Implementasi Model Steganografi Dalam Mengelola Kerahasiaan Informasi Dengan Metode LSB (*Least Significant Bit*)

Irfan Santiko
STMIK AMIKOM Purwokerto
Fakultas Teknik Informatika
Purwokerto-Jawa Tengah, Indonesia
Email : irfan.santiko@amikompurwokerto.ac.id

***Abstract*—Secara umum program steganografi ini mempunyai fungsi untuk menyembunyikan informasi berupa data digital dibalik data digital lainnya dalam hal ini media yang digunakan adalah citra digital dan harus menjadi perhatian bahwa dalam proses modifikasi perubahan yang terjadi antara media penampung dengan hasil modifikasi media penampung tidak boleh terlalu mencolok atau dengan kata lain terlihat secara kasat mata, perubahan pada citra penampung yang telah termodifikasi tidak terlalu terlihat. Agar suatu kerahasiaan dari informasi yang terkandung dalam objek citra penampung tetap terjaga kerahasiaanya.**

Setelah dilakukan eksperimen dengan menggunakan metode LSB, ternyata metode LSB baik digunakan untuk program steganografi ini, karena dengan metode LSB ukuran teks yang dapat di sisipkan ke dalam gambar lebih besar dan perubahan ukuran gambar setelah disisipkan teks tidak terlalu besar, sehingga dapat menghemat media penyimpanan.

Kata kunci: *Steganografi, LSB (Least Significant Bit)* , gambar.

I. PENDAHULUAN

Keamanan suatu informasi pada jaman global ini makin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut keamanan. Di mana informasi-informasi tersebut tentunya akan semakin banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Saat ini internet sudah berkembang menjadi salah satu media yang populer di dunia, karena fasilitas dan kemudahan yang dimiliki oleh internet, maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasinya semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Sejalan dengan berkembangnya media internet harus diimbangi dengan teknologi pengamanan sistem informasi. Ada tiga teknik melindungi informasi, yaitu:

1. Secara fisik, misalnya menyimpan dalam suatu ruangan khusus dan dikunci dalam lemari besi.
2. Secara organisasi, misalnya menunjuk personil khusus dengan regulasi yang jelas, melakukan pendidikan, dan pelatihan masalah keamanan informasi untuk meningkatkan kesadaran karyawan tentang pentingnya pengamanan informasi yang baik.
3. Secara logik, misalnya dengan menerapkan kriptografi, steganografi, atau memasang antivirus.

Pada teknik pengamanan informasi secara logik di atas terdapat dua teknik yang umum digunakan dalam pengiriman informasi rahasia, yaitu steganografi dan kriptografi. Pada dasarnya steganografi itu berbeda dari kriptografi berdasarkan tujuannya. Pada steganografi, terdapat data atau pesan yang bersifat terbuka, artinya bisa dibaca oleh semua pihak dan terlihat normal, tetapi ternyata menyembunyikan pesan lainnya yang bersifat rahasia dan tidak terlihat, di sini steganografi bertujuan menjaga kerahasian keberadaan pesan.

Di lain pihak, pesan pada kriptografi yang bersifat rahasia tersebut keberadaannya jelas terlihat tetapi terlihat acak, sehingga tidak terbaca oleh pihak yang tidak diinginkan, dengan kata lain kriptografi bertujuan menjaga kerahasiaan isi pesan.

Oleh karena itu, steganografi semakin dibutuhkan guna memberikan keamanan yang maksimal dalam proses pengiriman informasi. Teknik steganografi umum digunakan bersamaan dengan menggunakan dua media yang berbeda, di mana salah satunya berfungsi sebagai media yang berisikan informasi dan yang lain berfungsi sebagai media pembawa informasi tersebut. Penggunaan teknologi steganografi diharapkan dapat membantu upaya peningkatan pengamanan pengiriman informasi dan mempermudah perlindungan atas hak cipta hasil karya media eleltronik.

Citra (*image*) merupakan salah satu bentuk media yang banyak dijumpai. Dengan metode Steganografi maka penyembunyian data di dalam citra (*image*) dapat dilakukan sehingga dapat memungkinkan dilakukannya pengiriman data dengan menggunakan citra digital sebagai pembawa *(carrier).*

Pada metode *steganography* cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format *file digital* yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan diantaranya:

1. Format *image* : *bitmap (bmp), gif, pcx, jpeg, png*, dan lain-lain.
2. Format audio : *wav, voc, mp3*, dan lain-lain.
3. Format lain : *teks file, html, pdf*, dan lain-lain.

Dalam penelitian ini penulis menggunakan *file image* sebagai metode yang digunakan untuk menyembunyikan pesan. Pada *file image* pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah LSB (*Least Significant Bit*) pada data *pixel* yang menyusun *file* tersebut. Alasan pemilihan LSB (*Least Significant Bit*) karena LSB (*Least Significant Bit*) dapat memanipulasi nilai suatu titik warna *(pixel)* sehingga data dapat disembunyikan ke dalam titik warna tersebut namun perubahan yang terjadi diminimalisasi sehingga seakan-akan perubahannya tidak dapat dideteksi oleh mata manusia.

Pentingnya menjaga keamanan informasi rahasia adalah seperti pentingnya menjaga uang dari tindak kejahatan. Dalam penelitian ini akan dibahas pengamanan informasi secara logik, yaitu dengan menerapkan steganografi.

II. TINJAUAN PUSTAKA

A. Definisi Citra

Citra (*image*) adalah gambar pada bidang dua dimensi. Ditinjau dari sudut pandang matematis, *image* merupakan fungsi terus-menerus (*continue*) dari intensitas cahaya pada bidang dua dimensi. Citra (*image*) sebagai output dari suatu sistem perekaman data dapat bersifat optik, berupa foto bersifat analog berupa sinyal video, seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu pita magnetic.[1]

Citra (image) dapat dikelompokkan menjadi dua bagian yaitu citra diam (*still image*) adalah citra tunggal yang tidak bergerak dan citra bergerak (*moving image*) yaitu rangkaian citra diam yang ditampilkan secara beruntun (*sekuensial*), sehingga memberi kesan pada mata sebagai gambar yang bergerak. Setiap citra di dalam rangkaian itu disebut *frame*. Gambar-gambar yang tampak pada film layar lebar atau televisi yaitu terdiri dari ratusan sampai ribuan *frame*.

Dari sudut pandang pencitraan, citra (*image*) adalah rekaman hasil interaksi antara gelombang dengan benda (*object*), yang memberikan sebagian gambaran atau informasi dari benda tersebut. Proses pembentukan citra dengan merekam hasil interaksi inilah yang disebut sebagai proses pencitraan (*imaging*). Dengan demikian ada 3 (tiga) komponen utama dalam pencitraan, yaitu :

1. Gelombang pengindera (*sensing waves*).
2. Benda (*object*).
3. Alat pengindera (*sensor*).

Untuk sebuah sistem koordinat merah-hijau-biru, nilai instanious trimulusnya adalah:

$$R(x,y,t) = C(x,y,t,\lambda)RS(\lambda)d\lambda \int\infty$$
$$G(x,y,t) = C(x,y,t,\lambda)GS(\lambda)d\lambda \int\infty$$
$$B(x,y,t) = C(x,y,t,\lambda)BS(\lambda)d\lambda \int\infty$$

Jika RS(λ),GS(λ),BS(λ) adalah nilai spectral trimulusnya untuk himpunan warna primer merah, hijau dan biru, maka spectral trimulus adalah dalam efek, nilai trimulus dibutuhkan untuk memperlihatkan sejumlah cahaya dengan panjang gelombang λ. Dalam sebuah sistem citra *multispectral*, *field* citra diamati dan dimodelkan sebagai sebuah integral berat *spectral* dari fungsi cahaya citra. *Field spectral* citra adalah:

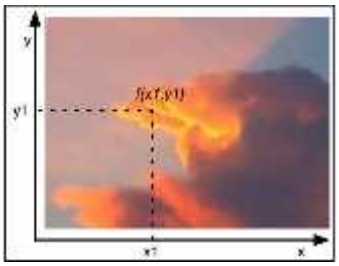
$$F1(x,y,t) = C(x,y,t,\lambda)RS(\lambda)d\lambda \int\infty$$

Di mana $S1(\lambda)$ adalah respon *spectral sensor*. *Image digital* dapat disimpan dalam beberapa format yang berbeda.[1]

Berdasarkan paparan diatas dapat disimpulkan bahwa citra merupakan suatu larik dua dimensi atau suatu matriks yang elemen-elemennya menyatakaan tingkat keabuan dari elemen gambar, jadi informasi yang terkandung bersifat diskret. Dengan demikian untuk mendapatkan suatu citra (*image*) diperlukan konversi, sehingga *image* tersebut selanjutnya dapat diproses menggunakan komputer.

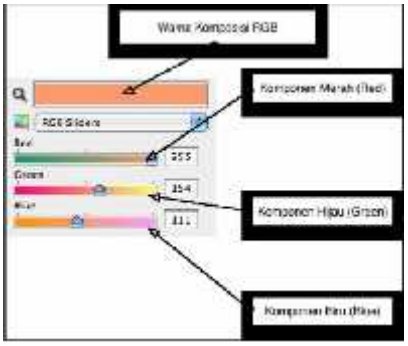
B. *Citra Digital*

Citra (*image*) dapat digambarkan sebagai fungsi dua variabel, f(x,y), di mana *x* dan *y* adalah koordinat spasial dan nilai f(*x, y)* adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada Gambar 1. 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) (http://repository.usu.ac.id).



Gambar 1. Koordinat Nilai Intensitas Pada Citra [2]

Sebuah citra diubah ke bentuk digital agar dapat disimpan dalam memori komputer atau media lain. Proses mengubah citra ke bentuk digital bisa dilakukan dengan beberapa perangkat, misalnya *scanner*, kamera digital, dan *handycam*. Ketika sebuah citra sudah diubah ke dalam bentuk digital (selanjutnya disebut citra digital), bermacam-macam proses pengolahan citra dapat dilakukan terhadap citra tersebut. [2]



Gambar 2. Komposisi Warna RGB [2]

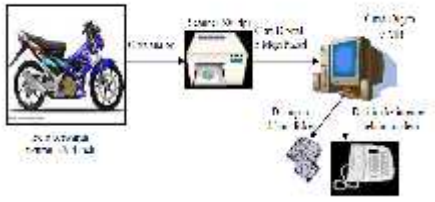
Ada banyak aplikasi pengolahan citra digital, namun pada dasarnya tujuan dari pengolahan citra digital adalah: [2]

1. Peningkatan kualitas citra (*Image enhancement*), operasi peningkatan kualitas citra bertujuan untuk menekankan ciri-ciri tertentu pada citra yang kemudian digunakan sebagai bahan analisis. Contohnya antara lain : kecerahan dan peningkatan kualitas tepi , penapisan derau, dan penajaman. Peningkatan kualitas citra berguna dalam operasi ektraksi ciri, analisis citra, dan tampilan informasi visual. Proses peningkatan kualitas itu sendiri tidak akan menambah isi informasi yang sudah ada, tetapi akan meningkatkan cakupan dinamis dari ciri yang dipilih sehingga ciri yang akan dianalisis tersebut akan dapat dideteksi dengan mudah.
2. Pemulihan citra (*Image restoration*), perbaikan citra berhubungan dengan penghilangan atau peminimalisasian degradasi yang diketahui pada citra. Hal ini termasuk penghilangan *blur* pada citra yang mengalami degradasi yang berhubungan dengan keterbatasan sensor atau lingkungannya, penapisan derau, dan koreksi terhadap distorsi geometris atau ketidaklinearan yang disebabkan oleh sensor.
3. Pengukuran dan analisis citra (*Image measurement and analysis*), pengukuran dan analisis citra bertujuan untuk melakukan pengukuran kuantitatif dari sebuah citra untuk menghasilkan deskripsi tentang citra tersebut. Dalam bentuk yang paling sederhana berupa pembacaan label dari barang belanjaan, atau mengukur besar dan orientasi sel darah dalam sebuah citra medis.
4. Rekonstruksi citra (*Image reconstruction*), rekonstruksi citra dari proyeksi adalah kelas khusus dari permasalahan perbaikan citra dimana sebuah objek dua (atau lebih) dimensi direkonstruksi dari beberapa proyeksi satu dimensi. Tiap-tiap proyeksi diperoleh dengan memproyeksikan sinar-X paralel (atau radiasi tajam lainnya) melalui objek tersebut.
5. Pemampatan data citra (*Image data compression*), Jumlah data yang diasosiasikan dengan informasi visual adalah sangat besar, sehingga penyimpanannya akan membutuhkan kapasitas penyimpanan yang sangat-sangat besar. Meskipun kapasitas penyimpanan dari beberapa media penyimpanan cukup besar, kecepatan aksesnya biasanya berbanding terbalik terhadap kapasitasnya. Pemampatan data citra berhubungan dengan minimisasi jumlah bit yang diperlukan untuk menyajikan sebuah citra.

Tujuan dari pemampatan data citra yaitu untuk mengurangi ukuran berkas yang menyimpan data citra tersebut. Berkas data citra biasanya berisi sejumlah besar informasi yang berulang dan banyak bagian yang tidak relevan. Teknik pemampatan data mengeksploitasi redundansi dan ketakrelevanan dengan mentransformasi berkas data menjadi berkas yang lebih kecil dari yang mana berkas citra aslinya nanti dapat direkonstruksi sama persis atau hampir sama dengan aslinya.

Secara umum teknik pemampatan dapat dibagi menjadi dua bagian besar, *lossy* dan *lossless*. Algoritma pemampatan *lossy* menghilangkan hanya informasi berulang saja, sehingga pada saat penirmampatkan, citra yang telah dimampatkan dapat ditampilkan tepat seperti aslinya. Algoritma pemampatan *lossless* selain menghilangkan informasi yang berulang, juga menghilangkan informasi yang tidak relevan, dan dengan demikian hanya memungkinkan rekonstruksi yang mendekati citra aslinya, bukannya duplikat yang sama persis. Sebagaimana dapat di perkirakan, algoritma pemampatan *lossless* memungkinkan rasio yang lebih tinggi. Contoh jenis pemampatan data citra yang berkarakteristik tak berugi adalah GIF *Encoding*. Dalam skripsi ini, akan membahas tentang pemampatan citra yang berkarakteristik *lossy.*

Pemampatan citra bertujuan untuk meminimalkan jumlah bit yang diperlukan untuk menunjukkan citra. Apabila sebuah foto berwarna berukuran 3 inci x 4 inci diubah ke bentuk digital dengan tingkat resolusi sebesar 500 (dpi), maka diperlukan 3 x 4 x 500 x 500 = 3.000.000 piksel. Setiap piksel terdiri dari 3 *byte* dimana masing-masing *byte* menunjukkan warna merah, hijau, dan biru. sehingga citra digital tersebut memerlukan volume penyimpanan sebesar 3.000.000 x 3 *byte* +1024 = 9.001.024 *byte* setelah ditambahkan jumlah *byte* yang diperlukan untuk menyimpan format awalan citra. Citra tersebut tidak bisa disimpan ke dalam disket yang berukuran 1.4 MB. Selain itu, pengiriman citra berukuran 9 MB memerlukan waktu lebih lama. Untuk koneksi *internet dial-up* 8 (56 kbps), pengiriman citra berukuran 9 MB memerlukan waktu 21 menit. Untuk itu diperlukan pemampatan citra sehingga ukuran citra tersebut menjadi lebih kecil dan waktu pengiriman citra menjadi lebih cepat. Citra yang belum dimampatkan disebut citra mentah (*raw image*). Sementara citra hasil pemampatan disebut citra termampatkan (*compressed image*). Proses pengiriman dan penyimpanan citra tersebut diilustrasikan pada Gambar 3.



Gambar 3. Proses Konversi citra analog ke citra digital beserta pengirimannya

Berdasarkan paparan diatas dapat disimpulkan bahwa sebuah citra dapat diubah ke bentuk digital agar dapat disimpan ke dalam memori komputer atau media lain. Ketika sebuah citra sudah diubah ke dalam bentuk digital (selanjutnya disebut citra digital), bermacam-macam proses pengolahan citra dapat dilakukan terhadap citra tersebut, misalnya dengan memanfaatkan citra sebagai media untuk menyembunyikan pesan dengan cara steganografi.[3]

III. PEMBAHASAN

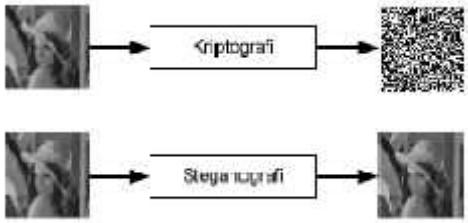
A. Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, di mana fungsi dari teknik *steganography* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas (Waheed, 2000). Kata steganografi berasal dari bahasa Yunani, yaitu dari kata Steganï£¡ (tersembunyi) dan Graptos (tulisan). Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video. Teknik *Steganography* ini telah banyak digunakan dalam strategi peperangan dan pengiriman sandi rahasia sejak jaman dahulu kala. Dalam perang Dunia II, teknik *steganography* umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman. [3]

Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi *steganography* dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, *steganography* digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi [3]

Satu hal penting yang menjadi kelebihan steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Namun begitu terbentuk pula suatu teknik yang dikenal dengan steganalysis, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu arsip. Seorang steganalyst tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya. [7]

Steganografi berbeda dengan kriptografi, di mana pihak ketiga dapat mendeteksi adanya data (*chipertext*), karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan, tetapi dapat dikembalikan ke bentuk semula. Ilustrasi mengenai perbedaan kriptografi dan steganografi dapat dilihat pada gambar 4.



Gambar 4. Ilustrasi kriptografi dan steganografi pada citra digital

Perbedaan yang mendasar antara steganografi dan kriptografi terletak pada proses penyembunyian data dan hasil akhir proses tersebut. Kriptografi melakukan proses pengacakan data asli sehingga dihasilkan data terenkripsi dan benar-benar acak dan berbeda dengan aslinya. Sementara itu, steganografi menyembunyikan data dalam data lain dengan cara menumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga tampilan data tetap terlihat sama. Lebih detailnya ada pada table berikut:

TABEL I. PERBEDAAN STEGANOGRAFI DENGAN KRIPTOGRAFI [3]

Steganografi	**Kriptografi**
1. Menyembunyikan pesan pada pesan lainnya dan tampak seperti normal grafik, video, dan file suara	1. Pesan disembunyikan dengan menggunakan enkripsi, sehingga tidak memiliki arti
2. Disimpan dalam bentuk koleksi gambar, video file, sound file, didalam harddisk, disket, CD, DVD, flashdisk sehingga tidak mencurigakan	2. Disimpan dalam bentuk koleksi karakter acak pada harddisk, disket, CD, DVD, USB, flashdisk sehingga menimbulkan kecurigaaan
3. Seorang Eavesdropper bisa mendeteksi sesuatu yang berubah pada format pesan (seperti text ke graphic image)	3. Seorang Eavesdropper bisa mendeteksi komunikasi rahasia dari pesan yang sudah di enkodekan
4. Memerlukan kewaspadaan ketika menggunakan kembali gambar/sound file	4. Memerlukan kewaspadaan ketika menggunakan kembali kunci yang pernah digunakan
5. Tidak ada assosiasi hukum pada steganografi	5. Ada beberapa assosiasi hukum untuk kriptografi
6. Kerahasiaan tergantung pada media dan teknik yang akan ditumpangi	6. Kerahasiaan tergantung pada/dari algoritma dan kunci yang akan digunakan
7. Berbasis multimedia	7. Berbasis huruf dan angka

Steganografi membahas bagaimana sebuah pesan dapat disisipkan ke dalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem indera manusia seperti mata dan telinga. Dengan adanya keterbatasan inilah, metoda steganografi ini dapat diterapkan pada berbagai media digital. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi di sini sebatas oleh kemampuan indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya.

Media penyisipan pesan rahasia yang digunakan dalam teknik Steganografi antara lain adalah: [4]

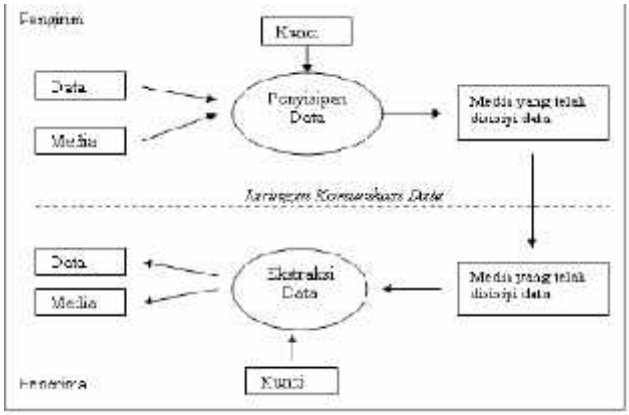
1. Teks, dalam algoritma *Steganography* yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik NLP sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya. Contoh format teks : *text file, html, pdf,* dan lain-lain.
2. Audio, format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula. Contoh format audio : *wav, voc, mp3*, dan lain-lain.
3. Citra, format ini pun paling sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma Steganografi untuk media penampung yang berupa citra. Contoh format citra : *bitmap (bmp), gif, pcx, jpeg, png* dan lain-lain.
4. Video, format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.Contoh format video : *mpeg, avi* dan lain-lain.

Penyembunyian data rahasia ke dalam media digital mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data diantaranya adalah [4]:

1. *Fidelity*, mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
2. *Robustness*, pesan yang disembunyikan harus ditahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada *stego-data*, seperti pengubahan kontras, penajaman, pemempatan, rotasi, perbesaran gambar, pemotongan *cropping*, enkripsi dan sebagainya. Bila pada citra penampung dilakukan operasi-operasi pengolahan citra tersebut, maka pesan yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstrasi kembali).
3. *Recovery*, data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

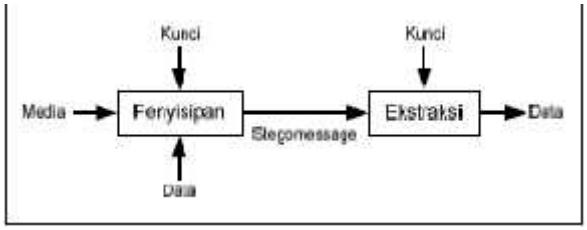
Teknik penyembunyian data ke dalam *covertext* dapat dilakukan dalam dua macam domain: [7]

1. Domain spasial/waktu (*spatial/time domain*), teknik ini memodifikasi langsung nilai *byte* dari *covertext* (nilai *byte* dapat merepresentasikan intesitas/warna *pixel* atau amplitude). Metode yang tergolong ke dalam teknik ranah spasial adalah metode LSB (*Least Significant Bit*).
2. Domain transform (*frequency transform domain*), teknik ini memodofikasi langsung hasil transformasi frekuensi sinyal. Metode yang tergolong ke dalam teknik ini ranah frekuensi adalah *spread spectrum*.



Gambar 5. Diagram Sistem Steganografi

Steganografi menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Penyisipan pesan ke dalam media *covertext* dinamakan encoding, sedangkan ekstraksi pesan dari *stegotext* dinamakan decoding. Kedua proses ini memerlukan kunci rahasia (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan Proses tersebut dapat dilihat pada gambar 2.6. Penambahan kunci yang bersifat opsional dimaksudkan untuk lebih meningkatkan keamanan (SUH04).



Gambar 6. Proses penyisipan dan ekstraksi pesan dalam steganografi

Terdapat beberapa istilah yang berkaitan dengan steganografi [4] :

1. *Hiddentext* atau *embedded message*: pesan atau informasi yang disembunyikan.
2. *Covertext* atau *cover-object*: pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stegotext* atau *stego-object*: pesan yang sudah berisi *embedded message*. Dalam steganografi digital, baik *hiddentext* atau *covertext* dapat berupa teks, audio, gambar, maupun video.

Semua file - fileberharga perusahaan di simpan di ruang bawah tanah rumah, file tersebut tersimpan pada sebuah lemari besi yang tersembunyi dibalik lemari tua dengan serial kunci 16A05m11p.		
Hiddentext	Covertext/Cover-object	Stegotext/Stego-object

Gambar 7. Contoh Hiddentext, Covertext dan Stegotext

Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra *(image)*, *audio*, atau *video*. Satu hal penting yang menjadi kelebihan steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Namun begitu, dikenal juga suatu teknik *steganalysis*, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu arsip.

Seorang *steganalyst* tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya. Terdapat beberapa cara yang dapat digunakan untuk mendeteksi steganografi seperti melakukan pengamatan terhadap suatu arsip dan membandingkannya dengan salinan arsip yang dianggap belum direkayasa, atau berusaha mendengarkan dan membandingkan perbedaannya dengan arsip lain bila arsip tersebut adalah dalam bentuk citra.

Berdasarkan paparan diatas dapat disimpulkan bahwa steganografi (*steganography*) adalah ilmu atau seni menyembunyikan pesan didalam pesan lain sehingga keberadaan pesan yang pertama tidak diketahui [4] berbeda dengan kriptografi, dimana pihak ketiga dapat mendeteksi adanya data (*chipertext*), karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya data tersebut seolah-olah berantakan, tetapi dapat dikembalikan ke bentuk semula.

B. LSB (Least Significant Bit)

Faktor yang mendasari dibentuknya perangkat lunak dengan metode LSB (*Least Significant Bit*) ini adalah keamanan data. Keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah sistem informasi umumnya ditujukan bagi segolongan orang tertentu, oleh karena itu sangatlah penting untuk mencegahnya agar tidak jatuh pada pihak-pihak yang tidak berhak. Untuk keperluan tersebut, maka diperlukan sebuah teknik steganografi dengan metode LSB (*Least Significant Bit*). Karakter-karakter teks yang disisipkan ke dalam gambar atau yang dikenal dengan proses *steganografi* adalah seperti pada Tabel II.

TABEL II. KODE ASCII [5]

No	Karakter	Kode ASCII
1	Spasi	32
2	!	33
3	#	35
4	$	36
5	%	37
6	&	38
7	(	40
8	)	41
9	*	42
10	+	43
11	,	44
12	-	45
13	.	46
14	/	47
15	0	48
16	1	49
17	2	50
18	3	51
19	4	52
20	5	53
21	6	54
22	7	55
23	8	56
24	9	57
25	:	58
26	;	59
27	<	60
28	=	61
29	>	62
30	?	63
31	@	64
32	A	65
33	B	66
34	C	67
35	D	68
36	E	69
37	F	70
38	G	71
39	H	72
40	I	73
41	J	74
42	K	75
43	L	76
44	M	77
45	N	78
46	O	79

47	P	80
48	Q	81
49	R	82
50	S	83
51	T	84
52	U	85
53	V	86
54	W	87
55	X	88
56	Y	89
57	Z	90
58	[	91
59	\	92
60	]	93
61	^	94
62	_	95
63	{	123
64	|	124
65	}	125

Gambar 8. Doggy

Misal Gambar 8. menggunakan format pewarnaan RGB, artinya tiap pixel dari gambar ini direpresentasikan dengan nilai sepanjang 24 bit. Pesan Rahasia yang dicoba untuk dimasukkan adalah “aku#“, yang jika direpresentasikan ke dalam *binary* kata “aku#“ini menjadi”[5]

Tabel III. KODE ASCII

character	ASCII value (decimal)
a	97
k	107
u	117
#	35

Kode ASCII tersebut untuk selanjutnya diubah menjadi 8 bit kode-kode biner sehingga di dapat:

Tabel IV. Kode Biner

character	biner
a	01100001
k	01101011
u	01110101
#	00100011

Konversi citra ke biner citra Gambar 8 di atas sebagai berikut:

TABEL V. CITRA DALAM BENTUK BINER

11000100	00001010	01100000	10110110	01100101	00101000	…
01000011	11001000	01100101	00110010	01011010	00110010	…
00011000	10010110	00101101	11001000	01001011	00011100	…
10110001	00111000	01001100	01100101	00011001	11001000	…
01100101	00100010	11111010	00101000	01100100	00111100	…
00101100	01000010	01100010	01111101	10111110	11001000	…
…	…	…	…	…	…	…

Untuk selanjutnya, tiap bit kode biner pesan rahasia digunakan untuk menggantikan bit terakhir dari kode *biner image* doggy. Proses penggantian dilakukan dengan memilih *byte* tertentu secara acak. Proses pengacakan tersebut bergantung pada kata kunci (*password*) yang menjadi *random seed* atau titik awal dilakukannya pengacakan. Kata kunci yang coba dimasukkan adalah “IBU” dengan asumsi gambar 3.8 berukuran 256 x 256 pixel dengan total byte yang dimiliki adalah 196608 byte. Berikut merupakan nilai desimal dari kata kunci yang dimasukkan.

TABEL VI. TABEL BINER

character	ASCII value (decimal)	biner
I	73	01001001
B	66	01000010
U	85	01010101

Proses penempatan bit citra rahasia pada citra sebagai berikut:

Tabel VII. PROSES PENYISIPAN PESAN

11000100	00001010	01100000	10110110	01100101	00101000	…
01000011	11001000	01100101	00110010	01011010	00110010	…
00011000	10010110	00101101	11001000	01001011	00011100	…
10110001	00111000	01001100	01100101	00011001	11001000	…
01100101	00100010	11111010	00101000	01100100	00111100	…
00101100	01000010	01100010	01111101	10111110	11001000	…
11000100	00001010	01100001	10110110	01100101	00101001	…
01000010	11001000	01100101	00110011	01011010	00110011	…
00011000	10010110	00101101	11001000	01001011	00011100	…
10110000	00111000	01001101	01100001	00011001	11001000	…
01100101	00100010	11111010	00101000	01100100	00111100	…
00101100	01000010	01100011	01111101	10111110	11001000	…
…	…	…	…	…	…	…

Citra dalam bentuk biner ini akan dipetakan kembali ke bentuk citra. Ekstraksi pesan dapat dengan mudah dilakukan dengan mengambil bit terakhir dari kode biner citra. Jika diperhatikan, penggantian bit terakhir tersebut tidak terlalu berpengaruh terhadap perubahan warna citra.

Proses pengiriman pesan rahasia dari pengirim hingga sampai kepada orang yang menerima sebagai berikut: [6]

1. Tentukan pesan yang akan dikirimkan dan juga kata kunci (*password*) untuk melindungi pesan rahasia tersebut.
2. Tentukan *image* penampung yang akan digunakan *image* penampung dan pesan rahasia yang akan dikirimkan diubah kedalam bentuk biner.
3. Lakukan proses penempatan pesan rahasia pada *byte image* penampung secara acak dimana bilangan acak diperoleh dari pembangkitan acak semu dimana kata kunci berperan sebagai titik awal pengacakan.
4. Proses pengambilan pesan rahasia di mulai dengan memasukan kata kunci yang digunakan, selanjutnya kata kunci tersebut akan membangkitkan bilangan acak yang sama dengan sewaktu proses penempatan pesan rahasia, pembacaan bit-bit pesan rahasia dilakukan sesuai dengan urutan *byte* yang telah ditentukan secara acak.
5. Pesan rahasia yang telah berhasil di baca *bit-bit*nya kemudian akan diubah kembali kepada bentuk asalnya.

Berdasarkan analisis yang dilakukan terhadap kebutuhan perangkat lunak dapat disimpulkan bahwa perangkat lunak yang dibangun untuk mengimplementasikan steganografi pada *file image*. Perangkat lunak ini diberi nama *ImageStego*. Perangkat lunak yang akan dibangun nantinya akan menghasilkan sebuah *file image* berisi pesan dari proses *encode* dan file pengungkapan *file image* dari proses *decode*. Pengguna dari perangkat lunak ini adalah setiap individu yang memerlukan keamanan data, untuk itu sistem yang dibangun nantinya harus dapat dipakai oleh setiap orang secara umum, sehingga perangkat lunak yang akan dibangun harus memiliki antarmuka (*interface*) yang sederhana dan mudah digunakan. Adapun sumber daya sistem untuk membangun perangkat lunak tersebut menggunakan *Windows Seven Ultimate* dan menggunakan bahasa pemrograman *Java*. Analisis perangkat lunak yang dibangun meliputi spesifikasi system.

Pada spesifikasi sistem ini meliputi kebutuhan perangkat lunak, tujuan pengembangan perangkat lunak, dan arsitektur perangkat lunak.

a. Kebutuhan Perangkat Lunak
   Berdasarkan uraian pada bab-bab sebelumnya, maka diperlukan suatu perangkat lunak yang dapat memenuhi kebutuhan berikut:
   1). Menerima masukan file image digital asli maupun file image digital yang sudah disisipi data
   2). Mampu menyisipkan data kedalam file image digital.
   3). Mampu menyimpan file image digital yang sudah disisipi data.
   4). Mampu mengekstrasi *file image* yang sudah disisipi data untuk mendapatkan data yang valid.
   5). Mampu menampilkan *file image* untuk mengamati perubahan yang terjadi sebelum dan sesudah *file image* yang telah disisipi data.
b. Tujuan Pengembangan Perangkat Lunak
   ImageStego ditujukan untuk menyisipkan *file* data *biner* kedalam *file image*. *ImageStego* juga mampu mengekstrasi data yang disisipkan kedalam *file image* tersebut, serta mampu menampilkan *file image* sebelum maupun setelah disisipi data.
c. Arsitektur Perangkat Lunak
   Secara garis besar, perangkat lunak *ImageStego* memiliki dua komponen utama yaitu komponen penyisipan data kedalam *file image* dan komponen ekstraksi *file image* yang telah disisipi data. Masukan untuk komponen penyisipan data kedalam *file image* ini adalah *file image* sebagai *cover*, data yang akan disispkan, dan sebuah kunci

Komponen ekstrasi *file image* melakukan proses ektraksi kembali *file image* yang telah disisipi data untuk mendapatkan data yang valid. Masukan dari komponen ini adalah *file image* dan sebuah kunci. Keluaran dari komponen ini adalah *file image* dan *file* data yang disisipkan. Perangkat lunak StegoImage dikembangkan pada komputer dengan sistem operasi microsoft *Windows Seven Ultimate*. Bahasa yang digunakan dalam implementasi perangkat lunak *StegoImage* adalah bahasa Pemrograman *Java* dan *NetBeans IDE 6.8* sebagai editornya.

IV. KESIMPULAN

Dari analisis dan hasil implementasi Perancangan dan Implementasi Aplikasi Steganografi dengan Metode LSB (*Least Significant Bit*) dapat disimpulkan bahwa program aplikasi steganografi ini dapat digunakan untuk:

1. Menyembunyikan informasi berupa teks ke dalam objek digital.
2. Objek digital yang digunakan sebagai objek penampung tidak harus merupakan objek gambar/*image* dengan ekstensi PNG.
3. Teks yang disembunyikan berupa teks yang langsung diketikkan.
4. Setelah dilakukan eksperimen dengan menggunakan metode LSB, ternyata metode LSB baik digunakan untuk program steganografi ini, karena dengan metode LSB ukuran teks yang dapat di sisipkan ke dalam gambar lebih besar dan perubahan ukuran gambar setelah disisipkan teks tidak terlalu besar, sehingga dapat menghemat media penyimpanan.
5. Dengan metode LSB juga dapat dilakukan penghematan *file* yang cukup signifikan, dengan konsekuensi kecerahan gambar yang dihasilkan pada objek stego ini sedikit berkurang.
6. Dengan metode LSB keamanan dan kerahasiaan informasi yang disampaikan lebih terjamin karena dilengkapi dengan *password* untuk membuka *file*.
7. Adapun kelebihan dari aplikasi steganografi ini yaitu dapat digunakan untuk menghemat media penyimpanan.

Selain itu, juga dapat digunakan untuk menjaga keamanan informasi yang telah dibuat oleh seseorang.

Pada aplikasi Steganografi ini, Sifat LSB yang *fragile* membuat pesan rahasia yang mengalami serangan akan hilang, *file image* yang dihasilkan setelah proses penyisipan mengalami pengurangan kualitas yang cukup banyak bergantung dari jumlah karakter yang disisipkan, dimana semakin banyak karakter yang disisipkan maka semakin besar pula pengurangan kualitas *image* yang diperoleh. Oleh karena itu, untuk meningkatkan kualitas *image* dihasilkan maka kedepannya diharapkan dapat dikembangkan suatu aplikasi Steganografi dengan metode lain yang lebih baik agar kualitas *image* yang dihasilkan tidak jauh berbeda dengan kualitas *image* yang asli.

DAFTAR PUSTAKA

[1] Munir, R. (2004). Pengolahan Citra Digital dengan Pendekatan Algoritmik, Informatika Bandung.
[2] B. Achmad & Firdausy K. (2005) Teknik Pengolahan Citra Digital. Andi Offset: Yogyakarta.
[3] Ariyus Dony. (2007). Keamanan Multimedia. Andi Offset: Yogyakarta.
[4] Munir, R. (2008). Steganografi dan Watermarking : Informatika Bandung
[5] Simmons., G. (1983). The prisoner's problem and the subliminal channel In Crypto'83
[6] Waheed, Q. (2000). Steganography and Steganalysis. Disertasi, Universitas Gunadarma.
[7] Kadir, A. (2004). Dasar Pemrograman Java 2. Andi Offset:Yogyakarta.