Pengamanan File Teks Dengan Menggunakan Metode *Enhanced LSB SteganografiI* (4 BIT)

[1]Mangisi Parulian, [2]Parasian Silitonga
[1]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
[2]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
e-mail : parulianmangisi2@gmail.com; [2]parsianirene@gmail.com

Abstrak

Informasi-informasi rahasia perlu disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahuioleh pihakyang tidak dikehendaki atau berwenang.Salah satu caranya adalah dengan menggunakanteknik Steganografi.Padakesempatan ini, penulisakanmembahastentang pengamanan fileteksmenggunakan algoritma Enhanced LSB Steganografi. Dimana pertama-tamamenyembunyikan data rahasia sedemikian sehingga keberadaan data rahasia tidak terdeteksi oleh indera manusia.Algoritma steganografi Enhanced Least Significant Bit (Enhanced LSB) dapat mengoptimalkan mekanisme Least Significant Bit (LSB) dengan memanfaatkan warna RGB pada keseluruhan pixel dalam citra dan dapat menampung sampai 4 bit dalam setiap pixel RGB. Tidak jauh berbeda dengan LSB, pada Enhanced Least Significant Bit (Enhanced LSB) dilakukan peningkatan dalam penyembunyian pesan yang awalnya hanya penyisipan pada 1 digit paling kanan, kini ditingkatkan dengan penyisipan pada 4 digit paling kanan.

Kata Kunci : *Keamanan data, steganografi, Enhanced Least Significant Bit (Enhanced LSB).*

Abstract

Confidential information should be stored or transmitted in a certain way so as not to be known by unwanted or authorized parties. One way is to use the Steganography technique. On this occasion, the author will discuss about securing text file using Enhanced LSB Steganography algorithm. Where it first conceals confidential data in such a way that the existence of secret data is not detected by the human senses. The Enhanced Least Significant Bit (LSB) Enhanced Least Significant Bit (LSB) algorithm optimizes the Least Significant Bit (LSB) mechanism by utilizing RGB color on the entire pixel in the image and can hold up to 4 bits in each RGB pixel. Not much different from the LSB, in Enhanced Least Significant Bit (Enhanced LSB) an increase in the concealment of messages originally only insertion on the rightmost 1 digit, now enhanced by insertion on the 4 rightmost digits.

Keywords *:Data security, steganography, Enhanced Least Significant Bit (Enhanced LSB).*

1. PENDAHULUAN

Di dalam penggunaan media internet untuk melakukan pertukaran informasi yang telah berkembang menyebabkan kekhawatiran terkait keamanan dan kerahasiaan data yang di kirimkan. Untuk mengamankan data yang di kirimkan melalui media internet, maka diperlukan suatu teknik keamanan yaitu *Steganografi.*

Steganografi adalah ilmu dan seni menyembunyikan data rahasia sedemikian sehinggakeberadaan data rahasia tidak terdeteksi oleh indera manusia. *Steganografi* digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Sedangkan data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Cara paling umum untuk menyembunyikan data adalah dengan memanfaatkan *Least Significant Bit* (LSB), yaitu bit data rahasia disisipkan pada bit terakhir pada *byte* file penampung. Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Kekurangan dari metode LSB ini adalah pesan penyisip dapat dengan mudah ditebak keberadaanya karena letak penyisip sudah pasti berada pada bit-bit terakhir dari file penampung.

Algoritma steganografi *Enhanced Least Significant Bit* (*Enhanced* LSB) dapatmengoptimalkan mekanisme *Least Significant Bit* (LSB) dengan memanfaatkan warna RGB pada keseluruhan pixel dalam citra dan dapat menampung sampai 4 bit dalam setiap pixel RGB. Tidak jauh berbeda dengan LSB, pada *Enhanced Least Significant Bit* (*Enhanced LSB*) dilakukan peningkatan dalam penyembunyian pesan yang awalnya hanya penyisipan pada 1 digit paling kanan, kini ditingkatkan dengan penyisipan pada 4 digit paling kanan. Dengan menggunakan *Enhanced LSB*, maka keberadaan data yang disembunyikan akan lebih sulit untuk di deteksi.

Berdasarkan uraian diatas, maka penulis mengangkat permasalahan ini ke dalam satu topik pembahasan yang di beri judul *Pengamanan File Teks Dengan Menggunakan Metode Enhanced LSB Steganografi (4 Bit).*

2. METODE PENELITIAN

2.1. Steganografi

Keamanan merupakan salah satu aspek yang paling terpenting dari sebuah sistem informasi. Masalahkeamanan sering kurang diperhatikandari para perancang dan pengelola sisteminformasi. Masalah keamanan sering beradadiurutan awal setelah tampilan, atau bahkan diurutanterakhir dalam daftar hal-hal yang dianggap sangat penting. Keamanan adalah keadaan bebas dari bahaya.Istilah ini dapat digunakan dengan hubungan kepada tindak kriminal atau kejahatan, manipulasi dan segala bentuk kecelakaan.Keamanan merupakan topik yang sangat luas termasuk keamanan nasional terhadap serangan teroris,keamanan komputer terhadap *hacker,* keamanan rumah terhadap maling, keamanan pada atm [2]. Keamanan komputer meliputi lima aspek, antara lain [2] :

1. *Authentication*: agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar dari orang yang dikehendaki.
2. *Non-repudiation*: merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
3. *Authority*: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
4. *Privacy*: lebih ke arah data-data yang bersifat pribadi.
5. *Access Control*: aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses

seringkali dilakukan dengan menggunakan kombinasi user id dan password ataupun dengan mekanisme lain.

2.2. Metode LSB

Algoritma steganografi *Enhanced Least Significant Bit* (*Enhanced* LSB) dapatmengoptimalkan mekanisme *Least Significant Bit* (LSB) dengan memanfaatkan warna RGB pada keseluruhan pixel dalam citra dan dapat menampung sampai 4 bit dalam setiap pixel RGB. Tidak jauh berbeda dengan LSB, pada *Enhanced Least Significant Bit* (*Enhanced LSB*) dilakukan peningkatan dalam penyembunyian pesan yang awalnya hanya penyisipan pada 1 digit paling kanan, kini ditingkatkan dengan penyisipan pada 4 digit paling kanan. Dengan menggunakan *Enhanced LSB*, maka keberadaan data yang disembunyikan akan lebih sulit untuk di deteksi.

Metode LSB merupakan teknik substitusi pada steganografi. Biasanya, arsip 24-bit atau 8-bit digunakan untuk menyimpan citra digital. Representasi warna dari piksel–piksel bisa diperoleh dari warna–warna primer, yaitu merah, hijau dan biru. Citra 24-bit menggunakan 3 byte untuk masing–masing piksel, dimana setiap warna primer direpresentasikan dengan ukuran 1 byte. Penggunaan citra 24-bit memungkinkan setiap piksel direpresentasikan dengan nilai warna sebanyak 16.777.216. Dua bit dari saluran warna tersebut biasa digunakan menyembunyikan data yang akan mengubah jenis warna piksel-nya menjadi 64 warna. Hal itu akan mengakibatkan sedikit perbedaan yang tidak bisa dideteksi secara kasat mata oleh manusia (Ariyus, 2009).

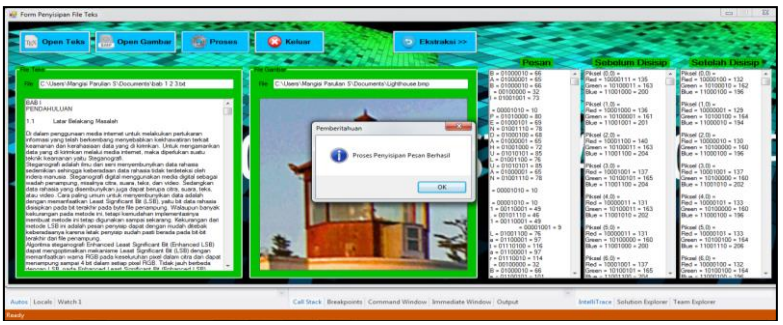
Untuk menjelaskan metode ini, digunakan citra digital sebagai *stegomedium*. Pada setiap byte terdapat bit yang tidak signifikan. Misalnya pada byte 00011001, maka bit LSB-nya adalah 1. Untuk melakukan penyisipan pesan, bit yang paling tepat untuk diganti dengan bit pesan adalah bit LSB, sebab pengubahan bit tersebut hanya akan mengubah nilai byte-nya menjadi satu lebih tinggi atau satu lebih rendah. Sebagai contoh, urutan bit berikut ini menggambarkan 3 piksel pada stegomedium24-bit.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Sistem

Setelah tahap implementasi selesai, maka akan dilanjutkan kepada tahap pengujian sistem.Dalam hal ini sistem akan diuji coba dalam melakukan proses penyisipan dan ekstraksi. Sehingga dapat diketahui keberhasilan dari sistem yang dibangun.

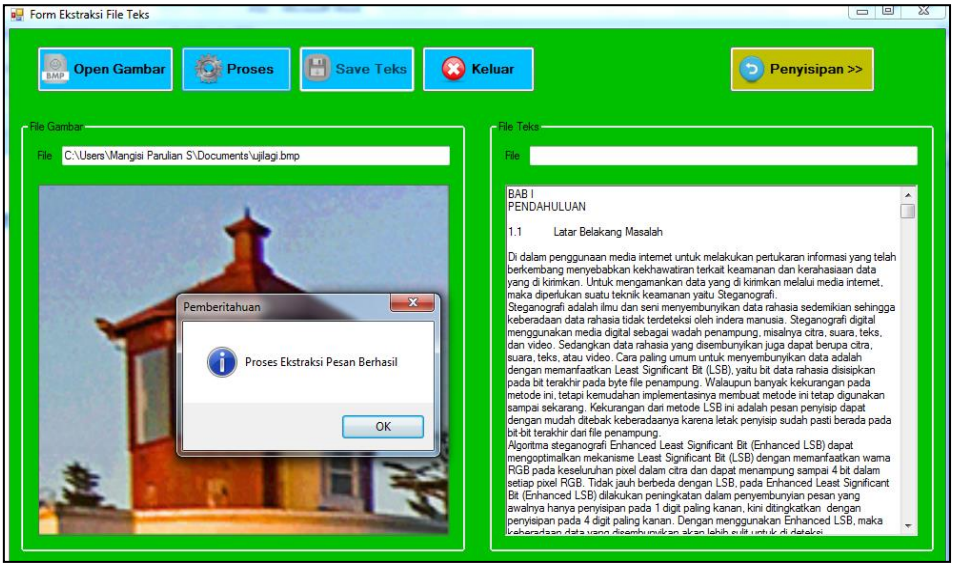
Untuk melakukan proses penyisipam pesan,pertama-tama jalankan aplikasisehingga akan muncul form utama. Lalu klik menu*"Penyisipan"*,sehinggaformpenyisipan pesanakan muncul. Selanjutnya klik *"open teks"* lalu masukkan pesan yang berupa file teks (txt), kemudian klik *"open gambar"* lalu masukkan gambar yang akan menjadi penampung yang berekstensi BMP. Setelah itu klik tombol "*proses*" maka akan muncul kata "Proses Penyisipan Pesan Berhasil" Tampilan proses penyisipan pesan.



Gambar 3.1. **Proses Penyisipan Pesan**

3.2. Pembahasan

Setelah proses penyisipan pesan berhasil dilakukan, tahap selanjutnya adalah melakukan prosesekstraksi. Klik menu"*ektraksi*"yang terdapat pada form utama, lalu pilih sub menu "*open gambar*" kemudian klik menu *"proses"*sehingga akan muncul hasil dari yang kita sisipi sebelumnya. Tampilan proses ekstraksi pesan.



Gambar 3.2. Proses Ekstraksi Pesan

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan, dan pengujian yang telah dilakukan maka penulis memperoleh beberapa kesimpulan,d iantaranya adalah sebaga iberikut :

1. Sistem yang dibangun mampu mengamankan file teks da nmemberikan kemudahan bagi pengguna dengan menggunakan algoritmaEnhanced LSB Steganografi.
2. Semakin panjang jumlah karakter pesan maka semakin lama waktu yang dibutuhkan untuk memproses kedalam gambar.
3. Ukuran(size) file gambar yang berekstensi BMP semakin tinggi maka proses hasil RGB nya semakin lama waktu yang dibutuhkan untuk prosesnya.

5. SARAN

Untuk pengembangan lebih lanjut maka penulis memberikan saran yang sangat bermafaat yaitu :

1. Aplikasi dapat dikombinasikan dengan metode yang berbeda sehingga proses keamanan menjadi lebihbaik.
2. Kombinasi file dapat dilakukan dengan teks, gambar, maupun audio.

DAFTAR PUSTAKA

[1] Adelia, Setiawan Jimmy,2011, *Implementasi Customer Relationship Management (CRM) pada Sistem Reservasi Hotel berbasisi Website dan Desktop*Vol. 6

[2] Ariyus, D.2008.Pengantar Ilmu Kriptografi, Andi:Yogyakarta.

[3] Mahgribi Maulana Ricky, Oktaviana Tri Lucky.*Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) Dalam Pengamanan Data File Audio Mp3*

[4] Pardosi Adiputra Irpan,dkk,2015, *Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi,*ISSN. 1412-0100,VOL 16

[5] Rinaldi Munir,2004*,Steganografi dan Watermarking*, If5054: Bandung

[6] Sadikin Rifki,2012, *Kriptografi untuk Keamanan Jaringan*,Andi:Yogyakarta.

[7] Satriya Wijaya Ermadi, Prayudi Yudi,2015*, Integrasi Metode Steganografi DCS Pada Image Dengan Kriptografi Blowfish Sebagai Model Anti Forensik untuk Keamanan Ganda Konten Digital,*ISSN: 1907 – 5022.