

TUGAS REVIEW JURNAL MATA KULIAH MULTIMEDIA

TEKNIK KEAMANAN MULTIMEDIA

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

Yudo Bismo Utomo¹ , Danang Erwanto² 1,2Teknik Elektro,

Fakultas Teknik, Universitas Islam Kediri Kediri

E-mail: *1 yudobismo@uniska-kediri.ac.id, 2 danangerwanto@uniska-kediri.ac.id



Disusun oleh :

Nining Kurnia (3217614)

PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

BANDUNG

2020

1. Identifikasi Masalah

- bagaimana cara menyembunyikan suatu pesan ke dalam sebuah gambar dengan menggunakan Net Tools supaya memenuhi kriteria steganografi yang baik?
- bagaimana cara menganalisa suatu gambar tersebut ada suatu pesan didalamnya dengan menggunakan Hex Editor?

2. Tujuan

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.

3. 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 menganalisisnya, setelah itu menuliskan hasil percobaan dan analisa tersebut, dituangkan ke dalam laporan.

4. Hasil Akhir

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.

1. 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 ditunjukkan pada gambar 4 berikut ini:



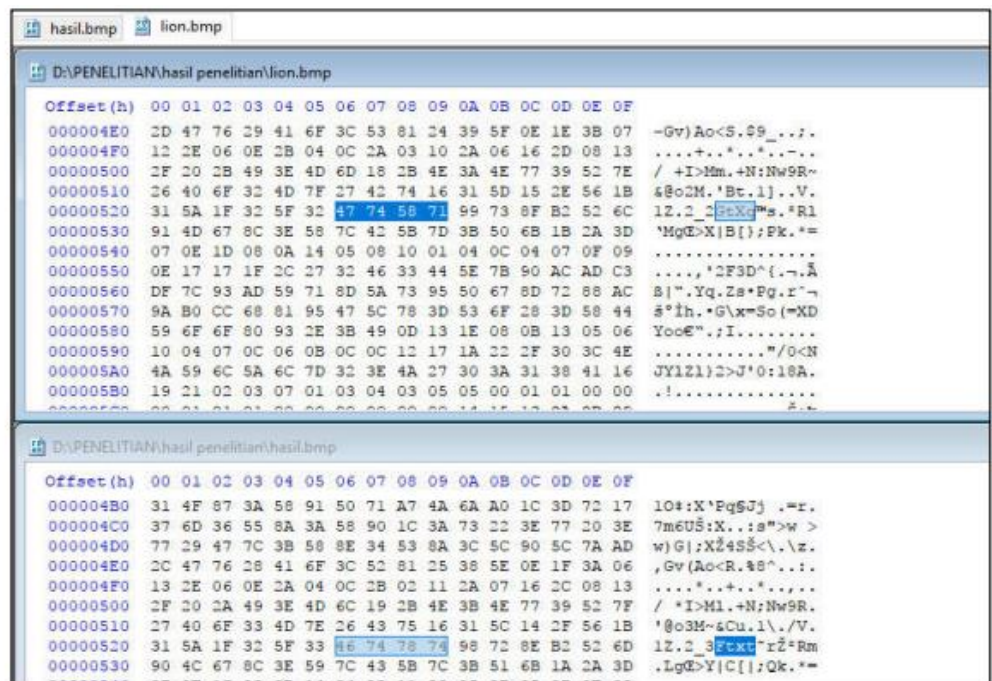
Gambar 4. Media Penyimpanan Gambar (*Stegomedium*)

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)

2. 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.s

5. Kesimpulan

- ✚ 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.
- ✚ Aplikasi Hex Editor ini juga sangat bermanfaat bagi stakeholder, jika ingin mengetahui apakah di dalam sebuah gambar terdapat suatu pesan tersembunyi didalamnya atau tidak.
- ✚ Aplikasi Hex Editor ini juga sangat bermanfaat bagi stakeholder, jika ingin mengetahui apakah di dalam sebuah gambar terdapat suatu pesan tersembunyi didalamnya atau tidak.
- ✚ 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).