Implementasi Enkripsi Triple Transposition Vigenere Cipher Dan Steganografi Metode Least Significant Bit (Lsb) Pada Citra Bitmap

Romanus Damanik
Fakultas Ilmu Komputer Universitas Katolik Santo Thomas Medan
Jl. Setia Budi No. 479-F Tanjung Sari Medan 20132 061-8210161 061-8213269
Email: rdfikom@gmail.com

Abstrak

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Berbeda dengan kriptografi yang merahasiakan makna pesan namun keberadaan pesan tetap ada, steganografi merahasiakan dengan menutupi atau menyembunyikan pesan. Dengan menggabungkan kriptografi dan steganografi maka akan dapat memberikan keamanan yang lebih baik pada pesan rahasia, dimana pesan rahasia (plainteks) yang dimiliki terlebih dahulu dienkripsi dengan menggunakan algoritma Triple Transposition Vigenere Cipher, kemudian cipherteks hasil enkripsi tersebut disembunyikan di dalam media citra bitmap dengan metode steganografi Least Significant Bit (LSB). Implementasi algoritma kriptografi dan metode steganografi diharapkan dapat lebih meningkatkan keamanan pada pesan rahasia.

***Kata Kunci**: Kriptografi, steganografi, plainteks, cipherteks, triple transposition vigenere cipher, least significant bit*

Abstract

Cryptography is both a science and an art to maintain the confidentiality of a message by disguising it as an encrypted form that has no meaning. Unlike cryptography which conceals the meaning of the message but the existence of the message remains, steganography keeps it a secret by covering or hiding the message. By combining cryptography and steganography, it will be able to provide better security for secret messages, where the secret message (plaintext) that is owned is first encrypted using the Triple Transposition Vigenere Cipher algorithm, then the encrypted ciphertext is hidden in the bitmap image media by the steganography method Least Significant Bit (LSB). The implementation of cryptographic algorithms and steganographic methods is expected to further improve security of secret messages.

***Keywords**: Cryptography, steganography, plaintext, ciphertext, triple transposition vigenere cipher, least significant bit*

1. PENDAHULUAN

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. 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).

Dengan menggabungkan kriptografi dan steganografi maka akan dapat memberikan keamanan yang lebih baik pada pesan rahasia, dimana pesan rahasia yang dimiliki terlebih dahulu dienkripsi dengan menggunakan algoritma Triple Transposition Vigenere Cipher, kemudian cipherteks hasil enkripsi tersebut disembunyikan di dalam media citra bitmap dengan metode steganografi Least Significant Bit (LSB). Implementasi algoritma kriptografi dan metode steganografi diharapkan dapat lebih meningkatkan keamanan pada pesan rahasia. Berdasarkan uraian di atas, maka penulis mengambil judul "Implementasi Enkripsi Triple Transposition Vigenere Cipher Dan Steganografi Metode Least Significant Bit (Lsb) Pada Citra Bitmap".

2. METODE PENELITIAN

Metode diperlukan sebagai kerangka dan panduan proses penelitan, sehinga rangkaian proses penelitan dapat dilakukan secara teratur dan sistematis.

2.1 Analisis Algoritma Triple Transposition Vigenere Cipher

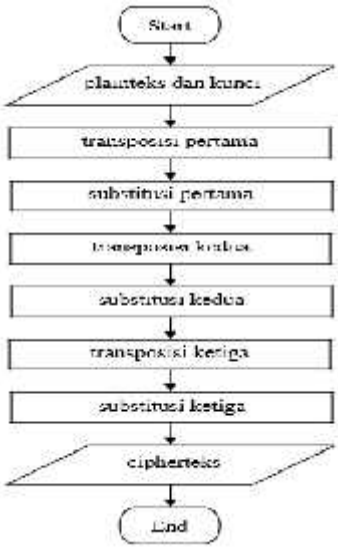
Berikut ini penulis akan menjelaskan seluruh tahapan yang dilakukan pada algoritma Triple Transposition Vigenere Cipher, seperti berikut ini:

1. Proses Enkripsi

Langkah-langkah dalam melakukan proses enkripsi pada algoritma Triple Transposition Vigenere Cipher adalah sebagai berikut:

a. Input plainteks yang akan di enkripsi beserta kunci.
b. Lakukan operasi transposisi pertama (T1)
c. Lakukan operasi substitusi pertama (S1)
d. Lakukan operasi transposisi kedua (T2)
e. Lakukan operasi substitusi kedua (S2)
f. Lakukan operasi transposisi ketiga (T3)
g. Lakukan operasi substitusi ketiga (S3), sehingga akan menghasilkan cipherteks

Seluruh tahapan proses enkripsi pada algoritma Triple Transposition Vigenere Cipher dapat dilihat selengkapnya pada gambar 1



Gambar 1 Proses enkripsi Triple Transposition Vigenere Cipher

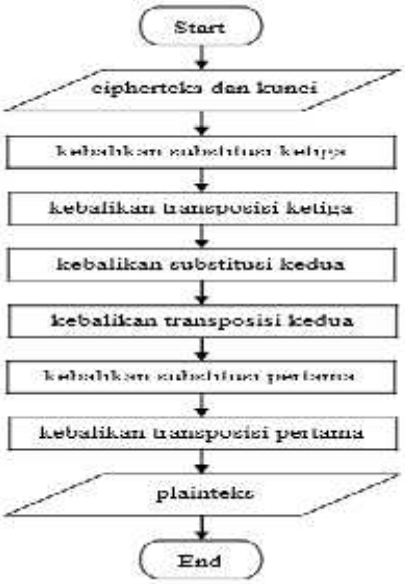
2. Proses Dekripsi

Langkah-langkah dalam melakukan proses dekripsi pada algoritma Triple Transposition Vigenere Cipher adalah sebagai berikut:

a. Input cipherteks yang akan di dekripsi beserta kunci.

b. Lakukan operasi kebalikan substitusi ketiga (S3‟‟)
c. Lakukan operasi kebalikan transposisi ketiga (T3‟‟)
d. Lakukan operasi kebalikan substitusi kedua (S2‟‟)
e. Lakukan operasi kebalikan transposisi kedua (T2‟‟)
f. Lakukan operasi kebalikan substitusi pertama (S1‟‟)
g. Lakukan operasi kebalikan transposisi pertama (T1‟‟), sehingga akan menghasilkan plainteks.

Seluruh tahapan proses dekripsi pada algoritma Triple Transposition Vigenere Cipher dapat dilihat selengkapnya pada gambar 2



Gambar 2 Proses dekripsi Triple Transposition Vigenere Cipher

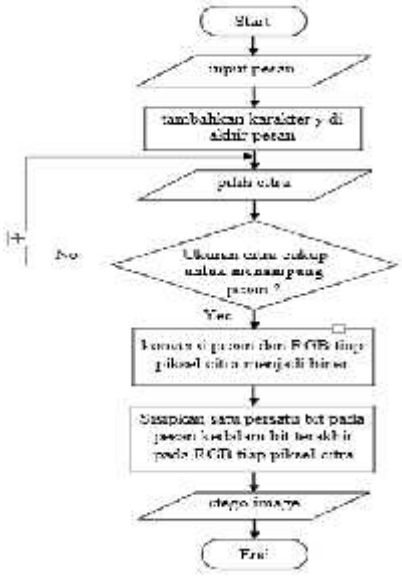
2.2 Analisis Algoritma Least Significant Bit (LSB)

Berikut ini penulis akan menjelaskan seluruh tahapan yang dilakukan pada algoritma Least Significant Bit (LSB), seperti berikut ini:

1. Proses Penyisipan Pesan Langkah-langkah dalam melakukan proses penyisipan pesan menggunakan algoritma LSB adalah sebagai berikut:

a. Input pesan yang akan disisipkan kedalam citra.
b. Tambahkan karakter penanda (**ÿ**) di akhir pesan yang akan disisip.
c. Pilih citra digital (*cover image*).
d. Ubah pesan yang akan disisip kedalam bentuk biner 8 bit.
e. Cek apakah ukuran citra dapat menampung semua bit pesan.
f. Ubah masing-masing nilai RGB pada setiap piksel citra kedalam bentuk biner 8 bit.
g. Ganti bit terakhir pada masing-masing nilai RGB untuk setiap piksel citra dengan bit pesan.
h. Setelah semua bit pada pesan selesai di sisipkan ke citra, selanjutnya ubah kode biner citra digital yang sudah disisipi pesan menjadi nilai RGB citra baru *(stego image*).

Seluruh tahapan proses penyisipan pesan menggunakan algoritma Least Significant Bit (LSB) dapat dilihat selengkapnya pada gambar 3

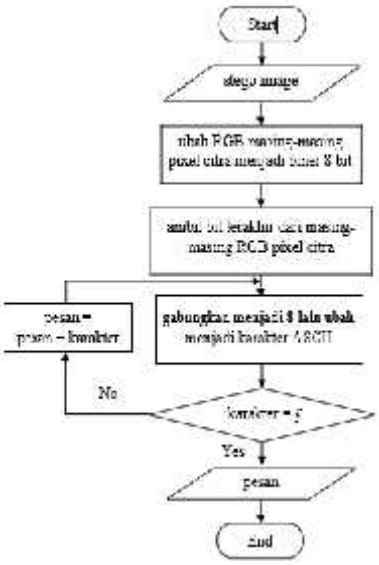


Gambar 3 Proses penyisipan pesan dengan algoritma LSB

2. Proses Ekstraksi Pesan.
   Langkah-langkah dalam melakukan proses ekstraksi pesan menggunakan algoritma LSB adalah sebagai berikut:

a. Pilih file citra (*stego image*).
b. Ubah nilai RGB pada tiap piksel stego image dalam bentuk biner 8 bit
c. Ambil bit terakhir dari masing-masing nilai RGB pada setiap piksel.
d. Gabungkan menjadi 8 bit lalu ubah menjadi karakter sesuai table ASCII.
e. Bila ditemukan karakter penanda (**ÿ**), maka proses berhenti dan hapus karakter penanda (**ÿ**), lalu tampilkan pesan.

Seluruh tahapan proses ekstraksi pesan dengan algoritma Least Significant Bit (LSB) dapat dilihat selengkapnya pada gambar 4



Gambar 4 Proses ekstraksi pesan dengan algoritma LSB

3. HASIL DAN PEMBAHASAN

1 Form Utama

Pada form utama ini terdapat enam buah menu utama. Diantaranya adalah menu "*Ciptakan Kunci*" yang berfungsi untuk menampilkan form input kunci, menu "*Pengamanan*" yang berfungsi untuk menampilkan form enkripsi dan penyisipan file teks, menu "*Pengungkapan*" yang berfungsi untuk menampilkan form ekstraksi dan dekripsi file teks, menu "*Bantuan*" yang berfungsi untuk menampilkan form bantuan, menu "*Informasi*" yang berfungsi untuk menampilkan form informasi, dan yang terakhir menu "*Keluar*" yang berfungsi untuk menutup aplikasi. Form utama merupakan form yang pertama sekali muncul ketika aplikasi dijalankan. Fungsi dari form utama ini adalah sebagai kontrol pada sistem, dimana untuk melakukan aksi ke form yang lain, maka harus di kontrol dari form utama. Tampilan form utama dapat dilihat selengkapnya pada Gambar 5

Gambar 5 Tampilan Form Utama

2. Form Input Kunci

Form input kunci ini merupakan form yang berfungsi untuk menginputkan kunci, yang nantinya dapat digunakan untuk melakukan proses enkripsi dan juga proses dekripsi file teks (.txt). Setelah kunci di input, selanjutnya kunci disimpan dengan cara mengklik tombol "*Simpan*". Tampilan form input kunci dapat dilihat seperti pada gambar 6

Gambar 6 Tampilan Form Input Kunci

3. Form Enkripsi dan Penyisipan File Teks

Form enkripsi dan penyisipan file teks ini merupakan form yang berfungsi untuk melakukan proses enkripsi file teks dan juga melakukan proses penyisipan file teks kedalam citra digital. Tampilan form enkripsi dan penyisipan file teks dapat dilihat seperti pada gambar 7

Gambar 7 Tampilan Form Enkripsi dan Penyisipan File Teks

Sebelum melakukan proses enkripsi, pertama-tama yang harus dilakukan adalah memilih file teks (.txt) yang akan di enkripsi. Bila proses enkripsi dilakukan sebelum memasukkan file teks maka akan muncul pesan peringatan seperti gambar 8

Gambar 8 Peringatan File Teks Belum Dimasukkan

Untuk memasukkan file teks kedalam form, dapat dilakukan dengan cara mengklik tombol "*Open Teks*", lalu mencari file teks yang akan dienkripsi pada direktori yang telah ditempatkan. Setelah file teks dipilih, selanjutnya klik tombol "*Enkripsi*" untuk melakukan proses enkripsi terhadap file teks. Setelah proses enkripsi selesai, maka tahap selanjutnya adalah melakukan proses penyisipan file teks. Sebelum melakukan proses penyisipan, yang harus dilakukan adalah memilih file citra (.bmp) yang akan dijadikan penampung pesan. Bila proses penyisipan dilakukan sebelum memasukkan file citra maka akan muncul pesan peringatan seperti gambar 9

Gambar 9 Peringatan File Citra Belum Dimasukkan

Untuk memasukkan file citra, dapat dilakukan dengan cara mengklik tombol "*Open Citra*", lalu cari file citra digital yang akan dijadikan sebagai penampung pesan pada direktori yang telah ditempatkan. Setelah citra digital berhasil dimasukkan, selanjutnya *user* dapat mengklik tombol "*Penyisipan*", supaya sistem melaksanakan proses penyisipan pesan kedalam citra digital. Apabila dimensi file citra terlalu kecil dan tidak dapat menampung semua pesan, maka akan muncul pemberitahuan seperti gambar 10

Gambar 10 Peringatan Dimensi Citra Tidak Cukup Untuk Menampung Pesan

Namun apabila dimensi file citra dapat menampung pesan yang akan disisipkan dan proses penyisipan telah selesai, maka akan muncul pemberitahuan seperti gambar 10

Setelah proses penyisipan pesan selesai dilakukan, selanjutnya klik tombol "*Save Citra*" untuk menyimpan file citra hasil proses penyisipan ke direktori yang diinginkan. Apabila proses penyimpanan file citra selesai, maka akan muncul pesan pemberitahuan seperti gambar 11

Gambar 11 Pemberitahuan File Citra Berhasil Disimpan

Setelah proses penyimpanan file citra hasil penyisipan selesai, selanjutnya klik tombol "*Keluar*" untuk menutup form enkripsi dan penyisipan file teks.

4 Form Ekstraksi Dan Dekripsi File Teks

Form ekstraksi dan dekripsi file teks ini merupakan form yang berfungsi untuk melakukan proses ekstraksi file teks dan juga melakukan proses dekripsi file teks. Tampilan form ekstraksi dan dekripsi file teks dapat dilihat seperti pada gambar 12

Gambar 12 Tampilan Form Ekstraksi dan Dekripsi File Teks

Sebelum melakukan proses ekstraksi, pertama-tama yang harus dilakukan adalah memilih file citra (.bmp) yang akan di ekstraksi. Bila proses ekstraksi dilakukan sebelum memasukkan file citra maka akan muncul pesan peringatan seperti gambar 13

Gambar 13 Peringatan File Citra Belum Dimasukkan

Untuk memasukkan file citra kedalam form, dapat dilakukan dengan cara mengklik tombol "*Open Citra*", lalu mencari file citra yang akan diekstraksi pada direktori yang telah ditempatkan. Setelah file citra dipilih, selanjutnya klik tombol "*Ekstraksi*" untuk melakukan proses ekstraksi terhadap file citra. Setelah proses ekstraksi selesai, maka akan muncul pemberitahuan seperti gambar 14

Gambar 14 Pemberitahuan Proses Ekstraksi Pesan Berhasil

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan, dan pengujian yang telah dilakukan. Maka penulis memperoleh beberapa kesimpulan, diantaranya adalah sebagai berikut :

1. Plainteks yang di input akan di enkripsi dengan algoritma triple transposition vigenere cipher untuk menghasilkan cipherteks.
2. Cipherteks akan disisipkan kedalam citra bitmap dengan algoritma least significant bit(LSB).
3. Citra bitmap yang telah disipsip akan di ekstrak untuk menhasilkan cipherteks.
4. Cipherteks akan di dekripsi untuk menghasilkan plainteks semula.
5. File citra yang digukan sebagai penampung pesan adalah file citra 24 bit bitmap.
6. Ukuran file teks yang dapat disisipkan kedalam citra harus lebih kecil dari ukuran file citra.

Stego image yang dihasilkan memiliki ukuran yang tidak berbeda jauh dari citra asli dan keberadaan pesan rahasia sulit untuk dilihat oleh indera penglihatan karena secara visual kedua citra terlihat sama.

DAFTAR PUSTAKA

[1] Anindyawati Nina, Suryani Esti, 2012, Pembangunan Aplikasi Penyembunyian Pesan Menggunakan Metode End Of File (EOF) ke dalam Citra Digital Terhadap Pesan yang Terenkripsi Dengan Algoritma RSA, Jurnal ITSMART. Vol 1 (1)

[2] Ariyus Dony, 2008, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Andi Offset, Yogyakarta

[3] Lubis Ali Akbar, Wong Ng Poi, Arfiandi Irfan, Damanik V Immanuel dan Maulana Adithya, 2015, Steganografi Pada Citra Dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher, JSM STMIK Mikroskil. Vol 16 (2) : 125-134

[4] Munir Rinaldi, 2006, *Kriptografi*, Informatika, Bandung

[5] Saefullah Asep, Himawan, Agani Nazori, 2012, Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Media Image Dengan Menggunakan Metode LSB, Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)

[6] Sadikin R, 2012, *Kriptografi Untuk Keamanan Jaringan*, Andi Offset,Yogyakarta

[7] Suarga, 2012, *Algoritma dan Pemrograman*, Andi Offset, Yogyakarta

[8] Zain, Ruri Hartika, 2012, Perancangan dan Implementasi Cryptography Dengan Metode Algoritma RC4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6.0, Jurnal Momentum. Vol 12 (1)