PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB

SKRIPSI

Disusun oleh:
VALERY NICOLAY
22105011

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2016

PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB

SKRIPSI

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh:
VALERY NICOLAY
22105011

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2016

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 2 Desember 2016

VALERY NICOLAY

22105011

HALAMAN PERSETUJUAN

Judul Skripsi	: Perbandingan Citra Hasil Steganografi Menggunakan Metode Dct Dan Lsb
Nama	: VALERY NICOLAY
NIM	: 22105011
Mata Kuliah	: Tugas Akhir
Kode	: TIW276
Semester	: Ganjil
Tahun Akademik	: 2016/2017

Telah diperiksa dan disetujui
di Yogyakarta,
Pada tanggal _____

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom., M.Cs.	Gani Indriyanta, Ir.M.T.

HALAMAN PENGESAHAN

PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB

Oleh : VALERY NICOLAY / 22105011

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal _____

Yogyakarta, 2 Desember 2016

Mengesahkan,

Dewan Penguji:

- Willy Sudiarto Raharjo, S.Kom.,M.Cs. _____
- Gani Indriyanta, Ir. M.T. _____
- Budi Susanto, S.Kom.,M.T. _____
- Restyandito, S.Kom.,MSIS, Ph.D. _____

Dekan

(_____)

Ketua Program Studi

(_____)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat– Nya sehingga penulis dapat menyelesaikan laporan Tugas Akhir dengan judul "*Perbandingan Citra Hasil Steganografi Menggunakan Metode DCT dan LSB*" dengan baik dan lancar. Penulisan laporan ini merupakan persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam usaha menyusun laporan Tugas Akhir ini, penulis telah mendapat banyak bantuan dan bimbingan yang tak ternilai dari berbagai pihak, baik berupa dukungan, saran dan kritik. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih yang setulus - tulusnya kepada :

- Tuhan Yang Maha Esa yang telah memberikan Rahmat – Nya sehingga penulis bisa menyelesaikan Laporan Tugas Akhir.
- Ibunda Ratnawati yang selalu mendorong penulis agar tidak patah semangat
- Bapak Willy Sudiarto Raharjo, S.Kom.,M.Cs. selaku Dosen Pembimbing I yang telah membimbing penulis dengan sabar dan bijaksana.
- Bapak Gani Indriyanta, Ir. M.T. selaku Dosen Pembimbing II yang telah membimbing penulis dengan sabar dan bijaksana.
- Bapak Budi Susanto, SKom.,M.T. dan Bapak Restyandito, S.Kom.,MSIS, Ph.D. selaku Dosen Penguji Skripsi yang telah menguji skripsi penulis dengan sabar dan bijaksana.
- Lidya Agnes Puspitasari, Cicilia Rini Astuti dan Ayu Rahmawati Windianingrum yang selalu memberikan dukungan semangat dan berjuang bersama selama masa pengerjaan Tugas Akhir.
- Teman – teman kost Parkit dan DoTA yang selalu ada untuk menghibur
- Serta semua pihak yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa dalam penyusunan Laporan Tugas Akhir ini masih banyak kekurangan yang harus diperbaiki. Penulis sangat mengharapkan saran dan kritik yang

membangun. Melalui laporan ini, penulis berharap menjadi tambahan wawasan dan pengetahuan yang berguna bagi pembaca.

Demikian laporan ini dibuat, mohon maaf yang setulus – tulusnya jika terdapat kata – kata yang tidak berkenan dalam penulisan laporan.

Yogyakarta, _____

Valery Nicolay

INTISARI

PERBANDINGAN CITRA HASIL STEGANOGRAFI MENGGUNAKAN METODE DCT DAN LSB

Pesatnya perkembangan teknologi, telah membuat banyak perkembangan di dalam kehidupan sehari – hari, seperti berkomunikasi, menyampaikan dan bertukar informasi telah menjadi semakin mudah. Mengirimkan pesan atau gambar yang dahulu dapat memakan waktu berhari – hari, sekarang dapat dengan mudah dilakukan kapan saja dan langsung sampai ketujuan. Melalui media digital, berkomunikasi menjadi semakin mudah karena tidak terkendala jarak dan waktu dan dapat dilakukan secara *real time*.

Permasalahan muncul ketika seseorang ingin mengirimkan suatu informasi yang bersifat rahasia, media digital yang banyak digunakan saat ini masih mempunyai beberapa kekurangan, sehingga informasi yang ingin dikirimkan rentan terhadap pencurian. Ada beberapa hal yang dapat digunakan untuk mengurangi resiko pencurian data, diantaranya adalah dengan menggunakan enkripsi terhadap informasi yang ingin dikirim. Salah satu teknik enkripsi yang digunakan adalah steganografi.

Dalam tugas akhir ini, peneliti akan membahas mengenai bagaimana suatu pesan disisipkan ke dalam pesan lainnya yaitu citra menggunakan metode *Discrete Cosine Transform (DCT), Least Significant Bit (LSB)* ,serta melakukan perbandingan pada kualitas citra yang dihasilkan pada setiap metode.

Dan dari hasil pengujian penulis menyadari bahwa tidak ada sistem yang sempurna. Oleh karena itu penulis mengembangkan aplikasi ini dengan tujuan agar setidaknya permasalahan pengiriman suatu data rahasia dapat lebih terjaga.

Kata Kunci: *Steganography, Discrete Cosine Transform* (DCT*), Least Significant bit* (LSB).

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Pesatnya perkembangan teknologi, telah membuat banyak perkembangan di dalam kehidupan sehari – hari, seperti berkomunikasi, menyampaikan dan bertukar informasi telah menjadi semakin mudah. Melalui media digital, berkomunikasi menjadi semakin mudah karena tidak terkendala jarak dan waktu dan dapat dilakukan secara *real time*. Tetapi permasalahan muncul ketika seseorang ingin mengirimkan suatu informasi yang bersifat rahasia, media digital yang banyak digunakan saat ini masih mempunyai beberapa kekurangan, sehingga informasi yang ingin dikirimkan rentan terhadap pencurian. Ada beberapa hal yang dapat digunakan untuk mengurangi resiko pencurian data, diantaranya adalah dengan menggunakan enkripsi terhadap informasi yang ingin dikirim. Salah satu teknik enkripsi yang digunakan adalah steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Teknik steganografi ini menyisipkan pada media lain (*cover object*) yang umum digunakan dalam kehidupan. Pesan yang dikirimkan melalui media yang telah disisipi pesan (*stego-object*) tidak akan mengundang kecurigaan orang lain, karena perbedaannya tidak dapat dilihat secara kasat mata. Media yang paling mudah dimanfaatkan untuk steganografi adalah berkas multimedia. Berkas yang sering dijumpai adalah citra digital.

Dalam tugas akhir ini, peneliti akan membahas mengenai bagaimana suatu pesan disisipkan kedalam citra lainnya yaitu citra menggunakan metode *Discrete Cosine Transform (DCT), Least Significant Bit (LSB)* ,serta melakukan perbandingan pada kualitas citra yang dihasilkan pada setiap metode.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka rumusan masalah penelitian ini adalah :

1. Bagaimana melakukan penyembunyian dan pengambilan pesan ke dalam citra digital dengan metode *DCT* dan *LSB*?
2. Bagaimana membandingkan kualitas atau ukuran file antara citra digital asli dengan citra digital yang sudah disisipkan pesan?

1.3. Batasan Masalah

Pada penelitian ini penulis membatasi permasalahan dalam ruang lingkup, sebagai berikut :

1. Penyembunyian pesan dilakukan pada citra digital berformat JPG, PNG, dan BMP.
2. Algoritma yang digunakan dalam metode DCT dan LSB.
3. Citra digital yang digunakan untuk pengujian adalah *true color*.
4. Aplikasi dibuat pada MATLAB
5. Data set image yang digunakan diambil dari https://testimages.org/

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan analisa citra steganografi melalui pengujian menggunakan metode DCT dan LSB pada format citra yang berbeda.

1.5. Metode Penelitian

1. Studi Literatur

   Pada metode studi literatur, dilakukan pencarian dan pemahaman literatur yang berhubungan dengan penelitian guna dibuatnya aplikasi. Literatur yang digunakan meliputi buku referensi dan dokumentasi internet.

2. Analisis data

   Pada metode ini penulis mempelajari lebih dalam tentang steganografi, dan metode yang digunakan pada penyembunyian pesan beserta teknik ekstraksinya.

3. Perencanaan dan perancangan

   Pada metode ini, dilakukan perencanaan kebutuhan guna proses perancangan aplikasi berdasarkan hasil analisis pada metode sebelumnya.

4. Implementasi

   Pada metode implementasi ini, aplikasi sudah dibuat secara keseluruhan pada aplikasi pendukung MATLAB. Aplikasi pada tahap ini sudah siap untuk dilakukan pengujian.

5. Pengujian

   Pada metode pengujian, aplikasi yang sudah selesai dibuat untuk kemudian diujikan guna mengetahui apakah aplikasi berjalan dengan lancar tanpa ada kekurangan dan kesalahan serta menganalisa hasil uji citra digital dengan acuan data yang diperoleh dan dengan menganalisa lebih dalam mengenai teknik steganografi dan algoritma yang digunakan.

1.6. Sistematika Penulisan

Untuk memudahkan penulisan, maka tugas akhir ini disajikan dalam lima bab yang berbeda dengan sistematika sebagai berikut:

1. Bab I: Pendahuluan

   Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, serta sistematika penulisan.

2. Bab II: Landasan Teori

   Di dalam bab ini akan ditulis mengenai uraian dari teori-teori yang digunakan untuk mendukung pembuatan tugas akhir ini.

3. Bab III: Analisis dan Perancangan Sistem

   Bab ini berisi rancangan pembuatan sistem yang digambarkan dalam bentuk flowchart beserta desain antarmuka yang aka dibuat.

4. Bab IV: Implementasi dan Analisis Sistem

   Pada bab ini penulis akan mengimplementasikan rancangan sistem yang telah ditulis pada bab III menggunakan bahasa pemrograman.

5. Bab V: Kesimpulan dan Saran

   Bab ini adalah bab terakhir yang akan berisi tentang kesimpulan yang dapat diambil dari sistem yang telah dibuat, serta saran untuk keperluan pengembangan sistem.

BAB II
LANDASAN TEORI

2.1. Tinjauan Pustaka

Penelitian yang dilakukan oleh Basuki dengan judul "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4", menjelaskan bahwa algoritma steganografi LSB bisa digabungkan dengan algoritma kriptografi klasik untuk meningkatkan keamanan data yang disisipi kedalam citra. Kekurangan dari penelitian tersebut adalah program yang dibuat hanya mampu menggunakan 1 jenis format citra saja. (Rakhmat, Basuki, Fairuzabadi, Muhammad, 2010)

Penelitian lain yang dilakukan oleh Bhattacharya, Dey dan Chaudhuri dengan judul "A Session based Multiple Image Hiding Technique using DWT and DCT" meneliti tentang steganografi dengan metode DWT dan DCT yang digabungkan untuk proses stegano, dengan sebelumnya membagi citra menjadi 3 buah citra dengan warna dasar yaitu merah, hijau dan biru (RGB). Setelah citra dibagi menjadi 3 buah warna dasar maka akan dilakukan proses DWT pada masing-masing citra warna dasar, dan proses DCT dilakukan pada sub band HH. 3 buah gambar rahasia akan dikonversi menjadi vector 1-D, lalu akan dipilih frekuensi tertentu untuk dimodifikasi. Menggunakan pseudo random 2D. Setelah proses embedding dilakukan pada masing-masing citra warna dasar maka akan dilakukan proses inver untuk mendapatkan form spatial, yang selanjutnya 3 buah citra warna dasar tersebut akan digabungkan kembali untuk mendapatkan citra stegano yang berwarna. Hasil yang didapat dengan melakukan embedding pada frekuensi yang random adalah semakin sulit untuk mendeteksi adanya sebuah pesan rahasia yang tertanam menggunakan proses steganalysis yang umum digunakan. Dan juga PSNR yang didapat tidak mengecewakan. (Bhattacharya, Tanmay, Dey, Nilanjan, Chaudhuri, S.R. Bhadra, 2012)

Pada penelitian ini penulis mencoba membantu agar pihak awam yang hendak melakukan penyembunyian data mendapat hasil yang diharapkan. Tidak semua orang menguasai teknik tentang steganografi, sehingga ketika mencoba untuk melakukan

penyembunyian data, mereka hanya memilih media penyimpanan sembarangan. Hasil yang didapat ketika melakukan penyembunyian secara sembarangan tersebut tidak selalu mendapatkan hasil yang memuaskan. Dan terkadang dapat dideteksi dengan kasat mata bahwa media yang digunakan telah disisipi oleh data. Untuk mengatasi hal tersebut penulis mencoba membuat aplikasi yang bisa membandingkan kualitas citra hasil stegano dengan menggunakan metode DCT dan LSB pada citra yang berformat JPG, BMP dan PNG.

2.2. Landasan Teori

2.2.1. Kriptografi

Menurut Kamus Besar Bahasa Indonesia, kriptografi adalah penyelidikan tentang kode rahasia; teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut. Dengan kata lain dapat disebut sebagai sebuah cabang ilmu pengetahuan yang mempelajari bagaimana mengamankan data sehingga orang yang tidak mempunyai hak tidak dapat mengakses data tersebut.

Sedangkan menurut Rakhmat & Fairuzabadi (2010), kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dari banyak jenis skema yang digunakan untuk kriptografi terdapat 3 jenis kriptografi yaitu :

- Secret key Cryptography

Tipe kriptografi jenis ini hanya menggunakan single key saja. Pengirim membuat key untuk enkrip sebuah pesan dan penerima menggunakan key yang sama untuk melakukan dekrip. Enkripsi jenis ini disebut juga sebagai symmetric encryption. Permasalahan terbesar dari teknik ini adalah distribusi dari key tersebut.

- Public key Cryptography

Tipe kriptografi jenis ini menggunakan dua buah key, yang dapat membuat komunikasi secara aman di jalur yang kurang terjaga keamanannya. Enkripsi jenis ini disebut juga sebagai asymmetric encryption. Pada metode ini, setiap pihak mempunyai dua buah key yaitu public dan private key. Private key bersifat rahasia dan tidak

disebarkan sedangkan public key dibagikan kepada setiap pihak yang ingin berkomunikasi. Jika Alice ingin mengirimkan pesan kepada Bob, maka Alice akan melakukan enkrip menggunakan Bob public key dan Bob akan dapat melakukan dekrip dengan menggunakan private key-nya.

- Hash function

Teknik ini tidak menggunakan key melainkan menggunakan sebuah nilai hash tertentu yang telah dikomputasi kepada sebuah plain text. Fungsi hash digunakan untuk menggecek keabasahan sebuah pesan, untuk meyakinkan bahwa pesan tersebut tidak pernah dimodifikasi oleh pihak lain ataupun terkena virus.

Dalam kehidupan sehari-hari tidak semua informasi yang akan kita berikan kepada seseorang bersifat umum, oleh karena itu informasi yang bersifat bukan untuk komsumsi umum atau pribadi sebaiknya diamankan dengan menggunakan kriptografi.

2.2.2. Steganografi

Menurut Bhattacharya, Tanmay, Dey (2012), Steganografi adalah proses penyembunyian pesan rahasia didalam sebuah pesan biasa dan melakukan ekstrasi pesan ketika sampai pada tujuannya. Steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang berarti tersembunyi atau terselubung, dan *graphein* yang artinya menulis. Steganografi dapat diartikan tulisan tersembunyi (*covered writing*). Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui.

Steganografi membutuhkan dua properti, yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lain. Proses penyisipan pesan ke dalam media *covertext* dinamakan encoding, sedangkan ekstraksi pesan dari *stegotext* dinamakan decoding. Kedua proses ini mungkin memerlukan kunci rahasia (yang dinamakan *stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi.

2.2.3. JPEG

Menurut Uma (2011), pengertian *JPEG* yang dikembangkan oleh Joint Photographic Expert Group merupakan metode kompresi yang lossless untuk warna sehingga banyak digunakan. Keuntungan dari format JPEG adalah dengan banyaknya parameter yang digunakan, sehingga pengguna dapat menyesuaikan banyaknya data yang hilang dan kompresi ratio. Keuntungan lainnya adalah dapat diterima pada hampir semua program-program komputer. Sedangkan kelemahan dari format JPEG ini adalah kompresi citra pada format ini mempengaruhi kualitas citra itu sendiri.

2.2.4. PNG

Mulyanta (2005) mengemukakan bahwa PNG bukan merupakan format baru karena telah dikembangkan pada tahun 1995 untuk mengganti format GIF (*Graphics Interchange Format*) dan format TIFF (*Tagged Image File Format*). Tipe file PNG sendiri merupakan kompresi citra yang bagus dengan warna yang lebih banyak. Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (*lossles compression*). Kelebihan file PNG adalah adanya warna transparan dan *alpha*. Warna *alpha* memungkinkan sebuah citra transparan, tetapi citra tersebut masih dapat dilihat mata seperti samar-samar atau bening. Kekurangan dari PNG adalah ukurannya yang besar.

2.2.5. BMP

Bitmap merupakan representasi dari citra grafis yang terdiri dari susunan titik (*pixel*) yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu bit data (untuk citra hitam putih) atau lebih (untuk citra berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam citra ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 800×600).

Citra bitmap sangat bergantung pada resolusi. Jika citra diperbesar maka citra akan tampak kurang halus atau pecah, sehingga mengurangi detailnya. Selain itu citra bitmap akan mempunyai ukuran file yang lebih besar.

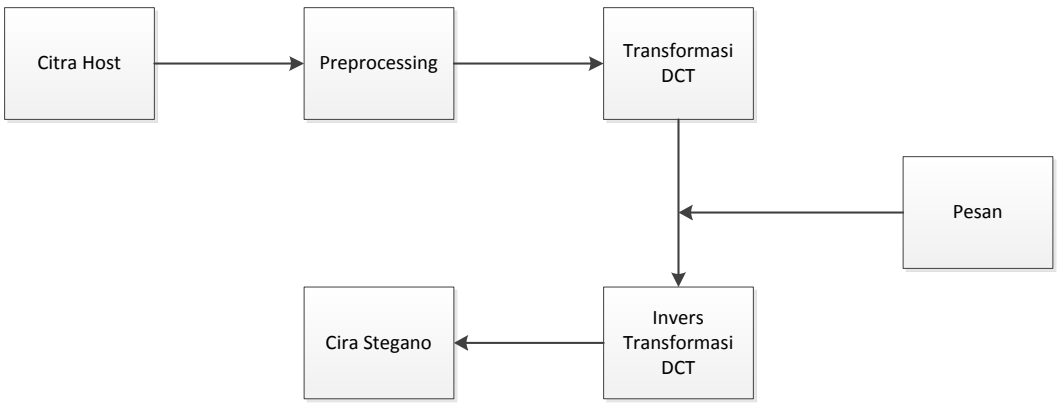
Keuntungan dan kekurangan dari citra bitmap tergantung dari resolusinya. Semakin besar resolusi citra akan semakin besar pula ukuran filenya. Resolusi yang semakin tinggi membuat gambar tidak mudah pecah ketika di zoom.

2.2.6. DCT

Menurut Uma (2011) DCT merupakan sebuah metode yang telah diterapkan di berbagai bidang pengetahuan. DCT merupakan metode yang mentransfrormasikan sebuah informasi dari domain ruang atau waktu ke dalam domain frekuensi dengan tujuan untuk mempercepat transmisi, mengurangi penyimpanan di dalam memori, menyediakan representasi *compact*, dan sebagainya.

Keunggulan dari DCT adalah memiliki invers yang artinya nilai keluaran setelah transformasi dapat digunakan kembali untuk menghasilkan nilai asli sebelum ditransformasikan. Langkah yang pertama kali dilakukan ketika melakukan proses DCT adalah dengan membagi citra kedalam blok – blok berukuran tertentu. Ukuran blok yang umum digunakan adalah berukuran 8 x 8.

Menurut Nelson, Mark, and Gailly (1996) semakin besar ukuran blok yang digunakan mungkin akan memberikan hasil yang lebih baik, tetapi tidak memakan waktu yang lama hingga mencapai *Point of diminishing returns.* DCT dengan blok berukuran 64x64 mungkin tidak lebih baik dari 4 blok berukuran 16x16. Dan yang membuat lebih jelek adalah, waktu pengerjaan penghitungannya akan lebih lama.



Gambar 2. 1 Proses penyembunyian pesan dengan metode DCT

Gambar 2. 2 Proses ekstraksi pesan

Rumus DCT dan invers DCT secara umum (Khayam,2003) adalah sebagai berikut:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad \textbf{[2.1]}$$

Dan rumus inver dari DCT adalah sebagai berikut:

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad \textbf{[2.2]}$$

Dengan α u dan α v = $\sqrt{\frac{1}{N}}$ jika u dan v = 0 , dan

bernilai $\sqrt{\frac{2}{N}}$ jika kondisi nilai u dan v = 0 tidak terpenuhi.

Dimana :

C(u,v) = Nilai pixel hasil transformasi pada baris ke-u dan kolom ke-v

N = Dimensi matriks

f(x,y) = Nilai pixel citra pada baris ke-x dan kolom ke-y

α = konstanta

2.2.7. LSB

Menurut Rakhmat & Fairuzabadi (2010) metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext*. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir , digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB,

sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.

Misalkan segmen *pixel-pixel* citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110
10010110 11001001 11111001 10001000 10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi (digarisbawahi):

00110011 10100011 11100011 10101010 00100110
10010111 11001000 11111001 10001001 10100011

2.2.8. MSE dan PSNR

Menurut Bhattacharya, Tanmay, Dey (2012) menjelaskan bahwa *Peak Signal to Noise Ratio* (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan decibel (dB). Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan *Mean Square Error* (MSE). Adapun MSE adalah nilai error kuadrat rata-rata antara citra *cover* dengan citra steganografi, secara matematis dapat dirumuskan sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M} \quad \sum_{j=1}^{N}[I(x,y) - K(x,y)]^2 \qquad \textbf{[2.3]}$$

Diketahui:

MSE = Nilai Mean Square Error citra steganografi

M = Panjang citra stego (dalam *pixel*)

N = Lebar citra stego (dalam *pixel*)

I (x,y) = nilai *pixel* dari citra *cover*

K(x,y) = nilai *pixel* pada citra stego

Setelah diperoleh nilai MSE maka nilai PSNR dapat dihitung dari kuadrat nilai maksimum dibagi dengan MSE. Secara matematis, nilai PSNR dirumuskan sebagai berikut :

$$PSNR = 10.log_{10}\left(\frac{MAX_i^2}{MSE}\right) = 10.log_{10}\left(\frac{MAX_i}{\sqrt{MSE}}\right) \quad \textbf{[2.4]}$$

Diketahui:

MSE = nilai MSE,

MAXi = nilai maksimum dari *pixel* citra yang digunakan

Semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi. Nilai acuan PSNR bisa dikatakan baik adalah bernilai ≥ 30.

BAB III
PERANCANGAN SISTEM

Perancangan sistem merupakan bab yang menguraikan analisis teori dan menerjemahkan teori tersbut ke dalam suatu sistem, yang dibuat, meliputi analisis kemampuan dan kebutuhan sistem, perancangan sistem, diagram alir struktur program dan perancangan antarmuka sistem. Sehingga mampu memberikan dukungan pemahaman dengan steganografi yang menggunakan metode DCT (*Discrete Cosine Transform*) dan LSB (*Least Significant Bit*).

Aplikasi yang digunakan untuk membangun sistem menggunakan Matlab. Secara garis besar sistem steganografi yang akan dibuat ini terbagi menjadi 2 (dua) bagian utama, yaitu :
Sistem dapat meng-enkripsi suatu informasi rahasia yang kemudian menyembunyikan informasi rahasia tersebut pada suatu media perantara (citra) agar tidak terlihat.

3.1. Kebutuhan System

Secara umum analisis kebutuhan sistem dalam membangun aplikasi steganografi adalah sebagai berikut :

3.1.1. Kebutuhan Perangkat Lunak

Spesifikasi perangkat lunak yang digunakan dalam pembangunan sistem digital watermarking ini adalah sebagai berikut:

1. Sistem Operasi Windows 7 Ultimate
2. Bahasa pemrograman Matlab

3.1.2. Kebutuhan Perangkat Keras

Spesifikasi perangkat keras yang digunakan dalam pembangunan sistem pada Tugas Akhir ini adalah sebagai berikut:

1. Processor AMD phenom II
2. Memory 4096 MB RAM
3. Harddisk 250 GB

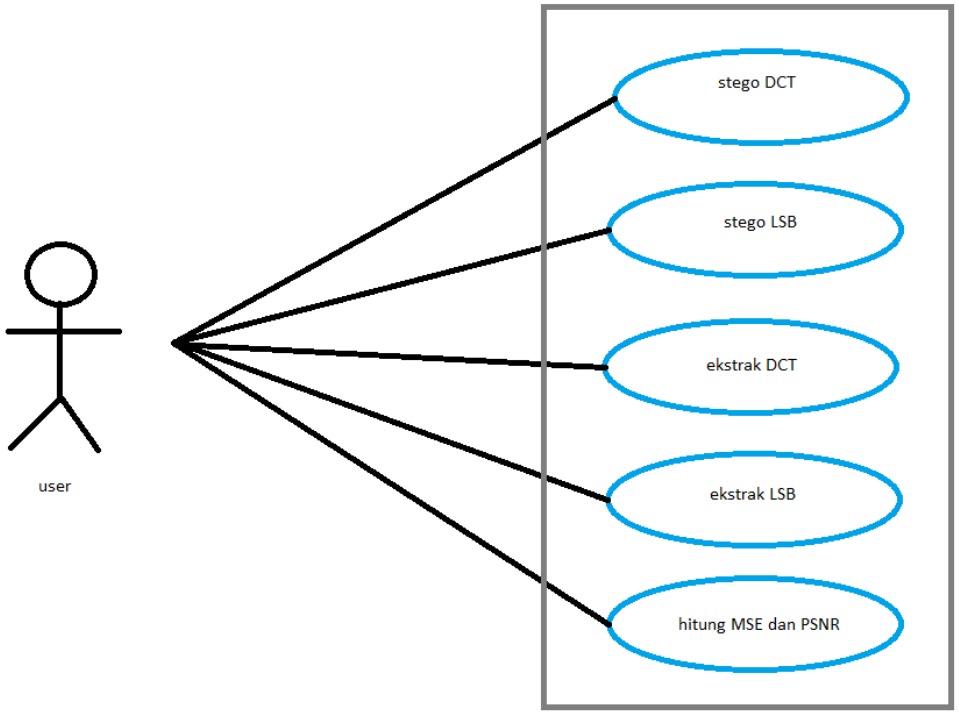
3.1.3. Spesifikasi Sistem

Sistem yang akan dibuat di dalam Tugas Akhir ini memiliki spesifikasi sebagai berikut:

1. Algoritma yang akan digunakan adalah algoritma *Discrete Cosine Transform* dan *Least Significant Bit*.
2. Input terdiri dari dua macam, yaitu pesan teks serta citra digital penampung yang berupa file JPG,BMP atau PNG
3. Output untuk sistem steganografi berupa satu file citra digital yang telah disisipi oleh pesan teks. Sedangkan output untuk sistem ekstraksi steganografi berupa pesan teks yang disisipkan.

3.2. Perancangan Proses

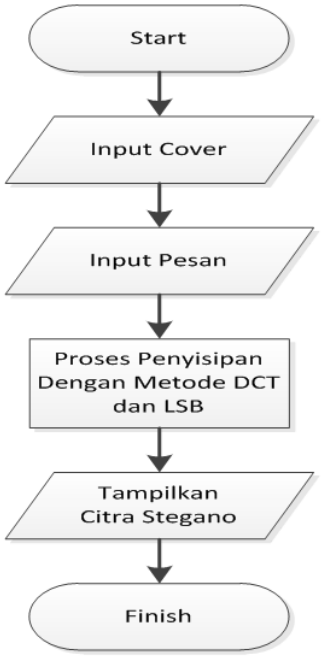
Dalam penelitian ini, penulis merancang sebuah sistem yang dapat mengamankan sebuah pesan dengan menggunakan 2 metode steganografi yaitu DCT (*Discrete Cosine Transform*) dan LSB (Least Significant Bit). Adapun kemampuan dari sistem dapat terlihat pada gambar 3.1



Gambar 3. 1 Use Case Diagram

3.2.1. Algoritma Penyisipan Pesan

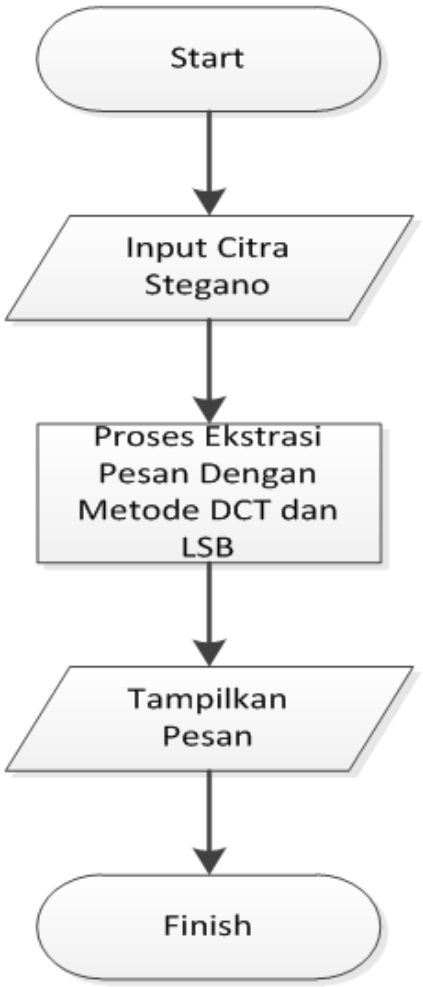
- Input :
  1. File teks
  2. Citra digital yang memiliki format JPG, PNG, dan BMP 24bit
- Proses :
  1. Pilih file citra yang digunakan sebagai media penyisipan pesan.
  2. Pilih jenis pesan yaitu teks yang akan disisipkan dan masukan pesan ke dalam textbox.
  3. Program melakukan proses penyisipan pesan (DCT atau LSB)
  4. Jika proses penyisipan berhasil maka akan tercipta file citra baru yang telah disisipi file teks.
- Output :
  1. File citra digital yang berektensi sesuai dengan ekstensi yang diinginkan sebagai media penyisipan pesan.
  2. Untuk output file citra berekstensi JPG pada LSB akan digunakan file citra JPG lossless.



Gambar 3. 2 Diagram alur penyisipan pesan

3.2.2. Algoritma Ekstraksi Pesan

- Input :
  1. Citra digital yang sudah disisipi pesan
- Proses :
  1. Pilih file citra yang telah disisipi pesan.
  2. Program melakukan ekstraksi pesan (*DCT* atau *LSB*).
  3. Jika proses ekstrasi pesan berhasil maka akan muncul *file text* asli yang disembunyikan sebelumnya.
- Output : File teks atau citra digital yang isinya sama dengan file aslinya sebelum dilakukan proses enkripsi dan penyisipan.



Gambar 3. 3 Diagram alur ekstraksi pesan

3.3. Perancangan Antarmuka

Antarmuka sistem yang dibangun oleh penulis terdiri dari tiga tampilan, yaitu tampilan Home, tampilan Steganografi dan tampilan Ekstrak.

3.3.1. Tampilan Home

Tampilan home pada program dapat dilihat pada gambar 3.4 Pada tampilan home akan terdapat 2 tombol pilihan yaitu stego dan ekstrak

Gambar 3. 4 Perancangan tampilan awal sistem

1. Di dalam form Home ini terdapat dua tombol yang dapat dipilih, yaitu Stego dan Ekstrak
2. Tombol Stego adalah sebuah tombol yang dapat digunakan untuk memilih proses steganografi.
3. Tombol Ekstrak adalah sebuah tombol yang dapat digunakan untuk memilih proses ekstraksi.

3.3.2. Tampilan Steganografi

Pada saat user memilih tombol stego, maka akan muncul tampilan steganografi. Gambar 3.5 akan menampilkan perancangan tampilan steganografi tersebut.

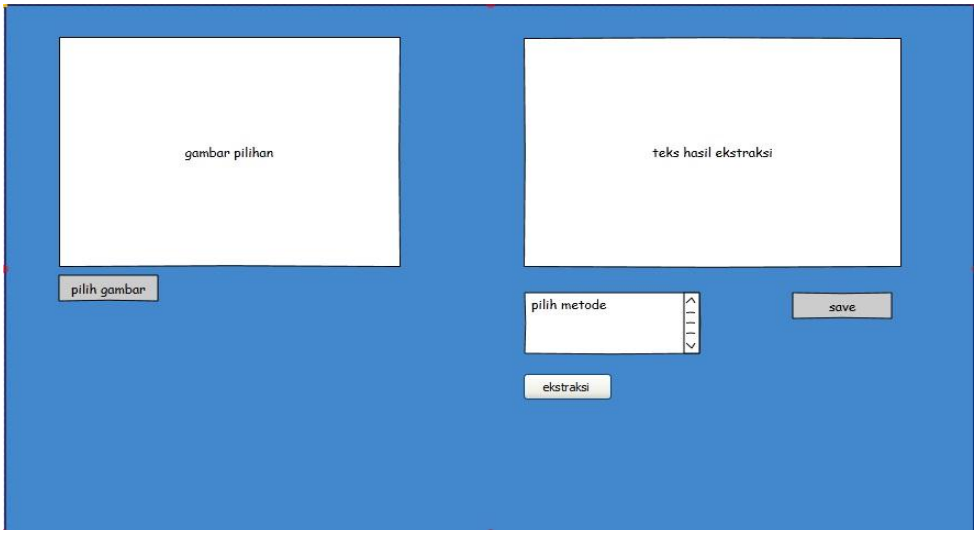
Gambar 3. 5 Rancangan tampilan steganografi

Penjelasan dari form Steganografi ini adalah sebagai berikut:

1. Tombol “pilih gambar” digunakan untuk memilih file citra digital dari lokasi penyimpanan file citra yang akan disisipi teks.
2. Kotak “gambar pilihan” adalah tempat dimana file citra pilihan akan ditampilkan
3. Tombol “pilih teks” digunakan untuk memilih teks yang akan disisipkan dari lokasi penyimpanan teks.
4. Kotak “isi teks pilihan” adalah tempat dimana isi dari file teks yang dipilih ditampilkan.
5. Kotak “pilih metode” digunakan untuk memilih metode steganografi yang akan digunakan.
6. Tombol “stego” adalah tombol yang digunakan untuk memulai proses steganografi.
7. Kotak ”gambar hasil steganografi” adalah tempat menampilkan gambar yang telah disisipi oleh file teks.
8. Tombol “save” adalah tombol untuk menyimpan gambar hasil steganografi.

3.3.3. Tampilan Ekstraksi

Pada saat user memilih tombol “Ekstrak” di tampilan Home, maka akan muncul tampilan Ekstraksi seperti pada gambar 3.6



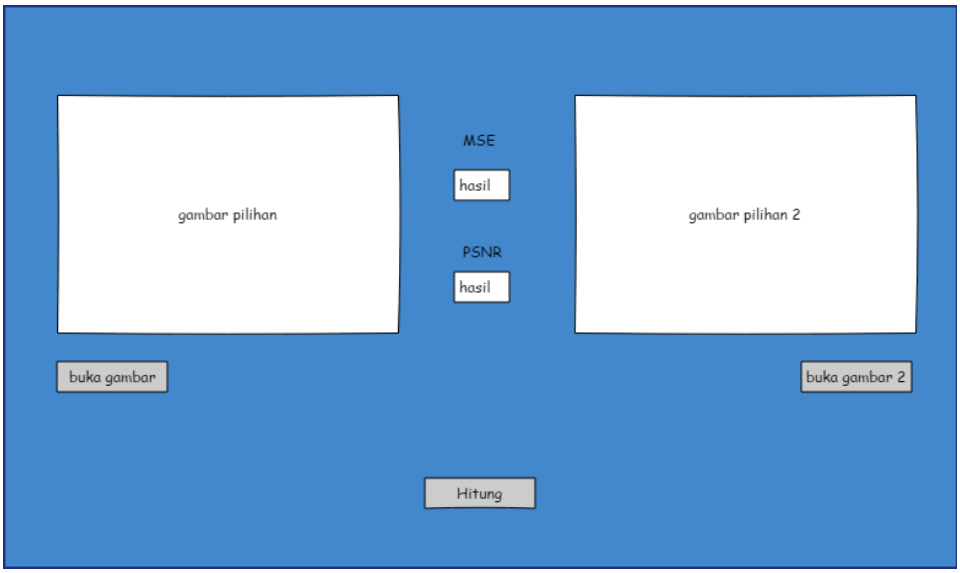
Gambar 3. 6 Rancangan tampilan ekstraksi

Penjelasan dari tampilan Ekstrasi ini adalah sebagai berikut:

1. Tombol “pilih gambar” digunakan untuk memilih file citra digital hasil steganografi dari lokasi penyimpanan file citra .
2. Kotak “gambar pilihan” adalah tempat dimana file citra pilihan akan ditampilkan
3. Kotak “teks hasil ekstraksi” adalah tempat dimana isi dari file teks yang telah diekstraksi dari file gambar pilihan.
4. Kotak “pilih metode” digunakan untuk memilih metode ekstraksi yang akan digunakan.
5. Tombol “ekstaksi” adalah tombol yang digunakan untuk memulai proses ekstraksi.
6. Tombol “save” adalah tombol untuk menyimpan teks hasil ekstraksi.

3.3.4. Tampilan MSE dan PSNR

Tampilan MSE dan PSNR pada gambar 3.7 merupakan tempat dimana user dapat melakukan perbandingan pada gambar asli dengan gambar yang telah disisipi pesan.



Gambar 3. 7 Rancangan tampilan MSE dan PSNR

Penjelasan dari tampilan MSE dan PSNR ini adalah sebagai berikut:

1. Kotak “gambar pilihan ” adalah tempat dimana file citra pilihan pertama akan ditampilkan.
2. Kotak “gambar pilihan 2” adalah tempat dimana file citra pilihan kedua akan ditampilkan.
3. Tombol “buka gambar ” adalah tombol untuk memilih file citra digital yang akan dibandingkan.
4. Tombol “buka gambar 2 ” adalah tombol untuk memilih file citra digital yang akan dibandingkan.
5. Tombol “hitung” berfungsi untuk melakukan perhitungan MSE dan PSNR dari kedua file citra yang dibandingkan.
6. Kotak “hasil” berfungsi untuk menampilkan hasil perhitungan.

BAB IV
IMPLEMENTASI DAN ANALISIS SISTEM

4.1. Implementasi Sistem

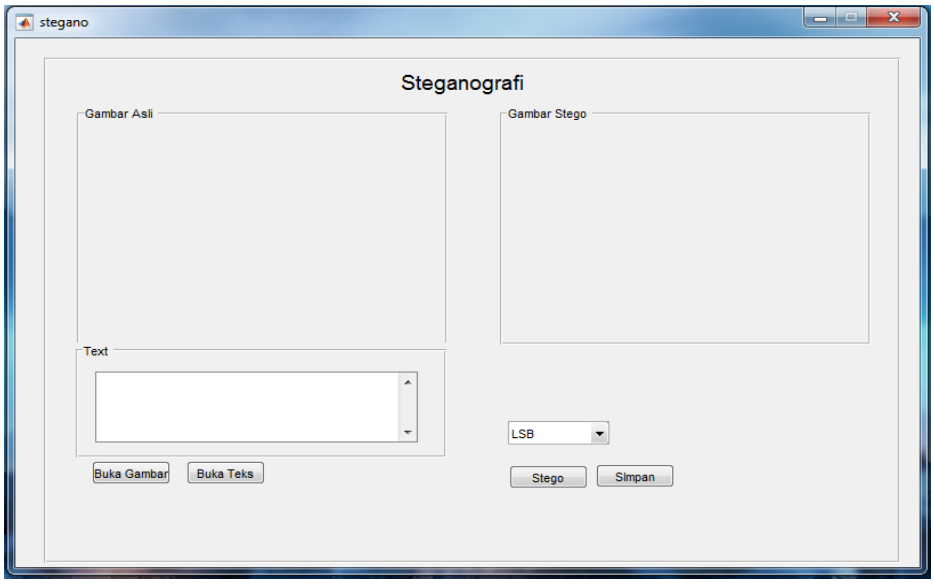
4.1.1. Antarmuka Sistem

Halaman awal pada antarmuka sistem dapat terlihat pada gambar 4.1. Pada halaman ini user dapat memilih untuk melakukan proses stegano atau proses ekstraksi pesan

.

Gambar 4. 1 Tampilan awal sistem

Jika user memlih untuk melakukan proses stegano maka user akan dibawa kepada halaman stegano seperti yang ditunjukan pada gambar 4.2

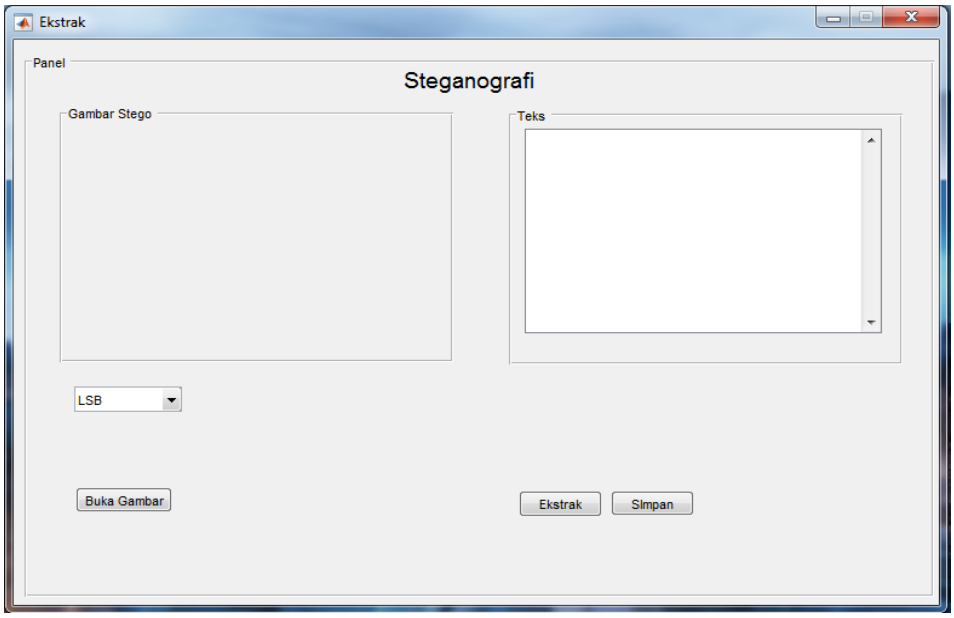


Gambar 4. 2 Tampilan stegano pada sistem

Pada halaman stegano, user dapat memlih untuk membuka gambar, membuka teks, memilih metode stegano, melakukan proses stegano dan menyimpan hasil stegano.

Di halaman ini user juga dapat melihat gambar asli dan gambar hasil stegano secara langsung, yang akan ditampilkan pada bagian kiri dan kanan halaman pada kotak gambar asli dan gambar stego. Teks yang akan disisipkan pada gambar juga dapat terlihat di kotak teks sehingga user dapat memastikan teks yang terpilih tidaklah salah. Metode untuk melakukan stegano dapat dipilih melalui listbox yang tersedia. Jika user sudah mendapatkan hasil stegano yang diinginkan, user dapat menyimpan gambar hasil stegano tersebut melalui tombol simpan.

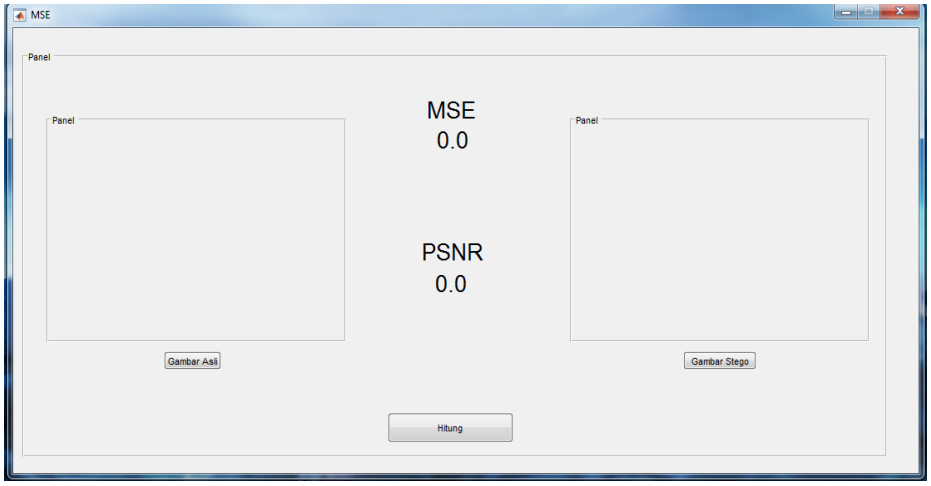
Jika pada halaman awal user memlih untuk melakukan proses ekstrasi, maka user dibawa kepada halaman ekstrak yang tampak pada gambar 4.3



Gambar 4. 3 Tampilan ekstrak pada sistem

Pada halaman ekstrak ini, user dapat memilih gambar yang akan diekstrasi melalui tombol buka gambar yang kemudian gambar tersebut akan ditampilkan pada kotak gambar stego di bagian sebelah kiri halaman. User juga dapat memilih metode yang digunakan pada listbox yang tersedia. Setelah user memilih gambar dan metode, user dapat melakukan proses ekstraksi, maka teks hasil ekstraksi akan ditampilkan pada kotak teks di bagian kanan halaman. Hasil ekstrasi dapat disimpan melalui tombol simpan.

Untuk membandingkan nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) dari gambar, tersedia tampilan tersendiri yang tampak seperti pada gambar 4.4



Gambar 4. 4 Tampilan halaman penghitungan MSE dan PSNR

Pada halaman ini user dapat melihat langsung nilai MSE dan PSNR dari gambar hasil stegano yang dibandingkan dengan gambar asli pilihannya. Tombol yang tersedia hanya 3 yaitu 2 tombol untuk memilih gambar yang akan dibandingkan, serta 1 tombol untuk menghitung perbandingan MSE dan PSNR dari kedua gambar tersebut.

4.1.2. Penyisipan Dan Ekstraksi Pesan Pada Metode LSB

Penyisipan pesan pada metode *Least Significant Bit* (LSB) dilakukan pada bit terakhir tiap komponen warna yaitu pada tiap bit terakhir bit RGB (*Red Green Blue*). Adapun caranya dapat terlihat pada gambar 4.5. Tiap huruf akan disembunyikan dan dibagi pada 3 komponen warna tersebut.

```
function [red,green,blue] = hidetext(redc,greenc,bluec,text)
red=bitand(redc,248);
green=bitand(greenc,248);
blue=bitand(bluec,252);


if bitand(text,128)== 128
    red=bitor(red,4);
end

if bitand(text,64)== 64
    red=bitor(red,2);
end

if bitand(text,32)== 32
    red=bitor(red,1);
end

if bitand(text,16)== 16
    green=bitor(green,4);
end

if bitand(text,8)== 8
    green=bitor(green,2);
end

if bitand(text,4)== 4
    green=bitor(green,1);
end

if bitand(text,2)== 2
    blue=bitor(blue,2);
end

if bitand(text,1)== 1
    blue=bitor(blue,1);
end

return

end
```

Gambar 4. 5 Proses penyisipan pesan dengan metode LSB

Untuk ekstrasi pesan pada metode LSB dapat terlihat pada gambar 4.6 dimana sistem melakukan pengecekan pada tiap bit RGB. Ketika huruf yang telah disembunyikan ditemukan maka bit huruf tersebut akan dibangun ulang pada variabel txt.

```
function data = findtext(redc,greenc,bluec)
txt=0;
if bitand(redc,4)== 4
txt=bitor(txt,128);
end
if bitand(redc,2)== 2
txt=bitor(txt,64);
end
if bitand(redc,1)== 1
txt=bitor(txt,32);
end
if bitand(greenc,4)== 4
txt=bitor(txt,16);
end
if bitand(greenc,2)== 2
txt=bitor(txt,8);
end
if bitand(greenc,1)== 1
txt=bitor(txt,4);
end
if bitand(bluec,2)== 2
txt=bitor(txt,2);
end
if bitand(bluec,1)== 1
txt=bitor(txt,1);
end
data=txt;
return
end
```

Gambar 4. 6 Proses ekstraksi pesan dengan metode LSB

4.1.3. Penyisipan Dan Ekstraksi Pesan Pada Metode DCT

Pada metode *Discrete Cosine Transform* (DCT) ini penyisipan pesan hanya pada komponen R(*red*) dari gambar. Komponen R dari gambar tersebut kemudian akan diproses DCT dan setelah proses DCT selesai maka akan disisipkan huruf per huruf dari teks yang terpilih dan dilakukan inverse DCT. Proses penyisipan dapat terlihat pada gambar 4.7

```
% Take the block and perform DCT
block = dct2(img(posx, posy));

c1 = block(s1x, s1y);
c2 = block(s2x, s2y);

if (secret_teks_i <= secret_length)
    secret_bit = teksbin(secret_teks_i);
    bits_written = bits_written + 1;
else
    secret_bit = insufficient_bit;
    bits_unused = bits_unused + 1;
end
secret_teks_i = secret_teks_i + 1;

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

% Ensure (Abs(c1-c2) > x)
[c1 c2] = push_apart(c1, c2, persistence);

block(s1x, s1y) = c1;
block(s2x, s2y) = c2;

% Inverse DCT and build up the stego-image
stego(posx, posy) = idct2(block);
```

Gambar 4. 7 Proses penyisipan dengan metode DCT

Untuk proses ekstrak pada metode DCT dapat terlihat pada gambar 4.8. Sistem akan melakukan DCT pada blok yang terpilih kemudian akan melakukan proses pembangunan ulang huruf yang disembunyikan.

```
% Take the block and perform DCT
block = dct2(img(posx, posy));

c1 = block(s1x, s1y);
c2 = block(s2x, s2y);

if (c1 > c2)
    img_bin(img_bin_i) = 1;
else
    img_bin(img_bin_i) = 0;
end

img_bin_i = img_bin_i + 1;
```

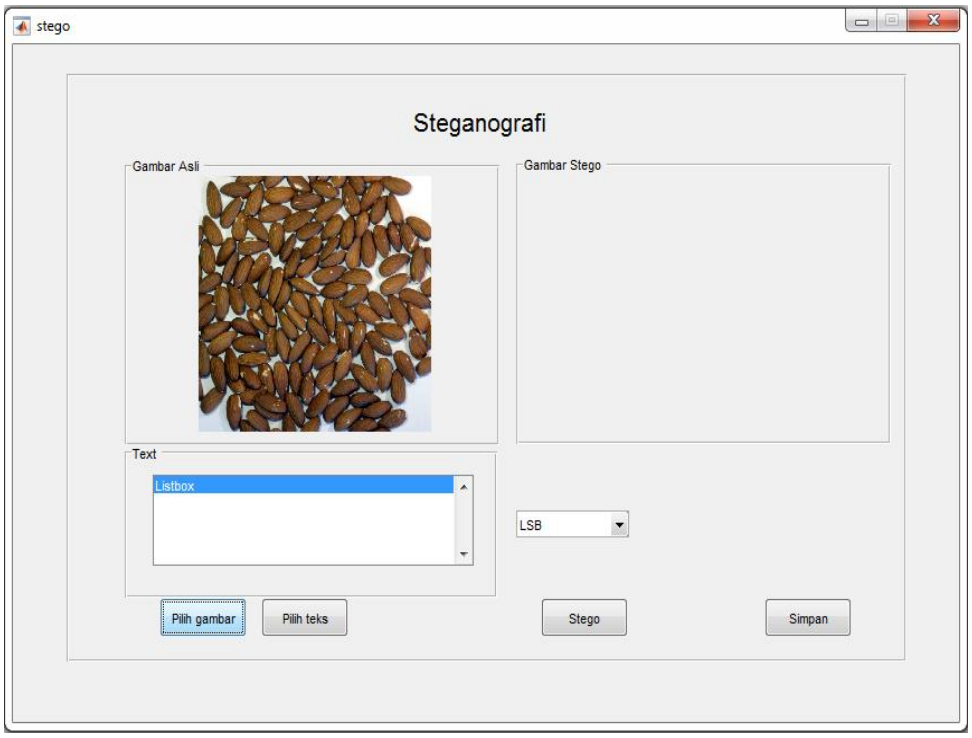
Gambar 4. 8 Proses ekstraksi dengan metode DCT

4.2. Uji Coba Sistem

Pada uji coba sistem ini akan dilakukan langkah demi langkah pada proses stegano dan ekstraksi pesan dengan menggunakan metode LSB dan DCT

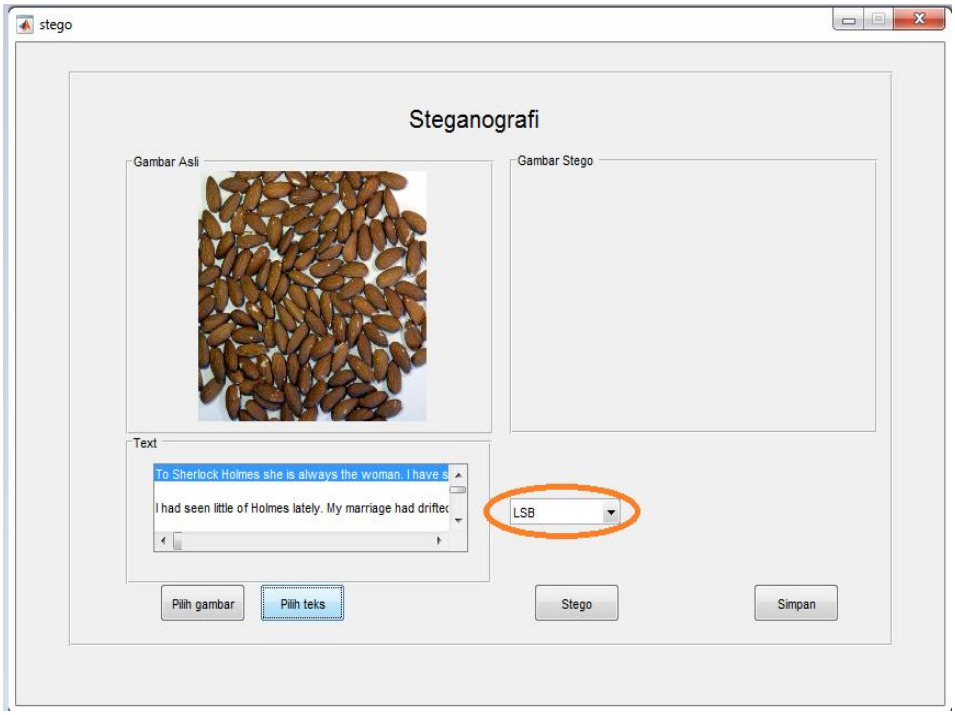
4.2.1. Proses Stego Menggunakan Metode LSB Dan DCT

Pada proses stego ini pertama kita pilih gambar yang akan disisipi pesan gambar tersebut akan ditampilkan pada kotak gambar asli di bagian sebelah kiri, dapat terlihat seperti pada gambar 4.9

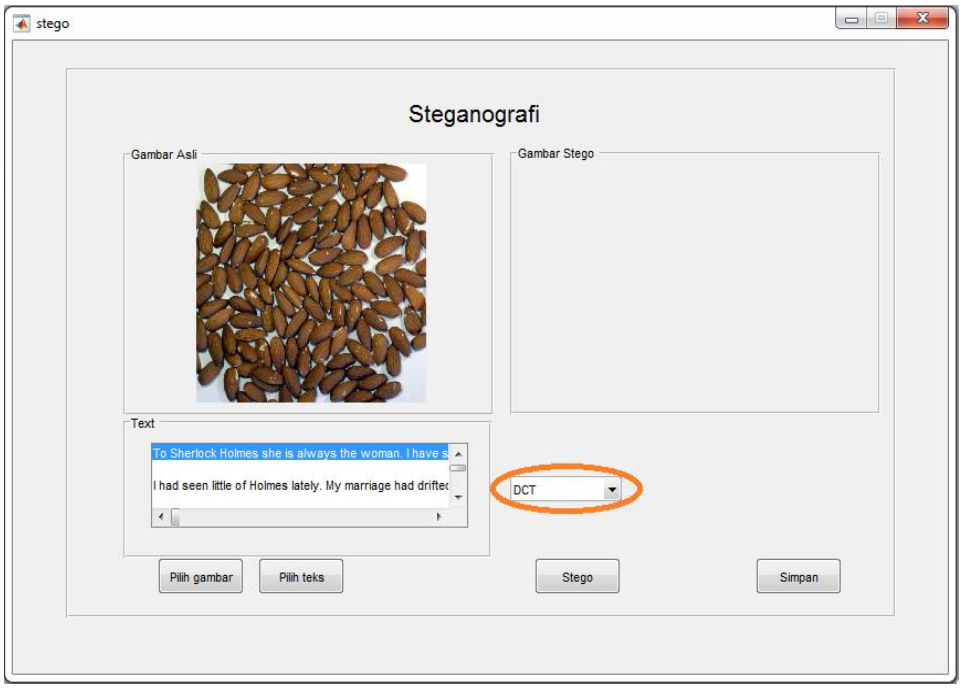


Gambar 4. 9 Tampilan halaman stegano dengan input gambar

Setelah gambar terpilih, user dapat memilih teks yang akan disembunyikan melalui tombol buka teks, yang isi dari teks tersebut akan ditampilkan pada kotak text. Pemilihan metode stegano dapat dipilih melalui menu. Perbedaan metode tampak pada menu yang dilingkari pada gambar 4.10 dan 4.11

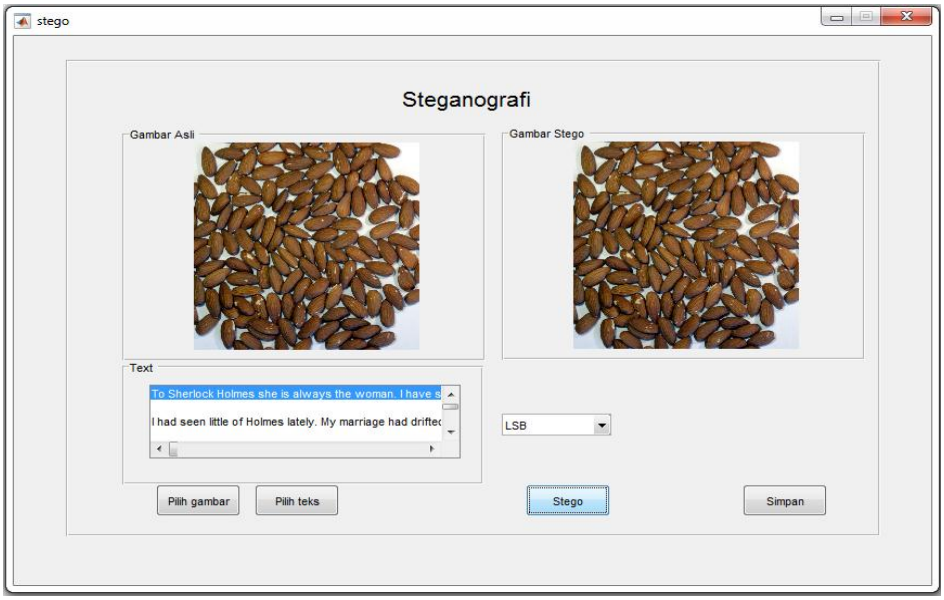


Gambar 4. 10 Tampilan halaman stegano dengan pilihan metode LSB



Gambar 4. 11 Tampilan halaman stegano dengan pilihan metode DCT

Ketika input gambar, teks serta metode sudah dipilih, proses stego dapat dilakukan dengan menekan tombol stego. Hasil dari stego akan ditampilkan pada kotak gambar stego yang tampak pada gambar 4.12

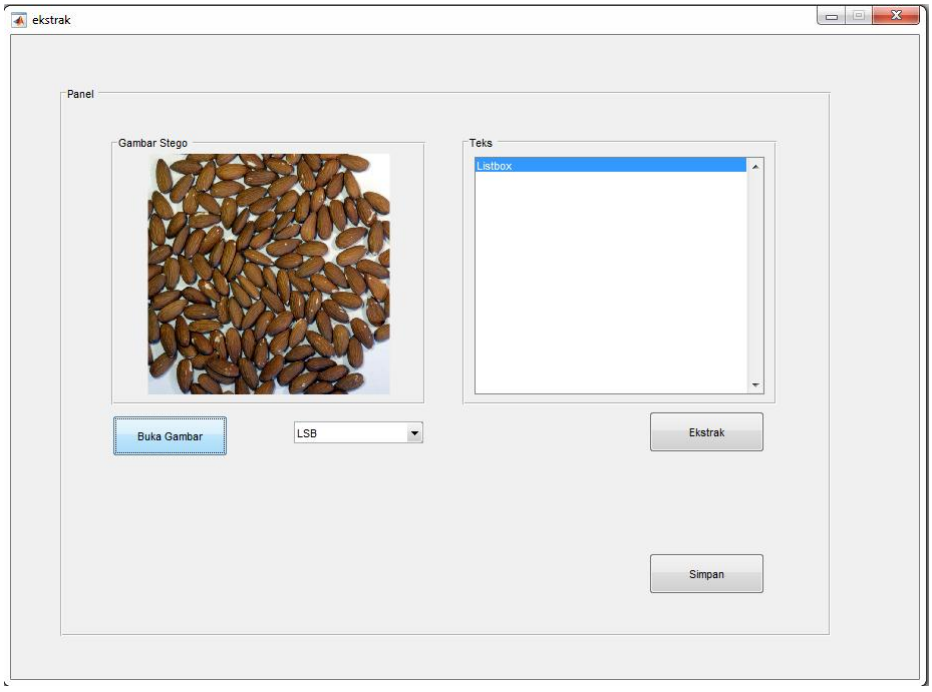


Gambar 4. 12 Tampilan halaman stegano dengan ouput gambar setelah proses

Setelah proses selesai, maka user dapat menyimpan gambar stego tersebut melalui tombol simpan.

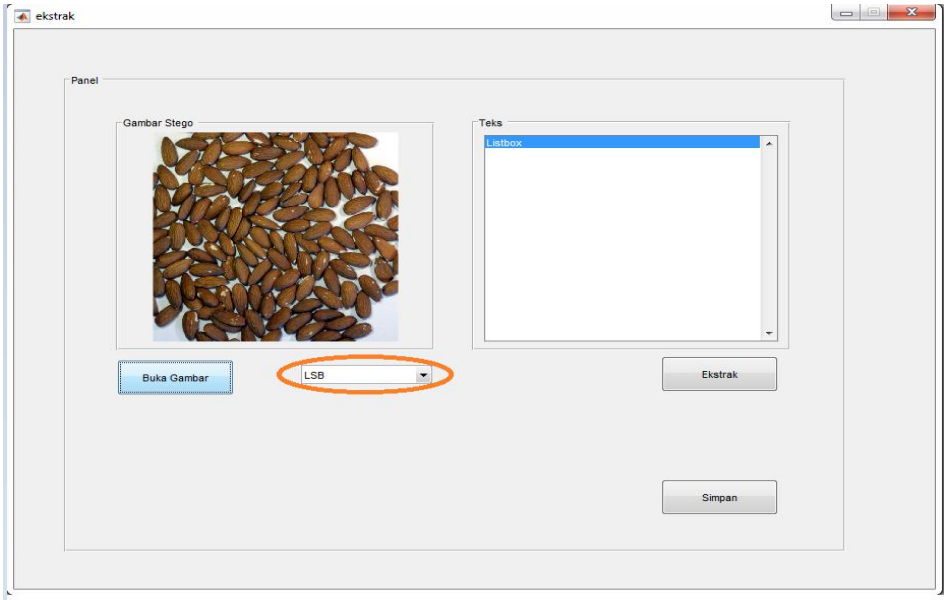
4.2.2. Proses Ekstraksi Menggunakan Metode LSB Dan DCT

User dapat membuka gambar yang akan diproses melalui tombol buka gambar yang kemudian gambar tersebut akan ditampilkan pada kotak gambar stego seperti yang tampak pada gambar 4.13

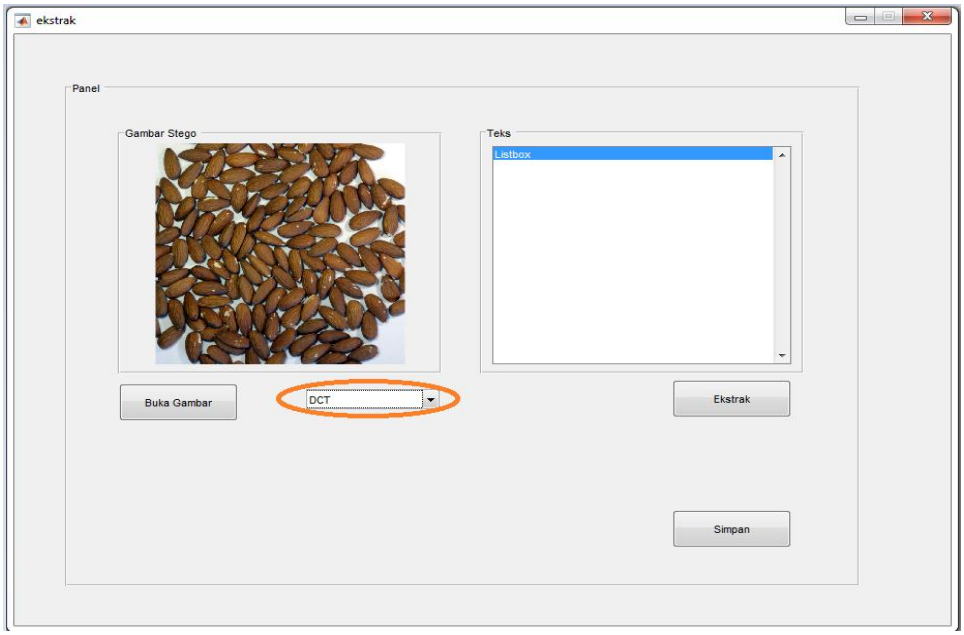


Gambar 4. 13 Tampilan halaman ekstrak dengan input gambar

Metode untuk ekstraksi dapat dipilih melalui menu yang terdapat di bawah tampilan gambar stego, perbedaan pemilihan metode dapat terlihat dengan menu yang dilingkari pada gambar 4.12 dan 4.13



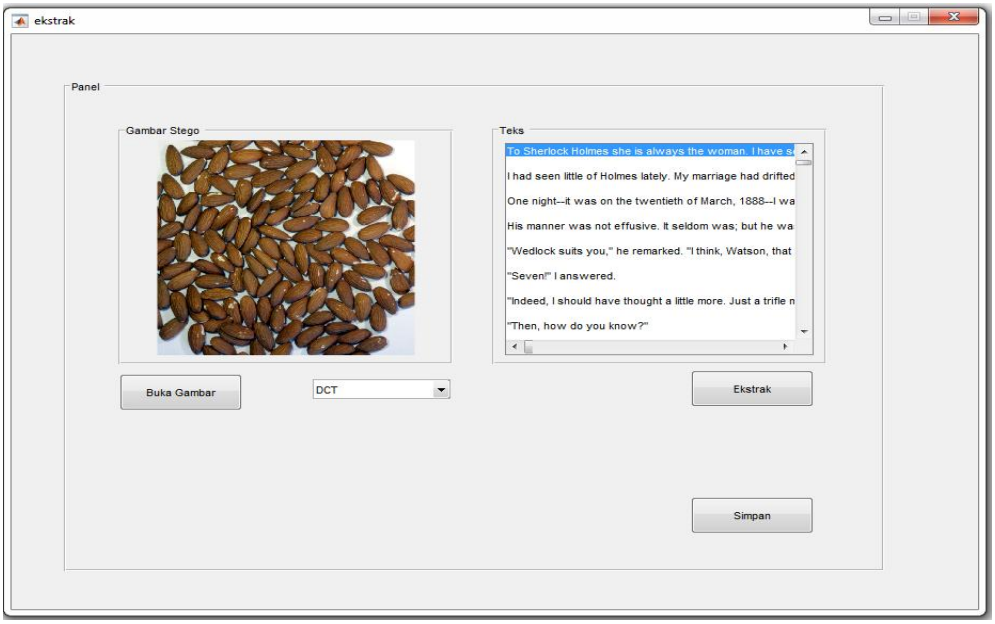
Gambar 4. 14 Tampilan halaman ekstrak dengan metode pilihan LSB



Gambar 4. 15 Tampilan halaman ekstrak dengan metode pilihan DCT

Ketika gambar dan metode sudah terpilih, proses ekstrasi dapat dilakukan dengan menekan tombol ekstrak. Hasil ekstrasi dari gambar yang berupa teks akan ditampilkan pada kotak teks yang terdapak di bagian kanan,

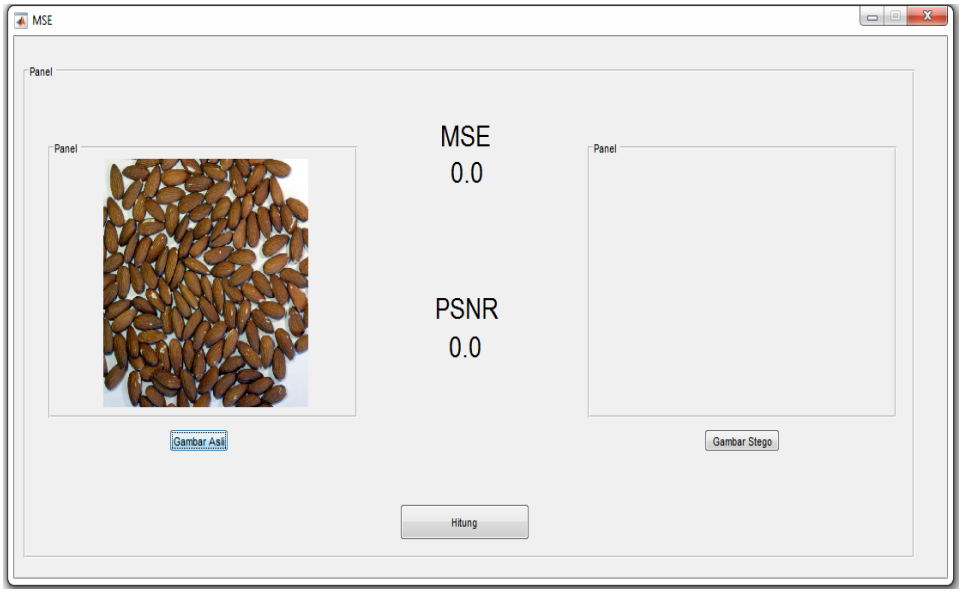
terlihat pada gambar 4.14. Hasil ekstraksi yang berupa teks dapat disimpan dengan menggunakan tombol simpan.



Gambar 4. 16 Tampilan halaman ekstrak dengan hasil ekstraksi berupa teks

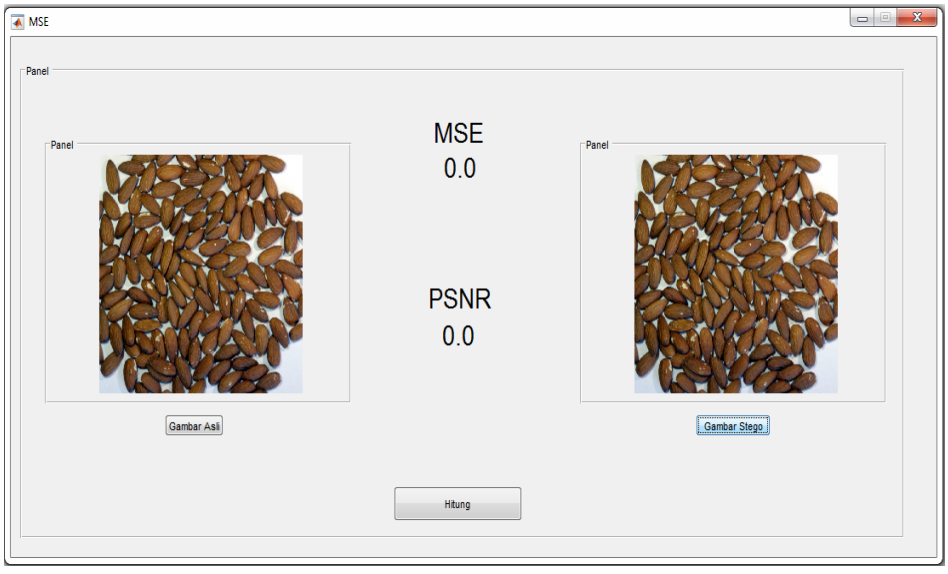
4.2.3. Proses Perhitungan MSE Dan PSNR

Pemilihan gambar yang akan dibandingkan dilakukan dengan memilih gambar asli dan dibandingkan dengan gambar hasil stegano. Gambar asli akan ditampilkan di kotak gambar asli seperti pada gambar 4.15



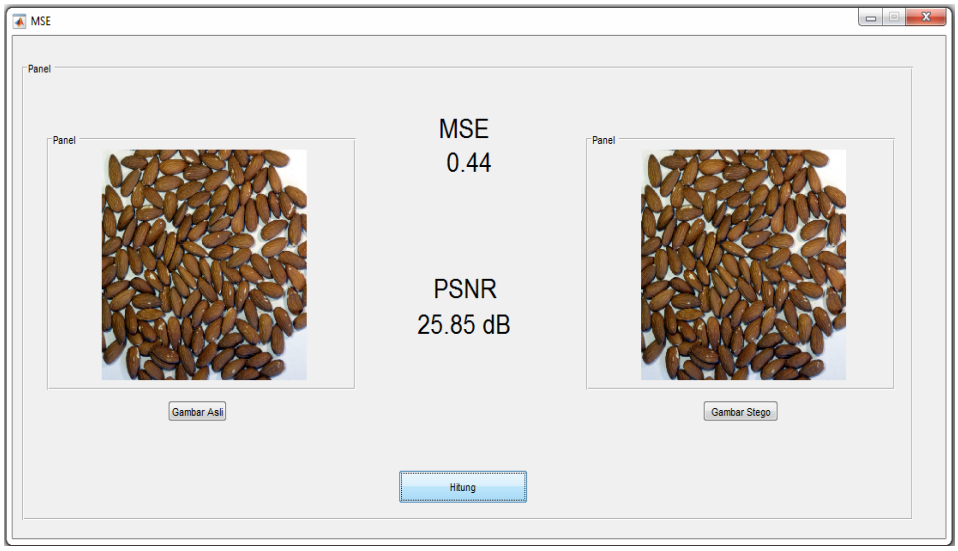
Gambar 4. 17 Tampilan halaman dengan input 1 gambar

Gambar yang akan dibandingkan dipilih dengan tombol gambar stego, yang kemudian gambar tersebut akan ditampilkan pada bagian kanan tampilan. Dapat terlihat hasil tampilan gambar stego pada gambar 4.16



Gambar 4. 18 Tampilan halaman dengan input 2 gambar

Ketika kedua gambar yang akan dibandingkan sudah muncul, perhitungan akan ditampilkan dengan menekan tombol hitung. Hasil perhitungan akan langsung tampak di tampilan seperti pada gambar 4.17



Gambar 4. 19 Tampilan halaman dengan perhitungan MSE dan PSNR

4.3. Parameter Analisis

Melalui analisa dari berbagai format citra pada metode *Discrete Cosine Transform* (DCT) dan metode *Least Significant Bit* (LSB) yang telah dilakukan, penulis mengambil 2 parameter, yaitu :

- Nilai *mean squared error* (MSE)
- Nilai *peak signal to noise ratio* (PSNR)

Setiap parameter yang digunakan mengacu pada hasil citra uji. Berdasarkan hasil analisa dengan berdasarkan menggunakan 2 parameter yang digunakan, maka penulis dapat menyimpulkan kualitas citra mana yang paling terbaik diantara ketiga citra yang diujikan dan mana metode yang lebih baik.

Analisis ini bertujuan untuk mengetahui nilai MSE dan PSNR apakah mengalami perubahan kualitas citra atau tidak pada setiap pemrosesan steganografi yang dilakukan.

Berikut ini adalah tabel nilai hasil analisa MSE dan PSNR yang dilakukan oleh penulis:

Tabel 4. 1 Tabel hasil **penghitungan MSE dan PSNR dengan metode LSB**

Pengujian	Format Citra							
	BMP		PNG		JPG		JPG lossless	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
1	0.03	31.35dB	0.03	31.35dB	-	-	0.03	31.35dB
2	0.05	30.53dB	0.05	30.53dB	-	-	0.05	30.53dB
3	0.01	33.39dB	0.01	33.39dB	-	-	0.01	33.39dB
4	0.03	31.35dB	0.03	31.35dB	-	-	0.03	31.35dB
5	0.04	31.06dB	0.04	31.06dB	-	-	0.04	31.06dB
6	0.05	30.61dB	0.05	30.61dB	-	-	0.05	30.61dB
7	0.06	30.05dB	0.06	30.05dB	-	-	0.06	30.05dB
8	0.05	30.45dB	0.05	30.45dB	-	-	0.05	30.45dB
9	0.47	25.72dB	0.47	25.72dB	-	-	0.47	25.72dB
10	0.04	30.91dB	0.04	30.91dB	-	-	0.04	30.91dB
11	0.04	31.16dB	0.04	31.16dB	-	-	0.04	31.16dB
12	0.05	30.56dB	0.05	30.56dB	-	-	0.05	30.56dB
13	0.03	31.41dB	0.03	31.41dB	-	-	0.03	31.41dB
14	0.03	31.52dB	0.03	31.52dB	-	-	0.03	31.52dB
15	0.04	31.00dB	0.04	31.00dB	-	-	0.04	31.00dB
16	0.06	30.36dB	0.06	30.36dB	-	-	0.06	30.36dB
17	0.06	30.10dB	0.06	30.10dB	-	-	0.06	30.10dB
18	0.03	31.46dB	0.03	31.46dB	-	-	0.03	31.46dB
19	0.43	25.89dB	0.43	25.89dB	-	-	0.43	25.89dB
20	0.03	31.97dB	0.03	31.97dB	-	-	0.03	31.97dB
Nilai rata2	**0.0815**	**30.5425dB**	**0.0815**	**30.5425dB**	**-**	**-**	**0.0815**	**30.5425dB**

Setelah menghitung hasil perhitungan MSE dan PSNR dari 20 pengujian, pada metode LSB penulis mengambil kesimpulan sebagai berikut:

- Citra berekstensi PNG, BMP dan JPG lossless tidak ada perbedaan ketika disisipi oleh pesan teks.
- Ketika disimpan dengan format JPG maka pesan tersembunyi ikut mengalami perubahan, sehingga tidak dapat diekstrak kembali.
- Metode LSB tidak dapat menyimpan citra stegano berformat JPG, adapun jika dipaksakan dapat digunakan format JPG lossless.
- Metode LSB tidak mempunyai keterbatasan pada ukuran citra yang akan digunakan.
- Format JPG lossless tidak dapat menampilkan citra pada image viewer biasa, dikarenakan format JPG pada umumnya merupakan kompresi lossy sehingga image viewer biasa tidak dapat menampilkan citra tersebut.
- Panjang pesan yang akan disembunyikan berpengaruh terhadap kulitas citra stegano, citra akan lebih "rusak" ketika disisipi dengan pesan yang panjang, dapat terlihat pada percobaan no 7, 9, 17 dan 19 pada tabel 4.1.
- Pada percobaan yang dilakukan penulis, citra yang dihasilkan oleh proses stegano dengan menggunakan metode LSB dapat dikatakan bagus dikarenakan nilai rata-rata MSE rendah dan nilai PSNR >30

Tabel 4. 2 Tabel hasil penghitungan MSE dan PSNR dengan metode DCT

Pengujian	Format Citra							
	BMP		PNG		JPG		JPG lossless	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
1	26.81	16.92dB	26.81	16.92dB	34.05	16.40dB	26.81	16.92dB
2	24.56	17.11dB	24.56	17.11dB	14.86	18.21dB	24.56	17.11dB
3	25.24	17.06dB	25.24	17.06dB	26.05	16.99dB	25.24	17.06dB
4	25.17	17.06dB	25.17	17.06dB	22.31	17.32dB	25.17	17.06dB
5	24.83	17.09dB	24.83	17.09dB	15.17	18.16dB	24.83	17.09dB
6	25.17	17.06dB	25.17	17.06dB	18.46	17.73dB	25.17	17.06dB
7	27.77	16.85dB	27.77	16.85dB	16.11	18.03dB	27.77	16.85dB
8	30.33	16.66dB	30.33	16.66dB	82.78	14.48dB	30.33	16.66dB
9	24.92	17.08dB	24.92	17.08dB	38.76	16.12dB	24.92	17.08dB
10	24.77	17.10dB	24.77	17.10dB	50.52	15.55dB	24.77	17.10dB
11	24.04	17.16dB	24.04	17.16dB	15.05	18.18dB	24.04	17.16dB
12	27.47	16.87dB	27.47	16.87dB	68.01	14.90dB	27.47	16.87dB
13	26.81	16.92dB	26.81	16.92dB	31.80	16.55dB	26.81	16.92dB
14	24.41	17.13dB	24.41	17.13dB	12.03	18.66dB	24.41	17.13dB
15	25.43	17.04dB	25.43	17.04dB	16.71	17.95dB	25.43	17.04dB
16	26.46	16.95dB	26.46	16.95dB	13.11	18.48dB	26.46	16.95dB
17	26.24	16.97dB	26.24	16.97dB	37.33	16.21dB	26.24	16.97dB
18	26.99	16.91dB	26.99	16.91dB	33.91	16.41dB	26.99	16.91dB
19	25.01	17.08dB	25.01	17.08dB	25.28	17.05dB	25.01	17.08dB
20	25.10	17.07dB	25.10	17.07dB	20.35	17.52dB	25.10	17.07dB
Nilai rata2	**25.8765**	**17.0045dB**	**25.8765**	**17.0045dB**	**29.6325**	**17.045dB**	**25.8765**	**17.0045dB**

Pada steganografi dengan menggunakan metode DCT penulis mengambil kesimpulan sebagai berikut:

- Citra berekstensi PNG, BMP, dan JPG lossless tidak ada perbedaan ketika disisipi oleh pesan teks. Perbedaan muncul ketika citra stegano disimpan sebagai JPG.

- Metode DCT lebih mempunyai fleksibelitas dengan mampu menyimpan citra stego dalam format JPG.

- Citra cover yang akan digunakan pada metode DCT ini terbatas pada citra dengan ukuran berkelipatan 8.

- Format JPG lebih baik digunakan pada metode DCT ini dengan mempunyai nilai rata-rata PSNR 17.474775 ,yang lebih tinggi jika dibandingkan dengan citra format BMP dan PNG.

- Jumlah pesan yang dapat disembunyikan dengan menggunakan metode DCT lebih terbatas, dikarenakan setiap 1 bit yang akan disembunyikan menggunakan 64 pixel pada citra

- Panjang pesan tidak mempunyai pengaruh terhadap kuailtas citra stegano, dapat terlihat pada percobaan no 7, 9, 17 dan 19 pada tabel 4.2 dikarenakan semua pixel pada citra mengalami proses DCT.

- Citra yang dihasilkan oleh proses stegano dengan menggunakan metode DCT memiliki nilai MSE cukup tinggi dan PSNR yang rendah, hal ini dikarenakan semua pixel pada citra telah diproses menggunakan DCT.

Dari kedua metode yang diujikan, penulis dapat mengambil kesimpulan sebagai berikut:

- Citra yang menggunakan metode LSB mampu menyimpan lebih banyak pesan dari pada citra yang diproses menggunakan metode DCT.

- Semakin banyak pesan yang disembunyikan maka kualitas PSNR citra stegano yang diproses dengan menggunakan metode LSB semakin menurun.

- Citra stegano yang diproses dengan metode DCT dapat disimpan dengan format JPG, sehingga pengguna mempunyai lebih banyak pilihan format penyimpanan.

- Banyaknya pesan yang dapat disimpan dengan citra yang diproses dengan metode DCT terbatas, tetapi itu juga dapat menjadi kelebihan. Secara teori karena 1 bit disimpan pada 64 pixel citra, maka menjadi lebih tahan terhadap percobaan stegoanalysis.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah dilakukan penelitian dan pengujian sistem yang telah dibuat, dapat disimpulkan bahwa :

1. Citra yang menggunakan metode LSB mampu menyimpan lebih banyak pesan dari pada citra yang diproses menggunakan metode DCT, tetapi semakin banyak pesan yang disembunyikan maka kualitas PSNR citra stegano yang diproses dengan menggunakan metode LSB semakin menurun.

2. Metode DCT lebih mempunyai fleksibelitas dengan mampu menyimpan citra stego dalam format JPG. Karena mampu menyimpan dengan format JPG maka "*size*" dari citra stegano pun lebih kecil dari format BMP, PNG dan JPG lossless.

3. Secara umum citra yang diproses menggunakan metode LSB mempunyai nilai PSNR yang lebih baik dibandingkan dengan citra yang diproses dengan metode DCT.

4. Dari hasil pengujian menggunakan acuan PSNR yang dilakukan pada citra steganografi didapatkan bahwa citra steganografi format JPG mempunyai nilai rata-rata tertinggi dibandingkan format BMP, PNG dan JPG lossless. Adapun nilai rata-rata PSNR ketiga format citra steganografi yang diujikan nilainya belum melebihi 30, sehingga hasil citra steganografi ketiga format tersebut belum bisa dikatakan baik.

5.2. Saran

Untuk pengembangan lebih lanjut, saran yang dapat diberikan adalah sebagai berikut :

1. Banyaknya pesan yang dapat disimpan dengan citra yang diproses dengan metode DCT terbatas, tetapi itu juga dapat menjadi kelebihan. Secara teori karena 1 bit disimpan pada 64 pixel citra, maka menjadi lebih tahan terhadap percobaan stegoanalysis dari pada citra yang diproses dengan metode LSB.

2. Bagaimana kekuatan citra steganografi jika dilakukan perubahan fisik, di-"*resize*", di-"rotate" dan fungsi sejenis lainnya.

DAFTAR PUSTAKA

1. Bhattacharya, T., Dey, N., & Chaudhuri,B., S.R. (2012). A Session based Multiple Image Hiding Technique using DWT and DCT. International Journal of Computer Applications, 38 (5), 18-21.

2. Khayam,S.A. (2003). The Discrete Cosine Transform : Theory and Application. Retrieved April 8 ,2015, from www.lokminglui.com/DCT_TR802.pdf

3. Mulyanta, E.S. (2005). Menjadi Desainer Layout Andal dengan Adobe InDesign. Yogyakarta: ANDI. page. 175.

4. Nelson, M., & Gailly, J. (1996), The data compression Book, 2nd edition. New York: M &T Books

5. Rakhmat, B., Fairuzabadi,M.,M.Kom. (2010). Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4. Jurnal Dinamika Informatika, 5 (2)

6. Uma, R., (2011). FPGA Implementation of 2-D DCT for JPEG Image Compression. International Journal of Advanced Engineering Sciences and Technologies, 7 (1)

Lampiran

Contoh Proses Penyisipan Pesan dengan Metode LSB

Algoritma penyisipan pesan dapat dilihat di laporan utama Bab IV pada gambar 4.5

Misal:

- nilai teks yang disisipkan adalah 83 (01010011)
- nilai pixel Red adalah 224 (11100000)
- nilai pixel Green adalah 137 (10001000)
- nilai pixel Blue adalah 120 (01111000)

Langkah pertama yang akan dilakukan adalah proses AND terhadap nilai pixel Red,Green dan Blue yang kemudian akan mendapatkan nilai yang baru sebagai berikut:

- Red = 11100000
- Green = 10001000
- Blue = 01111000

Proses AND ini dilakukan untuk membuat nilai 3 bit terakhir dari pixel warna Red dan Green menjadi 000 dan Blue menjadi 00 yang berguna sebagai wadah untuk disisipi nilai teks

Setelah nilai Red, Green dan Blue yang baru didapatkan maka proses selanjutnya adalah melakukan penyisipan teks kedalam nilai - nilai pixel tersebut. Langkah – langkah yang akan dilakukan adalah dengan melakukan pengecekan terhadap nilai teks dengan nilai tertentu

- Pada proses pengecekan ke-1 nilai Red tidak mengalami perubahan
- Pada proses pengecekan ke-2 nilai Red mengalami perubahan menjadi 11100010
- Pada proses pengecekan ke-3 nilai Red tidak mengalami perubahan
- Pada proses pengecekan ke-4 nilai Green mengalami perubahan menjadi 10001100
- Pada proses pengecekan ke-5 nilai Green tidak mengalami perubahan
- Pada proses pengecekan ke-6 nilai Green tidak mengalami perubahan
- Pada proses pengecekan ke-7 nilai Blue mengalami perubahan menjadi 01111010
- Pada proses pengecekan ke-8 nilai Blue mengalami perubahan menjadi 01111011

Nilai pixel yang baru sebagai berikut:

- Red = 11100010 (226)
- Green = 10001100 (140)
- Blue = 01111011 (123)

Nilai yang didapat dari proses pengecekan tersebut merupakan nilai yang telah disisipi oleh nilai teks dan akan dikembalikan untuk menggantikan nilai pixel pada gambar.

Contoh Proses Ekstrasi Pesan dengan Metode LSB

Algoritma yang digunakan dapat terlihat di Bab IV pada gambar 4.6. Nilai yang akan digunakan merupakan nilai yang sama dengan nilai yang digunakan pada proses penyisipan dengan metode LSB

- nilai teks yang disisipkan adalah 83 (01010011)
- nilai pixel Red adalah 226 (11100010)
- nilai pixel Green adalah 140 (10001100)
- nilai pixel Blue adalah 123 (01111011)
- nilai teks adalah 0 (00000000)

Proses Ekstrasi akan mengambil nilai pixel warna dan melakukan proses pengecekan dengan nilai tertentu dan melakukan perubahan pada nilai teks jika ditemukan kecocokan. Langkah – langkah pengecekan yang akan dilakukan sebagai berikut:

- Pada proses pengecekan ke-1 nilai teks tidak mengalami perubahan
- Pada proses pengecekan ke-2 nilai teks mengalami perubahan menjadi 01000000
- Pada proses pengecekan ke-3 nilai teks tidak mengalami perubahan
- Pada proses pengecekan ke-4 nilai teks mengalami perubahan menjadi 01010000
- Pada proses pengecekan ke-5 nilai teks tidak mengalami perubahan
- Pada proses pengecekan ke-6 nilai teks tidak mengalami perubahan
- Pada proses pengecekan ke-7 nilai teks mengalami perubahan menjadi 01010010
- Pada proses pengecekan ke-8 nilai teks mengalami perubahan menjadi 01010011

Nilai teks yang baru adalah: 01010011 (83)

Setelah melalui proses pengecekan maka akan didapatkan nilai teks baru yang kemudian akan dikembalikan dan disusun menjadi pesan awal

Contoh Proses Penyisipan Pesan dengan Metode DCT

Algortima yang digunakan dapat terlihat pada Bab IV gambar 4.7. Proses penyisipan pada metode DCT ini akan mengambil contoh sebagai berikut:

Misal:

- Nilai bit yang akan disembunyikan adalah 0

- koordinat c1= [4.2]
- koordinat c2= [1.5]
- persistence = 100

Blok 8x8 pixel warna Red yang digunakan tampak pada gambar 1.

	1	2	3	4	5	6	7	8
1	215	215	215	216	216	217	217	217
2	216	216	216	216	216	217	217	217
3	216	216	216	216	216	216	216	217
4	215	215	215	216	216	216	216	216
5	215	215	215	215	215	215	215	215
6	215	215	215	215	215	215	215	215
7	216	216	216	216	215	215	215	215
8	216	216	216	216	216	216	217	217

Gambar 1.

Langkah pertama yang dilakukan adalah melakukan proses DCT pada blok gambar 1. Proses DCT akan mengubah nilai blok pada gambar 1 menjadi nilai yang tampak pada gambar 2.

	1	2	3	4	5	6	7	8
1	1.7259e+03	-1.7150	0.3943	-0.1750	0.1250	0.2460	-0.0280	-0.3939
2	1.7385	-1.9935	-0.0451	0.4849	-0.0143	-0.1345	0.2467	-0.3614
3	2.5291	-0.8530	0.5152	-0.0410	-0.2986	0.2841	-0.0366	-0.1007
4	-2.5869	0.2022	-0.4149	0.3708	-0.2371	0.1296	0.0532	-0.1594
5	-0.1250	-1.4372	-0.2590	0.3153	0.1250	0.1484	-0.2986	0.0218
6	-0.3648	0.2629	-0.5550	-0.0900	0.3549	0.1166	-0.0795	-0.2978
7	-0.1005	-0.6715	0.2134	-0.0917	0.2590	-0.2577	-0.0152	0.1709
8	-0.3005	0.9190	0.2265	-0.3655	0.0718	-0.1186	0.1466	0.0060

Gambar2.

Kemudian diambil nilai dari koordinat c1 dan koordinat c2 yaitu :

- c1= 0.2022
- c2= 0.1250

nilai akan dibandingkan dan ditukar jika syarat terpenuhi. Karena pada contoh ini nilai c1 lebih besar dari c2 dan nilai bit yang akan disembunyikan adalah 0 maka dilakukan pertukaran nilai antara c1 dan c2 menjadi :

- c1= 0.2022
- c2= 0.1250

Ketika nilai c1 dan c2 sudah dipastikan maka dilakukan proses selanjutnya yaitu melakukan pemisahan nilai sejauh 100(nilai persistence) hal ini dilakukan agar nilai yang telah dipilih tidak terlalu mengalami perubahan ketika dilakukan proses invers DCT

Nilai yang dikembalikan setelah dilakukan proses pemisahan menjadi:

- c1= -49.836417714522810
- c2= 50.163582285477200

lalu nilai tersebut dimasukkan kembali kedalam blok hasil DCT pada gambar 2 sehingga menghasilkan blok dengan nilai yang telah diubah seperti pada gambar 3.

	1	2	3	4	5	6	7	8
1	1.7259e+03	-1.7150	0.3943	-0.1750	50.1636	0.2460	-0.0280	-0.3939
2	1.7385	-1.9935	-0.0451	0.4849	-0.0143	-0.1345	0.2467	-0.3614
3	2.5291	-0.8530	0.5152	-0.0410	-0.2986	0.2841	-0.0366	-0.1007
4	-2.5869	-49.8364	-0.4149	0.3708	-0.2371	0.1296	0.0532	-0.1594
5	-0.1250	-1.4372	-0.2590	0.3153	0.1250	0.1484	-0.2986	0.0218
6	-0.3648	0.2629	-0.5550	-0.0900	0.3549	0.1166	-0.0795	-0.2978
7	-0.1005	-0.6715	0.2134	-0.0917	0.2590	-0.2577	-0.0152	0.1709
8	-0.3005	0.9190	0.2265	-0.3655	0.0718	-0.1186	0.1466	0.0060

Gambar 3.

Blok pada gambar 3 kemudian akan dilakukan proses invers DCT yang akan mengembalikan nilai blok menjadi mendekati nilai blok asal seperti pada gambar 4.

	1	2	3	4	5	6	7	8
1	211.0533	200.0967	202.9665	220.2256	224.2840	216.5239	219.3936	233.4564
2	224.6484	211.7744	211.1011	222.7309	221.7787	209.3893	208.7160	220.8612
3	234.2883	219.9467	216.5616	224.6484	219.8612	202.9287	199.5436	211.2213
4	228.0713	214.5239	212.6064	223.6107	220.8989	205.8840	203.9665	215.4384
5	214.4384	202.9665	204.8840	219.8989	222.6107	212.6064	214.5239	228.0713
6	209.2213	198.5436	201.9287	218.8612	223.6484	215.5616	218.9467	233.2883
7	219.8612	207.7160	208.3893	221.7787	221.7309	210.1011	210.7744	223.6484
8	232.4564	218.3936	215.5239	224.2840	220.2256	203.9665	202.0967	213.0533

Gambar 4.

Blok hasil invers DCT tersebut selanjutnya akan dilakukan proses konversi menjadi integer 8 bit sehingga hasil akhir dapat terlihat pada gambar 5.

	1	2	3	4	5	6	7	8
1	211	200	203	220	224	217	219	233
2	225	212	211	223	222	209	209	221
3	234	220	217	225	220	203	200	211
4	228	215	213	224	221	206	204	215
5	214	203	205	220	223	213	215	228
6	209	199	202	219	224	216	219	233
7	220	208	208	222	222	210	211	224
8	232	218	216	224	220	204	202	213

Gambar 5.

Proses penyisipan dilakukan berulang sampai semua nilai bit disembunyikan atau ketika sudah tidak ada blok untuk menyembunyikan.

Contoh Proses Ekstraksi Pesan dengan Metode DCT

Algortima yang digunakan dapat terlihat pada Bab IV gambar 4.8. Nilai yang akan digunakan merupakan nilai yang sama dengan nilai yang digunakan pada proses penyisipan dengan metode DCT

Langkah pertama ambil blok yang akan dilakukan proses DCT ,blok yang digunakan tampak pada gambar 5 hasil dari DCT dari gambar 5, akan tampak pada gambar 6.

	1	2	3	4	5	6	7	8
1	1.7264e+03	-1.7150	-0.2590	-0.1750	49.6250	0.2460	-0.2986	-0.3939
2	1.7385	-1.6082	-0.0451	0.6202	-0.0143	0.1016	0.2467	-0.4380
3	1.8758	-0.8530	1.0152	-0.0410	-0.0280	0.2841	0.4634	-0.1007
4	-2.5869	-49.8836	-0.4149	0.9475	-0.2371	-0.2556	0.0532	-0.4860
5	-0.6250	-1.4372	-0.5296	0.3153	-0.3750	0.1484	0.3547	0.0218
6	-0.3648	0.5896	-0.5550	0.0247	0.3549	0.0400	-0.0795	-0.6348
7	-0.3711	-0.6715	-0.2866	-0.0917	-0.3943	-0.2577	0.4848	0.1709
8	-0.3005	0.3423	0.2265	-0.3503	0.0718	0.0167	0.1466	0.1207

Gambar 6.

Kemudian ambil nilai dari koordinat c1 dan c2 pada gambar 6 yang akan didapatkan nilai sebagai berikut:

- c1: -49.8836
- c2: 49.6250

Nilai dari c1 dan c2 akan dibandingkan, jika nilai c1 lebih besar maka akan didapat nilai bit =1, dan sebaliknya jika nilai c2 lebih besar maka nilai bit=0. Proses ini dilakukan berulang sampai semua nilai bit disembunyikan diekstraksi.