

¹Hanny Hikmayanti H, ²Garno, ³Arfian Pua Meno, ⁴Carudin

Implementasi Penyembunyian Informasi pada Citra Digital dengan Menggunakan Metode *Least Significant Bit*(Lsb)

¹Hanny Hikmayanti H, ²Garno, ³Arfian Pua Meno, ⁴Carudin

¹²Universitas Buana Perjuangan Karawang

³Universitas Budi Luhur Jakarta

⁴Universitas Singaperbangsa Karawang

¹hanny.hikmayanti@ubpkarawang.ac.id, ²muhammad.garno@ubpkarawang.ac.id,

³arfianmaulidan@gmail.com ⁴carudin@staff.unsika.ac.id

Jl. HS.Ronggo Waluyo, Telukjambe Timur, Karawang, Jawa Barat 41361

ABSTRAK

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan Least Significant Bit (LSB). Penelitian ini adalah untuk dapat memberikan keamanan pada pesan rahasia untuk menyembunyikan pesan tersebut pada gambar menggunakan Metode Least Significant Bit (LSB) dengan tools yang digunakan yaitu matlab.

Kata kunci : steganografi, LSB, matlab

ABSTRACT

Steganography is the art and science of writing hidden messages or hide messages in a way that besides the sender and the recipient, no one knows or realizes that there is a secret message . The method used to hide messages in digital media is different . For example , the image file message can be hidden by using paste on low bit or bits of the rightmost least significant bit (LSB) . This research is to be able to provide security at a secret message to the message conceal the image using the method of Least Significant Bit (LSB) with the tools that are used ie matlab .

Keywords : steganography , LSB , matlab

PENDAHULUAN

Kemajuan teknologi tentu saja berdampak pula terhadap kemajuan perangkat-perangkat teknologi informasi dan komunikasinya seperti kartu ATM, internet, mobile phone, mobile banking, online banking, dan lain sebagainya. Dari sekian banyak manfaat dan kemudahan yang dapat dirasakan oleh perkembangan teknologi tersebut tentu saja harus diimbangi dengan perkembangan aspek keamanannya. Operasional akan perangkat teknologi tersebut rentan terhadap serangan karena melibatkan transaksi internet dan simpan data/informasi. Sebagai contoh kasus kejahatan dalam dunia cyber telah marak terjadi dan dampaknya tentu akan sangat merugikan produktivitas, kinerja dan reputasi. Oleh karena itu, biasanya pesan rahasia akan dikirim secara sembunyi-sembunyi untuk menghindari kebocoran data/informasi. Namun tetap saja terdapat celah keamanan untuk mendapatkan data/informasi tersebut, untuk itu diperlukan ada teknik pengamanan informasi agar data/informasi yang ingin disampaikan dapat sampai pada tujuan. Salah satu caranya yaitu dengan menghilangkan pesan sehingga pesan tersebut tidak dapat terlihat, Teknik ini disebut steganography.

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "*steganografi*" berasal dari bahasa Yunani *steganos*, yang artinya "tersembunyi atau terselubung", dan *graphein*, "menulis".

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, *image*, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis

terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi computer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan dan adapun format yang biasa digunakan adalah diantaranya diantaranya, format image: bitmap(bmp), gif, pcx, jpeg, dll, format audio: wav, voc, mp3, dll, format lain: teks, html, pdf, dll.

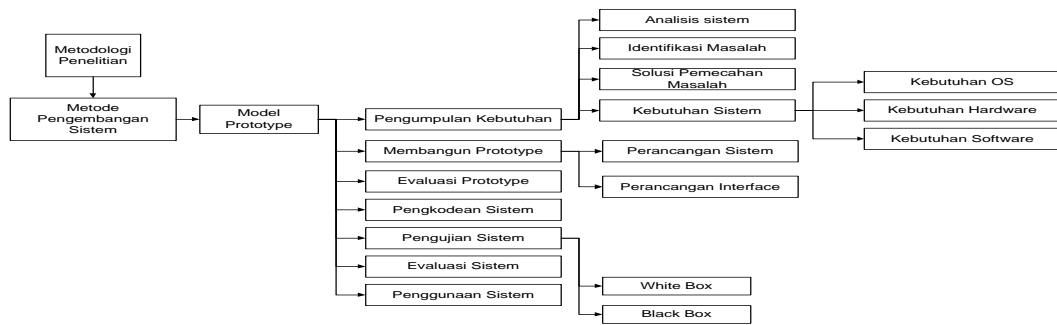
Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan Least Significant Bit (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut 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 berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.

Dalam penulisan ini, penulis akan melakukan implementasi penyembunyian informasi pada citra digital menggunakan Metode Least Significant Bit (LSB).

METODE PENELITIAN

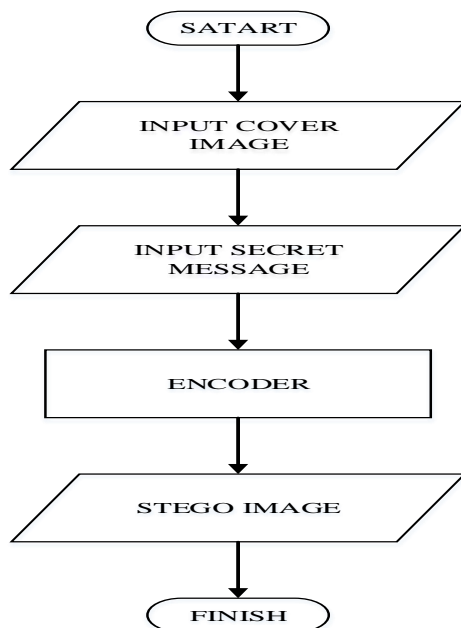
Metode yang digunakan yaitu metode rekayasa dengan pendekatan metode model *prototype*. Alasan penelitian menggunakan model *prototype* ini karena model ini memberikan pendekatan yang terbaik jika mendefinisikan aturan-aturan main pada saat awal.



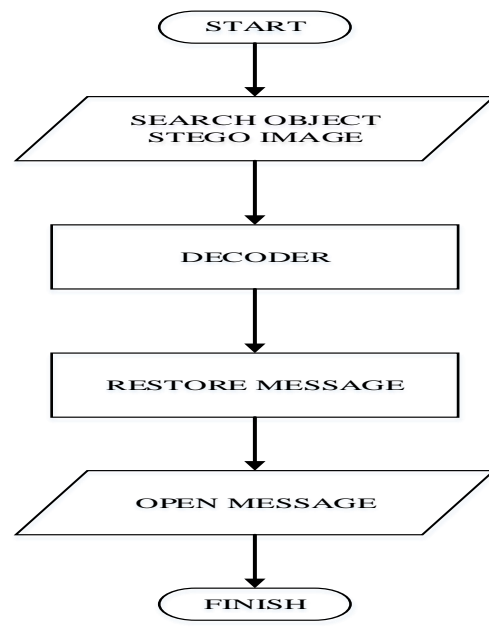
Gambar 3 Tahapan Rancangan Penelitian

PEMBAHASAN

Steganografi merupakan cabang dari informasi bersembunyi. Hal ini memungkinkan orang untuk berkomunikasi secara diam-diam. *Asincreasingly* lebih banyak bahan menjadi tersedia elektronik, pengaruh steganografi pada *liveswill* kami terus tumbuh. Banyak informasi rahasia yang bocor ke perusahaan saingan menggunakan steganografi toolsthat menyembunyikan informasi dalam musik dan file gambar. Penerapan steganografi adalah important motivation untuk seleksi fitur. Sebuah baru algoritma steganografi untuk 8 bit (*grayscale*) atau 24 bit (gambar warna) disajikan dalam artikel ini, berdasarkan pada operasi logis. Algoritma tertanam kode Ascii teks ke LSB dari gambar *cover*. Adapaun proses jalannya steganografi dapat digambarkan flowchart sebagai berikut;



Gambar 1 Flowchart encode



Gambar 2 Flowchart Decode

1. Terminologi Steganografi

a. *Cover Image*

Sebuah gambar di mana informasi rahasia yang akan disembunyikan. Itu Istilah "cover" digunakan untuk menggambarkan asli, pesan yang tidak salah, data, *audio*, masih, *Video* dll gambar *cover* kadang-kadang disebut sebagai "host".

b. *Stego-Image*

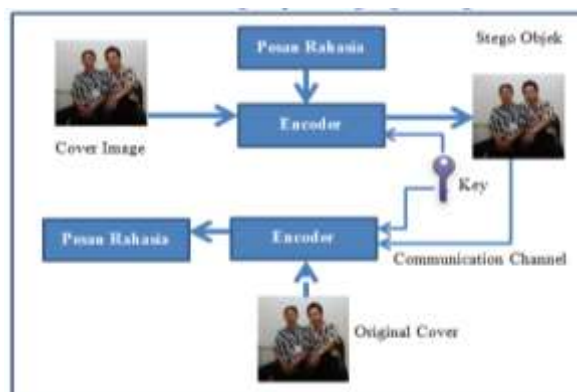
Media di mana informasi yang tersembunyi. The "stego" data data yang mengandung gambar *cover* dan "embedded" informasi. Logikanya, pengolahan menyembunyikan informasi rahasia di gambar cover dikenal sebagai *embedding*.

c. *Payload*

Informasi yang akan disembunyikan. Informasi yang akan disembunyikan di data penutup dikenal sebagai " *embedded*" data.

d. Kunci rahasia: ini adalah kunci yang digunakan sebagai password untuk mengenkripsi dan mendekripsi penutup dan *stego* masing-masing dalam rangka untuk mengekstrak pesan tersembunyi. Kunci rahasia adalah opsional.

2. Gambaran umum mengenai proses steganografi sebagai berikut :



Gambar 3 Struktur sistem steganografi

3. Implementasi Aplikasi

Implementasi aplikasi Steganografi dengan menggunakan metode LSB dengan tools Matlab sebagai berikut;

a. Bagian Penyembunyian Pesan pada gambar

1) Cari Gambar

Tombol cari saat di klik, maka aplikasi akan mencari letak atau lokasi sebuah gambar atau objek yang akan disisipkan sebuah pesan rahasia. Gambar dibawah ini menunjukkan saat tombol cari di pilih.



Gambar 4 Pencarian gambar

2) Inputkan Gambar

Setelah memilih tombol dan menemukan gambar yang terpilih, gambar akan ditampilkan pada inputkan gambar. Gambar dibawah ini memperlihatkan gambar yang terpilih.

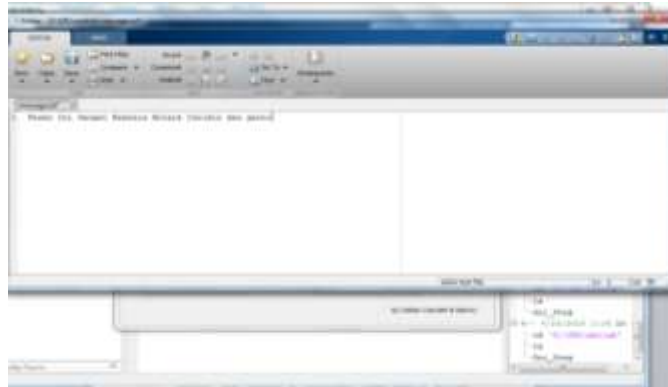


Gambar 5 insert gambar

3) Buka Pesan

Tombol buka pesan saat dipilih maka akan tampil sebuah layar yang digunakan untuk menulis atau membuat sebuah pesan rahasia yang diinginkan atau yang akan disisipkan pada gambar, setelah membuat pesan tersebut jangan lupa untuk menyimpannya.

Gambar dibawah ini menunjukkan pada saat membuat pesan rahasia yang akan disisipkan pada sebuah gambar.



Gambar 6 Input pesan rahasia

4) Sembunyikan Pesan

Bagian yang terpenting pada aplikasi ini adalah tombol sembunyikan pesan, dimana tombol tersebut berfungsi untuk menyembunyikan pesan yang telah dibuat sebelumnya pada objek gambar, jika pesan yang disembunyikan maka akan ada alat yang memberikan informasi bahwa data atau pesan berhasil disembunyikan.

Jika data berhasil disembunyikan maka, akan terbentuk sebuah file baru yang didalamnya terdapat objek yang berisi pesan rahasia yang berekstensi.bmp.

Gambar dibawah ini menunjukkan data berhasil dibuat.



Gambar 7 Save objek dengan pesan

b. Bagian Sembunyikan Pesan

1) Cari

Tombol cari saat di klik, maka dia aplikasi akan mencari letak atau lokasi sebuah gambar atau objek yang telah disisipi sebuah pesan rahasia. Gambar dibawah ini menunjukkan saat tombol cari di pilih.



Gambar 8 Pencarian gambar objek untuk di decrypt

2) Stego Gambar

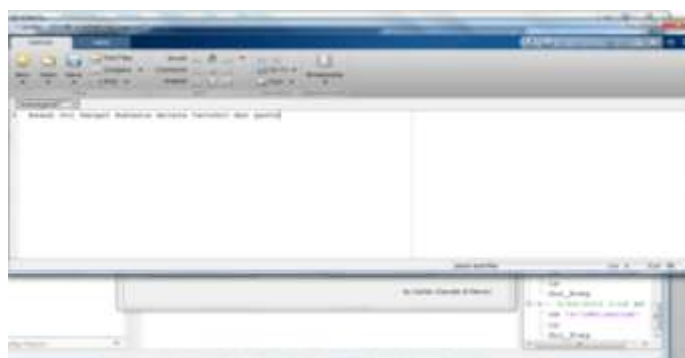
Setelah memilih tombol dan menemukan gambar yang tersisipi yang terpilih, gambar akan ditampilkan pada stego gambar. Gambar dibawah ini memperlihatkan gambar yang terpilih.



Gambar 9 Input objek untuk di decrypt

3) Buka Pesan

Tombol buka pesan saat dipilih maka akan tampil sebuah layar yang digunakan untuk membuka sebuah pesan rahasia yang telah disisipkan pada gambar. Gambar dibawah ini menunjukkan pada saat membuka pesan rahasia yang telah disisipkan pada sebuah gambar.



Gambar 11 Proses decrypt keluar pesan

4) Pemulihan Pesan

Bagian yang terpenting pada aplikasi ini adalah tombol pemulihan pesan, dimana tombol tersebut berfungsi untuk memulihkan pesan yang telah diberi pesan rahasia sebelumnya pada objek gambar, jika pesan yang disembunyikan berhasil dipulihkan maka akan ada alat yang memberikan informasi bahwa data atau pesan berhasil dipulihkan.

Jika data berhasil dipulihkan maka, akan terbentuk sebuah file baru yang didalamnya terdapat objek yang berisi pesan rahasia yang berekstensi.txt.

Gambar dibawah ini menunjukkan data berhasil dibuat.



Gambar 12 Pemulihan gambar

PENUTUP

Kesimpulan

Kesimpulan dari penelitian ini bahwa aplikasi yang dirancang dapat memberikan keamanan pada pesan rahasia untuk menyembunyikan pesan tersebut pada gambar menggunakan Metode Least Significant Bit (LSB) dengan tools yang digunakan yaitu matlab.

Saran

Saran dari penulis bahwa untuk pengembangan selanjutnya penulis menyarankan bahwa aplikasi ini di harapkan kedepannya mampu untuk melakukan enkripsi terlebih dahulu ke MD5 baru disimpan dipesan, kemudian mampu mendeskripsikan kembali. Dengan menggunakan MD5 sebanyak apapun

pesan yang akan disembunyikan jika di encrypt ke MD5 menjadi ukuran kecil dan tidak mempengaruhi gambar yang mejadi objek serta bila di decrypt kembali akan kembali seperti semula.

DAFTAR PUSTAKA

- Alatas, Putri, 2009, “*Implementasi Teknik Steganography dengan Metode LSB pada Citra Digital*”.Universitas Gunadarma.
- Ariyus, Deny, 2009, “*Keamanan Multimedia*”, Yogyakarta, ANDI.
- Hapsari, Dian, Dwi dan Bonowosari, Yuniar, Lintang, “*Aplikasi Vide teganography dengan Metode least significant bit (lsb)*.”
- Noertjahyana, Agustinus, Hartono, Samuel, dkk. “*Aplikasi Metode Steganography Pada Citra Digital Dengan Menggunakan Metode LSB (Least Significant Bit)*.”
- Jalid , Abdul, Alfian. “*Aplikasi Pengamanan Data dan Informasi dengan Metode Steganografi LSB dan Algoritma Kriptografi Tripledes Menggunakan Bahasa Pemrograman C#*”.
- Perdamean, Agus. “*Implementasi Steganography Algoritma Elgamal dan Digital Signature Untuk Pengamanan Data Pada CV. Tridian Hariwangsa Palembang*”.