IMPLEMENTASI TEKNIK STEGANOGRAFI SEBAGAI ANTI FORENSIK PENYISIPAN TEKS PADA CITRA

Eri Haryanto

Program Studi Teknik Informatika, Fakultas Teknik, Universitas Janabadra
Jalan Tentara Rakyat Mataram 55-57 Yogyakarta 55231, Telp/Fax. (0274) 543676
E-Mail : eri@janabadra.ac.id

ABSTRACT

In the world of data and information security, there are two techniques that can be used to secure data and information, namely cryptography and steganography. In this study developed applications for the implementation of steganography techniques. Application of steganography by inserting a text message into a medium image or image file. Steganography applications created in this web-based research so that users simply access the application's domain address to encode and decode text messages.

***Keyword* :** *steganografi, security, anti forensics*

PENDAHULUAN

Keamanan data dan informasi saat ini merupakan sebuah hal yang menjadi prioritas bagi pemilik informasi tersebut. Informasi yang memiliki tingkat sensitivitas yang tinggi juga membutuhkan teknik pengamanan yang tinggi. Media internet saat ini merupakan media transmisi paling banyak digunakan dalam melakukan pengiriman dan transaksi informasi.

Internet memberikan kenyamanan dan kemudahan dalam media komunikasi. Dengan internet komunikasi menjadi mudah karena dapat dilakukan dari berbagai tempat, dimanapun, dan kapanpun kita berada. Akan tetapi komunikasi jarak jauh menggunakan media internet memiliki resiko yang besar dalam pentransmisian informasi khususnya kaitannya dengan keamanan informasi yang dikirimkan. Informasi dapat dilakukan penyadapan, pengambilan secara tidak legal, perubahan isi dari informasi, dan resiko yang lainnya.

Dalam dunia keamanan data dan informasi, ada dua teknik yang dapat digunakan untuk mengamankan data dan informasi tersebut, yaitu kriptografi dan steganografi. Masing-masing memiliki kelebihan dan kemampuan yang dapat diandalkan untuk dapat menjaga integritas dari informasi yang akan disampaikan.

Kriptografi merupakan teknik dalam keamanan data yang akan melakukan pengacakan informasi yang dikirim menggunakan algoritma tertentu, sehingga informasi tersebut tidak akan dapat terbaca oleh pihak lain yang tidak memiliki wewenang. Sedangkan steganografi merupakan teknik dan seni dalam penyembunyian data dan informasi digital yang data tersebut akan disisipkan ke dalam data digital yang lainnya, sehingga orang lain tidak akan pernah bisa membaca dan menyangka adanya informasi di dalamnya.

Steganografi telah ada sejak jaman Yunani kuno, yang pada masa itu pesan rahasia akan dituliskan pada kepala orang yang menjadi pengirim pesan, dan orang tersebut akan dikirimkan ketika rambut kepalanya telah tumbuh panjang. Pada masa itu penyembunyian informasi sudah sedemikian rahasianya sehingga pihak lain yang tidak mengetahui teknik tersebut tidak akan menyadari adanya pesan yang dikirimkan.

Penerapan steganografi saat ini yaitu dengan menyisipkan pesan berupa teks ke dalam sebuah media *image*. Media gambar atau *image* banyak dipakai dikarenakan gambar menjadi sebuah objek digital yang paling sulit dibedakan antara gambar asli yang tanpa penyisipan teks dengan gambar yang telah disisipkan teks berupa pesan rahasia. Oleh karena itu gambar atau *image* dianggap merupakan media yang paling ideal dalam penerapan teknik steganografi.

Untuk membatasi ruang lingkup pada penelitian ini maka diberikan batasan masalah, diantaranya adalah sebagai berikut :

1. Teknik penyisipan informasi menggunakan steganografi.
2. Informasi yang disisipkan berupa teks yang berbentuk *plaintext* yang disisipkan ke dalam citra berbentuk *image*.
3. Bahasa pemrograman yang digunakan dalam pengembangan aplikasi steganografi adalah bahasa pemrograman PHP.

Tujuan dari penelitian ini adalah untuk mengembangkan aplikasi penyisipan pesan teks ke dalam media *image* sehingga pesan atau informasi yang akan disampaikan dapat dijaga kerahasiaanya dari mulai dikirim hingga diterima oleh yang pihak yang memiliki wewenang. Penelitian ini diharapkan dapat mengamankan informasi yang dikirim dari tindakan forensik yang bisa dilakukan secara tidak *legal*.

Steganografi

Istilah steganografi berasal dari Yunani, berasal dari kata *Steganos* yang berarti penyembunyian dan *Graphien* yang berarti tulisan. (Ben Le, 2002). Menurut Rinaldi Munir (2004) steganografi (*steganography)* adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak diketahui dan terdeteksi oleh indera manusia. Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan.

Pada jaman Yunani kuno steganografi sudah dikenal dan diterapkan, mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit yang telah dibotaki sebagai media. Pesan rahasia akan ditulis pada kulit kepala budak atau prajurit, ketika rambut sudah tumbuh maka akan diutus untuk menyampaikan pesan rahasia di balik rambutnya. Bangsa romawi mengenal steganografi dengan menggunakan tinta tidak tampak *(invisible ink)* untuk menuliskan pesan. Tinta digunakan untuk menulis dan tidak akan tampak secara kasat mata. Tulisan di atas kertas hanya akan terbaca dengan cara memanaskan kertas tersebut.

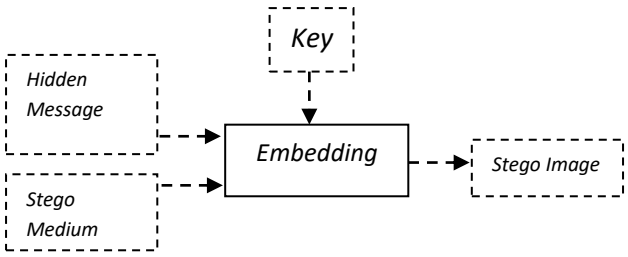
Steganografi dapat menjadi kelanjutan dari disiplin ilmu kriptografi. Dalam ilmu kriptografi data atau pesan telah yang disandikan (*ciphertext)* tetap dapat terbaca, tetapi dalam ilmu steganografi pesan berupa *ciphertext* dapat disembunyikan sehingga tidak akan terlihat.

Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra (gambar), suara, teks, dan video. Sedangkan data rahasia yang disembunyikan dapat berupa berkas apapun. Media yang telah disisipi data disebut *stego message* atau *image*. Proses penyembunyian data ke dalam media disebut penyisipan (*encoding*), sedangkan proses sebaliknya disebut ekstraksi (*decoding)*. Penambahan kunci yang bersifat opsional dapat dilakukan dimaksudkan untuk lebih meningkatkan keamanan data.

Dalam beberapa negara yang menerapkan kebijakan penyensoran informasi, teknik steganografi banyak digunakan dan pesan sering disembunyikan melalui media gambar *(image),* video, atau suara *(audio).* Dalam penggunaan secara *legal* steganografi dapat menjadi teknik ideal untuk melindungi informasi yang bersifat privasi dan sensitif. Tetapi sebagai implikasinya steganografi sering juga digunakan untuk media transaksi informasi tindak kejahatan.

Proses Steganografi

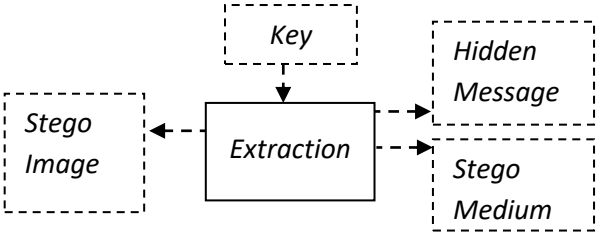
Pada umumnya teknik steganografi memiliki dua proses di dalamnya, yaitu proses *Embedding* atau *Encoding* (menyembunyikan pesan rahasia) dan *Extraction* atau *Decoding* (mengekstrasi pesan yang disembunyikan). Proses *embedding* dan *extraction* pada teknik kriptografi disebut enkripsi dan deskripsi.



Gambar 1. *Embedding* Gambar

Gambar di atas merupakan proses *embedding* pesan ke dalam media *image* dengan ditambahkan kunci untuk pengamanan data. Proses diawali dari penanaman pesan rahasia ke dalam file gambar dengan

ditambahkan kunci sebagai pengamannya, setelah itu file gambar hasilnya akan terbuat. Secara kasat mata file gambar sebelum disisipkan pesan dengan file gambar yang sudah disisipkan tidak akan terlihat.



Gambar 2. Ekstraksi Gambar

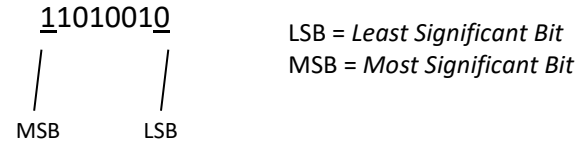
Pada gambar tersebut menunjukkan proses ekstraksi pada *image* hasil steganografi dengan memasukkan kunci yang sama sehingga didapatkan kembali pesan tersembunyi. Dapat dilihat bahwa *embedding* merupakan proses membungkus pesan, dan *extraction* adalah proses mengeluarkan pesan yang terbungkus untuk dapat dibaca.

Metode Steganografi

Penyembunyian data dengan steganografi dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode modifikasi LSB *(Least Significant Bit Modification).*

Metode yang digunakan untuk penyembunyian pesan rahasia pada metode ini adalah dengan cara menyisipkan pesan ke dalam bit rendah (*least significant bit*) pada data *pixel* yang menyusun file gambar *(image)* yang digunakan sebagai media penampung.

Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Berikut susunan bit pada sebuah byte: 11010010



Gambar 3. Posisi MSB dan LSB dalam 1 byte

PHP

PHP yaitu bahasa pemrograman web *server-side* yang bersifat *open source*. PHP merupakan *script* yang menyatu dengan HTML dan berada pada *server*. PHP adalah *script* yang digunakan untuk membuat halaman web yang dinamis. Dinamis berarti halaman yang akan ditampilkan dibuat saat halaman itu diminta oleh *client*. Mekanisme ini menyebabkan infromasi yang diterima *client* selalu yang terbaru (*up-to-date*).

Meskipun PHP secara khusus merupakan bahasa pemrograman untuk pembuatan aplikasi berbasis website, bahasa pemrograman PHP karena sifatnya yang fleksibel dapat digunakan dalam pengembangan aplikasi yang lebih luas lagi, termasuk untuk pembuatan aplikasi tool untuk keamanan data dan informasi.

Digital Forensik

Menurut Palmer (2001) Digital Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan, validasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital (berupa file) yang berasal dari sumber-sumber digital yang bertujuan melakukan rekonstruksi peristiwa dari kejadian kejahatan atau pidana, atau membantu antisipasi tindakan yang tidak sah, proses digital forensik akan dilakukan ketika dibutuhkan data-data yang perlu ditelusuri dari suatu sistem komputer.

Menurut Casey (2014) digital forensik adalah karakteristik bukti yang mempunyai kesesuaian dalam mendukung pembuktian fakta dan mengungkap kejadian berdasarkan bukti statistik yang meyakinkan.

Jadi dapat disimpulkan bahwa digital forensik adalah penggunaan teknik atau prosedur dalam langkah pengumpulan barang bukti digital yang meliputi tahap pemeliharaan, identifikasi, pengambilan, dokumentasi, dan pembuatan laporan terhadap barang bukti digital dalam sebuah kasus kejahatan untuk dapat dipresentasikan di pengadilan dan berfungsi sebagai penegakan hukum. Bukti digital tersebut berupa file dalam komputer yang memilki spesifikasi dan kesesuaian dengan apa yang dicari. Digital forensik akan menjadi *legal* ketika mengikuti tata cara dan prosedur yang berlaku, tanpa

mengikuti prosedur kegiatan digital forensik dianggap tidak sah dan *ilegal.*

Anti Forensik

Menurut Liu dan Brown (2006) anti forensik adalah "*Applicaton of the scientific method to digital media in order to invalidate factual information for judicial review*". Jika digital forensik menitik beratkan kepada tindakan pencarian, pemeliharaan, identifikasi, pengambilan, dokumentasi, dan pembuatan laporan maka anti forensik merupakan kebalikannya. Anti forensik bertujuan untuk menjaga data tetap aman sehingga tidak dapat dibuka bahkan dibaca oleh pihak lain kecuali pemilik data dan informasi tersebut.

Tujuan anti forensik adalah untuk menggagalkan tindakan investigasi dan segala tindakan penelusuran data pada perangkat elektronik. Pada dasarnya tujuan dari anti forensik adalah:

- Membuat agar data digital tidak dapat ditemukan dan diakses, misalnya dengan cara menyembunyikan, memberikan sandi, melakukan enkripsi, menghapus, merubah integritas data.
- Melakukan usaha untuk menjadikan bukti digital tidak layak dengan standar hukum, karena adanya pengubahan integritas data yang ditemukan.

Kegiatan anti forensik dapat memperlama pekerjaan investigator karena tingkat kesulitan yang harus dihadapi oleh investigator digital forensik.

METODE PENELITIAN

Dalam penelitian ini menggunakan beberapa metode diantaranya sebagai berikut:

1. Studi Pustaka, digunakan sebagai sumber teori dan landasan dalam penelitian, serta sebagai acuan dalam penyusunan laporan penelitian.
2. Metode Analisis dan Perancangan, digunakan untuk membuat rancangan sistem yang digunakan sebagai objek penelitian yang dilakukan sampai pada hasil penelitian yang diharapkan. Metode pengembangan aplikasi yang digunakan pada penelitian ini adalah *Waterfall* yang meliputi tahap *requirement analysis, system design, implementation, integration & testing, operations & maintenance (*Pressman, 2005*).*

HASIL DAN PEMBAHASAN

Kebutuhan Sistem

Analisis kebutuhan sistem adalah penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya, dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan. Dalam merancang aplikasi steganografi ini diperlukan beberapa analisis yang terdiri atas analisis kebutuhan perangkat keras (*hardware*), analisis kebutuhan perangkat lunak (*software*), dan analisis fungsional agar aplikasi yang dibuat dapat berjalan seperti dengan tujuan yang telah dirancang.

Analisis Kebutuhan Perangkat Keras (*Hardware)*

Perangkat keras adalah komponen utama dalam sebuah sistem komputer. Perangkat keras yang digunakan untuk membuat dan melakukan uji coba aplikasi steganografi ini adalah perangkat keras satu unit komputer dengan spesifikasi *minimum* sebagai berikut:

- Prosesor Intel Pentium Dual Core
- RAM (*Random Access Memory*) 2 GB
- VGA (*Video Graphic Adapter*) dengan driver standar
- Masukan berupa *mouse* dan *keyboard*
- Keluaran berupa layar *monitor*
- Media penyimpanan *hardisk* dengan kapasitas 80 GB

Analisis Kebutuhan Perangkat Lunak (*Software)*

Selain perangkat keras, sisi perangkat lunak juga salah satu faktor yang dibutuhkan dalam pembuatan aplikasi. Perangkat lunak yang digunakan adalah:

- Sistem Operasi Microsoft Windows 7 Ultimate
- XAMPP web server versi 3.2.1
- *Editor* Notepad++
- Aplikasi *browser* Mozilla Firefox dan Google Chrome

Kebutuhan Fungsional

Aplikasi ini diharapkan dapat memenuhi kebutuhan fungsional untuk

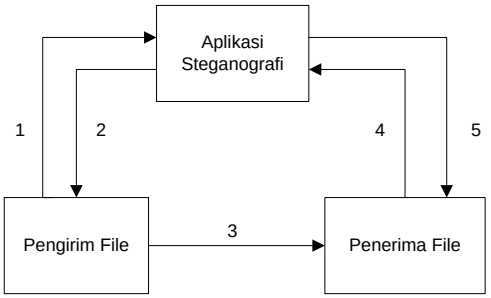
melakukan fungsi penyembunyian data dengan teknik steganografi, antara lain:

- Dapat memberikan kemudahan kepada pengguna dalam menggunakan aplikasi steganografi.
- Dapat meningkatkan keamanan data dengan cara menyisipkan informasi pada media gambar melalui aplikasi steganografi yang dibuat.

Perancangan Sistem

Blok Diagram

Blok diagram sistem yang dibangun dapat dilihat pada gambar di bawah ini. Pada blok diagram terlihat komponen-komponen yang ada di sistem dan alur *input output* sistem.



Gambar 4. Blok Diagram Aplikasi

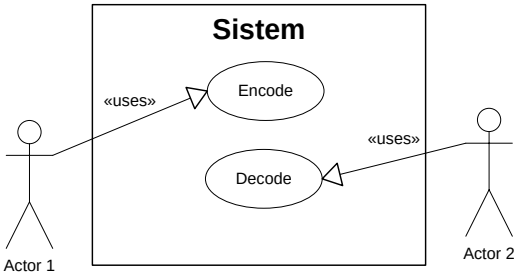
Antara blok pengirim file dengan penerima file tidak akan pernah dikirimkan file dalam bentuk *plaintext (*terbuka). File berupa pesan dan data rahasia akan dikirimkan dari pengirim file menuju penerima file dalam bentuk *stego image* yang merupakan merger dari gambar dan pesan teks.

Pengirim file akan melakukan konversi pesan teks asli yang telah dimasukkan ke dalam file berbentuk gambar menggunakan bantuan aplikasi steganografi (1). Dari dua *input* (teks dan gambar) akan menghasilkan satu output berupa gambar yang sama dengan gambar *input* (2). File berbentuk gambar inilah yang akan dikirimkan kepada penerima (3).

Penerima akan menerima file berbentuk satu gambar yang sebenarnya di dalamnya terdapat pesan rahasia yang disembunyikan. Dengan menggunakan aplikasi steganografi penerima dapat melakukan ekstrak pesan teks yang ada pada gambar (4). Aplikasi steganografi akan mengeluarkan *output* satu file yaitu file berisi pesan teks (5).

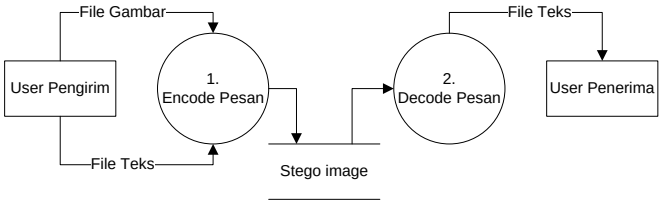
Use Case Diagram

Berikut use case diagram aplikasi steganografi yang dibuat.



Gambar 5. Diagram *Use Case*

Data Flow Diagram (DFD)



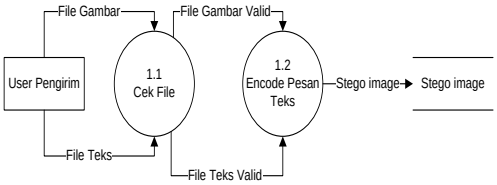
Gambar 6. Konteks Diagram (DFD Level 0)

Pada konteks diagram di atas terdapat dua proses yaitu proses *Encode* pesan dan *Decode* pesan. Pada proses *encode* pesan user akan diminta melakukan input dua file yaitu file berbentuk gambar dan file berbentuk teks (pesan).

Hasil proses *encode* pesan akan menghasilkan satu file gambar (*stego image).* *Stego image* akan dikirimkan kepada *user* penerima dan akan dilakukan ekstrak pesan pada proses *Decode* pesan.

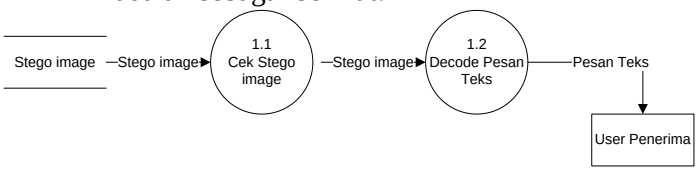
DFD Level 1

DFD Level 1 dari Proses 1 *Encode* Pesan adalah sebagai berikut:



Gambar 7. DFD Level 1 Proses *Encode* Pesan

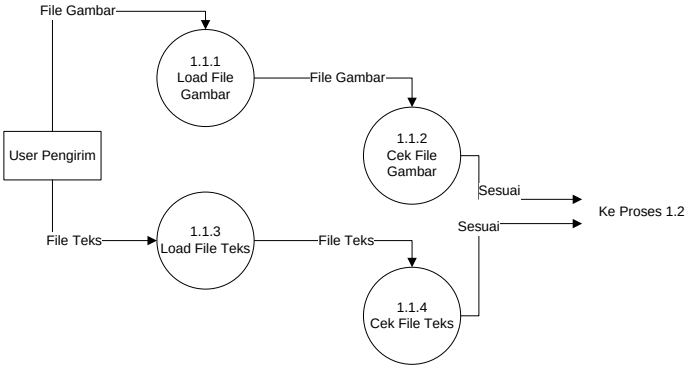
DFD Level 1 dari Proses 2 *Decode* Pesan adalah sebagai berikut:



Gambar 8. DFD Level 1 Proses *Decode* Pesan

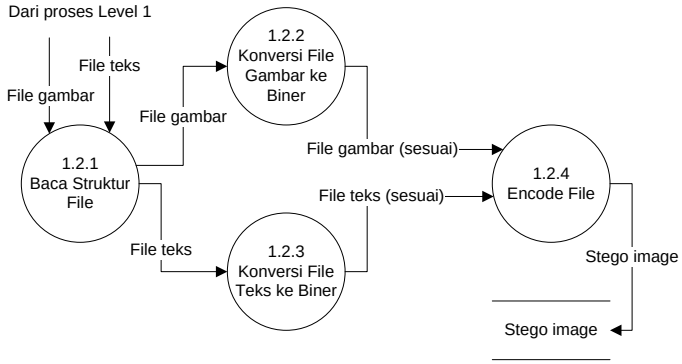
DFD Level 2

DFD Level 2 dari proses 1.1 Cek File adalah sebagai berikut.



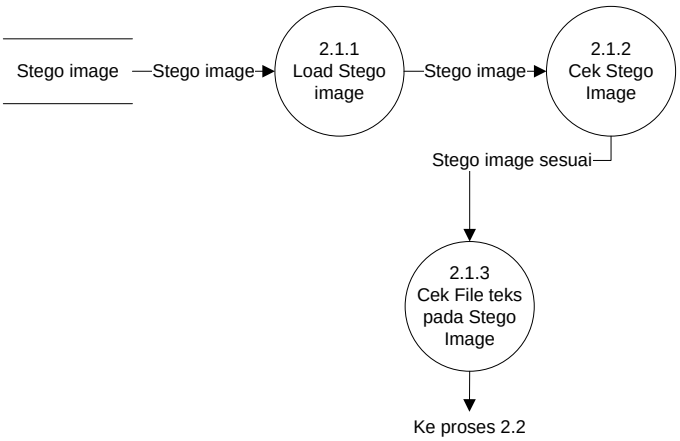
Gambar 9. DFD Level 2 Proses Cek File

DFD Level 2 dari proses 1.2 Encode Pesan Teks adalah sebagai berikut.



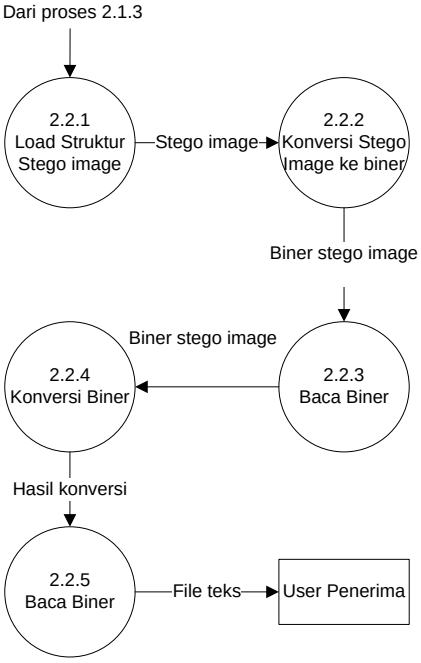
Gambar 10. DFD Level 2 Proses *Encode* Pesan Teks

DFD level 2 dari Proses 2.1 Cek *Stego Image* adalah sebagai berikut.



Gambar 11. DFD Level 2 Proses Cek *Stego Image*

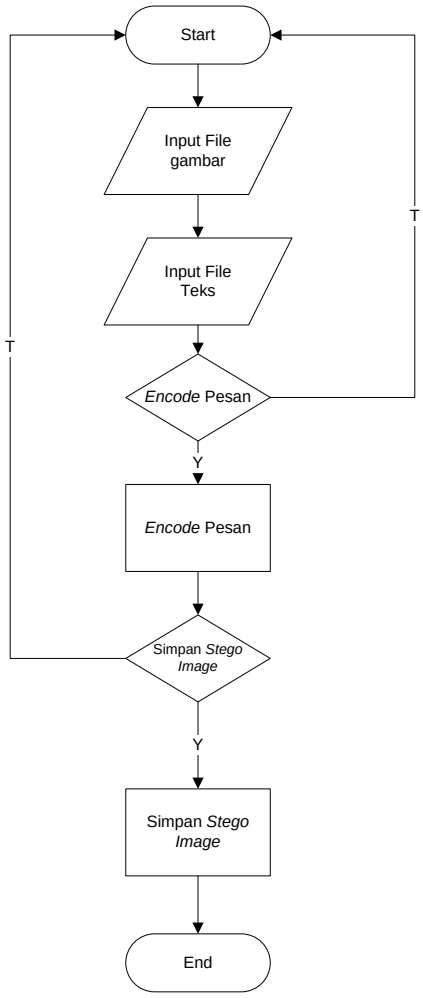
DFD level 2 dari Proses 2.2 *Decode Stego Image* adalah sebagai berikut.



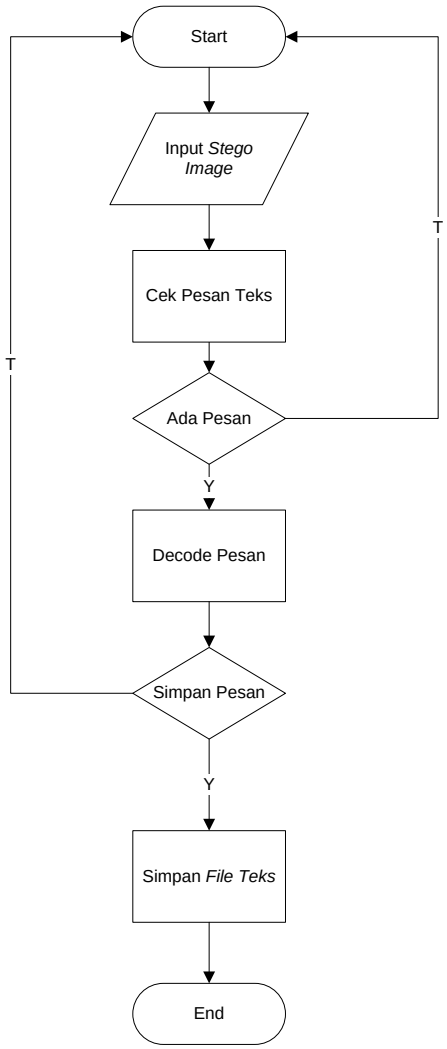
Gambar 12. DFD Level 2 Proses *Decode Stego Image*

***Flow Chart* (Diagram Alir)**

Logika pada program dalam dibuat menggunakan diagram alir di bawah ini



Gambar 13. Diagram Alir Aplikasi Steganografi Proses *Encode* Pesan



Gambar 14. Diagram Alir Aplikasi Steganografi Proses *Decode* Pesan

Implementasi Sistem

Aplikasi steganografi yang dikembangkan adalah aplikasi berbasis web yang dibuat dengan menggunakan bahasa pemrograman PHP. Basis web dipilih dikarenakan lingkungan pemrograman aplikasi berbasis web mempermudah dalam proses instalasi dan penggunaan. Aplikasi akan bersifat *client-server*, aplikasi tinggal diinstalasi pada komputer server maka *client* akan dengan mudah mengakses aplikasi tersebut.

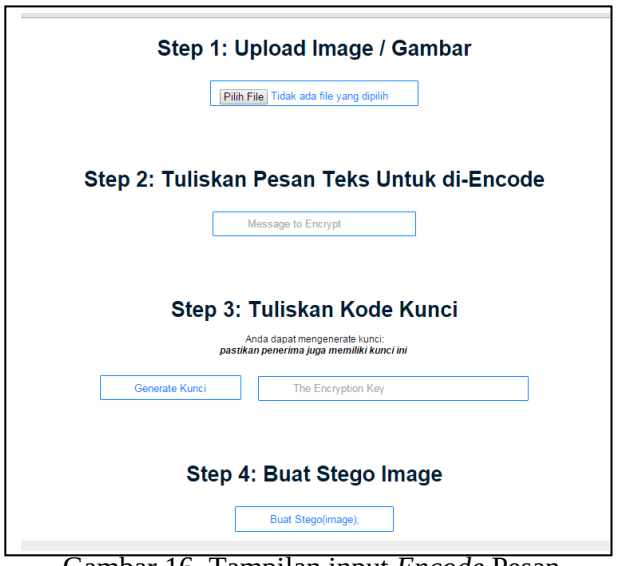
Pada implementasinya pengirim file cukup mengirimkan alamat *domain* aplikasi diinstal, file *stego image*, dan kunci *stego* maka pesan teks yang dikirim hanya akan bisa dibuka dan dibaca oleh penerima.

Tampilan Utama

Gambar 15. Tampilan Utama Aplikasi

Pada tampilan utama terdapat dua tombol navigasi yang bisa digunakan yaitu tombol *Encode* dan tombol *Decode*.

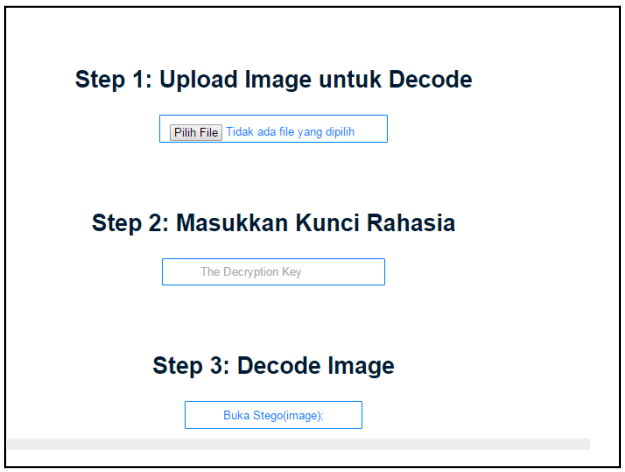
Navigasi tersebut berfungsi sebagai pilihan menu yang disediakan untuk pengguna dalam menggunakan aplikasi. Sebagai pengguna yang ingin mengirim data yang aman, dapat memulai aplikasi dengan memilih tombol *Encode*.



Gambar 16. Tampilan input *Encode* Pesan

Pada gambar di atas ditampilkan formulir *input* untuk proses *Encode* Pesan menjadi *stego image*. Aplikasi untuk *Encode* pesan dibuat dengan 4 tahap (step) yang harus dilakukan user. Diawali dari *input upload* gambar. Aplikasi membutuhkan gambar untuk pembuatan *stego image* dan butuh dilakukan *upload* ke *server* aplikasi.

Setelah dipilih file gambar maka terdapat inputan pesan teks yang akan dikirimkan ke user pengguna. Pesan teks ditulis dalam bentuk *plaintext* (teks biasa). Pada tahap ketiga aplikasi meminta pengguna untuk memberikan kunci untuk membuka *stego image* nantinya hasil keluaran. Pada tahap ini pengguna penting membuat catatan, karena kunci ini penting diingat untuk dijadikan kunci pula saat proses *decode.*



Gambar 17. Formulir Proses *Decode*

Proses *decode* memiliki input formulir tidak sebanyak proses *encode*. Proses *decode* memiliki tiga langkah untuk membuka pesan dari *stego image.* Awali dengan memilih *input* gambar *stego image* lalu masukkan kunci rahasia yang dibuat ketika proses *encode*. Untuk membuka pesan teks pada *stego image* klik tombol Buka Stego(Image), maka sebuah file teks akan diekspor oleh aplikasi dan pengguna perlu menyimpan dan dapat membuka isi pesan yang ada pada file tersebut.

Pengujian Sistem

Pengujian sistem dilakukan untuk melihat unjuk kerja dan fungsionalitas dari aplikasi yang dikembangan. Aplikasi yang dikembangan adalah aplikasi yang digunakan untuk menyembunyikan pesan teks yang dinilai rahasia. Pesan teks tersebut akan disembunyikan dengan cara disisipkan pada sebuah file berbentuk gambar dengan format jpg, png dan gif.

Pesan teks yang telah dikonversi ke dalam bentuk biner akan disebarkan di bit-bit *pixel* dari gambar sehingga pesan teks tidak akan terlihat dan terbaca. Pada media gambar juga tidak akan mengalami perubahan yang signifikan dikarenakan adanya penyisipan teks

tersebut. Bentuk dan warna dari file gambar tidak akan berubah dan tidak akan mudah dibaca oleh orang lain.

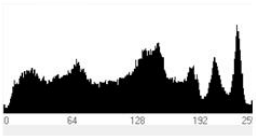
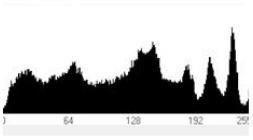
Proses *Encode*

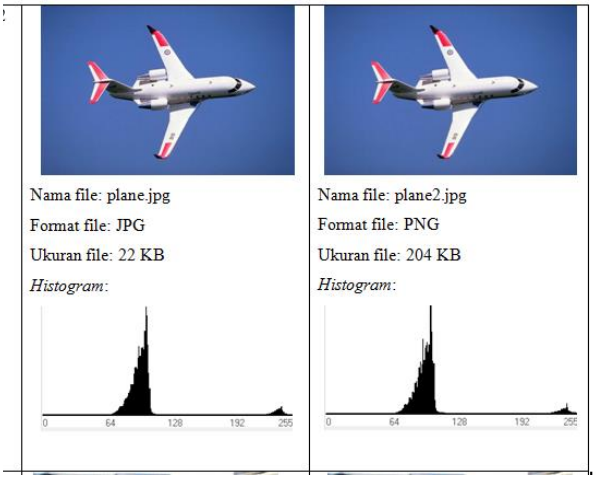
Proses *encode* akan dilakukan oleh user pengirim pesan. Uji coba proses *encode* diawali dengan menyiapkan file gambar untuk media menyisipkan pesan teks. Dalam hal ini disiapkan 2 file gambar untuk media penyisipan teks.

Tabel 1. File Gambar Proses *Encode*

No	Gambar	Nama File	Ukuran File	Format File
1		Car.jpg	26 KB	JPG File
2		Plane.jpg	22 KB	JPG File

Tabel 2. Perbandingan File Gambar Sebelum dan Sesudah *Encode*

No	Gambar Asli	*Stego Image*
1	 Nama file: car.jpg Format file: JPG Ukuran file: 26 KB *Histogram*: 	 Nama file: car2.png Format file: PNG Ukuran file: 187 KB *Histogram*: 



Proses *Decode*

Proses *decode* akan dilakukan oleh *user* penerima pesan. Uji coba proses *decode* diawali dengan mendapatkan file *stego image* berbentuk file gambar tempat dimana pesan teks disisipkan. Dalam hal ini hasil *encode* dari 3 file gambar yang telah menjadi *stego image* akan dijadikan *input* untuk membuka pesan teks.

Pada langkah *decode user* penerima pesan selain perlu mendapatkan *stego image* dari *user* pengirim pesan juga memerlukan kode kunci rahasia untuk proses *decode*. Kode kunci rahasia tersebut bisa didapatkan dari *user* pengirim pesan.

Gambar 18. Disiapkan file gambar yang sudah menjadi *stego image*

Dari temuan dan hasil di atas s*tego image* menjadi media cukup aman digunakan untuk menjaga keamanan dan konsistensi data berbentuk pesan teks. Pihak ketiga yang tidak memiliki hak untuk membuka pesan teks tidak akan pernah dapat mengetahui isi pesan teks yang dikirimkan. Walaupun pihak ketiga memiliki *stego image* tetap tidak akan dapat membuka isi pesan teks tanpa menggunakan aplikasi steganografi yang dibuat dalam penelitian ini ditambah adanya kode kunci yang harus dimasukkan setiap membuka pesan teks.

Perawatan Aplikasi Steganografi

Aplikasi steganografi yang dikembangkan dibuat berbasis web, aplikasi cukup diinstal pada komputer *server* maka *client* dimanapun berada akan dapat mengaksesnya. Hanya dengan memanggil alamat *domain* tempat aplikasi diinstall aplikasi akan dapat terbuka.

Aplikasi berbasis web dalam hal perawatan tidak perlu dilakukan perawatan khusus pada sisi aplikasi. Ketika ada *update* dari aplikasi yang dibuat cukup menimpa aplikasi yang ada di *server* maka di sisi *client* otomatis aplikasi juga akan ikut *update*. Dalam menjaga kestabilan dan performa aplikasi, perlu dilakukan *update* keamanan dari sistem operasi server yang digunakan.

KESIMPULAN

Dalam penelitian yang dilakukan penulis dapat mengambil beberapa kesimpulan, antara lain:

1. Teknik steganografi dapat dilakukan dengan menggunakan alat bantu berbentuk aplikasi perangkat lunak yang dikembangkan.
2. Teknik steganografi menjadi pilihan ideal untuk menjaga keamanan data berbentuk pesan teks.
3. Aplikasi steganografi yang dibuat dalam penelitian ini berbasis web sehingga pengguna cukup mengakses alamat domain aplikasi untuk melakukan *encode* dan *decode* pesan teks.
4. Steganografi tidak dapat sepenuhnya menggagalkan kegiatan forensik, sedikit celah pada algoritma dan aplikasi dapat dengan mudah menjadi pintu masuk forensik investigator untuk membongkar pesan rahasia.

Konsep dari teknik steganografi adalah menyisipkan pesan rahasia ke dalam file lain berbentuk file gambar sehingga dalam distribusi pesan tersebut dengan mengirimkan file gambar yang sudah berbentuk *stego image.*

DAFTAR PUSTAKA

D. Lilyani. 2014. *Implementasi Steganografi Pada Citra Digital Dengan Menggunakan Metode Dynamic Cell Spreading.* STMIK Budi Darma.

Eoghan Casey. 2014. Digital Evidence and Komputer Crime, 2nd ed.. halaman 20

Garfinkel, Simson L. 2010. Digital forensics research: The next 10 years. Digital Investigation Journal.

L. Truong. 2002. Steganography. Ece

Palmer, G. (2001). A Road Map For Digital Forensic Research (DTR – T001-01 FINAL). DFRW. http://www.dfrws.org/2001/dfrws-rm-final.pdf. diakses pada tanggal 28 Oktober 2015

Pressman, R. 2002. Rekayasa Perangkat Lunak Pendekatan Praktisi. Andi Offset. Yogyakarta.

R. Munir. 2004. Steganografi dan Watermarking. ITB.

T. Utomo. 2014. Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online. UIN Sunan Gunung Djati Bandung.

V. Liu, Brown F. 2006. *K2 Bleeding Edge Anti Forensic.* K2 Bleeding Edge