# Aplikasi Steganography untuk Enkripsi Image to Image dengan Metode Spread Spectrum

**Khasadika Donavan[1], Ekojono[2], Imam Fahrur Rozi[3]**
[1,2,3]Jurusan Teknik Elektro, Prodi Teknik Informatika, Politeknik Negeri Malang
khasadikadonavan@gmail.com

**ABSTRAK**

*Steganography* adalah suatu seni dan ilmu (*science*) dalam menyembunyikan keberadaan pesan menggunakan metode tertentu sehingga hanya penerima saja yang mengetahui keberadaan pesan tersebut. Dalam *steganography*, ada beberapa media digital yang dapat digunakan sebagai *cover* untuk menyembunyikan keberadaan sebuah pesan, seperti : citra, audio, teks, video. Dalam tugas akhir ini, media *cover* yang digunakan adalah citra digital dengan format piksel 24-bit

Metode Steganografi yang dimaksud adalah metode yang menempatkan informasi di dalam derau semu dikeseluruhan cover image. Untuk mencapai tujuan yang diinginkan tersebut, maka akan dibutuhkan komponen tambahan, yaitu spread spectrum yang akan mentransmisikan sebuah sinyal pita informasi yang sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi.

Hasil analisis menunjukkan bahwa implementasi ini dapat menjalankan kedua tugas utama dalam sistem *steganography* (penyisipan dan pengekstrakan) dengan baik. Dan dari hasil percobaan yang dilakukan terhadap beberapa citra uji, dapat diketahui bahwa citra yang baik untuk digunakan sebagai citra *cover* adalah citra yang memiliki kekontrasan yang tinggi.

***Kata kunci** : pengaman data, enkripsi, steganografi, citra digital, spread spectrum*

## I. PENDAHULUAN

Kemajuan cara berpikir manusia membuat masyarakat menyadari bahwa teknologi informasi merupakan salah satu *tool* penting dalam peradaban manusia untuk mengatasi (sebagian) masalah derasnya arus informasi. Teknologi informasi (dan komunikasi) saat ini adalah bagian penting dalam manajemen informasi. Selain memiliki potensi dalam mem*filter* data dan mengolah menjadi informasi, teknologi informasi mampu menyimpan dengan jumlah kapasitas jauh lebih banyak dari cara-cara manual. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan, yaitu pekerjaan manusia dalam menyembunyikan data atau pesan.

Kerahasiaan dan keamanan suatu data pada jaman globalisasi sekarang ini semakin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu data akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana data-data tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya. Dengan berkembangnya teknologi informasi semakin berkembang pula kejahatan yang berhubungan dengan data itu sendiri. Dengan berbagai teknik banyak yang mencoba untuk mengakses data yang bukan haknya. Salah satu data yang memerlukan pengamanan adalah data dari kepolisian, dalam kepolisian terdapat data yang tidak boleh dipublikasikan kemasyarakat luas, salah satu data itu adalah TO (Target Operasi). Target operasi adalah sasaran yang dipertajam berdasarkan skala prioritas dan dapat diukur untuk ditangani, dicapai dalam penyelenggaraan operasi kepolisian, dalam kata lain Target Operasi adalah target kepolisian yang telah menjadi prioritas dalam menjalankan operasi kepolisian. Data target operasi merupakan data berupa gambar yang dimana data tersebut akan dikirim ke kantor-kantor kepolisian lain. Dengan maraknya pencurian data yang terjadi belakangan ini menjadi perhatian khusus pihak kepolisian, apabila data target operasi sampai menyebar ke publik hal ini bisa menyulitkan pihak kepolisian dalam proses penanganan target tersebut. Maka dari itu sejalan dengan berkembangnya teknologi informasi ini harus juga dibarengi dengan perkembangan pengamanan.

Keamanan pada suatu data pada saat ini dapat dibagi menjadi dua, yakni: *Cryptography* dan *Steganography*. Dari dua metode tersebut, metode yang satu dapat menjadi tambahan bagi metode yang lain. Menurut terminologinya *cryptography* adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Berbeda dengan *cryptography*, *Steganography* adalah seni menyamarkan / menyembunyikan pesan secara tertulis kedalam pesan lainnya. (Dony Ariyus : 2008)

Teknik *Steganography* ini mempunyai beberapa metode yang digunakan untuk mengamankan suatu data atau pesan salah satunya adalah metode spread spectrum. Metode *Spread Spectrum* mentransmisikan sebuah sinyal pita informasi yang sempit kedalam sebuah kanal pitalebar dengan penyebaran frekuensi (Dony Ariyus : 2008). *Spread spectrum image steganography* adalah metode yang menempatkan informasi di dalam derau semu dikeseluruhan cover

image. Dengan kata lain pada metode ini pesan yang hendak di sembunyikan dimasukkan secara menyeluruh pada cover image,sehingga akan lebih sulit untuk dideteksi keberadaannya dan pesan akan terlihat seperti *noise*. Dalam *Steganography* memerlukan suatu media sebagai tempat penyembunyian informasi. Secara teori penyisipan informasi pada data digital dengan menggunakan teknik *Steganography* dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai media covernya seperti format teks, format gambar, bahkan untuk format audio dan sebagainya asalkan file-file tersebut mempunyai bit-bit data yang dapat dimodifikasi.

Penggunaan file image sebagai salah satu media *Steganography* merupakan langkah yang baik. Lalu lintas pertukaran file image di internet merupakan hal biasa, sehingga *Steganography* menggunakan file image adalah teknik yang baik untuk mengamankan pesan rahasia melalui media internet. Selain itu jika kita tidak bicara dalam konteks internet, *Steganography* juga menjadi media yang paling digemari karena paling sering digunakan sebagai sarana hiburan. Semakin sering file itu atau semakin terlihat file itu maka akan semakin kecil kecurigaan bahwa terdapat pesan tersembunyi dalam file tersebut.

Didorong oleh hal-hal tersebut, maka kali ini penulis mencoba membuat aplikasi Steganography yang dapat menyisipkan pesan ke dalam file image tersebut sehingga pesan tersebut dapat terjaga kerahasiannya. Oleh karena itu penulis memilih judul ***Aplikasi Steganography untuk Enkripsi Image to Image dengan Metode Spread Spectrum.***

## II. METODE PENELITIAN

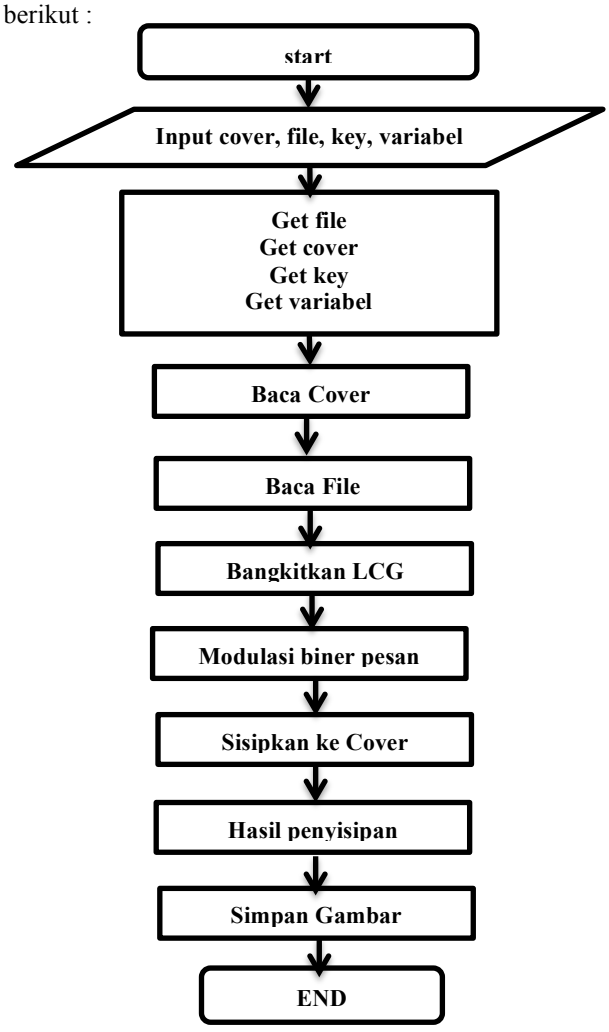
Teknik *Steganography* ini mempunyai beberapa metode yang digunakan untuk mengamankan suatu data atau pesan salah satunya adalah metode spread spectrum. Metode *Spread Spectrum* mentransmisikan sebuah sinyal pita informasi yang sempit kedalam sebuah kanal pitalebar dengan penyebaran frekuensi. *Spread spectrum image steganography* adalah metode yang menempatkan informasi di dalam derau semu dikeseluruhan cover image. Dengan kata lain pada metode ini pesan yang hendak di sembunyikan dimasukkan secara menyeluruh pada cover image,sehingga akan lebih sulit untuk dideteksi keberadaannya dan pesan akan terlihat seperti *noise*. Dalam *Steganography* memerlukan suatu media sebagai tempat penyembunyian informasi. Secara teori penyisipan informasi pada data digital dengan menggunakan teknik *Steganography* dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai media covernya seperti format teks, format gambar, bahkan untuk format audio dan sebagainya asalkan file-file tersebut mempunyai bit-bit data yang dapat dimodifikasi.

### C. Pengumpulan Data

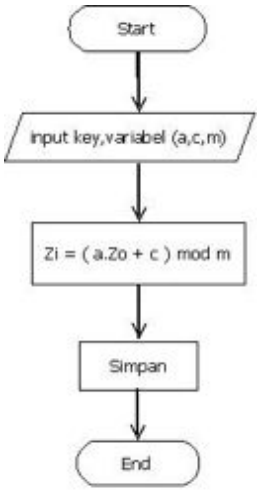
Pengumpulan data dilakukan dengan melakukan Tanya jawab dengan salah satu perusahaan milik Negara, dalam hal ini adalah Badan Meteorologi, Klimatologi dan Geofisika (BMKG). Adapun hal yang ditanyakan adalah bagaimana proses yang selama ini dilakukan oleh BMKG dalam mengirim pesan gambar, bagai mana cara mengatasi masalah tersebut dan seberapa efektif cara tersebut mengatasi pencurian data.

### D. Pemodelan Sistem Flowchart

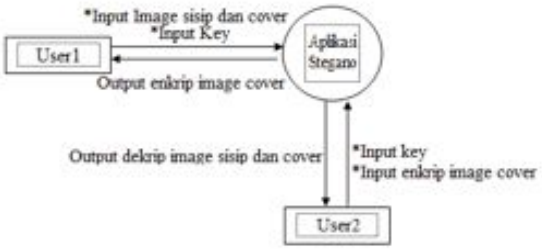
*Flowchart* proses penyisipan (*Enkripsi*) file image ditunjukkan pada Gambar 2sebagai berikut :




Gambar 1.*Flowchart* proses*Enkripsi*




*Gambar 2. Flowchart bangkitkan LCG*




*Gambar 3. Context Diagram*

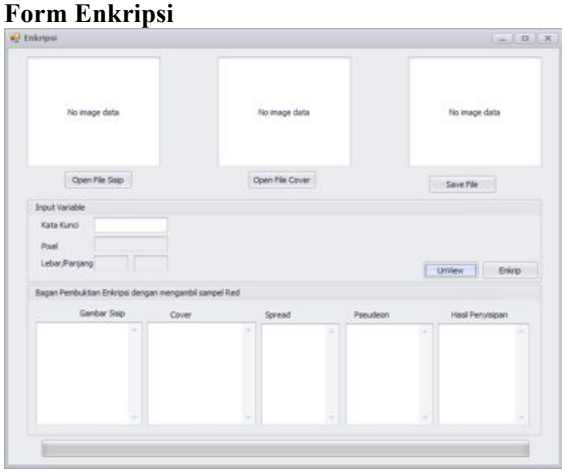
## III. METODE PENELITIAN

Pengujian hasil dilakukan dengan cara mencoba menjalankan komponen-komponen dari aplikasi dengan berbagai image.

**Form utama**

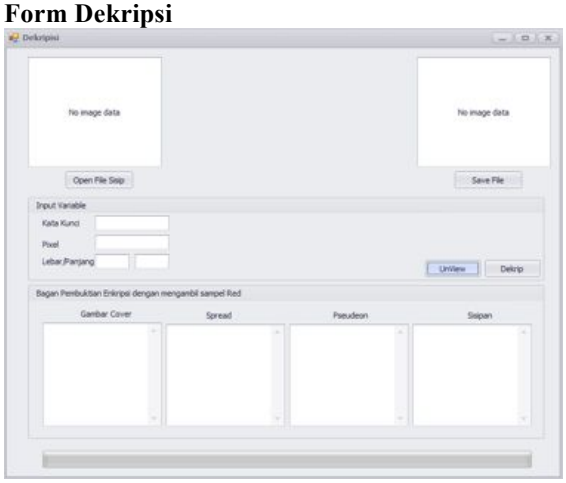

*Gambar 4. Tampilan Utama*

**Form Enkripsi**



*Gambar 5. Tampilan Enkripsi*

**Form Dekripsi**



*Gambar 6. Tampilan Dekripsi*

## IV. PEMBAHASAN

Berisi tentang penerapan metode didalam sistem aplikasi. Dilakukan dengan tahap implementasi dan pengujian sistem. Penggunaan aplikasi Steganography dengan metode Spread Spectrum ini sebagai berikut

**Proses Enkripsi**

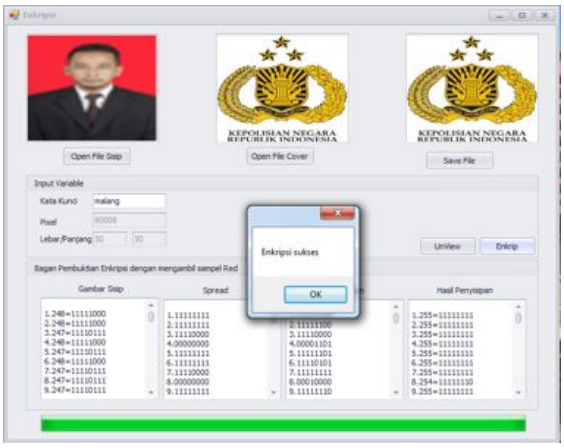
Untuk proses pertama adalah proses enkripsi file image, dimana pada proses Enkripsi ini terdapat beberapa tahapan – tahapan dalam pemrosesan file. Proses Enkripsi file image menggunakan *spread spectrum image steganography*. Untuk langkah – langkah pengujiannya adalah sebagai berikut :

1. User me-load file sisip yang yang akan disisipkan, sebagai contoh : informasi.bmp
2. User me-load cover file yang akan digunakan sebagai cover file contoh : Cover.bmp
3. User menginputkan kata kunci sebagai pembangkit bilangan acak contoh : kata kunci “malang”. Gambar dibawah ini menunjukkan

user setelah melakukan load file dan cover image serta input variable.

*Gambar 7. Tampilan Form Enkripsi*

4. Klik tombol enkripsi dan Proses Enkripsi menggunakan *spread spectrum image steganography* akan berjalan dan akan muncul pesan "Enkripsi Sukses" jika proses sudah selesai, seperti ditunjukkan pada gambar dibawah ini.

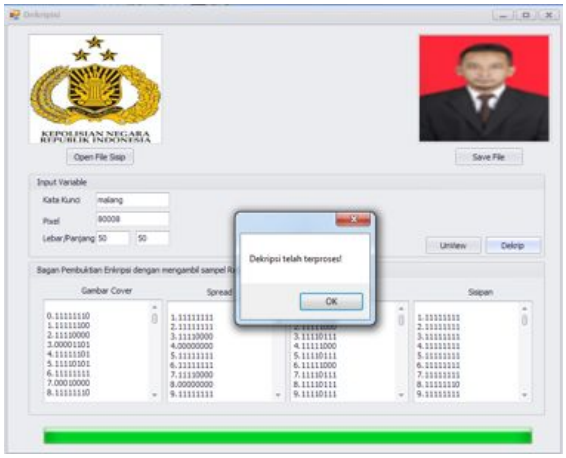


*Gambar 8. Tampilan ProsesEnkripsi*

**Proses Deskripsi**

Untuk proses selanjutnya adalah proses deskrpsion file image, dimana pada proses deskripsi ini terdapat beberapa tahapan – tahapan dalam pemrosesan file. Proses deskripsi data file image yang ada pada cover image yang sudah disisipi sebelumnya. Proses deskripsi file image menggunakan *spread spectrum image steganography*. Untuk langkah – langkah pengujiannya adalah sebagai berikut :

1. User me-load file image yang sudah disisipi pesan, sebagai contoh : enkripsi.bmp
2. User menginputkan kata kunci yang sama pada saat proses mengenkrip sebagai pembangkit bilangan acak contoh : kata kunci "malang"
3. Klik tombol Dekrip dan Proses Dekripsi menggunakan *spread spectrum image steganography* akan berjalan dan akan muncul pesan "Deskripsi telah terproses!" jika proses sudah selesai, seperti ditunjukkan pada gambar dibawah.



*Gambar 9. Tampilan Proses Deskripsi*

4. Klik tombol save setelah proses deskripsi berhasil.
   Dari kedua proses dapat diperoleh hasil adapun hasil untuk proses diatas dapat dilihat pada gambar berikut ini :


sebelum sesudah

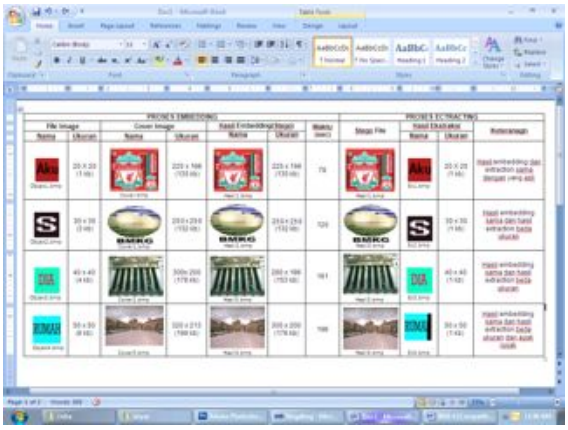
*Gambar 10. Tampilan Cover Image*

cover image sebelum dan sesudah disisipi file image.

sebelum sesudah

*Gambar 9. Tampilan File Sisip*

File image sebelum dan sesudah diekstraksi Untuk proses keseluruhan dari uji coba Proses Enkripsi dan Deskripsi file image menggunakan *spread spectrum image steganography* dapat dilihat pada Tabel berikut ini:



*Gambar 10. Tampilan Beberapa hasil Enkripsi*

## V. KESIMPULAN DAN SARAN

Setelah menganalisa dan merancang serta mengimplementasikan pembuatan Aplikasi Steganography Enkripsi image to image dengan metode Spread Spectrum, maka dapat diambil kesimpulan dan saran sebagai berikut :

A. Kesimpulan

- Penyisipan file image ke dalam cover image dapat dilakukan dengan cara menghitung masing-masing biner dari file yang disisipkan kemudian menghitung biner dari kata kunci. Kedua biner tersebut di XOR kan. Hasil dari XOR digabungkan ke dalam image cover.
- Proses dekripsi dapat dilakukan dengan kebalikan dari perhitungan proses enkripsi.

B. Saran

Untuk menyempurnakan sistem pakar diagnosa hama dan penyakit tanaman apel, maka penulis memberikan saran sebagai berikut:

- Aplikasi Stegnografi ini tidak bisa digunakan untuk format image GIF, diharapkan kedepannya aplikasi ini bisa digunakan untuk format image GIF.
- Teknik steganografi yang digunakan adalah metode *spread spectrum image steganography*, tidak menuntut kemungkinan digunakan teknik lain yang lebih baik dalam kinerja dan kecepatan prosesnya.

## DAFTAR PUSTAKA

Arius Dony. 2008. *Kriptografi Keamanan Data &Komunikasi*.Yogyakarta: Graha Ilmu.

Budi Sutedjo Dharma Oetomo, "*Perencanaan Dan Pembangunan Sistem Informasi*",

Bin, Chaeriah.A.W.,2006.SISTEM KEAMANAN DATA MENGGUNAKAN SPREAD SPECTRUM IMAGE STEGANOGRAPHY (SSIS) DAN ALGORITMA KRIPTOGRAFI DES ( DATA SECURITY SYSTEM USING SPREAD SPECTRUM IMAGE STEGANOGRAPHY (SSIS) AND DES CRYPTOGRPHY ALGORITHM )

Dony Ariyus. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis, danImplementasi* Yogyakarta: Andi.

Ir. Yusuf Kurniawan, MT., 2004, "*Kriptografi: Keamanan Internet dan Jaringan Komunikasi*" Penerbit Informatika Bandung, Yogyakarta

Munir, Rinaldi (2006). *Kriptografi.*Informatika, Bandung

Munir, Rinaldi. (2004). *Steganografi dan Watermarking.*URL

Susanto, Agus. 2006. *Studi dan Implementasi Steganografi pada Berkas MIDI*. Departemen Tehnik Informatika: Institut Teknologi Bandung.

Vembrina, Y. G. (2006). Spread Spectrum Steganography.

Wandani, Henny, Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem, Universitas Sumatra Utara

Widyawan, Tri. (http://www.academia.edu/5306496/Pengamanan_Pesan Steganografi_dengan_Metode_LSB_Berlapis_Enkripsi_dalam_PHP). Diakses tanggal 06/03/2014