PENYISIPAN PESAN RAHASIA PADA CITRA DIGITAL DENGAN TEKNIK STEGANOGRAFI

Catur Iswahyudi, Iwan Risgianto
Jurusan Teknik Informatika
Institut Sains & Teknologi AKPRIND Yogyakarta
Jl. Kalisahak No. 28 Komplek Balapan Yogyakarta
E-mail : catur@staff.akprind.ac.id, gaza_kawai@telkom.net

ABSTRACT

Steganography is a concealment technique of secret data into a place of (media) so that hidden data difficult to recognize by human being indera. Steganography require two priority that consist of hidden secret data and temporary. Digital Steganography use digital media as temporary of image, voice, video and text. Secret data which hide also can in the form of image, voice, video and text. Implementation of Steganography for example aim to disguise existence of difficult secret data and to protect product copyrights.

In this research, method used is usage of two colour binary picture media as carrier media input secret data. Divided media draw input data in fairish blocks of n x m, this technique can insert secret information into one block of maximum counted 1 bit so that change that happened do not seen clearly.

Designed application program have ability to hide secret message and reveal the message, consisting of Hide: concealment process of secret message into host (carrier file in the form of picture) and Unhide: process of intake and read message of picture file. Both above process is the part of an entire system called Steganosystem.
Key words: *encryption, data hiding, steganography*

INTISARI

Steganografi merupakan teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit untuk dikenali oleh indera manusia. Steganografi membutuhkan dua *priority* yaitu wadah penampung dan data rahasia yang disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung misalkan citra, suara, teks dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks dan video. Penggunaaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi dan melindungi hak cipta suatu produk.

Dalam penelitian ini, metode yang digunakan adalah penggunaan media gambar biner dua warna sebagai data masukan media pembawa pesan rahasia. Dengan membagi media gambar data masukan dalam blok-blok berukuran m x n, teknik ini diharapkan dapat menyisipkan informasi rahasia ke dalam satu blok maximum sebanyak 1 bit sehingga perubahan yang terjadi tidak terlihat mencolok.

Program aplikasi yang dirancang memiliki kemampuan untuk menyembunyikan pesan rahasia dan memunculkannnya kembali pesan tersebut, yang terdiri dari Hide: proses penyembunyian pesan rahasia ke dalam host (file pembawa pesan berupa gambar) dan UnHide: proses pengambilan dan pembacaan pesan dari file gambar.

Kedua proses di atas merupakan bagian dari suatu sistem keseluruhan yang disebut Steganosistem.

Kata kunci: *enkripsi, data hiding, steganography*

PENDAHULUAN

Steganografi adalah teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit untuk dikenali oleh indera manusia. Steganografi membutuhkan dua *priority* yaitu wadah penampung dan data rahasia yang disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung misalkan citra, suara, teks dan video. Data rahasia yang di sembunyikan juga dapat berupa citra, suara, teks dan video. Penggunaaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi dan melindungi hak cipta suatu produk.

Steganografi berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan (Stellars,1996). Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Digital Steganografi

Steganografi juga diterapkan dalam dunia digital sehingga berkembanglah berbagai seni dan algoritma steganografi modern dengan dukungan kecepatan teknologi komputasi pada media komputer. Banyak format digital yang dapat digunakan dalam steganografi. Format yang digunakan antara lain: (1) Format image : bitmap, gif, png dan jpeg, (2) Format audio : wav dan mp3, (3) Format lain : teks file, html dan pdf.

Pada komputer, gambar yang tampil di layar monitor merupakan kumpulan *array* yang merepresentasikan intensitas cahaya yang bervariasi pada *pixel*. *Pixel* adalah titik di layar monitor yang dapat diatur untuk menampilkan warna tertentu. *Pixel* disusun di layar monitor dalam susunan baris dan kolom. Susunan pixel dalam baris dan kolom ini yang dinamakan resolusi monitor. Melalui *pixel* inilah suatu gambar dapat dimanipulasi untuk menyimpan informasi yang akan digunakan sebagai salah satu pengimplementasian steganografi.

Steganografi pada media digital *file* gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada *file* gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada *file* gambar yang telah disisipi pesan rahasia.

Metode Penyembunyian Data

Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam *bit* rendah (*least significant bit*) pada data *pixel* yang menyusun file gambar BMP 24 bit tersebut.

Pada *file* gambar BMP 24 bit setiap *pixel* pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 *bit* (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Informasi dari warna biru berada pada *bit* pertama sampai *bit* delapan, dan informasi warna hijau berada pada *bit* sembilan sampai dengan *bit* 16, sedangkan informasi warna merah berada pada *bit* 17 sampai dengan *bit* 24.

Metode penyisipan LSB (*least significant bit*) ini adalah menyisipi pesan dengan cara mengganti *bit* ke 8, 16 dan 24 pada representasi biner *file* gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap *pixel* file gambar BMP 24 *bit* dapat disisipkan 3 *bit* pesan, misalnya terdapat data raster original file gambar adalah sebagai berikut:

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya kedalam *pixel* di atas maka akan dihasilkan

00100111 11101001 11001000
00100111 11001000 11101000
11001000 00100111 11101001

Terlihat pada *bit* ke-8, 16 dan 24 diganti dengan representasi biner huruf A, dan hanya tiga *bit* rendah yang berubah (cetak tebal), untuk penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada *file* gambar yang sudah diisi pesan rahasia jika dibandingkan dengan *file* gambar asli sebelum disisipi dengan pesan rahasia.

Sebelum melakukan penggantian bit LSB, semua data citra yang bukan tipe 24-bit diubah menjadi format 24-bit. Jadi, setiap dua *pixel* sudah mengandung komponen RGB. Setiap *byte* di dalam data bitmap diganti satu *bit* LSB-nya dengan *bit* data yang disembunyikan. Jika *byte* tersebut merupakan komponen hijau (G), maka penggantian 1 *bit* LSB-nya hanya mengubah sedikit kadar warna hijau, dan perubahan ini tidak terdeteksi oleh mata manusia.

Pada citra 24-bit, karena data *bitmap* pada citra 24-bit sudah tersusun atas komponen RGB, maka tidak perlu dilakukan perubahan format. Setiap *byte* di dalam data *bitmap* diganti satu *bit* LSB-nya dengan *bit* data yang akan disembunyikan.

Perubahan Jumlah Warna

Pada citra 8-bit, jumlah warna terbatas, hanya 256 warna. Pengubahan format citra 8-bit menjadi 24-bit akan menghasilkan warna baru yang semula tidak terdapat di dalam palet RGB. Setiap elemen RGB pada tabel palet berpotensi menjadi 8 warna berbeda setelah proses pergantian bit LSB. Hal ini karena setiap data bitmap terdiri atas 3 byte, maka tersedia 3 *bit* LSB untuk penggantian. Penggantian 3 *bit* LSB menghasilkan 2^3 = 8 kombinasi warna . dengan demikian, steganografi pada citra 256 warna berotensi menghasilkan 256 x 8 = 2048 warna.

Untuk menghindari kelebihan warna pada 256, maka sebelum proses penyembunyian data, warna citra 8-bit diturunkan terlebih dahulu menjadi 32 warna (jika jumlah warnanya kurang dari 32, tidak perlu dilakukan penurunan warna). Dengan demikian, jika setiap warna menghasilkan 8 warna baru, jumlah warna seluruhnya maksimum 32 x 8 = 256 warna.

Ukuran Data Yang Disembunyikan

Ukuran data yang disembunyikan bergantung pada ukuran citra penampung. Pada citra 8-bit yang berukuran 256 x 256 pixel terdapat 65536 *pixel*, setiap *pixel* berukuran 1 *byte*. Setelah diubah menjadi citra 24-bit, ukuran data *bitmap* menjadi 65536 x 3 = 196608 *byte*. Karena setiap *byte* hanya bisa menyembunyikan satu *bit* di LSB-nya, maka ukuran data yang akan disembunyikan di dalam citra maksimum 196608/8 = 24576 *byte*. Ukuran ini harus dikurangi dengan panjang nama berkas, karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama berkasnya.

Semakin besar data yang disembunyikan di dalam citra, semakin besar pula kemungkinan data tersebut rusak akibat manipulai pada citra penampung.

Teknik Pengungkapan Data

Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau *extraction*). Posisi *byte* yang menyimpan *bit* data dapat diketahui dari bilangan acak yang dibangkitkan dari PRNG. Karena algoritma kriptografi yang digunakan menggunakan kunci pada proses enkripsi, maka kunci yang sama digunakan untuk membangkitkan bilangan acak. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, *bit-bit* rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

Format Berkas Bitmap

Citra disimpan di dalam berkas (*file*) dengan format tertentu. Format citra yang baku di lingkungan sistem operasi Microsoft Windows dan IBM OS/2 adalah berkas *bitmap* (BMP). Saat ini format BMP memang kalah popular dibandingkan format JPG atau GIF. Hal ini karena berkas BMP pada umumnya tidak dimampatkan, sehingga ukuran berkasnya relative lebih besar daripada berkas JPG maupun GIF.

Meskipun format BMP tidak bagus dari segi ukuran berkasnya, namun format BMP mempunyai kelebihan dari kualitas gambar. Citra dalam format BMP lebih bagus daripada citra dalam format yang lainnya, karena citra dalam format BMP umumnya tidak dimampatkan sehingga tidak ada informasi yang hilang. Terjemahan bebas dari *bitmap* adalah pemetaan bit. Artinya, nilai intensitas *pixel* di dalam citra dipetakan ke seumlah bit tertentu. Peta bit yang umum adalah 8, artinya setiap *pixel* panjangnya 8 bit. 8 bit ini merepresentasikan nilai intensitas *pixe*l. Dengan demikian ada sebanyak 2^8 = 256 derajat keabuan, mulai dari 0 sampai 255.

Saat ini ada tiga versi berkas *bitmap* yaitu : berkas *bitmap* versi lama dari Microsoft Windows atau IBM OS/2, berkas *bitmap* versi baru dari Microsoft Windows, dan berkas *bitmap* versi IBM OS/2 (64 byte). Yang membedakan ketiga versi berkas tersebut adalah panjang *header*-nya. *Header* adalah data yang terdapat pada bagian awal berkas citra. Data didalam *header* berguna untuk mengetahui bagaimana citra dalam format *bitmap* dikodekan dan disimpan. Data di dalam header misalnya ukuran citra, kedalaman *pixel*, *offset* ke dalam *bitmap*, dan sebagainya. Setiap berkas *bitmap* terdiri atas *header* berkas, *header bitmap*, informasi palet dan data *bitmap*.

Hasil Eksperimen

Program aplikasi yang dirancang memiliki kemampuan untuk menyembunyikan pesan rahasia dan memunculkannnya kembali pesan tersebut.

a. Program Hide : proses penyembunyian pesan rahasia ke dalam host (file pembawa pesan berupa gambar)
b. Proses UnHide : proses pengambilan dan pembacaan pesan dari file gambar.

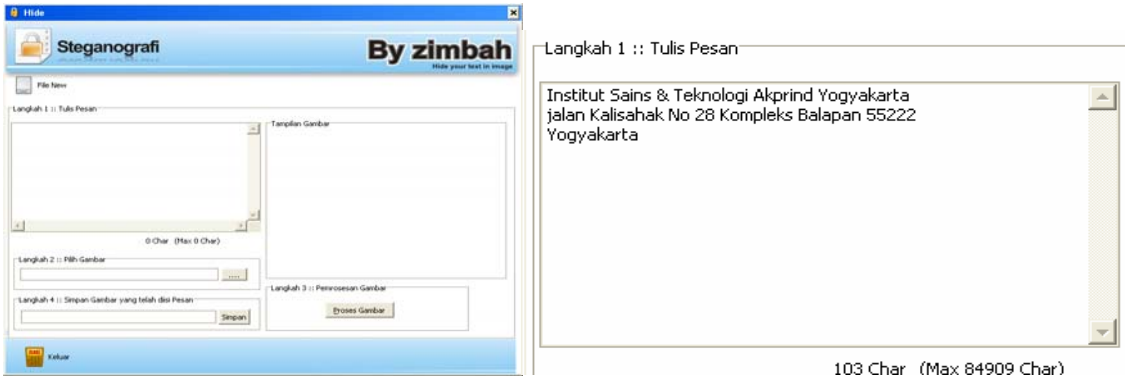
Kedua proses di atas merupakan bagian dari suatu sistem keseluruhan yang disebut Steganosistem.

Penyembunyian Pesan

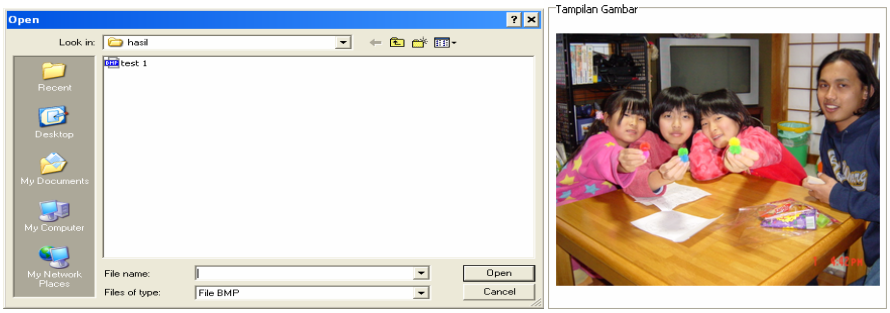
Tahap hiding memberikan keleluasaan bagi user untuk melakukan proses penyembunyian data, diawali dengan menuliskan teks atau pesan yang akan disembunyikan, kemudian memilih gambar sebagai *carrier*.

Penyembunyian Pesan

Tahap hiding memberikan keleluasaan bagi user untuk melakukan proses penyembunyian data, diawali dengan menuliskan teks atau pesan yang akan disembunyikan, kemudian memilih gambar sebagai *carrier*

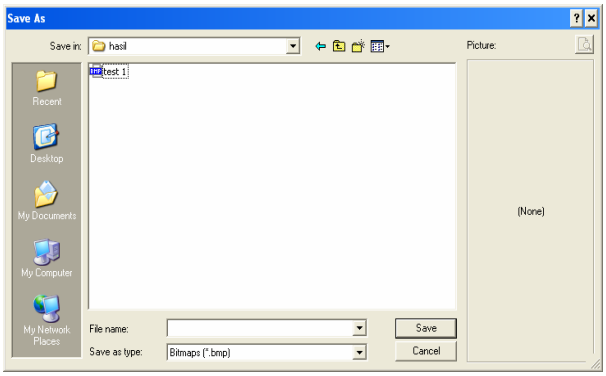


Gambar 1. Penulisan pesan



Gambar 2. Pemilihan citra digital

Proses selanjutnya adalah penyimpanan hasil file image terbaru yang telah terisi oleh pesan dan akan disimpan ke dalam *path* dalam bagian *Simpan gambar yang telah diisi Pesan.*



Gambar 3. Penyimpanan citra digital

Pengungkapan Pesan

Pengambilan file gambar pembawa pesan rahasia dapat dilakukan dengan menggunakan tombol Browse dalam bagian *Pilih Gambar* pada menu Unhide. Dengan menekan tombol ini, proses akan merujuk pada kode program Browse

.

Gambar 4. Pengambilan citra digital

Setelah memilih tombol UnHide maka kotak Pesan akan menampilkan hasil dari pendeteksian sistem informasi tehadap pesan rahasia yang telah disisipkan dalam file image pembawa :

Gambar 5. Tampilan pesan yang disisipkan

Analisa Hasil Keluaran

Setelah dilakukan pengujian program, akan ada perubahan yang terdapat pada file image pembawa pesan yaitu ketika dilihat dalam susunan Heksa, file image pembawa terdapat tanda yang akan membedakan dengan file image sebelum di isi oleh pesan rahasia. Seperti ditunjukkan di bawah ini :

Susunan file image pembawa dilihat menurut susunan Heksanya sebelum diisi pesan rahasia :

```
9F 38 4E 7C 20 4B 7F 1A  ¤¥«´´´®▌▌▌8N| K▌.
7C 9D BF 85 9C BD 65 62  Fy'W▌v Ä|▌¿▌▌½eb
2D 48 22 3A 55 1E 3C 51  u>4C25M -H":U.<Q
B8 C9 C7 C3 CA C7 C1 CA  y▌▌ÃÌÆÀÀ¸ÉÇÃÊÇÁÊ
                         Ç¾ÆÅ¹.
```

Penanda yang diberikan pada file image setelah pesan dimasukkan ke dalamnya:

```
9F 38 4E 7C 20 4B 7F 1A  ¤¥«´´´®▌▌▌8N| K▌.
7C 9D BF 85 9C BD 65 62  Fy'W▌v Ä|▌¿▌▌½eb
2D 48 22 3A 55 1E 3C 51  u>4C25M -H":U.<Q
B8 C9 C7 C3 CA C7 C1 CA  y▌▌ÃÌÆÀÀ¸ÉÇÃÊÇÁÊ
                         Çencr.
```

Ukuran file image sebelum pesan rahasia disisipkan

Ukuran file image setelah pesan rahasia disisipkan

KESIMPULAN

Dari pengujian program diperoleh kesimpulan sebagai berikut :

1. Media yang digunakan sebagai *carrier* pada penelitian ini masih terbatas pada image bertipe .*bmp.
2. Ukuran file baru yang sudah disisipi teks atau pesan tidak berubah
3. Metode penyembunyian pesan rahasia adalah dengan cara menyisipkan pesan rahasia ke dalam bit rendah (LSB) pada byte yang menyusun file image sehingga proses ini tidak mempengaruhi kapasitas & ukuran file host

4. Gambar yang baru tidak memiliki perbedaan jika dibandingkan dengan gambar aslinya sehingga sangat sulit untuk dibedakan oleh penglihatan manusia dikarenakan penyisipan dilakukan dengan mengganti bit-bit terakhir dari masing-masing biner sample data

DAFTAR PUSTAKA

Budi Raharjo, (2005), *Keamanan Sistem Informasi Berbasis Internet*.

Darmawan, M.S. (2003), *Steganografi, Sebuah Pendekatan Baru dalam Pengamanan Data*, http://overclockerindo.com/ moduls.php? name:reviews.

IlmuKomputer.Com (2007), *Free eBook and Tutorial _ Indonesia e-Learning and Distance Learning Community on the Computer Science and Information Technology.htm*

Martina, Inge (2004), *Pemrograman Visual Borland Delphi 7*, PT. Elex Media Komputindo, Jakarta.

Sellar, D. (1996), An Introduction to Steganography, http://www.Cs.Utc.ac.za/courses/cs 400 w/ NIS/ paper 99/d sellars/ stego.htm.

Sukmawan, Budi (2003), *Steganografi*, http: //bdg.Centria.net.id/budslwn/artikel.htm.

Yudha, C. Setiawan (2003), *Trik & Tip Delphi*, Penerbit ANDI,Yogyakarta.