BAB I
PENDAHULUAN

A. Latar Belakang

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.

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, dimana disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya “tersembunyi atau terselubung”, dan graphein, “menulis”. Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (file) komputer. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan tetap tersedia, maka dengan steganografi dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tapi metoda ini sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan. Kedua teknik ini dapat digabungkan untuk mendapatkan metoda pengiriman rahasia yang sulit dilacak. Pertama pesan dienkrip, kemudian cipherteks disembunyikan dengan cara steganografi pada media yang tampak tidak mencurigakan. Cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan.

B. Perumusan Masalah

Adapun rumusan masalah yang kami buat yaitu :

1. Apakah itu Steganografi ?
2. bagaimana cara menggunakan aplikasi Steganografi ?

C. Batasan Masalah

Adapun ruang lingkup makalah ini yaitu meliputi :

1. Data yang akan dienkripsi bisa semua format files.
2. Gambar yang digunakan untuk menyembunyikan pesan teks adalah dengan ekstensi .bmp, .jpg, .gif, .png, .wmf, .emf, dan .ico.

D. Tujuan dan Manfaat

1. Tujuan

   Adapun Tujuan dari ini adalah :

   a) Menjelaskan sebuah perangkat lunak yang dapat mengenkripsi, dekripsi dan menyisipkan teks kedalam gambar dengan menggunakan algoritma MMB (Modular Multiplication-based Block Cipher) dan LSB (Least Significant Bit).

   b) Menerapkan algoritma MMB (Modular Multiplication-based Block Cipher) sebelum disisipkan kedalam gambar.

c) Menerapkan algoritma LSB (Least Significant Bit) untuk menyisipkan file kedalam gambar.

2. Manfaat

Adapun manfaat yang dapat diperoleh dari penyusunan makalah ini ini, yaitu diharapkan menjadi memotivasi pihak-pihak yang tertarik untuk melakukan penelitian lanjutan mengenai perrmasalahan di bidang sistem pengamanan komputer dengan menggunakan steganografi.

BAB II

TINJAUAN PUSTAKA

A. Dasar Teori

1. Pengertian 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, dimana disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas.

Steganography juga berbeda dengan cryptography yaitu terletak pada hasil keluarannya.Hasil dari cryptography biasanya berupa data yang berbeda dari bentuk aslinya dan biasanyadatanya seolah-olah berantakan namun dapat dikembalikan ke data semula. Sedangkan hasil dari keluaran steganography memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh komputer atau pengolah data digital lainnya. Selain itu pada *steganography* keberadaan informasi yang disembunyikan tidak terlihat/diketahui dan terjadi penyampulan tulisan *(covered writing*).

Sedangkan pada *cryptography* informasi dikodekan dengan enkripsi atau teknik pengkodean dan informasi diketahui keberadaanya tetapi tidak dimengerti maksudnya. Namun secara umum *steganography* dan *cryptography* mempunyai tujuan yang sama yakni mengamankan data, bagaimana supaya data tidak dapat dibaca, dimengerti atau diketahui secara langsung. *Steganography* memanfaatkan kekurangan - kekurangan indra manusia seperti mata dan telinga. Dengan kekurangan inilah maka teknik ini dapat diterapkan dalam berbagai media digital. Media *cover* merupakan data digital yang akan ditempeli dengan data yang akan disembunyikan atau sering disebut dengan stego medium. Berbagai media yang dapat digunakan sebagai cover dari data atau informasi yang akan disembunyikan dengan berbagai teknik *steganography*. Media yang

dimaksudkan adalah media dalam bentuk file digital dengan berbagai format, antara lain :Images (bmp, gif, jpeg, tif, dll), Audio (wav, Mp3, dll), Video, Teks

2. Kegunaan Steganografi

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 cara untuk membuat pengganti suatu nilai hash satu arah (yaitu pengguna mengambil suatu masukan panjang variabel dan membuat sebuah keluaran panjang statis dengan tipe string untuk melakukan verifikasi bahwa tidak ada perubahan yang dibuat pada variabel masukan yang asli). Selain itu juga, steganografi dapat digunakan sebagai tag-notes untuk citra online. Steganografi juga dapat digunakan untuk melakukan perawatan atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotasi, pencuri, atau dari pihak yang tidak berwenang.

3. Teknik Steganografi

Tujuan dari teknik-teknik steganografi adalah menyembunyikan keberadaan pesan.Teknik *watermarking*, merupakan bagian dari steganografi yang ditujukan untuk perlindungan hak cipta, tidak hanya dimaksudkan untuk menyembunyikan keberadaan pesan atau informasi, tapi lebih diarahkan untuk menjamin informasi dapat selamat dari beragam serangan yang dimaksudkan untuk menghancurkan watermark.

4. Terminologi dalam Steganografi

Terdapat beberapa istilah yang berkaitan dengan steganografi.

a. Hiddentext atau embedded message: pesan atau informasi yang disembunyikan.

b. Covertext atau cover-object: pesan yang digunakan untuk menyembunyikan embedded message.
c. Stegotext atau stego-object: pesan yang sudah berisi embedded message. Dalam steganografi digital, baik hiddentex atau covertext dapat berupa teks, audio, gambar, maupun video.

5. kriteria yang harus dipenuhi.
   a. Impercepbility. Keberadaan pesan tidak dapat dipersepsi oleh indrawi.Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata.Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
   b. Fidelity. Mutu media penampung tidak berubah banyak akibat penyisipan.Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.
   c. Recovery. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan
6. Teknik Watermarking

   Ada berbagai tujuan yang ingin dicapai dari penggunaan watemarking, sebagai suatu teknik penyembunyian data pada data digital lain yaitu**:**
   a. Tamper-proofing **:***Watemarking* digunakan sebagai alat indikator yang menunjukkan apakah data *digital* yang asli telah mengalami perubahan dari aslinya (mengecek integritas data).
   b. Feature location **:***Watemarking* sebagai alat identifikasi isi dari data *digital* pada lokasi-lokasi tertentu, misalnya penamaan suatu objek tertentu dari beberapa objek yang ada pada suatu citra *digital*.
   c. Annotation/caption **:***Watermark* berisi keterangan tentang data *digital* itu sendiri, misalnya pada *broadcast monitoring* pada penayangan iklan di stasiun TV. Selain itu, *watermark* juga dapat digunakan untuk mengirimkan pesan rahasia.

d. Copyright-Labeling **:***Watemarking* digunakan sebagai metoda untuk menyembunyikan label hak cipta pada data *digital* atau sebagai bukti autentik kepemilikan atas dokumen *digital* tersebut.
e. Robust watermarking : Jenis watermark ini tahan terhadap serangan (attack), namun biasanya watermark yang dibubuhi ke dokumen masih dapat ditangkap oleh indera penglihatan atau pendengaran manusia.
f. *Fragile watermarking :*Jenis *watermark* ini akan mudah rusak jika terjadi serangan, namun kehadirannya tidak terdeteksi oleh indera manusia. Jika diinginkan untuk membuat suatu algoritma yang dapat mengimplementasikan watemarking yang memiliki fidelity yang tinggi (adanya watermark tidak disadari oleh pengamatan manusia) maka hasilnya akan semakin rentan terhadap serangan.

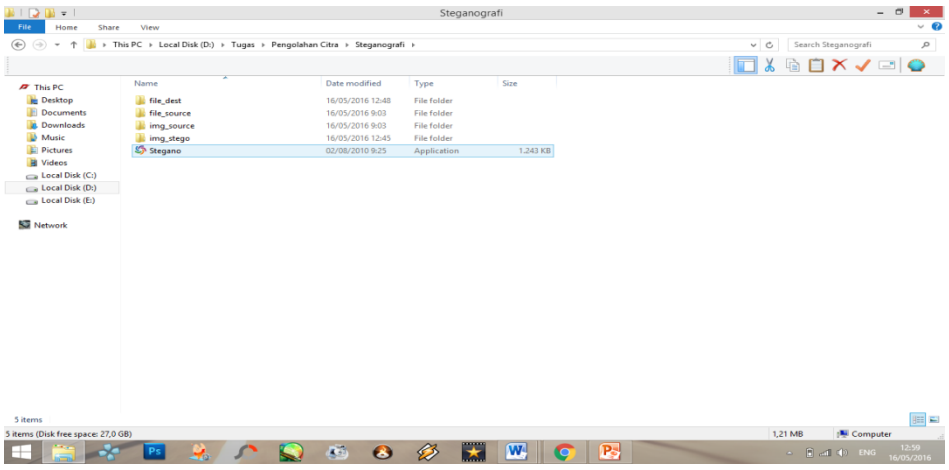
BAB III

PEMBAHASAN

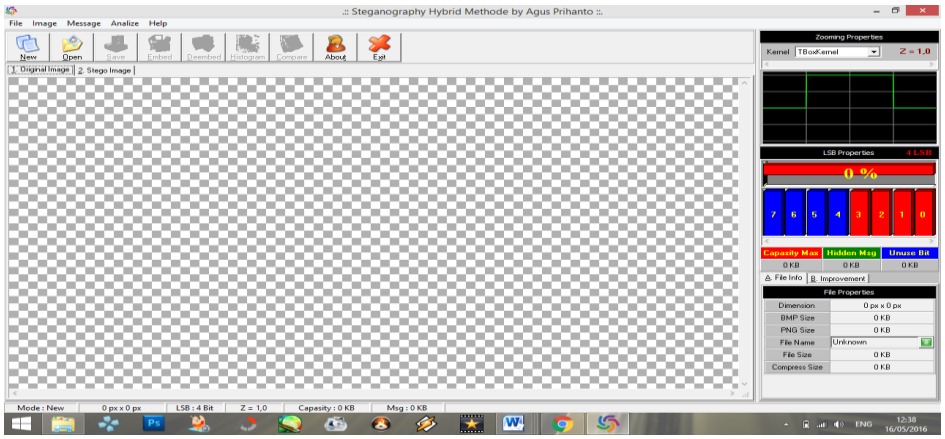
A. Cara Menggunakan Program

Adapun langkah-langkah menggunakan aplikasi steganografi ini adalah sebagai berikut:

1. Bukalah aplikasi yang bernama Stegano.exe

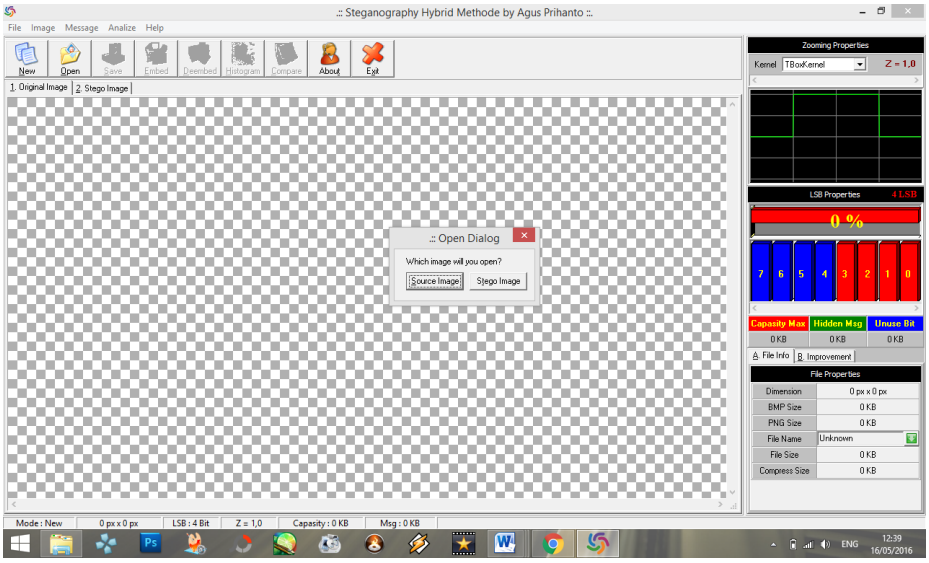


2. Setelah anda membuka aplikasi tersebut, maka akan tampil halaman utama aplikasi steganografi tersebut.



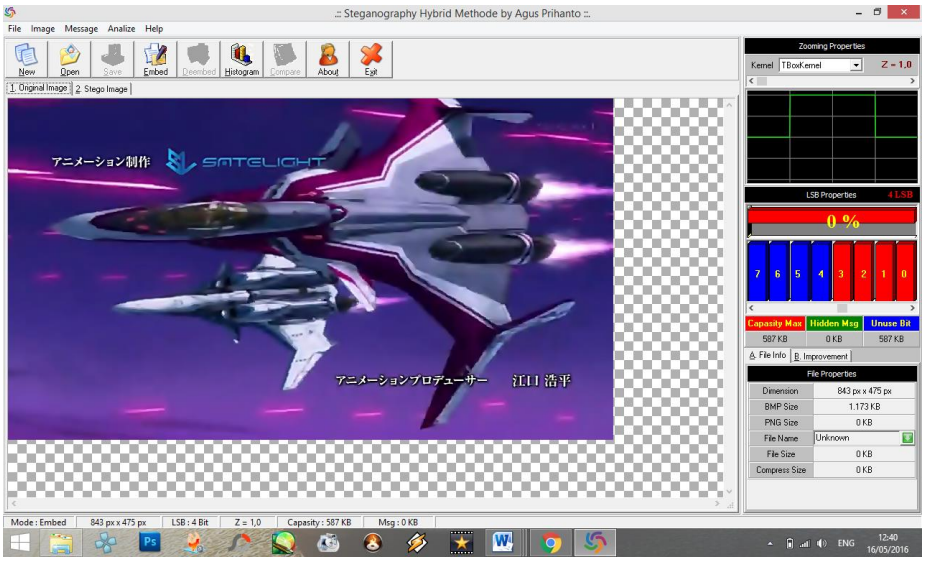
Gambar

3. Untuk membuka gambar yang akan digunakan untuk menyembunyikan file rahasia yang ingin dimasukkan, klik icon open kemudian klik tombol ‘Source Image’.



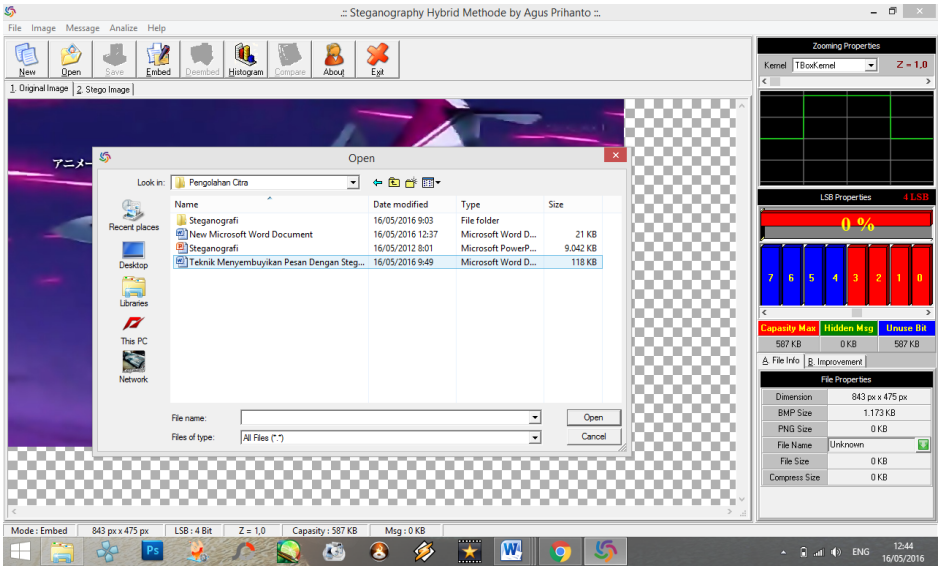
Gambar

4. Setelah menentukan gambar yang akan digunakan, maka akan tampil gambar yang telah dipilih.

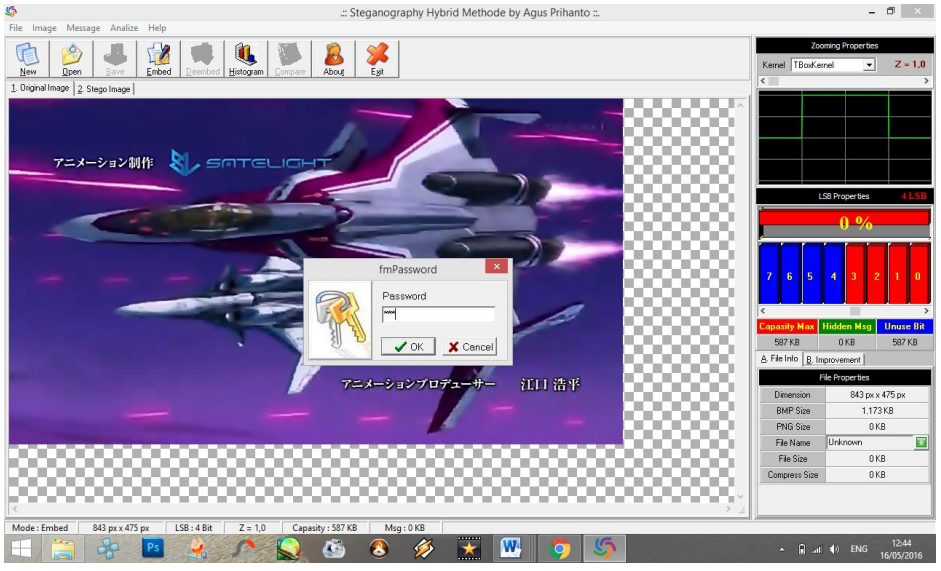


Gambar

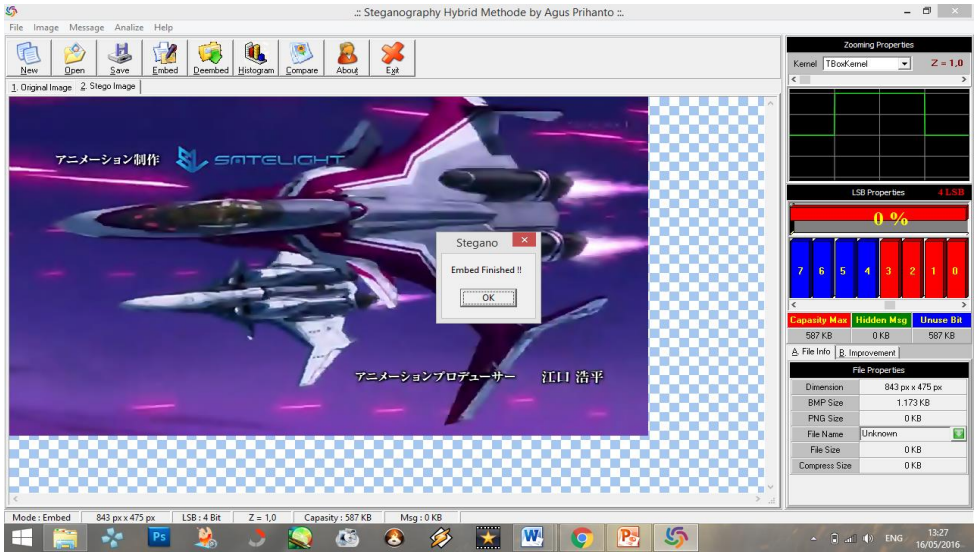
5. Selanjutnya, untuk menyisipkan file ke dalam gambar yang dipilih, klik icon ‘Embed’ kemudian pilih file yang akan disisipkan.



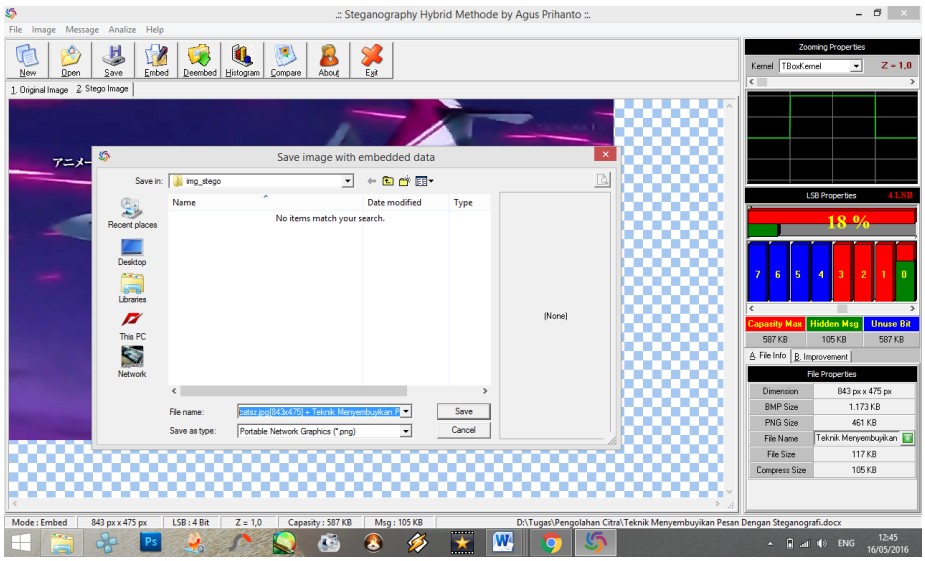
6. Setelah file dipilih, maka akan otomatis muncul tampilan seperti dibawah ini, kemudian silahkan masukkan password yang anda inginkan.



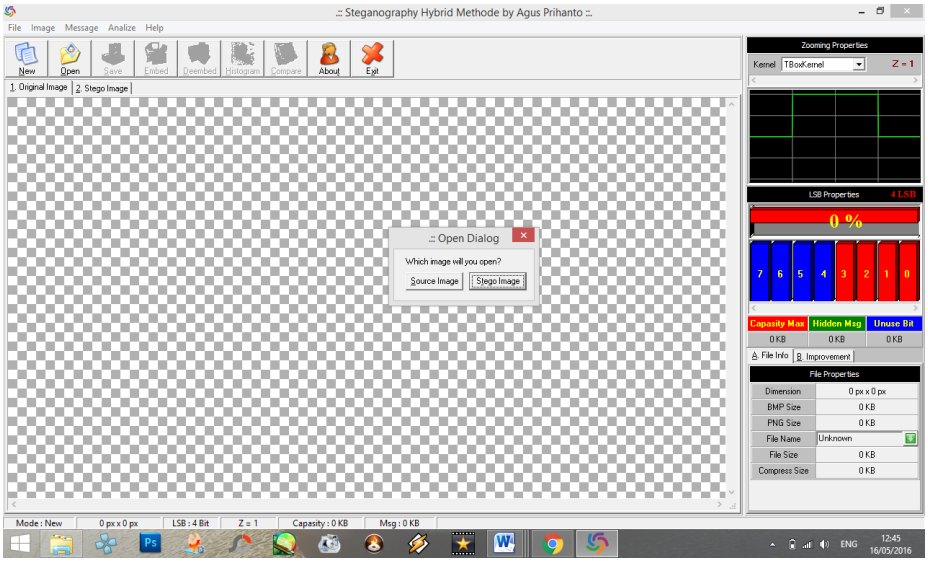
7. Setelah itu akan muncul tampilan seperti di bawah ini.



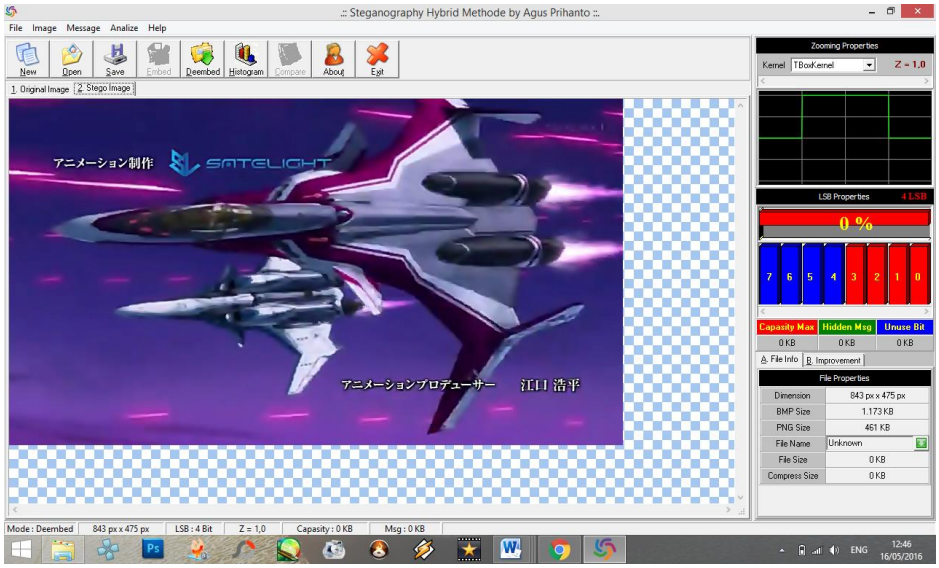
8. Simpan gambar yang telah di embed tadi dengan mengklik ikon Save ke folder yang anda inginkan. Jika sudah selesai tutup program dengan mengklik ikon Exit.



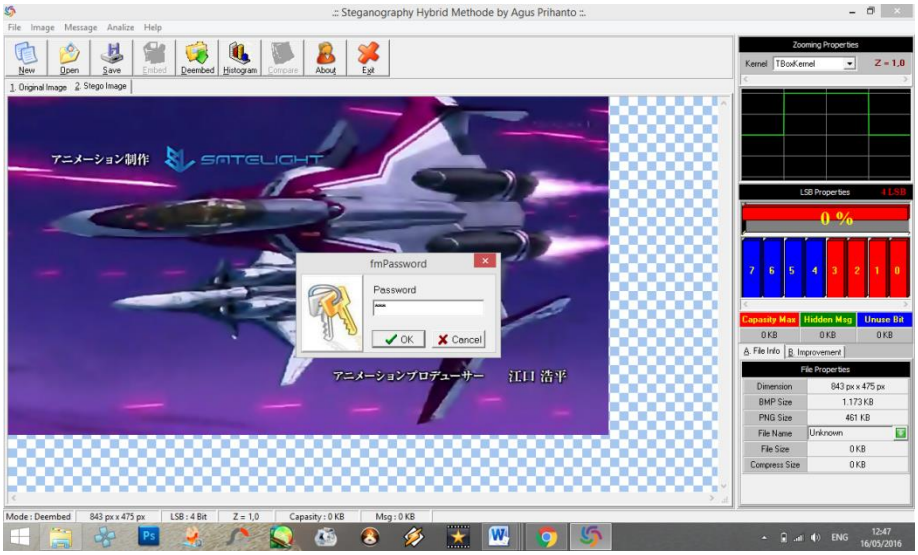
9. Jika anda ingin membuka gambar yang telah di embed tadi, klik tombol Open kemudian pilih ‘Stego Image’.



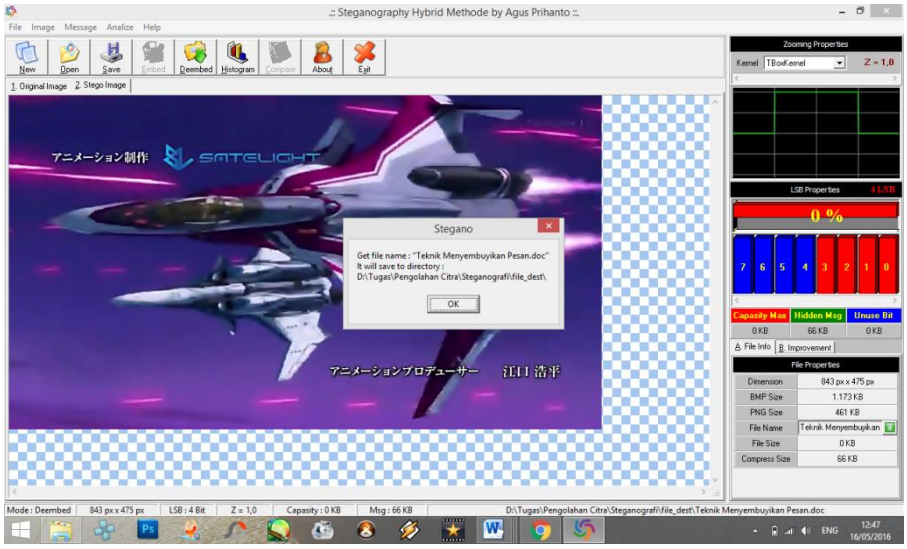
10. Setelah itu akan muncul tampilan seperti di bawah ini.



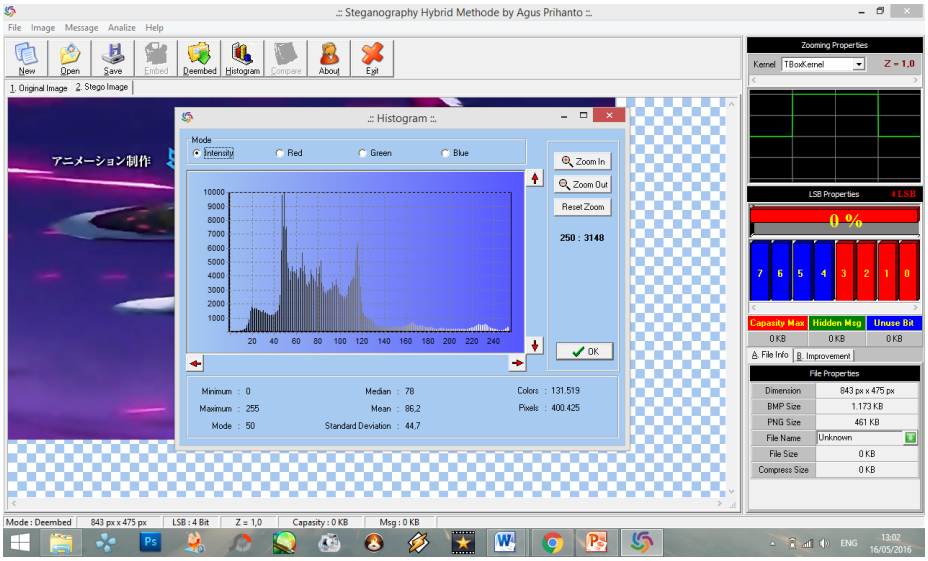
11. Setelah itu untuk membuka file yang akan di keluarkan, klik icon ‘Deembed’ maka akan otomatis muncul tampilan form password seperti dibawah ini kemudian masukkan password yang telah ditentukan sebelumnya untuk membuka file.



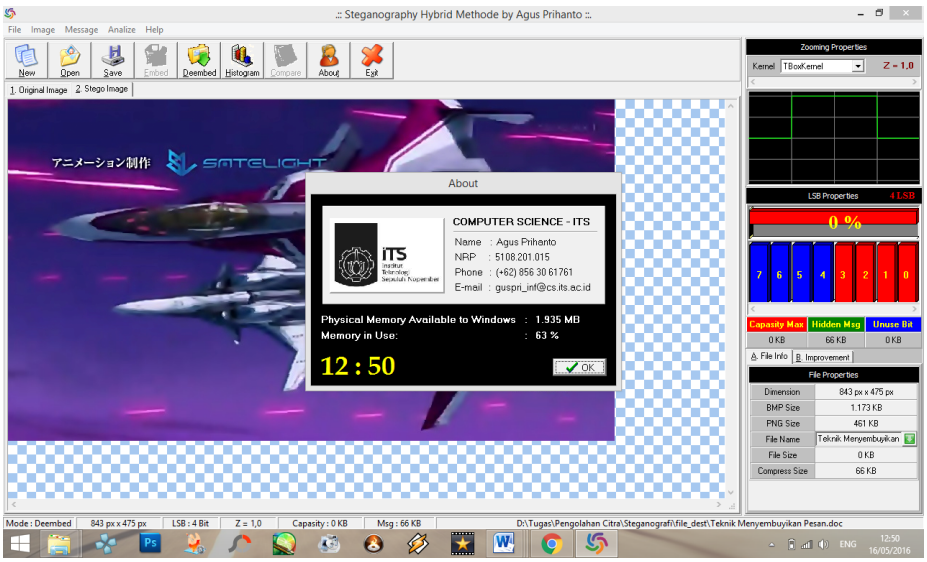
12. Setelah itu muncul pesan seperti di bawah ini. File yang sudah dikeluarkan tadi akan otomatis disimpan dalam folder ‘file_dest’.



13. Jika anda mengklik ikon Histogram, maka muncul form sebagai berikut. Tampilan ini menampilkan grafik dari tabulasi frekuensi warna dari citra digital yang digambarkan dengan grafis batangan sebagai manifestasi data binning.



14. Jika anda mengklik ikon About maka akan muncul tampilan yang berisi sekilas tentang nama pembuat program.



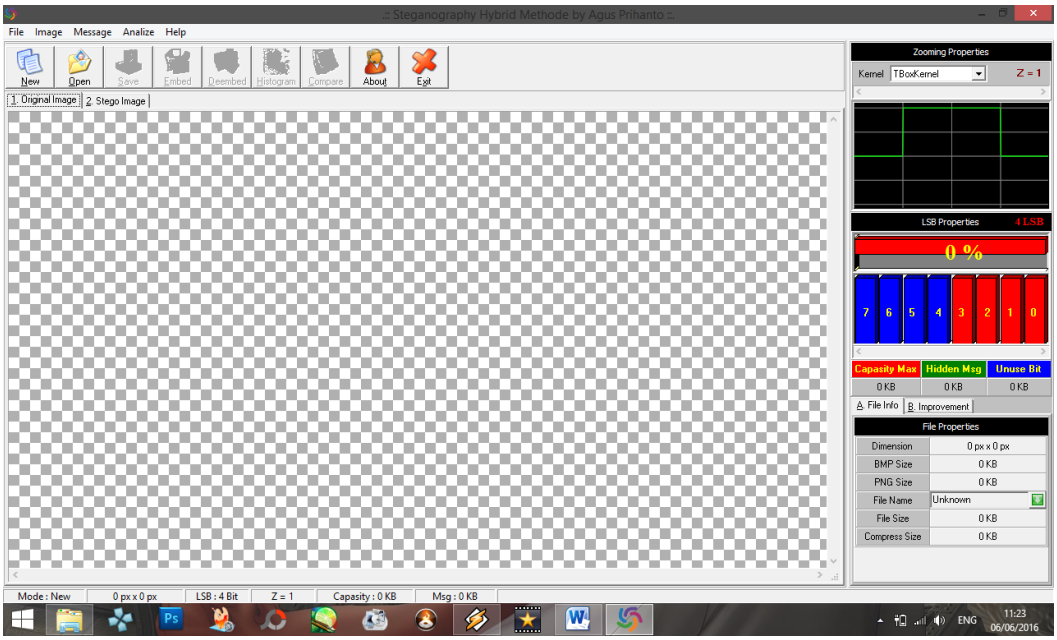
BAB III

KESIMPULAN

Teknik steganografi dibandingkan dengan kriptografi memiliki keunggulan yaitu dengan steganografi keberadaan dari informasi yang disembunyikan tidak dapat dideteksi dengan mudah, dengan steganografi informasi disembunyikan sedemikian rupa sehingga menghilangkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui.

Keterbatasan manusia pada indera penglihatan dapat dimanfaatkan, terutama pada perubahan warna yang sangat sedikit dan perubahan kecil pada intensitas gambar. Penulis berkesimpulan bahwa dengan memberikan perubahan kecil pada warna di sebagian daerah berintensitas sangat rendah dari suatu citra digital (watemarking parsial), maka akan diperoleh citra yang sudah diberi tanda yang memiliki fidelity yang sangat baik, yaitu tingkat degradasinya tidak dirasakan oleh pengamatan manusia.

PROGRAM STEGANOGRAFI



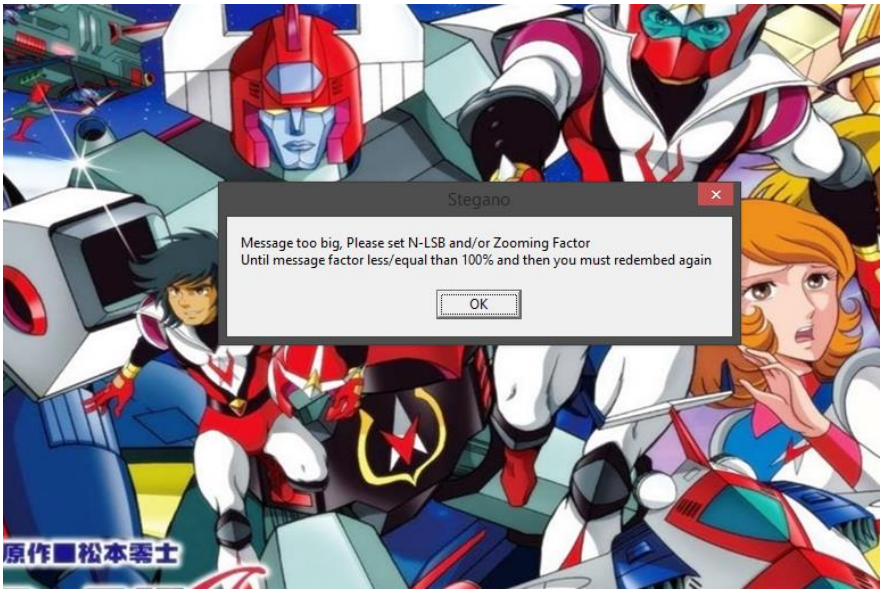
Program yang kami gunakan untuk membuat Steganografi adalah"Steganography Hybrid Methode"

Program ini memiliki kelebihan di bagian fidelity dan recovery. Untuk bagian fidelity, kami sudah mencoba dengan program ini setelah terjadi penambahan file rahasia, Kualitas gambarnya sama dengan yang asli dan ukuran Stegano Image-nya tidak jauh berbeda dengan gambar yang asli. Orang tidak mengetahui kalau di dalam gambar stegano-data tersebut terdapat data rahasia. Kemudian di bagian recovery

kami telah mencoba pada data yang sebelumnya yang telah di stego image dan datanya dapat dikembalikan dan dibaca isinya.

Kemudian untuk kelemahan program yang kami miliki adalah ada pada bagian Robustness. Pada program ini, telah kami coba untuk melakukan cropping pada file yang telah di Stegano Image. Kami buka gambar yang telah di crop tadi dan kemudian di klik "Deembed" ternyata file rahasia yang ada di dalamnya tidak dapat dikembalikan dan malah muncul pesan seperti disamping ini, walaupun kita sudah memasukkan password yang benar.

Selain itu untuk kapasitas file rahasia yang ingin dimasukkan ke gambar harus kurang dari kapasitas maksimal gambar tempat kita ingin menyembunyikannya. Kalau tidak akan muncul pesan seperti di bawah ini:



Sumber Makalah

https://muhammadrida14.wordpress.com

http://rhyoeozonit29tugaskuliah.blogspot.co.id