Jurnal TAM (Technology Acceptance Model) Volume 8, No 1, Juli 2017 *Hal. 13-17*
p-ISSN : 2339-1103
e-ISSN : 2579-4221

APLIKASI STEGANOGRAFI UNTUK MENYISIPKAN PESAN DALAM MEDIA IMAGE

Nunung Nurmaesah [1)], Tutik Lestari [2)], Arni Retno Mariana [3)]
[1)] *Pascasarjana Magister Komputer, Universitas Budi Luhur*
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
Email : syahmae5@gmail.com[1)], tutiklestari89@gmail.com[2)], arnie.mariana@gmail.com[3)]

ABSTRACT

In the course of employment, the employee is not uncommon to find the problems in the software and hardware used. However, handling the problem by system developers must be done in the initiation and control of the project to be or underway, because recording is still a simple process that affects the performance of the company. This can have a negative impact, ie, there is a risk of problems noted repeatedly, the problem is not an accurate calculation and a long wait to get a report. For the software development process using UML models (The Unified Modeling Language). Done starting from the identification and analysis of problems, requirements analysis, system design, system implementation and testing. PHP and Database Management System (DBMS) MySQL will be used for the preparation of the information system. With the implementation of this application is expected to facilitate the processing of data and generate reports quickly and accurately which can be used for corporate decision-making.

***Keyword**: System Information of Service, System Integration Test, Testing, System*

1. PENDAHULUAN

1.1 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, telepon genggam atau yang kita kenal dengan ponsel terus berkembang hingga menjadi ponsel cerdas yang makin menggeser komunikasi telepon rumah hingga komunikasi secara langsung.

Namun, seiring dengan kemudahan tersebut banyak kejahatan sistem informasi yang sudah mengintai. Banyak orang diluar sana yang mencoba mengakses informasi yang bukan haknya. Keamanan menjadi sangat penting apabila informasi yang dikirimkan merupakan informasi yang bersifat rahasia. Maka dari itulah diperlukan keamanan data.

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.

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.

1.2. Rumusan Masalah

Rumusan masalah dari penelitian adalah:

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

1.3. Ruang Lingkup

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

2. LANDASAN TEORI

2.1. 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.

2.2. Pengertian Steganografi

Steganografi adalah seni dan ilmu menyembunyikan pesan ke dalam sebuah media

p-ISSN : 2339-1103
e-ISSN : 2579-4221

dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa sebenarnya ada suatu pesan rahasia

2.2.1. Kriteria Steganografi

a. *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.

b. *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.

c. *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

2.2.2. Teknik Steganografi

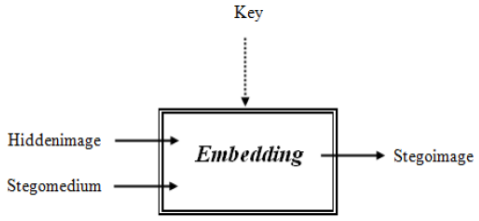
Menurut Ariyus (2009), ada tujuh teknik dasar yang digunakan dalam *steganografi*, yaitu:

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*

2.2.3. Proses Steganografi

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

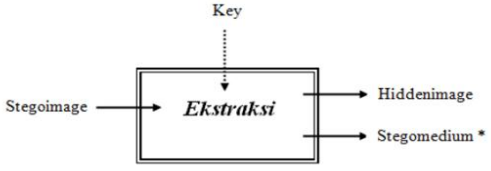
a. *Embedding*, yaitu proses untuk menyembunyikan pesan.



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)

b. *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 s*tegomedium* awal persis sama dengan *stegomedium* setelah dilakukan *ekstraksi*

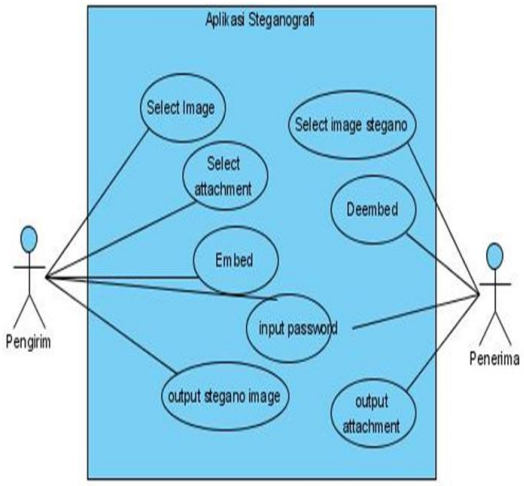
p-ISSN : 2339-1103
e-ISSN : 2579-4221

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)

3. HASIL DAN ANALISA

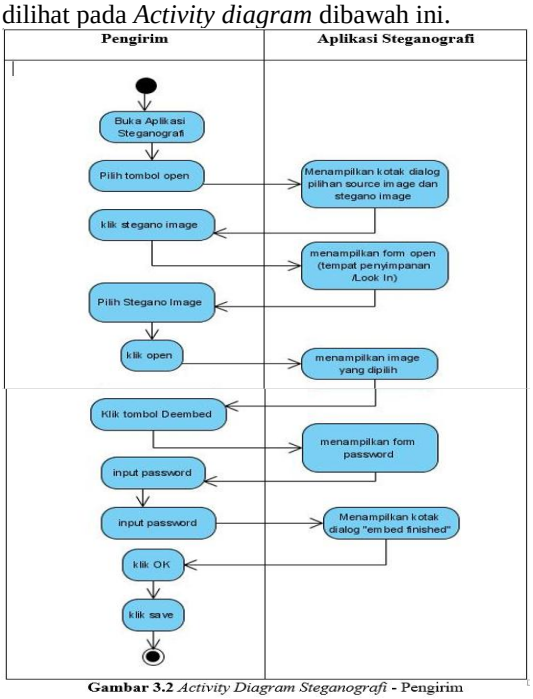
3.1. Hasil

Berdasarkan dari penjelasan diatas berikut merupakan *activity* sistem berjalan saat ini.



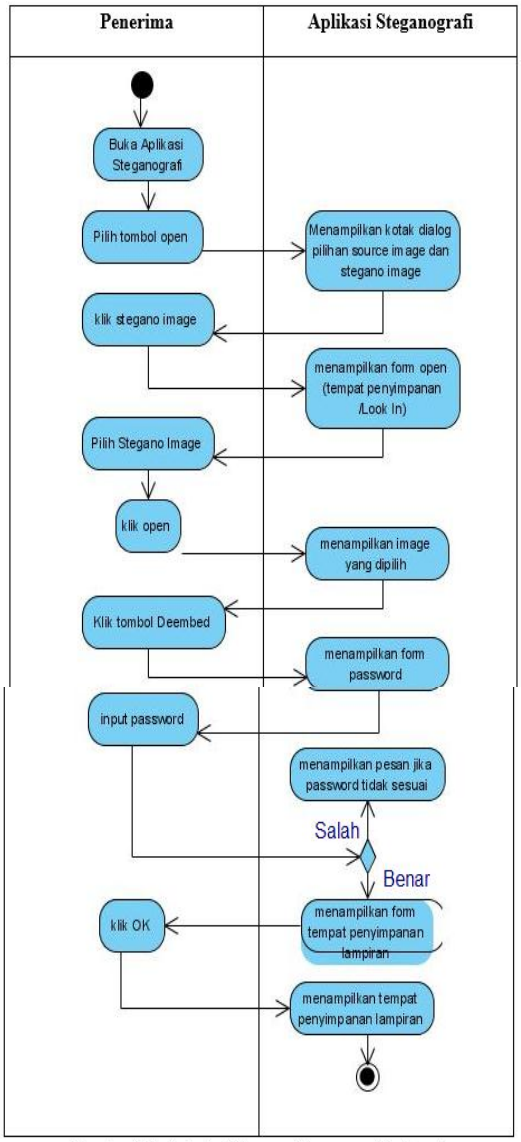
Gambar 3.1 *Use Case Diagram Steganografi*

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

Steganografi - Pengirim

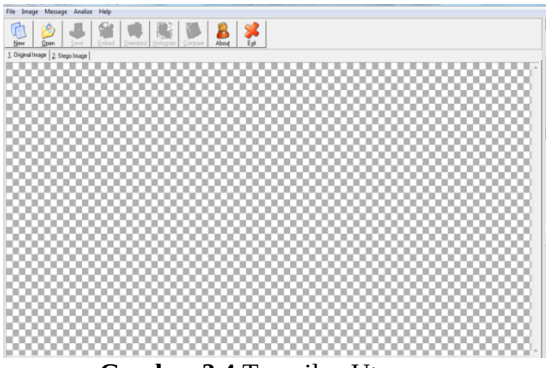


Gambar 3.3 *Activity Diagram Steganografi* - Penerima

Steganografi – Penerima

3.1.1 Aplikasi Steganografi

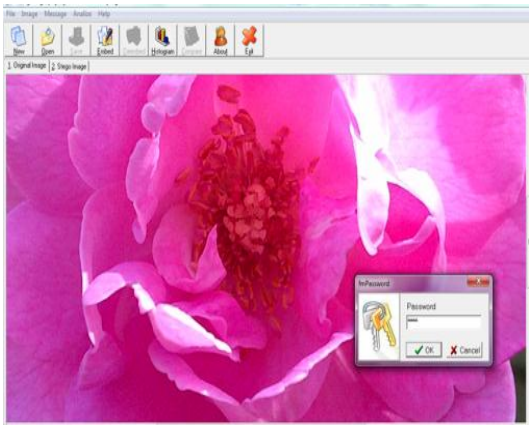
Aplikasi steganografi untuk menyisipkan pesan dalam media *image*, dapat dilihat seperti pada gambar dibawah ini :



Gambar 3.4 Tampilan Utama

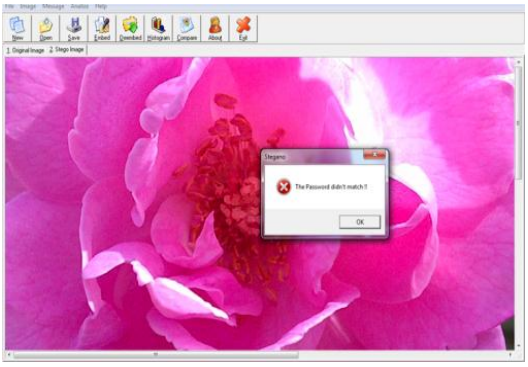
p-ISSN : 2339-1103
e-ISSN : 2579-4221

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

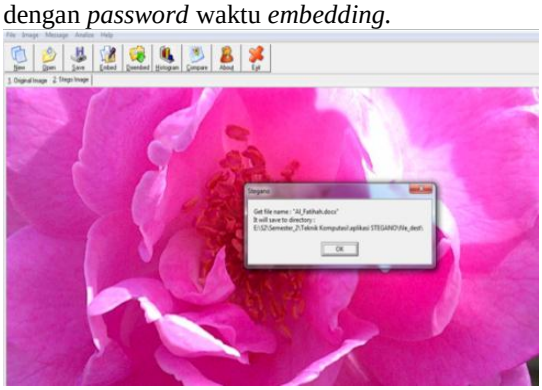
Jika Penerima salah memasukkan *password*, maka akan muncul pesan jika password tidak sesuai. Proses ekstraksi akan gagal, pesan (lampiran) tidak dapat dilihat. Oleh karena itu, *Password* yang diinput haruslah sama dengan *password* waktu *embedding*.



Gambar 3.6 Kotak pesan ketika *Password* salah

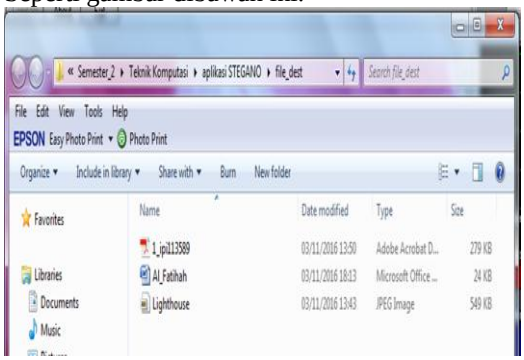
Untuk melakukan *embedding* (menyembunyikan pesan), pengirim(pengguna aplikasi) harus mengklik tab Open, selanjutnya muncul kotak dialog, lalu pilih *source Image* (mencari gambar yang akan disisipi). Pada gambar yang akan disisipi, pengirim perlu menginputkan password. Parsword ini selanjutnya digunakan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

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

3.2 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

p-ISSN : 2339-1103
e-ISSN : 2579-4221

4. PENUTUP

4.1. Kesimpulan

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa:

a. Cara menyisipkan pesan dalam media image dapat menggunakan aplikasi steganografi. Pesan yang disisipkan dapat berbentuk gambar, teks, ppt, pdf, dll.
b. 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.

4.2. 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, dll.

DAFTAR PUSTAKA

[1] A.S, Rosa, Shalahuddin, M. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek.* Bandung: Informatika Bandung, 2014.
[2] Alfebra Stavina Ardhayana, Asep Juarna. *Aplikasi Steganografi pada MP3 Menggunakan Teknik LSB*. Jakarta: Universitas Gunadarma, 2012.
[3] Saefullah, Hilmawan, Agani, Nazori. *Aplikasi Steganografi untuk Menyembunyikan Teks dalam Media Image dengan Menggunakan Metode LSB*. Jakarta: Universitas Budi Luhur, 2012.
[4] EMS, Tim. *Teori dan Praktik PHP-MySQL untuk Pemula*. Jakarta: PT Elex Media Komputindo, 2014.
[5] Kadir, Abdul. *Pemrograman Database MySQL untuk Pemula*. Yogyakarta: MediaKom, 2013.