ABSTRAK

PERBANDINGAN METODE *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT* (AMELSBR) DAN *DISCRETE COSINE TRANSFORM* (DCT) UNTUK STEGANOGRAFI CITRA DIGITAL

Oleh

FAJAR SIDIK

Penyisipan pesan rahasia dengan steganografi merupakan salah satu cara untuk menyembunyikan data rahasia sampai dengan aman ke penerima. Pada penelitian ini, peneliti membandingkan metode AMELSBR dan DCT pada steganografi berbasis aplikasi web, dengan media penampung berupa gambar dengan format file (.png), sebagai *input (cover)* dan output *(stegoimage)* serta data yang dapat disisipkan berupa berkas dengan format file (.txt). Kesimpulan yang didapat dari penelitian ini adalah metode AMELSBR lebih baik dibandingkan metode DCT untuk ketahanan media *stegoimage* pada pengujian manipulasi *brightness, contrast*, dan *cropping*. Metode AMELSBR merupakan metode yang lebih tahan terhadap manipulasi perubahan *brightness, contrast*, serta pemotongan *(cropping) stegoimage* dibandingkan dengan metode DCT. Ini terlihat dari hasil dari manipulasi yang dilakukan peneliti terhadap kedua metode dimana kedua metode lebih mempunyai resiko kehilangan data paling kecil di media gambar yang dominan warna hitam/putih dan area pemotongan di kanan dan bawah berdasarkan skala pemotongan dan resolusi gambar *stegoimage*.

Kata Kunci: AMELSBR, DCT, Steganografi.

ABSTRACT

THE COMPARISON BETWEEN ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT (AMELSBR) AND DISCRETE COSINE TRANSFORM (DCT) FOR DIGITAL IMAGE STEGANOGRAPHY

By

FAJAR SIDIK

Insertion of secret messages with steganography is one way to hide secret messages. In this research we will compare AMELSBR and DCT methods based on web application using image as the media for hiding the secret message. The file format used are (.png) as input cover and stegoimage, and (.txt) as data inserted. The result shows that AMELSBR method better than DCT method for manipulation of brightness, contrast, and cropping.

Keywords : amelsbr, dct, steganography.

Judul Skripsi	: **PERBANDINGAN METODE *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT* (AMELSBR) DAN *DISCRETE COSINE TRANSFORM* (DCT) UNTUK STEGANOGRAFI CITRA DIGITAL**
Nama Mahasiswa	: Fajar Sidik
Nomor Pokok Mahasiswa	: 1017032023
Jurusan	: Ilmu Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Dra. Wamiliana, M.A., Ph.D.
NIP 19631108 198902 2 001

Febi Eka Febriansyah, M.T.
NIP 19800219 200604 1 001

2. Ketua Jurusan Ilmu Komputer

Dr. Ir. Kurnia Muludi, M.S.Sc.
NIP 19640616 198902 1 001

MENGESAHKAN

1. Tim Penguji

Ketua : **Dra. Wamiliana, M.A., Ph.D.** .....

Sekretaris : **Febi Eka Febriansyah, M.T.** .....

Penguji
Bukan Pembimbing : **Tristiyanto, S.Kom., M.I.S., Ph.D.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Prof. Warsito, S.Si., D.E.A., Ph.D.
NIP 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : **29 September 2017**

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul "Perbandingan metode *Adaptive Minimum Error Least Significant Bit Replacement* (AMELSBR) dan *Discrete Cosine Transform (DCT)* pada Steganografi Citra Digital" merupakan karya saya sendiri dan bukan karya orang lain. Semua tulisan yang tertuang di skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila dikemudian hari terbukti skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, 29 September 2017

Fajar Sidik
NPM. 1017032023

RIWAYAT HIDUP

Penulis dilahirkan pada tanggal 21 Januari 1993 di Panjang, Bandar Lampung sebagai anak ketiga dari tiga bersaudara dari Ayah yang bernama (alm) Hi. Dahrial dan Ibu yang bernama Hj. Mairi S.Pd.

Penulis menyelesaikan pendidikan formal pertama kali di TK Kartika pada tahun 1998, kemudian melanjutkan pendidikan dasar yang berpindah pindah sekolah karena mengikuti ayahnya dinas di Lampung dan Jambi. Sekolah Dasar pertamanya yakni SDN 2 Panjang Utara. Setelah pindah ke Jambi, penulis melanjutkan pendidikan di SD Adhyaksa Jambi, lalu pindah lagi ke Bandar Lampung dengan melanjutkan 6 bulan di SD Al-Azhar 2 untuk melaksanakan Ujian Nasional dan selesai pada tahun 2004. Pendidikan menengah pertama di SMP Al-Kautsar Bandar Lampung yang diselesaikan pada tahun 2007, kemudian melanjutkan ke pendidikan menengah atas di SMA Al-Kautsar yang diselesaikan penulis pada tahun 2010.

Pada tahun 2010 penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Selama menjadi mahasiswa beberapa kegiatan yang dilakukan penulis antara lain:

1. Pada bulan Januari 2013 penulis melaksanakan kerja praktek di LP2S.

2. Pada bulan Juli 2013 penulis melaksanakan Kuliah Kerja Nyata (KKN) di Desa Purworejo, Kecamatan Pasir Sakti, Kabupaten Pesisir Barat.

MOTO

“Baik dan buruk, yang terpenting adalah bertumbuh”

Fajar Sidik

Persembahan

Dengan segala kerendahan hati sebuah skripsi yang sederhana ini kupersembahkan untuk yang teramat kucintai

Ibuku Hj. Mairi S.Pd. dan (alm) Hi. Dahrial

Terima kasih mama untuk tetap jadi kepala rumah tangga yang hebat setelah ayah sudah tiada.

Untuk almarhum ayah, kudoakan ayah dapat menikmati surga dan rahmat-Nya,

Kakak-kakakku, terima kasih..

Untuk menjaga adikmu ini yang terkadang menjengkelkan.

Untuk Ilmu Komputer angkatan 2010 , Keluarga yang berjuang bersama untuk menuju wisuda,

Serta almamater tercinta,

Universitas Lampung

SANWACANA

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa atas segala berkat, rahmat, cinta kasih, bimbingan, perlindungan dan pertolongan-Nya sehingga penulis dapat menyelesaikan skripsi ini.

Skripsi ini disusun sebagai syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Ilmu Komputer Universitas Lampung. Penyelesaian skripsi ini tidak terlepas dari bantuan banyak pihak yang membantu baik secara materi, moril, saran, dan bimbingan. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Ibu dan almarhum ayahku, serta kedua kakakku yang selalu memberi dukungan berupa doa dan motivasi.
2. Ibu Dra. Wamiliana, M.A., Ph.D sebagai pembimbing utama, yang telah membimbing penulis dan memberikan ide, kritik serta saran sehingga penulisan skripsi ini dapat diselesaikan.
3. Bapak Febi Eka Febriansyah, M.T. sebagai pembimbing kedua, yang telah memberikan saran, bantuan, dan membimbing penulis sehingga penulisan skripsi ini dapat diselesaikan.
4. Bapak Tristiyanto, S.Kom., M.I.S., P.Hd. sebagai pembahas, yang telah memberikan masukan yang bermanfaat dalam perbaikan skripsi ini.
5. Bapak Prof. Warsito, S.Si.,D.E.A.,Ph.D selaku Dekan FMIPA Universitas Lampung.

6. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc selaku Ketua Jurusan Ilmu Komputer dan Bapak Didik Kurniawan, S.Si., MT selaku Sekretaris Jurusan Ilmu Komputer FMIPA Universitas Lampung.
7. Ibu Anie Rose Irawati, S.T., M.Cs. selaku Pembimbing Akademik, serta Bapak dan Ibu Dosen Jurusan Ilmu Komputer yang telah memberikan ilmu dan pengalaman dalam hidup untuk menjadi lebih baik.
8. Kawan-kawan seperjuangan: Pita Utari, M. Harry Haryono, Togu, Herman, Gilang, Irul, Beny, Febra dan seluruh keluarga Ilmu Komputer 2010.
9. Ibu Ade Nora Maela dan Mas Irsan yang telah membantu segala urusan administrasi dan Mas Ardi Novalian yang telah membukakan MIPA Terpadu dan ruang baca serta menyiapkan ruang seminar dan Mbak Lia yang memberi motivasi dan semangat dalam pengerjaan skripsi.

Penulis menyadari bahwa laporan ini masih jauh dari kata sempurna. Secara pribadi penulis mohon maaf yang sebesar-besarnya atas segala kekurangannya. Besar harapan agar skripsi ini dapat berguna bagi penulis dan semua pembacanya

Bandar Lampung, 29 September 2017

Penulis

Fajar Sidik

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Media digital sekarang adalah media yang lumrah digunakan saat ini. Dengan perkembangannya yang semakin pesat, media digital telah memudahkan seseorang untuk berinteraksi dengan orang lain. Media juga banyak rupanya, dapat berupa surat, gambar, video atau suara sekalipun. Keuntungan menggunakan media saat ini ialah mempercepat pengerjaan suatu hal seperti halnya mahasiswa mengerjakan skripsi. Dulu skripsi dikerjakan dengan mesin tik dan apabila terjadi kesalahan maka harus ditulis ulang kembali dan tidak bisa dihapus dengan manual menggunakan alat penghapus seperti *tipe-x*. Sekarang, alat mesin tik mulai ditinggalkan dan beralih ke penggunaan komputer.

Terdapat masalah seiring dengannya perkembangan pesat media dan teknologi saat ini yakni amankah pengiriman data yang berlangsung saat ini. Mungkin saja dengan ada internet seperti saat ini seseorang dapat mengambil data atau pekerjaan seseorang dengan pura pura menjadi *client* palsu suatu perusahaan. Dengan itu, informasi rahasia yang seharusnya tidak boleh dilihat oleh sembarang orang dapat dilhat orang yang mencuri tersebut dan digunakan dengan tidak bertanggung jawab. Oleh karena itu, diperlukan suatu cara agar pesan rahasia

dapat dikirimkan dengan aman salah satunya dengan teknik steganografi. Steganografi adalah satu teknik penyembunyian pesan pada suatu media misalnya media berupa gambar, suara dan yang lainnya.

Pada penelitian ini akan dibandingkan dua metode yaitu metode AMELSBR (*Adaptive Minimum Error Least Significant Bit Replacement*) dan DCT (*Discrete Cosine Transform*). Untuk AMELSBR, sifat metode ini beradaptasi dengan media yang digunakan untuk menyembunyikan datanya. Karakteristik lokal pada media yang menampung teks tadi tidak diubah secara signifikan sehingga dengan kasat mata media tersebut hanyalah sebuat media yang biasa digunakan. Untuk AMELSBR, penulis merujuk ke penelitian dari Panditatwa (2015) tentang Implementasi Teknik Steganografi Menggunakan Metode AMELSBR. Panditatwa (2015) dalam penelitiannya membuat aplikasi berbasis web yang dapat melakukan *embedding* dan ekstraksi *stegoimage* dengan media gambarnya memakai format file .jpg dan input file berkasnya berupa .txt. Pada penelitian ini *source code* AMELSBR yang digunakan adalah *source code* yang dibuat oleh Panditatwa (2015) dengan melakukan pergantian file cover dari .jpg/jpeg ke .png. Sedangkan DCT, metode ini pada dasarnya akan merepresentasikan suatu citra menjadi jumlahan dari gelombang sinusoidal yang berbeda frekuensi dan magnitudo. DCT juga sering digunakan sebagai kompresi citra. Transformasi ini digunakan sebagai dasar pengembangan kompresi JPEG yang sudah sering digunakan pada saat ini.

Pada penelitian ini akan digunakan gambar dengan jenis file .png, *output stego image* berupa berkas gambar tadi dengan data yang telah disisipkan berupa file .txt. Jenis berkas input berupa file .png dan *output stego image* juga berupa file

.png karena jenis file menggunakan kompresi yang rendah yang dapat mengurangi *noise* pada gambar saat file .txt sudah disisipkan.

Implementasi penelitian aplikasi steganografi ini berbasis *web* karena pengguna dapat mudah menggunakan komputer atau laptop sehingga data rahasia yang akan dikirim tadi dapat mudah diproses menjadi *stego image* dan bagi penerima data rahasia ini bisa mengekstrak data untuk dimunculkan kembali dengan cepat menggunakan aplikasi ini dan nantinya dapat dikembangkan sesuai kebutuhan pengguna.

1.2 Rumusan masalah

Rumusan masalah yang diselesaikan yakni bagaimana hasil perbandingan antara metode AMELSBR (*Adaptive Minimum Error Least Significant Bit Replacement*) dengan DCT (*Discrete Cosine Transform*) pada teknik Steganografi.

1.3 Batasan masalah

Agar ruang lingkup yang dibahas menjadi terarah dan tersusun dengan baik dan sesuai maka batasan masalah di penelitian ini adalah :

1. Media yang digunakan adalah gambar yang berupa file .png sebagai *input* dan *output* serta berkas pesan dalam bentuk .txt.
2. Implementasi teknik ini tidak menggunakan *stego key*.
3. Aplikasi ini mengunakan dua metode *steganografi* yakni AMELSBR dan DCT yang nantinya akan dibandingkan antara keduanya yang basisnya berupa *web* dengan bahasa pemrograman PHP

4. Ada beberapa elemen yang dibandingkan yakni membandingkan besar ukuran file setelah proses *embedding*, *running time*, histogram, dan keutuhan isi teks saat dilakukannya manipulasi pada gambar seperti *brightness*, *contrast*, dan *cropping*

1.4 Tujuan

Tujuan penelitian ini adalah untuk :

1. Membandingkan Metode *Adaptive Minimum Error Least Significant Bit Replacement* (AMELSBR) dan *Discrete Cosine Transform* (DCT)
2. Menguji kedua metode tersebut dengan melakukan *contrast*, *brightness*, dan *cropping* terhadap *stego image*

1.5 Manfaat

Manfaat yang diperoleh di penelitian ini adalah :

1. Data rahasia yang dikirim dapat sampai aman ke pihak yang dituju.
2. Data rahasia tidak digunakan oleh sembarang orang karena tersimpan ke *stego image* yang secara kasat mata seperti gambar biasa.
3. Pengirim mudah untuk membuat *stego image* untuk menyimpan data rahasia.
4. Penerima pesan rahasia dapat mengekstrak *file* rahasia yang sesuai dengan yang dibuat pengirim.

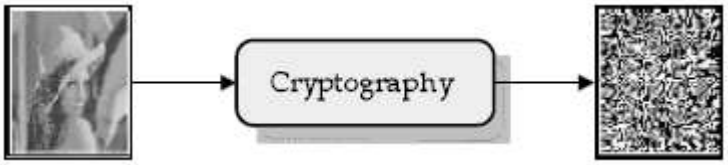
BAB II

TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi yaitu teknik pengenkripsian pesan. Namun teknik ini dapat menimbulkan kecurigaan karena pesan acak tidak memiliki makna secara kasat mata, sehingga mudah dicurigai (Iza, 2013).

Menurut Munir (2006), kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*message).* Kriptografer adalah praktisinya (pengguna kriptografi). Algoritma teknik kriptografi adalah aturan untuk enkripsi dan deskripsi dimana enkripsi adalah proses penyandian *plain text* atau pesan menjadi *ciphertext* (*enchiphering*) dan deskripsi adalah proses pengembalian *cipherteks* menjadi *plain text* (*deciphering)* (Munir, 2006). Ilustrasi kriptografi disajikan pada Gambar 2.1.



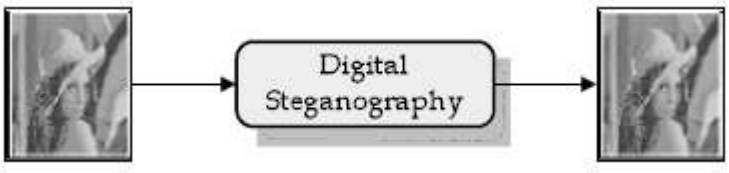
Gambar 2.1 Kriptografi (Prayudi dan Kuncoro, 2005).

2.2 Steganografi

Steganography (steganografi) merupakan seni untuk menyembunyikan pesan rahasia kedalam pesan lainnya sedemikian rupa sehingga membuat orang lain tidak menyadari adanya sesuatu di dalam pesan tersebut. Kata *Steganography* berasal dari bahasa Yunani, yaitu gabungan dari kata *steganos* (tersembunyi atau terselubung) dan *graphein* (tulisan atau menulis), sehingga makna *Steganography* kurang lebih bisa diartikan sebagai menulis tulisan yang tersembunyi (Sellars, 2006).

Steganografi digital memiliki dua properti dasar yaitu media penampung (*cover data* atau *data carrier*) dan data digital yang akan disisipkan (*secretdata*), dimana media penampung dan data digital yang akan disisipkan dapat berupa file multimedia (teks/dokumen, citra, audio maupun video). Terdapat dua tahapan umum dalam steganografi digital, yaitu proses *embedding* atau *encoding* (penyisipan) dan proses *extracting* atau *decoding* (pemekaran atau pengungkapan kembali (*reveal*). Hasil yang didapat setelah proses *embedding* atau *encoding* disebut *stego object* (apabila media penampung hanya berupa data citra maka

disebut s*tego image*) (Prayudi dan Kuncoro, 2005). Ilustrasi steganografi disajikan pada Gambar 2.2.



Gambar 2.2 Steganografi (Prayudi dan Kuncoro, 2005).

Provos dan Honeyman (2003) mendefinisikan steganografi adalah ilmu dan seni menyembunyikan dalam komunikasi. Sistem steganografi ini menyisipkan konten pada suatu media tanpa menimbulkan kecurigaan. Pada dasarnya, proses informasi-bersembunyi dalam sistem steganografi dimulai dengan mengidentifikasi *bit* yang berlebihan pada media penutup (dapat dimodifikasi tanpa merusak integritas medium). Proses penyisipan menciptakan media stego dengan mengganti bit-bit yang berlebihan dengan data dari disembunyikan yaitu pesan. Tujuan modern steganografi adalah untuk menjaga data rahasia tidak terdeteksi dengan media penutup *(cover).* Media tersebut dapat terlihat perbedaannya dengan menemukan distorsi pada media, proses menemukan distorsi ini disebut *steganalysis statistik.* (Provos dan Honeyman, 2003).

2.2.1 Kriteria *Steganografi*

Kriteria *steganografi* menurut Munir (2004) adalah :

1. *Fidelity*. Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia, *stego object* dalam kondisi yang masih terlihat baik dan pengamat tidak mengetahui kalau di dalam citra tersebut ada data rahasianya.
2. *Robustness*. Data rahasia yang disembunyikan harus tahan *(robust)* terhadap berbagai operasi manipulasi atau *editing* pada media penampung. Apabila pada media penampung dilakukan operasi manipulasi atau *editing*, maka data tetap valid atau tidak rusak.
3. *Recovery*. Data yang disembunyikan harus dapat di ungkapkan kembali *(reveal)*, karena dikaitkan dengan tujuan dari steganografi digital itu sendiri yaitu *data* sewaktu-waktu data rahasia di dalam media penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.3 Citra *Digital*

Citra atau gambar dapat didefinisikan sebagai sebuah fungsi yang terdiri dari dua variabel f(x,y), dengan x dan y adalah koordinat bidang datar, dan harga fungsi f disetiap pasangan koordinat (x,y) disebut intensitas atau *level* keabuan (*grey level)* dari gambar dititik itu. Jika x,y dan f semuanya berhingga (*finite),* dan nilainya diskrit, maka gambarnya disebut citra digital (gambar *digital*). Suatu citra digital terdiri dari sejumlah elemen berhingga, dimana masing-masing mempunyai lokasi dan nilai tertentu. Elemen-elemen ini disebut sebagai *picture element,*

image element, *pels* atau *pixels* (Hermawati, 2013). Purnomo dan Muntasa (2010) menjelaskan bahwa nilai dari intensitas bentuknya atau *level* keabuan adalah diskrit mulai dari 0 sampai 255. Citra yang ditangkap oleh kamera dan telah dikuantisasi dalam bentuk nilai diskrit disebut dengan citra *digital* (*digital image*)

2.3.1 Jenis *File* Citra *Digital*

Bermacam-macam jenis file citra *digital* yaitu jpg/jpeg, png, gif, tiff dan lain sebagainya mempunyai ciri-ciri, karakteristik, keunggulan dan kelemahan dibagiannya. Disetiap jenis *filedigital* terdapat kompresi atau dapat diartikan sebagai proses reduksi jumlah data yang diperlukan untuk menyatakan suatu jumlah informasi yang diberikan (Hermawati, 2013).

Teknik-teknik kompresi data dapat dibagi menjadi 2 yaitu (Widhiartha, 2008) :

1. *lossy compression.*

Lossy compression menyebabkan adanya perubahan data dibandingkan sebelum dilakukan proses kompresi. Sebagai gantinya *lossy compression* memberikan derajat kompresi lebih tinggi. Tipe ini cocok untuk kompresi file suara digital dan gambar digital. File suara dan gambar secara alamiah masih bisa digunakan walaupun tidak berada pada kondisi yang sama sebelum dilakukan kompresi.

2. *lossless compression.*

Sebaliknya *Lossless Compression* memiliki derajat kompresi yang lebih rendah tetapi dengan akurasi data yang terjaga antara sebelum dan sesudah proses kompresi. Kompresi ini cocok untuk basis data, dokumen atau *spreadsheet*. Pada

lossless compression ini tidak diijinkan ada bit yang hilang dari data pada proses kompresi.

Jenis-jenis file citra digital (Ichsan, 2011).

1. JPG/JPEG (*Joint Photographic Experts Group).*

   Joint Photographic Experts Group (JPEG) adalah format gambar yang banyak digunakan untuk menyimpan gambar-gambar dengan ukuran lebih kecil.

   Beberapa karakteristik gambar JPEG adalah sebagai berikut :

   - Memiliki ekstensi .jpg atau .jpeg.
   - Mampu menayangkan warna dengan kedalaman 24-bit *true color*.
   - Mengkompresi gambar dengan sifat *lossy*.

2. PNG (*Portable Network Graphics).*

   PNG (*Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut (*lossless compression*). PNG dibaca "ping", namun biasanya dieja apa adanya untuk menghindari kerancuan dengan istilah "ping" pada jaringan komputer. Format PNG ini diperkenalkan untuk menggantikan format penyimpanan citra GIF. Secara umum PNG dipakai untuk Citra Web.

2.3.2 Konsep Citra Warna (*True Color)*

Setiap *pixel* pada citra warna yang merupakan kombinasi dari tiga warna dasar (RGB=*Red Green Blue)*. Setiap warna dasar menggunakan penyimpanan 8 bit = 1 *byte*, yang berarti setiap warna mempunyai gradasi sebanyak 255 warna. Berarti setiap *pixel* mempunyai kombinasi warna sebanyak 16 juta warna lebih. Itulah sebabnya format ini dinamakan *true color* karena mempunyai jumlah warna yang cukup besar sehingga bisa dikatakan hampir mencakup semua warna di alam.

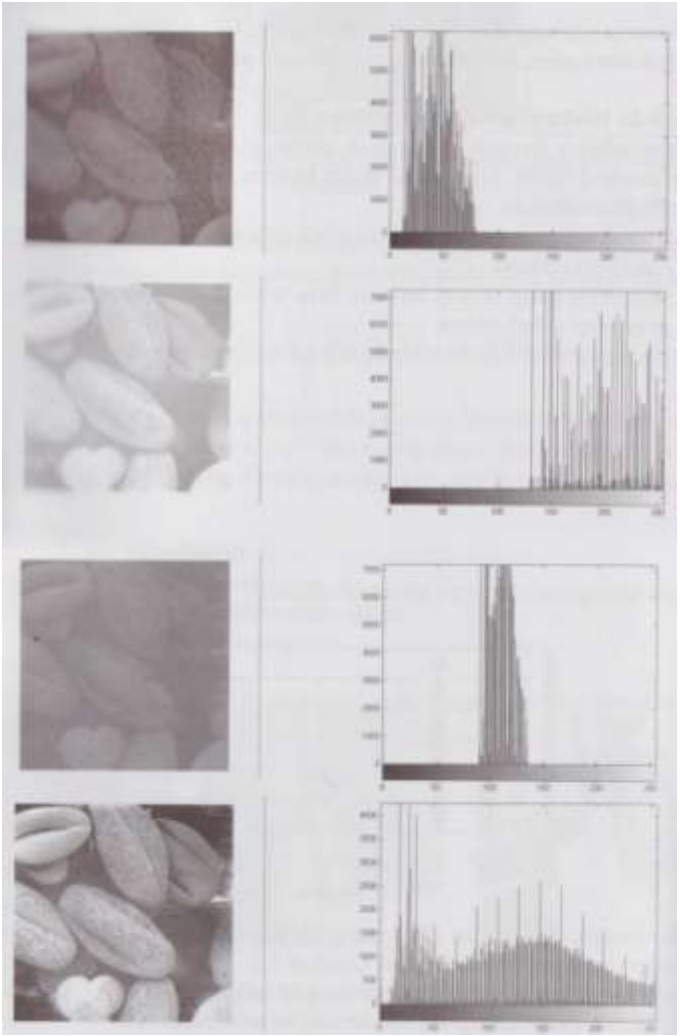
Penyimpanan citra *true color* di dalam memori berbeda dengan citra *grayscale*. Setiap *pixel* dari citra *grayscale* 256 gradasi warna diwakili oleh 1 *byte*. Sedangkan 1 *pixel* citra *true color* diwakili oleh 3 *byte*, dimana masing-masing *byte* mempresentasikan warna merah (*Red*), hijau (*Green*), dan biru (*Blue*) (Widhiartha, 2008).

2.3.3 Histogram

Histogram adalah diagram yang menunjukan jumlah kemunculan nilai *grey level (*kecerahan) pada suatu citra, dimana sumbu-x dari diagram ini menggambarkan nilai *grey level (*Kecerahan) dan sumbu-y mewakili jumlah kemunculan *grey level (*kecerahan) tertentu. Ada 4 tipe dasar citra yang dapat digambarkan dengan histogram yaitu (Hermawati, 2013) :

- Citra gelap: histogram cenderung ke sebelah kiri
- Citra terang: histogram cenderung ke sebelah kanan
- Citra *low contrast*: histogram mengumpul disuatu tempat
- Citra *high contrast*: histogram merata disemua tempat

Histogram pada citra digital disajikan pada Gambar 2.3.



Gambar 2.3 Tipe Dasar Histogram (Hermawati, 2013).

2.4 Teks Sederhana (*Plain Text)*

Format data teks (.txt) merupakan contoh format teks yang paling popular. Saat ini, perangkat lunak yang paling banyak digunakan untuk memanipulasi format data ini adalah Notepad. Format data teks (.txt) adalah format teks yang digunakan untuk menyimpan huruf, angka, karakter kontrol (tabulasi, pindah baris, dan sebagainya) atau simbol-simbol lain yang biasa digunakan dalam

tulisan seperti titik, koma, tanda petik, dan sebagainya. Satu huruf, angka, karakter kontrol atau simbol pada arsip teks memakan tempat satu byte. Berbeda dengan jenis teks terformat (.doc) yang satu huruf saja dapat memakan tempat beberapa byte untuk menyimpan format dari huruf tersebut seperti font, ukuran, tebal atau tidak dan sebagainya. Kelebihan dari format data teks ini adalah ukuran datanya yang kecil karena tidak adanya fitur untuk memformat tampilan teks (Purnomo dan Zacharias, 2005).

2.5 Manipulasi Citra Gambar

2.5.1 *Brightness*

Brightness adalah atribut dari persepsi visual di mana sumber tampaknya memancar atau mencerminkan jumlah tertentu cahaya. Kecerahan sering menentukan apakah sebuah benda dapat dilacak atau tidak karena paparan tingkat (jumlah cahaya) - apa yang dapat dilihat dan apa yang tidak bisa. Tingkat kecerahan yang tepat adalah yang paling penting saat mengambil gambar video sehingga objek tersebut benar ditampilkan dan dapat dilacak. (Carellas, 2010)

Sebuah citra dengan derajat keabuan 256, akan tampak gelap jika seluruh komponen warna berada mendekati 0. sebaliknya, citra akan tampak terang jika seluruh komponennya mendekati angka 255.

Brightness adalah proses untuk kecerahan citra, jika intensitas pixel dikurangi dengan nilai tertentu maka citra akan menjadi lebih gelap, dan sebaliknya jika intensitas pixelnya ditambah dengan nilai tertentu maka akan lebih terang

2.5.2 *Contrast*

Contrast adalah properti visual obyek yang memisahkannya dari benda-benda lain dalam gambar video. Kontras suatu benda dengan latar belakang gambar video penting untuk dua fungsi: mengidentifikasi sebuah objek dan kemudian melacaknya. Dalam rangka untuk memiliki objek yang dapat dilihat bahwa masing-masing dapat dicatat dengan baik dan dilacak, tingkat kontras yang benar harus dimanfaatkan untuk membedakan satu objek dari yang lain. (Carellas, 2010)

Didalam ilmu Fotografi *Contrast* adalah perbedaan gradasi,kecerahan, atau nada (warna) antara bidang gelap (shadow) dengan bidang terang, atau warna putih yang mencolok sekali pada suatu objek.

2.5.3 *Cropping*

Cropping adalah pemgambilan suatu bagian pada gambar. Dengan cropping, kita dapat menghilangkan suatu bagian tertentu pada gambar yang tidak kita inginkan, atau hanya sekedar mengambil suatu bagian tertentu dengan ukuran tertentu saja (Wijaya, 2006)

Praktik *cropping* foto sudah dilakukan sejak awal mula fotografi. Sejak kamera masih manual dan film masih dalam bentuk lembaran-lembaran kaca cropping sudah dilakukan. Banyak foto-foto yang jadi icon (iconik) dan terkenal adalah hasil *cropping*. Tujuan Memotong Foto (*Cropping*) adalah untuk mendapatkan foto dengan komposisi yang lebih enak dilihat atau agar objek terlihat lebih dekat.

2.6 Metode AMELSBR

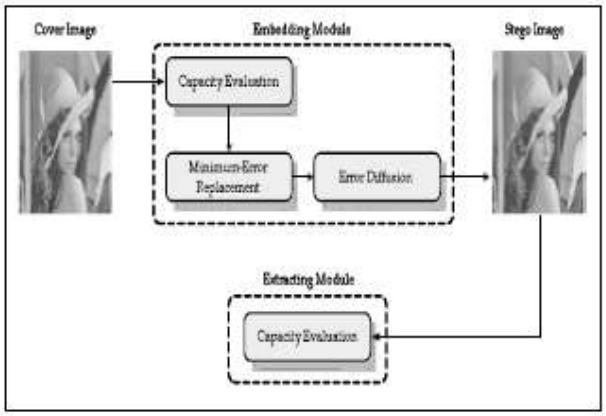
Metode ini pertama kali diperkenalkan oleh Lee dan Chen (1999). Lee dan Chen menerapkan citra hitam-putih *(grayscale image)*sebagai media penampung *(cover image)* dan kemudian Gan (2003) mengimplementasikan metode ini dengan citra berwarna *24 bit (true colors image)* sebagai media penampungnya.

Dari hasil penelitian tersebut ternyata metode ini menawarkan beberapa kelebihan dibandingkan dengan metode LSB, yaitu *bit* data rahasia yang akan disisipkan lebih banyak (pada metode LSB umumnya hanya 1 *bit*) tanpa menimbulkan banyak perubahan pada media penampung (dalam hal ini adalah data citra). Dengan metode ini, setiap *pixel* memiliki kapasitas penyembunyian yang berbeda-beda tergantung dari nilai toleransi *pixel* tersebut terhadap proses modifikasi atau penyisipan. Suatu *pixel* pada data citra bisa dikatakan dapat ditoleransi apabila dilakukan proses modifikasi (penyisipan) dengan skala yang tinggi terhadap nilainya adalah memungkinkan tanpa merubah tampak asli dari data citra tersebut, atau dengan kata lain area yang halus dan solid pada suatu data citra memiliki kadar toleransi yang rendah (*less tolerant*) terhadap proses modifikasi dibandingkan dengan area yang memiliki tekstur yang kompleks (Gan, 2003).

Metode *AMELSBR* yang diterapkan pada citra berwarna (*jpg/jpeg 24-bit*) memiliki beberapa langkah atau tahapan utama untuk melakukan proses penyisipan, antara lain *Capacity Evaluation,*MER dan *Error Diffusion* (Gan, 2003). Untuk proses pengungkapan, tahapan yang dilakukan yaitu *Capacity Evaluation* (Lee dan Chen, 1999).

Sebelum dilakukan proses penyisipan, maka langkah pertama yang harus dilakukan adalah mengevaluasi kapasitas penyisipan *(capacity evaluation)* dan mencari nilai *color variation*. Kemudian setelah mendapatkan nilai *color variation*, nilai tersebut diproses kembali untuk mendapatkan kapasitas penyisipan sejumlah *K-bit*. Setelah itu, untuk beradaptasi dengan karakteristik lokal *pixel*, maka sejumlah *K-bit* tersebut ditangani dengan proses evaluasi kapasitas (*capacity evaluation*).

Proses selanjutnya adalah mencari *MER*, dimana proses ini akan menentukan apakah *bit* ke *K+1* akan dilakukan perubahan atau tidak, dan yang akan menentukan itu adalah berdasarkan pada nilai *embedding error (Er)*. Proses tersebut disajikan pada Gambar 2.4.

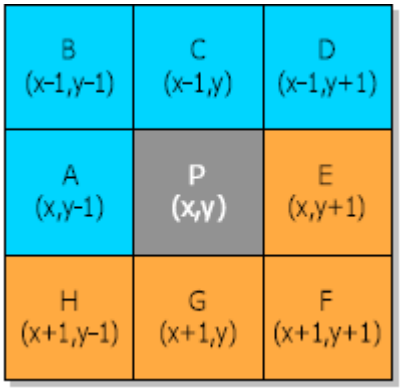


Gambar 2.4 Gambaran Umum Metode AMELSBR (Gan, 2003).

Proses penyisipan *(embedding)* di dalam metode AMELSBR, prosesnya tidak sama dengan metode LSB. Apabila proses penyisipan di dalam metode LSB dilakukan langsung per *pixel* pada *byte*-nya, dimana 1 *bit* terakhir (LSB) per *byte*-nya diganti dengan 1 *bit* data rahasia yang akan disisipkan, tetapi tidak dengan

metode AMELSBR. Di dalam metode ini, citra penampung *(cover image)* akan dibagi dulu menjadi beberapa blok. Setiap blok akan berukuran 3 x 3 *pixel* atau sama dengan 9 *pixel* (Bailey, et al; 2004).

Ketiga tahapan utama akan diterapkan per bloknya atau per operasi penyisipannya, dimana *bit-bit* data rahasia hanya akan disisipkan pada salah satu komponen warna di *pixel* P, dan disajikan pada Gambar 2.5.



Gambar 2.5 *Pixel* Tetangga dari *Pixel* P (Lee dan Chen, 1999).

Capacity evaluation, merupakan tahap pertama dan yang paling krusial dari metode penyisipan AMELSBR. Tahap ini mengacu pada karakterisitik *human visual system* (HVS) yang tidak sensitif terhadap *noise* dan perubahan warna yang terdapat di dalam citra (Lee dan Chen, 1999). Langkah pertama yang akan dilakukan pada evaluasi kapasitas adalah mencari nilai variasi warna (V) yang melibatkan*pixelA, B, C* dan *D*. (Gan, 2003)

Persamaan (1) *V* adalah sebagai berikut

$$V = round\ \{(|C-A|+|A-B|+|B-C|+|C-D|)/4\} \quad (1)$$

$$K = round\ (|log2\ V|) \quad (2)$$

dimana :

V = variasi warna *(color variation)*

Round = fungsi matematika untuk pembulatan

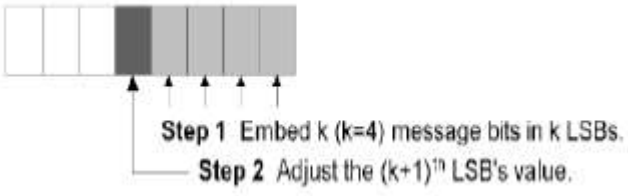
K = kapasitas penyisipan pada *pixel P* dalam *bit*.

V = variasi warna

Round = fungsi matematika untuk pembulatan

Rumus tersebut akan menghasilkan ketentuan toleransi modifikasi yang akurat di setiap *pixelP*. Langkah ke-dua adalah mencari kapasitas penyisipan *(K)* pada *pixelP* (Gan, 2003)

Tahap selanjutnya adalah mencari MER. Tahap ini berfungsi untuk meminimalkan terjadinya perubahan *pixel* pada citra penampung akibat dari proses penyisipan. Proses MER dilakukan dengan mengubah nilai *bit* ke *K+1* pada *pixel P*. Perubahan ini akan terjadi pada salah satu dari ke-tiga komponen warna (R, G atau B) yang terpilih (Lee dan Chen, 1999). Proses ini disajikan pada Gambar 2.6.



Gambar 2.6 Proses MER (Lee dan Chen, 1999).

Bila pada langkah sebelumnya (evaluasi kapasitas) didapat *K* = 4, maka *bit* yang ke-lima akan diubah nilainya, misal nilai awal adalah 1, maka akan diubah

menjadi 0, begitu juga sebaliknya. Namun demikian pengubahan *bit* ke *K+1* belum tentu dilakukan, karena pada tahap MER juga dilakukan proses pengecekan nilai *embedding error*. *Embedding error (Er)* adalah selisih nilai (dalam desimal) pada komponen warna yang terpilih di *pixel P*, sebelum (original) dan sesudah dilakukan proses penyisipan, atau dengan rumus seperti di bawah ini

$Er = Abs\ [P(x,y) - P'(x,y)]$

dimana :

Abs = Nilai absolut

Er = Nilai *embedding error*

P(x,y) = *PixelP* asli

P'(x,y) = *PixelP* yang telah dimodifikasi

Pengubahan pada *bit* ke *K+1* akan dilakukan apabila nilai *embedding error* memenuhi syarat pada saat pengecekan, uraiannya bisa dijelaskan sebagai berikut. Asumsi *P(x,y)* adalah *pixel P* original, *P'(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* tanpa mengubah *bit* ke *K+1* dan *P''(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* sekaligus mengubah *bit* ke *K+1*. *Minimum error* yang dapat terjadi di *pixel P* haruslah *P'(x,y)* atau *P''(x,y)* (Lee dan Chen, 1999).

Kemudian proses pengecekan nilai *embedding error* dilakukan lewat rumus sebagai berikut

$Er1 = Abs\ [P(x,y) - P'(x,y)]$

$Er2 = Abs\ [P(x,y) - P''(x,y)]$

Apabila *Er1 < Er2*, maka *P'(x,y)* yang akan menggantikan *P(x,y)*. Jika sebaliknya maka *P''(x,y)* yang akan menggantikan *P(x,y)* (Lee dan Chen, 1999).

Menurut Panditatwa (2015) AMELSBR adalah metode yang baik untuk melakukan teknik steganografi. File citra gambar yang digunakan sebagai media penampung (cover) berhasil menyembunyikan atau menyisipkan data khususnya berkas tanpa terlihat mencurigakan dan terlihat seperti file gambar biasa atau tidak ada perbedaannya dengan gambar lain. Setelah dikompres, media gambar tidak terlalu berubah dengan melebihi batas wajar dari suatu file gambar itu sendiri.

2.7 Metode DCT

Discrete Cosine Transform (DCT) biasa digunakan untuk mengubah sebuah sinyal menjadi komponen frekuensi dasarnya. DCT pertama kali diperkenalkan oleh Ahmed, Natarajan dan Rao pada tahun 1974 dalam makalahnya berjudul "On image processing and a discrete cosine transform" (Watson, 1994).

DCT mempunyai dua sifat utama untuk kompresi citra dan video yaitu :

- Mengkonsentrasikan energi citra ke dalam sejumlah kecil koefisien (*energy compaction*).
- Meminimalkan saling ketergantungan diantara koefisien-koefisien (*decorrelation*).

DCT dirumuskan sebagai berikut :

$$S(u) = \sqrt{2/n} \quad (1)$$

$$C(u) = \sum_{x=0}^{n-1} \cos \frac{(2x+1)u\pi}{2n} \quad (2)$$

dengan $u = 0, \dots, n-1$

$$C(u) = \begin{cases} 2^{-1/2}, untuk\ u = 0 \\ 1\ ,\ \ untuk\ lainnya \end{cases}$$

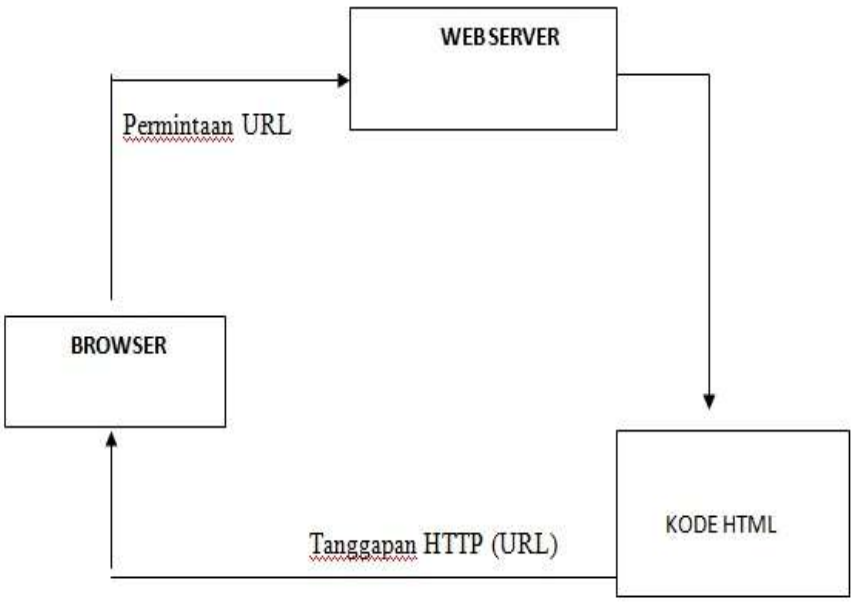
Setiap elemen dari hasil transformasi S(u) merupakan hasil dot product atau inner product dari masukan s(x) dan basis vektor. Faktor konstanta dipilih sedemikian rupa sehingga basis vektornya orthogonal dan ternormalisasi. DCT juga dapat diperoleh dari produk vektor (masukan) dan n x n matriks orthogonal yang setiap barisnya merupakan basis vektor. *Discrete Cosine Transform* merepresentasikan sebuah citra dari penjumlahan sinusoida dan magnitude dan frekuensi yang berubah-ubah. Sifat dari DCT adalah mengubah informasi citra yang signifikan dikonsentrasikan hanya pada bebrapa koefisien DCT. Oleh karena itu sering untuk kompresi citra seperti pada JPEG.

2.8 Pemrograman PHP

Saputra (2012) mengatakan bahwa PHP (*Hypertext Preprocessor*) adalah suatu bahasa pemprograman yang difungsikan untuk membangun suatu web dinamis. PHP menyatu dengan kode HTML yang artinya dimana HTML digunakan sebagai pembangun atau pondasi dari kerangka layout web, sedangkan PHP digunakan sebagai prosesnya, sehingga dengan adanya PHP tersebut sebuah web akan sangat mudah di *maintenance*. PHP berjalan pada sisi server, sehingga PHP disebut juga sebagai bahasa *server side scripting*, artinya bahwa dalam setiap/ untuk menjalankan PHP wajib membutuhkan web server dalam menjalankannya.

PHP bersifat *open source*, sehingga dapat dipakai secara cuma-cuma dan mampu digunakan pada berbagai platform yakni sistem operasi windows maupun Linux.

PHP juga dibangun sebagai modul pada web server apache dan sebagai binary yang dapat berjalan sebagai CGI.



Gambar 2.7 Cara Kerja PHP (Saputra, 2012).

Pada gambar di atas dapat dijelaskan cara kerja PHP yaitu:

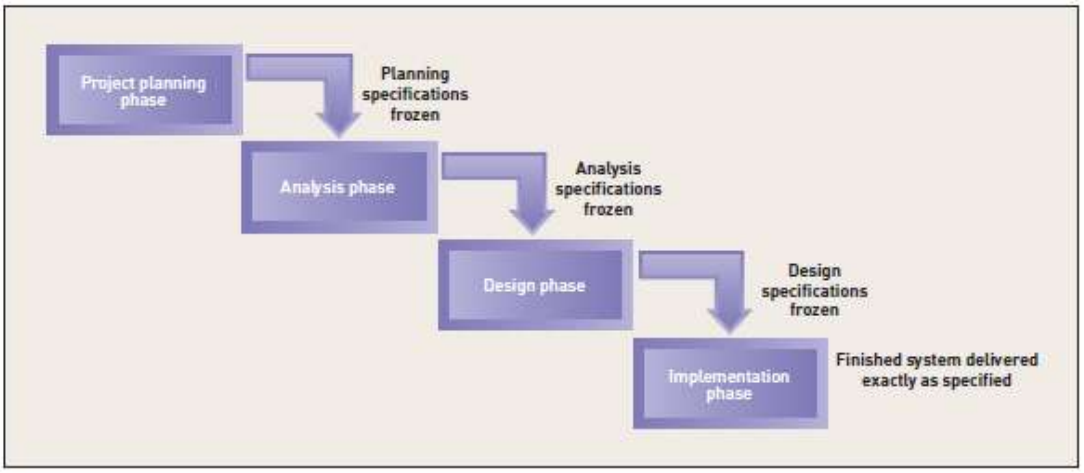
a. Server membaca permintaan dari client/browser.
b. Kemudian dilanjutkan untuk mencari halaman/page pada server.
c. Server melakukan instruksi yang diberikan oleh PHP untuk melakukan modifikasi pada halaman/page.
d. Selanjutnya hasil modifikasi tersebut akan dikembalikan kepada *client/browser*.

2.9 Metode Pengembangan Sistem *Waterfall*

Metode pengembangan sistem *waterfall* adalah pendekatan SDLC yang penyelesaian proyeknya diselesaikan dengan tahapan-tahapan yang berurutan.

Tahap-tahap pada metode *waterfall* adalah perencanaan sistem, analisis kebutuhan, desain dan implementasi (Satzinger, et al; 2010).

Tahapan-tahapan dalam metode pengembangan sistem *waterfall* disajikan pada Gambar 2.8.



Gambar 2.8 *Waterfall* (Satzinger, et al; 2010).

BAB III

METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

Peneliti melakukan penelitian di Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Lampung. Waktu penelitian dilakukan pada semester genap tahun ajaran 2016-2017.

3.2 Perangkat

Perangkat keras yang digunakan pada penelitian perbandingan teknik *steganografi* dengan menggunakan metode AMELSBR dan DCT adalah satu unit komputer dengan spesifikasi sebagai berikut :

- Processor: Intel(R) Core(TM)2 Duo CPU E4500 @ 2.20 GHz
- Memory: 4,00 GB RAM.
- DirectX Version: DirectX 11.
- Card name: NVIDIA GeForce GT 630
- Display Memory: 3565 MB.

Perangkat lunak yang digunakan peneliti adalah sebagai berikut :

- Windows 7 Ultimate
- XAMPP

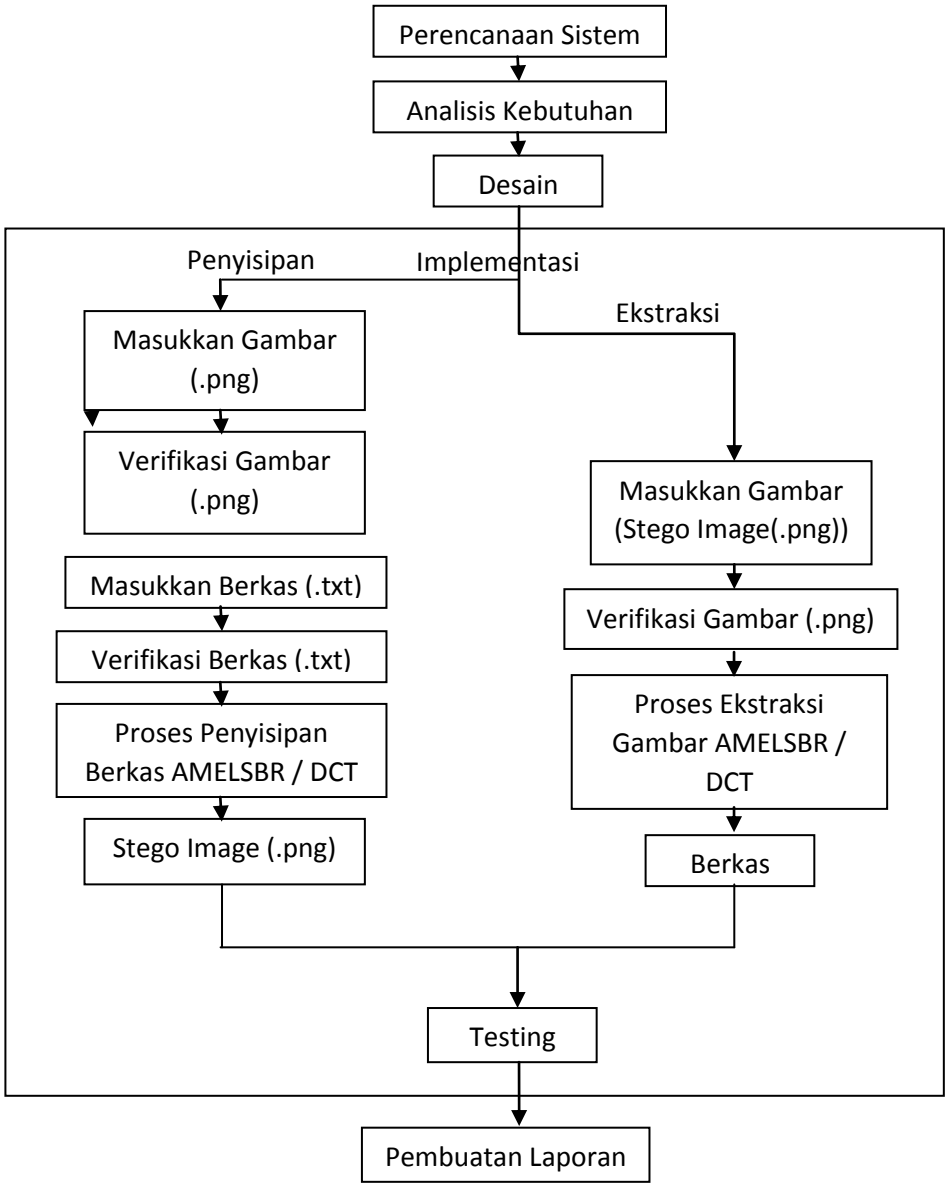
- Star UML
- PHP
- Notepad++ versi 6.8.3
- Mozilla Firefox versi 41.0.2

3.3 Metode Penelitian

Metode penelitian yang dilakukan oleh peneliti adalah studi literatur. Peneliti membaca buku-buku dan jurnal-jurnal yang berkaitan dengan teknik *steganografi* dan pengolahan citra. Tujuan metode literature dalah untuk memperoleh sumber referensi sehingga memudahkan dalam penelitian ini.

3.4 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan peneliti adalah metode *prototype.* Tahap-tahap pada metode *prototype* adalah perencanaan sistem, analisis kebutuhan, desain dan implementasi. Tahap penelitian dan pengembangan sistem disajikan pada Gambar 3.1.



Gambar 3.1 Tahap Penelitian dan Pengembangan Sistem

3.4.1 Perencanaan Sistem

Tahap awal yaitu pendefinisian masalah yang akan diselesaikan dari sistem yang akan dibangun yaitu bagaimana mengirimkan berkas rahasia dengan aman tanpa terlihat mencurigakan bagi orang lain yang tidak berkepentingan dengan berkas tersebut. Dari masalah tersebut maka akan dibangun suatu sistem penyisipan

berkas dengan bantuan media gambar sebagai *cover* atau disebut teknik *steganografi* dengan metode AMELSBR.

3.4.2 Analisis Kebutuhan

Terdapat analisis kebutuhan yang digunakan dalam pengembangan sistem ini yaitu berupa perangkat keras komputer beserta spesifikasi sebagai berikut : Processor: Intel(R) Core(TM)2 Duo CPU E4500 @ 2.20 GHz Memory: 4,00 GB RAM. DirectX Version: DirectX 11. Card name: NVIDIA GeForce GT 630 Display Memory: 3565 MB.

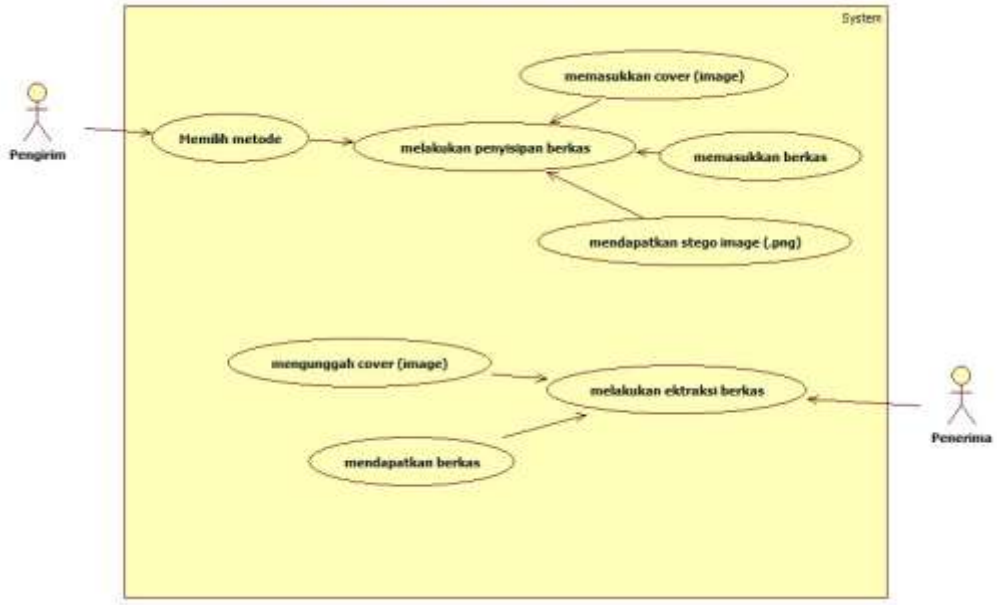
3.4.3 Desain

Proses desain yaitu proses alur kerja sistem, tahap-tahap pengerjaan sistem serta tahap-tahap berjalannya sistem dengan baik. Berikut adalah penjabaran darit ahap-tahap tersebut disajikan dalam bentuk diagram serta rancangan antarmuka sistem.

3.4.3.1 Diagram Sistem

1. *Use Case* Diagram.

Use Case diagram berikut ini menjelaskan bagaimana pengguna menggunakan sistem. Pengguna yang terdapat didalam sistem teknik *steganografi* ini adalah pengirim dan penerima. Pada bagian pengirim dilakukan 3 interaksi yaitu memasukkan gambar (*cover image)*, memasukkan berkas, dan mendapatkan gambar (*stego image)*. Sedangkan dibagian penerima dilakukan 2 interaksi yaitu memasukkan gambar (*stego image)* dan mendapatkan berkas. *Use Case* diagram disajikan pada Gambar 3.2.



Gambar 3.2 *Use Case* Diagram

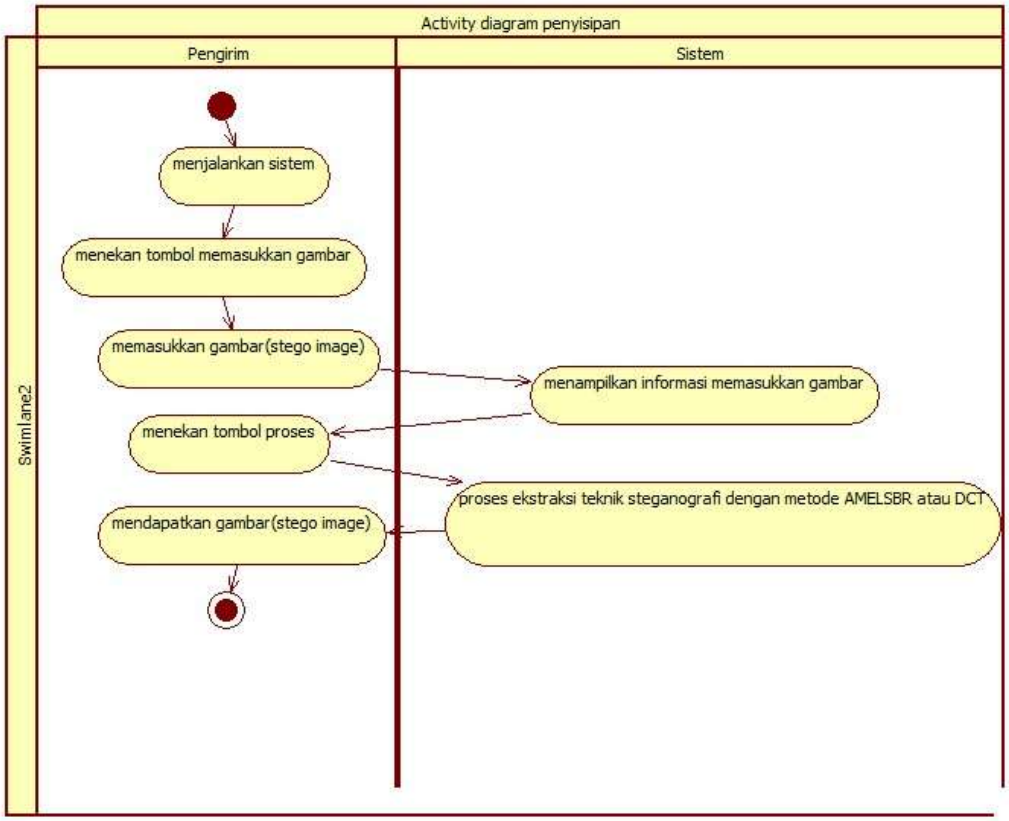
2. *Activity* Diagram.

Activity diagram digunakan untuk menggambarkan aliran kerja (*workflow)* dari kejadian *use case* sistem. Gambar 3.2 dan Gambar 3.3 adalah diagram aktivitas yang berhubungan dengan aliran kejadian untuk *use case* sistem teknik *steganografi* dengan metode *AMELSBR (Adaptive Minimun Error Least Significant Bit Replacement)* dan *DCT (Discrete Cosine Transform)*. *Activity* diagram pada sistem ini terbagi atas 2 bagian yaitu *activity* diagram untuk pengirim dan *activity* diagram untuk penerima.

a. *Activity* Diagram Pengguna Sebagai Pengirim.

Pada *activity diagram* pengirim dimulai dengan menjalankan sistem kemudian pengirim memasukkan gambars ebagai media penampung sedangkan sistem menampilkan informasi untuk memasukan gambar. Begitu juga dengan proses pemasukan berkas yang dimulai dengan memasukkan berkas dan sistem

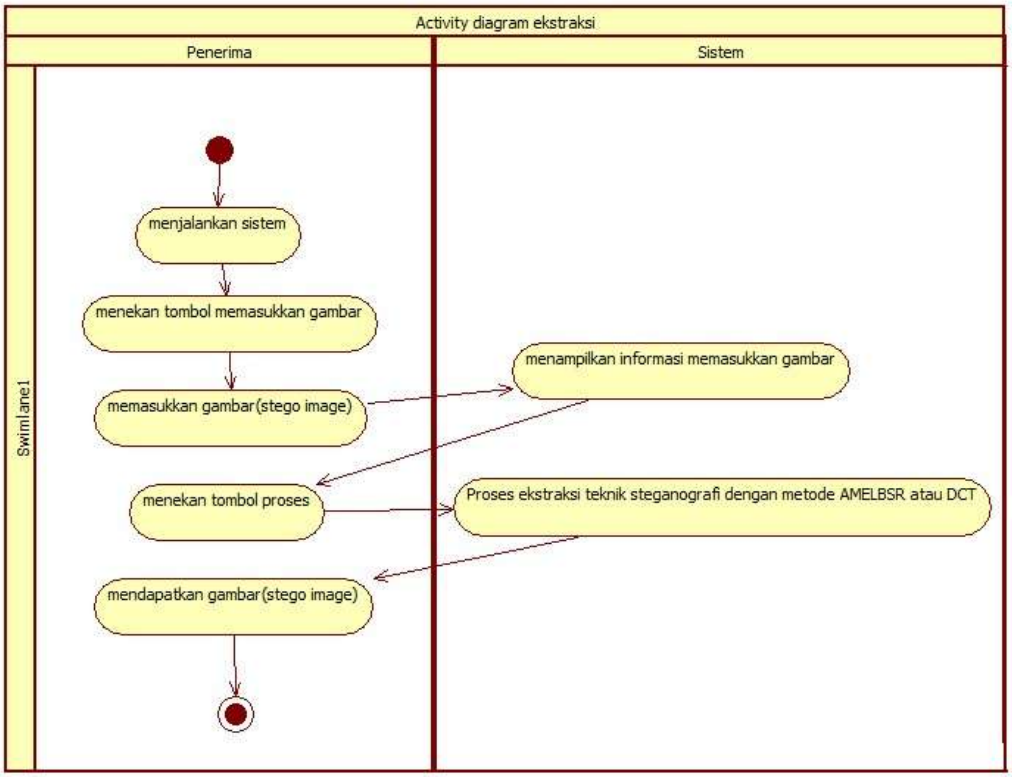
menampilkan informasi memasukkan berkas serta setelah semua proses selesai maka sistem memproses gambar dan berkas tadi dengan teknik *steganografi* menggunakan metode AMELSBR maupun DCT. Terakhir pengguna mendapatkan gambar (*stego image)*. Proses ini disajikan pada Gambar 3.3.



Gambar 3.3 *Activity* Diagram Pengirim

b. *Activity* Diagram Pengguna sebagai Penerima.

Pada *activity diagram* penerima dimulai dengan menjalanka nsistem kemudian memasukkan gambar (*stego image)* kedalam sistem dengan sistem menampilkan informasi untuk memasukkan gambar. Proses selanjutnya yaitu proses ekstraksi dari gambar tersebut dengan teknik *steganografi* menggunakan metode AMELSBR, terakhir pengguna mendapatkan berkas rahasia sebagai hasil ekstraksi. Proses ini disajikan pada Gambar 3.4.

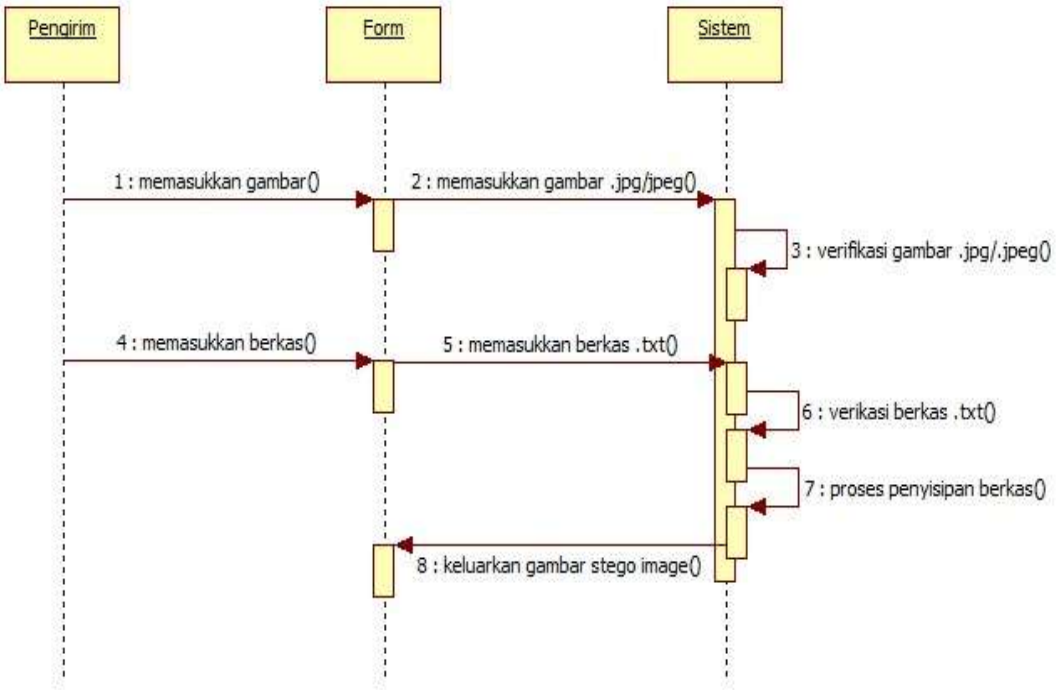


Gambar 3.4 *Activity* Diagram Penerima

3. *Sequence* Diagram.

Sequence diagram digunakan untuk menunjukkan aliran fungsionalitas dalam *use case.* Pada sistem ini terdapat 2 bagian *sequence* diagram yaitu diagram untuk pengirim dan diagram untuk penerima, sesuai dengan *use case* diagram yang telah digambarkan. *Sequence* diagram sistem disajikan pada Gambar 3.5 dan Gambar 3.6.

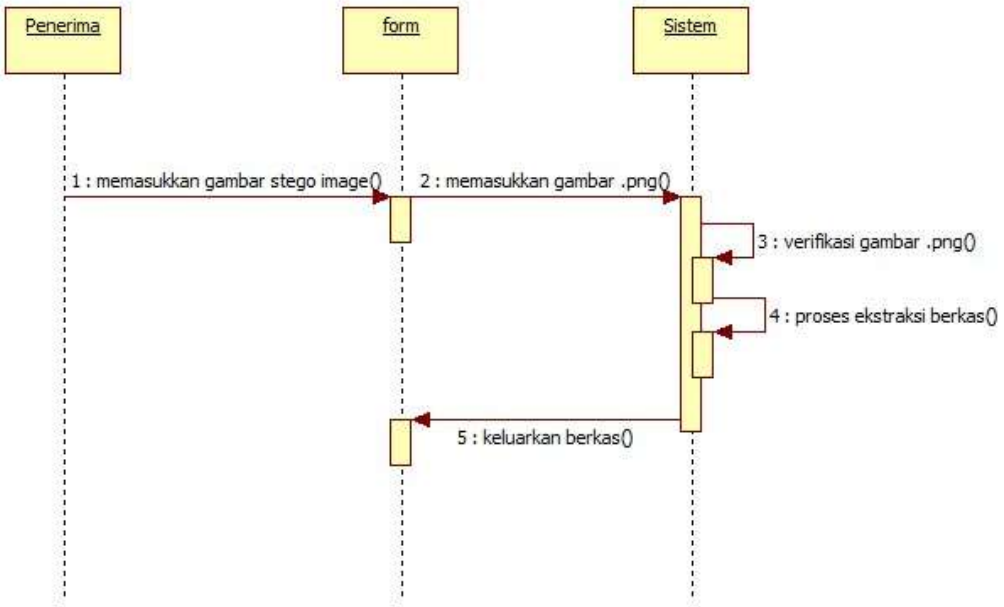
a. *Sequence* Diagram Pengguna Sebagai Pengirim.



Gambar 3.5 *Sequence* Diagram Pengirim

Dari Gambar 3.5 dijelaskan bahwa terdapat 2 proses yaitu proses memasukkan gambar sebagai media penampung dan memasukkan berkas sebagai media yang akan disisipkan. Pada sistem terdapat verifikasi gambar berjenis *file* (.png) dan berkas berjenis *file* (.txt). Setelah semua terpenuhi maka proses penyisipan Berkas dilakukan sehingga ada akhirnya didapatkan gambar (*stego image).*

b. *Sequence* Diagram Pengguna Sebagai Penerima.



Gambar 3.6 *Sequence* Diagram Penerima

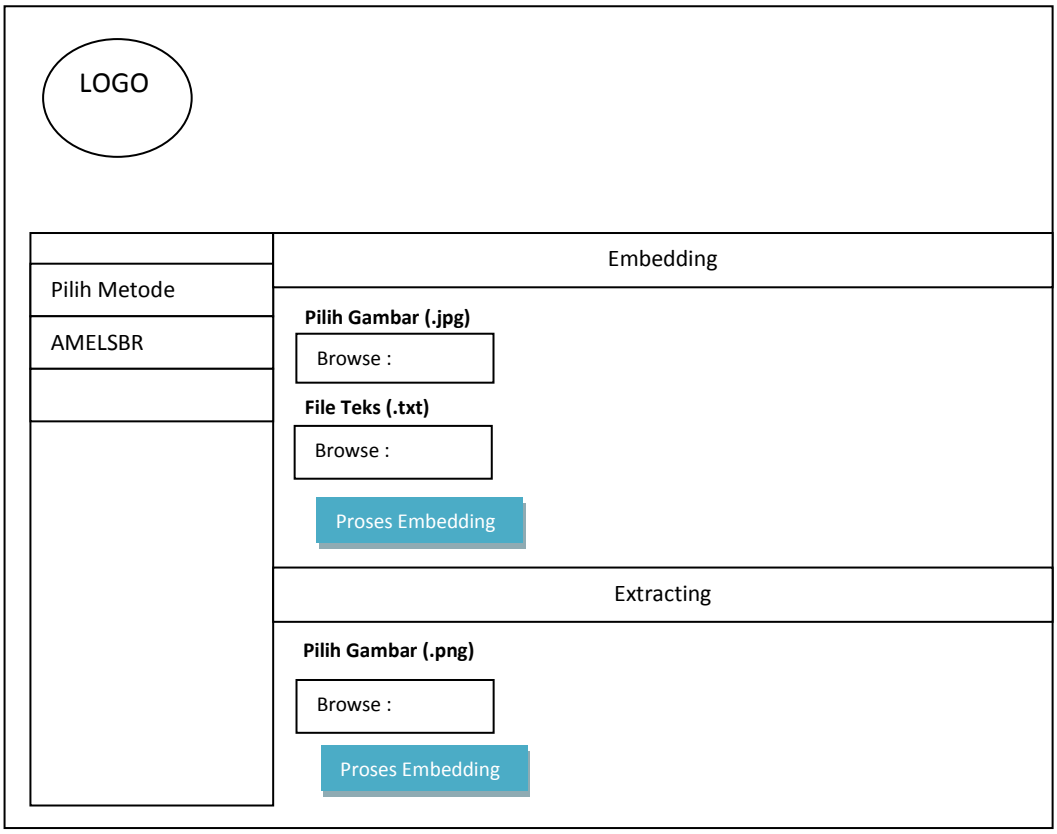
Dari Gambar 3.6 dijelaskan bahwa terdapat proses pemasukan gambar (*stego image*) kedalam sistem kemudian dilakukan verifikasi gambar berjenis *file* (.png). Selanjutnya dilakukan proses ekstraksi gambar dan pada akhirnya diterima kembali berkas yang telah disisipi sebelumnya.

3.4.3.2 Rancangan Antarmuka

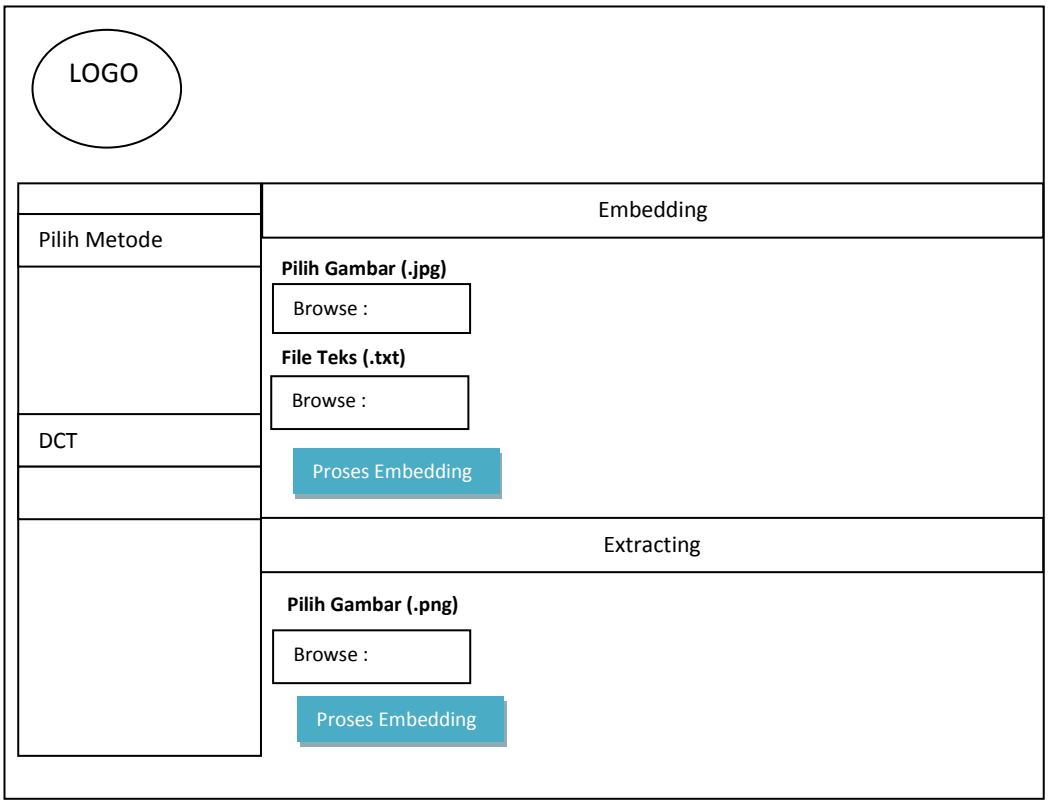
Perancangan antarmuka implementasi teknik *steganografi* menggunakan metode AMELSBR dan DCT ini dirancang dengan tampilan yang *user friendly*, sehingga diharapkan dapat mempermudah pengguna dalam menggunakan sistem ini. Berikut rancangan antarmuka sistem.

1. Tampilan Proses Penyisipan dan Proses Ekstraksi

Tampilan Proses Penyisipan dan Proses Ekstraksi dirancang dihalaman yang sama. Pengguna dapat melakukan kedua proses tersebut dengan membaca aturan dan tata caranya di bagian tampilan bantuan. Tampilan Proses Penyisipan dan Proses Ekstraksi baik itu AMELSBR maupun DCT disajikan pada Gambar 3.7 dan 3.8.



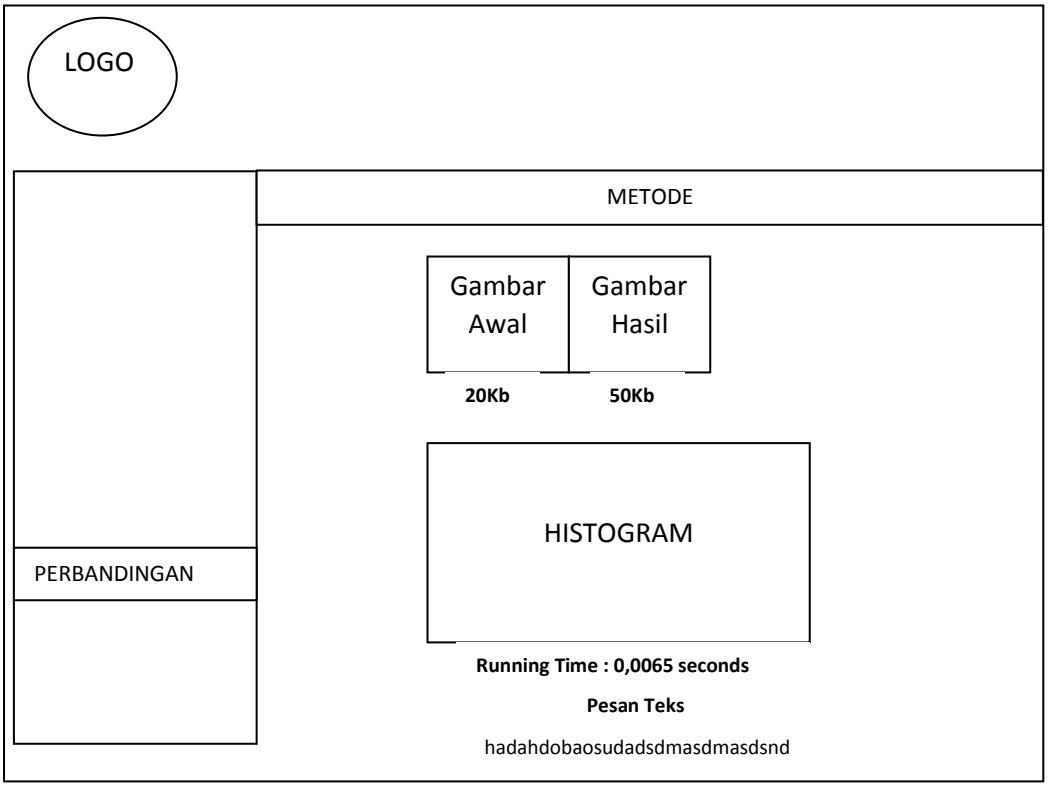
Gambar 3.7 Tampilan Proses Metode AMELSBR



Gambar 3.8 Tampilan proses Metode DCT

2. Tampilan Halaman Perbandingan

Tampilan Halaman Perbandingan ini dirancang untuk menampilkan dan membandingkan Hasil gambar yang sudah diproses pada *embedding* kedua metode. Halam perbandingan AMELSBR dan DCT disajikan pada Gambar 3.9



Gambar 3.9 Tampilan Halaman Perbandingan

3.4.4 Implementasi

Implementasi penelitian ini yaitu menerjemahkan teori teknik *steganografi* menggunakan metode *AMELSBR* dalam melakukan proses penyisipan berkas dengan format *file* (.txt) sebagai berkas yang akan disisipi, media gambar dengan format *file* (.png) sebagai media penampung dan melakukan ekstraksi berkas dengan memasukan *stego image* hasil proses penyisipan untuk mendapatkan kembali berkas yang disisipi kedalam bentuk kode-kode program berbasis web (*PHP).*

3.4.4.1 Tahap-Tahap Penyisipan Berkas

1. *Input file* gambar.

   Input file gambar adalah proses pemilihan gambar yang akan dijadikan *cover*, yang digunakan untuk media tempat berkas akan disisipi. Proses i*nput file* gambar dengan cara meng-*upload file* tersebut ke dalam sistem.

2. Verifikasi *file* gambar, harus berformat (.png).

   File gambar yang digunakan pada proses *encode* adalah gambar yang berformat (.png) karena jenis format tersebut merupakan jenis format *file* gambar yang sering digunakan.

3. *Input* berkas.

   Input berkas adalah proses pemilihan berkas rahasia yang disisipkan pada media gambar dengan format (.png). Proses *input* berkas dengan cara meng-*upload file* tersebut ke dalam sistem.

4. Verifikasi berkas, harus berformat (.txt).

   File berkas yang digunakan pada proses *encode* adalah berkas yang berformat (.txt) karena jenis format tersebut merupakan jenis format berkas dengan ukuran data kecil dan tidak memerlukan waktu yang lama dalam pemrosesan data *steganografi*.

5. Proses *Steganografi.*

   Proses metode *AMELSBR* berjalan pada tahap penyisipan berkas (.txt).

6. Selesai.

   Setelah melalui tahap-tahap *output* dari sistem ini adalah *stego image* berupa gambar berformat (.png) karena format tersebut baik dalam akurasi penyimpanan data (*losseless)*

3.4.4.2 Tahap-Tahap Pengembalian Berkas

1. *Input file* gambar.

   Input file gambar adalah proses pemilihan gambar yang telah dijadikan *cover* pada proses *encode* atau *stego object.* Proses *input file* gambar dengan cara mengunggah *file* tersebut ke dalam sistem.

2. Verifikasi *file* gambar, harus berformat (.png).

   File gambar yang digunakan pada proses *decode* adalah gambar yang berformat (.png) karena format tersebut baik dalam akurasi penyimpanan data (*losseless)*

3. Proses *Steganografi.*

   Proses metode *AMELSBR* maupun *DCT* pada tahap pengembalian berkas (.txt).

4. Selesai.

   Pesan rahasia berhasil disembunyikan. *Output* dari proses ini adalah berkas berformat (.txt).

3.4.4.3 *Testing* (Pengujian)

Tahap *testing* atau pengujian adalah tahap untuk memastikan seluruh kebutuhan yang telah diimplementasikan serta mengidentifikasi kekurangan pada sistem. Pada pengujian sistem terdapat rencana pengujian atau sekenario pengujian yaitu :

1. Pengujian terhadap gambar berjenis *file* (.png) sebagai *input* dan *output*.

   Proses ini untuk membuktikan bahwa gambar berjenis *file* (.png) sebagai *input* dan *output* adalah jenis *file* yang baik dalam teknik *steganografi* menggunakan metode AMELSBR maupun DCT.
2. Pengujian terhadap perubahan *brightness* dan *contrast.*

   Proses ini untuk membuktikan bahwa perubahan *brightness* dan *contrast* pada *stego image* mempengaruhi berkas yang telah disisipi.
3. Pengujian terhadap pemotongan gambar pada hasil proses penyisipan (*stego image).*

   Proses ini untuk membuktikan bahwa melakukan pemotongan gambar pada *stego image* mempengaruhi berkas yang telah disisipi.
4. Pengujian terhadap perbandingan beberapa komponen hasil kedua metode

   Proses ini membuktikan metode manakah yang lebih baik dalam menyisipkan suatu pesan rahasia terhadap gambar. Komponen-komponen hasilnya yakni *file size* gambar, *running time*, dan histogramnya.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut :

1. Kedua metode AMELSBR dan DCT adalah metode yang baik yang digunakan untuk menyimpan pesan rahasia dengan baik
2. AMELSBR lebih unggul dalam ketahanan menjaga pesan rahasia ketimbang DCT dengan dapat mengembalikan pesan rahasia pada sejumlah percobaan
3. Sistem implementasi teknik steganografi dengan metode AMELSBR dan DCT ini dapat digunakan dengan baik untuk menyembunyikan berkas di dalam media penampung gambar dan dapat memberikan keamanan dalam pengiriman data.
4. Ketahanan gambar pada manipulasi seperti *brightness*, *contrast*, dan *cropping* ditentukan oleh komposisi warna, metode yang dipakai, dan ukuran gambar
5. Tidak terlihat perbedaan yang signifikan pada gambar dikarenakan penggunaan format *file* gambar (.png) sebagai *input* dan *output*. Dengan demikian format *file* (.png) tersebut baik digunakan untuk teknik *steganografi*.

5.2 Saran

Saran dalam penelitian ini adalah sebagai berikut :

1. Dalam pengembangan sistem selanjutnya dapat menambahkan tingkat keamanan dari sistem, sehingga data yang diproses dalam sistem dapat lebih terjaga dengan baik.
2. Dalam pengembangan sistem selanjutnya media penampung berupa gambar dapat disisipi data selain berkas seperti gambar, suara, video dan-lain-lain.
3. Implementasi teknik *steganografi* dapat dikembangkan serta ditambahkan dengan metode pemrograman yang lain sehingga penyisipan berkas dan ekstraksi pesan dapat sepenuhnya tahan terhadap proses manipulasi gambar.
4. Karena kekurangan bahasa pemrograman PHP, pengembangan sistem selanjutnya dapat menggunakan bahasa pemrograman yang lain.

DAFTAR PUSTAKA

Ahmed, N., Natarajan, T., & Rao, *K. R. 1974. Discrete Cosine Transform*. IEEE Transactions on Computers, C-23(1), 90-93. DOI: 10.1109/T-C.1974.223784.

Bailey, K., Curran, K., dan Condell, J. 2004. An Evaluation of Automated Stegodetection Methods In Images,http://www.ittconference.com/anonftp/pdf/2004%20presentations/presentations/session%20a/Karen%20Bailey-1.ppt, diakses tanggal 28 Oktober 2015.

Carellas, Peter T. 2010. *Image Processing: Brightness, Contrast, Gamma, and Exponential/ Logarithmic Settings in ProAnalyst®*, http://www.xcitex.com/Resource%20Center/ProAnalyst/Application%20Notes/App%20Note%20151%20%20Image%20Processing%20Brightness,%20Contrast,%20Gamma%20and%20Exponential.pdf diakses tanggal 28 Mei 2016

Gan, M. D. 2003. Chameleon Image Steganography, http://chameleonstego.tripod.com/downloads/Chameleon_Technical_Paper.pdf, diakses tanggal 10 Februari 2015.

Hermawati, Fajar A. 2013. *Pengolahan Citra Digital.* Yogyakarta : Andi Offset.

Ichsan. 2011.Implementasi Teknik Kompresi Gambar Dengan Algoritma Set Partitioning In Hierarchical Trees Pada Perangkat Bergerak.Departemen Teknik Elektro Fakultas Teknik Universitas Sumatera Utara Medan, Medan.

Iza, Dzikru Rohmatul. 2013. Steganografi Pada Citra Digital Menggunakan Metode Discrete Wavelet Transform. Universitas Brawijaya. Malang.

Lee, Y. K., dan Chen, L. H. 1999. *An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*, http://citeseer.ist.psu.edu/205600.html/lee99adaptive.pdf, diakses tanggal 10 Februari 2015.

Munir, Rinaldi. 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung : Penerbit Informatika Bandung.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Penerbit Informatika Bandung.

Panditatwa, Pandya. 2015. Implemetasi Teknil Steganografi Menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement

(AMELSBR). Skripsi Strata 1 pada Universitas Lampung. Tidak Diterbitkan

Prayudi, Y dan Kuncoro, S. 2005. Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR). Program Studi Teknik Informatika, Fakultas Teknologi Industri Universitas Islam Indonesia. Yogyakarta.

Provos, N and Honeyman, P. 2003. *Hide and Seek: An Introduction to Steganography.* University of Michigan.

Purnomo, Herry dan Zacharias, Theo. 2005. *Pengenalan Informatika Perspektif Teknik dan Lingkungan* . Yogyakarta: Andi.

Purnomo, Mauridhi H dan Muntasa A. 2010. *Konsep Pengolahan Citra Digital dan Ekstrasi Fitur*. Yogyakarta : Graha Ilmu.

Satzinger, John W. Robert Jackson. and Stephen D. Burd. 2010. *Systems analysis and design in a changing world, Five Edition* . Course Technology, Cengage Learning, Boston, Massachusetts. Canada.

Saputra, Agus.2012. *Sistem Informasi Nilai Akademik untuk Panduan Skripsi*. Jakarta: Elex Media Komputindo.

Sellars, D. 2006.*An Introduction to Steganography,* ,http://www.cs.uct.ac.za/ courses/CS400W/NIS/papers99/dsellars/ stego.html, diakses tanggal 29 Oktober 2015.

Wijaya, Muksin. 2006.*Manipulasi Gambar dan Citra Digital dengan COREL Paint Shop Pro Photo XI*. Jakarta: Elex Media Komputindo

Watson, Andrew B. 1994. *Image Compression Using the Discrete Cosine Transform*. Washington D. C. : NASA Ames Research Center : Mathematica Journal

Widhiartha, Putu. 2008.*Pengantar Kompresi Data,* www.ilmukomputer.org/wp-content/uploads//2008/10/widhiartha_kompresidata.pdf,diakses tanggal 11 Februari 2015.