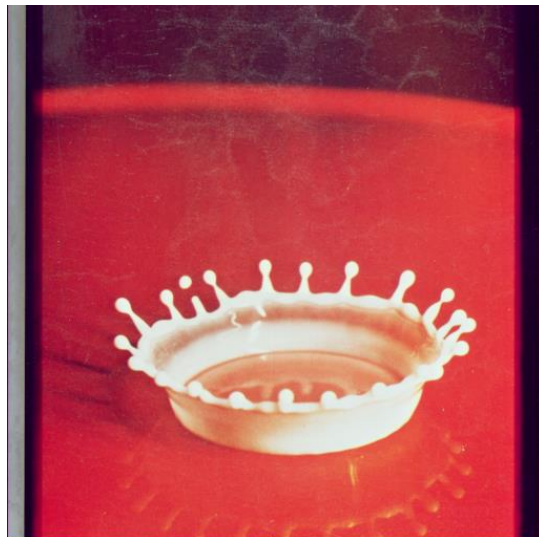
- Abduljabbar, R. B. (2016). Steganography System using Slantlet Transform. *Journal of Information, Communication, and Intelligence Systems (JICIS) Volume 2, Issue 1*, 1-6.
- Aji, I. B., & Wijanarto. (2015). Implementasi Metode Huffman Untuk Kompresi Citra Hasil Dari Steganografi Discrete Cosine Transform (Dct). *Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro*, 1-9.
- Bansal, D., & Chhikara, R. (2014). An Improved DCT based Steganography Technique. *International Journal of Computer Applications (0975 – 8887)*, Volume 102–No.14.
- Batarius, P., & Maslim, M. (2012). PERBANDINGAN METODE DALAM TEKNIK STEGANOGRAFI. *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)*.
- Challoob, I. H., & Mahmood, R. R. (2017). Suggested hybrid Transform Technique for image compression. *Journal Of Madent Alelem College Vol 9 No 2*, 15-27.
- Cheddad, A. (2010). Digital image steganography : Survey and analysisof. *Northern Ireland,UK:ELSEVIER*.
- Faruqi, A. A., & Rozi, I. F. (2015). Implementasi Steganography Menggunakan Algoritma DCT. *Teknik Informatika, Teknologi Informasi, Politeknik Negeri Malang ISSN: 2407-070X*, Volume 2, Edisi 1,.
- Garno, & Solehudin, A. (2017). Teknik Steganografi dengan Metode Discrete Cosines Transform (DCT) pada Citra Interpolasi Bilinear untuk Pengamanan Pesan. *INFORMATIKA UPGRIS Vol 3. No.2*, 116-121.
- Herlinawati. (2016). Steganografi Video H263 dengan Metode Discrete Cosine Transform. *Jurusan Teknik Elektro Universitas Lampung, Bandar Lampung*, Volume 10, No. 1.
- Imamah. (2015). Enkripsi Data Menggunakan Steganografi Untuk Keamanan Data Pada Cloud. *Jurnal Ilmiah NERO Vol. 1 No. 3*, 204-210=.
- Innuddun, M. (2016). *Hybrid Image Watermarking RDWT dengan SVD untuk Perlindungan Hak Cipta pada Citra Digital*. yogyakarta: Universitas Islam Indonesia.

- KUMAR, S., & dkk. (2013). A New Method In Image Steganography With Improved Image Quality. *International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 6*,.
- Kumar, S., & Muttou, S. K. (2013). A Reversible Image Steganographic Algorithm Based on Slantlet Transform. *BIJIT - BVICAM's International Journal of Information Technology*, 556-562.
- Kurniawan, B. (2013). Metode Contrast Stretching Kamera CMUcam3 dan Metode Histogram Equalization untuk Ground Station Payload Roket. *TELEKONTRAN, VOL. 1, NO. 1*, 1-7.
- Morkel, T., Eloff, J., & Oliver, M. (2005). An Overview Of Image Steganography. *Information and Computer Security Architecture (ICSA) Research Group*, Vol 2, No 3, June, pp.103-112.
- Munir, R. (2004). *Pengolahan Citra digital dengan Pendekatan Algoritmik*. Bandung: Informatika.
- Nithya, R., Ranjani, J. J., & Thenmozhi, T. (2013). The Image Steganography Techniques to Improve the Security and the Stego Image Quality. *International Journal of Latest Trends in Engineering and Technology (IJLTET) ISSN: 2278-621X*, Vol. 3 Issue2.
- NS, P. (2015). *Pemrograman Matlab*. Putra Ns.
- Pamungkas, A. (2012). *Contrast Stretching dan Histogram Equalization*. Adi Pamungkas.
- Prabowo, A., Hidayatno, A., & Christyono, Y. (2011). Penyembunyian Data Rahasia pada Citra Digital Berbasis Chaos dan Discrete Cosine Transform. *Transmisi vol. 13, no. 2*.
- Putri, A. R. (2016). Pengolahan Citra dengan Menggunakan Web CAM pada Kendaraan Bergerak Di Jalan Raya. *JUPI (Jurnal Ilmiah Pendidikan Informatika) Volume 1, Nomor 1*, 1-6.
- Rachmawanto, E. H., & Sari, C. A. (2014). Gabungan Slit-Dct Untuk Steganografi Pengamanan Data Gambar Penyakit. *Techno.COM, Vol. 13, No. 1*, 38-44.
- Riadi, I., Fadhil, A., & Sari, T. (2017). Image Forensic for detecting Splicing Image with Distance Function. *International Journal of Computer Applications (0975 – 8887) Volume 169 – No.5*.
- Shejul, A. A., & Kulkarni, U. (2010). A DWT based Approach for Steganography Using Biometrics. *International Conference on Data Storage and Data Engineering*.
- Solichin, A. (2015). *Mengukur Kualitas Citra Hasil Steganografi*. Achmatim.Net.

- Utama, J. (2012). Akuisisi Citra Digital Menggunakan Pemrograman Matlab. *Majalah Ilmiah UNIKOM Vol.9, No.1*, 71-80.
- vyas, K., & Pal, B. (2014). A Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique. *International Journal of Advanced Research in Computer and Communication Engineering*, ISSN (Online) : 2278-1021.
- Wijaya, E. S., & Prayudi, Y. (2015). Integrasi Metode Steganografi DCS Pada Image. *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*, ISSN: 1907 – 5022.
- Wijaya, M. C., & Prijono, A. (2007). *Pengolahan Citra Digital Menggunakan MatLAB Image Processing Toolbox*. Bandung: Informatika.
- Wirayasa, A. (2015). *Pengertian MSE dan PSNR pada Citra Digital dan Contoh Perhitungannya*. Ketutrare.com.
- Wissarto, R. (2014). Implementasi Slantlet Transform (SLT) Dan Huffman Coding Pada Steganografi Citra Grayscale. *Fakultas Ilmu Komputer, Universitas Dian Nuswantoro*.
- zulfikar, d. h., & harjoko, a. (2016). Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement. *IJCCS, Vol 10. NO 1*, 35-46.

LAMPIRAN

Cover Image





Citra Stganografi

