PERANCANGAN APLIKASI STEGANOGRAFI PADA MEDIA CITRA DIGITAL TERKOMPRESI *JOINT PHOTOGRAPHIC EXPERTS GROUP (JPEG)*

DESIGN OF STEGANOGRAPHY APPLICATIONS IN DIGITAL IMAGE IMAGE MEDIA JOINT PHOTOGRAPHIC EXPERTS GROUP (JPEG)

Marhaeni, Danu Ivan GP
Program Studi Teknik Informatika, Institut Sains dan Teknologi Nasional
marhaenie@gmail.com

Naskah Diterima tanggal 10 Mei 2017 dan naskah di setujui tanggal 18 Juni 2017

ABSTRAKS

Pada saat ini keamanan data merupakan masalah yang sangat penting pada saat sebuah data tersebut merupakan data rahasia dan tidak oleh diketahui oleh orang lain atau pun pihak yang tidak berkepentingan. Maraknya pencurian data-data atau informasi rahasia oleh pihak yang tidak berkepentingan dan rendahnya tingkat keamanan pada saat pertukaran data menjadi masalah yang harus segera diatasi. Untuk mengatasi masalah tersebut membutuhkan teknik pengamanan data. Untuk membantu mengamankan data, teknik steganografi adalah salah satu solusi yang diperlukan. Dari berbagai media steganografi, dalam penelitian ini menggunakan media gambar sebagai wadah penampung pesan rahasia. Steganografi bertujuan untuk menyembunyikan pesan dengan suatu cara sehingga selain sipengirim dan sipenerima tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Pengamanan yang dilakukan dengan membuat pesan tersebut seolah-olah tidak ada padahal pesan tersebut ada. Dengan meningkatnya keamanan data, telah membantu mengurangi dan mempersulit pencurian data-data oleh pihak yang tidak berkepentingan. Dengan penelitian ini, dapat digunakan secara efektif. Penelitian ini dimulai dengan analisis sebelum memilih ekstensi yang digunakan, dan kemudian membuat desain dan pengkodean aplikasi setelah itu pengujian penyisipan *file compress* ke dalam gambar dan pengambilan *file* dari dalam gambar. Dari hasil penelitian menunjukan bahwa menyembunyikan *file* di dalam gambar dapat membantu meningkatkan keamanan data.

Kata Kunci : Ekstraksi, *Joint Photographic Experts Group*, Keamanan Data, Penyisipan File, Steganografi

ABSTRACT

At this time the data security is an issue that is very important when a data is the data confidential and should not be known by others or unauthorized parties.Rampant theft of data or confidential information by unauthorized parties and the low level of security during data exchange becomes a problem that must be addressed immediately.To overcome these problems require data security techniques.To help secure data, steganography techniques is one solution that is needed.From various media of steganography, in this study using media images as a container vessel secret message. Steganography aims to hide a message in a way that besides the sender and the recipient no one knows or realizes that there is a secret message. Security is done by making the message as though nothing when the message is there. With increasing data security, has helped to reduce and complicate the theft of data by unauthorized parties. With this research, can be used effectively. The study began with an analysis before selecting the extensions being used, and then make the design and coding of the application after testing it compress files into image insertion and retrieval of files from within the image. From the results of the study showed that hide files inside images can help increase data security.

Keyywords : *Extraction, Joint Photographic Experts Group, Data Security, File Insertion, Steganography*

1. PENDAHULUAN

Pada saat ini keamanan data merupakan masalah yang sangat penting pada saat sebuah data tersebut merupakan data rahasia dan tidak boleh diketahui oleh orang lain ataupun pihak yang tidak berkepentingan. Data yang ada sebelumnya akan diubah terlebih dahulu kedalam bentuk yang berbeda dari bentuk format aslinya, aman dan tidak dapat dimengerti oleh seseorang, sehingga orang lain yang tidak mempunyai hak atas data tersebut tidak dapat mengetahui isi dari data tersebut. Pengamanan yang dilakukan dengan membuat pesan tersebut seolah-olah tidak ada padahal pesan tersebut ada. Aplikasi Steganografi tercipta karena terinspirasi dari maraknya pencurian data-data atau informasi rahasia oleh pihak yang tidak berkepentingan, selain itu aplikasi ini dibuat dengan alasan untuk meningkatkan keamanan informasi dengan menyembunyikan *file*ke dalam media digital.

Dari uraian latar belakang tersebut, maka masalah yang dihadapi yaitu: Maraknya pencurian data-data atau informasi rahasia oleh pihak yang tidak berkepentingan. Rendahnya tingkat keamanan pada saat pertukaran data. Agar masalah tidak menyimpang dari rumusan masalah, maka perlu batasan masalah. Adapun batasan masalah yaitu sebagai berikut : Format Gambar yang dipakaiadalahformat *Jpeg files* (*.jpg), File yang ingin disisipkan atau disembunyikan harus berbentuk *compress* (*.rar). Hasil *output* hanya bisa di lihat atau *extract* dengan aplikasi WinRAR. Aplikasi ini berjalan hanya pada system operasi*Windows.* Aplikasi ini dibuat dengan *Microsoft Visual Basic* 2010 *Express.* Sebagai tujuan dari proyek tersebut adalah mengamankan data dengan cara menyisipkan data ke dalam media citra digital dengan teknik steganografi, meningkatkan keamanan data.

Manfaat dari penilitian yang dilakukan adalah dapat menyisipkan pesan rahasia ke dalam media citra jpeg, dapat mengamankan pesan rahasia sehingga aman dari orang-orang yang tidak berkepentingan yang berusaha untuk mengetahui atau pun merusak pesan ataupun data rahasia, dapat digunakan sebagai salah satu program operasional untuk peningkatan efisiensi keamanan penyimpanan maupun pengiriman data.

Steganografi

Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan cara tertentu sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Istilah steganografi *(steganography)* berasal dari bahasa Yunani, yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein yang berarti tulisan. Jadi steganografi *(steganography)* bisa diartikan sebagai seni menyamarkan / menyembunyikan pesan tertulis ke dalam pesan lainnya.[3]

Kriteria Steganografi Yang Baik

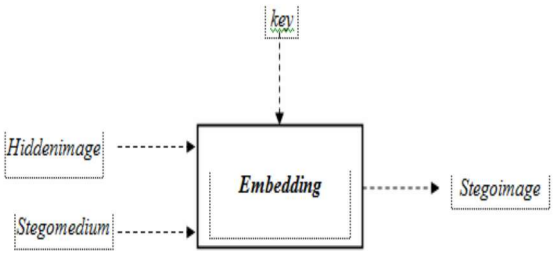
Beberapa kriteria yang harus diperhatikan dalam steganografi[3], yaitu *Imperceptibility*. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika *cover text* berupa citra, maka penyisipan pesan membuat citra *stegotext* sulit dibedakan oleh mata dengan citra *cover text*-nya. Jika *cover text* berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio *stegotext*-nya.

Fidelity. Mutu *stegomedium* tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat di persepsi oleh inderawi. Misalnya, jika cover text berupa citra, maka penyisipan pesan membuat citra *stegotext* sulit dibedakan oleh mata dengan citra *cover text*-nya. Jika *cover text* berupa audio, maka *audio stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.

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

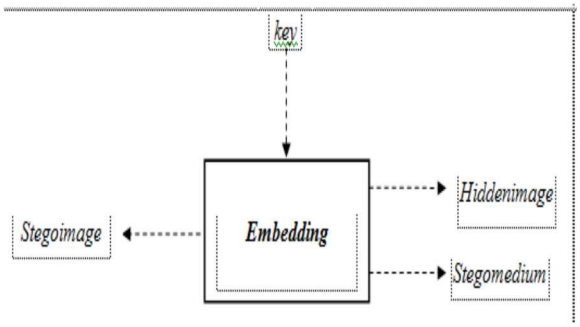
Proses Steganografi

Secara umum, terdapat dua proses di dalam steganografi, yaitu proses *embedding* untuk menyembunyikan pesan dan ekstraksi untuk mengekstraksi pesan yang disembunyikan[4]. Proses-proses tersebut dapat dilihat pada Gambar 1.



Gambar 1. Embedding

Gambar 1 adalah proses *embedding*, yakni proses penyembunyian pesan dimana pada bagian pertama dilakukan proses *embeddinghiddenimage* yang hendak disembunyikan ke dalam *stegomedium* sebagai media penyimpanan, dengan memasukkan kunci (*key*), sehingga dihasilkan media dengan data tersembunyi di dalamnya (*stegoimage*).[7]



Gambar 2. Ekstraksi Gambar

Gambar 2 menunjukkan proses ekstraksi pada *stegoimage* dengan memasukkan *key* yang sama sehingga didapatkan kembali *hiddenimage*.[7] Dalam 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[4].

Teknik Steganografi

Menurut Ariyus, ada tujuh teknik dasar yang digunakan dalam steganografi[5], yaitu :

- *Injection*, merupakan 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*.
- *Substitusi*, data normal digantikan dengan data rahasia. Hasil dari teknik ini tidak mengubah ukuran data asli, tetapi tergantung pada *file* media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
- *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.
- *Spread Spectrum*, merupakan teknik pentransmisian menggunakan *pseudo-noise code*, 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 dan menggunakan replika *pseudo-noise code* tersinkronisasi.
- *Statistical Method*, teknik ini disebut juga skema *steganographic* 1-bit 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 mempunyai kemampuan penerima dalam membedakan antara informasi yang dimodifikasi.
- *Distortion*, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
- *Cover Generation*, metode ini lebih unik daripada metode lainnya karena *cover object* dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah *Spam Mimic*

2. METODOLOGI PENELITIAN

Perancangan Umum

Aplikasi yang akan dibangun bertujuan untuk membantu meningkatkan keamanan data dalamsebuah proses pertukaraninformasi. Jika pertukaran informasi apalagi sebuah data penting tanpa adanya sebuah keamanan yang lebih akan mempermudah pihak yang tidak berkepentingan untuk mengetahui atau mencuri sebuah informasi dari data tersebut. Sehingga tujuan dari aplikasi ini adalah untuk menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.

Analisa Sistem

Pada tahapan analisis system bertujuan menganalisa semua kebutuhan sistem yang akan dibangun, dalam hal ini ialah tentang Perancangan Aplikasi Steganografi Pada Media Citra Digital Terkompresi *Joint Photographic Expert Group* (JPEG).

Analisa Sumber Daya

Dalam analisa sumber daya ini berisi mengenai sumber daya – sumber daya yang dibutuhkan untuk merancangAplikasi Steganografi Pada Media Citra Digital Terkompresi *Joint Photographic Expert Group* (JPEG).

Analisa Perangkat Keras

Perangkat keras menggunakan notebook dengan spesifikasi sebagai berikut :

- *Processor* Intel Celeron *Dual-Core* CPU T3100 1.9 GHz
- Memori RAM 1 GB
- *Hard Drive* 250 GB
- *Optical Drive* DVD-RW
- LCD 14.1” dengan resolusi 1280 x 800 pixel

Analisa Perangkat Lunak

- Sistem Operasi *Windows* XP
- *Microsoft Visual Basic* 2010 *Express*
- WinRaR
- Dummy Data

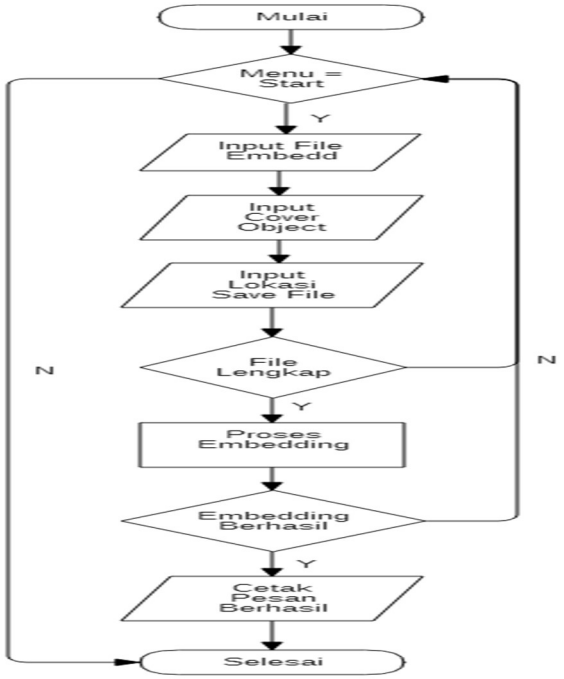
Analisa Media

- *File* Gambar *.jpg
- *File* Pesan *.rar

Perancangan Aplikasi Steganografi

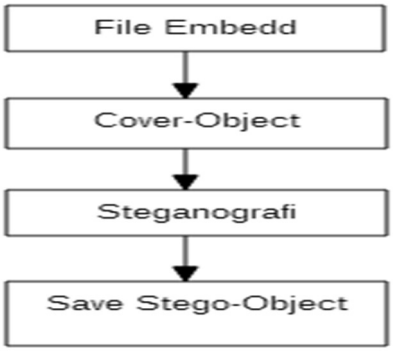
Untuk merealisasikan hasil dari gagasan yang didasari pada teori yang dikaji sehingga menghasilkan suatu rancangan yang dapat membantu dalam membuat aplikasi pembelajaran sehingga menghasilkan aplikasi pembelajaran yang menyenangkan dan memiliki fungsi, yaitu sebuah aplikasi yang mudah untuk dipelajari dan efisien dalam penggunaannya.

Perancangan Proses



Gambar 3. Diagram alir

Tahap perancangan proses dilakukan untuk perancangan, evaluasi dan memperbaiki sistem sesuai dengan kebutuhan, agar sistem yang sedang di buat dapat dimanfaatkan secara optimal. Pada penyembunyian pesan, pesan dapat di ambil/ *copy* yang berupa *file*yang telah di *compress* ke dalam bentuk Rar Files (*.rar).Kemudian disisipkan ke media penampungnya. Sehingga menghasilkan *stego-object* berupa *file* *.jpg yang telah disisipi pesan.Untuk memperjelas gambaran proses penyembunyian pesan dapat dilihat pada Gambar 4.



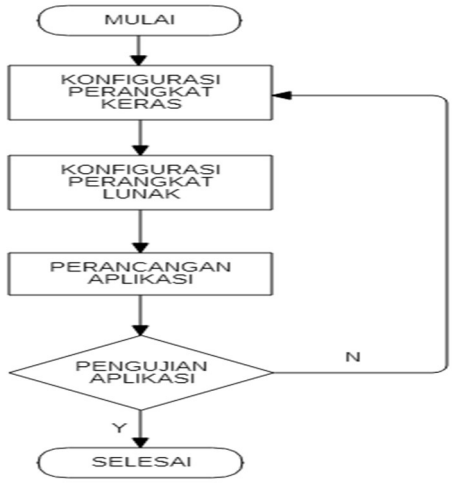
Gambar 4. Proses Penyisipan Pesan

Perancangan Sistem

Adapun perancangan sebuah Aplikasi ini diperlukan sebuah rancangan yang terstruktur dengan baik. Untuk mempermudah proses perancangan pengimplementasian diperlukan *flowchart* yang membantu dalam memahami proses perancangan yang akan dibuat.

Perancangan Antarmuka

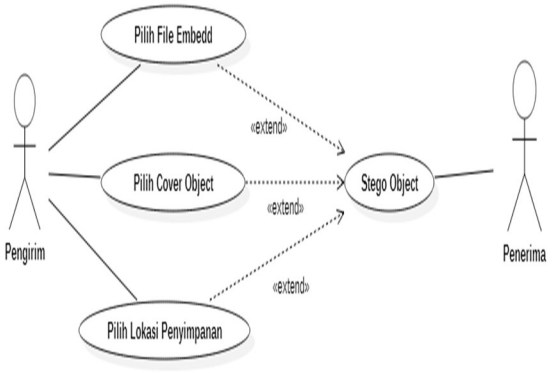
Pada tahap perancangan antarmuka sistem yang akan dibuat menggunakan *flowchart* dan *usecase* yang akan menjelaskan berupa penggambaran dari suatu aktifitas antarmuka sistem yang dibuat. Alur proses penyisipan pesan rahasia seperti Gambar 5.



Gambar 5. Proses Penyisipan Pesan Rahasia

Gambar 5 menjelaskan informasi apa saja yang harus di*input* untuk memulaiproses penyisipan pesan rahasia. Informasi yang di*input* haruslah lengkap,apabila tidak lengkap maka akan terjadi *error* pada saat proses *embedding*.

Setelah semua informasi terisi lengkap, program akan menjalankan proses penyisipan pesan pada*File image*. Setelah semua proses selesai makaterbentuklah *file* *.jpg yang telah disisipkan pesan rahasia.



Gambar 6. *Use Case* Diagram

Skenario *use case* pada Gambar 6 dapat dideskripsikan sebagai berikut:

- ***Actor***

Tabel 1. Definisi *Actor*

No	*Actor*	Deskripsi
1.	Pengirim	Orangyang menggunakan perangkat lunak untuk menyisipkan *file* rahasia lalu mengirimkan stego *object* kepada penerima.
2.	Penerima	Orang yang menerima pesan rahasia dan mengerti cara ekstraksi *file* tersebut.

- ***Use Case***

Tabel 2. Definisi *Use Case*

No	*Use Case*	Keterangan	
1.	Pilih *File Emmbed*	Deskripsi	Memungkinkan *user* untuk memilih *file* yang akan disisipkan pada citra digital.
		Pre kondisi	*User* sudah menjalankan perangkat lunak.
		Proses	*User* terlebih dahulu memilih *file* yang diinginkan.
		Kondisi Akhir	Perangkat lunak akan menampilkan *file* yang akan di-*embedding.*
2.		Deskripsi	Memungkinkan *user* untuk memilih media

	Pilih *Cover Object*		citra yang akan di-*emmbedding*.
		Prekondisi	*User* sudah menjalankan perangkat lunak.
		Proses	*User* terlebih dahulu memilih media citra digital.
		Kondisi Akhir	Perangkat lunak akan menampilkan citra digital yang akan di-*embedding*.
3.	Pilih Lokasi Penyimpanan	Deskripsi	Memungkinkan *user* memilih tempat untuk menyimpan hasil dari proses *embedding*.
		Prekondisi	*User* sudah menjalankan perangkat lunak.
		Proses	*User* terlebih dahulu memilih lokasi penyimpanan *file* hasil *embedding*.
		Kondisi Akhir	Perangkat lunak akan menampilkan lokasi penyimpanan untuk hasil *embedding*.
4.	Stego *Object*	Deskripsi	Hasil dari proses *embedding*.
		Prekondisi	*User* sudah menjalankan perangkat lunak.
		Proses	*User* telah memilih *fileembed , cover object* dan lokasi penyimpanan.
		Kondisi Akhir	Perangkat lunak akan menampilkan hasil dari proses *embedding*.

3. HASIL DAN PEMBAHASAN

Implementasi

Implementasi merupakan tahap dimana program aplikasi siap dioperasikan pada keadaan yang sebenarnya sehingga dari sini akan mengetahui apakah program aplikasi benar-benar dapat menghasilkan hasil yang sesuai dengan tujuan yang diinginkan.

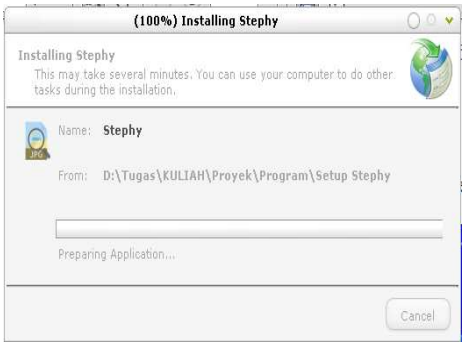
Instalasi Aplikasi

Sebelum menggunakan aplikasi pada proyek ini, perlu dilakukan instalasi terlebih dahulu agar aplikasi berjalan dengan baik. Adapun cara untuk melakukan instalasi aplikasi pada proyek ini, yaitu :

Klik pada folder Setup Stephy, maka akan tampil seperti pada Gambar 7.

Gambar 7. Instalasi Stephy

Selanjutnya klik tombol "*Install*" pada Gambar 7, setelah itu akan tampil proses instalasi seperti yang terlihat pada Gambar 8.

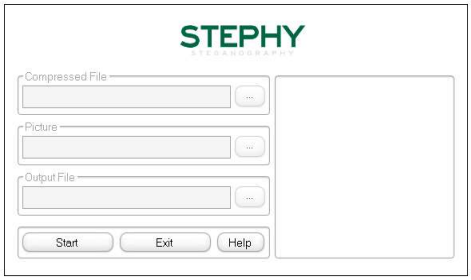


Gambar 8. *Loading* Instalasi Steph

Setelah proses instalasi selesai , maka setelah itu program aplikasi siap untuk digunakan

Tampilan Program

Setelah selesai melakukan proses instalasi program. Tampilan dari program aplikasi yang telah selesai di instal maka akan seperti terlihat pada Gambar 9.



Gambar 9. Tampilan Utama

Pada awal tampilan utama terdapat 3 tombol yang aktif yaitu tombol "*Start*" untuk memulai penyisipan file , tombol "*Exit*" untuk keluar

dari aplikasi dan tombol "*Help"* untuk memberikan petunjuk cara penggunaan aplikasi dan proses ekstraksi *file.* Untuk mengetahui cara ekstraksi *file* yaitu dengan klik tombol "*Help*" dan bisa juga untuk mengetahui cara penggunaan aplikasi, Maka tampilan setelah mengklik tombol "*Help"* adalah seperti pada Gambar 9.

Gambar 10. Tampilan *Help*

Pada Gambar 10 terdapat dua pilihan yaitu "*How to use"* yaitu untuk mengetahui bagaimana cara penggunaan aplikasidan *"How to extract"* untuk mengetahui bagaimana cara untuk ekstrak *file* hasil proses penyisipan.

Gambar 11. Tampilan *How to extract*

Pada Gambar 11 terdapat tombol "OK" yaitu untuk kembali ke menu utama.

Penyisipan *File*

Jalankan aplikasi Stephy dengan cara *double* klik Stephy.exe yang ada di desktop. Sebagai contoh *file* yang akan disisipkan adalah *file* Do.rar yang berisi *file* arsip.docx dengan *file* gambar STEPHY*black*.jpg. Klik tombol *Start* lalu klik tombol *browse (...)* di kotak *Compressed File,* kemudian pilih *file* Do.rar. Setelah memasukan *file* ke dalam kotak *Compressed File* maka kotak *Picture* akan aktif dan kotak *Compressed File* menjadi tidak aktif. Kemudian klik tombol *browse* (…) di kotak *Picture* lalu pilih *file* gambar STEPHY*black*.png. Setelah memasukan gambar ke dalam kotak *Picture* maka gambar akan tampil didalam kotak seperti terlihat pada Gambar 4.12 dan kotak *Output File* akan aktif dan kotak *Picture* menjadi tidak aktif. Kemudian klik tombol *browse* (…) di kotak *Output File* lalu ketik *file name* dengan nama Hasilstephy dan pilih lokasi direktori untuk menyimpan hasil penyisipan *file* nanti setelah proses penyisipan berhasil. Setelah selesai memberi nama dan memilih lokasi penyimpanan *file,* Kemudian kotak *Output File* akan menjadi tidak aktif dan tombol *Build* aktif. Klik tombol *Build* dan jika proses penyisipan berhasil maka akan tampil pesan "*Emmbeding file successfully".* Setelah penyisipan *file*berhasil dilakukan , isi dari *file* Do.rar akan berada didalam *file* gambar STEPHY*black*.jpg. Berikut ini adalah tampilan perbandingan gambar atau media citra sebelum dan sesudah disisipkan *file* : Dari hasil proses penyisipan *file* diperoleh data gambar sebelum dan sesudah disisipkan *file* seperti terlihat pada Tabel 3.

Tabel 3. Data Gambar hasil Penyisihan

Nama Gambar	Dimensi Gambar	Ukuran Gambar
STEPHY*black*.jpg	550 x 400	23.4 KB
Hasilstephy.jpg	550 x 400	33.2 KB

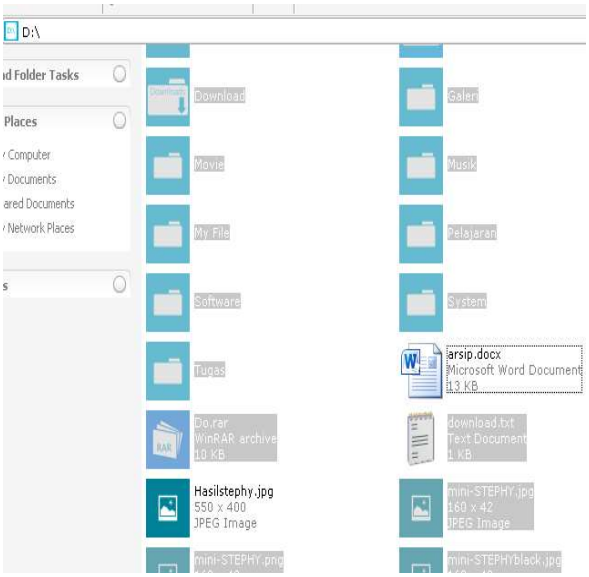
Ekstraksi *File*

Klik kanan pada *file* hasil penyisipan yaitu *file* Hasilstephy.jpg pilih *open with* lalu pilih *Choose Program.*

Setelah itu akan tampil *Open With* lalu pilih WinRaR *Archiver*. Karena *file* Do.rar menggunakan *password* maka akan keluar tampilan *Enter password* seperti pada gambar 12, jika tidak menggunakan *password* maka langsung muncul tampilan seperti pada Gambar 12.

Gambar 12. Enter password

Lalu masukan *password* ":dong". Klik *Extract to* untuk mengeluarkan *file* rahasia dari gambar lalu pilih lokasi untuk ekstraksi. Setelah itu akan muncul *file* arsip.docx di lokasi yang telah ditentukan.



Gambar 13. Hasil Ekstraksi

4. SIMPULAN

Dari hasil implementasi dan hasil pengujian yang dilakukan, maka dapat diambil kesimpulan sebagai berikut : Menyembunyikan *file* di dalamgambar dapat membantu meningkatkan keamanan data. Aplikasi Stephy berhasil mengimplementasikan teknik steganografi dalam mengamankan data. Hal ini dibuktikan melalui pengujian penyisipan dan pengekstraksian bahwa *file* dapat disisipkan ke dalam *file* gambar dan dapat diambil kembali dari *file* gambar tersebut. Pada proses penyisipan pesan membutuhkan dua buah properti pendukung yaitu gambar sebagai media penampung *file* dan juga *file* rahasia yang akan disisipkan sedangkan untuk proses ekstraksi hanya membutuhkan *filestegoimage*. Berdasarkan hasil pengujian dapat dinyatakan bahwa *file* sebelum disisipkan dengan *file* setelah diekstraksi memiliki jumlah *byte* yang sama, dimana artinya penyisipan *file* tidak mempengaruhi besar ukuran *file* awal maupun akhir. Berdasarkan hasil pengujian dapat dinyatakan bahwa ukuran *file* gambar setelah disisipkan *file* menjadi lebih besar namun tidak merubah isi ataupun kualitas gambar.

UCAPAN TERIMA KASIH

Ucapan terima kepada prodi Teknik Informatika Fakultas Sains dan Teknologi Informasi

DAFTAR PUSTAKA

Rahman, Angga Syamditia. 2015. *Perancangan Perangkat Lunak Steganography Menggunakan Algoritma Jsteg.* Medan: STMIK Budidarma.

Hariyanto, Bambang. 2004. *Rekayasa Sistem Berorientasi Objek.* Bandung : Informatika.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika.

Sejati, Adiputra. 2010.*Studi dan Perbandingan Steganografi Metode EOF (End of File) dengan DCS (Dynamic Cell Spreading)*. Institut Teknologi Bandung.

Bandung.Ariyus, Dony. 2009. *Keamanan Multimedia*. Yogyakarta : Andi.

Nazelliana, Dian dan Ambar Tri Hapsari. 2015. *Implementasi Penyisipan Pesan File Ke Dalam Gambar Dengan Algoritma Huffman.* Universitas Budi Luhur.

Munir, Rinaldi. 2006. *Metode Komunikasi Untuk Menyembunyikan Pesan Rahasia*. Bandung : Informatika