Implementasi Steganografi Metode LSB Menggunakan Program PHP untuk Keamanan Pesan Gambar

Wiyata
Program Studi Ilmu Komputer, Fakultas Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260
.
Email : puspawiyata@gmail.com

Abstraksi : Steganografi meruapakan karya seni dan cara pengamanan pesan baik berupa gambar atau text yang di sisipkan dalam gambar, untuk menghindari ancaman-ancaman dari penyadapan, interupsi, modifikasi maupun fabrikasi dari luar. Dengan steganografi memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya. Softwere pendukung dalam melakukan proses steganografi ini, penulis menggunakan metode Least Significant Bit (LSB) yang menggunakan program Hypertext Prepocessor (PHP) dengan nama aplikasi softwerenya adalah Stegger, yang mana bisa bisa mengirim gambar atau citra digital yang di proses encoding dan decoding berdasarkan kunci enkrip atau dekrip data, untuk mengirim atau untuk melihat kata yang tersebunyi di dalam gambar, sedangkan metode LSB adalah proses pembuatan pesan dengan mengambil karakter yang paling kanan, yang dikombinasi sehingga membentuk suatu pesan, dan dalam penulisan makalah ini, penulis juga menggunakan Message-Digest algortihm 5 (MD5) yang mana memproses variabel yang di ubah menjadi output sepanjang 128 bit. MD5 sering digunakan dalam pembuatan password untuk keamanan internet.
Kunci : steganografi, PHP, stegger, enkripsi, MD5

Abstract: Steganography is the art work and how security in the form of picture messages or paste text in the picture, to avoid threats of interception, interruption, modification and fabrication from the outside. With steganography has a shape similar to the perception of the original form, of course, the perception here by human senses, but not by a computer or other digital processing devices. Softwere support in the process of steganography, the author uses the method of Least Significant Bit (LSB) which uses Hypertext Prepocessor program (PHP) with the application name softwerenya is Stegger, which can be send a picture or a digital image in the process of encoding and decoding based on the key enkrip or decrypt the data, to send or to see the hidden words in the image, while the LSB method is the process of making the message by taking the rightmost characters, which combined to form a message, and in the writing of this paper, the authors also use the Message-Digest algortihm 5 (MD5) which process variables are transformed into outputs 128 bits long. MD5 is often used in the manufacture of passwords for Internet security.
Keywords : Steganografi, LSB, PHP ,Stegger, enkripsi, MD5.

I. Pendahuluan

Seiring dengan perkembangan teknologi Informasi dan Komunikasi, penggunaan alat – alat teknologi sering di gunakan. Dan yang menjadi proritas utama adalah menjaga keamanan pesan tersebut sampai tujuan tanpa diketahui pihak yang tidak berkepentingan.

Dengan alasan tersebut lahirlah kriptografi, yaitu metode pengolahan informasi dengan algoritma tertentu sehingga menjadi samar dan sulit dimengerti maknanya. Namun metode ini sering menimbulkan kecurigaan pihak ketiga, sebab pesan yang sulit dimengerti pasti sudah diolah dan menunjukkan bahwa pesan itu merupakan informasi penting.

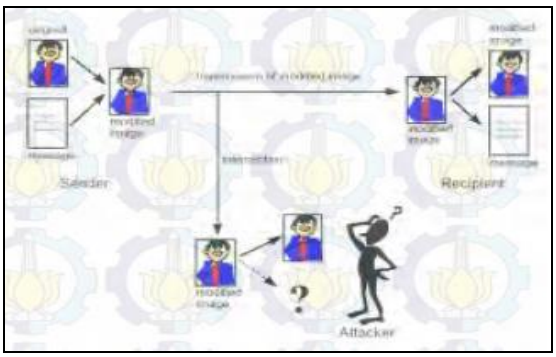
Untuk menghindari permasalahan tersebut maka lahirlah steganografi, yaitu metode menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Aspek terpenting dari steganografi adalah tingkat keamanan penyembunyian informasinya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi.

Steganografi yang umum dipakai adalah penyembunyian informasi pada media gambar, di mana informasi text dimasukkan ke dalam bit pixel gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan.

Oleh karena itu makalah ini membahas tentang sebuah implementasi yang membuat steganografi text pada media gambar menjadi lebih kuat dan aman. Implementasi ini mengenkripsi pesan text dengan sebuah password menggunakan algoritma kriptografi Data Encryption Standard (DES). Informasi yang terenkripsi kemudian dimasukkan pada pixel yang diambil dari region menggunakan algoritma Region-Embed Data Density (REDD).

II. Konsep Steganografi

Pengamanan data selalu yang dipikirkan setiap benak pengguna komputer. Pengamanan bisa menggunakan Kriptografi atau Steganografi. Dengan Kriptografi akan mudah dicurigai karena ada tulisan yang sulit di baca dan menggunakan Steganografi akan sulit diketahui karena data atau gambar persis dengan aslinya. Penulis akan menggunakan metode Steganografi , dengan konsep seperti gambar 1 yaitu Ilustrasi Dasar Konsep Steganografi.

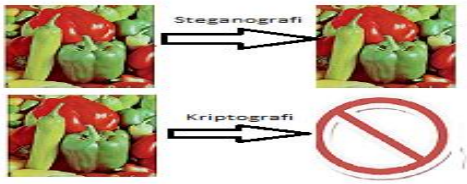


Gambar 1 Ilustrasi Dasar Konsep Steganografi

Steganografi adalah seni dan ilmu menulispesan tersembunyi dengan suatu cara sehingga selain si penerima yang dimaksud tak ada satupun orang yang mengetahui atau menyadari bahwa suatu pesam tersimpan. Sebaliknya, kriptografi adalah menyamarkan arti suatu pesan tanpa menyembunyikan keberadaanya dan

membuat siapapun menyadari bahwa ada sesuatu yang mencurigakan dari pesan tersebut. Kelebihan steganografi dibanding kriptografi adalah pesanpesannya tidak menarik perhatian orang lain.

Namun pada saat ini seringkali kita temukan penggunaan steganografi dan kriptografi secara bersamaan untuk menjamin kerahasiaan sebuah pesan.



Gambar 2 : Ilustrasi Konsep Steganografi

Pada dasarnya citra digital (diskrit) dihasilkan dari citra analog (kontinu) melalui digitalisasi. Digitalisasi citra analog terdiri atas *sampling* dan kuantisasi (*quantization*). *Sampling* adalah pembagian citra ke dalam elemen-elemen diskrit (piksel), sedangkan kuantisasi adalah pemberian nilai intensitas warna pada setiap piksel dengan nilai yang berupa bilangan bulat[1]. Dan citra tersebut adalah citra biner, citra grayscale dan citra berwarna.

Adapun Citra Digital memiliki beberapa format yang memiliki karakteristk tersendiri. Format pada citra digital ini umumnya berdasarkan tipe dan cara kompresi yang digunakan pada citra digital tersebut.

Menurut Awcock (2006 : 18), "Ada empat format citra digital yang sering dijumpai, antara lain :

1. *Bitmap* (BMP)

Merupakan format Gambar yang paling umum dan merupakan format *standard windows*. Ukuran *file*nya sangat besar karena bisa mencapai ukuran *Megabytes*. *File* ini merupakan format yang belum terkompresi dan menggunakan sistem warna RGB (*Red, Green, Blue*) di mana masing-masing warna *pixel*nya terdiri dari 3 komponen R, G, dan B yang dicampur menjadi satu. *File* BMP dapat dibuka dengan berbagai macam *software* pembuka Gambar seperti *ACDSee*, *Paint*, Irvan *View* dan lain-lain. *File* BMP tidak bisa (sangat jarang) digunakan di *web (internet)* karena ukurannya yang besar.

Tabel 1 : Bitmap Info Header

Nama Field	Size in Bytes	Keterangan
bfType	2	Mengandung karakter "BM" yang mengidentifikasikan tipe file
bfSize	4	Memori file
bfReserved1	2	Tidak dipergunakan
bfReserved1	2	Tidak dipergunakan
bfOffBits	4	Offset untuk memulai data pixel

Tabel 2 : Bitmap Core Header

Field Name	Size in Bytes	Keterangan
bcSize	4	Memori Header
bcWidth	2	Lebar Gambar
bcHeight	2	Tinggi Gambar
bcPlanes	2	Harus 1
bcBitCount	2	Bits per pixels – 1,4,8 atau 24

2. *Joint Photographic Expert Group* (JPEG/JPG)

Format JPEG merupakan format yang paling terkenal sampai sekarang ini. Hali ini karena sifatnya yang berukuran kecil

(hanya puluhan/ratusan KB saja), dan bersifat portable. *File* ini sering digunakan pada bidang fotografi untuk menyimpan *file* foto. *File* ini bisa digunakan di *web* (*internet*).

3. *Graphic Intrechange Format* (GIF)
Tipe file GIF memungkinkan penambahan warna transparan dan dapat digunakan untuk membuat animasi sederhana, tetapi saat ini standar GIF hanya maksimal 256 warna saja. File ini menggunakan kompresi yang tidak menghilangkan data (*lossles compression*) tetapi penurunan jumlah warna menjadi 256 sering membuat gambar yang kaya warna seperti pemandangan menjadi tidak realistis. Pada program MS Paint, tidak ada fasilitas penyesuaian warna yang digunakan (*color table*) sehingga menyimpan file GIF di MS Paint seringkali menghasilkan gambar yang terlihat rusak atau berubah warna. Pada program pengolah gambar yang lebih baik, seperti *Adobe Photoshop*, *color table* bisa diatur otomatis atau manual sehingga gambar tidak berubah warna atau rusak.

File GIF cocok digunakan untuk:

a. Gambar dengan jumlah warna sedikit (dibawah 256).
b. Gambar yang memerlukan perbedaan warna yang tegas seperti logo tanpa gradien.
c. Gambar animasi sederhana seperti banner-banner iklan, header, dan sebagainya.
d. *Print shoot* (hasil dari print screen) dari program-program simple dengan jumlah warna sedikit.

File GIF tidak cocok digunakan untuk:

a. Gambar yang memiliki banyak warna seperti pemandangan.
b. Gambar yang didalamnya terdapat warna gradien atau semburat.

4. *Portable Network Graphics* (PNG)
Tipe file PNG merupakan solusi kompresi yang powerfull dengan warna yang lebih banyak (24 bit RGB + alpha). Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (*lossles compression*). Kelebihan file PNG adalah adanya warna transparan dan alpha. Warna alpha memungkinkan sebuah gambar transparan, tetapi gambar tersebut masih dapat dilihat mata seperti samar-samar atau bening. File PNG dapat diatur jumlah warnanya 64 bit (true color + alpha) sampai indexed color 1 bit. Dengan jumlah warna yang sama, ko mpresi file PNG lebih baik daripada GIF, tetapi memiliki ukuran file yang lebih besar daripada JPG. Kekurangan tipe PNG adalah belum populer sehingga sebagian browser tidak mendukungnya.
File PNG cocok digunakan untuk :
a. Gambar yang memiliki warna banyak.
b. Gambar yang mau diedit ulang tanpa menurunkan kualitas.
File PNG tidak cocok digunakan untuk gambar yang jika dikompress dengan JPG hampir-hampir tidak terlihat penurunan kualitasnya.

5. *Tagged Interchange File Format* (TIFF)
Merupakan format file terkompresi yang biasa digunakan di paket desktop

publishing dan merupakan format file bagi perusahaan percetakan. File ini diindikasikan dengan ekstensi .TIF Kekuatan dari format file TIFF adalah lebih fleksibel dari format gambar bitmap yang didukung secara ritual oleh seluruh *point*, *image editing* dan aplikasi kedalaman *layout*.

6. PCX Format

file ini dikembangkan oleh perusahaan bernama Zoft Cooperation. Format file ini merupakan format yang fleksibel karena hampir semua program dalam PC mampu membaca gambar dengan format file ini. Format file ini mampu menyimpan informasi bit depth sebesar 1 hingga 24 bit namun tidak mampu menyimpan alpha channel. Format file ini mampu menyimpan gam bar dengan mode warna RGB, Grayscale, Bitmpa dan Indexed Color.

7. Photoshop Document (PSD)

Format file ini merupakan format asli dokumen Adobe Photoshop. Format ini mampu menyimpan informasi layer dan alpha channel yang terdapat pada sebuah gambar, sehingga suatu saat dapat dibuka dan diedit kembali. Format ini juga mampu

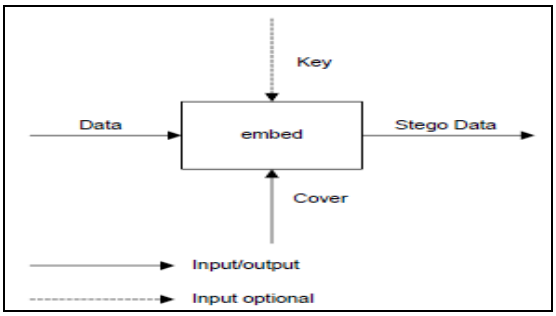
menyimpan gambar dalam beberapa mode warna yang disediakan Photoshop. Anda dapat menyimpan dengan format file ini jika ingin mengeditnya kembali.

Steganografi terdiri atas dua teknik yaitu :

a. Teknik Penyembunyian data

Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Hingga saat ini sudah banyak dikemukakan oleh para ilmuwan metode-metode penyembunyian data. Metode yang paling sederhana adalah metode modifikasi LSB. Pada susunan bit di dalam sebuah byte (1byte = 8bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti yaitu LSB.

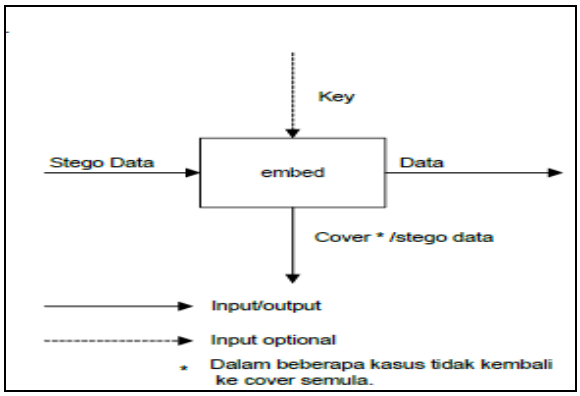
Misalnya pada byte 11010010, bit 1 yang pertama (digaris bawahi) adalah bit MSB dan bit 0 yang terakhir (digaris bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna tertentu, maka perubahan satu bit LSB tidak mengubah warna keabuan tersebut secara berarti. Selain itu, mata manusia tidak dapat membedakan perubahan yang kecil.



Gambar 3: Penyembunyian data

b. Teknik Pengungkapan Data

Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (reveal atau extraction). Dengan cara mengumpulkan kembali bit-bit data rahasia yang bertaburan di dalam citra.



Gambar 4 : Pengungkapan Data

Beberapa metode untuk membuat suatu steganografi yaitu Least Significant Bit (LSB), Algorithms and Transformation, Redundant Pattern Encoding, Spread Spectrum method dan End Of File. Metode-metode tersebut digunakan dalam steganografi dalam media dan fungsi yang berbeda-beda untuk memaksimalkan pengamanan suatu data (informasi) agar menjadi rahasia. Dalam pembangunan metode yang digunakan yaitu Least Signifacant Bit (LSB) yang berfungsi sebagai tempat penyisipan data.

Metode ini banyak digunakan karena metode ini paling sederhana dan mudah diimplementasikan. Media penampung yang paling sering digunakan dalam mengimplementasikan steganography adalah gambar. Kehandalan penggunaan file gambar dibandingkan dengan media lain adalah kualitas gambar yang telah disisipi pesan rahasia tidak berbeda jauh dengan kualitas citra aslinya.

III. Metode Least Significant Bit (LSB)

1. Least Significant Bit (LSB)

Metode Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri.

Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 1111 1111b). Bilangan tersebut dapat berarti:

1 * 2^7 + 1 * 2^6 + 1 * 2^5 + 1 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0

= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1

= 255

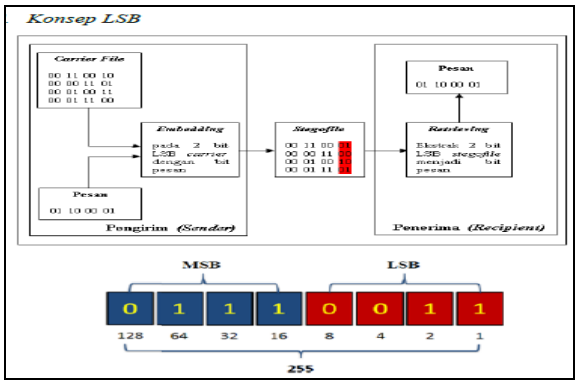
Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan least significant bit (bit yang paling tidak berarti), sedangkan bagian paling kiri bernilai 128 dan disebut dengan most significant bit (bit yang paling berarti).Least significant bit sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain, salah satu yang memanfaatkan Least significant bit sebagai metode penyembunyian adalah steganografi audio.

Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image 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 bitmap 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 bitmap 24 bit kita dapat menyisipkan 3 bit data.

Kekurangan dari LSB Invertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion 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.



Gambar 5 : Least Significant Bit

Berikut adalah konsep *Significant Bit.*
Untuk setiap byte pesan kita harus :

a. Ambil pixel

b. Dapatkan bit pertama dari byte pesan

c. Dapatkan salah satu komponen warna pixel

d. Dapatkan bit pertama dari komponen warna

e. Jika warna bit berbeda dari bit pesan, set/reset

f. Lakukan hal yang sama untuk tujuh bit lainnya.

2. STEGGER

Stegger adalah aplikasi program yang digunakan untuk membuat pesan pengiriman data lewat penyisipan text di8 dalam gambar, yang mana gambar sumber akan berubah menjadi gambar yang berextension png dan stegger ini merupakan koding program open source yang berbasis web yang di buat dengsn program php dan dalam penelitian ini penulis mengembangkan design dengan style CSS untuk lebih menarik dan mudah di mengerti.

Stegger mengambil keuntungan dari konsep dasar gambar untuk menyembunyikan data dengan cara mengubah nilai setiap warna primer yang ada pada setiap pixel baik 1 atau 0. Seperti yang kita tahu bahwa semua digital data hanya berupa urutan dari kedua angka ini yakni 1 dan 0, ada beberapa cara untuk mengubah sebuah 1 dan 0, cara yang digunakan oleh stegger adalah mengubah angka berdasarkan urutan ganjil maupun genap. Langkah ini memungkinkan kita untuk menyimpan 1 bit data pada setiap

warna primer yang berarti kita bisa menyimpan 3 bit symbol data didalam setiap pixels.

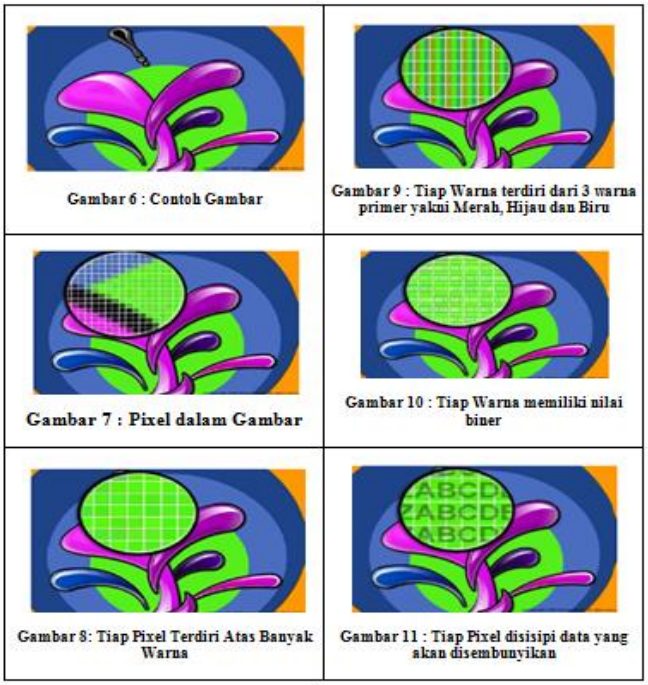
Sekarang 3 bit per pixels terdengar kurang untuk menyembunyikan data. Tapi satu hal yang perlu di perhatikan adalah jika sebuah gambar dengan ukuran 800 x 600 pixels mempunyai 480000 pixels. Berarti kita bisa menyimpan sekitar 1440000 bit data atau sekitar 175 KB.

Terdapat beberapa limitasi pada metode ini. File gambar yang bisa digunakan adalah gambar yang lossless atau dengan katalain gambar yang memanfaatkan semua bit. Jika tidak maka semua data yang secara simbolik tersimpan di dalam gambar akan terhapus atau hancur. Oleh sebab itu metode ini tidak bisa digunakan pada gambar GIF dan JPEG oleh sebab itu Stegger menyimpan semua gambar yang terencode sebagai PNG.

PNG merupakan ekstensi untuk file gambar dengan kualitas baik,ringkas,kapasitas penyimpanan terkompresi untuk gambar raster, PNG Menyediakan paten yang bebas untuk sebagai solusi alternative pengganti GIF dan TIFF seperti yang banyak digunakan. Gambar dengab Warna Terindex, Grayscale,Warna Asli di dukung dengan file extensi ini

Selain itu terdapatnya sebuah tambahan alpha channel untuk mengukur kedalaman gambar antara 1 sampai 16 bit. PNG dirancang untuk dapat di lihat pada kebanyakan aplikasi online seperti world wide web, dimana dapat di stream pada tampilan yang berubah ubah. PNG merupakan file yang sangat kokoh , disamping menyediakan fasilitas integrity checking yang berguna untuk memeriksa keutuhan file. PNG juga dapat menyimpan Gamma dan kromatisitas data untuk meningkatkan pencocokan pada platform warna yang berbeda.

Di bawah ini adalah proses penyisipan pesan ke dalam gambar dengan proses ekripsi, dekripsi dengan disertai kunci untuk bisa membuka gambar tersebut,



Gambar 6 : Contoh Gambar

Gambar 9 : Tiap Warna terdiri dari 3 warna primer yakni Merah, Hijau dan Biru

Gambar 7 : Pixel dalam Gambar

Gambar 10 : Tiap Warna memiliki nilai biner

Gambar 8: Tiap Pixel Terdiri Atas Banyak Warna

Gambar 11 : Tiap Pixel disisipi data yang akan disembunyikan

Kita bisa menyimpan tiga karakter data dalam 8 pixel dengan asumsi tiap karakter mengambil tempat sampai satu byte yang terdiri dari 8 bit. Sebagai contoh, karakter ‘A’ pada gambar diatas disimpan dalam format biner 00001010.

3. ENKRIPSI

a. ENKRIPSI

Untuk meembuat keamanan berlapis, ditambahkan enkripsi di dalam steganografi. Enkripsi sendiri adalah

proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa "kunci" yang telah ditentukan sebelumnya. Enkripsi banyak digunakan dalam kepentingan militer maupun agen pemerintah yang memang bertujuan untuk menjaga kerahasiaan informasi. Namun saat ini enkripsi telah digunakan untuk kebutuhan yang lebih luas, seperti pembayaran online untuk situs e-commerce.

Enkripsi mempunyai algoritma untuk mengenkripsi data. Data yang telah terenkripsi disebut sebagai *ciphertext*. Rumus ini memerlukan sebuah variabel untuk mengembalikan data tersebut kembali ke bentuk asal. Variabel ini biasa disebut kunci. Tanpa kunci, seseorang sangat sulit bahkan hampir tidak mungkin, untuk dapat memecahkan kode enkripsi tersebut. Maka kunci ini memegang peranan vital di dalam enkripsi.

Enkripsi terbagi menjadi dua: simetris dan asimetris (juga disebut sebagai public key). Enkripsi simetris memungkinkan sebuah file dijalankan melalui program dan membuat sebuah kunci untuk mengacak file tersebut. Kemudian file terenkripsi dan kunci dikirimkan secara terpisah kepada penerima. Penerima menjalankan aplikasi enkripsi yang sama dan menggunakan kunci yang diberikan untuk menyatukan kembali file yang telah diacak. Kelebihan enkripsi simetris adalah sangat mudah dan sangat cepat dalam penggunaannya, tetapi tidak seaman enkripsi asimetris, karena jika kunci tersebut jatuh ke tangan orang lain, maka mudah untuk menyatukan file.

Berbeda dengan enkripsi simetris, enkripsi asimetris lebih rumit tapi lebih aman. Hal ini dikarenakan dibutuhkan dua kunci yang saling berhubungan untuk membuka file. Kunci tersebut adalah kunci publik dan kunci pribadi. Kunci publik disediakan bagi siapa saja yang ingin dikirimkan informasi yang terenkripsi. Namun, kunci tersebut hanya dapat digunakan untuk mengkodekan data. Jika ingin mendekodekan data, maka dibutuhkan kunci pribadi yang disimpan oleh pemilik kunci. Kelebihan dari enkripsi asimetris adalah tingkat keamanannya sangat tinggi, tapi kekurangannya adalah dibutuhkan proses dan waktu yang lebih banyak untuk mengenkripsi dan mendekripsi data.

b. MD5 Checsum

Message-Digest algortihm (MD5) adalah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit (sumber: wikipedia). Password MD5 merupakan salah satu perlindungan kepada user dalam menggunakan fasilitas internet di dunia maya, terutama yang berhubungan dengan password, karena sebuah password adalah kunci yang sangat berharga bagi kita yang sering melakukan aktifitas di dunia maya, bisa kita bayangkan apabila seorang cracker mampu menjebol database website misalnya situs pemerintah yang sifatnya sangat rahasia kemudian cracker tersebut mencari bug dari situs targetnya dengan berbagai macam metode/teknik hacking (seperti : SQL Injection, Keylogger, Social Engineering, Trojan Horse, DDOS d.l.l) supaya cracker bisa menembus ke database dan mendapatkan password korbannya dalam bentuk hash, dan kalau berhasil mencuri passwordnya dalam bentuk hash yang totalnya berjumlah 32bit (contoh hash :

fdf0ef0ea5c1620f77107f3f1047fb4c)
maka dengan mudah password hash hasil encrypt MD5 tersebut tinggal di decrypt ke dalam bentuk plain text (teks biasa) dengan menggunakan tools/software yang bisa didownload gratis dari paman google maupun website penyedia layanan decrypt password hash MD5 ke password yang sebenarnya, dengan demikian secara otomatis sang cracker pun dengan leluasa melakukan semua hal yang dia inginkan seperti mencuri data, merubah data, mengganti tampilan suatu website (Deface) dan bahkan ada yang hanya mendiamkannya saja karena maksud utamanya adalah untuk mengetes security dari situs targetnya saja dan untuk memenuhi rasa penasarannya sampai dia bisa menembus database nya dan tidak berniat untuk merusak, setelah bisa ditembus databasenya ditinggalkan begitu saja , biasanya hal tersebut dilakukan oleh seorang hacker golongan putih (WhiteHat).

Sejarah singkat MD5 di mulai pada tahun 1991 yang didesain oleh Prof. Ronald Rivest dari universitas di Amerika Serikat yaitu MIT, Prof. Ronald Rivest mendesain MD5 karena telah ditemukan kelemahan pada MD4 yang ditemukan Hans Dobbertin. Pada Tahun 1996 Hans Dobbertin menemukan sebuah kerusakan/celah pada fungsi kompresi MD5, namun hal ini bukanlah serangan terhadap hash MD5 sepenuhnya, sehingga dia mengumumkan untuk para pengguna kriptografi menganjurkan supaya mengganti dengan WHIRLPOOL, SHA-1, atau RIPEMD-160.

Namun lambat laun MD5 sudah tidak bisa diandalkan lagi karena hash hasil encrypt MD5 mulai menampakkan kerusakannya dan sudah diketahui rahasia algoritma pada MD5, hal tersebut ditemukan kerusakannya pada tanggal 17 Agustus 2004 oleh Xiaoyun Wang, Dengguo Feng, Xuejia Lay dan Hongbo Yu, kalau dilihat dari namanya mereka berasal dari negri tirai bambu China, sekedar info saja bahwa serangan yang mereka lakukan untuk bisa men-decrypt hash MD5 ke plain text hanya membutuhkan waktu satu jam saja, dengan menggunakan IBM P690 cluster.

c. SHA Checsum

Secure Hash Agoritma (SHA) merupakan slah satu algoritma fungsi hash yang di gunakan . SHA adalah fungsi hash satu-arah yang di buat oleh NIST dan di gunakan bersama DSS (digital signature standar). SHA didasarkan pada MD4 yang dibuat oleh Ronald L.Rivest . SHA di sebut aman (secure) karena di rancang sedimikian rupa sehingga secara komputasi tidak mungkin menemukan pesan yang berkoresponden dengan message di gest yang di brikan.

Langkah-langkah pada SHA-1 adalah sebagai berikut:

a. Melakukan padding terhadap pesan sehingga panjangnya adalah 448 modulus 512.
b. 64 bit sisanya adalah representasi biner dari panjang pesan.
c. Melakukan inisialisasi5 word buffer (160 bit)A, B, C, D, dan E dengan nilai A=67452301, B=efcdab89,

C=98badcfe, D= 10325476, dan E=c3d2e1f0.

d. Memproses pesan dalam blok-blok 16 word (512 bit) dengan ketentuan
e. Ekspansi 16 words menjadi 80 words dengan teknik mixing dan shifting.
f. Menggunakan 4 round dari 20 operasi bit pada blok pesan dan buffer.
g. Menambahkan output dengan input untuk mempeoleh nilai buffer yang baru
h. Output nilai hash adalah nilai terakhir dari buffer.

Gambar 12 : Overview Untuk Encode aplikasi

4. SECRYPT

Untuk mengamankan data atau informasi yang dikirim, data perlu harus di enkripsi dan tujuannya bila nanti mencoba membuka data yang dikirim perlu dengan kata kunci yang di sebut secryp.

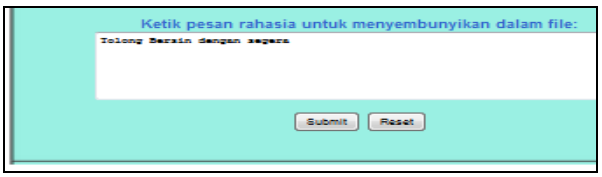
Gambar 13 : Upload gambar

IV. IMPLEMENTASI

1. Proses Encode

Berikut ini adalah mekanisme *encoding* dari program (http://prismasanjaya.sch.id/?module=donload&id=A), yang memiliki fungsi steganografi dan enkripsi berbasis web untuk diuji coba :

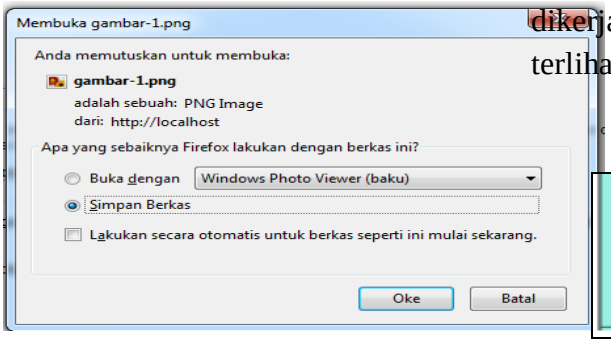
Jika telah dimasukkan file gambar yang ingin disisipi pesan kemudian aplikasi memerintahkan untuk memasukan kata kunci seperti yang ada pada gambar di atas. Setelah itu dilakukan penginputan pesan sebagai berikut:



Gambar 14 Pesan metode MSB

Langkah terakhir yang perlu dilakukan adalah men-*submit* pesan tersebut. Setelah

semua langkah itu dilakukan maka akan muncul informasi sebagai berikut :



Gambar 15 : Konfirmasi

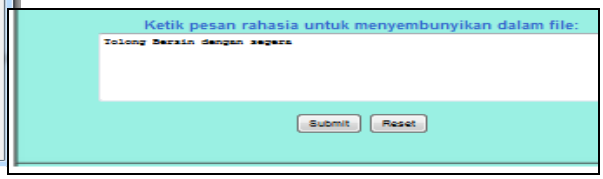
Setelah gambar yang berisi pesan terdownload, setelah dibuka maka yang akan tertampil adalah isi dari pesan yang sudah di masukan sebelumnya seperti yang terlihat di gambar 16.

Gambar Sebelum di encode	Gambar Sesudah di encode
	

Gambar 16 : Perbandingan hasil gambar

2. Proses Decode

Kalau melihat gambar tersebut sulit di bedakan, padahal gambar tersebut sudah di enkripsi hasil proses stegger, gambar sudah di sisipi berupa text " Tolong Beresin dengan Segera" pesan pada gambar 15 mengalami enkripsi yang dikerjakan oleh secrypt seperti yang terlihat di gambar 17 berikut :

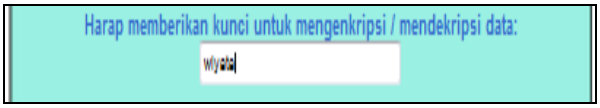


Gambar 17 : Hasil Enkripsi Pesan

Berikut ini adalah layout untuk proses retrieve gambar :

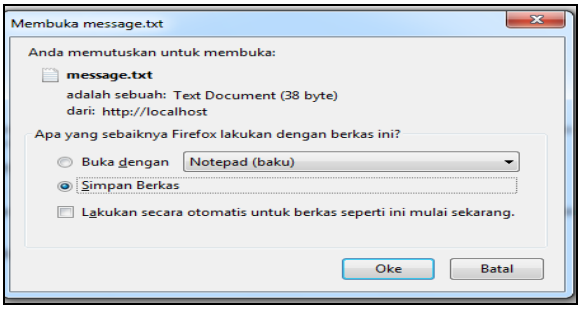
Gambar 18 : Overview Untuk Decode Gambar

Setelah itu yang perlu dilakukan adalah mengupload gambar yang telah berisi pesan rahasia



Gambar 19 : Input Sercet Key

Setelah dilakukan submit maka pesan secara otomatis terdownload



Gambar 21 : Pesan Rahasia yang terdownload

Seperti yang terlihat pada gambar 16, secara kasat mata gambar biasa dengan gambar berisi pesan rahasia tidak memiliki perbedaan, namun bila dilakukan komparasi secara lebih mendalam maka dapat kami temukan perbedaannya. Komparasi yang kami lakukan adalah komparasi secara objective.. Berikut 5 contoh hasil encode dan decode :

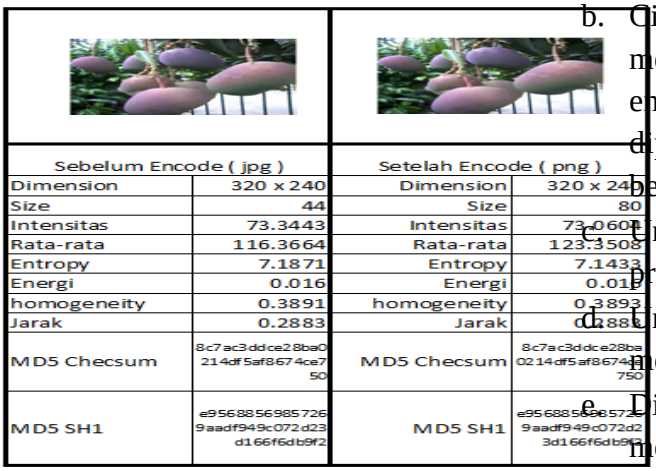
Tabel 1 : Komparasi Sebelum dan Sesudah Encode

			
Sebelum Encode (jpg)		Setelah Encode (png)	
Dimension	320 x 240	Dimension	320 x 240
Size	43	Size	86
Intensitas	74.3443	Intensitas	74.0604
Rata-rata	126.3664	Rata-rata	126.3508
Entropy	7.8787	Entropy	7.9263
Energi	0.016	Energi	0.016
homogeneity	0.3891	homogeneity	0.3893
Jarak	0.2883	Jarak	0.2883
MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750	MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750
MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2	MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2

Tabel 2 : Komparasi Sebelum dan Sesudah Encode

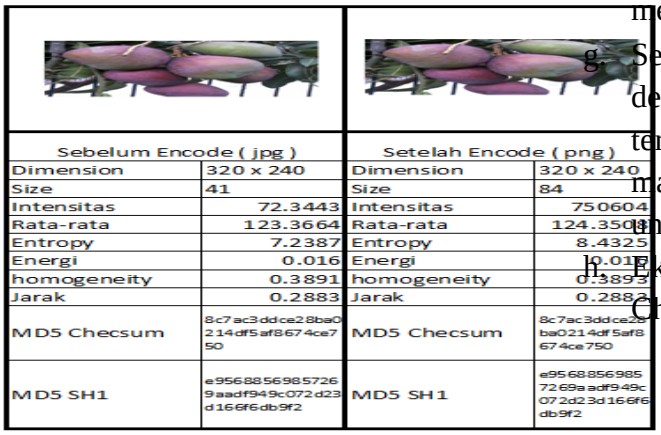
			
Sebelum Encode (jpg)		Setelah Encode (png)	
Dimension	320 x 240	Dimension	320 x 240
Size	40	Size	80
Intensitas	75.8353	Intensitas	76.4234
Rata-rata	125.4356	Rata-rata	127.5463
Entropy	7.8787	Entropy	7.9263
Energi	0.016	Energi	0.016
homogeneity	0.3891	homogeneity	0.3893
Jarak	0.2883	Jarak	0.2883
MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750	MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750
MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2	MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2

Tabel 3 : Komparasi Sebelum dan Sesudah Encode



Sebelum Encode (jpg)		Setelah Encode (png)	
Dimension	320 x 240	Dimension	320 x 240
Size	44	Size	80
Intensitas	73.3443	Intensitas	73.0604
Rata-rata	116.3664	Rata-rata	123.3508
Entropy	7.1871	Entropy	7.1433
Energi	0.016	Energi	0.016
homogeneity	0.3891	homogeneity	0.3893
Jarak	0.2883	Jarak	0.2883
MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750	MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750
MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2	MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2

Tabel 4 : Komparasi Sebelum dan Sesudah Encode



Sebelum Encode (jpg)		Setelah Encode (png)	
Dimension	320 x 240	Dimension	320 x 240
Size	41	Size	84
Intensitas	72.3443	Intensitas	750604
Rata-rata	123.3664	Rata-rata	124.3508
Entropy	7.2387	Entropy	8.4325
Energi	0.016	Energi	0.016
homogeneity	0.3891	homogeneity	0.3893
Jarak	0.2883	Jarak	0.2883
MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750	MD5 Checsum	8c7ac3ddce28ba0214df5af8674ce750
MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2	MD5 SH1	e95688569857269aadf949c072d23d166f6db9f2

V. KESIMPULAN

Strategi keamanan berlapis pada steganografi dengan menggunakan metode LSB dengan pemanfaatan algoritma stegger dan enkripsi menggunakan secrypt telah meningkatkan keamanan informasi atau data yang disisipkan pada citra digital.

Berikut kelebihan dari keamanan berlapis ini:

a. Metode LSB dapat menyembunyikan pesan yang sulit untuk dipecahkan.
b. Citra digital yang disisipkan dengan metode LSB ditambah dengan enkripsi akan makin sulit untuk dipecahkan oleh orang yang tidak berkepentingan.
c. Untuk mengetahui matrik di gunakan program MATLAB
d. Untuk membuat ecoding menggunakan PHP
e. Dibutuhkan *secret key* untuk mendekodekan enkripsi yang di*generate* dengan menggunakan secrypt.
f. Kunci untuk mendekodekan enkripsi secrypt berupa citra digital asli sebelum disisipi pesan, sehingga tidak menimbulkan kecurigaan.
g. Secret Key dikirimkan terpisah dengan pesan rahasia sehingga bila terjadi hal-hal yang tidak diinginkan maka kemungkinan pesan tersebut untuk terpecahkan masih sangat kecil.
h. Ekcripsi menggunakan MD5 Checksum dan SHA 1 Checksum

VI. DAFTAR PUSTAKA

[1] Awcock, G.W. 1996. Applied Image Processing.Singapore. McGraw-Hill Book.

[2] Pengertian dan Jenis Enkripsi, Shvoong, http://id.shvoong.com/

[3] Provos, Niels, Honeyman. Peter. (2003), “Hide And Seek: An Introduction To Steganography”, IEEE Computer Society.

[4] Raghunathan, A., 2011. *Proofs in Cryptography*, Stanford University.

[5] Gies Masita Arini, 2012, Pengamanan Pesan Steganografi dengan Metode

LSB Berlapis Enkripsi dalam PHP, Universitas Budi Luhur.

[6] Adira, 2110, Analisis dan Perancangan Aplikasi Steganografi pada Citra Digital menggunakan metode LSB, UIN Syarif Hidayatullah.

[7] Adipura Sejati, 2010, Studi dan Perbandingan Steganografi Metode EOF dengan DCS, ITB

[8] Paul Gunawan Hariyanto, 2011, Studi Dan Implementasi Steganografi Pada Video Digital Di Mobile Phone Dengan DCT Modification,ITB

[9] Rizqi Firmansyah, 2011, Implementasi Kriptografi Dan Steganografi Pada Media Gambar Dengan Menggunakan Metode Des Dan Region-Embed Data Density, ITB