Jurnal Dinamika Informatika
Volume 5, Nomor 2, September 2010 :

STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN KOMBINASI ALGORITMA KRIPTOGRAFI VIGENÈRE DAN RC4

Oleh:

Basuki Rakhmat[1]
Muhammad Fairuzabadi, M.Kom.[2]

[1]Mahasiswa S1 Program Studi Teknik Informatika, Universitas PGRI Yogyakarta
[2]Dosen Tetap Program Studi Teknik Informatika, Universitas PGRI Yogyakarta

ABSTRAK

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan melalui media jaringan/internet. Teknik kriptografi dan stegano-grafi dapat digunakan untuk memberi perlindungan keamanan pada pesan rahasia.Pengembangkan teknik kriptografi ganda dengan kombinasi algoritma Vigenère dan RC4, yang diintegrasikan ke dalam steganografidengan metode *Least Significant Bit*(LSB) diharapkan dapat melindungi pesan rahasia.

Penelitian ini bertujuan untuk mengkombinasikan kriptografi Vigenère dan RC4 yang terintegrasi dengan metode steganografi, untuk memberikan proteksi ganda pada pesan rahasiadi dalam sebuah gambar/citra digital. Hasil dari penelitian ini adalah sebuah aplikasi yang diberi nama “StegoKripto”yang telah berhasil mengkombinasikan kriptografi dan steganografi.

Aplikasi “StegoKripto”berjalan pada sistem operasi berbasis Windows, dan hanya dapat menyembunyikan pesan teks dalam gambarberformat bitmap. Oleh sebab itu diperlukanpengembangan aplikasi lebih lanjut untuk dapat menyembunyikan pesan dalam ke dalam format gambar selain bitmap, dan dapat menyembunyikan file ke dalam media selain gambar seperti audio dan video, serta dapat digunakan secara global pada semua sistem operasi.

Kata kunci: Vigenère, RC4, LSB, Kriptografi, Steganografi, dan Keamanan data.

PENDAHULUAN

Latar Belakang Masalah

Teknologi informasi dan komunikasi telah berkembang pesat, memberikan pengaruh yang besar bagi kehidupan manusia.Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu.

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/internet,karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan/informasi yang dikirimkan melalui jaringan/internet.

Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan agar terhindar dari orang yang tidak berhak, salah satunya yaitu teknik kriptografi. Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan

dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.Kriptografi telah ada dan digunakan sejak berabad-abad yang lalu dikenal dengan istilah kriptografi klasik, yang bekerja pada mode karakter alfabet. Kelemahan kriptografi klasik adalah mudah dipecahkan dengan metode analisis frekuensi, karena keterbatasan kunciyang sedikit yaitu 26 kunci. Salah satu teknik kriptografi klasik adalah algoritma Vigenère Cipher.

Pada saat ini, algoritma kriptografi telah berkembang secara modern dengan bantuan teknologi komputasi digital.Kriptografi modern menggunakan gagasan yang sama seperti kriptografi klasik, namun tidak beroperasi dalam modus karakter alfabet seperti pada algoritma kriptografi klasik.Kriptografi modern beroperasi pada mode bit, yang berarti semua data dan informasi (kunci, plainteks, maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Salah satu teknik kriptografi modern adalah algoritma RC4.

Kriptografi memiliki dua konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses menyandikan *plaintext* menjadi *ciphertext* dengan mengubah pesan menjadi bentuk lain yang disamarkan agar tidak dikenali secara langsung, sedangkan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext*. Proses enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi. Hasil (*output*) kriptografi adalah sebuah bentuk yang berbeda dari pesan/informasi asli, dan memiliki ciri yang seolah-olah acak/tidak teratur. Perubahan pada hasil tersebut dapat membuat kecurigaan tentang informasi apa yang terkandung didalamnya. Teknik kriptografi dapat dipecahkan dengan kemampuan teknologi komputasi.

Kriptografi klasik dan modern secara teori dapat digabungkan dengan bantuan teknologi komputasi modern, agarmendapatkan proteksi ganda dalam melindungi pesan rahasia. Algoritma kriptografi Vigenère dan RC4 dapat dikombinasikansecara digital untuk menghasilkan dua lapis keamanan yang dapat memberi perlindungan lebih pada pesan rahasia.

Teknik menjaga kerahasiaan pesan tidak hanya menggunakan kriptografi. Teknik lain yang dapat digunakan yaitu steganografi. Steganografi adalah seni dan ilmu untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Berbeda dengan kriptografi yang merahasiakan makna pesan namun keberadaan pesan tetap ada, steganografi merahasiakan dengan menutupi atau menyembunyikan pesan.

Implementasi steganografi saat ini telah menggunakan media digital sebagai media penampung atau penyembunyi pesan, salah satunya media gambar (citra digital). Steganografi menyisipkan atau menyembunyikan pesan di dalam sebuah gambar (*covertext*), agar pihak lain tidak menyadari keberadaan informasi yang ada di dalam gambar tersebut. Steganografi menjadikan gambar stego (*stegotext*) dalam bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut sebatas kemampuan indera manusia secara visual, artinya mata manusia tidak dapat mem-bedakan gambar stego dengan gambar asli yang tidak memiliki pesan di dalamnya.

Steganogafi memiliki dua proses, yaitu *encoding* dan *decoding*. *Encoding* merupakan proses penyisipan pesan kedalam media penampung (*covertext*) dalam hal ini adalah gambar/citra digital, sedangkan *decoding* adalah proses ekstraksi pesan dari gambar stego (*stegotext*). Kedua proses tersebut mungkin memerlukan kunci rahasia (*stegokey*) untuk proses penyisipan pesan dan ekstraksi pesan, agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Salah satu metode steganografi citra digital adalah *Least Significant Bit* (LSB), dengan teknik penyembunyian pesan pada lokasi bit terendah dalam citra digital. Pesan dikonversi ke dalam bentuk bit biner dan disembunyikan pada citra digital dengan metode LSB. Implementasi metode LSB tanpa dilengkapi dengan sistem keamanan berpeluang untuk dapat dibongkar dengan mudah melalui teknik pemecahan analisis frekuensi dengan

membaca bit terendah.

Steganografi dapat dipandang sebagai kelanjutan kriptografi, terkait dengan fungsi *stegokey* sebagai kunci untuk proses enkripsi/dekripsi. Pesan rahasia dienkripsi dengan kunci lalu disembunyikan dalam citra, dan pesan rahasia dapat diekstraksi dan didekripsi kembali persis sama seperti aslinya dengan menggunakan kunci yang sama. Kombinasi kriptografi dan steganografi dapat memberikan keamanan pada pesan rahasia. Pesan rahasia terlebih dahulu dienkripsi dengan kombinasi algoritma Vigenère dan RC4, kemudian cipherteks hasil kriptografi tersebut disembunyikan di dalam media gambar/citra dengan metode steganografi. Implementasi algoritma kriptografi ganda dan metode steganografi dapat lebih meningkatkan keamanan pesan rahasia.

Identifikasi Masalah

Berdasarkan latar belakang masalah, proses pertukaran pesan melalui jaringan/internetmemerlukan jaminankeamanan dan kerahasiaan. Diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik pada pesan rahasia, dan menjaga kerahasiaan pesandengan menyembunyikannya ke dalam media lain(gambar) agar keberadaan pesan rahasia tidak diketahui.

Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah mengembangkan aplikasi kriptografi yang mengkombinasikan algoritma kriptografi klasik Vigenère dan algoritma kriptografi modern RC4 untuk mendapatkan proteksi ganda yang lebih baik dalam menjaga keamanan dan kerahasiaan pesan, serta terintegrasi dengan steganografi untuk menyembunyikan pesan dalam sebuah gambar bitmapguna melindungi keberadaan pesan rahasia.

LANDASAN TEORI

Tinjuan Pustaka

Lenti (2000) menganalisa dan menguji beberapa teknik steganografi pada citra digital. Salah satu teknik dalam penelitian tersebut adalah *Least Significant Bit* untuk menyisipkan pesan dalam citra digital, yang tidak mengubah tampilan citra digital secara signifikan ketika citra telah disisipi dengan pesan.

Rezky (2008) meneliti tentang metode LSB steganografi pesan pada citra digital, dengan implementasi metode kriptografi menggunakan kunci citra (gambar) asli. Proses penyisipan pesan dengan mengkonversi citra dan pesan menjadi bit biner, kemudian melakukan operasi XOR antara citra dan pesan. Proses rekonstruksi atau ekstraksi pesan membutuhkan kunci gambar asli, menggunakan operasi yang sama yaitu XOR antara citra asli dan citra hasil steganografi (gambar stego).

Truman (2010) meneliti tentang aspek kerahasiaan pada algoritma Vigenère Cipher yang ditinjau berdasarkan kompleksitas algoritma, dan karakteristik penyandian plainteks terhadap cipherteks, menggunakan aplikasi Visual Basic 6. Algoritma Viginère Cipher dapat dipecahkan dengan mudah menggunakan komputer melalui teknik pemecahan analisis frekuensi.

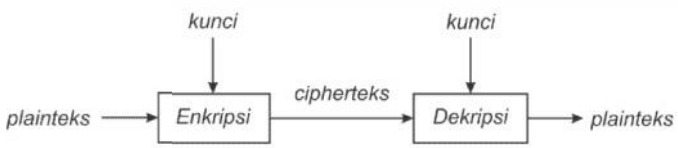
Wildan (2010) meneliti tentang perlindungan pesan rahasia pada citra digital menggunakan metode LSB, dengan algoritma kriptografi Ultra untuk memberikan perlindungan pada pesan yang disisipkan. Kelemahan steganografi dengan satu lapis kriptografi dapat dengan mudah dipecahkan.

Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*"

(rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan), sehingga kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Kriptografi memiliki dua konsep utama, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi. Gambar 1 memperlihatkan skema enkripsi dan dekripsi dengan menggunakan kunci.



Gambar 1: Skema enkripsi dan dekripsi.

Kriptografi terbagi menjadi 2 (dua) yaitu:
1. Kriptografi klasik (mode karakter):
   a. Cipher Substitusi
   b. Cipher Transposisi
2. Kriptografi modern (mode bit/*binary*):
   a. Cipher kunci simetri: cipher aliran (*stream cipher*), cipher blok (*block cipher*)
   b. Cipher kunci publik (*public key cryptography*)

Algoritma Vigenere

Vigenère Cipher dibuat oleh Blaise de Vigenère pada abad 16, yang merupakan metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasar-kan deretan huruf-huruf pada kata kunci.Algoritma Vigenère dapat dinyatakan secara matematis, dengan menggunakan penjumlahan dan operasi modulus:
Algoritma enkripsi dinyatakan:

C*i* ≡ (P*i* + K*i*) mod 26

Algoritma dekripsi dinyatakan:

P*i* ≡ (C*i* – K*i*) mod 26

C adalah nilai desimal karakter cipherteks ke-i, P adalah nilai desimal karakter plainteks ke-i, dan K adalah nilai desimal karakter kunci ke-i, dengan asumsi angka desimal karakter A = 0, B = 1, ..., Z = 25. Jika hasil dekripsi bernilai negatif, maka nilai tersebut ditambah dengan angka 26 untuk mendapatkan plainteks.

Algoritma RC4

RC4 merupakan salah satu jenis cipher aliran (*stream cipher*), didesain oleh Ron Rivest di Laboratorium RSA (RSA Data Security Inc.) pada tahun 1987. Cipher RC4 merupakan teknik enkripsi yang dapat dijalankan dengan panjang kunci yang variabel dan memproses data dalam ukuran *byte*. Algoritma RC4 adalah sebagai berikut:
1. Inisialisasi larik S sehingga $S_0 = 0$, $S_1 = 1$, …, $S_{255} = 255$.
   Dalam notasi algoritmik, langkah 1 ditulis sebagai berikut:

```
for i ← 0 to 255 do
S[i] ← i
end for
```

2. Jika panjang kunci U < 256, lakukan padding yaitu penambahan *byte* semu sehingga panjang kunci menjadi 256 *byte*. Misalnya U = “abcde” yang hanya terdiri dari 5 *byte* (5 huruf), maka lakukan padding dengan penambahan byte (huruf) semu, misalnya U = “abcdeabcdeabcdea…” sampai panjang U mencapai 256 *byte*.

3. Lakukan permutasi terhadap nilai-nilai didalam larik S dengan cara:

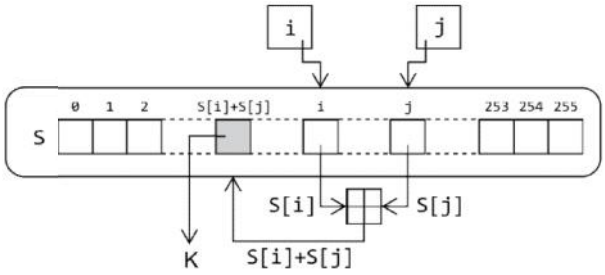
```
j ← 0
for i ← 0 to 255 do
j ← (j + S[i] + U[i]) mod 256
swap (S[i], S[j])
end for
```

4. Bangkitkan *keystream* dan lakukan enkripsi dengan cara:

```
i ← 0
j ← 0
for idx ← 0 to PanjangPlainteks – 1 do
i ← (i + 1) mod 256
j ← (j + S[i]) mod 256
swap (S[i], S[j])
t ← (S[i] + S[j]) mod 256
K ← S[t]
C ← K XOR P[idx]
end for
```

P adalah *array*(larik) yang menyimpan karakter-karakter plainteks.

Proses pembangkitan *keystream*K diperlihatkan pada Gambar 2. *Keystream*K dipilih dengan mengambil nilai `S[i]` dan `S[j]` dan menjumlahkannya dalam modulo 256. Hasil penjumlahan adalah indeks `t` sedemikian sehingga S[t] menjadi *keystream*K yang kemudian digunakan untuk mengenkripsi plainteks ke-`idx`. Karena karakter-karakter kunci di-*copy* berulang-ulang (untuk mengisi kekurangan 256 *byte*) maka ada kemungkinan nilai-nilai di dalam larik S ada yang sama.



Gambar 4: Diagram pembangkitan *keystream* K.

Steganografi

Steganografi (*steganography*) berasal dari bahasa Yunani yaitu “*steganos*” yang berarti “tersembunyi” atau “terselubung”, dan “*graphein*” yang artinya “menulis”. Steganografi dapat diartikan “tulisan tersembunyi” (*covered writing*). Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia

tersebut tidak dapat diketahui.

Steganografi membutuhkan dua properti, yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, kode program, atau pesan lain.

Proses penyisipan pesan ke dalam media *covertext* dinamakan *encoding*, sedangkan ekstraksi pesan dari *stegotext* dinamakan *decoding*. Kedua proses ini mungkin memerlukan kunci rahasia (yang dinamakan *stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi.

Metode *Least Significant Bit* (LSB)

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 *byte* = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.
Misalkan segmen pixel-pixel citra/gambar sebelum penambahan bit-bit adalah:

```
00110011  10100010  11100010  10101011  00100110
10010110  11001001  11111001  10001000  10100011
```

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan ’1110010111’, maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi (digarisbawahi):

```
00110011  10100011  11100011  10101010  00100110
10010111  11001000  11111001  10001001  10100011
```

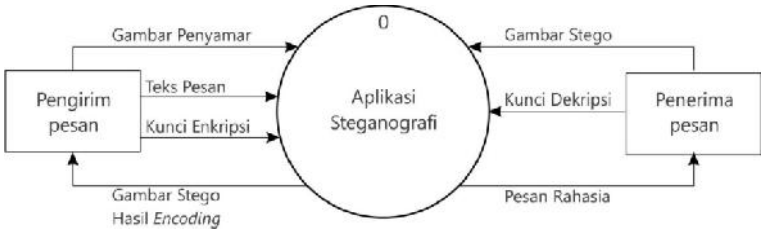
ANALISIS DAN PERANCANGAN

Desain Sistem

Kriptografi dan Steganografi dengan penyembunyian pesan dalam citra digital terdiri dari beberapa proses yang meliputi proses pengolahan teks, proses enkripsi/dekripsi, proses pengolahan citra, dan proses hasil keluaran. Desain sistem bertujuan untuk menentukan kebutuhan-kebutuhan sistem yang akan dikembangkan dengan membuat desain model untuk menggambarkan secara umum proses yang terjadi dalam sistem.Desain model disajikan dalam Diagram Alir Data.

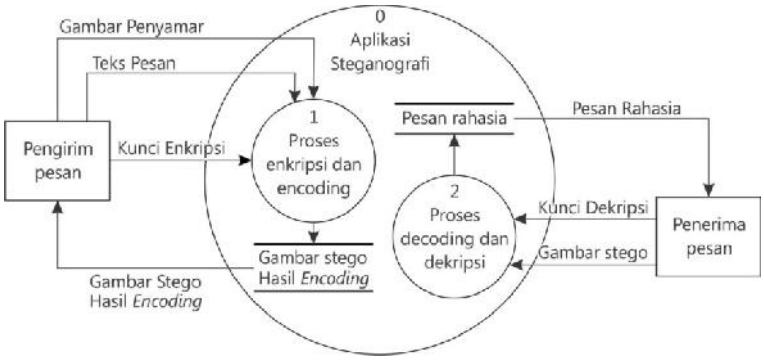
Diagram Konteks

Diagram Konteks memberikan gambaran umum tentang entitas luar yang terlibat, input, dan data/informasi yang dihasilkan, ditunjukkan pada Gambar 5 berikut.



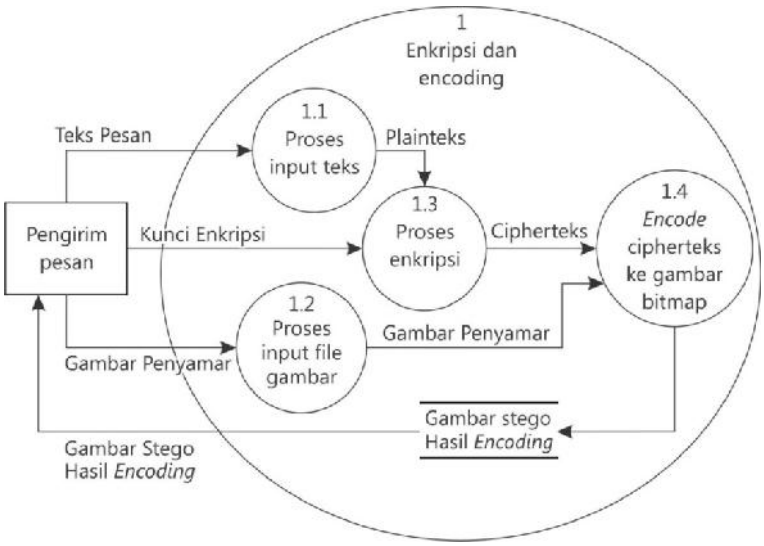
Gambar 5: Diagram Konteks.

Diagram Alir Data Level 0



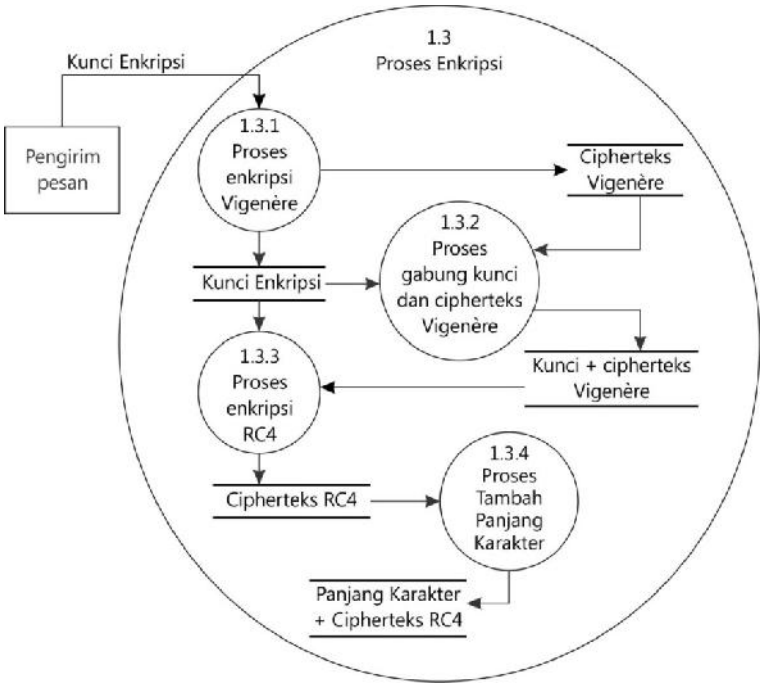
Gambar 6.DAD level 0.

DAD level 1, enkripsi dan *encoding* (Proses 1)



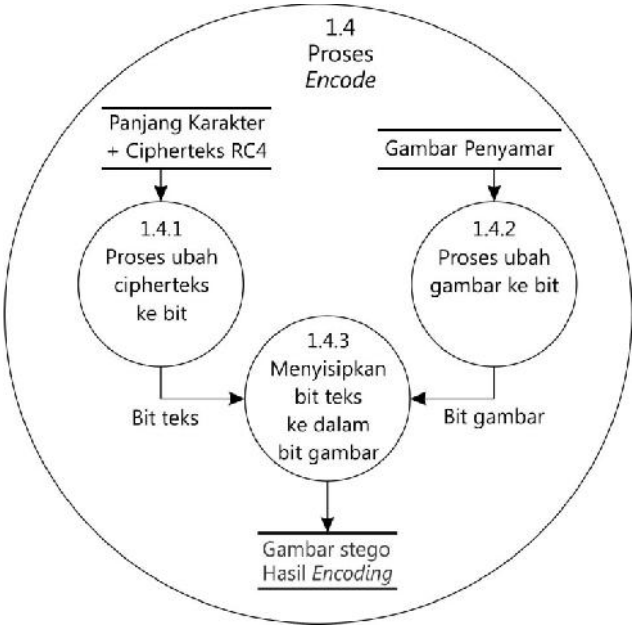
Gambar 7: DAD Level 1, enkripsi dan encoding (Proses 1).

DAD level 1, proses enkripsi (Proses 1.3)



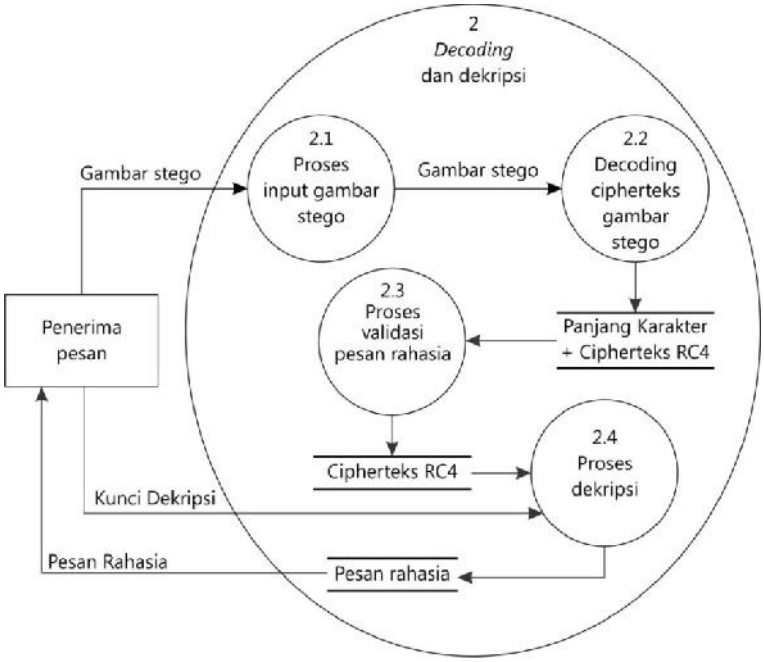
Gambar 8: DAD Level 1, Proses enkripsi (1.3)

DAD level 1, proses *encode* (Proses 1.4)



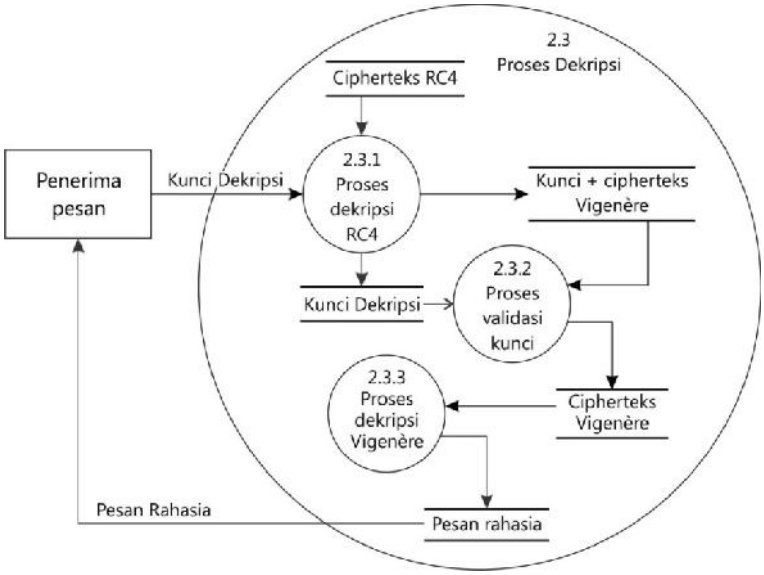
Gambar 9: DAD Level 1, Proses *encode* (1.4).

DAD level 2, *decoding* dan dekripsi (Proses 2)



Gambar 10: DAD level 2, *decoding* dan dekripsi (Proses 2).

DAD level 2, proses dekripsi (Proses 2.3)



Gambar 11: DAD level 2, *decoding* (Proses 2.3)

IMPLEMENTASI DAN PEMBAHASAN

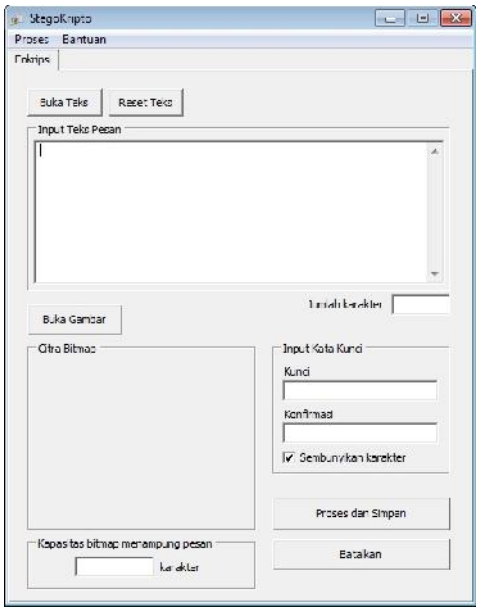
Implementasi Sistem

Implementasi sistem kombinasi kriptografi dan steganografi diprogram dengan bahasa pemrograman Delphi 2010, dan diberi nama aplikasi “StegoKripto”. Aplikasi ini terbagi dalam dua bagian, yaitu Enkripsi dan Dekripsi. Enkripsi digunakan oleh pengguna yang ingin mengirimkan pesan secara rahasia yang disembunyikan dalam sebuah gambar bitmap (stego), sedangkan dekripsi digunakan oleh pengguna yang menerima gambar stego berisi pesan rahasia.

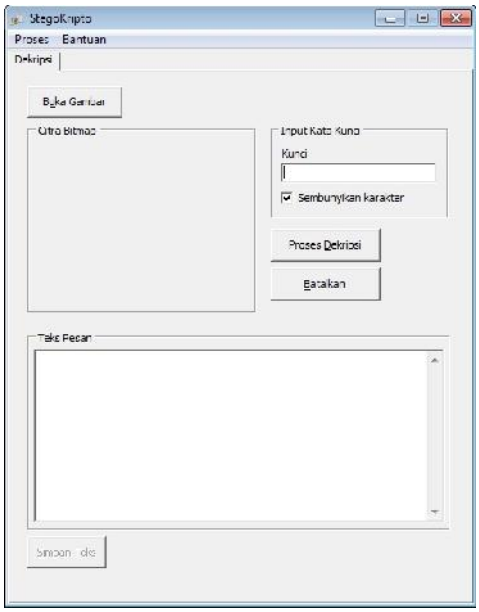
Enkripsi merupakan proses untuk menyembunyikan pesan, yang terbagi menjadi tiga bagian dengan urutan enkripsi Vigenère, enkripsi RC4, dan *encoding*. Proses enkripsi membutuhkan masukan/input berupa teks, gambar, dan kunci. Kebalikan dari proses enkripsi adalah Dekripsi, yaitu proses pembacaan pesan rahasia, yang terbagi juga menjadi tiga bagian dengan urutan decoding, dekripsi RC4, dan dekripsi Vigenère. Proses dekripsi membutuhkan masukan/input berupa gambar dan kunci.

Pembahasan

Pengembangan aplikasi kombinasi kriptografi dan steganografi ini didasarkan pada kebutuhan akan keamanan pesan rahasia. Kombinasi teknik kriptografi dan teknik steganografi dapat memberi perlindungan keamanan pada pesan rahasia. Kriptografi membutuhkan kunci sebagai proses otentikasi, agar hanya pihak yang berhak saja yang mengetahui kunci dan dapat membuka/membaca pesan rahasia. Metode steganografi menyembunyikan pesan rahasia dalam sebuah gambar agar pesan rahasia tersamarkan.



Gambar 12: Tampilan Enkripsi.



Gambar 13: Tampilan Dekripsi.

Untuk dapat menggambarkan proses kriptografi dan steganografi, digunakan contoh:
Plainteks: **UNIVERSITAS PGRI YOGYAKARTA**
Kunci: **abcd1234**

Enkripsi Vigenere
Plainteks :**UNIVERSITAS PGRI YOGYAKARTA**
Kunci : **abcd1234**

Karena algoritma Vigenere bekerja pada mode karakter, maka karakter selain alfabet akan dihilangkan, dan mode karakter akan diubah sesuai huruf besar dan kecil.

Konversi kunci : **ABCD**

Kode ASCII plainteks : 85, 78, 73, 86, 69, 82, 83, 73, 84, 65, 83, 32, 80, 71, 82, 73, 32, 89, 79, 71, 89, 65, 75, 65, 82, 84, 65.

Kode ASCII kunci : 65, 66, 67, 68.

Enkripsi Vigenere : 85, 79, 75, 89, 69, 83, 85, 76, 84, 66, 85, 32, 83, 71, 83, 75, 32, 66, 79, 72, 65, 68, 75, 66, 84, 87, 65.

Cipherteks Vigenere : **UOKYESULTBU SGSK BOHADKBTWA**.

Enkripsi RC4

Cipherteks Vigenere akan dimodifikasiterlebih dahulu dengan menambahkan kunci dan tanda "**|**" sebagai validasi pada saat proses dekripsi.

Cipherteks Vigenere : **abcd1234|UOKYESULTBU SGSK BOHADKBTWA**.

Kode ASCII cipherteks : 97, 98, 99, 100, 49, 50, 51, 52, 124, 85, 79, 75, 89, 69, 83, 85, 76, 84, 66, 85, 32, 83, 71, 83, 75, 32, 66, 79, 72, 65, 68, 75, 66, 84, 87, 65.

Kunci : abcd1234

Kode ASCII kunci : 97, 98, 99, 100, 49, 50, 51, 52.

Larik U (kunci) : 97, 98, 99, 100, 49, 50, 51, 52, 97, 98, 99, 100, 49, 50, 51, 52.

Larik S : 37, 181, 199, 56, 176, 134, 194, 145, 93, 45, 87, 51, 240, 123, 236, 159, 105, 129, 135, 142, 36, 102, 41, 34, 161, 91, 225, 43, 65, 88, 237, 201, 152, 248, 146, 63, 84, 235, 9, 151, 47, 140, 29, 74, 73, 86, 160, 40, 185, 106, 206, 2, 203, 197, 69, 173, 95, 42, 182, 85, 110, 76, 162, 80, 250, 241, 193, 31, 226, 122, 175, 17, 211, 144, 154, 188, 243, 222, 32, 115, 55, 242, 167, 94, 3, 249, 8, 67, 172, 216, 33, 16, 150, 39, 165, 126, 166, 219, 25, 231, 205, 53, 136, 245, 177, 111, 61, 27, 157, 49, 190, 153, 125, 195, 97, 92, 81, 89, 191, 234, 38, 104, 220, 141, 7, 132, 252, 223, 192, 109, 58, 30, 189, 244, 100, 83, 209, 218, 170, 48, 221, 171, 44, 19, 57, 198, 70, 90, 112, 178, 50, 11, 98, 46, 114, 72, 10, 246, 13, 251, 212, 183, 158, 1, 238, 108, 35, 213, 120, 128, 202, 121, 62, 229, 137, 156, 214, 54, 210, 64, 22, 124, 78, 68, 75, 164, 228, 215, 139, 169, 14, 200, 15, 138, 168, 186, 79, 174, 0, 24, 247, 253, 196, 6, 20, 23, 204, 52, 28, 149, 119, 117, 180, 82, 208, 207, 155, 113, 184, 227, 233, 26, 66, 107, 77, 255, 118, 96, 99, 59, 230, 163, 187, 71, 239, 127, 21, 217, 143, 254, 4, 116, 103, 101, 224, 133, 232, 147, 130, 5,

18, 179, 148, 12, 60, 131.

Keystream : 196, 27, 247, 253, 210, 151, 124, 239, 195, 142, 109, 222, 36, 253, 202, 69, 156, 37, 127, 116, 141, 86, 175, 99, 112, 25, 221, 109, 48, 153, 94, 125, 239, 103, 251, 142.

Kode ASCII Cipherteks RC4 : 165, 121, 148, 153, 227, 165, 79, 219, 191, 219, 34, 149, 125, 184, 153, 16, 208, 113, 61, 33, 173, 5, 232, 48, 59, 57, 159, 34, 120, 216, 26, 54, 173, 51, 172, 207.

Cipherteks RC4 : **¥y ã¥OÛ¿Û" }¸ Ðq=!-è0;9 "xØ6-3¬Ï**

Encoding

Ilustrasi proses *encoding* (penyisipan) pesan dalam gambar digunakan contoh potongan bit gambar bitmap 24-bit sebagai berikut:

```
11101101 00100100 00011100 11101101 00100100 00011100 11101101 00100100
00011100 11101101 00100100 00011100 11101101 00100100 00011100 11101101
00100100 00011100 11101101 00100100 00011100 11101101 00100100 00011100
11101101 00100100 00011100 11101101 00100100 00011100 11101101 00100100
00011100 11101101 00100100 00011100 11101101 00100100 00011100 11101101
00100100 00011100 11101101 00100100 00011100 11101101 00100100 00011100
11101101 00100100 00011100 11101101 00100100 00011100 11101101 00100100
00011100 11101101 00100100 00011100 11101101 00100100 00011100 11101101
00100100 00011100 11101101 00100100 00011100 11101101 00100100 00011100
11101101 00100100 00011100 11101101 00100100 00011100 11101101 00100100
00011100 11101101 00100100 00011100 11101101 00100100 00011100 11101101
00100100 00011100 11101101 00100100 00011100 11101101 00100100 00011100
11101101 00100100 00011100 11101101 00100100 00011100 11101101 ...dst
```

Bit cipherteks:

```
10100101 01111001 10010100 10011001 11100011 10100101 01001111 11011011
10111111 11011011 00100010 10010101 01111101 10111000 10011001 00010000
11010000 01110001 00111101 00100001 10101101 00000101 11101000 00110000
00111011 00111001 10011111 00100010 01111000 11011000 00011010 00110110
10101101 00110011 10101100 11001111
```

Proses *encoding* akan mengubah bit gambar seperti berikut, diambil contoh penyisipan bit cipherteks sebanyak 5 *byte*:

1110110***1*** 0010010***0*** 0001110***1*** 1110110***0*** 0010010***0*** 0001110***1*** 1110110***0*** 0010010***1***
0001110***1*** 1110110***0*** 0010010***0*** 0001110***1*** 1110110***1*** 0010010***1*** 0001110***1*** 1110110***0***
0010010***0*** 0001110***0*** 1110110***1*** 0010010***0*** 0001110***1*** 1110110***0*** 0010010***0*** 0001110***1***
1110110***1*** 0010010***0*** 0001110***0*** 1110110***1*** 0010010***1*** 0001110***0*** 1110110***0*** 0010010***1***
0001110***1*** 1110110***1*** 0010010***0*** 0001110***0*** 1110110***0*** 0010010***1*** 0001110***1*** 1110110***1***

Bit cipherteks tersisipkan per 1 (satu) bit di setiap bit gambar, disisipkan terbalik pada bit terakhir gambar, ditandai dengan cetak tebal dan miring. Penyisipan dilakukan terbalik agar mempersulit proses pemecahan analisis frekuensi pada gambar/citra stego.

Dekripsi RC4

Proses dekripsi dilakukan secara terbalik, yaitu dekripsi RC4 kemudian dekripsi Vigenere. Proses validasi kunci menentukan apakah pesan asli dapat dibaca atau tidak, jadi ditentukan oleh input kunci. Misalkan kunci yang digunakan salah: **abc123**

Kode ASCII Cipherteks RC4	:	165, 121, 148, 153, 227, 165, 79, 219, 191, 219, 34, 149, 125, 184, 153, 16, 208, 113, 61, 33, 173, 5, 232, 48, 59, 57, 159, 34, 120, 216, 26, 54, 173, 51, 172, 207.
Kode ASCII kunci	:	97, 98, 99, 49, 50, 51.
Keystream	:	10, 220, 32, 119, 85, 162, 29, 111, 209, 155, 131, 254, 161, 27, 200, 12, 35, 205, 98, 152, 103, 45, 133, 228, 246, 2, 59, 60, 152, 205, 90, 118, 122, 224, 142, 222.
Cipherteks Vigenere ASCII	:	175, 165, 180, 238, 182, 7, 82, 180, 110, 64, 161, 107, 220, 163, 81, 28, 243, 188, 95, 185, 202, 40, 109, 212, 205, 59, 164, 30, 224, 21, 64, 64, 215, 211, 34, 17.
Cipherteks Vigenere	:	**¯¥´î¶R´n@¡kÜ£Qó¼_¹Ê(mÔÍ;¤-à@@×Ó"**

Hasil dekripsi tidak menunjukkan kunci dan tanda “|” pada cipherteks, oleh karena itu proses dekripsi dinyatakan gagal, dan proses dihentikan.

Berikut adalah proses dekripsi dengan menggunakan kunci yang sama: **abcd1234**

Kode ASCII Cipherteks RC4	:	165, 121, 148, 153, 227, 165, 79, 219, 191, 219, 34, 149, 125, 184, 153, 16, 208, 113, 61, 33, 173, 5, 232, 48, 59, 57, 159, 34, 120, 216, 26, 54, 173, 51, 172, 207.
Kode ASCII kunci	:	97, 98, 99, 100, 49, 50, 51, 52.
Keystream	:	196, 27, 247, 253, 210, 151, 124, 239, 195, 142, 109, 222, 36, 253, 202, 69, 156, 37, 127, 116, 141, 86, 175, 99, 112, 25, 221, 109, 48, 153, 94, 125, 239, 103, 251, 142.
Cipherteks Vigenere ASCII	:	97, 98, 99, 100, 49, 50, 51, 52, 124, 85, 79, 75, 89, 69, 83, 85, 76, 84, 66, 85, 32, 83, 71, 83, 75, 32, 66, 79, 72, 65, 68, 75, 66, 84, 87, 65.
Cipherteks Vigenere	:	**abcd1234|UOKYESULTBU SGSK BOHADKBTWA**

Hasil dekripsi menunjukkan kunci dan tanda “|” pada cipherteks, oleh karena itu proses dekripsi dinyatakan berhasil dan selanjutnya diproses untuk dekripsi Vigenere.

Dekripsi Vigenere

Dekripsi Vigenere dilakukan dengan memodifikasi cipherteks hasil dekripsi RC4, yaitu menghilangkan kunci dan tanda “|” dari cipherteks.

Cipherteks Vigenere	:	**UOKYESULTBU SGSK BOHADKBTWA**
Kunci	:	abcd1234
Konversi Kunci	:	ABCD
Kode ASCII cipherteks Vigenere	:	85, 79, 75, 89, 69, 83, 85, 76, 84, 66, 85, 32, 83, 71, 83, 75, 32, 66, 79, 72, 65, 68, 75, 66, 84, 87, 65.
Kode ASCII kunci	:	65, 66, 67, 68.
Dekripsi Vigenere	:	85, 78, 73, 86, 69, 82, 83, 73, 84, 65, 83, 32, 80, 71, 82, 73, 32, 89, 79, 71, 89, 65, 75, 65, 82, 84, 65.
Plainteks	:	**UNIVERSITAS PGRI YOGYAKARTA**.

Hasil proses dekripsi telah mendapatkan pesan rahasia.

Keunggulan

Aplikasi steganografi dan kriptografi ini mempunyai keunggulan dalam beberapa hal, antara lain sebagai berikut:

1. Program mengimplementasikan tiga lapis proteksi untuk menjaga keamanan pesan

rahasia, yaitu kombinasi kriptografi algoritma Vigenère dan algoritma RC4, serta teknik Steganografi dengan metode Least Significant Bit yang menyisipkan bit pesan secara terbalik untuk mempersulit proses pemecahan analisis frekuensi pada gambar/citra stego.
2. Hasil yang didapatkan dari proses steganografi tidak mengubah kualitas gambar secara visual, perubahan dalam gambar tidak terlihat oleh pandangan mata manusia.
3. Program didesain dengan tampilan sederhana untuk proses Enkripsi dan Dekripsi, agar mudah dipahami oleh pengguna.
4. Kode program dibuat dengan prosedur dan fungsi yang terpisah, sehingga dapat memudahkan pengembangan aplikasi lebih lanjut.
5. Program memiliki dokumentasi bantuan dan panduan bagi pengguna, untuk memberikan panduan dan penjelasan mengenai fitur aplikasi.

Kelemahan Program

Aplikasi steganografi dan kriptografi ini mempunyai kelemahan dalam beberapa hal, diantaranya sebagai berikut:

1. Implementasi steganografi hanya menggunakan media gambar/citra untuk menyisip-kan pesan, tidak dapat diimplementasikan dalam media lain seperti audio dan video.
2. Program hanya dapat melakukan penyisipan pesan teks pada format gambar bitmap (BMP), tidak dapat menggunakan format gambar yang lain (misal JPG atau PNG).
3. Program hanya dapat menyisipkan pesan teks karakter, tidak dapat menyisipkan data/file dokumen.
4. Aplikasi hanya dapat berjalan di lingkungan sistem operasi Windows, tidak dapat digunakan oleh pengguna sistem operasi lainnya, seperti Linux, MacOSX, FreeBSD, dan lain-lain.

KESIMPULAN DAN SARAN

Kesimpulan

1. Algoritma kriptografi klasik dan modern, yaitu Vigenère dan RC4 dapat dikombinasi-kan dalam sebuah sistem untuk memberikan dua lapis proteksi dalam menyembunyi-kan pesan rahasia.
2. Teknik steganografi dengan metode *Least Significant Bit* (LSB) untuk menyembunyi-kan pesan teks pada gambar bitmap dapat diaplikasikan menggunakan Delphi 2010.
3. Kriptografi dan steganografi dapat diintegrasikan menjadi satu dalam sebuah sistem aplikasi. Pesan teks terlindungi dengan algoritma kriptografi dan tersembunyi dalam sebuah gambar.

Saran

1. Teknik steganografi dapat dikembangkan untuk implementasi penyisipan pesan ke dalam media lain seperti audio dan video.
2. Implementasi steganografi pada gambar perlu dikembangkan untuk dapat mengimplementasikan proses penyisipan pesan ke dalam format gambar selain gambar bitmap, seperti JPG dan PNG.
3. Perlu pengembangan untuk teknik steganografi agar dapat menyisipkan data/file ke dalam media penyamar.
4. Implementasi program perlu dikembangkan untuk dapat berfungsi dalam berbagai sistem operasi, seperti Linux, MacOSX, atau FreeBSD.

DAFTAR PUSTAKA

Achmad, Balza. dan Firdauzy, Kartika. 2005. Teknik Pengolahan Citra Digital Menggunakan Delphi. Jakarta: Ardi Publishing.

Anadra, Rezky. 2008. Steganografi Pesan Pada Citra Menggunakan Metode LSB. Bogor: Fakultas Ilmu Komputer Institut Pertanian Bogor.

Awcock, G.J. and Thomas, R. 1996. *Applied Image Processing*. McGraw-Hill Book.

Candra, Marvin. 2007. Pengolahan Citra Digital Menggunakan Matlab. Bandung: Penerbit Informatika.

Cantù, Marco. 2010. *Delphi 2010 Handbook*. Scotts Valley: CreateSpace.

Cummins, Jonathan. 2004. *Steganography and Digital Watermarking*. Birmingham School of Computer Science, The University of Birmingham.

Girsang, Truman T. 2010. Analisis Kerahasiaan Data Menggunakan Algoritma Vigenere Cipher Dalam Sistem Pengamanan Data. Medan: Program Studi Ekstensi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sumatera Utara.

Hidayat, Wildan. 2010. Perlindungan Pesan Rahasia Pada Citra Digital Menggunakan Metode Least Significant Bit Steganografi. Medan: Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sumatera Utara.

Jogiyanto. 1990. Analisis dan Desain Sistem Informasi. Yogyakarta: Andi Offset.

Lenti, József. 2000. *Steganographic Methods*. Department of Control Engineering and Information Technology, Budapest University of Technology and Economics.

Munir, Rinaldi. 2004. Pengolahan Citra Digital Dengan Pendekatan Algoritmik. Bandung: Penerbit Informatika.

Munir, Rinaldi. 2006. Kriptografi. Bandung: Penerbit Informatika.

http://itte.no/delphi/Steganography.htm, diakses pada Agustus 2010.

http://www.wikipedia.org, diakses pada Agustus 2010.

http://fairuzelsaid.wordpress.com/2010/01/08/analisis-sistem-informasi-diagram-alir-data-dad-data-flow-diagramdfd/diakses pada Oktober 2010.