Implementasi Steganografi Lsb Dengan Enkripsi Vigenere Cipher Pada File Multimedia

Anik Nur Novitsari Eka .S[1], Triawan Adi Cahyanto[2]

[1,2] *Jurusan Teknologi Informasi*
Jalan Karimata No. 49, Sumbersari, Kabupaten Jember, Jawa Timur 68121
[1]aniknurn@ugm.ac.id
[3*]penulis3@ugm.ac.id (dosen)

***Abstrak*—Saat ini teknologi informasi sudah sangat berkembang menjadi salah satu media yang paling popular didunia. Sayangnya dengan berkembangnya teknologi informasi semakin berkembang pula tindak penyalah gunaan informasi yang bukan haknya. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan informasi. Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi. Pada makalah ini, dibuat aplikasi steganografi yang bertujuan untuk mengamankan informasi berupa pesan teks dengan menyisipkan (menyembunyikan) kedalam pesan lainnya yaitu pada file multimedia dengan menggunakan metode algoritma LSB (Least Significant Bit) dan dengan enkripsi Vigenere Cipher. Hasil dari aplikasi ini adalah dapat menyisipkan pesan tersembunyi berupa teks ke dalam berkas file multimedia berformat JPEG dan dapat mengekstraksi kembali pesan tersembunyi tersebut dari dalam file (stego-image).**
Kata kunci: Steganografi, Least Significant Bit (LSB), Vigenere Cipher.

***Abstract*— Today information technology has greatly evolved into one of the most popular media in the world. Unfortunately, with the rapid development of information technology is growing also follow misuse of information that is not right. With the many techniques that attempt to access information that is not right. Therefore in line with the growth of the Internet media should also be coupled with the development of information security. Various techniques are used to protect confidential information from unauthorized people, one of which is the technique of steganography. In this final report, made steganography application that aims to secure the information in the form of a text by inserting (hide) into another message that the file multimedia using the algorithm LSB (Least Significant Bit) and encryption Vigenere Cipher. The result of this application is to insert hidden messages (text file) into file multimedia (JPEG) and can extract the hidden message back from the file (stego-image).**
Keywords: Steganography, Least Significant Bit (LSB), Vigenere Cipher.

I. PENDAHULUAN

1.1 Latar Belakang

Steganografi adalah seni dan ilmu untuk menyembunyikan pesan dalam sebuah pesan. Seni dan ilmu ini telah diterapkan sejak dahulu oleh orang Yunani kuno yang menyembunyikan pesan dengan cara membuat tato di kepala pembawa berita yang dibotaki dan menunggu sampai rambutnya tumbuh. Teknik steganografi lainnya adalah dengan menggunakan "invisible ink" (tinta yang tidak tampak). Tulisan yang ditulis dengan menggunakan invisible ink ini hanya dapat dibaca jika kertas tersebut diletakkan di atas lampu atau diarahkan ke matahari.

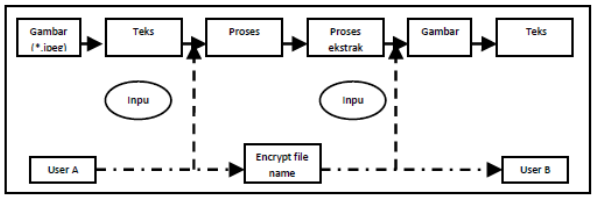
Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama sehingga digunakan metode steganografi. Dengan metode steganografi, pesan yang ingin disampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut. Oleh sebab itu metode steganografi terus digunakan dan dikembangkan sampai saat ini.

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan sistem informasi.

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

II. METODOLOGI PENELITIAN

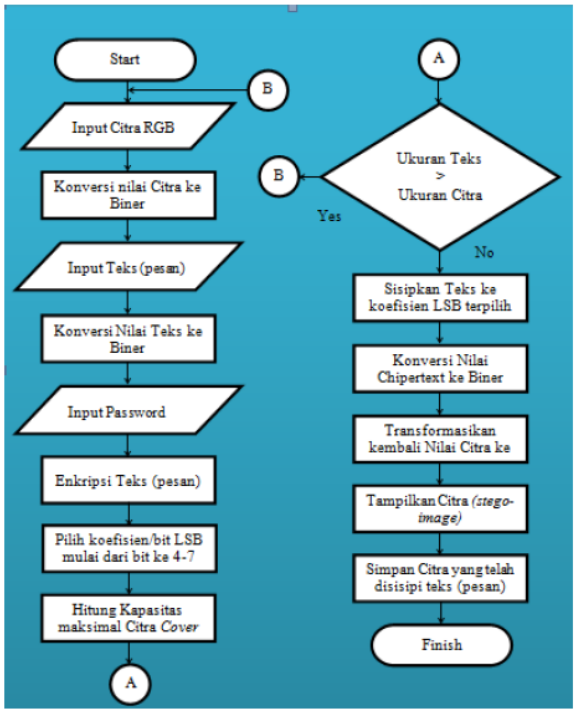
Metode Penelitian yang akan dipakai ialah dengan menggunakan metode diagram alir (flowchart). Diagram alir ini akan menjelaskan proses dari prosedur yang terjadi pada aplikasi dengan simbol-simbol tertentu sehingga dapat menggambarkan algoritma yang terjadi. Dengan penggunaan flowchart memungkinkan penggambaran keseluruhan dari pengambilan data awal hingga dihasilkan keluaran yang diinginkan. Blok diagram dari program implementasi secara umum dengan menggunakan Teknik Least Significant Bit yang diperlihatkan pada Gambar 3.1.



Gambar 3.1 Rancangan implementasi program secara umum.

3.1.1 Diagram alir program penyisipan teks ke dalam gambar

Diagram alir penyisipan teks ke dalam gambar dengan menggunakan Teknik Least Significant Bit pada perangkat lunak steganografi dapat dijabarkan dalam diagram alir pada Gambar 3.2.

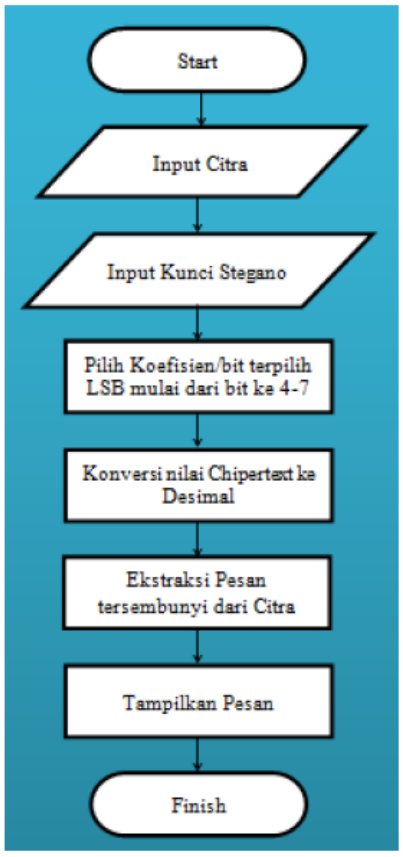


Gambar 3.2 Flowchart penyisipan (enkripsi) teks ke dalam gambar

Pada proses penyisipan (enkripsi) teks ke dalam gambar, gambar yang telah dipilih, nilai pixel file (cover-image) akan dikonversi ke biner (8-bit). Setelah itu memasukan atau memilih file teks (plaintext) yang akan disisipkan dan dilanjutkan dengan membangkitkan pseudo-number Vigenere Cipher. Setelah proses embedding selesai maka sistem akan menghitung daya tampung maksimal file, jika plaintext melebihi kapasitas kemampuan dari cover-image maka sistem akan menolak untuk melanjutkan dan meminta untuk mengurangi jumlah pesan. Jika cover-image mampu menampung maka proses melanjutkan mengkonversi nilai biner chiper-text (stego-image) ke nilai desimal dan dilanjutkan konversi nilai desimal ke nilai pixel dan akhirnya menyimpan (save) file cover-image yang sudah disisipi pesan (chiper-text).

3.1.2 Diagram alir program ekstraksi teks yang terdapat pada gambar

Diagram alir pengekstrakan teks yang ada pada gambar dapat dijelaskan pada Gambar 3.3.



Gambar 3.3 Flowchart untuk proses pengekstrakan teks yang ada dalam gambar

Pada proses ekstraksi (dekrpsi) teks yang terkandung di dalam stego-image dipilih dan nilai pixel citra (stego-image) akan dikonversi ke biner (8-bit) dan dilanjutkan dengan membangkitkan pseudo-number Vigenere Cipher. selanjutnya mengambil nilai bit terakhir (LSB) di tiap pixelnya, dan nilai

biner dikonversi dari biner ke desimal dan pesan (plain-text) ditampilkan.

III. HASIL DAN PEMBAHASAN

4.1 Batasan Implementasi

Aplikasi "Steganografi LSB dengan Enkripsi Vinegere Cipher Pada Citra Jpeg" ini dibuat dengan menggunakan bahasa pemrograman Visual Basic 6.0. Tahap implementasi merupakan tahap yang akan membangun sebuah sistem berdasarkan atas analisis kebutuhan sistem yang telah dirancang sehingga akan dihasilkan sistem yang dapat menghasilkan tujuan yang akan dicapai.

Sebelum program diterapkan dan diimplementasikan, maka program harus free error (bebas kesalahan). Kesalahan program yang mungkin terjadi antara lain kesalahan penulisan bahasa, kesalahan waktu proses, atau kesalahan logikal. Setelah program bebas dari kesalahan, program di tes dengan memasukkan data yang akan diolah.

4.2 Implementasi Antarmuka

4.2.1 Tampilan Menu

pembuatan perangkat lunak ini terdiri dari beberapa tahapan yaitu tahap pemrograman visual, tahap penulisan kode, dan tahap debugging. lunak yang dibuat dengan meng-compile program. Metode pengujian yang digunakan adalah trial and error, dimana setiap langkah yang menghasilkan output diteliti kembali keabsahannya, sehingga hasil yang didapatkan benar-benar dengan metode yang digunakan.

A. Proses Enkripsi :

1. Memilih gambar yang akan dijadikan media penyisipan.
2. Memasukkan atau mengetikkan teks yang akan disisipkan.
3. Memasukkan password
4. Memproses dan menyimpan file yang telah dilakukan proses steganografi.

B. Proses Dekripsi:

1. Memilih gambar yang akan diekstraksi yang sudah mengandung pesan.
2. Memasukkan kunci enkripsi (password).
3. Mengekstraksi file gambar (gambar stego) yang mengandung pesan proses steganografi sehingga menampilkan pesan yang tersembunyi di dalam gambar.

4.3 Pengujian

Pengujian merupakan tahap yang utama dalam pembuatan suatu aplikasi perangkat lunak. Hasil pengujian yang didapat, akan dijadikan sebagai tolak ukur dalam proses pengembangan selanjutnya. Pengujian ini dilakukan untuk mengetahui hasil yang didapat dari perangkat lunak yang telah dibuat. Aplikasi dibuat menggunakan perangkat lunak Microsoft Visual Basic 6.0 dan denganenggunakan Sistem Operasi Microsoft Windows 7 Home Premium.

Pelaksanaan Pengujian dengan Materi yang akan diujikan pada aplikasi Steganografi ini adalah sebagai berikut:

1. Penyisipan (enkripsi) Pesan.

Proses ini meliputi:

a. Input File (cover-image).
b. Input pesan.
c. Input Kunci Enkripsi (password).

2. Ekstraksi (dekripsi) Pesan.

Proses ini meliputi:

a. Input File (stego-image).
b. Input Kunci Enkripsi (password).
c. Ekstraksi (dekripsi) pesan.

3. Error

Akan dilakukan pengujian apakah error akan keluar apabila pengguna salah memasukkan sebuah data atau ukuran teks terlalu besar untuk disisipi ke dalam cover-image.

4.4 Analisis Hasil

Pada tahap ini akan dijelaskan analisis hasil kinerja dari aplikasi Steganografi LSB ini. Sebagai berikut:

4.4.1 Analisis Enkripsi Pesan

Pada proses penyisipan (enkripsi) teks ke dalam gambar, gambar yang telah dipilih, nilai pixel file(cover-image) akan dikonversi ke biner (8-bit). Setelah itu memasukan atau memilih file teks (plaintext) yang akan disisipkan dan dilanjutkan dengan membangkitkan pseudo-number Vigenere Cipher. Setelah proses embedding selesai maka sistem akan menghitung daya tampung maksimal file, jika plaintext melebihi kapasitas kemampuan dari cover-image maka sistem akan menolak untuk melanjutkan dan meminta untuk mengurangi jumlah pesan. Jika cover-image mampu menampung maka proses melanjutkan mengkonversi nilai biner chiper-text (stego-image) ke nilai desimal dan dilanjutkan konversi nilai desimal ke nilai pixel dan akhirnya menyimpan (save) file cover-image yang sudah disisipi pesan (chiper-text).

Sebagai contoh pengujian sebagai berikut :

Enkripsi Pesan.

Plaintext : "ATTACK"

Kunci : "NOW"

Nilai Citra Digital True Color 24-Bit RGB *(Cover-image)*

(100,121,80)	(90,74,190)	(100,81,80)
(81,180,34)	(80,122,201)	(84,120,100)
(100,120,80)	(80,122,200)	(80,122,200)
(100,121,80)	(90,74,190)	(100,81,80)
(81,180,34)	(80,122,201)	(84,120,100)
(100,120,80)	(80,122,200)	(80,122,200)

Enkripsi Vigenere Cipher :

Plaintext	A	T	T	A	C	K
Kunci	N	O	W	N	O	W
Ciphertext	N	H	P	N	Q	G

Konversi nilai piksel berkas citra digital 24-Bit RGB ke biner :

(01100100,01111000, 01010000)	(01011010,01001011, 10111110)	(01100100,01010000, 01010000)
(01010000,10110100, 00100011)	(01010000,01111010, 11001000)	(01010101,01111000, 01100100)
(01100100,01111000, 01010000)	(01010000,01111010, 11001000)	(01100100,01111010, 11001000)
(01100100,01111000, 01010000)	(01011010,01001011, 10111110)	(01100100,01010000, 01010000)
(01010000,10110100, 00100011)	(01010000,01111010, 11001000)	(01010101,01111000, 01100100)
(01100100,01111000, 01010000)	(01010000,01111010, 11001000)	(01100100,01111010, 11001000)

Konversi biner ke nilai piksel citra :

Nilai Citra Digital 24-Bit RGB yang sudah disisipi pesan.

(100, 121, 80)	(90, 75, 191)	(101, 80, 80)
(81, 180, 34)	(81, 122, 200)	(84, 120, 101)
(100, 121, 120)	(120, 122, 200)	(100, 123, 200)
(100, 121, 81)	(91, 74, 190)	(101, 80, 81)
(80 180, 34)	(81, 122, 201)	(84, 120, 100)
(101, 121, 81)	(120, 122, 200)	(100, 122, 200)

Konversi ciphertext ke biner :

1. Nilai ASCII huruf “N” : 78, Biner : 0100 1110
2. Nilai ASCII huruf “H” : 72, Biner : 0100 1000
3. Nilai ASCII huruf “P” : 80, Biner : 0101 0000
4. Nilai ASCII huruf “N” : 78, Biner : 0100 1110
5. Nilai ASCII huruf “Q” : 81, Biner : 0101 0001
6. Nilai ASCII huruf “G” : 71, Biner : 0100 0111

Nilai biner ciphertext disisipkan kedalam bit terakhir (LSB) berkas citra :

(01100100,01111001, 01010000)	(01011010,01001011, 10111111)	(01100101,01010000, 01010000)
(01010001,10110100, 00100010)	(01010001,01111010, 11001000)	(01010100,01111000, 01100101)
(01100100,01111001, 01010000)	(01010000,01111010, 11001000)	(01100100,01111011, 11001000)
(01100100,01111001, 01010001)	(01011011,01001010, 10111110)	(01100101,01010000, 01010001)
(01010000,10110100, 00100010)	(01010001,01111010, 11001001)	(01010100,01111000, 01100100)
(01100101,01111001, 01010001)	(01010000,01111010, 11001000)	(01100100,01111010,110 01000)

4.4.2 Analisis Dekripsi Pesan

Pada proses ekstraksi (dekrpsi) teks yang terkandung di dalam stego-image dipilih dan nilai pixel citra (stego-image) akan dikonversi ke biner (8-bit) dan dilanjutkan dengan membangkitkan pseudo-number Vigenere Cipher. selanjutnya mengambil nilai bit terakhir (LSB) di tiap pixelnya, dan nilai biner dikonversi dari biner ke desimal dan pesan (plain-text) ditampilkan. Hasil pendekripsian dengan password benar sebagai berikut:

Dekripsi Pesan.

Cipherteks : “NHPNQG”

Kunci : “NOW”

Nilai File Digital True Color 24-Bit RGB yang mengandung pesan (stego-image).

(100, 121, 80)	(90, 75, 191)	(101, 80, 80)
(81, 180, 34)	(81, 122, 200)	(84, 120, 101)
(100, 121, 120)	(120, 122, 200)	(100, 123, 200)
(100, 121, 81)	(91, 74, 190)	(101, 80, 81)
(80 180, 34)	(81, 122, 201)	(84, 120, 100)
(101, 121, 81)	(120, 122, 200)	(100, 122, 200)

Konversi nilai piksel berkas file stego-image ke biner :

(01100100,01111001, 01010000)	(01011010,01001011, 10111111)	(01100101,01010000, 01010000)
(01010001,10110100, 00100010)	(01010001,01111010, 11001000)	(01010100,01111000, 01100101)
(01100100,01111001, 01010000)	(01010000,01111010, 11001000)	(01100100,01111011, 11001000)
(01100100,01111001, 01010001)	(01011011,01001010, 10111110)	(01100101,01010000, 01010001)
(01010000,10110100, 00100010)	(01010001,01111010, 11001001)	(01010100,01111000, 01100100)
(01100101,01111001, 01010001)	(01010000,01111010, 11001000)	(01100100,01111010, 11001000)

Ambil nilai bit terakhir tiap byte (LSB) dan susun menjadi tiap 8-bit :

01001110 01001000 01010000

01001110 01010001 01000111

Konversi Nilai Biner Ciphertext ke Desimal dan Alfabet :

0100 1110	0100 1000	0101 0000	0100 1110	0101 0001	0100 0111
78	72	80	78	81	71
N	H	P	N	Q	G

Hasil dari Dekripsi Vigenere Cipher :

Ciphertext	N	H	P	N	Q	G
Kunci	N	O	W	N	O	W
Plaintext	A	T	T	A	C	K

Gambar 4.2 Hasil plaintext dengan kunci yang benar.

4.4.3 Pesan Error / Tidak bisa dibaca.

Berikut hasil jika penerima salah memasukkan password:

Cipherteks : “NHPNQG”

Kunci : “WON”

Plainteks : “8T]8CT”

IV. KESIMPULAN

Kesimpulan yang dapat diambil dari penulisan laporan tugas akhir ini adalah sebagai berikut :

1. Implementasi algoritma LSB (Least Significant Bit) dengan enkripsi Vinegere Cipher dapat digunakan cukup baik untuk menyembunyikan pesan di dalam pesan sebuah berkas file multimedia sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut.

2. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada file multimedia uji dalam aplikasi Steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan kecuali pengguna memasukkan password yang salah.

REFERENSI

[1] Menezes Alfred, Oorschot Paul Van and Vanston Sean, 1996. "*HandBook of Applied Cryptography*", CRC Press.

[2] Ariyus, Dony, Kriptografi – Keamanan Data Dan Komunikasi, Graha Ilmu, Yogyakarta, 2006.

[3] Triputra Safei, Timotius, Pengukuran dan Pengujian Kekuatan Algoritma Auto-key Vigenere Cipher, ITB, Bandung, 2012

[4] Leonardo, Kevin Handoyo, Modifikasi Vigenère Cipher dengan Metode Penyisipan Kunci pada Plaintext, ITB, Bandung, 2012

[5] Suranta, Ricardo Pramana, Perbandingan Ketahanan Algoritma LSB dan F5 dalam Steganografi Citra, ITB, Bandung, 2012

[6] B.Tjaru, Setia Negara, Modifikasi Full Vigenere Chipher dengan Pengacakan Susunan Huruf pada Bujur Sangkar Berdasarkan Kunci, ITB, Bandung, 2012

[7] Alatas, Putri, Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital, Universitas Gunadarma, Jakarta, 2009

[8] Suhartana, I Ketut Gede, Pengamanan Image True Color 24 Bit Menggunakan Algoritma Vigenere Cipher Dengan menggunakan Kunci Bersama, Universitas Udayana, Bali.

[9] Ramadhani, Budi, Steganografi pada Citra GIF mengggunakan bahasa pemrograman Delphi, UII, Yogyakarta, 2006

[10] www.cctv-information.co.uk/constant2/sn_ratio.html