Analisa Teknik *Steganografi* dan *Steganalysis* Pada File Multimedia Menggunakan Net Tools dan Hex Editor

Yudo Bismo Utomo[1], Danang Erwanto[2]
[1,2]Teknik Elektro, Fakultas Teknik, Universitas Islam Kadiri Kediri
E-mail: *[1]yudobismo@uniska-kediri.ac.id, [2]danangerwanto@uniska-kediri.ac.id

Abstrak – *Pada era perkembangan teknologi informasi saat ini, setiap stackholder mengirimkan suatu pesan informasi menggunakan media internet. Dengan adanya internet, pengiriman pesan menjadi mudah dan cepat. Akan tetapi, pada saat mengirimkan pesan menggunakan media internet, terdapat celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Maka dari itu, dibutuhkan teknik untuk mengatasi masalah tersebut, yaitu dengan menggunakan teknik steganografi. Pada penelitian ini menggunakan metode ekperimental, dimana peneliti akan melakukan suatu percobaan teknik steganografi menggunakan Net Tools, kemudian menganalisanya menggunakan Hex Editor, setelah itu menuliskan hasil percobaan dan analisa tersebut dituangkan ke dalam laporan. Hasil yang diperoleh dari penelitian ini adalah dengan menggunakan Net Tools telah memenuhi kriteria steganografi yang baik dalam mengirim sebuah pesan, yaitu fidelity dan recovery. Sedangkan Hex Editor berguna untuk mendeteksi ada atau tidaknya pesan yang tersembunyi di dalam sebuah citra, sehingga setiap stakeholder mengirimkan suatu pesan menggunakan media internet supaya aman dan isi dari pesan tersebut tidak dirubah kontennya oleh pihak yang tidak bertanggung jawab.*

Kata Kunci *— steganografi, steganalisis, internet, fidelity, recovery.*

Abstract – *In the current era of information technology development, each stackholder sends an information message using internet media. With the internet, sending messages is easy and fast. However, when sending messages using internet media, there are gaps that can be used by irresponsible parties. Therefore, a technique is needed to overcome this problem, namely by using the steganography technique. In this study using the experimental method, where the researcher will conduct an experimental steganography technique using Net Tools, then analyze it using Hex Editor, then write the results of the experiment and the analysis is poured into the report. The results obtained from this study are that using Net Tools has met the steganographic criteria which is good at sending a message, namely fidelity and recovery. While the Hex Editor is useful for detecting the presence or absence of messages hidden in an image, so stakeholder sends a message using internet media so that the content of the message is not changed by the irresponsible party.*

Keywords *— steganography, steganalysis,internet, fidelity, recovery.*

1. PENDAHULUAN

Sebelum adanya teknik *steganografi*, pada waktu perang dunia ke-II, bangsa Jerman menggunakan teknik *microdots* untuk menyampaikan informasi atau pesan yang sifatnya rahasia, sehingga strategi tersebut tidak diketahui oleh pihak musuh. Karena pada waktu itu, teknik tersebut merupakan teknologi baru dalam mengirimkan pesan informasi yang belum bisa terdeteksi oleh pihak musuh [1].

Pada saat ini, di era perkembangan teknologi informasi, semua orang bisa saling berkomunikasi, berinteraksi dan saling bertukar segala informasi meski dalam jarak yang jauh sekalipun dengan menggunakan internet. Dengan adanya internet, maka pengiriman pesan informasi semakin mudah dan cepat. Namun dalam kenyataanya, tanpa kita sadari pada saat mengirimkan suatu pesan informasi dengan menggunakan internet, terdapat celah keamanan sistem informasi yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, yaitu mengubah isi konten yang akan disampaikan, sehingga si penerima tidak tahu apakah isi pesan informasi yang telah dia terima tersebut asli atau tidak. Jika hal tersebut tidak segera diatasi, maka akan terjadi kesalah pahaman antara pihak pengirim dan pihak penerima terhadap pesan informasi yang akan disampaikan.

Untuk mengatasi permasalahan tersebut, munculah teknik keamanan sistem informasi yang baru dalam hal menyampaikan pesan supaya aman dan tidak diketahui oleh pihak yang tidak bertanggung jawab. Salah satu teknik keamanan sistem informasi itu menggunakan teknik *steganografi*. Jika kita tidak menggunakan teknik tersebut, maka segala pesan informasi yang akan disampaikan akan dirubah isi kontennya oleh pihak yang tidak bertanggung jawab.

Istilah *steganografi* berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan [6]. Jadi, *steganografi* merupakan teknik menulis pesan dengan menyembunyikan pesan tersebut ke suatu objek citra penampung atau sebuah gambar yang tampaknya tidak berbahaya, sehingga pihak yang tidak bertanggung jawab tidak menyadari bahwa ada suatu pesan yang penting di dalam gambar tersebut.

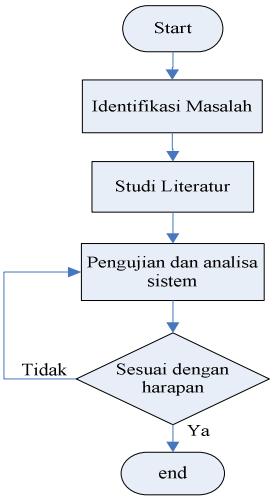
Tujuan dari penelitian ini adalah untuk menyembunyikan pesan ke dalam citra penampung dengan menggunakan Net Tools dan menganalisisnya dengan menggunakan Hex Editor tanpa merusak pesan yang telah disisipkan, sehingga kesalah pahaman antara pihak pengirim dan pihak penerima pesan informasi dapat diminimalisir.

2. METODE PENELITIAN

Metode yang akan di pakai dalam penelitian ini menggunakan metode eksperimental. Metode eksperimental adalah suatu metode dimana peneliti akan melakukan suatu percobaan, kemudian menganalisanya, setelah itu menuliskan hasil percobaan dan analisa tersebut, dituangkan ke dalam laporan [5]. Tahap dari metode eksperimental adalah sebagai berikut :

1. Identifikasi masalah.
   Penelitian ini dimulai dengan melakukan identifikasi masalah terlebih dahulu, yaitu bagaimana cara menyembunyikan suatu pesan ke dalam sebuah gambar dengan menggunakan Net Tools supaya memenuhi kriteria steganografi yang baik dan bagaimana cara menganalisa suatu gambar tersebuat ada suatu pesan didalamnya dengan menggunakan Hex Editor.
2. Studi literatur.
   Setelah dilakukan identifikasi masalah, langkah selanjutnya yang akan dilakukan adalah studi literatur. Dalam tahapan ini peneliti akan melakukan studi literatur yang berkaitan dengan teknik steganografi dan steganalisis.
3. Pengujian dan analisa
   Pada tahap ini akan dilakukan pengujian terhadap aplikasi Net Tools untuk menyembunyikan suatu pesan ke dalam sebuah gambar dan dapat diungkapkan kembali tanpa harus merusak pesan tersebut serta menganalisisnya dengan menggunakan aplikasi Hex Editor.

Langkah-langkah dalam penelitian eksperimental ini, dapat dilihat pada gambar 1. berikut ini:

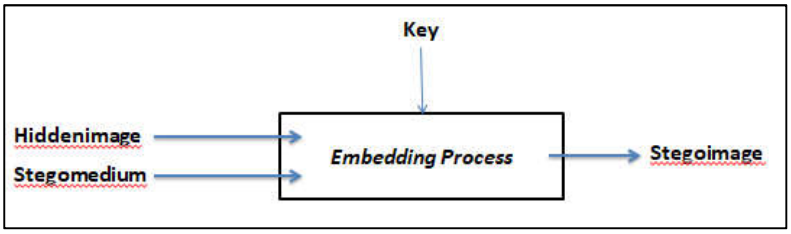


Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Proses Steganografi

Pada teknik staganografi terdapat 2 proses, yaitu: proses *embedding* dan proses *extracting* [4]. Yang dimaksud proses *embedding* adalah proses untuk menyembunyikan pesan didalam sebuah gambar sebagai media penyimpanan (*stegomedium)* dengan memasukkan kata kunci (*Key*), sehingga menghasilkan gambar dengan pesan tersembunyi di dalamnya (*stegoimage*). Alur dari proses *embedding* akan ditampilkan pada gambar 2 berikut ini:



Gambar 2. Proses *Embedding*

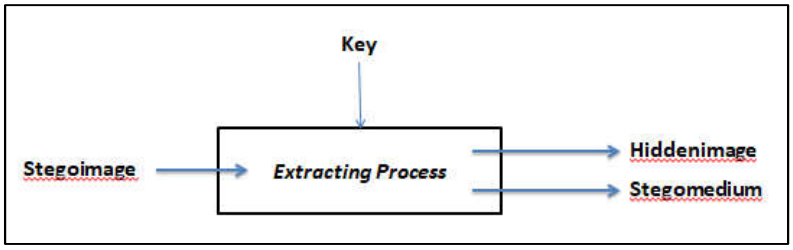
Untuk rancangan algoritma (*pseudocode*) dari proses menyembunyikan pesan (*embedding*) pada penelitian ini adalah sebagai berikut:

```
PROGRAM Embedding
KONSTANTA
   Offset = 50;
DEKLARASI
   message, input, output : string;
   in, data : DataInputStream;
   out : DataOutputStream;
   a, b, ukur, n, dataFileSize, tempInt, vectorSize: integer;
   messageSize, temp: short;
   by, byt, byb: byte;
ALGORITMA {inisialisasi nilai a, b, ukur sebagai 0}
   a ← 0
    b ← 0
    ukur ← 0

{konversi data-data inputan ke dalam data stream}
read (in, data)
 read (out)
  for a ← 0 to n do a <= Offset
   writeByte out readByte in
   messageSize ← (short) message.length
endfor

{Proses inti Embedding pesan}
for a ← 0 to n do a <messageSize>
 byt ← (byte) message.charAt(a)
  byt& ← 0x7F
  for b ← 6 to b ← -2 do b >= 0
   by ← byt
    by>> ← b
     by AND 0x03
      byb ← readByte in
       byb& ← 0xFC
        byb OR by
         writeByte(byb)out return
endfor
endfor
endfor
```

Proses steganografi kedua adalah *extracting process*, yang dimaksud dengan proses *extracting* adalah untuk mengekstraksi pesan yang disembunyikan [2]. Alur dari proses *extracting* akan ditampilkan pada gambar 3 berikut ini:



Gambar 3. Proses *Extracting*

Pada gambar tersebut diatas, proses *extracting* pada *stegoimage* dengan memasukkan kata kunci (*Key*) yang sama pada waktu proses *embedding*, sehingga pesan yang disembunyikan dapat diungkapkan kembali. Untuk rancangan algoritma (*pseudocode*) dari proses mengekstraksi pesan (*extracting*) pada penelitian adalah sebagai berikut:

```
PROGRAM extracting
KONSTANTA
   Offset = 50;
DEKLARASI
   message, output, input, inFile : string;
   in, data : DataInputStream;
   out : DataOutputStream;
   a, b, ukur, n, dataFileSize, tempInt, vectorSize: integer;
   messageSize, temp: short;
   by,byt,byb: byte;
   flag: Boolean;
   pesan: char;
ALGORITMA {inisialisasi nilai a, b, ukur sebagai 0}
   a ← 0
    b ← 0
     ukur ← 0

{inisialisasi variable baru untuk ekstrak pesan}
input ← inFile
flag ← true
pesan ← null

{konversi data-data inputan ke dalam data stream}
read (in)
messageSize ← 0{diperoleh ukuran pesan}

{skip nilai offset carrier file}
for a ← 0 to n do a <= Offset
  readByte in
endfor
if messageSize <= 0 return
endif
pesan ← messageSize
for a ← 0 to n do a<messageSize
  by= 0;
  for b ← 6 to b ← -2 do b>=0
   byt ← readByte in
    byt AND 0x03
     byt<<= b
      by OR byt;
       pesan [a] ← (char) (((char) by)& 0x00FF)
       return
endfor
endfor
```

3.2. Pengujian sistem

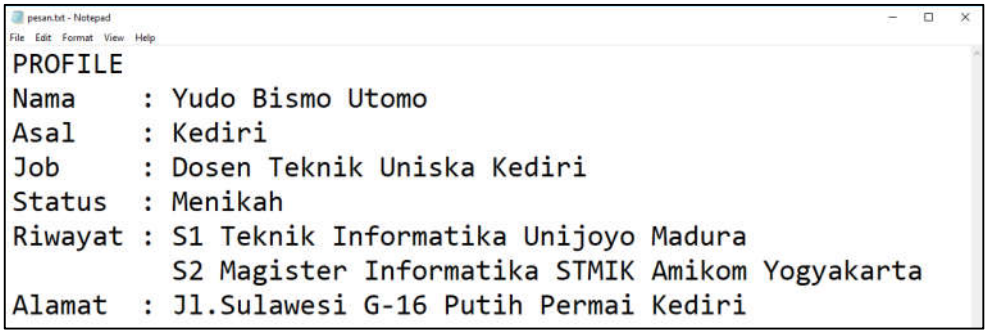
Kriteria steganografi yang baik ada 3, yaitu: *Fidelity, Robustness* dan *Recovery*. *Fidelity* merupakan mutu dari citra penampung (*stegoimage*) tidak jauh berbeda dengan citra aslinya (*stegomedium*). Sedangkan *robustness* merupakan pesan yang disembunyikan harus tahan terhadap

manipulasi yang dilakukan pada citra penampung (*stegoimage*). Lalu yang dimaksud dengan *recovery* adalah pesan yang disembunyikan harus dapat diungkapkan kembali.

Pada pengujian kali ini, menggunakan media gambar (*stegomedium*) dengan format BMP, resolusi 585 x 329 pixel dengan kedalaman warna 24 bits dan ukuran kapasitas gambar 565 Kb. Media gambar yang akan dijadikan penelitian akan ditunjukan pada gambar 4 berikut ini:

Gambar 4. Media Penyimpanan Gambar (*Stegomedium*)

Sedangkan pesan yang akan disisipkan dalam gambar (*stegomedium*) tersebut adalah file teks dengan format txt yang berukuran 247 Kb, yang akan ditunjukkan pada gambar 5 berikut ini:

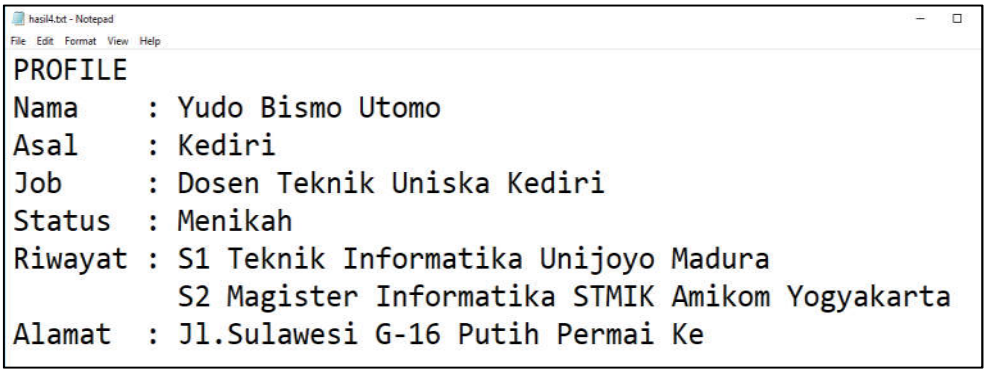


Gambar 5. Pesan Teks

Setelah dilakukan proses penyisipan pesan dengan kata kunci “dodo”, maka menghasilkan sebuah citra penampung (*stegoimage*) yang ukurannya sama persis dengan gambar aslinya (*stegomedium*) dengan ukuran resolusi, kedalaman warna dan besar kapasitasnya yang sama persis, keduanya mempunyai resolusi 585 x 329 pixel dengan kedalaman warna 24 bits dan kapasitas gambarnya 565 Kb. Hasil dari citra penampung (*stegoimage*) akan ditunjukkan pada gambar 6 berikut ini:

Gambar 6. Hasil *Stegoimage* (Citra Penampung)

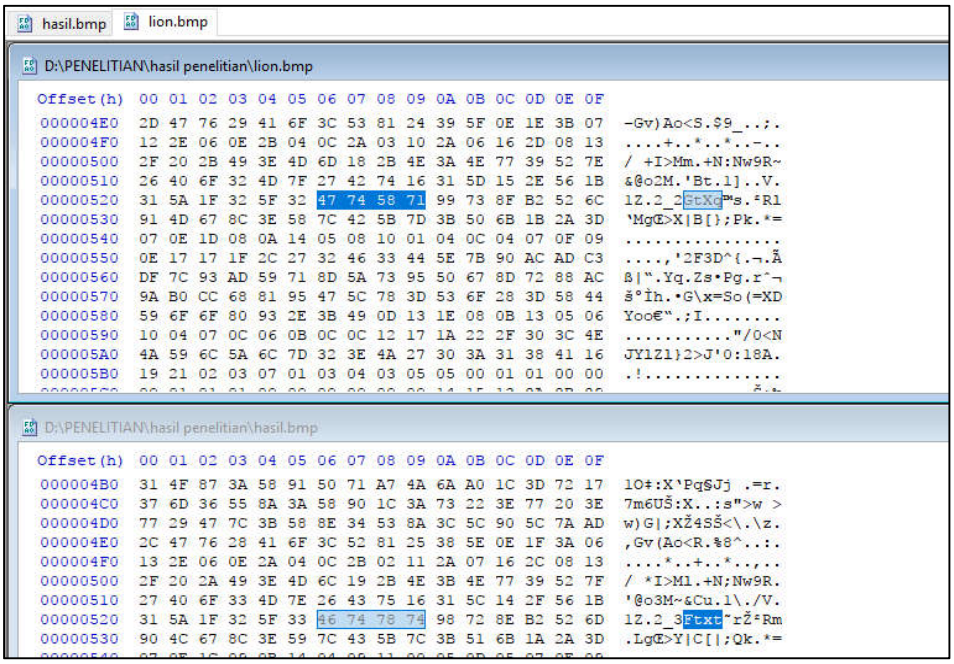
Akan tetapi, setelah dilakukan proses *extracting,* pesan yang dihasilkan mengalami kerusakan kecil, seperti yang ditunjukkan pada gambar 7 berikut ini:



Gambar 7. Hasil *Extracting* Pesan

3.3. *Steganalysis*

Proses *Steganalysis* bertujuan untuk mencari kelemahan atau mendeteksi ada atau tidaknya pesan yang disisipkan pada suatu objek gambar guna meningkatkan skema penyisipan pesan yang lebih aman [3]. Proses *steganalysis* pada penelitian ini digunakan untuk membedakan antara *stegomedium* (media penyimpanan citra) dengan *stegoimage* (citra penampung) yang telah dilakukan pada proses sebelumnya. Hasilnya seperti yang ditunjukkan pada gambar 8 berikut ini:



Gambar 8. Hasil *Steganalysis*

Dari hasil *steganalysis* menggunakan Hex Editor menunjukkan bahwa file lion.bmp merupakan file yang asli dan belum disisipkan pesan apapun didalamnya. Sedangkan file dengan nama hasil.bmp sudah ada pesan yang disisipkan berupa pesan berformat txt.

4. SIMPULAN

Berdasarkan percobaan yang telah dilakukan terhadap sistem, maka dapat disimpulkan sebagai berikut:

1. Aplikasi Net Tools ini sangat bermanfaat bagi stakeholder, jika ingin mengirim pesan melalui media internet supaya aman dan isi dari pesan tersebut tidak dirubah isinya oleh pihak yang tidak bertanggung jawab.

2. Aplikasi Hex Editor ini juga sangat bermanfaat bagi stakeholder, jika ingin mengetahui apakah di dalam sebuah gambar terdapat suatu pesan tersembunyi didalamnya atau tidak.
3. Aplikasi Net Tools ini telah memenuhi 2 kriteria steganografi yang baik dalam mengirim pesan, yaitu *fidelity*, dikarenakan ukuran citra penampung tidak jauh berbeda dari citra aslinya. Dan juga *recovery,* yang dapat mengungkapkan kembali sebuah pesan tanpa harus merusaknya.
4. Akan tetapi aplikasi Net Tools ini pada waktu melakukan proses *extracting*, pesan yang dihasilkan mengalami kerusakan kecil yang dikarenakan pada saat penyimpanan pesan tidak dilakukan pencatatan kondisi awal dari *stegomedium* yang digunakan waktu menyimpan pesan, sehingga aplikasi ini tidak tahan terhadap segala manipulasi (*robustness*).

5. SARAN

Untuk pengembangan lebih lanjut serta penyempurnaan dari penelitian ini, maka disarankan agar pesan yang disembunyikan ke dalam citra penampung harus tahan terhadap segala manipulasi atau *robustness* serta pesan yang disembunyikan dapat menyembunyikan pesan yang berformat word maupun pdf.

DAFTAR PUSTAKA

[1] Christy, Atika Sari, dkk. 2016. Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Chiper dan Bit Shiffting. *Jurnal of Applied Intelligent System*. Vol 1. No 3. Oktober 2016.

[2] Dedy, Abdullah, dkk. 2016. Implementasi Algoritma Blowfish dan Metode Least Significant Bit Insertion Pada Video MP4. *Jurnal Pseudocode*. Vol 3. No 2. September 2016.

[3] Friski, Gatra Pamungkas, dkk. 2017. Implementasi Teknik Steganalisis Menggunakan Metode Improvement Difference Image Histogram Pada Steganografi LSB. *Seminar Nasional Inovasi dan Aplikasi Teknologi Industri*. ITN Malang. 4 Pebruari 2017.

[4] Muhamad, Fitra Syawal, dkk. 2016. Implementasi Teknik Steganografi Menggunakan Vigenere Cipher dan Metode LSB. *Jurnal TICOM*. Vol 4. No 3. Mei 2016.

[5] Munir, Rinaldi. 2016. Eksperimen Steganalisis Dengan Metode Visual Attack Pada Citra Hasil Stego Berformat GIF. *Seminar Nasional Aplikasi Teknologi Informasi*. Yogyakarta. 6 Agustus 2016.

[6] Yunita, Sartika Sari, dkk. 2015. Steganografi Dengan Metode Gabungan File Melalui *Command Prompt* Serta Steganalisis Hasil Dengan Metode Pola Pengenalan Gambar, Kultur Gambar RGB 24 BIT dan Rentang Ukuran Pada File JPEG. *Jurnal TELEMATIKA*. Vol 7. No. 2. September 2015.