APLIKASI STEGANOGRAFI DENGAN METODE SPATIAL BLOCK DESYNCHRONIZATION

Painem[1], Achmad Solichin[2], Brian Agung Gultom[3]

Program Studi Teknik Informatika, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
Telp. (021) 5853753, Fax (021) 5866369
[1]painem@budiluhur.ac.id, [2]achmad.solichin@budiluhur.ac.id, [3]gultom.brian@gmail.com

ABSTRAK

Pengamanan data dalam bertukar informasi merupakan suatu hal yang sangat penting, mengingat informasi yang terkandung didalamnya adalah informasi yang bersifat penting dan rahasia. Dengan perkembangan teknologi saat ini, pencurian data dalam proses bertukar informasi dapat dilakukan oleh orang lain dengan mudah. Baik menggunakan perangkat teknologi ataupun mudahnya orang lain dalam mengakses informasi tersebut. Steganografi merupakan salah satu bentuk pengamanan data yang dapat dilakukan. Adapun tujuan dari steganografi adalah menyembunyikan suatu informasi kedalam informasi lainnya, baik dalam citra gambar, suara, tulisan ataupun bentuk video. Aplikasi steganografi yang dibangun adalah aplikasi steganografi yang mampu menyembunyikan suatu informasi dokumen kedalam informasi lain berupa citra gambar. Metode yang digunakan dalam penerapan aplikasi steganografi adalah menggunakan metode Spatial Block Desynchronization adapun fungsi dari metode ini adalah gambar citra yang akan digunakan dalam steganografi akan dilakukan perpotongan sebelum dilakukan proses penyisipan dokumen. Aplikasi steganografi yang dibangun ini adalah aplikasi steganografi yang mampu menyisipkan dokumen kedalam citra gambar.

Kata kunci: **Steganografi, *Spatial Block*, Penyisipan, Ekstraksi**

I. PENDAHULUAN

Kebutuhan manusia dalam berkomunikasi dengan orang lain merupakan tanda, bahwa manusia adalah sebagai mahkluk sosial, sehingga merupakan kebutuhan manusia yang mendasar. salah satu cara manusia dalam berkomunikasi adalah dengan saling bertukar informasi melalui komunikasi langsung, dengan media tulisan dan seiring dengan perkembangan teknologi, komunikasi juga dapat dilakukan mengguna media surat elektronik, *chatting* dan lain sebagainya.

Seiring dengan perkembangan zaman dan kemajuan teknologi tersebut. Manusia memasuki era internet, dimana perkembangan pertukaran informasi semakin berkembangan pesat. Namun dengan perkembangan yang pesat ini, pertukaran informasi tersebut juga menjadi kurang aman ketika informasi yang disampaikan mengandung unsur yang rahasia dan pribadi bagi perorangan maupun organisasi. Sehingga setiap orang yang sedang melakukan pertukaran informasi, memerlukan suatu perlindungan keamanan sekunder untuk melindungi informasi yang dimiliki oleh pengirim informasi, agar informasi dapat sampai ketangan penerima dengan baik dan tidak cacat keamanannya.

Terdapat berbagai cara untuk melakukan pengamanan data informasi yang sedang berjalan dalam komunikasi. Salah satu cara pengamanan tersebut adalah dengan menggunakan teknik steganografi sebagai media perlindungan sekunder bagi informasi tersebut.

Steganografi adalah suatu cara perlindungan data informasi dengan melakukan penyisipan informasi dokumen kedalam media lain berupa media gambar, *video,* audio ataupun media lainnya. Sehingga kemanan data informasi tersebut tetap terjaga.

II. LANDASAN TEORI

A. Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara. Sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa terdapat suatu pesan rahasia. Kata steganografi berasal dari bahasa Yunani *steganos,* yang artinya "tersembunyi atau terselubung", dan *graphein,* "menulis". Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi.

Pada umumnya, pesan steganografi muncul dengan rupa lain, seperti; gambar, artikel, daftar belanja, ataupun pesan – pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi pesan sesungguhya. Contohnya, suatu pesan bisa disembunyikan dengan menggunakantinta yang tidak terlihat di antara garis-garis yang kelihatan[1].

Teknik steganografi memiliki beberapa metode komunikasi yang dapat digunakan untuk menyembunyikan pesan rahasia didalam berkas-berkas lain, seperti; gambar, *video,* audio, teks, dan lainnya.

Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesan yang disembunyikan tidak menarik perhatian. Sementara pesan – pesan kriptografi memiliki sandi – sandi yang menarik perhatian orang. Walaupun sandi – sandi tersebut tidak dapat dipecahkan.

B. File Image Bitmap 24 bit

Bitmap 24 bit merupakan format file yang digunakan untuk menyimpan data. Dimana file dengan format ini dapat mendukung format warna *monochrome* hingga *true color*. File dengan format BMP (Bitmap) menyimpan warna dengan sistem RGB (*Red, Green, Blue*).

C. Citra Digital

Citra menurut kamus Webster adalah suatu representasi, kemiripan atau imitasi dari suatu obyek atau benda. Sebuah citra mengandung informasi tentang obyek yang direpresentasikan. Citra dapat dikelompokkan menjadi citra tampak dan citra tak tampak. Untuk dapat bisa dilihat manusia, citra tak tampak harus dirubah menjadi citra tampak, misalnya dengan menampilkannya di monitor, dicetak dalam kertas dan sebagainya. Salah satu contoh citra tak tampak adalah citra digital[2].

Citra sebagai Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optic berupa foto, bersifat analog berupa sinyal – sinyal video seperti gambar pada monitor televisi atau bersifat digital yang dapat langsung disimpan pada suatu pita magnetik. Citra digital merupakan suatu larik dua dimensi atau suatu matriks yang elemen – elemennya menyatakan tingkat keabuan dari elemen gambar. Jadi informasi yang terkandung bersifat diskret. Citra digital tidak selalu merupakan hasil langsung data rekaman suatu sistem. Terkadang hasil rekaman data bersifat continue seperti gambar pada monitor televisi, foto sinar-X dan lain sebagainya. Dengan demikian untuk mendapatkan suatu citra digital diperlukan suatu proses konversi, sehingga citra tersebut selanjutnya dapat diproses dengan komputer[3].

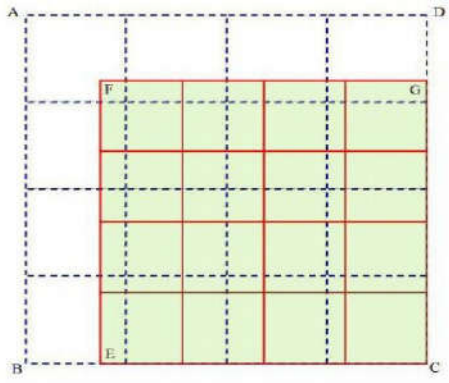
D. Spatial Block Desynchronization

Dalam format gambar JPEG, gambar dibagi menjadi blok *non – overlapping* dengan ukuran 8 X 8. Informasi yang terkandung dalam blok ini kemudian dikompresi dengan mengambil 2D *Discrete Cosine Transform (DCT)* dari blok dan diikuti dengan langkah kuantitasi yang kemudian digunakan untuk *embedding* bit data. Dengan sedikit perubahan pada pengaturan blok spasial ini dapat menyebabkan ketidak sinkronan diseluruh gambar. Perubahan dari susunan blok spasial tersebut disebut sebagai *spatial block desynchronization,* sebagai contoh : 8 X 8 *non overlapping blok* untuk *embedding* dapat diambil dari *subimage* dari gambar *cover* asli atau dapat dikatakan susunan blok sedikit bergeser dari *standard* pengaturan kompresi JPEG blok[4]. *Spatial block desynchronization* dapat dideskripsikan sebagai berikut :

Misalkan **I** dinyatakan sebagai Citra skala abu-abu ukuran (N X N). Subimage **I** dapat diperoleh dengan menghapus **u** baris dari kolom atas dan **v** dari kiri. Gambar foto yang dipotong oleh **$\hat{I}$ u; v** adalah **(N-u) × (N-v).**

Foto yang potong oleh **$\grave{I}^{\sigma}$ u, v**

$$\grave{I}^{\sigma}_{u,v} = I - \hat{I}_{u,v}$$



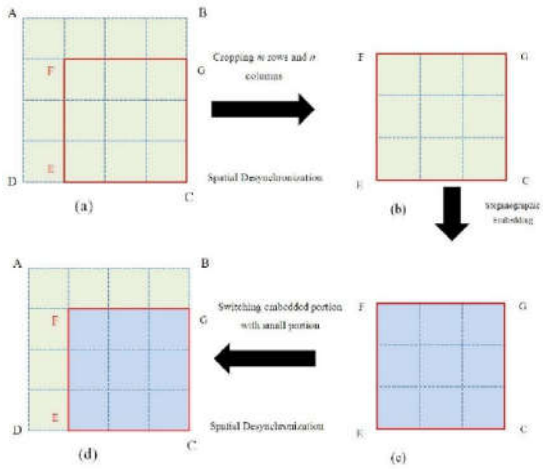
Gambar 1 :*Spatial Block Desynchronization*

Spatial Desynchronization juga dapat menggunakan ukuran blok selain dari **8 X 8**. Misalnya seperti ukuran **m X n** dimana **m ≠ 8** dan **n ≠ 8**. Akan tetapi jika menggunakan ukuran blok selain dari **8 X 8** maka, kuantisasi matriks **Q** harus diubah sesuai dengan ukuran **m X n** pada saat data *embedding*. Proses *desynchronization* ini dapat diperkuat dengan bantuan pengacakan. Dalam hal ini, penghapusan barisan tertentu dan kolom beserta ukuran blok dapat dipilih secara acak menggunakan kunci rahasia bersama[5].

E. Konsep Algoritma

Sebuah kerangka steganografi baru yang akan diusulkan dalam mendukung algoritma *spatial block desynchronization* adalah melakukan gangguan ataupun pengacakan blok pada pada cover gambar.

Tujuan dari skema ini adalah untuk menanamkan data dalam versi *spatial desynchronized* dari gambar *cover* sehingga statistik gambar *cover* tidak dapat dengan mudah dipulihkan atau diekstraksikan. Berikut ini adalah gambar tahapan dari proses algoritma yang akan diberikan[6].

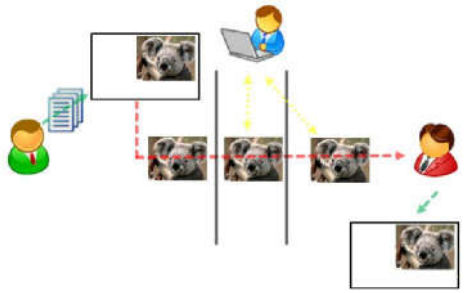


Gambar 2 : Deskripsi Algoritma

III. RANCANGAN APLIKASI STEGANOGRAFI

A. Rancangan Konsep

Tahapan rancangan konsep adalah tahapan dimana dilakukan kegiatan mengkonsepkan aplikasi steganografi yang akan dibangun. Konsep steganografi yang dibangun adalam proses penyisipan pesan kedalam media gambar.

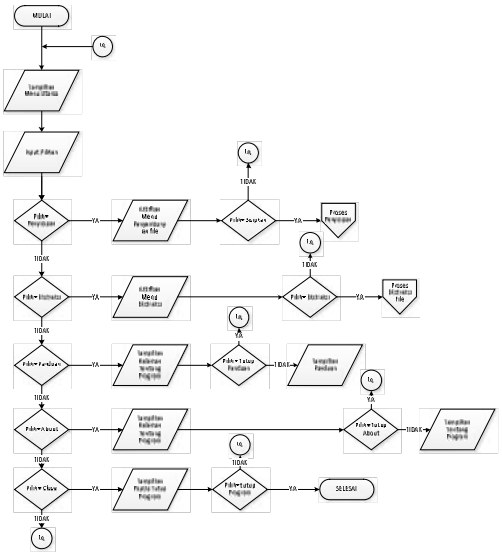


Gambar 3: Rancangan Konsep

B. Flowchart Aplikasi

1) Flowchart Penyisipan

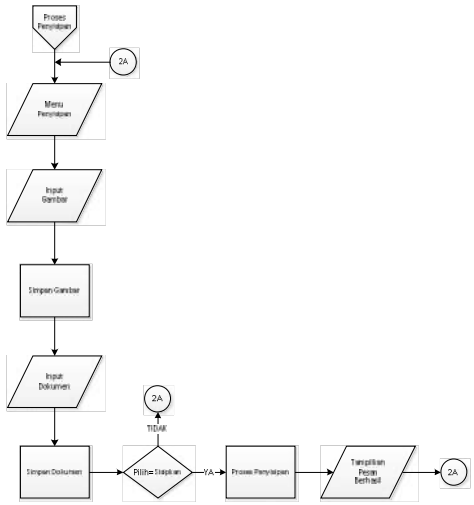
Perancangan flowchart penyisipan ini dilakukan sebelum gambar stego dikirimkan ke penerima pesan. Adapun rancangan flowchart penyisipan tersebut adalah :



Gambar 4 : Flowchart Penyisipan

2) Flowchart Ekstraksi

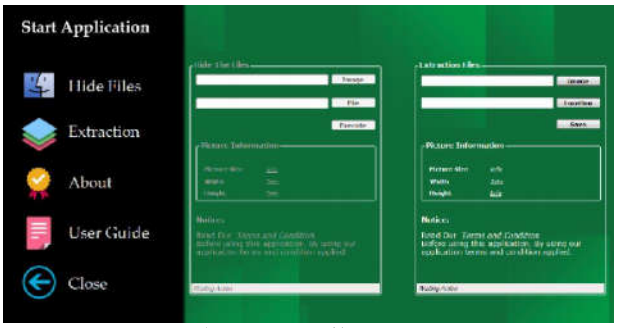
Perancangan flowchart ekstraksi ini dilakukan setelah gambar stego dikirimkan ke penerima pesan. Adapun rancangan flowchart ekstraksi tersebut adalah :



Gambar 5 : Flowchart Ekstraksi

C. Rancangan Layar Program

Program yang dikembangan adalah aplikasi steganografi berbasis *desktop* yang dapat berjalan pada *operating sysem windows*. Adapun rancangan antar muka program sebagai berikut :



Gambar 6 : Tampilan Program

IV. HASIL DAN PEMBAHASAN

A. Pembahasan

Aplikasi ini di buat dengan menggunakan *visal studio 2010* dengan bahasa pemrograman C#. aplikasi ini memiliki 5 menu utama dalam program, yaitu; *hide files, extraction, about, user guide* dan *close program.* Menu *hide files* merupakan menu yang digunakan *user* untuk mengaktifkan panel penyisipan dan untuk membuat file gambar stego. Sementara menu *extraction* digunakn untuk mengatifkan panel ekstrasi dan berguna untuk melakukan ekstraksi gambar stego dan mengambil pesan rahasia yang telah disisipkan. Menu *about* menampilkan informasi pengembang program, menu *user guide* panduan penggunaan program dan menu *close* untuk menutup program yang berjalan.

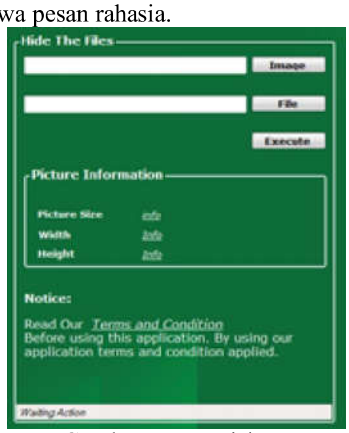
B. Hasil Pengujian

Program yang telah dikerjakan dan telah selesai dikembangkan ini. Saat ini akan dilakukan pengujian. Adapun fungsi dari pengujian adalah untuk memastikan setiap menu, konsep, metode dan tujuan pembuatan program telah tercapai serta sesuai dengan konsep pengembangan program pada pertama kali direncanakan.

Pengujian yang dilakukan meliputi pengujian aplikasi dalam melakukan penyisipan dokumen dan kemampuan program dalam menerjemahkan atau ekstraksi kembali file citra stego untuk mengambil file dokumen yang telah disisipkan sebelumnya. Sehingga dapat dipastikan bahwa aplikasi steganografi berjalan dengan baik.

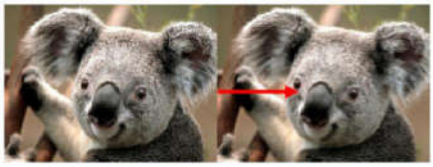
C. Pengujian Penyisipan

Pengujian penyisipan file adalah pengujian untuk memasukkan file dokumen kedalam citra gambar sebagai media pembawa pesan rahasia.



Gambar 7 : Penyisipan

Gambar 7 memperlihat menu tampilan dari proses penyisipan file. proses penyisipan dimulai dengan memasukkan terlebih dahulu gambar yang akan digunakan sebagai *cover* atau media pembawa pesan rahasia. Dan kemudian *user* memilih dokumen yang ingin disisipan kedalam gambar dengan menekan tombol file. untuk melakukan eksekusi penyisipan *user* menekan tombol *execute.*

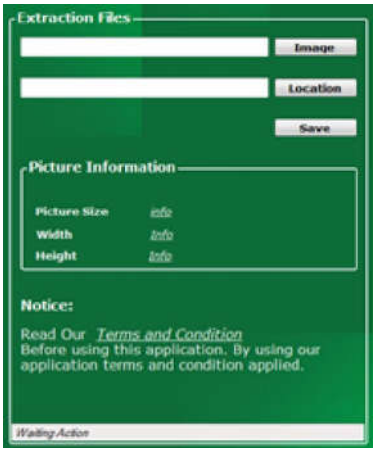


Koala.bmp (gambar sesudah stego)	→	Koala.jpg (gambar sebelum stego)

Gambar 8 : Perbandingan Citra Gambar

D. Pengujian Ekstraksi

Pengujian ekstraksi adalah pengujian untuk memastikan bahwa menu ekstraksi yang ada pada program telah berjalan. Adapun pengujian ekstraksi dilakukan dengan melakukan ektraksi file dokumen dari gambar stego.



Gambar 9 : Ekstraksi

Gambar 9 menunjukkan panel ekstraksi berisi tombol pilih gambar, yang bertujuan untuk memilih gambar stego. Tombol lokasi bertujuan mengarahkan lokasi penyimpanan dokumen dari hasil ekstraksi gambar stego. Dan tombol *save* untuk mengeksekusi proses ekstraksi.

Tabel 1 : Hasil Ekstraksi

	Surat_Perjanjian.docx
	Draft_Proposal.pdf
	SIMDUK_Budget.xlsx

V. KESIMPULAN DAN SARAN

1) Kesimpulan

Kesimpulan yang dapat diperoleh dari perancangan, pembuatan, pengembangan dan rangkaian implementasi program aplikasi steganografi, maka dapat diberikan kesimpulan antara lain :

1) Aplikasi yang dibangun telah berhasil menjalan tugasnya sebagai aplikasi penyisipan dan ekstraksi file dokumen. Sehingga dapat digunakan untuk menjaga keamanan data dokumen pengguna.
2) Aplikasi ini dibangun dengan memperhatikan kenyamanan pengguna dalam menggunakan program. Dimana program disatupadukan dalam satu buah *form* utama dimana semua

proses dilakukan dalam satu *form* tersebut. Sehingga memberikan kemudahan penggunda dalam mengakses setiap menu program.

3) Dengan menggunakan metode *Spatial Block Desynchronization* gambar yang disisipkan file dokumen, secara kasat mata atau tampilan visual tidak terlihat perbedaan dengan gambar asli, sehingga tidak menimbulkan kecurigaan.
4) Aplikasi dilengkapi dengan panduan yang cukup jelas dan panduan tambahan yang dihubungkan dengan alamat situs resmi bantuan program.

2) Saran

Berdasarkan hasil perancangan aplikasi steganograafi ini dan setelah dilakukan implementasi program. Terdapat beberapa saran yang dapat diperhatikan dan kedepannya dapat digunakan sebagai acuan dalam pengembangan program selanjutnya. Saran tersebut adalah sebagai berikut :

a. Untuk meningkatkan keamanan dokumen, kedepannya diharapkan dalam pengembangan aplikasi steganografi ini. Aplikasi dapat dilengkapi dengan pengaman tambahan berupa *password* yang juga disisipkan didalam citra gambar.
b. Diharapkan kedepannya hasil kompresi dokumen kedalam gambar menghasilkan ukuran file yang lebih kecil atau setara dengan ukuran asli gambar. Mengingat saat ini hasil citra gambar penyisipan memiliki selisih ukuran gambar yang cukup signifikan.

DAFTAR PUSTAKA

[1] El Said, 2010. *Keamanan Sistem Informasi.*
[2] Castleman,K.R., 1996. *Digital Image Processing Vol. 1 Ed 2.*
[3] Frinando,Hafid, 2010. *Aplikasi Steganografi Pada Citra.*
[4] Achmad,B, 2005. *Teknik Pengolahan Citra Digital Menggunakan Java.*
[5] Budiman A, 2010. *Steganograpy Application On Video With Least Significant Bit* (LSB).
[6] John Njenga Kimuhu, 2009. *Digital Image Cryptosystem with adptive steganography.*