Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume (2) No.1 Maret 2018, pp. 57-65
ISSN:2548-9771/EISSN:2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Penggunaan Algoritma *Kriptografi Steganografi Least Significant Bit* Untuk Pengamanan Pesan Teks dan Data Video

Indra Gunawan[1], Sumarno[2]
[1,2] STIKOM Tunas Bangsa
[1,2] Jl. Jend. Sudirman Blok A, No. 1, 2 dan 3 Kota Pematangsiantar, Sumatera Utara
[1]indra@amiktunasbangsa.ac.id, [2]sumarno@amiktunasbangsa.ac.id

Abstract

Some areas that are still discussed from a computer science research for a data security is the use of LSB steganography (Least Significant Bit) cryptography algorithm. Delivery of text and video data without being equipped with a security system from the LSB steganography algorithm can eliminate messages to be inserted into the video. The use of the LSB steganography algorithm can improve the security of messages to be sliced and sent to the recipients of messages. This analysis aims to improve text and video security by inserting text into video, then shuffling video so that the video can not be seen.

Keywords : *Criptography, Steganography, Least Significant Bit, Data Security*

Abstrak

Beberapa bidang yang masih dibahas dari sebuah penelitian ilmu komputer untuk sebuah keamanan data adalah penggunaan kriptografi algoritma steganografi LSB (Least Significant Bit). Pengiriman data teks dan video tanpa dilengkapi dengan sebuah sistem keamanan dari algoritma steganografi LSB dapat menghilangkan pesan yang akan disisipkan kedalam video. Penggunaan dari algoritma steganografi LSB dapat meningkatkan keamanan pesan yang akan disispkan dan dikirimkan kepada sipenerima pesan. Analisa ini bertujuan untuk meningkatkan pengamanan teks dan video dengan cara menyisipkan teks kedalam video, lalu mengacak video sehingga video tersebut pun tidak dapat dilihat.

Kata Kunci *: Kriptografi, Steganografi, Least Significant Bit, Keamanan Data*

1. PENDAHULUAN

Menjaga keamanan dan kerahasiaan data merupakan hal yang sangat penting untuk melakukan sebuah proses pengiriman data, baik itu data teks dan video melalui jaringan internet yang sudah terkoneksi dengan sangat luas. Telah banyak model dari keamanan data yang telah dikembangkan untuk kepentingan dari proses mengamankan data yang akan dikirim, salah satunya adalah algoritma steganografi. Algoritma steganografi memiliki alur yang searah dengan kriptografi, dimana steganografi memiliki tujuan untuk menyembunyikan pesan-pesan rahasia melalui sebuah perantara, yaitu media. Sedangkan kriptografi sendiri memiliki bentuk untuk memberikan beberapa samaran dari sebuah pesan melalui media digital. Dengan kata lain sebuah data berbentuk teks dapat disembunyikan kedalam sebuah video.

Algoritma steganografi mempunyai metode yang bisa digunakan, seperti Least Significant Bit dan End of File. Algoritma dari kedua ini mempunyai model yang berbeda-beda didalam proses penyamaran dan penyembunyian data. Lain dari pada itu, algoritma ini masih juga digunakan untuk sebuah pengembangan didalam ilmu steganografi itu sendiri agar dapat menghasilkan model-model terbaru dari algoritma itu sendiri didalam algoritma steganografi. Pada penelitian sebelumnya dengan judul Pengamanan Acakan BISS menggunakan Algoritma RSA [1], menjelaskan tentang proses penyisipan teks kedalam video lalu mengacak video tersebut. Akan tetapi terlihat perbedaan yang signifikan dari ukuran video yang sudah disisipkan teks.

Berdasarkan dari latar belakang tersebut peneliti mencoba untuk mengembangkan proses penyisipan teks kedalam sebuah video dan mengacak video tersebut tanpa harus mempengaruhi ukuran dari video menjadi sangat besar (*over size*).

2. METODOLOGI PENELITIAN

2.1. Steganografi

Steganografi (*steganography*) berasal dari bahasa yunani yaitu *steganos* yang memiliki arti tersembunyi dan *graphein* yang berarti menulis, sehingga jika disatukan, maka artinya adalah "menulis tulisan yang tersembunyi" [2]. Istilah lainnnya, steganografi adalah sebuah seni atau sebuah ilmu yang diimplementasikan untuk menyisipkan pesan rahasia dengan berbagai cara, sehingga hanya orang yang dituju saja yang dapat mengetahui maksud dan tujuan dari pesan tersebut.

Didalam metode steganografi, memiliki beberapa kriteria yang harus dimiliki, antara lain [3] :

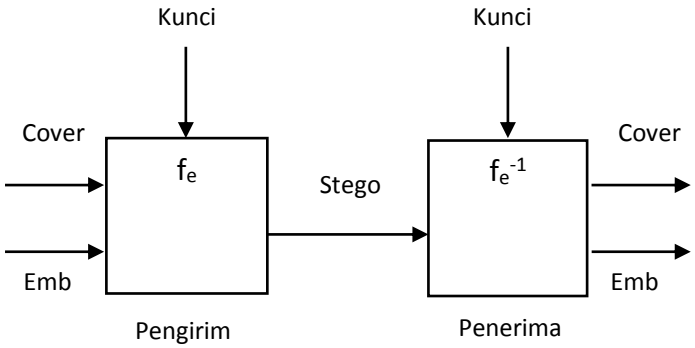
1. *Impercepbility*
   Keberadaan pesan tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan.
2. *Fidelity*
   Mutu dari citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau didalam citra tersebut masih terdapat teks rahasia.
3. *Recovery*
   Pesan rahasia yang disembunyikan didalam citra digital harus dapat diungkapkan kembali seperti aslinya.

Ada juga istilah-istilah yang lain yang memiliki kaitan erat dengan steganografi, yaitu :

1. *Hident Text* atau *embedded message* : pesan yang disembunyikan
2. *Covertext* atau *Cover-Object* : pesan yang digunakan untuk menyembunyikan pesan yang sudah tersembunyi (*embedded message*)

3. *Stegotext* atau *stego-object* : pesan yang sudah berisi pesan tersembunyi (*embedded message*).

Steganografi yang menggunakan media gambar *hiddent text* atau *embedded text* yang sudah disisipkan merupakan pesan yang akan disisipkan kedalam *convertext* atau *coverobject*, yaitu file gambar yang digunakan sebagai media penampung pesan kedalam file gambar yang dihasilkan *stegotext* atau *stego-object* yang merupakan sebuah file gambar yang memiliki pesan *embedded*.



Gambar1. Sistem Steganografi [4]

Penyisipan pesan teks kedalam media *Cover* disebut juga sebagai *encoding*. Sedangkan untuk ekstraksi pesan disebut juga sebagai stego dan biasa dinamakan sebagai *decoding*. Biasanya dari kedua proses ini akan membutuhkan kunci rahasia supaya agar hanya pihak-pihak yang memiliki hak saja yang dapat melaksanakan penyisipan pesan teks seperti yang dapat dilihat pada gambar 1.

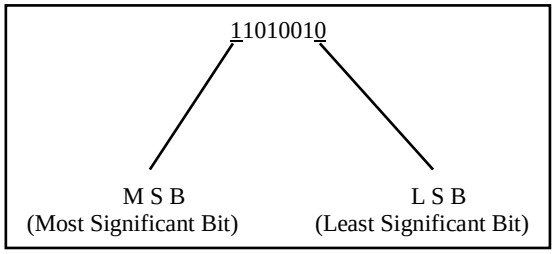
Pada dasarnya didalam algoritma steganografi, memiliki 6 (enam) teknik yang digunakan didalam steganografi [2]:

1. *Injection* (Penanaman) merupakan suatu teknik yang menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya, sehingga mudah dideteksi. Teknik ini sering juga disebut dengan *embedded*.
2. Subsitusi data normal digantikan dengan data rahasia. Biasanya hasil teknik itu tidak perlu mengubah ukuran data asli, akan tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas dari media yang ditumpangi.
3. *Transform domain* (transformasi domain) teknik ini sangat efektif. Pada dasarnya transformasi domain menyembunyikan data pada "*transform space*".
4. *Spread Spectrum* sebuah teknik pentransmisian menggunakan *Pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi signal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi telekomunikasi.

5. *Statistical Method* teknik ini disebut juga skema *steganograpic* 1 bit. Skema tersebut menanamkan 1 bit informasi pada media tumpangan dan mengubah statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0.
6. *Distortion Metode* ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

2.2. Least Significant Bit

Penyembunyian pesan dilakukan dengan merubah bit-bit didalam segmen citra dengan bit-bit pesan rahasia. Metode yang paling sering digunakan adalah dengan modifikasi LSB (*Least Significant Bit*) pada citra penampung. Pada susunan bit didalam sebuah byte, ada bit yang paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang significant atau LSB (*Least Significant Bit*).



Gambar 2. Sampel Susunan Bit pada LSB dan MSB

Contoh susunan Bit pada byte yang mendeskripsikan bit yang cocok untuk dirubah adalah bit LSB, karena pergantiannya hanya merubah nilai byte satu lebih tinggi atau lebih rendah dari nilai sebelumnya. Sampelnya byte didalam sebuah gambar dinyatakan sebuah warna tertentu, maka dilakukan perubahan pada bit LSB dan tidak akan mengganti warna secara signifikan. Sebelum melakukan pergantian bit-bit pada LSB, semua data citra harus dirubah terlebih dahulu kedalam format bit, jadi setiap data piksel dari gambar akan mengandung beberapa komponen warna merah, hijau dan biru (RGB) [5].

Contoh pemakaian metode LSB pada tahapan *encode* :

1. Misalkan penyisipan pada citra 24-bit. Setiap piksel memiliki panjang 24 bit (3 x 3 byte, masing-masing komponen R (1 byte), G (1 byte) dan B (1 byte)). 00110011 10100010 11100010 (sampelnya piksel berwarna merah).
   Sampel *embedded message* : 010
   Encoding 00110010 10100011 11100010
   (Piksel yang berwarna merah berubah sedikit, akan sulit untuk dibedakan dengan citra aslinya)
2. Jika pesan = 10 bit, maka jumlah dari byte yang akan digunakan adalah 10 byte.
   0011001110100010 11100010
   1010101100100110

1001011011001001 11111001
Pesannya adalah : 1110010111
Hasil penyisipan pesan pada bit LSB adalah :
0011001110100011 11100011
1010101000100110
1001011111001000 11111001
1000100110100011

2.3. Metode End of File (EOF)

Metode EOF adalah beberapa metode yang masih digunakan didalam algoritma steganografi. Metode ini menggunakan cara dengan melampirkan data pada akhir file. Sehingga tidak akan mempengaruhi kualitas data awal yang akan dilampirkan pesan. Akan tetapi ukuran file yang telah dilampirkan pesan rahasia akan sedikit bertambah dari ukuran sebelumnya [6].

Metode EOF menggunakan kelemahan indera manusia yang tidak sensitif, sehingga seolah-olah tidak memiliki perbedaan bila dilihat pesan tersebut apakah sudah disisipkan atau belum [7]. Didalam Metode EOF pesan teks yang akan dilampirkan pada media akan dikonversi terlebih dahulu kedalam bilangan nilai desimal berdasarkan yang tertera pada tabel ascii. Kode ascii (*American Standart Code for Information Interchange*) adalah representasi numerik dari karakter-karakter yang digunakan pada komputer dengan ketentuan huruf a-z, A-Z, 0-9 dan simbol standart yang tertera pada *keyboard*.

2.4. Video Digital

Video adalah merupakan sebuah gambar hidup yang bisa dihasilkan dengan rekaman dari benda atau seseorang (termasuk juga didalamnya sebuah fantasi ataupun peraga palsu) dengan menggunakan sebuah kamera yang memiliki fungsi dau atau lebih dimensi yang didapatkan dari sebuah penglihatan dari suatu tempat yang merupakan basis dari dibentuknya sebuah video. Pada umumnya, video terbagi menjadi 2 (dua) macam, yaitu [8]:

a. Analog, merupakan video hasil tangkapan sebuah lensa kamera terhadap tempat (*scane*) yang diambil secara horizontal maupun vertikal.
b. Digital, merupakan video yang direpresentasikan sebagai bagian dari matriks yang beberapa elemennya dapat memiliki sebuah nilai, yaitu nilai intensitas.

Video digital terusun dari serangkaian *frame*. Rangkaian *frame* tersebut ditampilkan pada layar dengan durasi yang memiliki kecepatan tertentu, tergantung dari *frame rate* yang diberikan. Kalau *frame rate* cukup tinggi, maka mata manusia tidak dapat mencerna gambar atau *frame*, tetapi hanya dapat mencerna rangkaian yang berkelanjutan (kontinu).

Jika pixel diletakkan saling bersejajar, maka yang hanya terlihat adalah hanya sebuah garis. Jadi semua garis halus yang terlihat didalam sebuah perangkat komputer merupakan deretan dari sebuah piksel. Sebuah piksel

biasanay bisa dianggap sebagai sebuai titik, namun sebuah piksel lenih mirip dengan sebuah persegi panjang kecil yang memiliki tinggi tidak sebanding dengan lebarnya.

2.5. Moving Picture Experts Group (MPEG-4)

Video digital terdiri dari beberapa frame-frame, dimana frame-frame tersebut dikompres menjadi sebuah file komputer yang dapat dijalankan menggunakan sebuah perangkat lunak multimedia player (Ian,2003). Berdasarkan bentuk-bentuk kompresan dari file video digital tersebut, banyak bermunculan format-format video digital yang ditawarkan kepada pengguna dengan kelebihan dan kekurangannya masing-masing. Salah satu contoh format video digital adalah MP4. MPEG-4 Bagian 14 atau MP4 format file, secara resmi ISO / IEC 14496-14:2003, adalah sebuah standar format multimedia container yang ditetapkan sebagai bagian dari MPEG-4. Hal ini paling sering digunakan untuk menyimpan video digital dan digital stream audio, terutama yang didefinisikan oleh MPEG, tetapi juga dapat digunakan untuk menyimpan data lain seperti subtitle dan gambar diam. Seperti format wadah paling modern, MPEG-4 Part 14 memungkinkan streaming melalui Internet. Trek petunjuk terpisah digunakan untuk menyertakan informasi dalam streming file. Filename extension resmi untuk MPEG-4 Bagian 14 file adalah MP4, sehingga format wadah sering disebut hanya sebagai MP4 [8].

3. HASIL DAN PEMBAHASAN

3.1. Perhitungan Algoritma Kriptografi Steganografi LSB

Dari dasar teoritis yang sudah dibahas, untuk mengenkripsi suatu data menggunakan kriptografi steganografi LSB dibutuhkan beberapa sampel bilangan untuk menampung beberapa karakter yang selanjutnya dikonversi ke bilangan biner, lalu disipkan kedalam sebuah file.

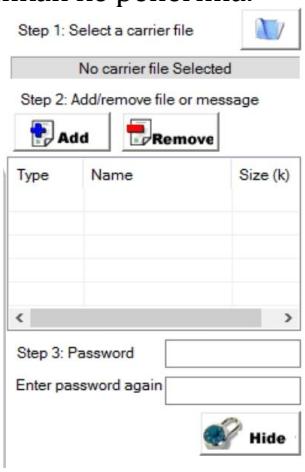
Untuk melihat langkah-langkah atau *Pseudocode* yang digunakan adalah :
Untuk proses enkripsi :

```
k = 1;
  for i = 1 : height
    for j = 1 : width
      LSB = mod(double(c(i,j)), 2);
      if (k>m || LSB == b(k))
        s(i,j) = c(i,j);
      else
        if(LSB == 1)
          s(i,j) = c(i,j) - 1;
        else
          s(i,j) = c(i,j) + 1;
        end
      k = k + 1;
```

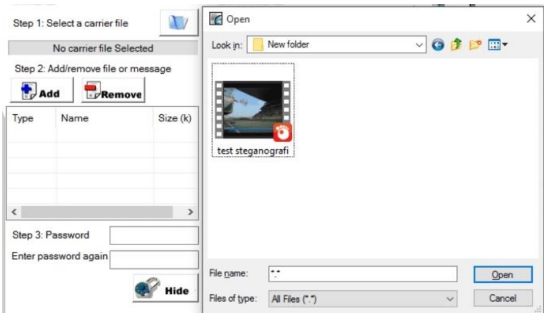
```
    end
    end
Untuk proses Dekripsi :
k = 1;
  for i = 1 : height
    for j = 1 : width
      if (k <= m)
        b(k) = mod(double(s(i,j)),2);
        k = k + 1;
      end
    end
  end
```

3.2. Hasil

Pada proses ini akan dihasilkan bagaimana memulai langkah-langkah untuk pegamanan file dan pesan. File yang akan diamankan terlebih dahulu akan dipilih lalu dilanjutkan dengan penyisipan sebuah pesan kedalam file yang sudah dipilih. Lalu file yang sudah disisipkan oleh pesan akan di protek atau diamankan dengan sebuah kata kunci yang selanjutnya file tersebut dikirimkan ke penerima.



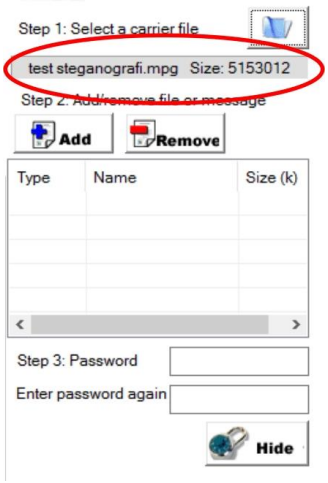
Gambar 3. Tampilan awal sistem



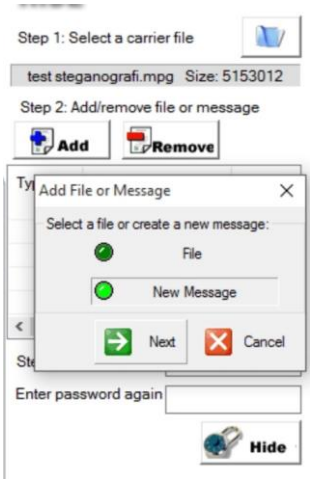
Gambar 4. Pemilihan file video

Pada gambar 3 menampilkan tampilan awal dari sistem untuk proses pengamanan file dan pesan.

Pada gambar 4, proses untuk pemilihan file video yang akan di enkripsi.



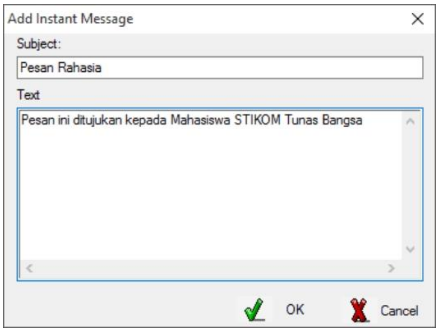
Gambar 5. Hasil file yang sudah dipiih



Gambar 6. Pemilhan Pesan yang akan disisipkan ke file.

Pada gambar 5, file yang sudah dipilih akan terseleksi bersasarkan nama filenya beserta ditampilkan ukuran filenya.

Pada gambar 6, proses pemilihan jenis file atau pesan yang akan disisipkan kedalam file video yang sudah terpilih sebelumnya. Karena yang ingin disisipkan adalah pesan teks, maka yang dipilih adalah pesan baru (*New Message*).

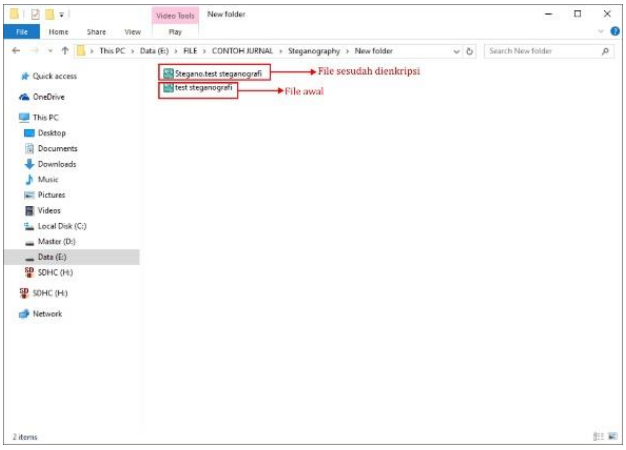


Gambar 7. Penambahan teks yang akan dijadikan pesan

Pada gambar 7, proses penyisipan teks yang akan dijadikan pesan untuk disisipkan kedalam file video yang sudah terpilih.

Gambar 8. Proteksi file yang dienkripsi

Pada gambar 8, proses untuk memberikan proteksi berupa password kedalam file video yang disisipkan pesan teks, agar tingkat keamanan file video bisa terjaga.



Gambar 9. Perbedaan file awal dan akhir

4. KESIMPULAN

Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit dapat digunakan untuk memberikan pengamanan terhadap file video yang disisipkan oleh pesan teks, sehingga dengan menggunakan algoritma kriptografi steganografi LSB, bisa dijadikan sebagai suatu cara untuk memberikan pengaman terhadap file vidieo yang akan dikirim kepada sipenerima.

DAFTAR PUSTAKA

[1] Indra Gunawan. "Pengamanan Acakan BISS Menggunakan Algoritma RSA". *JURNAL RISET SISTEM INFORMASI DAN TEKNIK INFORMATIKA (JURASIK),* Vol.2, Juli 2017, Pages 58-63.
[2] Ariyus. D. Keamanan Multimedia. Yogyakarta : Andi. 2009.
[3] Vembrina, Y. *Spread Spectrum Steganograpy*. Bandung : Sekolah Teknik Elektro dan Informatika. 2006.
[4] Sutoyo, T. Teori Pengolahan Citra Digital. Yogyakarta : Andi. 2009.
[5] Rahim, M. Teknik Penyembunyian Data Rahasia Dengan Menggunakan citra Digital Sebagai Berkas Penampung. Semarang : Universitas Diponegoro. 2006.
[6] Agustaviana, Ilmia. Aplikasi Pesan Rahasia Berbasis Web Menggunakan Vigenere Cipher dan Steganografi EOF. Skripsi Uiversitas Mulawarman. 2012.
[7] Edisuryana, M., Isnanto, R.R., Somantri, M. Aplikasi Steganografi Pada Citra berformat Bitmap Dengan Menggunakan Metode End of File. *JURNAL TEKNIK ELEKTRO*. Universitas Diponegoro Semarang. 2013.
[8] Ida Ayu Laksmini Dewi, *FRAME RATE MINIMUM PADA VIDEO TANPA KOMPRESI MENGGUNAKAN NORMALIZED FRAME DIFFERENCE SEBAGAI PENDESKRIPSI INTENSITAS GERAK*. Skripsi : Jurusan Teknik Elektro Fakultas Teknik Universitas Udayana. 2015.