Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image

Tutik Lestari[1], Nunung Nurmaesa[2], Arni Retno Mariana[3]
[1,2,3]Dosen di STMIK Bina Sarana Global
Email : [1]tutiklestari89@gmail.com, [2]syahmae5@gmail.com, [3]arnie.mariana@stmikglobal.ac.id

Abstrak— **Kondisi saat ini, untuk mendapatkan informasi apa saja, dimana saja dan kapan saja, asalkan tersedia jaringan internet maka akan sangat mudah mengakses informasi yang kita butuhkan, informasi atau data sekarang ini sumbernya bukan cuma lewat buku, surat kabar atau yang lainnya yang berupa fisik, melainkan lewat ponsel pintar maupun laptop, namun adanya berbagai kemudahan yang tersedia dibarengi juga dengan dampaknya tidak hanya dari segi positif saja, tapi dari segi negatif pun ada. Contohnya mudah bocornya informasi-informasi penting ke orang yang tidak berkepentingan yaitu oknum yang secara sengaja mengincar informasi tersebut untuk di selewengkan untuk kepentingan dan tujuan tertentu yang tentu saja merugikan kita sebagai pemilik data, misalkan kata sandi (password) dan nomor PIN. Hal ini tentu saja menjadi sesuatu yang patut diwaspadai apabila informasi yang dikirimkan merupakan informasi yang bersifat rahasia. Cara mengantisipasinya yaitu dengan cara tidak mudah memberikan informasi apapun kepada siapaun terlebih bila sumbernya tidak jelas, dan meningkatkan kepahaman akan pengetahuan tentang keamanan data. Untuk mengamankan data salah satunya dapat dilakukan dengan teknik steganografi, yaitu teknik untuk menyembunyikan keberadaan pesan kedalam sebuah media dengan suatu cara sehingga tidak ada seorang pun yang mengetahui atau menyadari sebenarnya ada suatu pesan rahasia yang hanya diketahui si pengirim dan si penerima. pada steganografi, data yang telah disandikan dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Dengan cara ini maka kita tidak perlu khawatir lagi apabila mengirimkan pesan apapun terlebih bila pesan itu bersifat rahasia ke siapapun dan dalam keadaan aman.**

Kata Kunci— informasi, keamanan data, steganografi

I. LATAR BELAKANG

Perkembangan teknologi pada saat ini sangat pesat, terutama teknologi dalam bidang informasi dan komunikasi. Komunikasi yang dahulu identik dengan menggunakan kabel pun mulai ditinggalkan dan digantikan dengan jaringan nirkabel (tanpa kabel). Tak hanya itu saja, dalam hal komunikasi, telepon genggam atau yang kita kenal dengan ponsel terus berkembang hingga menjadi ponsel cerdas yang tanpa batasan waktu dan tempat makin mudah dan murah untuk diperoleh dan bisa memperoleh informasi apapun yang makin menggeser komunikasi telepon rumah hingga komunikasi secara langsung.

Namun, hal positif selalu beriringan dengan hal negatif, seiring dengan kemudahan tersebut banyak kejahatan sistem informasi yang sudah mengintai. Banyak orang diluar sana yang mencoba mengakses informasi yang bukan haknya dengan tujuan untuk disalahgunakan. Keamanan menjadi sangat penting apabila informasi yang dikirimkan merupakan informasi yang bersifat rahasia. Maka dari itulah diperlukan pengetahuan tentang keamanan data yang bertujuan agar selalu berhati-hati dan tahu cara mencegah dari orang-orang yang tidak bertanggungjawab.

Untuk mengamankan data salah satunya dapat dilakukan dengan teknik steganografi, yaitu teknik untuk menyembunyikan pesan kedalam sebuah media dengan suatu cara sehingga tidak ada seorang pun yang mengetahui atau menyadari sebenarnya ada suatu pesan rahasia selain si pengirim dan si penerima. Contoh kasus pada peristiwa penyerangan gedung World Trade Center (WTC) di Amerika Serikat tanggal 11 September 2001. Pada peristiwa tersebut disebutkan bahwa para teroris menyembunyikan peta-peta, foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan web site lainnya dan tidak seorang pun menyadari bahwa ada pesan rahasia dibalik situs tersebut.

Tujuan penggunaan dari steganografi adalah untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit di deteksi dan melindungi hak cipta suatu produk. Pada steganografi, data yang telah disandikan (chipertext) dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

A. Rumusan Masalah

Rumusan masalah dari penelitian adalah:

1. Bagaimana cara menyisipkan pesan kedalam media image?
2. Apakah terdapat perbedaan dalam menyisipkan pesan?

B. Ruang Lingkup

Penulis membahas permasalahan penelitian hanya pada aplikasi yang dibangun yaitu aplikasi steganografi yang dapat digunakan untuk menyisipkan pesan dalam media image.

C. Tujuan Penulisan

Adapun tujuan yang ingin dicapai dengan adanya pembuatan makalah ini yaitu:

1. Untuk memenuhi tugas mata kuliah keamanan komputer.
2. Sebagai bahan referensi bagi pembaca

II. LANDASAN TEORI

A. Pengertian Aplikasi

Aplikasi adalah program siap pakai yang dapat digunakan untuk menjalankan perintah-perintah dari pengguna aplikasi tersebut dengan tujuan mendapatkan hasil yang lebih akurat

sesuai dengan tujuan pembuatan aplikasi tersebut, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu tehnik pemrosesan data aplikasi yang biasanya berpacu pada sebuah komputasi yang diinginkan atau diharapkan maupun pemrosesan data yang diharapkan.

Menurut Kamus Kamus Besar Bahasa Indonesia (1998 : 52) adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu. Aplikasi adalah suatu program komputer yang dibuat untuk mengerjakan dan melaksanakan tugas khusus dari pengguna

B. Pengertian Steganografi

Steganografi adalah seni dan ilmu menyembunyikan pesan ke dalam sebuah media dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa sebenarnya ada suatu pesan rahasia.

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.

Steganografi menurut Rinaldi Munir, 2004 adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia.

C. Kriteria Steganografi

1. Imperceptibility, keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra covertext-nya. Jika covertext berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio stegotext-nya.
2. Fidelity, mutu stegomedium tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra covertext-nya. Jika covertext berupa audio, maka audio stegotext tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.
3. Recovery, pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu pesan rahasia di dalam stegotext harus dapat diambil kembali untuk digunakan lebih lanjut

D. Teknik Steganografi

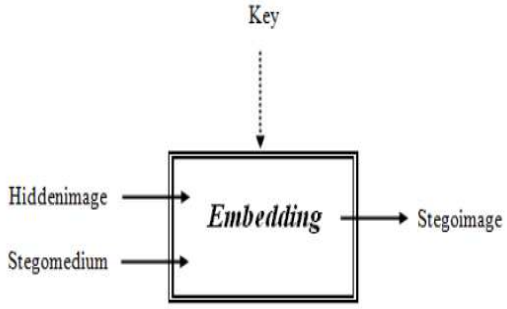
Menurut Ariyus (2009), ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu:

1. Injection, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut embedding.
2. Substitusi, data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
3. Transform Domain, teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space. Akan sangat lebih efektif teknik ini diterapkan pada file berekstensi JPG.
4. Spread Spectrum, sebuah teknik pengtransmisian menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwidth) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika pseudo-noise code tersinkronisasi.
5. Statistical Method, teknik ini disebut juga skema steganographic 1bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
7. Cover Generation, metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah Spam Mimic

E. Proses Steganografi

Umumnya terdapat dua proses dalam steganografi, yaitu embedding dan Ekstraksi.

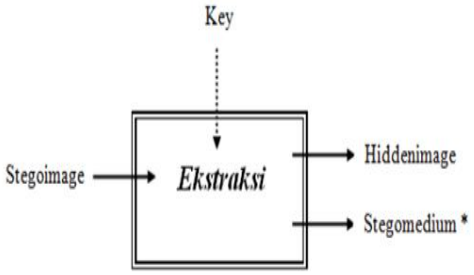
1. Embedding, yaitu proses untuk menyembunyikan pesan



Gambar 2.2 Proses Embedding Citra

Gambar diatas menunjukkan proses penyembunyian pesan dimana di bagian pertama, dilakukan proses embedding hidden image yang hendak disembunyikan secara rahasia ke dalam stegomedium sebagai media penyimpanan, dengan memasukkan kunci tertentu (key), sehingga dihasilkan media dengan data tersembunyi di dalamnya (stegoimage)

2. Ekstraksi, yaitu proses untuk mengektraksi pesan yang disembunyikan



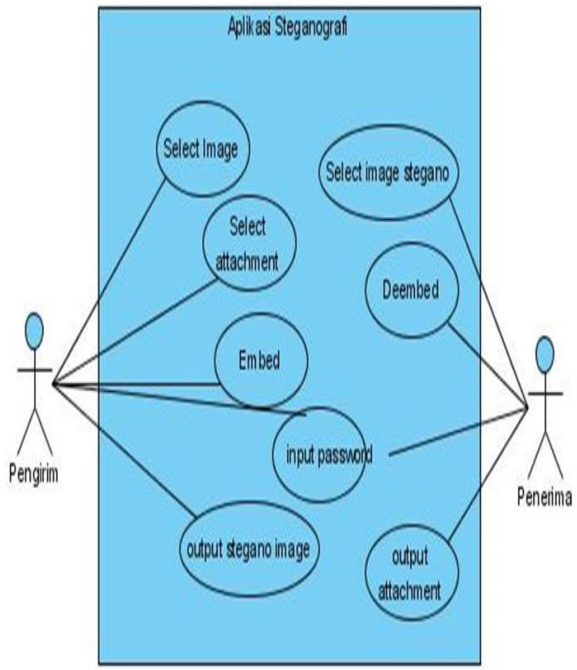
Gambar 2.3 Proses Ekstraksi Citra

Pada gambar diatas dilakukkan proses ekstraksi pada stegoimage dengan memasukkan key yang sama sehingga didapatkan kembali hiddenimage. Kemudian dalam kebanyakan teknik steganografi, ekstraksi pesan tidak akan mengembalikan stegomedium awal persis sama dengan stegomedium setelah dilakukan ekstraksi bahkan sebagian besar mengalami kehilangan. Karena saat penyimpanan pesan tidak dilakukan pencatatan kondisi awal dari stegomedium yang digunakan untuk menyimpan pesan (Cox et al, 2008).

III. HASIL DAN ANALISA

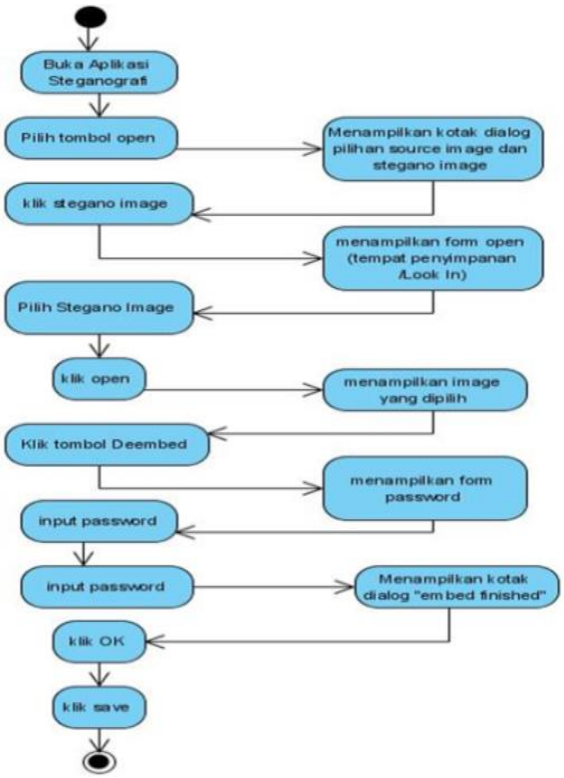
A. Hasil

Berdasarkan dari penjelasan diatas berikut merupakan activity sistem berjalan saat ini

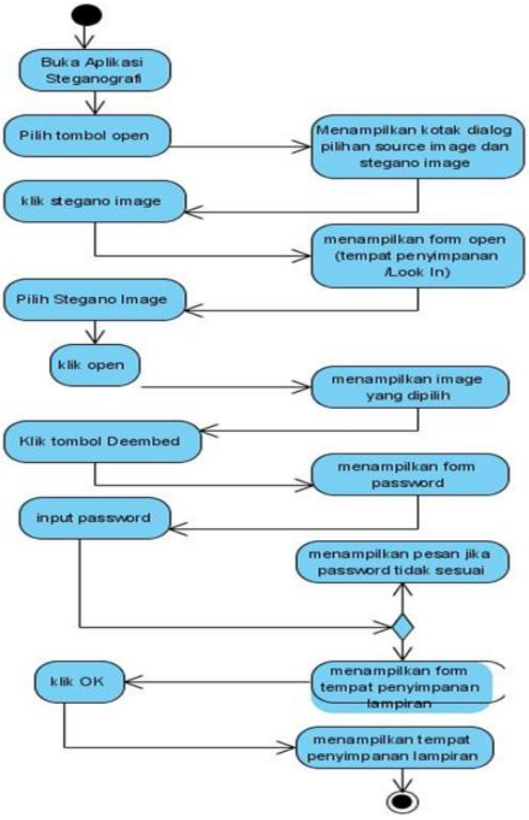


Gambar 3.1 Use Case Diagram Steganografi

Pada use case diagram, hanya menggambarkan penggunaan aplikasi steganografi secara umum. Agar lebih detail/jelas dalam penggunaan aplikasi steganografi bagi pengirim dan penerima dapat dilihat pada Activity diagram dibawah ini.



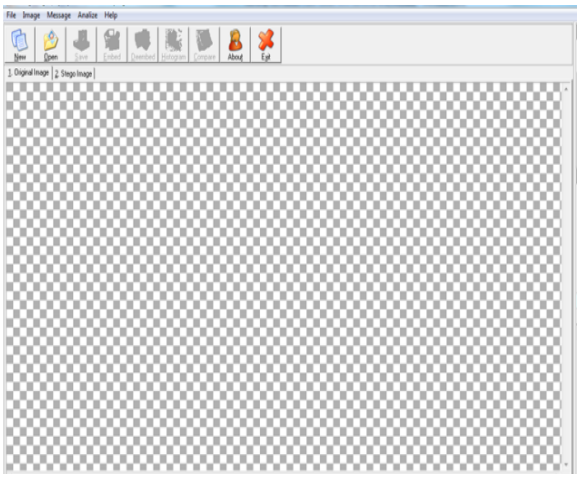
Gambar 3.2 Activity Diagram Steganografi - Pengirim



Gambar 3.3 Activity Diagram Steganografi – Penerima

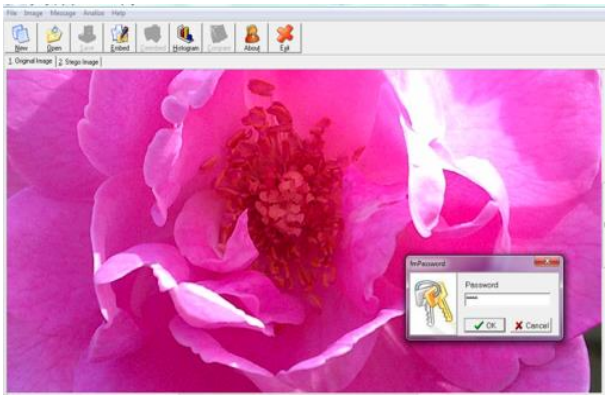
B. Aplikasi Steganografi

Aplikasi steganografi untuk menyisipkan pesan dalam media image, dapat dilihat seperti pada gambar dibawah ini :



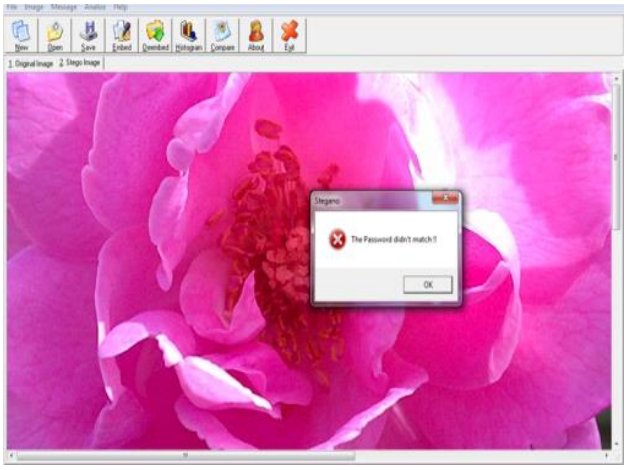
Gambar 3.4 Tampilan Utama

Untuk melakukan embedding (menyembunyikan pesan), pengirim (pengguna aplikasi) harus mengklik tab Open, selanjutnya muncul kotak dialog, lalu pilih source Image (mencari gambar yang akan disisipi). Pada gambar yang akan disisipi, pengirim perlu menginputkan password. Parsword ini selanjutnya digunakan untuk digunakan untuk mengekstraksi image.



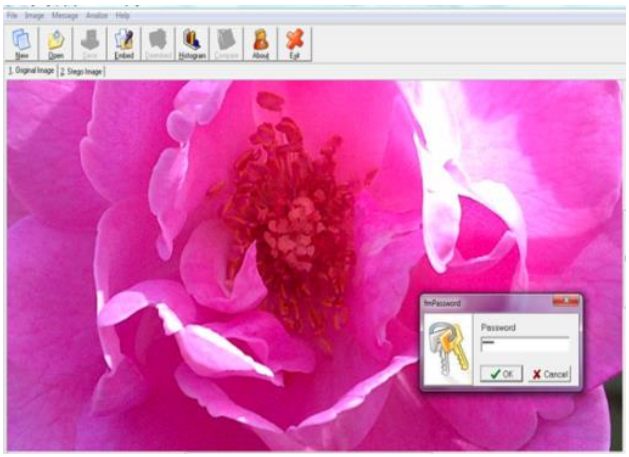
Gambar 3.5 Input Password untuk menyembunyikan pesan

Jika Penerima salah memasukkan password, maka akan muncul pesan jika password tidak sesuai. Proses ekstraksi akan gagal, pesan (lampiran) tidak dapat dilihat. Oleh karena itu, Password yang diinput haruslah sama dengan password waktu embedding.



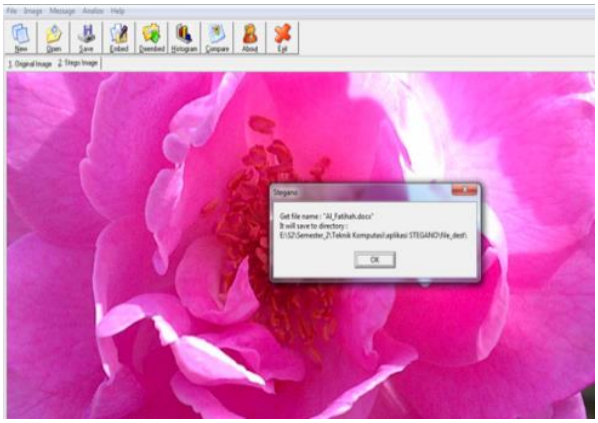
Gambar 3.6 Kotak pesan ketika Password salah

Untuk melakukan embedding (menyembunyikan pesan), pengirim(pengguna aplikasi) harus mengklik tab Open, selanjutnya muncul kotak dialog, lalu pilih source Image (mencari gambar yang akan disisipi). Pada gambar yang akan disisipi, pengirim perlu menginputkan password. Parsword ini selanjutnya digunakan untuk digunakan untuk mengekstraksi image.



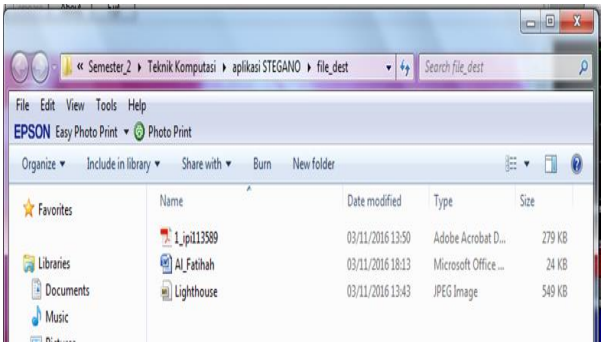
Gambar 3.7 Input Password untuk menyembunyikan pesan

Jika Penerima salah memasukkan password, maka akan muncul pesan jika password tidak sesuai. Proses ekstraksi akan gagal, pesan (lampiran) tidak dapat dilihat. Oleh karena itu, Password yang diinput haruslah sama dengan password waktu embedding



Gambar 3.8 Kotak pesan ketika Password benar

Jika password yang dimasukkan sesuai (benar), aplikasi steganografi akan langsung menampilkan tempat dimana pesan itu disimpan. Seperti gambar dibawah ini

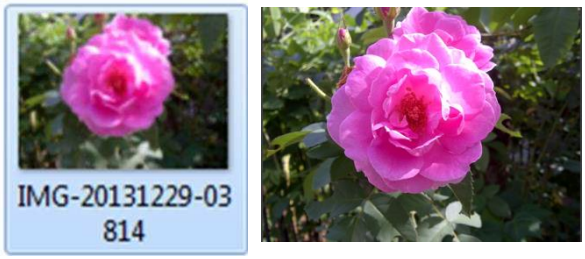


Gambar 3.9 Tampilan tempat penyimpanan file yang disisipkan

E. *Analisa*

Dari proses penyisipan pesan menggunakan aplikasi steganografi dapat dihasilkan image yang sudah disisipi pesan dan image tersebut tidak jauh berbeda dengan image aslinya. Pesan yang disipkan dapat berupa pesan image, doc, pdf, ppt, dll. Image asli dan image yang sudah disisipi pesan dapat dilihat perbandingannya seperti gambar dibawah ini.

Gambar 3.10 Image Asli



Gambar 3.11 Image setelah dilakukan penyisipan

IV. KESIMPULAN

A. *Kesimpulan*

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa:

1. Cara menyisipkan pesan dalam media image dapat menggunakan aplikasi steganografi. Pesan yang disisipkan dapat berbentuk gambar, teks, ppt, pdf, dll.
2. Dalam menyisipkan pesan tidak ada perbedaan yang menonjol, begitupun dengan media image yang digunakan. Image asli dan image yang sudah disisipi pesan, jika dilihat hampir sama. Namun size (ukuran) pesan yang sudah disisipi akan lebih besar daripada image asli

B. *Saran*

Aplikasi steganografi yang ada tidaklah sempurna, aplikasi ini hanya bisa untuk menyisipkan pesan dalam media image saja. oleh karena itu perlu dikembangkan agar dapat menyisipkan pesan dalam media lain, seperti audio.

DAFTAR PUSTAKA

[1] A.S. Rosa dan Shalahuddin, *M. Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika Bandung, 2014.
[2] A. S. Ardhayana, dan A. Juarna. *Aplikasi Steganografi pada MP3 Menggunakan Teknik LSB.* Universitas Gunadarma, 2012.
[3] A. Saefullah, Hilmawan dan N. Agani. *Aplikasi Steganografi untuk Menyembunyikan Teks dalam Media Image dengan Menggunakan Metode LSB*. Universitas Budi Luhur, 2012.
[4] EMS, Tim. *Teori dan Praktik PHP-MySQL untuk Pemula*. Jakarta: PT Elex Media Komputindo, 2014.
[5] A. Kadir. *Pemrograman Database MySQL untuk Pemula*. Yogyakarta: MediaKom, 2013.
[6] W. Komputer. *Adobe Dreamweaver CS5 untuk Beragam Desain Website Interaktif.* Yogyakarta: Andi, 2011.
[7] Kamus Kamus Besar Bahasa Indonesia 1998
[8] M. R. Fahlevi. *Aplikasi Steganografi untuk Menjaga Kerahasiaan Informasi menggunakan Bahasa pemrograman JAVA.*. Universitas Budi Luhur, 2014.
[9] R. Munir. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika, Bandung 2004
[10] I. P. B. E. Pratama. *Sistem Informasi dan Implementasinya.* Bandung: Informatika Bandung, 2014.
[11] Wikipedia bahasa indonesia
[12] T. Sutabri. *Konsep Sistem Informasi.* Yogyakarta: Andi, 2012.