IMPLEMENTASI METODE STEGANOGRAFI *LEAST SIGNIFICANT BIT (LSB)* UNTUK PENGAMANAN INFORMASI PADA SEBUAH CITRA

Rr. Dina Oktavia Hendrati[1], Amir Hamzah[2], Uning Lestari[3]
[1,2,3] Prodi Teknik Informatika, FTI, IST AKPRIND Yogyakarta
[1]dienaariatama@gmail.com, [2]Miramzah@yahoo.co.id, [3]uning@akprind.ac.id

ABSTRACT

Communication security is a top priority in the use of steganography. This concept allows us to deliver a message to the people that we want through a medium without arousing suspicion to others. In this case the medium used is digital media. More specifically yangdipakai digital media is the media image because the image is the most popular medium in the concealment of the message rahasia.Makin widespread use of the Internet as a communication medium is the reason why this message insertion technique using the PHP programming language that is currently popular as a programming language based application support the web.

Method of LSB (Least Significant Byte) is a steganographic technique in which messages concealment concealment of a secret message is done by replacing the bits of data in a segment of the picture with the message bits rahasia.Bit-bit secret messages embedded in low bit or bits in a pixel rightmost constituent image consisting of warnamerah, green and blue (RGB) that each have a value of 8 bits is 0 to 255 with a binary format 00000000 to 11111111. Thus, three bits of data can be inserted at each pixel image available. LSB method is then applied in a library that was later named as stegger which has a function to insert messages in images using the PHP programming language. For added protection to messages sent then added an encryption algorithm that has been developed in a class named secrypt that accompanied the inclusion of keywords that sent the message has a higher security level.
Keywords: Steganography, PHP, LSB, Stegger

INTISARI

Keamanan dalam berkomunikasi merupakan prioritas utama dalam penggunaan steganografi. Konsep ini memungkinkan kita untuk menyampaikan pesan kepada orang-orang yang kita inginkan melalui suatu media tanpa menimbulkan kecurigaan kepada orang lain. Dalam hal ini media yang digunakan adalah media digital. Secara lebih spesifik media digital yangdipakai adalah media gambar karena gambar adalah media yang paling populer dalam penyembunyian pesan secara rahasia.Makin maraknya penggunaan internet sebagai media komunikasi adalah alasan mengapa teknik penyisipan pesan ini menggunakan bahasa pemrograman PHP yang saat ini populer sebagai bahasa pemrograman pendukung aplikasi berbasis web.

Metode LSB (Least Significant Byte) merupakan teknik penyembunyian pesan dalam steganografi dimana penyembunyian pesan rahasia dilakukan dengan mengganti bit-bit data dalam segmen gambar dengan bit-bit pesan rahasia.Bit-bit pesan rahasia disisipkan pada bit rendah atau bit paling kanan dalam *pixel* penyusun gambar yang terdiri dari warnamerah, hijau dan biru (RGB) yang masing masing memiliki nilai 8 bit bernilai 0 sampai dengan 255 dengan format biner 00000000 sampai dengan 11111111. Dengan demikian, 3 bit data dapat disisipkan pada tiap-tiap *pixel* gambar yang tersedia. Metode LSB kemudian diterapkan dalam sebuah library yang kemudian dinamakan sebagai stegger yang memiliki fungsi untuk menyisipkan pesan dalam gambar dengan menggunakan bahasa pemrograman PHP. Untuk menambahkan proteksi pada pesan yang dikirim maka ditambahkan sebuah algoritma enkripsi yang telah disusun dalam sebuah class bernama *secrypt* yang disertai penyertaan kata kunci agar pesan yang dikirim tersebut memiliki tingkat keamanan yang lebih tinggi.
Kata Kunci : Steganografi, PHP, LSB, Stegger.

PENDAHULUAN

Steganografi adalah seni dan ilmu untuk menyembunyikan pesan dalam sebuah pesan. Seni dan ilmu ini telah diterapkan sejak dahulu oleh orang Yunani kuno yang menyembunyikan pesan dengan cara membuat tato di kepala pembawa berita yang dibotaki dan menunggu sampai rambutnya tumbuh. Teknik steganografi lainnya adalah dengan menggunakan "*invisible ink*" (tinta yang tidak tampak). Tulisan yang ditulis dengan menggunakan *invisible ink* ini hanya dapat dibaca jika kertas tersebut diletakkan di atas lampu atau diarahkan ke matahari. Ketika perang dunia pertama, orang Jerman menyembunyikan pesan dalam bentuk "*microdot*", yaitu titik-titik yang kecil. Agen dapat membuat foto kemudian mengecilkannya sampai sekecil titik di tulisan dalam buku. Buku ini kemudian bisa dibawa-bawa tanpa ada yang curiga bahwa tanda titik di dalam tulisan di buku itu berisi pesan ataupun gambar.

Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama sehingga digunakan metode steganografi. Dengan metode steganografi, pesan yang ingin disampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut. Oleh sebab itu metode steganografi terus digunakan dan dikembangkan sampai saat ini. Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan sistem informasi.

Atas dasar uraian diatas, maka pada penulisan tugas akhiri ini akan membahas mengenai bagaimana mengamankan suatu pesan dengan menyisipkan (menyembunyikan) kedalam pesan lainnya yaitu file citra dengan menggunakan algoritma LSB (*Least Significant Bit*) pada suatu aplikasi steganografi.

TINJAUAN PUSTAKA

Dalam penelitian ini, digunakan beberapa referensi yang berhubungan dengan obyek penelitian. Beberapa referensi diambil dari hasil penelitian yang berkaitan dengan teknik penyembunyian *file* gambar menggunakan steganografi dengan metode *Least Significant Bit* (LSB). Pada penelitian yang dilakukan oleh Maulana (2011), Steganografi data berupa pesan text atau informasi data ke dalam media gambar dapat diimplementasikan menggunakan metode modifikasi *Least Significant Bit* yaitu dengan mengkonversikan setiap nilai–nilai *bit* data kedalam nilai–nilai *bit* media gambar, Ukuran dari daya tampung media gambar tidak mempengaruhi seberapa besar jumlah data yang dapat disembunyikan. Ukuran media gambar harus lebih besar dari jumlah data yang akan disembunyikan atau diamankan. Perubahan yang terjadi pada steganografi tidak signifikan dan masih tampak seperti gambar normal karena *bit* yang mempengaruhi pada media gambar adalah *byte* yang terendah dan saran agar keamanan dan kualitas gambar steganografi lebih baik lagi dapat dilakukan penyembunyian secara random yaitu posisi peletakan nilai *bit* data ke *bit* gambar tidak lagi berurutan mengikuti titik awal.

Penelitian lain yang berkaitan dengan teknik penyembunyian data gambar menggunakan steganografi dengan metode LSB yang dilakukan oleh Astried (2011). Metode LSB merupakan metode penyembunyian data yang paling sederhana. Penggantian LSB dilakukan dengan memodifikasi *bit* terakhir dalam satu *byte* data, yang menyebabkan nilai *byte* menjadi satu lebih tinggi atau satu lebih rendah. Perubahan pada satu *bit* LSB hanya menyebabkan sedikit perubahan yang tidak dapat dideteksi oleh mata manusia.

Penelitian yang berkaitan dengan penggunaan steganografi berbasis LSB lainnya yang dilakukan oleh Neyman (2011) pada gambar dengan menyisipkan *variable size* mampu menyembunyikan informasi rahasia dengan baik. Selain itu penggunaannya dapat disesuaikan dengan ukuran media gambar yang digunakan.

Berdasarkan penelitian-penelitian yang dilakukan sebelumnya, pada penelitian ini akan dilakukan implementasi penyembunyian informasi penting pada sebuah citra diam yang berformat jpeg dan png.

Least Significant Bit (Lsb)

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas gambar pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada *bit* rendah atau *bit* yang paling kanan (LSB) pada data *pixel* yang menyusun *file* tersebut. Pada berkas *bit*map 24 *bit*, setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 *bit* (*byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap *pixel* berkas *bit*map 24 *bit* kita dapat menyisipkan 3 *bit* data.

Kekurangan dari LSB *insertion* antara lain dapat secara drastis mengubah unsur pokok warna dari *pixel*. Ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 *bit image*, bagaimanapun *file* tersebut sangatlah besar. Antara 8 *bit* dan 24 *bit image* mudah diserang dalam pemrosesan *image*, seperti *cropping* (kegagalan) dan *compression* (pemampatan).

Keuntungan dari LSB *Insertion* : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *pallete* (lukisan) (Adiria, 2010).

Metodologi Penelitian

Alur Perancangan Sistem

a. Analisa Kebutuhan
   Analisa kebutuhan merupakan tahap awal untuk menentukan desain sistem dengan menu-menu yang digunakan oleh *user* untuk melakukan pengelolaan data gambar yang akan disisipi pesan rahasia.
b. Desain Sistem
   Merupakan tahap penyusunan proses, data, aliran proses dan hubungan antar data yang optimal untuk menjalankan proses aplikasi dan memenuhi kebutuhan *user* sesuai dengan hasil analisa kebutuhan.
c. Penulisan Kode Program
   Merupakan tahap penerjemahan desain sistem yang telah dibuat kedalam perintah-perintah yang dapat dimengerti oleh komputer dengan menggunakan bahasa pemrograman. Bahasa pemrograman yang diguanakan dalam pembuatan sistem ini adalah bahasa pemrograman PHP.
d. Pengujian Program
   Pada tahap ini proses input output diuji coba sehingga kemungkinan terjadi error dapat segera diketahui dan segera dilakukan perbaikan pada penulisan kode program. Pengujian program dilakukan di *localhost* dengan menggunakan *xampp.*
e. Penerapan Program
   Penerapan program merupakan tahap dimana pengembang menerapkan aplikasi yang telah selesai dibuat dan diuji.

Alat Dan Bahan Penelitian

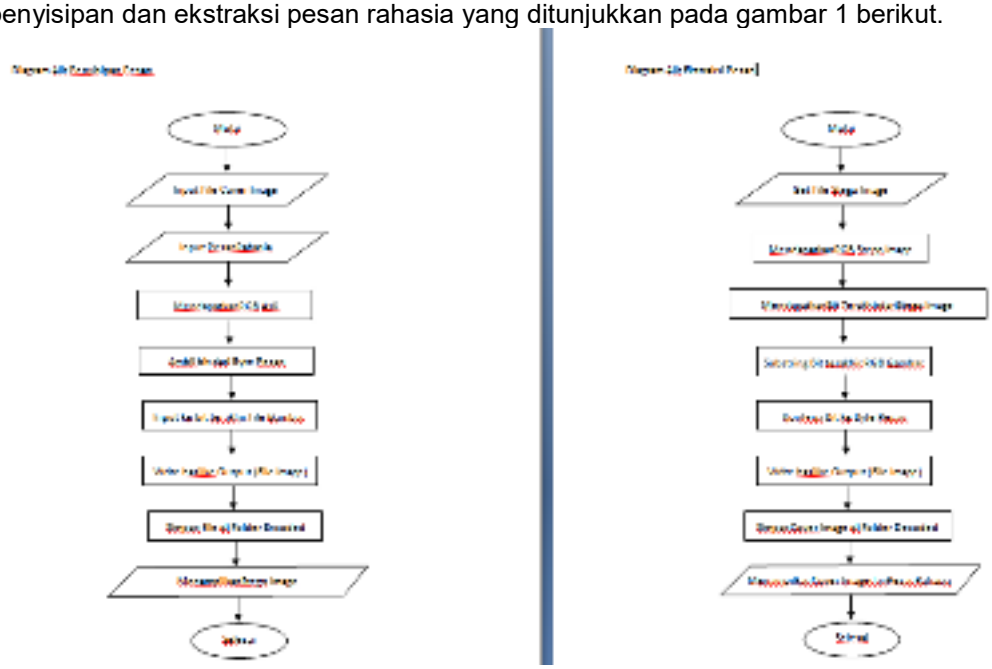
Dalam penelitian ini menggunakan alat penelitian yang berupa perangkat keras dan perangkat lunak, yaitu :

1. **Perangkat keras**
   Perangkat keras yang digunakan dalam melakukan penelitian ini hanya sebuah laptop dengan spesifikasi sebagai berikut ;
   - Nama laptop : THOSIBA
   - *Processor* : Intel (R) Pentium (R) 2.20GHz
   - RAM : 2GB
2. **Perangkat Lunak**
   Perangkat lunak yang digunakan dalam melakukan penelitian ini adalah

- *Windows 7 ultimate 32-bit*
- Bahasa pemrograman PHP
- *Web Server*

Sedangkan dalam penelitian ini data yang digunakan sebagai bahan penelitian adalah beberapa data dan beberapa berkas gambar yang akan disisipi pesan dan dijadikan bahan pada proses pengujian

Perancangan infastruktur pada penelitian ini dengan berupa *flowchart* proses penyisipan dan ekstraksi pesan rahasia yang ditunjukkan pada gambar 1 berikut.



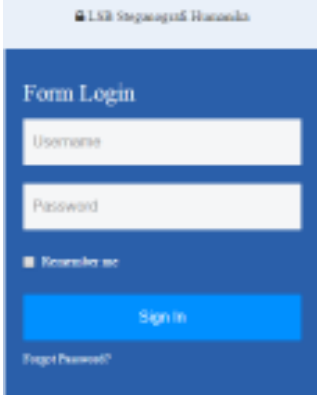
Gambar 1. *flowchart* penyisipan dan ekstraksi pesan

PEMBAHASAN

Sistem ini bernama "Aplikasi Steganografi LSB HUMANIKA" yang dibangun untuk mengamankan informasi atau pesan rahasia dengan menyisipkan informasi atau pesan rahasia tersebut ke dalam sebuah citra diam berformat JPEG dan PNG agar informasi atau pesan rahasia tersebut tidak dapat di akses oleh pihak yang tidak mendapat hak untuk mengaksesnya. Sistem ini hanya memiliki satu fitur yaitu fitur *login administrator. Administrator* memiliki seluruh hak akses yang ada pada sistem ini. Hak Akses yang dimiliki oleh *administrator* adalah login *administratror,* menambahkan anggota, menambahkan admin, menambahkan foto anggota, melakukan *encoding*, melakukan *decoding.* Sistem ini akan menampilkan menu-menu sebagai berikut :

1. Halaman Login

Halaman login pada sistem ini ditunjukkan pada gambar 2.



Gambar 2. Halaman Login

2. Halaman *Dashboard*

Halaman dasboard adalah halaman utama dalam sistem ini dimana setelah seorang admin melakukan proses login akan langsung masuk pada halaman dash board. halaman dashboard ditunjukkan pada gambar 3.

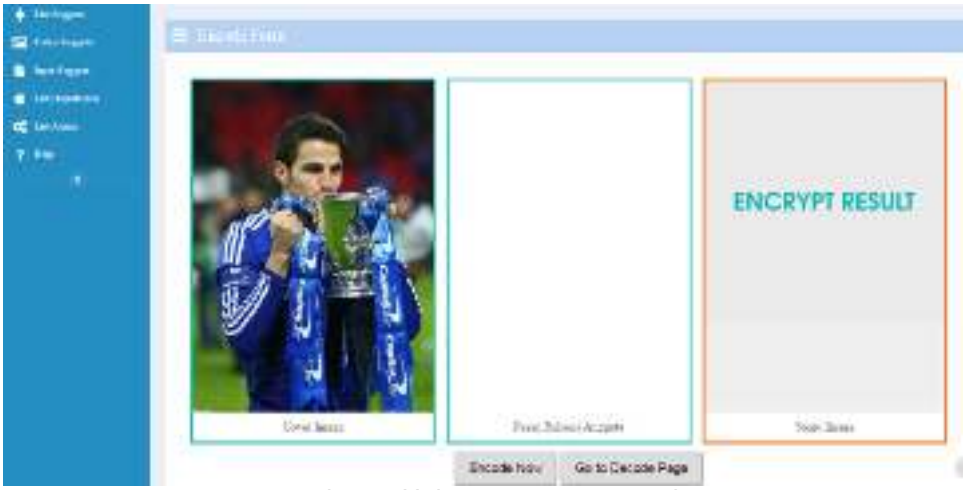
Gambar 3. Halaman Dashboard

3. Halaman Anggota

Halaman anggota adalah halaman ketika masuk ke menu *List* anggota. Pada halaman ini yang nantinya dapat dilakukan proses *encoding dan decoding* berikut adalah halaman list anggota yang ditunjukkan pada gambar 4.

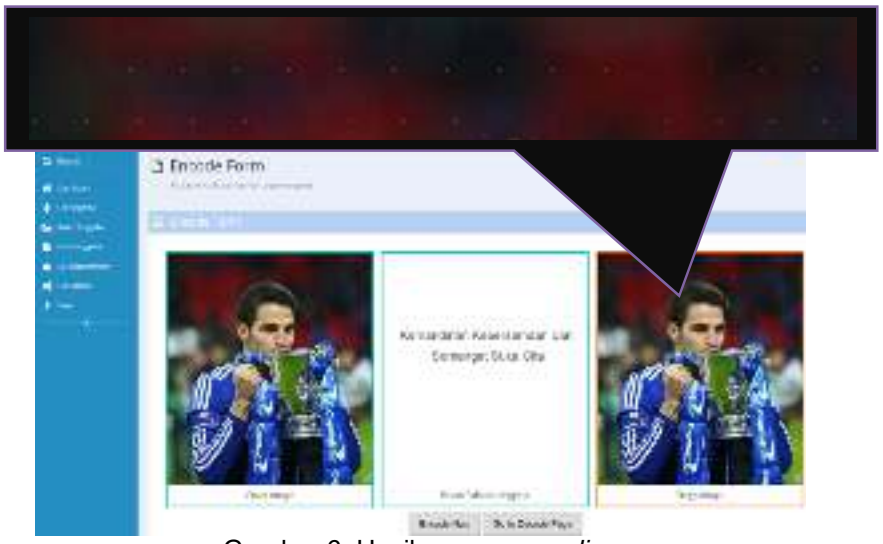
Gambar 4. Halaman anggota

Pada halaman ini terdapat menu *encode* dan *decode.* Dimana proses tersebut adalah bagian yang penting dari penelitian ini. Proses *encode* dapat dilakukan ketika memilih tombol aksi *encode*. Ketika sudah memilih aksi *encode* maka akan dibawa ke halaman *encode*. Halaman *encode* ditunjukkan pada gambar 5.



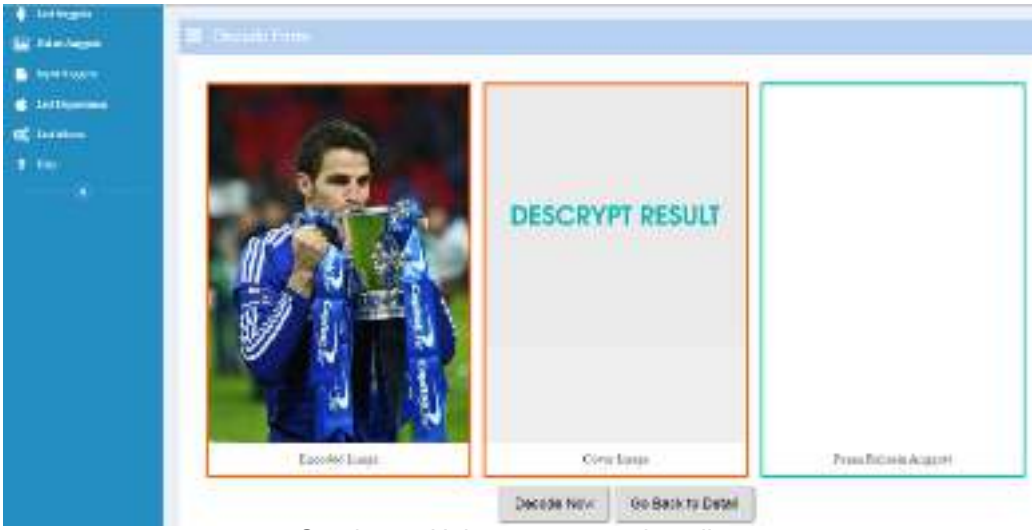
gambar 5. Halaman proses *encode*

Pada halaman *encode* terlihat tiga kolom. kolom pertama adalah kolom untuk gambar awal atau yang sering disebut dengan *cover image.* kolom kedua adalah kolom untuk memasukkan pesan rahasia yang akan disisipkan ke dalam *cover image.* Sedangkan kolom ketiga adalah kolom untuk gambar yang sudah disisipi pesan rahasia (*stego image*). Setelah dilakukan proses *encode* yang dilakukan dengan memilih lombol aksi *encode* maka *stego image* akan tertampil dikolom ketiga dengan perbedaan yang tidak begitu jauh dari *cover image.* Hanya terdapat titik-titik kecil yang berjumlah banyak pada *stego-image*. Semakin banyak jumlah karakter pesan rahasia yang dimasukkan maka, semakin banyak pula titik-titik kecil yang tertampil pada *stego image.* Hasil dari proses *encode* ditunjukkan pada gambar 6



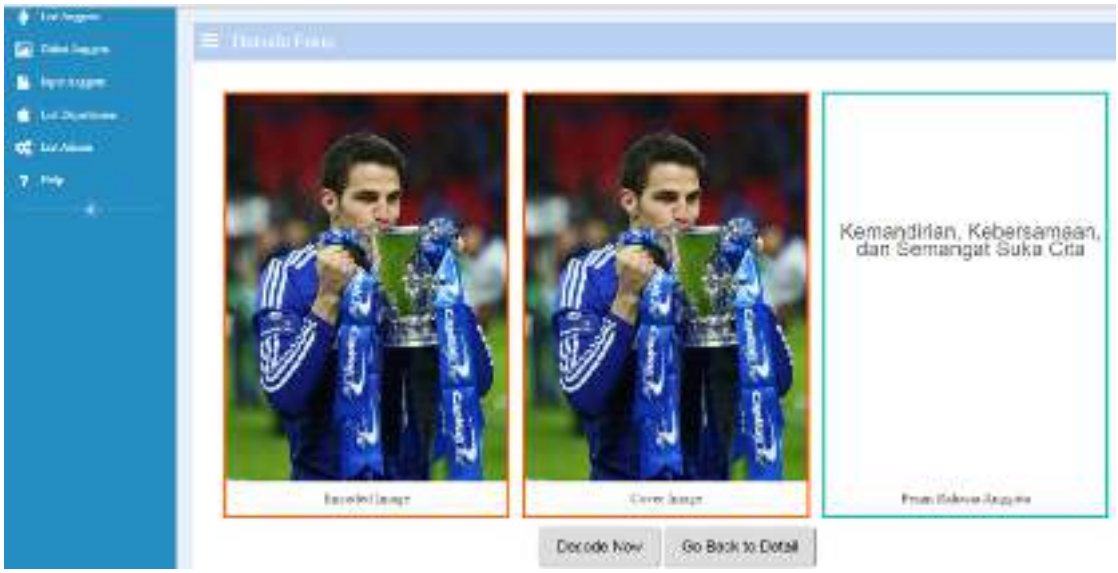
Gambar 6. Hasil proses *encoding*

Ketika sudah dilakukan proses *encode* maka akan dilakukan proses *decode*. Pada broses *decode* ini dapat dilakukan ketika sudah dipilih tombol aksi *decode* yang ada di bawah kolom-kolom gambar tersebut. Halaman proses *decode* ditunjukkan pada gambar 7.



Gambar 7. Halaman proses *decoding*

Pada halaman *decode* ini juga terdapat tiga kolom seperti pada halaman *encode*. Pada halaman *decode* ini kolom pertama adalah kolom untuk *stego image* atau gamar yang disisipi pesan kolom kedua dan ketiga adalah kolom yang akan terisi pada saat dipilih tombol aksi *decode*. Ketika tombol aksi *decode* sudah dipilih maka pada kolom kedua akan tertampil gambar awal atau *cover image* lagi dan kolom ketiga akan tertampil pesan rahasi yang sebelumnya sudah disisipkan. Halaman hasil *decode* ditunjukkan pada gambar 8.



Gambar 8. Hasil proses *decode*

Analisis Penyembunyian File

Analisis penyembunyian *file* ini dilakukan bertujuan untuk mengetahui apakah file gambar yang digunakan sebagai tempat penyembunyian atau penyisipan pesan rahasia dapat menampung *file* tanpa adanya perubahan ukuran pada file gambar. Kemudian apakah *file* pesan rahasia tersebut dapat diambil kembali seperti semula tanpa adanya perubahan. Tabel uji penyembunyian file ditunjukkan pada tabel 1.

Tabel 1. uji penyembunyian file

File gambar	*Size*\ *(byte)*	*File* rahasia	*Size*	*Output*	*Size (byte)*	*Retrieved*	*Size*
Fabregas.jpg	41.079	Apa.txt	332 karakter	Fabregas.jpg	41.079	Apa.txt	332 karakter
Andi.jpg	17.796	Satu.docx	662 karakter	Andi.jpg	17.796	Satu.docx	662 karakter
Dina.jpg	402.028	Dua.docx	1149 karakter	Dina.jpg	402.028	Dua.docx	1149 karakter
Arifah.jpg	26.400	Ini.txt	215 karakter	Arifah.jpg	26.400	Ini.txt	215 karakter
Cantik.png	312.270	Dua.docx	1149 karakter	Cantik.png	312.270	Dua.docx	1149 karakter
Korea.png	201.238	Satu.docx	662 karakter	Korea.png	201.238	Satu.docx	662 karakter
Cewek.png	1.037.305	Apa.txt	332 karakter	Cewek.png	1.037.305	Ini.txt	332 karakter

KESIMPULAN

1. Implementasi algoritma LSB (*Least Significant Bit*) dapat digunakan cukup baik untuk menyembunyikan pesan di dalam pesan sebuah berkas citra digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut.
2. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada *file* citra uji dalam aplikasi steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan.
3. Aplikasi steganografi LSB Humanika ini berbasis *web* menggunakan bahasa pemrograman PHP sehingga dapat lebih dikenali masyarakat awam dan tidak harus ada pelatihan khusus dalam penggunaannya.
4. Pengujian yang telah dilakukan pada aplikasi ini adalah dengan menguji beberapa gambar yang berekstensi .jpeg dan .png dengan beberapa pesan rahasia yang memiliki jumlah karakter yang beragam.
5. Sistem ini hanya dapat diakses dari sisi *administrator* dan belum ada dari sisi selain *admin*.

Saran

1. Algoritma pada implementasi steganografi ini kurang kuat meskipun untuk memecahkannya cukup sulit, tetapi jika kelemahan utamanya ditemukan maka sangat mudah untuk memecahkannya.
2. Kedepannya diharapkan dapat dikembangkan suatu aplikasi Steganografi dengan metode lain yang lebih variatif dan lebih seperti baik seperti penggabungan algoritma LSB dengan algoritma *Data Encryption Standard* (DES), *Triple Data Encryption Standard* (3DES), RC4, *Anvanced Encryption Standard* (AES) dan lain-lain agar pesan tersembunyi menjadi sangat sulit terdeteksi dan ukuran serta kualitas citra yang dihasikan tidak jauh berbeda dengan kualitas citra sebelumnya.
3. Perlu didukung dengan fitur-fitur yang berguna untuk *repoting* dan rekapitulasi data-data yang sudah masuk ke dalam sistem tersebut.

DAFTAR PUSTAKA

Adiria. (2010). *Analisis dan Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit.* Jakarata: UIN Syarif Hidayatullah.

Astried. (2011). *Steganografi Dengan Metode Penggantian Least Significant Bit (LSB).* Pekanbaru: Universitas Riau.

Maulana, A. M. (2011). Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit. *steganografi LSB* , 1-10.

Neyman, S. N. (2011). Teknik Penyembunyuan data rahasia pada berkas gambar digital menggunakan steganografi Least Significant Bit Variable-Siza. *Jurnal ilkom* , 34-35.