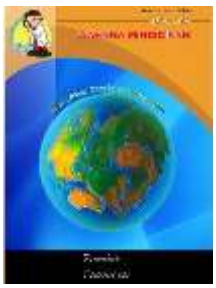
Jurnal Ilmiah Wahana Pendidikan

https://jurnal.peneliti.net/index.php/JIWP

Vol. 7, No. 5, September 2021



Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode *Least Significant Bit (LSB)*

Lasarus Pelipus Malese

Program Studi Teknik Informatika Universitas Tribuana Kalabahi
Email: lasarusmalese@gmail.com

Info Artikel
Sejarah Artikel:
Diterima: 30 Agustus 2021
Direvisi: 28 September 2021
Dipublikasikan: September 2021
e-ISSN: 2089-5364
p-ISSN: 2622-8327
DOI: 10.5281/zenodo.5563416

Abstract:
The rapid development of digital media and its use in various fields raises greater demands to create an information delivery system that is guaranteed to be secure. One of them is with steganography. Steganography is a method for inserting pieces of confidential information in an object or other media. With steganography, information is hidden in such a way that its whereabouts are unknown, which is known as information hiding. This method is different from the cryptographic method, which encodes existing information so that it cannot be read without knowing the key or password used, but its existence is still known and not hidden. This final project was developed using Microsoft Visual Basic 6.0 implementing the Simple Least Significant Bit Substitution ("simple LSB substitution") steganography method to hide information into a multimedia file. Multimedia files used are image files, audio files, and video files as a medium for carrying confidential information. The use of steganography technology is expected to increase security in the delivery of information, so that important information will be protected and its presence disguised in multimedia files. This is also expected to help the process of protecting the copyright of electronic media works.

Keywords: *steganography, multimedia, information insertion, simple LSB substitution*

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 tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana informasi-informasi tersebut

tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Oleh karena itu, *steganography* semakin dibutuhkan guna memberikan keamanan yang maksimal dalam proses pengiriman informasi. *Steganography* merupakan cara untuk menyembunyikan suatu pesan atau data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Teknik *steganography* umum digunakan bersamaan dengan menggunakan dua media yang berbeda, dimana salah satunya berfungsi sebagai media yang berisikan informasi (*carrier file*) dan yang lain berfungsi sebagai media pembawa informasi tersebut (*secret file*).

Melalui penelitian ini dibangun suatu aplikasi berbasis Microsoft Visual Basic 6.0 yang mengimplementasikan steganografi dengan menggunakan metode simple least lignificant bit substitution sebagai cara untuk menyembunyikan suatu informasi ke dalam file multimedia. Penggunaan teknologi steganografi ini diharapkan bukan hanya dapat membantu upaya meningkatkan keamanan penyampaian informasi, namun juga dapat membantu dalam proses perlindungan atas hak cipta hasil karya media elektronik.

KAJIAN PUSTAKA

Pengertian Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yang terdiri dari kata *steganos* yang artinya tersembunyi dan *graphein* yang artinya menulis, sehingga bisa diartikan sebagai tulisan yang tersembunyi. Dapat disimpulkan bahwa, steganografi adalah ilmu yang mempelajari teknik penyembunyian pesan rahasia didalam pesan yang lainnnya, sedemikian rupa sehingga orang lain tidak akan tahu bahwa terdapat pesan rahasia didalam pesan yang mereka baca (Bruce Schneier, John Wiley, 1996).

Hampir semua jenis berkas dapat digunakan untuk steganografi, tetapi format berkas yang cocok untuk steganografi ini adalah memiliki tingkat *redundancy* yang tinggi. *Redudancy* dapat didefinisikan sebagai jumlah bit berlebih dari sebuah objek yang menghasilkan akurasi jauh lebih besar dari yang dibutuhkan untuk penggunaan dan menampilkan objek. Bit berlebih dari suatu objek adalah bit-bit yang dapat diubah akan tetapi menghasilkan perubahan yang tidak dapat dideteksi dengan mudah pada objek tersebut (T. Morkel, J.H.P Eloff, M.S Olivier, 2005).

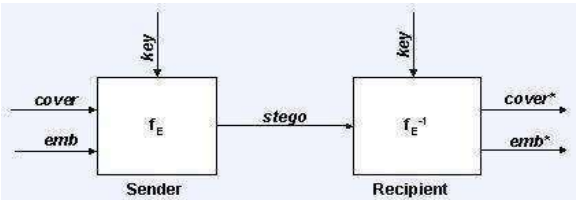
Steganografi biasanya sering disalahartikan dengan kriptografi karenanya keduanya sama-sama bertujuan untuk melindungi informasi yang berharga. Perbedaan yang mendasar antara keduanya yaitu steganografi berhubungan dengan informasi tersembunyi sehingga tampak seperti tidak ada informasi tersembunyi sama sekali. Jika seseorang mengamati obyek yang menyimpan informasi tersembunyi tersebut, maka dia tidak akan menyangka bahwa terdapat pesan rahasia dalam obyek tersebut, dan karenanya dia tidak akan berusaha memecahkan informasi dari obyek tersebut.

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 *steganografi* dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, *steganografi* digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi.

Dua teknik lain yang sangat erat kaitannya dengan steganografi adalah *watermarking* dan *fingerprinting*. Kedua teknik ini berfokus pada perlindungan hak cipta dengan menyisipkan informasi hak cipta pada media lain dan memberikan ijin kepada pihak ketiga untuk mengetahui keberadaan informasi yang disisipkan tersebut. Hal ini berbeda dengan steganografi yang menjaga informasi yang disisipkan pada media lain agar tidak terlihat oleh pihak ketiga. Jika ada pihak ketiga yang ingin meng*hack* isi informasi tersembunyi tersebut, maka tujuan mereka adalah berbeda. Jika pada *watermarking* dan *fingerprinting*, maka mereka berusaha menghilangkan informasi yang disisipkan, sedangkan jika pada steganografi, maka mereka berusaha sebatas mendeteksi keberadaan informasi tersembunyi.

Format yang biasa digunakan sebagai media penyimpan pesan di antaranya:

1. Format gambar: bitmap (bmp), gif, pcx, jpeg, dll
2. Format audio: wav, voc, mp3, dll
3. Format lain: teks file, html, pdf, dll



Gambar 1. Gambaran Umum Steganografi

Sejarah Steganografi

Steganografi sudah dikenal oleh bangsa Yunani sejak lama. Hedoratus, Penguasa Yunani mengirimkan pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut dikirim ke tempat tujuan pesan untuk membawa pesan rahasia di kepalanya. Di tempat penerima kepala budak dibotaki kembali untuk membaca pesan yang tersembunyi dibalik rambutnya. Pesan tersebut berisi peringatan tentang invasi dari bangsa Persia. Bangsa romawi mengenal steganografi dengan menggunakan tinta tak tampak *(invisible ink)* untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu dan cuka. Jika tinta digunakan untuk menulisa maka tulisannya tidak tampak. Tulisan di diatas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Selama Perang Dunia II, agen-agen spionase juga menggunakan steganografi untuk mengirim pesan. Caranya dengan menggunakan titik-titik biasa yang sangat kecil sehingga keberadaanya tidak dapat dibedakan pada tulisan biasa yang diketik.

Saat ini steganografi sudah banyak diimplementasikan pada media digital. Steganografi digital menggunakan media digital sebagai penampung, seperti citra digital, video digital, atau audio. Informasi yang disembunyikan juga berbentuk digital seperti teks, citra, data audio, atau data video. Steganografi digital dapat dipakai di negara-negara yang menerapkan sensor ketat terhadap informasi atau di negara dimana enkripsi pesan terlarang. Pada negara-negara seperti itu informasi rahasia dapat disembunyikan dengan menggunakan steganografi (Munir, 2006).

Perbedaan Steganografi dan Kriptografi

Steganografi dan kriptografi sangat erat kaitannya namun keduanya merupakan hal yang berbeda. Kriptografi mengacaukan pesan sehingga pesan tersebut tidak dapat dimengerti sedangkan steganografi menyembunyikan pesan sedemikian rupa sehingga tidak ada pihak yang mengetahui keberadaan pesan tersebut. Dalam beberapa situasi, mengirimkan sebuah pesan yang telah dienkripsi akan menimbulkan kecurigaan sedangkan sebuah pesan rahasia yang tidak tampak tentunya tidak akan dicurigai. Kedua teknik ini dapat digabungkan untuk menghasilkan

perlindungan yang lebih baik terhadap sebuah pesan, yaitu ketika steganografi gagal dan pesan dapat terlihat, pesan tersebut masih tidak dapat diartikan karena telah dienkripsi menggunakan teknik – teknik kriptografi. Namun, terdapat sebuah persamaan di antara kriptografi dan steganografi, yaitu kualitas kriptografi bergantung pada sebuah kunci, demikian pula dengan steganografi. Menemukan pesan rahasia baik yang disembunyikan melalui steganografi ataupun dienkripsi menggunakan kriptografi hanya mungkin terjadi jika mengetahui kunci yang tepat.

Kegunaan Steganografi

Seperti perangkat keamanan lainnya, *steganografi* dapat digunakan untuk berbagai macam alasan, beberapa diantaranya untuk alasan yang baik, namun dapat juga untuk alasan yang tidak baik. Untuk tujuan legitimasi dapat digunakan pengamanan seperti citra dengan *watermarking* dengan alasan untuk perlindungan *copyright*. *Digital watermark* (yang juga dikenal dengan *fingerprinting*, yang dikhususkan untuk hal-hal menyangkut *copyright*) sangat mirip dengan *steganografi* karena menggunakan metode penyembunyian dalam arsip, yang muncul sebagai bagian asli dari arsip tersebut dan tidak mudah dideteksi oleh kebanyakan orang.

Steganografi juga dapat digunakan sebagai tag-notes untuk citra online. Terakhir, *steganografi* juga dapat digunakan untuk melakukan penyimpanan atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotasi, pencuri, atau dari pihak yang tidak berwenang.

Sayangnya, *steganografi* juga dapat digunakan untuk alasan yang ilegal. Sebagai contoh, jika seseorang telah mencuri data, mereka dapat menyembunyikan arsip curian tersebut ke dalam arsip lain dan mengirimkannya keluar tanpa menimbulkan kecurigaan siapapun karena tampak seperti email atau arsip normal. Selain itu, seseorang dengan hobi menyimpan pornografi, atau lebih parah lagi, menyimpannya dalam hard disk, mereka dapat menyembunyikan hobi buruk mereka tersebut melalui *steganografi*. Begitu pula dengan masalah terorisme, *steganografi* dapat digunakan oleh para teroris untuk menyamarkan komunikasi mereka dari pihak luar.

Media Steganografi

Hampir semua file digital dapat digunakan untuk steganografi, tetapi format yang paling cocok adalah yang mempunyai nilai bits redundancy tinggi. Bit Redudancy adalah bit yang dapat dirubah tanpa merubah banyak karakteristik file secara keseluruhan. File gambar dan suara adalah yang memenuhi syarat ini, sehingga banyak periset steganografi yang telah menggunakan media tersebut.

Citra (Image)

File Citra pada komputer merupakan *array* bilangan yang merepresentasikan nilai intensitas cahaya yang bervariasi (*pixel*). Kumpulan *pixel-pixel* inilah yang membentuk suatu citra. Citra yang sering digunakan umum adalah citra 24 bit dan citra 8 bit (256 *colors*), (Johnson, 1998).

Table 1. Jenis Citra dilihat dari ukuran bitnya.

Jumlah Bit	Keterangan
1	binary-valued image (0 – 1)
8	gray level (0 – 255)
16	high color (216)
24	224 true color
32	true color (232)

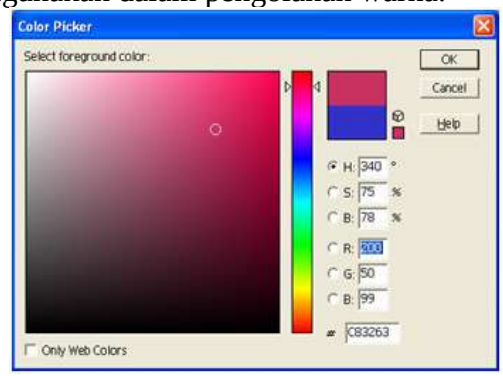
Format gambar digital memiliki 2 parameter:

- spatial resolution : pixels x pixels
- color encoding : bits / pixel

Misal: terdapat gambar berukuran 100 pixels x 100 pixels dengan color encoding 24 bits dengan R=8 bits, G=8 bits, B=8 bits per pixel, maka color encoding akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 100 * 100 * 3 byte (karena RGB) = 30.000 bytes = 30 KB atau 100 * 100 * 24 bits = 240000 bits.

Pada steganografi, citra yang biasa digunakan adalah citra 24 bit, karena citra tersebut dapat menyediakan space yang besar untuk disisipi oleh data. *Pixel* penyusun citra ini tersusun atas 3 warna primer yaitu merah, hijau, dan biru (RGB). Masing-masing warna primer tersusun atas 1 *byte* data. Untuk citra 24 bit berarti menggunakan *3 bytes per pixel* untuk merepresentasikan nilai warna *pixel*. *3 bytes* data ini dapat berupa hexadesimal, desimal, atau biner.

contoh color pallete yang sering digunakan dalam pengolahan warna.



Gambar 2. Color Pallete

Media Gambar Terkompresi dan pengaruhnya pada steganografi

Ketika bekerja dengan gambar bit depth tinggi, maka file size gambarnya akan menjadi terlalu besar untuk berada di standar halaman internet. Agar dapat menampilkan gambar dengan ukuran yang wajar, gambar tersebut harus diberi teknik-teknik tertentu. Teknik ini menggunakan rumus matematika untuk menganalisa data gambar dan menghasilkan gambar dengan ukuran file lebih kecil. Proses ini disebut dengan kompresi, (Morkel, dkk, 2005).

Dua jenis kompresi gambar adalah *lossless* dan *lossy*. Keduanya memperkecil ukuran file tetapi menghasilkan sesuatu yang berbeda. Hal ini tentunya dapat mengganggu karena gambar tersebut mengandung informasi yang hendak kita kirimkan. Lain halnya bila informasi itu tidak dikompresi.

Kompresi *lossy* menghasilkan gambar dengan ukuran file lebih kecil dengan cara menghilangkan beberapa data gambar dari aslinya. Kompresi ini menghilangkan detail-detail yang terlalu kecil bagi penglihatan mata, sehingga menghasilkan aproksimasi yang dekat dengan gambar aslinya walaupun bukan duplikat yang sama persis. Contoh format file yang menggunakan teknik kompresi ini adalah JPEG (*Joint Photographic Experts Group*), (Morkel, dkk, 2005).

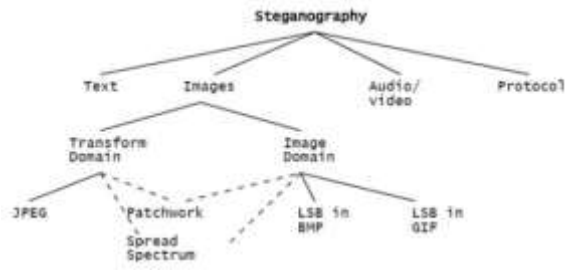
Lain halnya dengan kompresi *lossless* yang dapat dikembalikan ke pesan aslinya. Kompresi ini tidak pernah memindahkan informasi apapun dari gambar aslinya dan sebagai gantinya menggunakan rumus matematika tertentu untuk menyimpan datanya.Integritas gambar aslinya tetap dipertahankan dan gambar yang telah dikompresi, bitnya tetap sama bit demi bit dengan gambar aslinya. Format gambar yang paling sering digunakan untuk jenis kompres ini adalah GIF (Graphic Interchange Format) dan BMP 8-bit.

Kompresi memerankan peran yang sangat penting dalam memilih Algoritma yang tepat untuk steganografi. Kompresi *lossy* menghasilkan gambar dengan ukuran file lebih kecil, tetapi juga meningkatkan kemungkinan bahwa informasi yang tersimpan di dalamnya hilang karena data gambar yang tak terlihat akan dibuang. Kompresi *lossless* berusaha untuk mempertahankan gambarnya tanpa ada kemungkinan untuk hilang bagian gambarnya tetapi ukuran filenya tidak berubah banyak.

Teknik Steganografi Pada Gambar

Teknik steganografi gambar dapat dibagi menjadi dua bagian: *spatial domain* dan *transform / frekuensi domain*. Pada *spatial domain* informasi dimasukkan kedalam tiap pixel satu persatu. Sementara itu, pada *transform domain*, gambar ditransformasikan terlebih dulu kemudian informasi baru dimasukkan ke gambar. Teknik steganografi pada *spatial domain* menggunakan metoda *bit-wise* yang menggunakan penyisipan bit dan noise manipulation. Format gambar yang paling cocok untuk cara ini adalah tipe *lossless*. Namun, cara ini sangat bergantung kepada format gambarnya, (Morkel, dkk, 2005). Steganografi pada *transform domain* melibatkan manipulasi algoritma dan transformasi gambar. Metoda ini menyembunyikan informasi pada area yang lebih signifikan pada cover image dan membuat hasilnya jadi lebih baik. Cara ini juga tidak tergantung pada format gambar. Informasi yang disisipkan juga dapat bertahan walaupun menggunakan kompresi *lossy* maupun *lossless*.

Gambar 2 adalah skema image steganografi dan penggolongan berdasarkan domainnya.



Gambar 3. Skema penggolongan Steganografi berdasarkan domainnya

Kriteria Steganografi Yang Baik

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah,:

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*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
3. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Metode Steganografi Least Significant Bit Insertion (LSB)

Least Significant Bit Insertion merupakan salah satu metode steganografi yang yang paling sederhana, cepat dan mempunyai kapasitas penyisipan yang cukup besar (*ditunjukkan dalam table 2.1*). LSB insertion menggunakan cara menyisipkannya pada bit rendah atau bit paling kanan (LSB) pada data pixel yang menyusun file tersebut. Untuk file bitmap 24 bit, setiap pixel (titik) pada gambar 1 terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit dapat disisipkan 3 bit data, (Prihanto, 2009).

Implementasi Steganografi

Informasi rahasia dapat disembunyikan pada berbagai media termasuk media digital. Jaman sekarang ini, kebanyakan teknik steganografi digunakan untuk menyembunyikan pesan di dalam gambar karena merupakan hal yang paling mudah untuk diimplementasikan. Hal yang paling penting dari ' pemilihan media penyimpanan informasi adalah penyesuaian ukurannya dengan jumlah data yang akan disimpan di dalamnya agar ketika dilakukan steganografi, ukuran media penyimpanan tersebut tidak berubah jauh. Ketika sebuah gambar tampak rusak atau sebuah lagu terdengar aneh dari aslinya, maka media tersebut akan dengan mudah dicurigai.

Menyembunyikan pesan di dalam gambar merupakan teknik yang paling sering digunakan sekarang ini. Sebuah gambar dengan sebuah pesan rahasia di dalamnya dapat dengan mudah disebarluaskan melalui web atau forum. Penggunaan steganografi di dalam forum telah diriset oleh Niels Provos, ahli steganografi Jerman. Metode yang biasa digunakan untuk menyembunyikan informasi di dalam gambar adalah LSB, *masking*, *filtering* dan *transformation on the cover image*. Teknik – teknik tersebut dapat digunakan dengan berbagai tingkat kesuksesan pada berbagai tipe file gambar.

ANALISA DAN PERANCANGAN PROGRAM

Program dibuat menjadi 2 bagian utama, yaitu bagian *Encoder* dan bagian *Decoder*. Bagian *Encoder* digunakan untuk melakukan proses penyembunyian atau penyisipan data rahasia ke dalam data penampung, sedangkan bagian *Decoder* digunakan untuk melakukan proses pengambilan atau pengungkapan data rahasia yang tersembunyi atau tersisip di dalam data penampung.

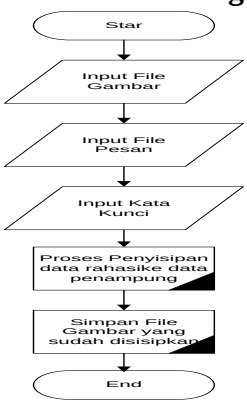
Pada proses penyisipan pesan (embedding message) dimulai dengan memilih gambar yang akan dijadikan cover object untuk menyisipkan dan menyembunyikan pesan ke dalam gambar kemudian menentukan key file yang akan digunakan sebagai password dalam proses extract dan menuliskan isi pesan text yang akan disisipkan kedalam gambar. Sedangkan pada proses pendeteksian pesan (extraction message) dimulai dengan memilih file gambar atau covert object yang akan akan di extract dan memasukan key file, yang hasil ekstraksi pesannya dapat disimpan pada satu file tertentu yang dipilih.

Berikut merupakan digram alir atau flowchart yang akan menjelaskan proses embedding message yaitu bagaimana suatu file gambar dapat disisipkan pesan sehingga menghasilkan stego object atau encoder dan proses extraction message yaitu bagaimana mengekstrak pesan dari suatu file gambar stego object agar dapat terbaca kembali pesan yang dienkripsi sebelumnya

Diagram alir proses

Pembuatan proyek akhir ini merujuk pada alur sistem yang telah dirancang sehingga dapat mengantar pada tujuan yang diharapkan. Secara umum, rancangan skema proses penyisipan informasi dapat digambarkan sebagai berikut :

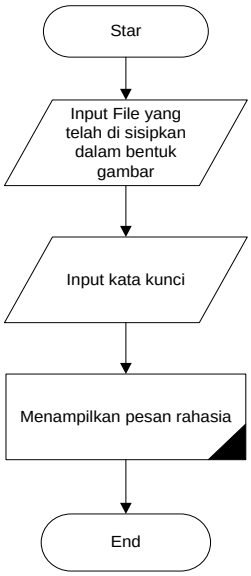
Proses encoding



Gambar 4. Diagram alir proses penyisipan gambar

Dari diagram alir encoding data di atas, dapat dijelaskan langkah-langkah proses yang pertama kita memulai sistem start, setelah itu kita input file gambar yang akan digunakan dalam proses penyisipan pesan, setelah proses pemilihan/input gambar selesai kita lanjutkan dengan memasukkan pesan dan kata kunci, jika dari ketiga proses itu sudah terpenuhi maka kita akan melakukan proses encoding atau proses penyisipan pesan kedalam bentuk gambar setelah itu kita simpan file gambar tersebut.

Proses Dencoding



Gambar 5. Diagram alir proses tampilan pesan rahasia

Dari diagram alir dencoding data di atas, dapat dijelaskan langkah-langkah proses sebagai berikut setelah memulai sistem start, selanjutnya user melakukan input file gambar yang telah disisipkan pesan, selanjutnya menginput kata kunci yang digunakan pada penyisipan pesan tersebut, hasilnya akan menampilkan pesan rahasia tersebut.

IMPLEMENTASI DAN PEMBAHASAN

Desain Antarmuka

Desain antar muka yang dibuat bertujuan untuk memudahkan user dalam melakukan proses penyisipan dan pengambilan data ke dan dari media gambar.

Dalam desain antar muka ini, penggunaan sistem antar muka dibedakan menjadi 2 bagian utama yaitu bagian untuk menyembunyikan informasi yang nantinya akan disebut encoding data dan bagian untuk mengambil informasi dari file stego yang nantinya akan disebut dencoding data.

Desain antar muka yang dibuat bertujuan untuk memudahkan user dalam melakukan proses penyisipan dan pengambilan data ke dan dari media gambar.

Berikut merupakan rancangan interface pada form

Pada saat pertama kali menjalankan aplikasi ini, user diminta untuk memasukkan dulu pasword untuk menjalankan aplikasinya.

Gambar 6. Gambar Antarmuka Pasword Aplikasi

Hal ini dikarenakan agar hanya orang yang berhak memakai aplikasi ini saja yang boleh menggunakannya. Dengan begitu akan dapat menambah tingkat keamanan dari pesan rahasia yang akan diberikan. Pasword diberikan oleh pemberi pesan rahasia kepada penerima dengan tujuan agar rahasia tidak bisa diketahui oleh orang yang tidak berhak.

Apabila user memasukkan pasword aplikasi dengan benar maka akan langsung keluar aplikasi steganografinya berikut ini:

Gambar 8. Antarmuka Program Steganografi

Pada program steganografi ini terlihat bahwa kita bisa melakukan penyimpanan pesan rahasia file berbentuk gambar. Dua proses steganografi berupa enkripsi untuk memasukkan pesan rahasia pada gambar dan deskripsi yaitu menguraikan gambar yang sudah ada pesan rahasianya agar kita bisa membaca pesan rahasia yang diberikan.

Gambar 9. Tombol Dalam Aplikasi Steganografi

Fungsi dari tombol-tombol pada gambar 9.

- Load Img :Tombol untuk menginput gambar
- Encode :Tombol untuk proses penyisipan pesan rahasia
- Decode :Tombol untuk menampilkan pesan rahasia
- Save As :Tombol untuk menyimpan pesan rahasia
- Get Out : Tombol untuk keluar

Eksekusi Program Encode

Sebelum kita memasukkan pesan rahasia yang akan dikirimkan, terlebih dahulu kita memasukkan gambar yang akan dipakai sebagai inang (induk) dari pesan rahasianya. File gambar bisa berupa format bmp, jpg atau gif.

Untuk memilih gambar yang yang akan dijadikan penampung pesan, klik tombol "Load Img". Kemudian akan muncul tampilan seperti gambar dibawah ini. Pilih gambar yang diinginkan.

Gambar *10 . Tampilan Layar Open File Image*

Dimana dari hasil pemilihan file gambar akan tampil hasil seperti pada gambar di bawah ini.

Gambar 11. Tampilan Stenografi setelah dimasukkan gambar.

Langkah selanjutnya adalah menginput pesan dan key. Setelah kita memasukkan file gambar, kita akan melanjutkan dengan memasukkan pesan dan key. Dengan cara clik tekx box pesan ketik pesan yang diinginkan dan klik tekx bok key masukkan key untuk pesan rahasia tersebut. Dari hasil ini kita dapat lihat pada gambar 12 di bawah ini.

Gambar 12. Proses penginputan pesan dan key

Untuk proses selanjutnya pencet tombol enkode maka akan dilakukan proses penyisipan file dari pesan rahasia nya kedalam gambar. seperti berikut ini:

Gambar 13. Proses Penyisipan Pesan Rahasia Ke Gambar

Pada gambar 13 dapat dilihat Proses penyisipan pesan rahasia ke dalam gambar ditandai dengan adanya sebuah teks pesan berwarna merah didalam gambar bagian sudut bawah (Pesan berhasil disimpan).

Langkah selanjutnya adalah aplikasi steganografi akan menyimpan file baru yang sudah disisipi dengan pesan rahasia kedalam dokumen, dengan cara clik tombol (Save As) pada tampilan form dan memberikan nama file gambar sesuai dengan keinginnan anda. Kita dapa melihat pada tampilan gambar di bawah ini.

Gambar 14. Tampilan prosen penyimpanan pesan rahasia

Pilih lokasi untuk menyimpan file gambar yang sudah disisipkan dengan pesan rahasia dan berinama pada file gambar tersebut, tujuannya agar kita dapat mengetahui file gambar mana yang telah kita sisipkan dengan pesan rahasia dan akan mempermuda kita pada saat pencarian file gambar tersebut.

Eksekusi Program Decode

Pada proses decode ini kita akan melihat proses penguraian dari gambar yang sudah berisi pesan rahasia agar kita bisa mengetahui pesan rahasia apa yang disisipkan ke gambar.

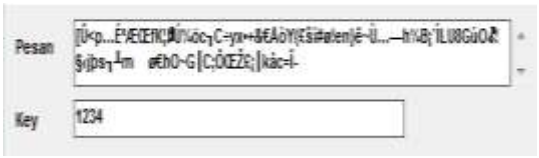
Untuk menampilkan pesan rahasia, kita harus memasukkan gambar yang sudah kita sisipkan dengan pesan rahasia, dengan cara clik tombol *Load Img* untuk menginput gambar, cari lokasi tempat penyimpanan gambar yang sudah disisipkan pesan rahasia tersebut.

Gambar 16. Tempat/lokasi penyimpanan gambar pesan rahasia

Gambar 16 Lokasi tempat penyimpanan gambar yang telah dsisipkan dengan pesan rahasia pilih gambar tersebut lalu clik open untuk menampilkan gambar pada form stenografi. Hasilnya dapat kita lihat pada gambar 17.

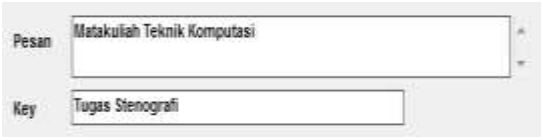
Gambar 17. Tampilan proses dekode

Langkah selanjutnya adalah masukkan kata kunci pada kolom key agar dapat membaca pesan rahasia pada gambar tersebut dan jika key yang kita masukkan salah maka pesan tersebut tidak dapat dibaca, dan hasilnya akan seperti pada tampilan gambar.



Gambar 18. Tampilan Pesan error

Jika key yang kita masuk kan benar maka pesan tersebut dapat kiita baca. Dapat dilihat pada gambar berikut ini.



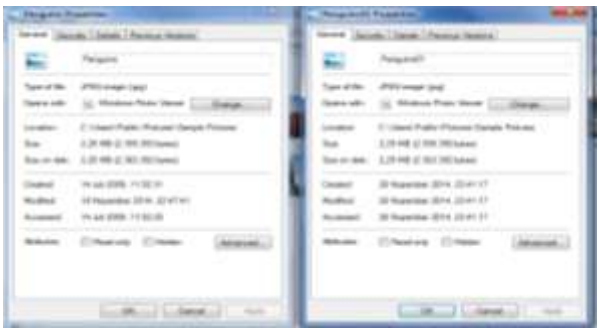
Gambar 19. Tampilan Pesan Rahasia

Gambar 20. Tampilan akhir decode

Setelah proses deskripsi dilakukan akhirnya kita bisa mengetahui pesan rahasia yang dikirimkan.

Gambar 21. Gambar asli dan gambar yang sudah di enskripsi

Kedua gambar diatas terlihat bahwa hampir tidak ada perbedaan antara gambar awal dengan gambar yang sudah disisikan dengan pesan rahasia. Hal itu lebih menguntungkan bagi kita karena untuk kebanyakan steganografi yang lain akan terlihat perbedaan yang sangat mencolok dari histogram gambar sebelum dan sesudah penyisipan pesan. Dengan perbedaan yang sangat tidak terlihat ini lebih membuat kesulitan bagi pihak ketiga untuk bisa mengetahui bahwa ada pesan rahasia yang tersembunyi didalam gambar tersebut.



Gambar 22. Tampilan ukuran gambar

Pada gambar 22 dapat kita lihat bahwa ukuran dari gambar awal/asli dan gambar yang sudah disisipkan pesan rahasia juga sama persis.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil analisa diketahui bahwa aplikasi steganografi yang telah dihasilkan dari implementasi algoritma LSB (*Least Significant Bit*) dapat digunakan dengan sangat baik untuk menyembunyikan pesan rahasia ke dalam sebuah gambar sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut karena perbedaan dari gambar asli dan gambar yang disisipi pesan rahasia sangat tipis. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada file citra uji dalam aplikasi steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan.

Hasil pengujian dengan histogram menunjukkan bahwa gambar asli dan gambar sesudah ada penyisipan pesan tidak mengalami perubahan yang signifikan. Dari segi warna pembentuknya benar benar tidak terlihat adanya perbedaan. Dengan demikian pesan yang disisipkan kedalam gambar tidak akan menimbulkan kecurigaaan dan menjaga keamanan pesan yang disisipkan dalam file citra digital tersebut. Bisa dkatakan bahwa kualitas gambar sebelum dan sesudah dilakukan penyisipan tidak mengalami perubahan.

Pada pengujian perbandingan ukuran gambar sebelum dan sesudah adanya penyisipan menunjukkan bahwa apabila diantara banyak gambar asli, disisipkan pesan rahasia dengan ukuran yang sama akan menghasilkan gambar dengan ukuran yang sama pula.

Banyaknya karakter pesan rahasia yang akan disisipkan pada gambar sangat dipengaruhi oleh besarnya file gambar induk nya. Semakin besar ukuran gambar induk nya maka semakin banyak pula pesan rahasia yang bisa dimasukkan ke dalam gambar tersebut.

Saran

1. Bagi perusahaan agar password yang digunakan harus dirahasiakan agar data rahasia yang telah disipkan tidak bisa diketahui oleh pihak-pihak yang tidak bertanggung jawab
2. Menambahkan teknik kompresi agar ukuran memori dari gambar yang disisipkan pesan dapat lebih kecil sehingga akan menurunkan tingkat kecurigaan pihak yang ingin mencuri informasi tersebut.
3. Metode *LSB* mempunyai sifat *fragile* (mudah rusak) apabila mengalami rotasi, perbesaran, *cropping*, dan gangguan, sehingga menyebabkan pesan hilang, untuk itu kedepannya agar metode ini dapat dikombinasikan dengan metode lain.

DAFTAR PUSTAKA

Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007

Johnson, Neil F. dan Jajodia, Sushil. (1998),*Exploring Steganography,Seeing theUnseen*, IEEE Computer Magazine.

Morkel, T., Eloff dan Olivier, M.S. (2005), *An Overview of Image Steganography*,Proceedings of the Fifth Annual Information Security South AfricaConference*(ISSA2005)*, Sandton, South Africa, (Publishedelectronically).

Prihanto, Agus. (2009), *Penyembuyian dan Pengacakan Pesan Data Text Menggunakan Steganografi dan Kriptografi Triple DES pada image*, Proceding Seminar Nasional Pengaman Jaringan - SNIPER,Banyuwangi.

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