MAKALAH SEMINAR TUGAS AKHIR

TEKNIK PENYEMBUNYIAN DATA RAHASIA DENGAN MENGGUNAKAN CITRA DIGITAL SEBAGAI BERKAS PENAMPUNG

Miftahur Rahim A. A*, Achmad Hidayatno**, R. Rizal Isnanto**

***Abstrak* – Kerahasiaan suatu informasi atau data sangatlah penting agar orang lain yang tidak memiliki hak tidak dapat mengetahui isi dari data atau informasi rahasia tersebut. Tugas akhir ini dilakukan untuk membuat suatu program yang mampu menyembunyikan data rahasia dalam bentuk citra, teks, suara, dan video ke dalam suatu berkas penampung berupa citra digital.**

Pembuatan program dilakukan dengan menggunakan bahasa pemrograman Borland Delphi 7.0. Proses penyembunyiannya diawali dengan mengambil berkas citra penampung, kemudian mengambil data yang akan disembunyikan. Sebelum disembunyikan, terlebih dahulu data tersebut dibuat dalam blok-blok berukuran 64-bit lalu di-XOR-kan dengan inisialisasi dan kunci 64-bit melalui proses enkripsi CBC, sehingga keamanan data rahasia dapat terjaga. Setelah proses enkripsi CBC, barulah data disembunyikan ke dalam berkas citra penampung. Program ini juga dapat mengungkapkan kembali data yang telah disembunyikan ke bentuk aslinya melalui proses dekripsi CBC. Proses penyembunyian data rahasia seperti tersebut termasuk dalam salah satu teknik Steganografi.

Hasil pengujian menunjukkan program berhasil menyembunyikan data rahasia dalam berbagai macam bentuk, asalkan besar data rahasia tidak lebih besar daripada citra penampung. Program juga berhasil mengungkapkan kembali data rahasia yang ada di dalam citra penampung ke bentuk aslinya. Untuk proses Encoder dengan penggunaan 1-bit sampai 4-bit, tampilan citra penampung masih terlihat bagus. Semakin besar jumlah bit yang digunakan, maka perubahan tampilan citra penampung akan semakin terlihat jelas. Kekurangan program ini adalah citra penampung tidak tahan terhadap operasi manipulasi, misalnya pengubahan tingkat kecerahan, pengubahan kontras, pemampatan data, dan sebagainya.

Kata kunci: program, data rahasia, citra digital, berkas, enkripsi CBC.

I. PENDAHULUAN

1.1 Latar Belakang

Keamanan data atau informasi pada komputer tidak hanya tergantung pada *firewall* tetapi keamanan data dari data itu sendiri merupakan hal yang sangat perlu diperhatikan. Jika *firewall* dapat dibobol oleh orang yang tidak memiliki hak maka data rahasia yang dimiliki akan menjadi tidak rahasia lagi.

Oleh karena itu perlu adanya suatu teknik untuk menyembunyikan data rahasia ini agar orang lain yang tidak memiliki hak, tidak akan mengetahui isi dari data rahasia tersebut.

1.2 Tujuan

Tujuan Tugas Akhir ini adalah membuat program yang dapat menyembunyikan suatu data rahasia baik dalam bentuk data citra digital, data teks, data audio, atau data video ke dalam berkas penampung yang berupa citra digital dan juga dapat mengungkapkan kembali data rahasia yang ada di dalam citra penampung menjadi ke bentuk aslinya. Program ini diharapkan dapat membantu semua orang agar data rahasia yang dimiliki tidak diketahui oleh orang lain yang tidak memiliki hak.

1.3 Batasan Masalah

1. Penyembunyian data rahasia melalui proses Steganografi dengan menggunakan citra digital sebagai berkas penampung.
2. Data rahasia yang disembunyikan dapat berupa data citra digital, data teks, data audio, atau data video asalkan besar data rahasia lebih kecil atau sama dengan besar perhitungan data maksimal yang dapat disembunyikan.
3. Menggunakan algoritma enkripsi CBC untuk menyandikan data rahasia sebelum masuk ke proses steganografi dan menggunakan algoritma dekripsi CBC untuk proses mengungkapkan data rahasia ke bentuk aslinya.
4. Pembuatan program dilakukan dengan menggunakan bantuan bahasa pemrograman Borland Delphi 7.0.

II. STEGANOGRAFI

Steganografi adalah teknik menyembunyikan data rahasia di dalam media digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain. Steganografi membutuhkan dua bagian yang sangat penting yaitu berkas atau media penampung dan data rahasia yang akan disembunyikan. Penggunaan steganografi adalah untuk menyamarkan keberadaan data rahasia sehingga sulit di deteksi, dan juga dapat melindungi hak cipta dari suatu produk. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, dengan steganografi maka *ciphertext* yang dihasilkan dari kriptografi dapat disembunyikan

* Mahasiswa Jurusan Teknik Elektro UNDIP
** Staf Pengajar Jurusan Teknik Elektro UNDIP

sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diungkapkan kembali persis sama seperti aslinya.

2.1 Berkas Penampung

Steganografi digital menggunakan media digital sebagai berkas penampung, misalnya citra digital, teks, audio, atau video. Pada Tugas Akhir ini proses steganografinya menggunakan citra digital sebagai berkas penampung.

2.1.1 Citra Digital

Secara harfiah citra adalah gambar pada bidang dua dimensi. Ditinjau dari sudut pandang matematis, citra merupakan fungsi malar (*continue*) dari intensitas cahaya pada bidang dua dimensi. Sumber cahaya menerangi objek, objek mementulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata pada manusia, kamera pemindai, dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam. Citra sebagai keluaran dari suatu sistem perekaman data dapat bersifat optik berupa foto, analog berupa sinyal video seperti gambar pada monitor televisi, dan digital yaitu yang dapat langsung disimpan pada suatu pita magnetik. Agar dapat diolah dengan komputer, maka suatu citra harus diwakili secara numerik dengan nilai-nilai diskret. Perwakilan citra dari fungsi malar menjadi nilai-nilai diskret disebut digitalisasi. Citra yang dihasilkan inilah yang disebut dengan citra digital.

2.1.2 Format Citra Digital

Citra digital disimpan dalam berkas dengan menggunakan format tertentu. Format citra yang baku dilingkungan sistem operasi Microsoft Windows dan IBM OS/2 adalah berkas **bitmap** (**BMP**). Saat ini format **BMP** memang kalah populer dibandingkan format **JPG** atau **GIF**, hal ini karena berkas **BMP** tidak dimampatkan sehingga ukuran datanya relatif besar daripada berkas **JPG** maupun **GIF**. Meskipun format **BMP** memiliki kekurangan dari segi ukuran tetapi format **BMP** memiliki kelebihan dari segi kualitas gambar, karena tidak dimampatkan sehingga tidak ada informasi yang hilang. Berkas **bitmap** warna 24 bit mempunyai tiga komponen warna yaitu **RGB** (*Red, Green, Blue*). Tiap-tiap komponen tersebut terdiri 8 bit. Karena 8 bit tersebut memiliki kombinasi 256 warna sehingga jika terdapat 3 komponen warna maka mempunyai 256 x 256 x 256 kombinasi warna. Sehingga jika ada berkas dengan format **bitmap** warna 24 bit dengan ukuran 800 x 600 maka besarnya ukuran berkas bitmap tersebut adalah (800 x 600 x 24) bit. Pada Tugas Akhir ini berkas penampungnya berupa citra digital dengan format **BMP** 24 bit.

2.2 Data/Informasi Rahasia

Informasi atau data rahasia adalah informasi atau data yang karena nilainya, perlu disembunyikan dan dilindungi agar tidak terbuka untuk umum atau jatuh kepada pihak lain. Apabila informasi tersebut diketahui oleh umum/pihak lain maka akan menimbulkan kerugian. Data rahasia dalam media digital dapat berbentuk data citra digital, data teks, data audio, atau data video.

2.3 Steganografi Pada Citra Digital

Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. ***Fidelity***

Mutu dari citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

2. ***Robustness***

Data rahasia yang disembunyikan di dalam citra digital harus tahan terhadap berbagai operasi manipulasi.

3. ***Recovery***

Data rahasia yang disembunyikan di dalam citra digital harus dapat diungkapkan kembali seperti aslinya.

2.4 Teknik Penyembunyian Data

Metode yang paling sering digunakan adalah metode modifikasi LSB (*Least Significant Bit*) pada citra penampung. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang signifikan atau LSB (*Least Significant Bit*). Bit yang cocok untuk diganti adalah bit LSB, sebab penggantian hanya mengubah nilai *byte* tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut di dalam gambar menyatakan warna tertentu, maka perubahan pada bit LSB-nya tidak mengubah warna tersebut secara signifikan.

Sebelum melakukan penggantian bit-bit LSB, semua data citra yang bukan tipe 24 bit diubah terlebih dahulu menjadi format 24 bit. Jadi setiap data piksel sudah mengandung komponen warna merah, hijau dan biru (RGB). Nilai-nilai dari bit-bit yang kurang signifikan atau LSB dari setiap *byte* di dalam data bitmap digantikan dengan bit-bit data yang akan disembunyikan. Jika *byte* tersebut merupakan komponen hijau (G), maka penggantian satu bit LSB-nya hanya mengubah sedikit kadar warna hijau, dan perubahan tersebut tak terdeteksi oleh mata manusia. Ukuran data yang akan disembunyikan tergantung pada ukuran citra penampung. Pada citra 8 bit yang berukuran 256 x 256 piksel terdapat 65536 piksel, setiap piksel berukuran 1 *byte*. Setelah diubah menjadi

citra 24 bit maka ukuran data bitmap menjadi 65536 x 3 = 196608 *byte*. Jika setiap *byte* menyembunyikan 1 bit di LSB-nya, maka ukuran data yang akan disembunyikan di dalam citra adalah 196608/8 = 24576 *byte*. Ukuran data ini harus dikurangi dengan panjang nama berkas, karena penyembunyian data tidak hanya isi data tetapi juga nama berkasnya.

2.4.1 Algoritma Kriptografi

Algoritma kriptografi terdiri atas tiga fungsi dasar yaitu:

1. Enkripsi

Suatu proses dimana pesan asli yang disebut dengan *plaintext* dirubah menjadi kode-kode yang tidak dimengerti yang disebut dengan *ciphertext.*

2. Dekripsi

Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk aslinya (*plaintext*). Algoritma yang digunakan untuk dekripsi berbeda dengan algoritma enkripsi.

3. Kunci

Kunci digunakan untuk melakukan enkripsi dan dekripsi. Kunci berfungsi sama seperti *password.*

Berdasarkan kunci yang digunakan algoritma kriptografi terbagi menjadi 3 yaitu:

1. Algoritma Asimetris

Algoritma Asimetris atau dikenal juga sebagai sistem sandi kunci publik. Disebut sandi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (*public-key*). Namun untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya yang disebut *private-key*.

2. Fungsi *Hashing*

Fungsi *Hashing* sering disebut juga dengan fungsi *hash* satu arah. Fungsi *hash* adalah fungsi yang secara efisien mengubah string masukan dengan panjang berhingga menjadi string keluaran dengan panjang tetap yang disebut nilai *hash*.

3. Algoritma Simetris

Algoritma Simetris adalah sebuah algoritma sandi yang metode menyandi dan membuka sandinya menggunakan kunci yang sama. Sistem sandi simetris sangat baik untuk menyandi data yang berukuran besar maupun kecil sebab sistem sandi ini secara umum diproses lebih cepat dibandingkan dengan sistem lainnya. Sistem sandi simetris modern dapat digolongkan ke dalam 2 kategori berdasarkan cara penyandiannya, yaitu *block cipher* dan *stream cipher*. *Block cipher* menyandi data dengan cara beberapa bit yang digabung menjadi satu blok. Sedangkan *stream cipher* menyandi data secara bit demi bit.

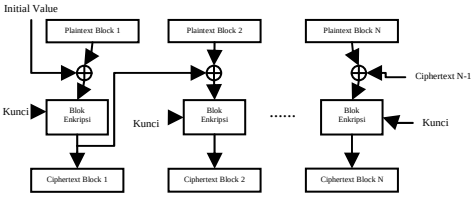
2.4.2 Mode CBC (*Cipher Block Chaining*)

Mode CBC termasuk kriptografi modern karena sudah menggunakan komputer dalam pengoperasiannya. Mode CBC adalah salah satu mode operasi pada *Block Cipher* yaitu masukan dan keluarannya berupa satu blok, dan setiap blok terdiri atas beberapa bit. Biasanya dalam 1 blok *Block Cipher* terdiri atas 64 bit atau 128 bit, dengan masing-masing blok yang saling berhubungan seperti rantai. Dalam proses enkripsi dan dekripsinya, mode CBC menggunakan operasi logika XOR

TABEL 2.1 TABEL KEBENARAN XOR.

Masukan	Keluaran
00	0
01	1
10	1
11	0

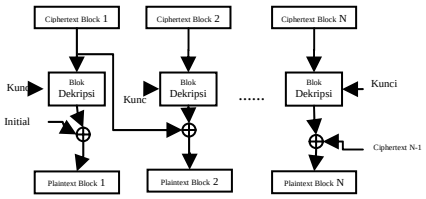
Untuk setiap masukan yang sama yaitu 00 atau 11 maka logika keluarannya adalah *low* (0), sedangkan untuk masukan yang berbeda yaitu 01 atau 10 akan menghasilkan logika keluaran *high* (1), seperti yang terlihat pada Tabel 2.1. Proses dari mode enkripsi CBC diilustrasikan pada Gambar 2.1.



Gambar 2.1 Proses Enkripsi CBC.

2.5 Teknik Pengungkapan Data

Data hasil enkripsi CBC (*ciphertext*) yang disembunyikan di dalam citra penampung dapat dibaca kembali melalui proses desteganografi, yaitu proses kebalikan dari steganografi. Setelah didapatkan data hasil enkripsi CBC (*ciphertext*), dengan menggunakan algoritma dekripsi CBC maka data hasil enkripsi tersebut dapat didekripsi kembali menjadi *plaintext* atau ke dalam bentuk data aslinya seperti ditunjukkan pada Gambar 2.3.



Gambar 2.2 Proses Dekripsi CBC.

III. PERANCANGAN DAN IMPLEMENTASI PROGRAM

Pada perancangan ini digunakan bantuan bahasa pemrograman Borland Delphi 7.0.

3.1 Perancangan *Form* Program

a. *Form* Menu Utama

Pada *form* **Menu Utama** terdiri atas judul Tugas Akhir, nama penyusun, gambar logo Universitas Diponegoro, serta tombol-tombol pilihan menu yaitu tombol **ENCODER** untuk

masuk ke *form encoder*, tombol **DECODER** untuk masuk ke *form decoder*, dan tombol **EXIT** untuk keluar dari program.

b. *Form* ENCODER

Form **ENCODER** terdiri atas tombol-tombol pilihan menu yaitu tombol **OPEN** untuk menampilkan citra penampung, tombol **ENCODE** untuk melakukan proses enkripsi dan steganografi dan sekaligus menampilkan citra hasil steganografi, tombol **SAVE** untuk menyimpan citra hasil steganografi, tombol **BROWSE** untuk mengambil data rahasia, dan tombol **BACK** untuk kembali ke *form* Menu Utama.

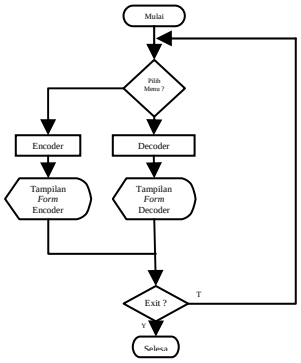
c. *Form* DECODER

Terdiri dari tombol-tombol pilihan menu yaitu tombol **OPEN** untuk menampilkan citra yang mengandung data rahasia, tombol **DECODE** untuk proses desteganografi dan dekripsi serta menampilkan hasil dekripsi dalam bentuk *file* sesuai dengan ekstensinya, tombol **BACK** untuk kembali ke menu utama.

3.2 Perancangan Diagram alir

a. Perancangan digram alir Menu Utama

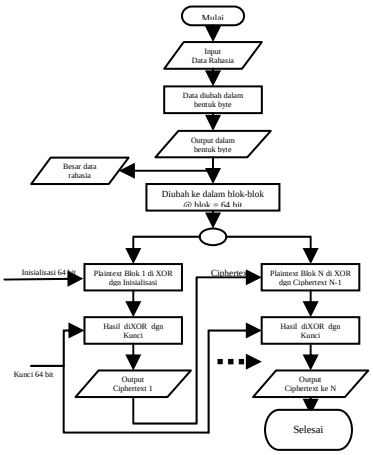
Diagram alir Menu Utama ditunjukkan pada Gambar 3.1.



Gambar 3.1 Diagram alir Menu Utama.

b. Perancangan diagram alir program *Encoder*

Perancangan diagram alir program *encoder* terdiri dari beberapa tahapan yang saling berhubungan. Tahap yang pertama adalah perancangan proses mengambil citra penampung. Tahap yang kedua adalah perancangan untuk proses masukan jumlah bit yang akan digunakan untuk penyisipan data rahasia. Tahap yang ketiga adalah perancangan untuk proses masukan inisialisasi dan kunci yang digunakan untuk proses enkripsi CBC. Tahap yang keempat adalah perancangan proses enkripsi CBC.

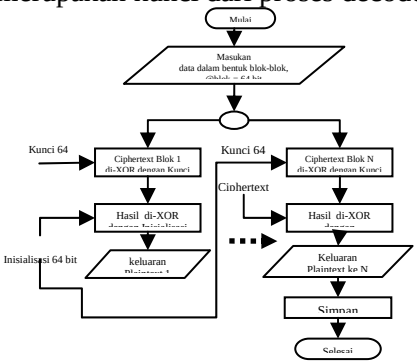


Gambar 3.2 Diagram alir enkripsi CBC.

Tahap yang ke lima adalah perancangan proses alur steganografi.

c. Perancangan diagram alir program *Decoder*

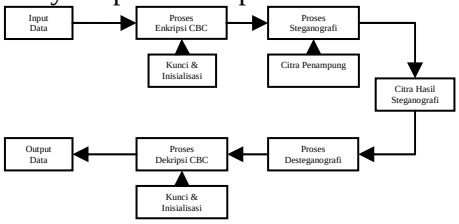
Pada perancangan diagram alir program program *decoder* juga terdiri dari beberapa tahapan yang saling berhubungan. Tahap yang pertama adalah perancangan diagram alir proses pengambilan citra yang mengandung data rahasia. Kedua adalah perancangan diagram alir masukan inisialisasi dan kunci untuk dekripsi CBC. Ketiga adalah perancangan diagram alir proses masukan jumlah bit yang digunakan untuk proses *decoder*. Keempat adalah perancangan diagram alir proses desteganografi. Tahap yang terakhir adalah perancangan diagram alir proses dekripsi CBC yang merupakan kunci dari proses decoder.



Gambar 3.3 Diagram alir proses Dekripsi CBC.

3.3 Implementasi

Tahap implementasi adalah realisasi tahap perancangan program. Proses penyembunyian data rahasia dan proses pengungkapannya secara garis besar alurnya dapat dilihat pada Gambar 3.6.



Gambar 3.4 Proses penyembunyian dan pengungkapan data rahasia.

Pada pembuatan program terdapat tiga tahapan yaitu:

1. Pembuatan program Menu Utama.
2. Pembuatan program Encoder.
3. Pembuatan program Decoder.

IV. PENGUJIAN DAN ANALISIS

4.1 Pengujian Program Dalam Berbagai Macam Bentuk Data Rahasia

4.1.1 Pengujian Menggunakan Data Rahasia Berbentuk Citra Digital

Pada proses pengujian ini data rahasia yang akan disembunyikan adalah dalam bentuk citra digital. Jumlah bit yang digunakan adalah 1 bit. Citra penampung dan data yang disembunyikan ditunjukkan pada Gambar 4.4.

(a)

(b)

Gambar 4.4 Citra Penampung dan data yang akan disembunyikan
(a) Citra penampung: **BapaknIbu.jpg** (1280 x 960 piksel, 121kB).
(b) Data yang akan disembunyikan: **rossi.jpg** (5 kB).

(a)

(b)

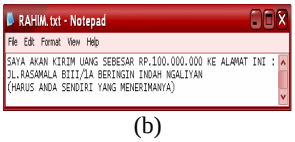
Gambar 4.5 Citra hasil *Encoder* dan Data hasil *Decoder*
(a) Citra hasil *Encode* : **HASIL1.bmp**.
(b) Data hasil *Decoder*: **rossi.jpg** (5 kB).

Dari Gambar 4.4 dan Gambar 4.5 terlihat bahwa setelah penyisipan data rahasia berupa berkas **rossi.jpg**, citra hasil *Encoder* tidak mengalami kerusakan dan masih terlihat sama dengan tampilan aslinya. Data rahasia yang ada didalam citra penampung berhasil diungkapkan kembali terlihat dari Gambar 4.5 (b).

4.1.2 Pengujian Menggunakan Data Rahasia Berbentuk Teks

Pada pengujian ini data rahasia yang akan disembunyikan adalah data teks. Citra penampung dan data yang akan disembunyikan ditunjukkan pada Gambar 4.6.

(a)



(b)

Gambar 4.6 Citra Penampung dan data teks yang akan disembunyikan
(a) Citra penampung**: BapaknIbu.jpg**(1280 x 960 piksel, 121kB).
(b) Data yang akan disembunyikan: berkas **RAHIM.txt**, 143 Byte

(a)

(b)

Gambar 4.7 Citra Hasil *Encoder* dan Data hasil *Decoder*
(a) Citra hasil *Encoder* : **HASIL2.bmp**.
(b) Data hasil *Decoder* : berkas **RAHIM.txt**, 143 *Byte* (ditampilkan pada Notepad).

Pada Gambar 4.6 dan 4.7 citra penampung setelah proses penyisipan data rahasia berbentuk teks tampilannya masih terlihat baik, dan setelah melalui proses *decoder* data **RAHIM.txt** dapat diperoleh kembali dan untuk melihat isi berkas ditampilkan dengan menggunakan bantuan Notepad.

4.1.3 Pengujian Menggunakan Data Rahasia Berbentuk Audio

Pengujian dilakukan dengan menggunakan data rahasia berbentuk audio atau suara. Data audio yang akan disembunyikan adalah data audio dengan nama berkas **hantu.mp3** sebesar 147 kB. Berkas **hantu.mp3** ini akan disembunyikan kedalam citra penampung **BapaknIbu.jpg**. Tampilan citra penampung dan hasil *encoder* dapat dilihat pada Gambar 4.8.

(a)

(b)

Gambar 4.8 Citra penampung dan citra hasil *Encoder*
(a) Citra penampung: **BapaknIbu.jpg** (1280 x 960 piksel, 121kB).
(b) Citra hasil *Encoder*: **HASIL3.bmp**.

Pada Gambar 4.8 (b) citra penampung setelah proses penyisipan data rahasia berbentuk audio tampilannya masih terlihat baik. Setelah melalui proses *decoder* berkas **hantu.mp3** dapat diperoleh kembali dan untuk mendengarkan berkas **hantu.mp3** dapat menggunakan bantuan Winamp. Setelah didengarkan dengan menggunakan bantuan Winamp hasil yang didapatkan baik, tidak ada kerusakan, hasil sama seperti aslinya.

4.1.4 Pengujian Menggunakan Data Rahasia Berbentuk Video

Data rahasia yang akan disembunyikan adalah data video. Contoh pengujian menggunakan data rahasia dengan bentuk berkas ***.3gp**. Data yang akan disembunyikan adalah berkas **sms bang.3gp** sebesar 1,1 MB. Karena ukuran berkas data rahasia yang akan disembunyikan besar maka untuk proses *encoder*nya menggunakan 4 bit. Tampilan citra penampung dan hasil *encoder* dapat dilihat pada Gambar 4.9.

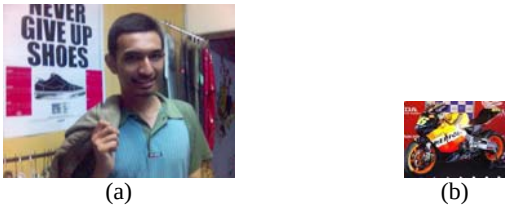
(a) (b)

Gambar 4.9 Citra penampung dan citra hasil *Encoder*
(a) Citra penampung : **BapaknIbu.jpg**
(1280 x 960 piksel, 121kB).
(b) Citra hasil *Encoder* : **HASIL4.bmp**.

Pada Gambar 4.9 (b) setelah proses penyisipan data rahasia berbentuk video tampilan citra penampung masih terlihat baik, dan setelah melalui proses *decoder* berkas **sms bang.3gp** yang tersembunyi didalam citra penampung dapat diperoleh kembali dan dengan menggunakan bantuan *windows media player* berkas **sms bang.3gp** dapat disimak dan hasilnya sama seperti aslinya.

4.2 Pengujian Pengaruh Penggunaan Jumlah Bit Pada Citra Hasil Steganografi

Pada tahap yang kedua ini pengujian yang dilakukan adalah tentang pengaruh penggunaan jumlah bit pada tampilan citra hasil steganografi. Citra penampung dan data yang akan disembunyikan dapat dilihat pada Gambar 4.10.

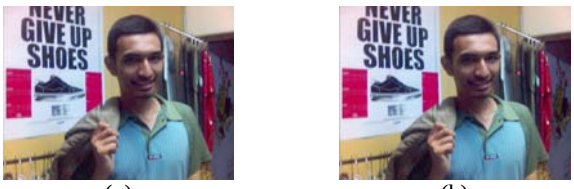


(a) (b)

Gambar 4.10 Citra penampung dan data yang disembunyikan
(a) Citra penampung : citra **d!StRo.Gu3.jpg**
(1280 x 960 piksel , 113 kB).
(b) Data yang disembunyikan : **1.jpg** (6 kB).

Tampilan citra hasil steganografi dengan berbagai macam variasi penggunaan jumlah bit untuk proses *encoder*nya dapat dilihat pada Gambar 4.11.

(a) (b)
(c) (d)
(e) (f)



(g) (h)

Gambar 4.11 Citra hasil steganografi
(a) Penggunaan 1-bit LSB.
(b) Penggunaan 2-bit.
(c) Penggunaan 3-bit.
(d) Penggunaan 4-bit.
(e) Penggunaan 5-bit.
(f) Penggunaan 6-bit.
(g) Penggunaan 7-bit.
(h) Penggunaan 8-bit.

Pada Gambar 4.11 (a), (b), (c), dan (d) citra penampung jika dilihat tampilannya masih terlihat bagus, tetapi setelah penggunaan jumlah bit diatas 4-bit maka citra penampung mulai terlihat sedikit perubahan pada bagian sisi kirinya, dan akan terlihat jelas jika menggunakan 8-bit yang terlihat pada Gambar 4.11 (h) karena jika dalam 1 komponen warna terdapat 8-bit, jika semuanya digantikan maka akan merusak komponen warna citra penampung. Citra penampung yang digunakan memiliki ukuran yang besar yaitu 113 kB sedangkan citra yang disembunyikan hanya berukuran 6 kB, maka kerusakan tampilan citra penampung hanya terlihat sedikit pada sisi kirinya. Sehingga untuk memilih penggunaan jumlah bit harus disesuaikan antara besar citra penampung dengan data rahasia yang akan disembunyikan.

4.3 Pengujian Hasil *Decoder* Jika Dilakukan Operasi Manipulasi Pada Citra Penampung

Pada tahap yang ketiga ini citra penampung yang telah disisipi data rahasia akan dilakukan operasi manipulasi. Operasi manipulasi dapat berupa pengubahan kontras, pemampatan, penajaman, kecerahan dan lain lain. Pada pengujian ini citra penampung pada Gambar 4.11 (a) akan dirubah tingkat kecerahannya. Perubahan tingkat kecerahan dilakukan dengan menggunakan bantuan ACDsee 5.0 sehingga didapatkan citra seperti pada Gambar 4.12.

Gambar 4.12 Citra yang dirubah tingkat kecerahannya.

Setelah melalui proses *decoder* ternyata hasilnya bukan data **1.jpg** tetapi adalah suatu berkas yang formatnya tidak dikenali dalam *windows*. Jika dicoba untuk mengetahui isi berkas tersebut dapat menggunakan bantuan Notepad dan hasilnya seperti terlihat pada Gambar 4.13.

Gambar 4.13 Hasil *decoder* setelah dilakukan perubahan tingkat kecerahan.

Dari hasil tersebut dapat dianalisis bahwa dengan adanya proses operasi manipulasi maka nilai dari komponen-komponen warna pada masing-masing piksel dalam citra penampung akan berubah sehingga saat dilakukan proses *decoder* data rahasia yang tersimpan didalamnya juga akan berubah. Dengan demikian kekurangan program ini adalah tidak tahan terhadap proses operasi manipulasi pada citra penampungnya.

V. KESIMPULAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penyusunan Tugas Akhir ini adalah sebagai berikut :

1. Pengujian program dalam berbagai macam bentuk data rahasia telah berhasil yaitu semua data rahasia dapat disembunyikan ke dalam citra penampung asalkan besar data rahasia lebih kecil atau sama dengan besar perhitungan data maksimal yang dapat disembunyikan.
2. Pengujian pengaruh penggunaan jumlah bit pada citra hasil steganografi telah berhasil dan tampilan citra penampung masih terlihat bagus pada penggunaan 1-bit sampai 4-bit, namun setelah penggunaan lebih dari 4-bit maka citra penampung mulai terlihat sedikit perubahan pada bagian sisi kirinya, dan akan terlihat jelas perubahan jika menggunakan 8-bit karena jika dalam 1 komponen warna terdapat 8 bit maka jika semuanya digantikan maka akan merusak komponen warna citra penampung.
3. Untuk data rahasia yang memiliki ukuran kecil dan menggunakan jumlah bit yang besar pada proses *encoder*-nya maka perubahan pada tampilan citra penampung tidak terlalu kelihatan, asalkan citra penampungnya memiliki resolusi yang tinggi.
4. Pengujian hasil *decoder* jika dilakukan operasi manipulasi pada citra penampung didapatkan bahwa dengan adanya proses operasi manipulasi maka nilai dari komponen-komponen warna pada masing-masing piksel dalam citra penampung akan berubah sehingga data rahasia yang ada didalamnya juga akan rusak. Dengan demikian data rahasia pada citra penampung tidak tahan terhadap proses operasi manipulasi pada citra penampungnya.
5. Pengujian program untuk proses *stacking* steganografi yaitu proses menyembunyikan data rahasia ke dalam citra penampung awal yang kemudian citra hasil steganografi disembunyikan lagi ke dalam citra penampung kedua telah berhasil dilakukan dan dengan melalui dua kali tahap proses *decoder* maka data rahasia tersebut dapat diungkapkan kembali ke bentuk aslinya.

5.2 SARAN

Berikut saran-saran untuk pengembangan program selanjutnya.

1. Program bisa dikembangkan tidak hanya citra digital sebagai berkas penampungnya tetapi dapat juga berupa media teks, media suara, ataupun media video.
2. Program bisa dikembangkan untuk masukan citra penampungnya tidak hanya **JPEG** atau **BMP** saja tetapi dapat juga dalam format citra yang lain, misalnya **Windows Meta File (WMF)**, **GIF**, **PNG** dan lain-lain.
3. Perlu dilakukan penelitian agar tidak hanya dapat menyembunyikan dan mengungkapkan data rahasia tetapi juga tahan atau *robust* terhadap berbagai operasi manipulasi pada citra penampungnya.

DAFTAR PUSTAKA

[1] Achmad, B. dan Firdausy, K., *Teknik Pengolahan Citra Digital Menggunakan Delphi*, Ardi Publishing, Yogyakarta, 2005.

[2] Ariyus, D., *Kriptografi Keamanan Data Dan Komunikasi*, Graha Ilmu, Yogyakarta, 2006.

[3] Hadiwibowo, *Pengamanan Informasi dan Kriptografi*. http://hadiwibowo.wordpress.com/tag/kriptografi, Januari 2007.

[4] Munir, R., *Pengolahan Citra Digital Dengan Pendekatan Algoritmik*, Informatika Bandung, 2004.

[5] ---, *Panduan Praktis Pemrograman Borland Delphi 7.0*, Penerbit Andi & Wahana Komputer, 2003.

[6] ---, *Tip & Trik Pemrograman Delphi 7.0*, Penerbit Andi & Wahana Komputer, 2003.

[7] ---, *ASCI*. http://en.wikipedia.org/wiki/ASCII, Januari 2007.

[8] ---, *Block cipher*. http://en.wikipedia.org/wiki/Block cipher, November 2006.

[9] ---, *Encryption*. http://en.wikipedia.org/wiki/Encryption, November 2006.

[10] ---, *Kriptografi*. http://id.wikipedia.org/wiki/Kriptografi, April 2006.

[11] ---, *Logic gate*. http://en.wikipedia.org/wiki/Logic gate, November 2006.

[12] ---, *Steganography*. http://en.wikipedia.org/wiki/Steganography, November 2006.

Biodata Penulis

Miftahur Rahim AL Anwary (L2F002597), lahir di Kota Barabai, Kalimantan Selatan, 23 Agustus 1984. Mahasiswa Jurusan Teknik Elektro Fakultas Teknik Angkatan 2002, konsentrasi Elektronika dan Telekomunikasi, Universitas Diponegoro, Semarang.
Email : rahiem_23@yahoo.co.id.

Menyetujui dan Mengesahkan

Pembimbing I

Achmad Hidayatno, S.T., M.T.
NIP. 132 137 933
Tanggal……

Pembimbing II

R. Rizal Isnanto, S.T., M.M., M.T.
NIP. 132 288 515
Tanggal…….