

Penentuan Jumlah, Titik Tengah dan Jenis dari Objek Geometri Digital dengan Metode *Boundaries* Menggunakan Matlab

Syafrijal Agus Mubarak^[1], Hafizh Novanda Ichwan^[2], Syamsudin Zubair^[3], Yulianto^[4]

Pascasarjana Magister Ilmu Komputer Universitas Budi Luhur

Jl. Ciledug Raya, Petukangan Utara, Pesanggrahan, Jakarta Selatan, DKI Jakarta, Indonesia 12260
syafrijalagus@gmail.com, hafizhnovanda@gmail.com, zubair.syamsudin@gmail.com, keretakudaq@gmail.com

Abstract—In this study, in the wake of a geometric object identification system contained in an image. Broadly speaking, this system works by reading an image contained therein image geometry. In determining an object geometry we often encounter problems either determine the type of object geometry, determines the number of geometry objects. The determination of a geometric object can help us to know the object which we will examine and may also reduce errors. Sometimes identification by conventional or manual often less precise and accurate, because this identification is done by using direct observation without the use of a digital image. With this program can be a tool for detecting an object geometry digitally and can also reduce errors at the time of detection of the object geometry.

Keywords: image processing; regionprops; edge detection; geometry; boundaries;

*Abstrak—*Pada penelitian ini di bangun sistem identifikasi objek geometri yang terdapat dalam suatu gambar. Secara garis besar sistem ini bekerja dengan cara membaca sebuah gambar yang terdapat gambar geometri didalamnya. Dalam menentukan sebuah objek geometri kita sering kali mengalami masalah baik itu menentukan jenis objek geometri, menentukan jumlah objek geometri. Penentuan suatu objek geometri ini dapat membantu kita untuk mengetahui objek yang akan kita teliti dan juga dapat mengurangi kesalahan. Kadang kala identifikasi yang dilakukan secara konvensional atau manual sering kali kurang tepat dan akurat, karena identifikasi ini dilakukan dengan menggunakan pengamatan langsung tanpa menggunakan citra digital. Dengan adanya program ini dapat menjadi sebuah tools untuk mendeteksi suatu objek geometri secara digital dan juga dapat mengurangi kesalahan pada saat pendeteksian objek geometri.

Kata Kunci : image processing; regionprops; deteksi tepi; geometri; boundaries;

I. PENDAHULUAN

Dalam menentukan sebuah objek geometri kita sering kali mengalami masalah, baik itu menentukan jenis objek geometri, menentukan jumlah objek geometri, maupun menentukan titik tengah suatu objek geometri. Penentuan suatu objek geometri dapat membantu kita untuk mengetahui objek yang akan kita teliti dan juga dapat mengurangi kesalahan.

Kadang kala identifikasi yang dilakukan secara konvensional atau manual sering kali kurang tepat dan akurat, hal ini dilakukan dengan menggunakan pengamatan langsung tanpa menggunakan citra digital, dan seiring dengan majunya perkembangan jaman dan ilmu pengetahuan maka pendeteksian objek tidak lagi di lakukan secara konvensional atau manual yaitu dengan menggunakan metode boundaries yang tekomputerisasi secara otomatis.

Suatu program komputer dapat melakukan identifikasi pengolahan suatu objek atau citra secara tepat. Pada suatu citra hasil pemotretan sekelompok benda yang seragam atau hampir seragam [3], terdapat ciri khas pada setiap benda tersebut. Ciri khas itulah yang digunakan untuk pendeteksian suatu objek atau citra.

A. Tujuan

Tujuan dari penelitian ini adalah untuk mendeteksi suatu objek atau citra digital geometri secara otomatis dengan metode boundaries berdasarkan pada ukuran objek geometri suatu citra.

B. Batas Masalah

Hal – hal yang perlu diperhatikan pada penulisan ini dibatasi pada pembatasan masalah yang akan di bahas yaitu :

- 1) Objek atau citra yang diolah hanya terbatas pada objek 2 (dua) dimensi saja, tidak bisa digunakan pada objek atau citra 3 (tiga) dimensi.
- 2) Aplikasi yang digunakan menggunakan matlab.
- 3) Gambar yang akan di olah mempunyai format JPG
- 4) Bentuk yang dapat diidentifikasi hanya berupa lingkaran, segitiga, bujur sangkar, persegi panjang atau objek geometri.

II. LANDASAN TEORI

A. Pengertian Citra Digital

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan/ diskrit nilai digital yang disebut pixel/ picture elements [1]. Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi. Citra digital adalah

citra $f(x,y)$ dimana dilakukan diskritisasi koordinat sampling/spasial dan diskritisasi tingkat kwantisasi (kabuan/kecemerlangannya). Citra digital merupakan fungsi intensitas cahaya $f(x,y)$, dimana harga x dan harga y adalah koordinat spasial. Harga fungsi tersebut di setiap titik (x,y) merupakan tingkat kecemerlangan citra pada titik tersebut [2]. Citra digital merupakan suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya (yang disebut sebagai elemen gambar/pixel/ piksel/ pels/ picture element) menyatakan tingkat keabuan pada titik tersebut.

B. Definisi Pengolahan Citra

Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan komputer, menjadi citra yang kualitasnya lebih baik. Meskipun sebuah citra kaya informasi, namun seringkali citra yang kita miliki mengalami penurunan mutu (degradasi), misalnya mengandung cacat atau derau (noise), warnanya terlalu kontras, kurang tajam, kabur (blurring), dan sebagainya. Tentu saja citra semacam ini menjadi lebih sulit diinterpretasi karena informasi yang disampaikan oleh citra tersebut menjadi berkurang. Agar citra yang mengalami gangguan mudah diinterpretasi (baik oleh manusia maupun mesin), maka citra tersebut perlu dimanipulasi menjadi citra lain yang kualitasnya lebih baik [7]

C. Citra Biner

Citra biner (binary image) adalah citra yang hanya mempunyai dua nilai derajat keabuan yaitu hitam dan putih. Meskipun saat ini citra berwarna lebih disukai karena memberi kesan yang lebih kaya daripada citra biner, namun tidak membuat citra biner mati.

D. Konversi Citra Hitam Putih ke Citra Biner

Pengkonversian citra hitam-putih (grayscale) menjadi citra biner dilakukan untuk alasan-alasan berikut [4]:

- 1) Untuk mengidentifikasi keberadaan objek, yang direpresentasikan sebagai daerah (region) di dalam citra. Misal kita ingin memisahkan objek dari latar belakangnya. Pixel-pixel objek ini dinyatakan dengan nilai 1 sedangkan pixel lainnya dengan 0. Objek ditampilkan seperti gambar siluet. Untuk memperoleh siluet yang bagus, objek harus dapat dipisahkan dengan mudah dari latar belakangnya.
- 2) Untuk lebih memfokuskan pada analisis bentuk morfologi yang dalam hal ini intensitas pixelnya tidak terlalu penting dibandingkan dengan bentuknya.
- 3) Untuk menampilkan citra piranti keluaran yang hanya mempunyai resolusi intensitas satu bit, yaitu piranti penampilan dua aras atau biner seperti pencetak (printer)
- 4) Mengkonversi citra yang telah ditingkatkan kualitas tepinya (edge enhancement) ke penggambaran garis-garis tepi. Ini perlu untuk membedakan tepi yang kuat yang berkoresponden dengan batas-batas objek dengan tepi lemah yang berkoresponden dengan perubahan illumination, bayangan dan lain-lain.

E. Metode Regionprops

Region properties (regionprops) adalah metode yang digunakan untuk mengukur sekumpulan properti – properti dari setiap region yang telah dilabeli dalam matriks label [6]. Bilangan integer positif yang merupakan elemen dari matriks berkorespondensi dengan region yang bersesuaian. Area, panjang major axis, dan panjang minor axis yang digunakan merupakan sebagian dari properti yang dihasilkan fungsi regionprops.

Dalam fungsi regionprops sebuah obyek direpresentasikan sebagai sebuah region dengan pendekatan bentuk persegi panjang.

III. PEMBAHASAN

A. Objek Geometri

Setiap hari, para siswa akan melihat, bekerja, dan mengotak-atik benda-benda yang berbentuk bangun-geometris seperti: permukaan kertas, permukaan meja, bola, tempat kapur, dos, tempat es-krim, maupun topi ulang tahun; bermain di lapangan petak umpet, lapangan bola; bekerja/bermain dengan buku, pensil, penghapus, papan tulis, meja, kursi, mobil-mobilan. Travers dkk (1987:6) menyatakan bahwa: "Geometry is the study of the relationships among points, lines, angles, surfaces, and solids". Geometri adalah ilmu yang membahas tentang hubungan antar titik, garis, sudut, bidang dan bangun-geometris ruang. Ada dua macam geometri, yaitu geometri datar dan geometri ruang. Geometri Bidang (G Datar atau G Dimensi Dua) membicarakan bangun-geometris datar; sedangkan G Ruang membicarakan bangun-geometris ruang dan bangun-geometris datar yang merupakan bagian dari bangun ruang. Suatu bangun disebut bangun datar apabila keseluruhan bangun itu terletak pada satu bidang. Suatu bangun disebut bangun ruang apabila titik-titik yang membentuk bangun itu tidak semuanya terletak pada satu bidang yang sama. Jenis-jenis Bangun Geometri. Macam-macam Bangun Geometri. Geometri adalah ilmu yang membahas tentang hubungan antara titik, garis, sudut, bidang dan bangun ruang. Bangun adalah semua informasi geometri yang tersisa pada saat lokasi, skala, dan efek putar yang disaring dari suatu objek. Secara garis besar Geometri di golongkan menjadi 2 macam, yaitu geometri datar (Bangun datar) dan geometri ruang (bangun ruang). Geometri datar bersifat 2 dimensi sedangkan geometri ruang bersifat 3 dimensi. Berikut ini adalah macam-macam bangun Geometri baik bangun datar maupun bangun ruang.

B. Pembacaan Objek Geometri yang diolah

Objek geometri yang didapat pertama kali dalam format JPG, hal ini dikarenakan file yang dapat di baca oleh program ini hanya file yang mempunyai ekstensi JPG, kemudian di rubah menjadi binary image. Dalam program objek geometri dimasukan ke dalam library dengan perintah :

```
Im = imread ('nama file objek');
```

Lalu di convert ke dalam binary image dengan menggunakan perintah :

```
Im(:,:,1) < 10; untuk nilai R G B kurang dari 10  
BW = im(:,:,1) < 10
```

C. Proses Deteksi Tepi

Suatu objek dapat dengan mudah dideteksi pada suatu citra jika objek cukup kontras dari latar belakangnya. Perubahan kekontrasannya dapat dideteksi dengan menggunakan fungsi *boundariy*, yang menciptakan suatu citra biner [5]. Untuk menentukan citra biner dengan menggunakan fungsi tepi. Hal ini dilakukan dengan menggunakan perintah sebagai berikut :

```
[B,L,N,A] = bwboundaries(BW);
```

D. Proses Pengukuran Objek

Pada metode ini kita melakukan proses pengukuran citra dengan menggunakan metode *regionprops* berikut perintah untuk melakukan proses pengukuran objek :

```
Stats=regionprops(L,'centroid','area','perimeter');
```

Dimana objek tersebut akan ditentukan titik tengahnya

E. Identifikasi Citra

Proses pengolahan citra digital berakhir dengan tampilan identifikasi citra hasil pengolahan. Karena program yang dibuat untuk mengidentifikasi objek geometri, maka analisa yang di ambil adalah jumlah, jenis dan centre point objek geometri tersebut. Hal ini dapat dilakukan dengan menggunakan perintah :

```
isCircle = (CircleMetric < 1.1);  
isTriangle = ~isCircle & (TriangleMetric < 0.6);  
isSquare = ~isCircle & ~isTriangle & (SquareMetric > 0.9);  
IsRectangle = ~isCircle & ~isTriangle & ~isSquare;
```

Lalu definisi tiap objek dengan menggunakan perintah

```
Whichshape = cell(N,1);  
Whichshape(isCircle) = {'Lingkaran'};  
Whichshape(isTriangle) = {'Segitiga'};  
Whichshape(isSquare) = {'Bujur sangkar'};  
Whichshape(isRectangle) = {'Persegi Panjang'};
```

IV. PENGUJIAN

A. Akusisi Data

Akuisisi data dapat dilakuakn dengan langkah – langkah berikut :

- 1) Mendapatkan objek geometri
Langkah ini dapat dilakukan dengan cara kita menggambar objek tersebut pada sebuah media digital maupun kita foto objek tersebut
- 2) Rubah format daa file menjadi JPG
Setelah kita mendapatkan data kita merubah format data tersebut menjadi sebuah file JPG agar dapat terbaca pada sistem yang kemudian di rubah menjadi file biner

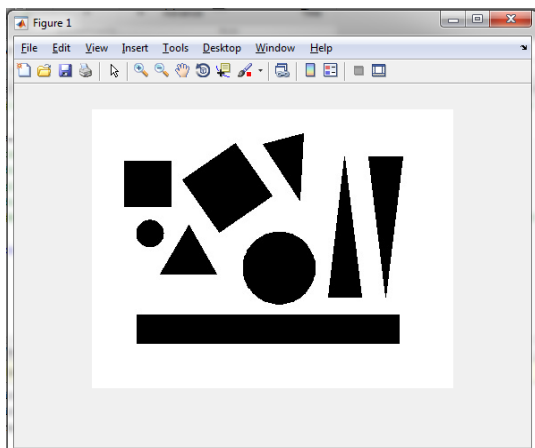
B. Hasil Pengujian

Penelitian ini di awali dengan membuat gambar geometri yang kemudian gambar – gambar tersebut disimpan ke dalam sebuah format JPG yang selanjutnya format JPG tersebut di konversi kedalam citra biner



Gambar 1. Objek geometri yang belum di konversi biner.

Setelah mendapatkan data dalam format bentuk JPG kemudian kita konversi data tersebut ke dalam format citra biner, berikut hasil konversi ke citra biner.



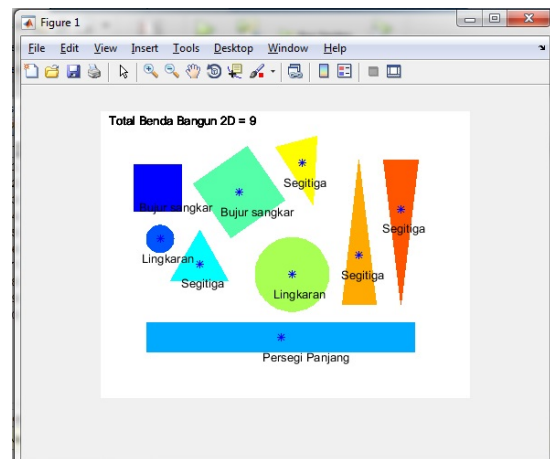
Gambar 2. Hasil konversi format JPG ke format citra biner.

Dari hasil konversi tersebut di dapatkan hasil perimeter dari setiap objek geometri

| No | Nama Objek | Hasil Perimeter |
|----|-----------------|-----------------|
| 1 | Bujur sangkar1 | 201.5160 |
| 2 | Linkaran1 | 94.5620 |
| 3 | Segitiga1 | 636.6360 |
| 4 | Bujur sangkar2 | 187.6420 |
| 5 | Lingkaran2 | 288.0400 |
| 6 | Segitiga2 | 254.8630 |
| 7 | Segitiga3 | 196.4330 |
| 8 | Segitiga4 | 354.7860 |
| 9 | Persegi panjang | 356.0100 |

Tabel 1. Hasil perimeter dari tiap objek

Dari hasil tersebut kita sudah bisa mendeteksi suatu objek, berikut hasil dari deteksi objek sebagai berikut :



Gambar 3. Hasil ouput

V. PENUTUP

A. Kesimpulan

Berdasarkan uraian yang telah diberikan pada bab – bab di atas dapat di tarik kesimpulan sebagai berikut :

- 1) Program yang dibuat dapat mengidentifikasi objek serta dapat menghitung objek
- 2) Program dapat menentukan centre point dari tiap – tiap objek
- 3) Program dapat menampilkan nilai perimeter dari tiap – tiap objek

B. Saran

- 1) Penelitian dapat dilakuakn dengan metode lain dan dapat dilakukan dengan objek yang berbeda
- 2) Penelitian dapat di tingkatkan lagi dengan menggunakan forma file yang berbeda serta dapat mengenali citra 3 (tiga) dimensi.
- 3) Agar citra hasil deteksi terlihat lebih baik perlu diteliti juga penggunaan operator tepi yang lain seperti Prewit, Robert, Laplacian dan sebagainya.

REFERENSI

- [1] Murni, A., *Pengantar pengolahan citra*, PT Elek Media Komputindo Kelompok Gramedia. Jakarta, 1992
- [2] Schalkoff, R. J. *Digital Image Processing adn Computer Vision*, John Wiley & Sons, New York, 1989
- [3] Oge Marquest, *Practical Image and Video Processing Using Matlab*, 2011, Jhon Willey and Son
- [4] Witeti, *Identifikasi Sel Kanker Prostat Menggunakan Metode Segmentasi Berdasarkan Ukuran Objek Pada Citra*, Teknik Elektro Fakultas Teknik Universitas Diponogoro. Semarang 2013 .
- [5] Elias Diana Gnting, *Deteksi Tepi Menggunakan Metode Canny dengan Matlab untuk Membedakan Uang Asli dan Uang Palsu*, Teknik Informatika Universitas Gunadarma, Jakarta 2012.
- [6] Regionprops. <http://www.mathworks.com/help/image/s/ref/regionprops.html> (diakses pada 19 September 2014)
- [7] Abdul Kadir dan Adhi Susanto, "Pengolahan Citra Teori dan Aplikasi", Yogyakarta : Penerbit Andi, 2013.

NLP sehingga teks yang telah disisipi pesan rahasia tidak akan dicurigai orang yang melihatnya.

2. Audio

Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar sehingga bisa menampung pesan rahasia dalam jumlah yang besar pula.

3. Citra

Format ini juga paling sering digunakan karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah tersedianya banyak algoritma steganografi untuk media penampung yang berupa citra.

4. Video

Format ini memang merupakan format dengan ukuran file yang relatif sangat besar, tetapi jarang digunakan karena ukurannya yang terlalu besar, tetapi jarang digunakan karena ukurannya yang terlalu besar itu mengurangi kepraktisannya.

II. LANDASAN TEORI

A. Steganografi

Steganography adalah ilmu dan seni menulis atau menyembunyikan pesan ke dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut. Kata steganography berasal dari bahasa Yunani, yaitu "steganos" yang berarti tersembunyi atau terselubung dan "graphein" yang berarti menulis.

Steganography membutuhkan dua aspek yaitu media penyimpan dan informasi rahasia yang akan disembunyikan. Metode *steganography* sangat berguna jika digunakan pada *steganography* komputer karena banyak format *file digital* yang dapat dijadikan media untuk menyembunyikan pesan. *Steganography digital* menggunakan media *digital* sebagai wadah penampung, misalnya teks, citra, suara, dan *video*. Data rahasia yang disembunyikan juga dapat berupa teks, citra, suara, atau *video*.

Steganography memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata (*Human Visual System*) dan telinga (*Human Auditory System*), sehingga tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran) dan mampu menghadapi proses-proses pengolahan sinyal *digital* dengan tidak merusak kualitas data yang telah disisipi sampai pada tahap tertentu. Terdapat tiga aspek yang perlu diperhatikan dalam menyembunyikan pesan: kapasitas, keamanan, dan ketahanan. Kapasitas merujuk kepada besarnya informasi yang dapat disembunyikan oleh media, keamanan merujuk kepada ketidakmampuan pihak lain untuk mendeteksi keberadaan informasi yang disembunyikan, dan ketahanan merujuk kepada sejauh mana medium *steganography* dapat bertahan sebelum pihak lain menghancurkan informasi yang disembunyikan.[7]

B. Teknik Steganografi

Pada dasarnya, terdapat tujuh teknik yang digunakan dalam steganografi.[8]

1. Injection, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik itu sering juga disebut Embedding.
2. Substitusi, data normal digantikan dengan data rahasia. Biasanya, hasil teknik itu tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusikan bisa menurunkan kualitas media media yang ditumpangi.
3. Domain Transform, teknik pada ranah transform memfokuskan penyisipan pesan ke dalam frekuensi dari *cover-file*. Salah satu metode yang bekerja dalam *domain transform* adalah *Discrete Wavelet Transform (DWT)*. Steganografi memiliki dua buah proses, yaitu penyisipan dan ekstraksi pesan. Proses penyisipan pesan pada steganografi membutuhkan dua buah masukan, yaitu pesan yang ingin disembunyikan dan media penyisipan. Hasil dari proses ini disebut dengan *stego-object*, yaitu suatu media yang mempunyai kemiripan dengan media penyisipan yang telah terdapat pesan tersembunyi di dalamnya.
4. Spread Spectrum, sebuah teknik pentransmisian menggunakan *pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energy sinyal dalam sebuah jalur gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
5. Statistikal Method, teknik ini disebut juga skema steganographic 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit Perubahan statistik ditunjukkan dengan *indikasi* 1 dan jika tidak ada perubahan, terlihat *indikasi* 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
7. Cover Generation, metode ini lebih unik dari pada metode lainnya karena *cover object* yang dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah spam mimic

C. Kriteria Steganografi

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah [2].

1. Fidelity, mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih dapat terlihat dengan baik.

Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat pesan rahasia.

2. Robustness, data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan terhadap citra penampung.

Recovery, data yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan dari steganografi adalah penyembunyian data, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

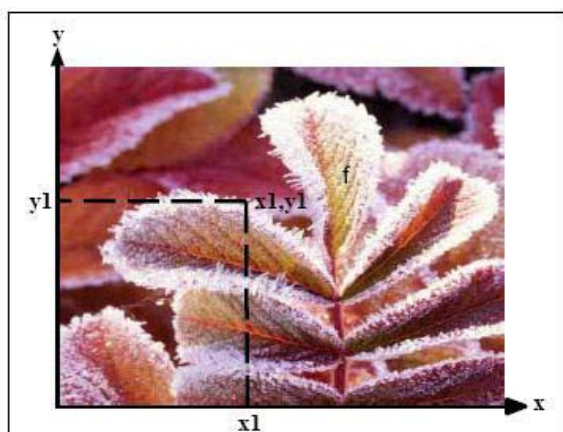
D. End Of File

Metode End Of File (EOF) merupakan salah satu teknik yang menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut. Dalam teknik EOF, data yang disisipkan pada akhir file diberi tanda khusus sebagai pengenalan start dari data tersebut dan pengenalan akhir dari data tersebut.

Metode EOF merupakan sebuah metode yang diadaptasi dari metode penanda akhir file (end of file) yang digunakan oleh sistem operasi windows. Dalam sistem operasi windows, jika ditemukan penanda EOF pada sebuah file, maka sistem akan berhenti melakukan pembacaan pada file tersebut. Prinsip kerja EOF menggunakan karakter/symbol khusus yang diberikan pada setiap akhir file. Karakter/symbol ini biasanya digunakan pada sistem operasi DOS untuk menandakan akhir dari sebuah penginputan data. Dengan berkembangnya sistem operasi windows, penggunaan karakter seperti ini dikembangkan untuk menandakan akhir dari sebuah file.

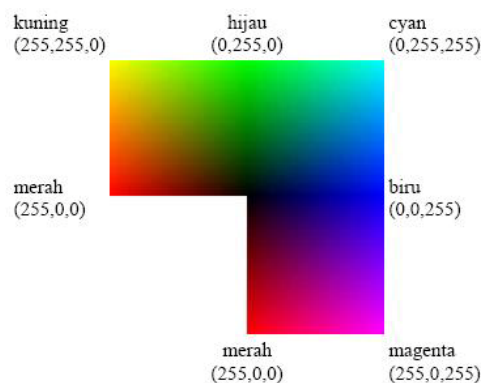
E. Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variabel, $f(x,y)$, dimana x dan y adalah koordinat spasial dan nilai $f(x,y)$ adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada gambar dibawah ini. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (Red, Green, Blue - RGB).[9]



Gambar 1. Ilustrasi Citra Digital

RGB adalah suatu model warna yang terdiri dari merah, hijau, dan biru, digabungkan dalam membentuk suatu susunan warna yang luas. Setiap warna dasar, misalnya merah, dapat diberi rentang-nilai. Untuk monitor komputer, nilai rentangnya paling kecil = 0 dan paling besar = 255. Pilihan skala 256 ini didasarkan pada cara mengungkap 8 digit bilangan biner yang digunakan oleh mesin komputer. Dengan cara ini, akan diperoleh warna campuran sebanyak $256 \times 256 \times 256 = 16777216$ jenis warna. Sebuah jenis warna, dapat dibayangkan sebagai sebuah vektor di ruang 3 dimensi yang biasanya dipakai dalam matematika, koordinatnya dinyatakan dalam bentuk tiga bilangan, yaitu komponen-x, komponen-y dan komponen-z. Misalkan sebuah vektor dituliskan sebagai $r = (x,y,z)$. Untuk warna, komponen-komponen tersebut digantikan oleh komponen R(ed), G(reen), B(lue). Jadi, sebuah jenis warna dapat dituliskan sebagai berikut: warna = RGB(30, 75, 255). Putih = RGB (255,255,255), sedangkan untuk hitam= RGB(0,0,0).



Gambar 2. Pewarnaan dalam RGB

F. Biner

Sistem bilangan biner atau sistem bilangan basis dua adalah sebuah sistem penulisan angka dengan menggunakan dua simbol yaitu 0 dan 1. Sistem bilangan biner modern ditemukan oleh Gottfried Wilhelm Leibniz pada abad ke-17. Sistem bilangan ini merupakan dasar dari semua sistem bilangan berbasis digital. Dari sistem biner, kita dapat mengkonversinya ke sistem bilangan Oktal atau Hexadesimal. Sistem ini juga dapat kita sebut dengan istilah bit, atau Binary Digit. Pengelompokan biner dalam komputer selalu berjumlah 8, dengan istilah 1 Byte. Dalam istilah komputer, 1 Byte = 8 bit. Kode-kode rancang bangun komputer, seperti ASCII, American Standard Code for Information Interchange menggunakan sistem peng-kode-an 1 Byte.

G. Bit

Bit digit sistem angka biner satuan teori komputasi informasi digital. Teori informasi juga sering merujuk pada sebuah dalam (basis 2). Sebagai contoh, angka 1001011 memiliki panjang 7 bit. Digit biner hampir selalu digunakan sebagai terkecil dalam penyimpanan dan komunikasi informasi di dalam dan menggunakan digit natural, disebut komputasi kuantum qubit, sebuah potongan informasi dengan kemungkinan informasi tersebut bernilai benar. *nit* atau *nat*. Sementara, menggunakan satuan Bit juga digunakan sebagai satuan ukuran, yaitu kapasitas informasi dari sebuah digit biner. Lambang yang digunakan adalah bit, dan kadang-

kadang (secara tidak resmi) b (contohnya, modem dengan kecepatan 56 kbps atau 56 kilo bit per second/detik). Satuan ini dikenal juga sebagai shannon, dengan lambang Sh.

H. Byte

Bit Bahasa Inggris: penyimpanan komputer. Satu bit terdiri dari delapan bit. (Byte) adalah istilah yang biasa dipergunakan sebagai satuan dari data dalam Huruf Cakram keras_B digunakan dalam singkatan kepada Byte. (bit menggunakan singkatan b.) seperti kB = kilobita. (hard disk) berkapasitas 40GB secara mudahnya bermaksud cakram keras tersebut mampu menyimpan hingga 40 ribu juta (milyar) bita atau gigabita data.

I. Piksel

Piksel inci. adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah gambar grafis yang dihitung per inci. Piksel sendiri berasal dari akronim bahasa Inggris resolusi, mesin cetak gambar berwarna dapat menghasilkan hasil cetak yang memiliki lebih dari 2.500 titik per *Picture Element* yang disingkat menjadi *Pixel*. Pada ujung tertinggi skala resolusi. mesin cetak gambar berwarna dapat menghasilkan hasil cetak yang memiliki lebih dari 2.500 titik perinci dengan pilihan 16 juta warna lebih untuk setiap inci, dalam istilah komputer berarti gambar seluas satu inci persegi yang bisa ditampilkan pada tingkat resolusi tersebut sepadan dengan 150 juta bit informasi.

Monitor atau layar datar yang sering kita temui terdiri dari ribuan piksel yang terbagi dalam baris-baris dan kolom-kolom. Jumlah piksel yang terdapat dalam sebuah monitor dapat kita ketahui dari resolusinya. Resolusi maksimum yang disediakan oleh monitor adalah 1024x768, maka jumlah piksel yang ada dalam layar monitor tersebut adalah 786432 piksel. Semakin tinggi jumlah piksel yang tersedia dalam monitor, semakin tajam gambar yang mampu ditampilkan oleh monitor tersebut.

J. Model Warna Red Green Blue (RGB)

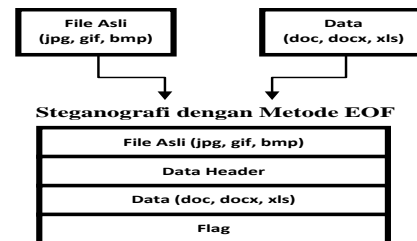
Model warna RGB adalah sebuah model warna tambahan dalam jenis merah, hijau, dan biru muda yang ditambahkan secara bersama dalam berbagai cara untuk memproduksi sebuah kesatuan warna secara luas. Nama dari model ini berasal dari inisial ketiga zat warna primer, yaitu Red (merah), Green (hijau), dan Blue (biru).

Tujuan utama model warna RGB adalah untuk menyajikan, dan menampilkan gambar di dalam sistem elektronik, seperti televisi dan komputer, dan digunakan pula pada fotografi konvensional. Sebelum zaman elektronik, model warna RGB telah mempunyai suatu teori yang kuat di belakang itu, yang didasarkan persepsi manusia terhadap warna.

Tipe alat yang menggunakan input RGB adalah televisi, kamera video, scanner, dan kamera digital. Tipe alat yang menggunakan output RGB adalah televisi satuan dengan berbagai teknologi (CRT, LCD, plasma), komputer, dan layar telepon genggam, proyektor video, dan layar besar seperti Jumbotron, dan lain-lain. Warna printer, bukanlah RGB, tetapi warna *subtractive* (model warna CMYK).

III. ANALISA DAN PERANCANGAN

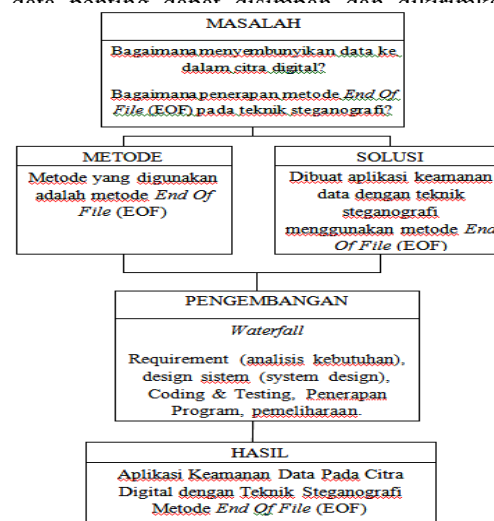
[2] Untuk menyembunyikan pesan pada citra digital ini menggunakan metode *End Of File* (EOF). Metode ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut. Metode EOF yang diimplementasikan pada aplikasi ini merupakan metode EOF dengan menggunakan tanda khusus yang diletakkan pada akhir media file citra digital (FILE ASLI) sebagai pengenal awal (DATA HEADER) dan pengenal akhir (FLAG) dari data yang disisipkan.



Gambar 3. Konsep metode *End Of File* (EOF)

Dari permasalahan yang telah diuraikan di atas, diperlukan adanya sebuah aplikasi yang dapat menjaga kerahasiaan dari sebuah informasi atau data. Sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Aplikasi tersebut nantinya dapat menyisipkan informasi atau pesan rahasia ke dalam citra digital berupa image. Pengguna pertama (pengirim pesan) dapat mengirim image yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (penerima pesan). Kemudian penerima pesan tersebut dapat mengekstraksi informasi rahasia yang ada di dalamnya.

Dengan adanya aplikasi ini diharapkan suatu informasi atau data penting dapat disimpan dan dikirimkan ke pihak yang diinginkan oleh



Gambar 4. Bagan konsep metode *End Of File* (EOF)

Secara umum proses penyisipan pesan teks dan file dokumen ke dalam citra digital yang dilakukan dengan menggunakan metode EOF yaitu menggunakan tanda khusus yang diletakkan pada akhir media file citra digital (FILE ASLI) sebagai pengenalan awal (DATA HEADER) dan pengenalan akhir (FLAG) dari data yang disisipkan. Metode ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut.

Untuk menghasilkan objek citra digital yang sudah dimodifikasi yang berisi informasi rahasia, yang dibutuhkan adalah media penampung berupa citra berekstensi jpg, gif, atau bmp dan informasi rahasia berupa teks atau file dokumen berekstensi docx, pdf, dan xlsx.

[5] Langkah-langkah proses penyisipan pesan rahasia ke dalam citra digital adalah sebagai berikut:

1. Masukkan pertama yaitu media penampung berupa citra digital berekstensi jpg, gif, atau bmp.
2. Masukkan kedua yaitu pesan rahasia berupa pesan teks atau file dokumen berekstensi docx, pdf, atau xlsx.
3. Masukkan password dengan ketentuan sebanyak 8 karakter yang bernilai integer atau angka.
4. Lakukan proses steganografi dengan metode *End Of File* (EOF).
5. Lakukan proses penyimpanan citra digital yang telah disisipkan pesan rahasia.

Langkah-langkah penerapan metode *End Of File* (EOF) dalam steganografi adalah sebagai berikut:

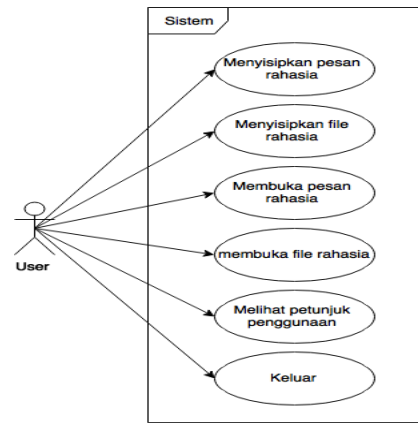
1. Masukkan citra digital berekstensi jpg, gif, atau bmp.
2. Masukkan data berekstensi docx, pdf, atau xlsx.
3. Lakukan penerapan metode *End Of File* (EOF) untuk proses steganografi yang menghasilkan 3 blok sebagai penanda khusus untuk penanda akhir posisi citra digital dan penanda awal posisi data yg disebut Data Header yang menghasilkan penanda akhir pada data berupa Flag.
4. Menghasilkan citra digital yang telah ditumpuk dengan data dan menghasilkan ukuran citra lebih besar dari ukuran sebelumnya.

Proses ekstraksi data dilakukan ketika citra digital sebagai media penampung terdapat data rahasia yang sudah disisipkan. Proses ini dilakukan memanggil data citra digital sebagai media penampung.

Langkah-langkah proses ekstraksi data rahasia adalah sebagai berikut:

1. Masukkan stego image.
2. Masukkan password.
3. Lakukan proses ekstraksi data.

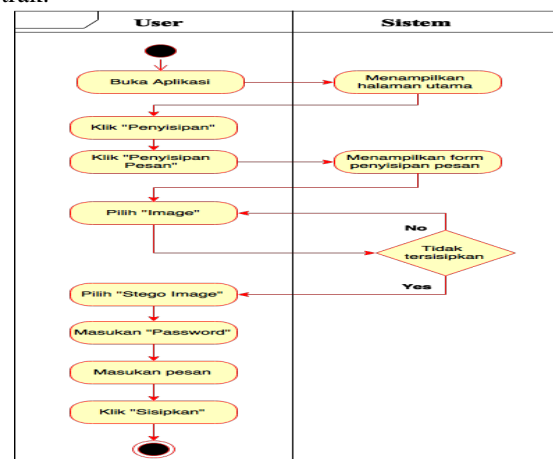
Adapun perancangan berdasarkan diagram *Use Case* menggambarkan pengguna yang akan menggunakan sistem dan perilaku pengguna terhadap sistem sebagai aktor yang terlibat dalam sistem. Berikut diagram *Use Case* Halaman utama :



Gambar 5. Use Case Diagram

Pada gambar diatas pengguna masuk ke halaman utama untuk menggunakan aplikasi yang ingin digunakan sesuai dengan apa yang dibutuhkan, pada halaman utama bisa menyisipkan pesan teks ke dalam citra digital, menyisipkan dokumen ke dalam citra digital, membuka pesan teks yang telah disisipkan, membuka dokumen rahasia yang telah disisipkan, melihat petunjuk penggunaan, dan keluar dari halaman utama.

[6] *Activity Diagram* mempermudah analisis dalam menentukan langkah atau proses yang dikerjakan aplikasi. Berikut *Activity Diagram* aplikasi *Steganografi* citra digital pada proses penyisipan pesan rahasia, dokumen rahasia dan ekstrak.

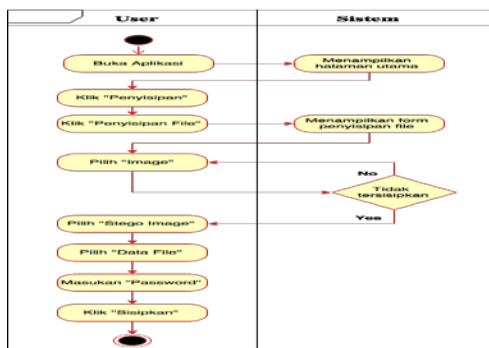


Gambar 6. Activity Diagram Penyisipan Pesan Teks

Dalam gambar *activity diagram* penyisipan pesan teks ini sistem saat mulai membuka aplikasi akan langsung menampilkan halaman utama yang merupakan *user interface* sistem tersebut.

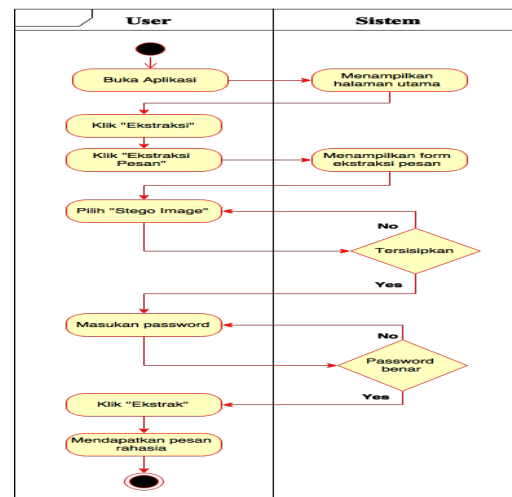
Klik "Penyisipan" lalu pilih "Penyisipan Pesan". Setelah itu pengguna mengklik "Pilih" dan memilih image yang akan di buka. Setelah user memilih image akan ada informasi apakah sebelumnya image tersebut sudah pernah disisipkan pesan atau belum. Jika image belum, akan ada informasi

“Tidak tersisipkan”. Jika sudah, akan ada informasi “Tersisipkan”. Lalu user memilih kembali image yang tidak disisipkan pesan. Lalu setelah image tersebut telah dipilih, pengguna mengklik tombol “Pilih” untuk menentukan stego image. Stego image adalah citra digital yang sudah disisipkan dengan pesan rahasia. Dan memasukkan “Password” lalu memasukkan pesan teks yang akan disisipkan. Setelah itu menekan tombol “Sisipkan” untuk menjalankan proses steganografi pesan teks ke dalam image. Setelah tombol “Sisipkan” ditekan maka system akan menjalankan proses steganografi tersebut.



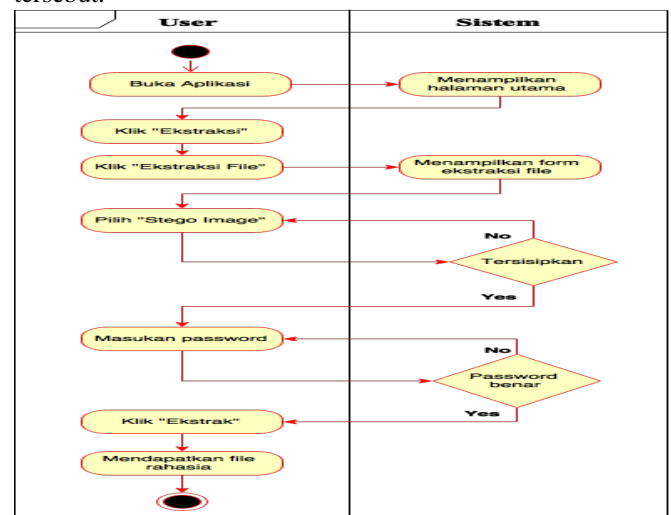
Gambar 8. Activity Diagram Penyisipan Data File

Dalam gambar *activity diagram* penyisipan file dokumen ini sistem saat mulai membuka aplikasi akan langsung menampilkan halaman utama yang merupakan *user interface* sistem tersebut. Klik “Penyisipan” lalu pilih “Penyisipan File”. Setelah itu pengguna mengklik “Pilih” dan memilih image yang akan di buka. Setelah user memilih image akan ada informasi apakah sebelumnya image tersebut sudah pernah disisipkan pesan atau belum. Jika image belum, akan ada informasi “Tidak tersisipkan”. Jika sudah, akan ada informasi “Tersisipkan”. Lalu user memilih kembali image yang tidak disisipkan pesan. Lalu setelah image tersebut telah dipilih, pengguna mengklik tombol “Pilih” pada “Stego Image” untuk menentukan stego image. Lalu menekan tombol “Pilih” pada “Data File” untuk memilih dokumen yang akan disisipkan. Setelah itu menekan tombol “Sisipkan” untuk menjalankan proses steganografi file dokumen ke dalam image. Setelah tombol “Sisipkan” ditekan maka system akan menjalankan proses steganografi tersebut.



Gambar 7. Activity Diagram Ekstrak Pesan

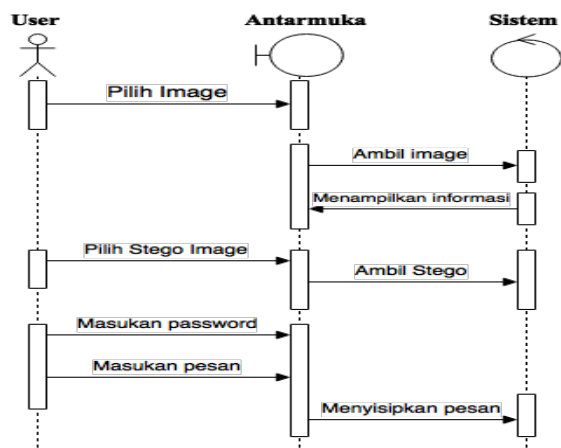
Dalam gambar *activity diagram* ekstrak pesan ini sistem saat mulai membuka aplikasi akan langsung menampilkan halaman utama yang merupakan *user interface* sistem tersebut. Setelah itu saat pengguna mengklik “Ekstraksi” dan memilih “Ekstraksi Pesan” pengguna mengklik “Pilih” pada Stego Image dan memilih citra yang akan di buka. Setelah user memilih Stego Image akan ada informasi apakah sebelumnya image tersebut sudah disisipkan pesan atau belum. Jika belum, akan ada informasi “Tidak tersisipkan”. Lalu user memilih kembali image yang sudah tersisipkan pesan. Jika sudah, akan ada informasi “Tersisipkan”. Lalu user memasukkan “Password”. Setelah melakukan hal tersebut lakukan proses ekstraksi dengan menekan tombol “Ekstrak”. Jika password salah, masukan kembali password. Jika password benar, proses ekstraksi dapat dijalankan dan menampilkan pesan rahasia pada citra digital penampung tersebut.



Gambar 9. Activity Diagram Ekstrak File

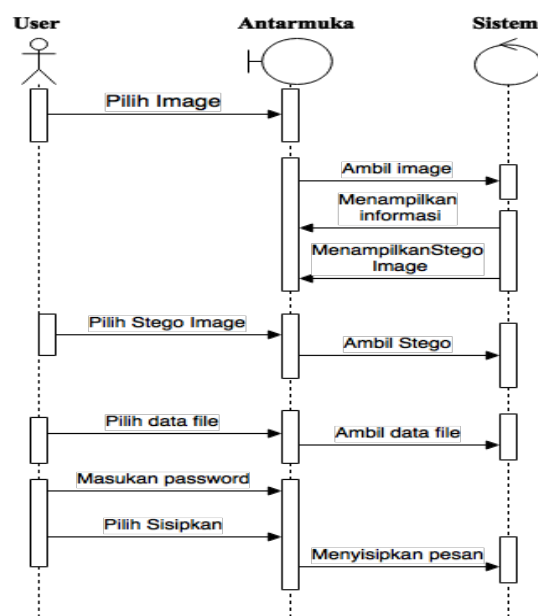
Dalam gambar *activity diagram* ekstrak file ini sistem saat mulai membuka aplikasi akan langsung menampilkan halaman utama yang merupakan *user interface* sistem tersebut. Setelah

itu saat pengguna mengklik “Ekstraksi” dan memilih “Ekstraksi File” pengguna mengklik “Pilih” pada Stego Image dan memilih citra yang akan di buka. Setelah user memilih Stego Image akan ada informasi apakah sebelumnya image tersebut sudah disisipkan pesan atau belum. Jika belum, akan ada informasi “Tidak tersisipkan”. Lalu user memilih kembali image yang sudah tersisipkan pesan. Jika sudah, akan ada informasi “Tersisipkan”. Lalu user memasukkan “Password”. Setelah melakukan hal tersebut lakukan proses ekstraksi dengan menekan tombol “Ekstrak”. Jika password salah, masukan kembali password. Jika password benar, proses ekstraksi dapat dijalankan dan membuka file rahasia pada citra digital penampung tersebut.



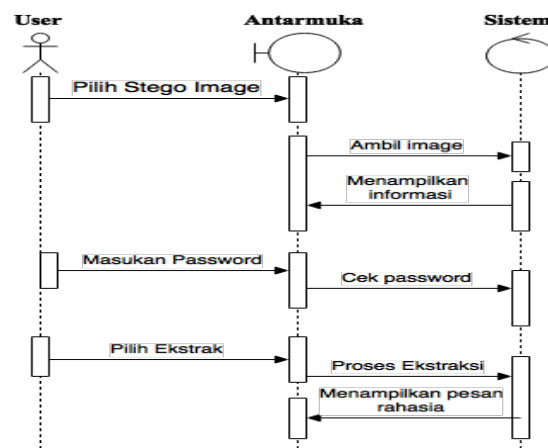
Gambar 10. Sequence Diagram Penyisipan Pesan Teks

Pada gambar diatas menjelaskan tentang menu penyisipan pesan teks, menu “Penyisipan Pesan” dapat ditampilkan dengan mengklik tombol “Penyisipan” pada halaman utama. Pada menu ini, proses awal yang harus dilakukan adalah memilih image yang digunakan sebagai penampung pesan dan akan muncul informasi apakah image tersebut sudah pernah di steganografi atau belum [3]. Setelah itu memilih “Stego Image” sebagai outputnya. Lalu memasukkan password dan mengetik pesan. Proses penyisipan akan dilakukan apabila semua teks box sudah terisi.



Gambar 11. Sequence Diagram Estrak File

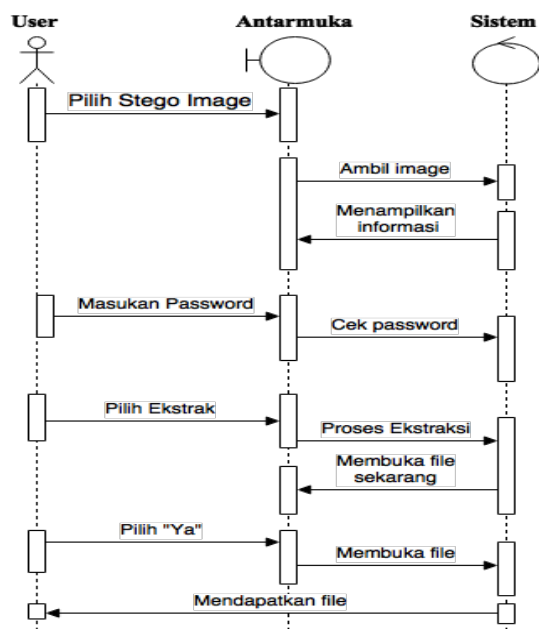
Pada gambar diatas menjelaskan tentang menu penyisipan file, menu “Penyisipan File” dapat ditampilkan dengan mengklik tombol “Penyisipan” pada halaman utama. Pada menu ini, proses awal yang harus dilakukan adalah memilih image yang digunakan sebagai penampung pesan dan akan muncul informasi apakah image tersebut sudah pernah di steganografi atau belum. Setelah itu memilih “Stego Image” sebagai outputnya. Lalu memilih data file yang akan disisipkan dan memasukkan password. Proses penyisipan akan dilakukan apabila semua teks box sudah terisi.



Gambar 12. Sequence Diagram Ekstraksi Pesan

Pada gambar 12, menjelaskan tentang menu ekstraksi pesan, menu “Ekstraksi Pesan” dapat ditampilkan dengan mengklik tombol “Ekstraksi” pada halaman utama. Pada menu ini, proses awal yang harus dilakukan adalah memilih Stego Image setelah itu akan muncul informasi apakah image tersebut sudah tersisipkan pesan atau belum. Setelah itu

memilih memasukkan password. Proses ekstraksi akan dilakukan apabila password benar.

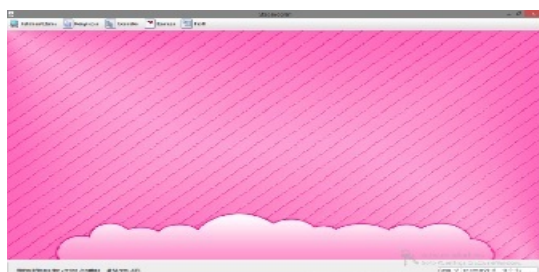


Gambar 13. Sequence Diagram Ekstraksi File

Pada gambar 13 menjelaskan tentang menu ekstraksi file, menu “Ekstraksi File” dapat ditampilkan dengan mengklik tombol “Ekstraksi” pada halaman utama. Pada menu ini, proses awal yang harus dilakukan adalah memilih Stego Image setelah itu akan muncul informasi apakah image tersebut sudah tersisipkan pesan atau belum. Setelah itu memilih memasukkan password. Proses ekstraksi akan dilakukan apabila password benar.

IV. PENGUJIAN APLIKASI

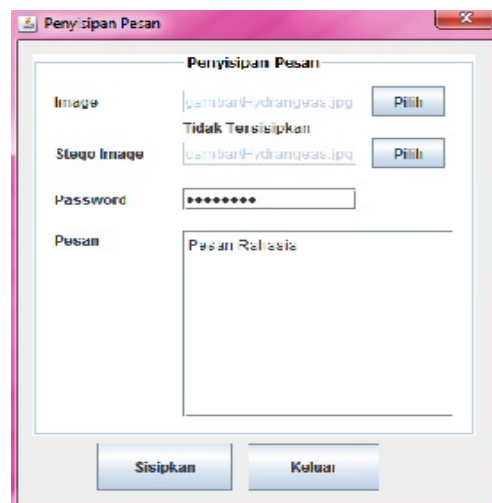
Tampilan halaman utama adalah layar dimana terdapat barisan menu yang dapat diakses oleh user yaitu menu Penyisipan Pesan, Penyisipan File, Ekstraksi Pesan, Ekstraksi File, Bantuan, dan Profil. Berikut beberapa tampilan menu yang telah disediakan :



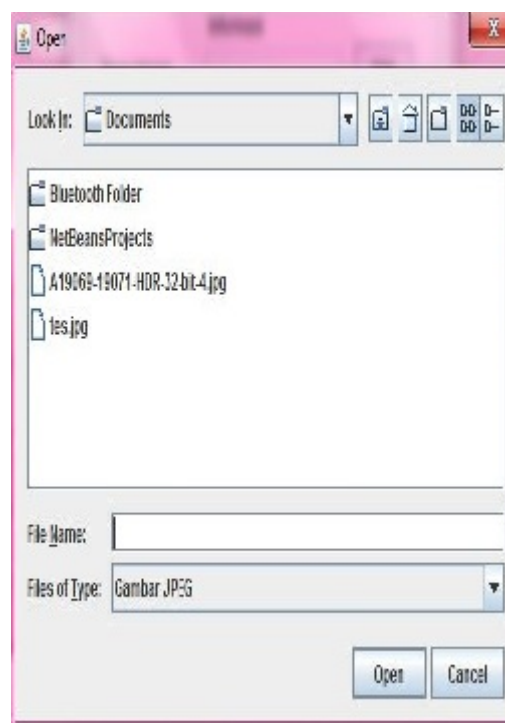
Gambar 14. Tampilan Layar Halaman Utama

Pada form Penyisipan Pesan, user dapat melakukan penyisipan pesan diantaranya dengan mengklik tombol “Pilih” pada Image, setelah memilih image akan ada informasi Tersisipkan atau Tidak Terisipkan. Kemudian klik “Pilih”

pada Stego Image untuk menentukan outputnya. Selanjutnya memasukan password dan mengetik pesan di dalam teks box Pesan. Lalu klik “Sisipkan” setelah itu akan muncul message box sukses atau klik “Keluar” jika ingin keluar dari form Penyisipan Pesan.



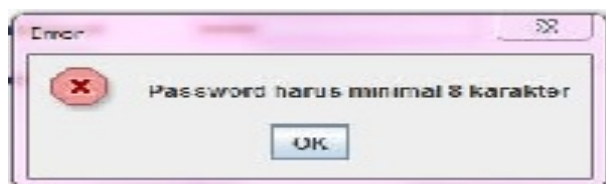
Gambar 15. Tampilan Form Penyisipan Pesan



Gambar 16. Tampilan Pilih Image



Gambar 17. Tampilan Message Box Jika Pesan Sukses

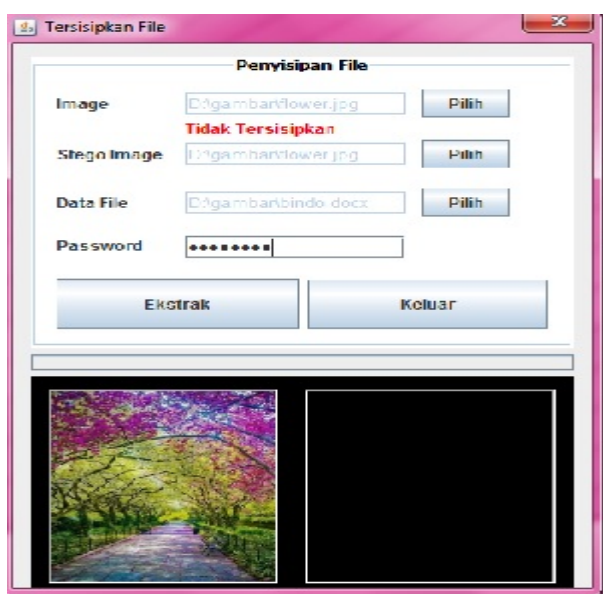


Gambar 18. Tampilan Message Box Password Kurang Dari 8

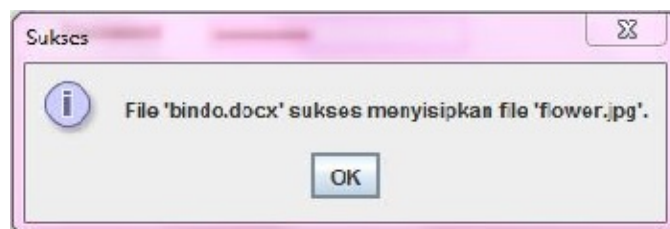


Gambar 19. Tampilan Peringatan Jika Data Belum Lengkap

Pada form Penyisipan File, user dapat melakukan penyisipan file dokumen diantaranya dengan mengklik tombol “Pilih” pada Image, setelah memilih image akan ada informasi Tersisipkan atau Tidak Tersisipkan. Kemudian klik “Pilih” pada Stego Image untuk menentukan outputnya. Selanjutnya klik tombol “Pilih” pada Data File untuk memilih file yang akan disisipkan. Setelah itu memasukan password dan mengklik “Sisipkan” lalu akan muncul message box sukses atau klik “Keluar” jika ingin keluar dari form Penyisipan File.

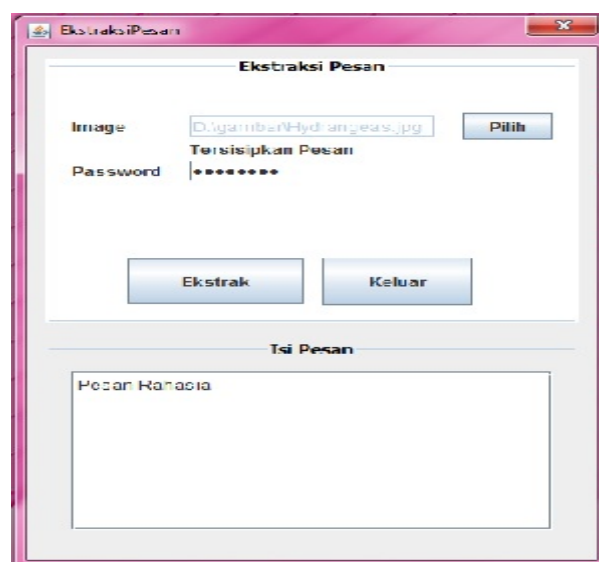


Gambar 20. Tampilan Form Penyisipan File



Gambar 21. Tampilan Message Box Jika File Sukses

Pada form Ekstraksi Pesan, user dapat melakukan ekstraksi pesan diantaranya dengan mengklik tombol “Pilih” pada Stego Image, setelah memilih stego image akan ada informasi Tersisipkan atau Tidak Tersisipkan. Setelah itu memasukan password dan mengklik “Ekstrak” lalu akan muncul pesan rahasia pada teks box pesan.

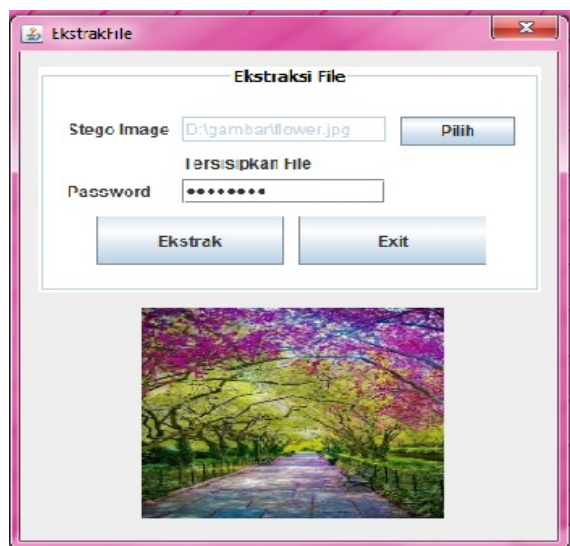


Gambar 22. Tampilan Form Ekstraksi Pesan



Gambar 23. Tampilan Message Box Password Salah

Pada form Ekstraksi File, user dapat melakukan ekstraksi file dokumen diantaranya dengan mengklik tombol “Pilih” pada Stego Image, setelah memilih stego image akan ada informasi Tersisipkan atau Tidak Tersisipkan. Setelah itu memasukan password dan mengklik “Ekstrak” lalu akan muncul message box “buka sekarang” lalu klik “Yes” maka file rahasia akan terbuka.



Gambar 24. Tampilan Form Ekstraksi File



Gambar 25. Tampilan Message Box Ekstraksi Sukses



Gambar 26. Tampilan Frame Bantuan



Gambar 25. Tampilan Frame About Steganografi

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil implementasi yang dilakukan, maka dapat diambil kesimpulan bahwa telah berhasil dirancang sebuah aplikasi steganografi dengan menggunakan metode End of

File yang berbasis pada pemrograman berorientasi objek (Computer Based) dengan menggunakan metode End Of File (EOF) sehingga mengirim data penting dan rahasia menjadi lebih aman.

B. Saran

Selain menarik kesimpulan, adapun beberapa saran yang disampaikan untuk pengembangan system lebih lanjut adalah sebagai berikut:

1. Aplikasi steganografi ini untuk selanjutnya dikembangkan agar file data rahasia hasil ekstrak dapat tersimpan dalam sebuah folder tertentu yang sudah disiapkan dengan cara penambahan database dalam direktori local dari aplikasi steganografi tersebut. Dan dalam pembuatan database tersebut menggunakan konsep *Create, Read, Update, Delete (CRUD)* dalam Netbeans.
2. Aplikasi steganografi ini untuk selanjutnya dapat dikembangkan dengan berorientasi pada Web Based. Untuk pembuatan aplikasi berbasis web tersebut dapat menggunakan bahasa pemrograman PHP, HTML 5, Java Script, CSS, MySql Server dengan menggunakan framework Code Igniter.

DAFTAR PUSTAKA

- [1] Ariyus, Dony. 2009. Keamanan Multimedia. Yogyakarta: Andi Publisher
- [2] Anggraini, yayuk. 2013. Penerapan Steganografi Metode EOF dan Enkripsi DES. Jakarta
- [3] Sembiring, Sanro. 2013. Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File. Medan
- [4] Wahana Komputer. 2010. Pengembangan Aplikasi Database Berbasis JavaDB Dengan Netbeans. Andi Offset
- [5] Wahana Komputer. 2009. Menguasai Java Programming. Jakarta: Salemba Infotek
- [6] Munawar. 2005. Pemodelan Visual dengan UML. Yogyakarta: Graha Ilmu.
- [7] Rahmat, Basuki, Fairuzabadi. Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4. Jurnal Dinamika Informatika Volume 5, Nomor 2, September 2010.
- [8] Armada, Implementasi Steganography Untuk Pesan Multimedia Menggunakan Android, http://Jurnal.Stmikelahma.Ac.Id/Assets/File/ARMADA_Stmikelahma.Pdf (Diakses Pada 29 Oktober 2015).
- [9] Fani Soniavita Hijjati, Asep Mulyana, Analisis Dan Implementasi Aplikasi Pengolahan Citra Berbasis Android Dengan Metode Cross Process Universitas Telkom.