Prosiding Seminar Nasional Hasil Penelitian dan Pengabdian kepada Masyarakat III
Universitas PGRI Ronggolawe Tuban
Tuban, 29 September 2018
PRINT ISSN: 2580-3913; ONLINE ISSN: 2580-3921

SISTEM INFORMASI TENAGA KERJA DALAM PEMBUATAN DAN PERBAIKAN ALAT TANGKAP NELAYAN

Amin Samsudin[1], Andy Haryoko[2], Adityo Nugroho[3]
[1]Universitas PGRI Ronggolawe, [2]Universitas PGRI Ronggolawe, [3]Universitas PGRI Ronggolawe
[1]amiincokro@gmail.com, [2]andyharyoko@gmail.com, [3]adityo.nugroho@gmail.com

Abstrak

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan melalui media jaringan/internet. Teknik kriptografi dan stegano-grafi dapat digunakan untuk memberi perlindungan keamanan pada pesan rahasiaSteganografi menyembunyikan data dilakukan dengan cara untuk mengubah atau menggeser beberapa informasi yang tidak terlihat di media. Metode yang digunakan adalah Least Significant Bit. Metode-metode ini akan diterapkan file yang dimasukkan ke multimedia audio (Mp3), teknik ini diharapkan dapat memasukkan informasi dalam frame tunggal maksimum 1 bit, sehingga perubahan tidak terlihat. Penelitian ini bertujuan untuk merancang program aplikasi dengan pengamanan data dengan metode steganografi dengan metode Least Significant Bit pada Mp3, text akan disisipkan pada berkas Mp3 sehingga tidak mudah dideteksi Dalam tulisan ini, akan dibahas perancangan steganografi yang diaplikasikan dalam perangkat mobile. Aplikasi ini diuji dengan cara mengacak lalu menyembunyikan berkas ke dalam file audio dan mengembalikan data yang disembunyikan dan diacak ke bentuk semula. Waktu yang dibutuhkan untuk proses cukup cepat, sehingga dapat disimpulkan bahwa hasil aplikasi penelitian ini dapat dipakai pada dunia nyata. Hasil yang didapat setelah simulasi, berupa Mp3 rekonstruksi yang diukur dengan parameter penilaian obyektif yang berdasarkan nilai Peak Signal to Noise Ratio yang efisien diperoleh nilai PSNR rata-rata adalah 32,02 dB yaitu memiliki kualitas bernilai cukup baik. Besarnya PSNR dipengaruhi dari banyaknya perubahan signal digital pada Mp3.

Kata Kunci : *Enkripsi, Steganografi, Kriptografi, Least Significant Bit*.

PENDAHULUAN

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/internet,karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan/informasi yang dikirimkan melalui jaringan/internet. Salah satu bidang yang masih sering menjadi bahan penelitian dalam ilmu komputer untuk teknik keamanan data adalah steganografi. Steganografi merupakan suatu teknik untuk menyembunyikan pesan atau data yang bersifat rahasia di dalam media.

Saat ini, *file audio* yang sangat populer di kalangan masyarakat adalah file berformat mp3. *File* mp3 adalah salah satu *file audio* yang banyak digunakan pada berbagai alat pemutar musik sampai ke telepon selular (ponsel). *File* mp3 memiliki ukuran yang kecil tetapi kualitasnya setara dengan kualitas musik CD (*compact disc*) sehingga dapat dengan mudah ditransmisikan maupun disimpan pada *media store*. Terbukti dengan mp3, masyarakat lebih mudah mengakses *file* ini di dunia teknologi yang dampaknya mengancam kemamanan data.

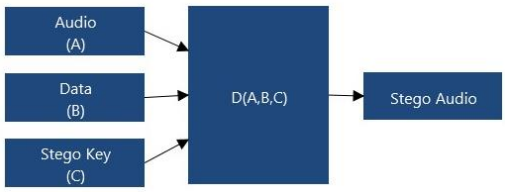
Steganografi merupakan sebuah seni dalam menyamarkan atau menyembunyikan pesan dimana tidak ada yang menyadari adanya pesan tersembunyi kecuali pengirim pesan dan penerima pesan yang dituju (Ariyus, 2 2008). Steganografi bersifat nonrepudiation sehingga dapat mencegah suatu pihak untuk menyangkal bahwa pesan tersebut berasal dari dirinya (Munir, 2006). Jika terdapat seseorang yang mencoba untuk membajak sebuah lagu dan mengklaim bahwa dirinyalah sebagai pemilik lagu tersebut dapat dibuktikan dengan penggunaan teknik steganografi.

Pada penelitian ini diterapkan sebuah aplikasi perangkat lunak berbasis Java yang mengimplementasikan *steganografi* dengan menggunakan metode *Least Significant Bit* sebagai cara untuk menyembunyikan suatu data ke dalam media *audio*.MP3. Diharapkan dengan adanya aplikasi ini merupakan salah satu solusi dalam menjaga keamanan data agar dapat

lebih terjamin, karena yang dapat mengambil dokumen yang tersembunyi hanya orang yang memiliki kata kunci untuk mengaksesnya.

METODE PENELITIAN

Teknik dari steganografi yaitu menyembunyikan data ke dalam sebuah penampung atau medium,dalam kasus ini adalah audio mp3. Data rahasia disisipkan ke sebuah audio mp3 yang menghasilkan audio mp3-stego. Dalam kasus ini adalah file*.text penambahan stego key digunakan untuk memperkuat pengamanan data dimana *key* ini memakai algoritma Vigenere pada data rahasia.



Gambar 3.1 Teknik steganografi

Proses penyisipan pesan rahasia yaitu bagaimana pesan rahasia disisipkan pada sebuah *file audio* sehingga *file* tersebut tidak diketahui keberadaannya. Pada proses ini, proses penyisipan membutuhkan dua buah masukan yaitu *media cover* sebagai tempat penyisipan pesan dan pesan rahasia.

Output yang dihasilkan juga bergantung pada proses yang akan dilakukan. Pada proses penyisipan, keluaran yang dihasilkan adalah *audio* yang telah disisipi pesan rahasia (*file stego*).

Pada susunan bit di dalam sebuah byte (l byte = 8 bit), ada bit yang paling berartj most significwtt bit atauMSB dan bit yang paling kurang berarti leasr sign ificant bit atavLSB.

MSB **1**0110100 *LSB*

Nilai desimal dari MSB di atas adalah 128 ,sedangkan nilai desimal dari LSB adalah 0, kemungkinan besarnya nilai dari LSB hanyalah 1 dan 0.

Jadi pada prinsipnya adalah mengganti bit terakhir dari data dengan nilai bit yang akan disisipkan. Algoritma penyisipan LSB adalah sebagai berikut:

Misalikan Nilai Bit yang disisipkan =0, dan data yang disisipi misalnya

1 01 1 1 1 1 1
Data :10111111
254 : 11111110 and
HasilAwal : 11111110,

(tujuannya adalah membuat bit terakhir menjadi 0) nilai ini kemudian di "or" kan dengan bit yang akan disisipkan

Hasil Awal : 11111110,
Bit : ___0 or
Data baru : 10111110

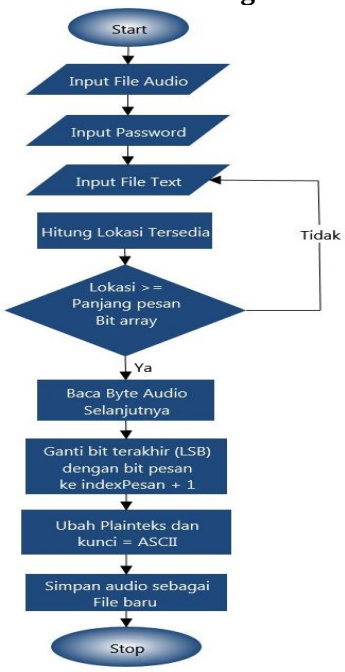
Setelah pesan text disisipkan pada file MP3 maka file wav dapat dikirimkan pada orang lain. Orang yang dapat membaca pesan adalah orang yang mengetahui password dari pengirim pesan. Langkah untuk membaca pesan adalah sebagai berikut!

1. Langkah 1: membuat blok-blok data ke dalam 8 byte per blok. Untuk setiap blok dikerjakan Langkah 2 sampai dengan langkah 3 untuk *i = 0,1,2,3, ..,..., 7.*
2. Langkah 2: Mengambil nilai bit terakhir byte pesan ke-i dengan meng-and-kan dengan 1.
3. Langkah 3: Menyimpan hasil setelah di-and-kan dengan 1, dan mengalikan dengan nilai _ (7-i)- posisi bit.
4. Langkah 4: Menjumlahkan semua hasil perhitungan untuk i=0 sampai dengan i=7.
5. Langkah 5: Menentukan karakter ASCII yang bersesuaian dengan hasil perhitungan. Sebagai contoh pembacaan pesan diberikan berikut ini.

01010010 01001001 01000110 01000110
11101000 01001111 00000100 00000000
01010010=>01010010 *and* 1=0 nilai=0x2^7=0
01001001=>01001001 *and* 1=1 nilai=1x2^6=64
01000110=>01000111 *and* 1=1 nilai=1x2^5=32
01000110=>01000110 *and* 1=0 nilai=0x2^4=0
11101000=>11101000 and 1=0 nilai=0x2^3=0
01001111=>01001110 *and* 1=0 nilai=0x2^2=0
00000100=>00000101 *and* 1=1 nilai=1x2^1=2=99

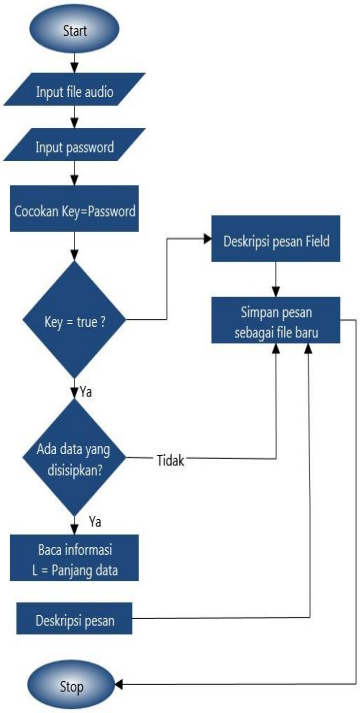
kode ASCII yaitu “c” seperti pada pembahasan di BAB II dimana angka decimal “99” ditabel ASCII = “c”.

Flowchart Proses Embedding Sistem



Gambar 3.3 *Flowchart* Proses Penyisipan

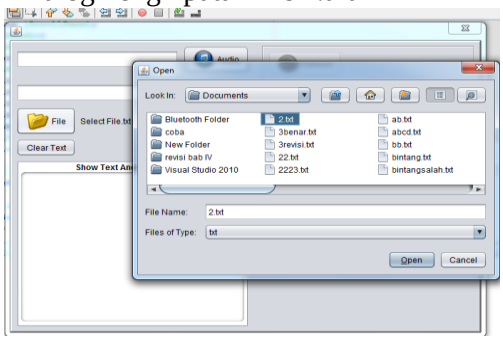
Flowchart Proses Ekstraksi



Gambar 3.4 *Flowchart* Proses Ekstraksi

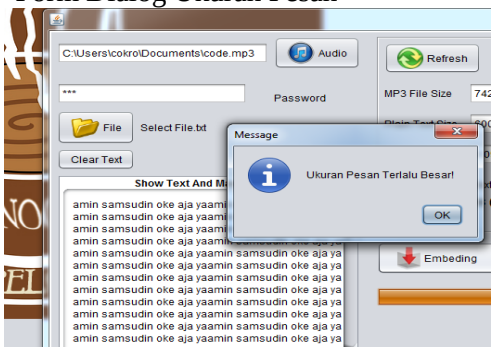
HASIL DAN PEMBAHASAN

1) Dialog Penginputan file *.txt



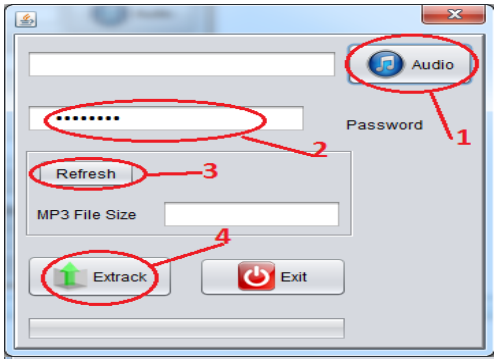
Gambar 4.3 input file pesan

2) Form Dialog Ukuran Pesan



Gambar 4.4 Form Menu pesan ukuran maksimal

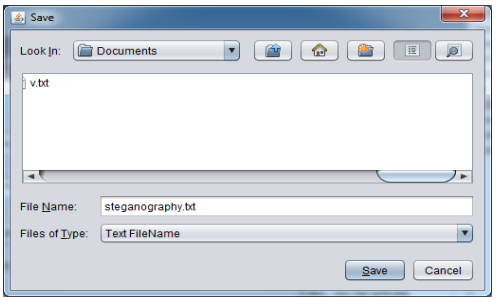
3) Form Extrack



Gambar 4.5 input file pesan

Pada gambar diatas merupakan proses extrack file audio steganografi diamana user yang akan mengeluarkan pesan didalam audio.mp3, dan format pesan yang dikeluarkan atau di Ekstrak berekstensi *.txt kemudian menyimpanya,jika password cocok maka pesan bisa dilihat dan dalam hal ini akan dijelaskan pada pengujian sistem.

4) Dialog Simpan



Gambar 4.6 input file pesan

Analisa Pengaruh Ukuran

Berdasarkan tabel,ukuran data atau pesan tidak mempengaruhi ukuran file audio semula sebelumdisisipi pesan atau di stego, akan tetapi audio sebagai media penampung jika panjang pesan terlalu panjang melebihi kapasitas media penampung,dan setiap audio memiliki kapasitas berbeda dan peneliti tidak bisa menjelaskan perbedaan media penamung yaitu audio yang berformat MP3.

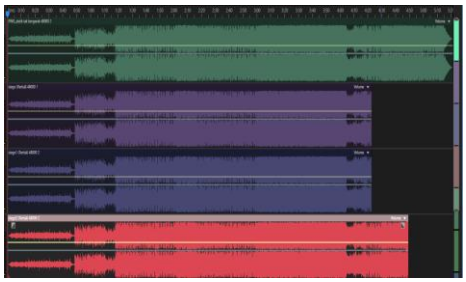
Tabel 4.4 Analisa Pengaruh Ukuran

Nama file audio.MP3	Ukuran file audio	Panjang pesan	Waktu	Ukuran Akhir
Audio 1	4.502.301 Bytes	500 Karakter	3 Detik	4.502.301 Bytes
		1000 Karakter	7 Detik	
		2000 Karakter	7 Detik	
		88.123 Karakter	10 Detik	

Tabel 4.5 Analisa Pengaruh Ukuran

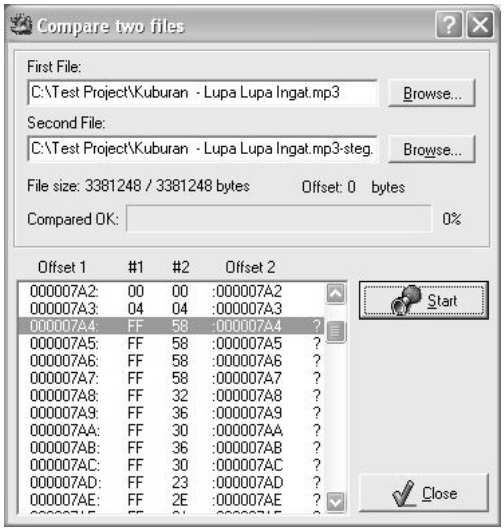
Bit rate	Durasi audio	Panjang plainteks
128 kbps	00:05:07	45.754 karakter
320 kbps	00:07:014	55.951 karakter
128 kbps	00:05:07	67.199 karakter
192 kbps	00:05:07	88.123 karakter

1. Analisa Digital



Gambar 4.7 Analisa Gelombang Audio Stego

Pada gambar diatas hasil analisa pengujian menunjukan bahwa audio.MP3 ada perubahan pada kualitas suara di akhir lagu,dimana terjadi kerusakan kualitas suara pada akhir lagu,dan panjang kerusakan audio ditentukan oleh berapa panjang file atau pesan yang disisipkan. Jadi kesimpulanya kualitas audio akan terpengaruh tergantung ukuran file atau pesan yang disisipkan.



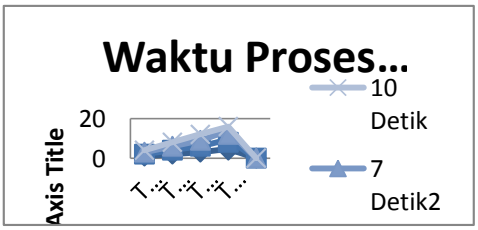
Gambar 4.8 Salah Satu Metode Steganalisis : Membandingkan Dua Berkas MP3 (dilihat dengan menggunakan *freeware* Audiograbber)

Dari penelitian di atas dapat dilihat bahwa ukuran kedua MP3 adalah sama yaitu 834 Kb(854961.0 bytes), namun byte-byte di urutan tertentu yang terdapat di dalamnya berbeda. Bagi para steganalisis hal ini akan menimbulkan kecurigaan dan mengundang untuk diperiksa lebih lanjut.

Analisa Waktu Proses

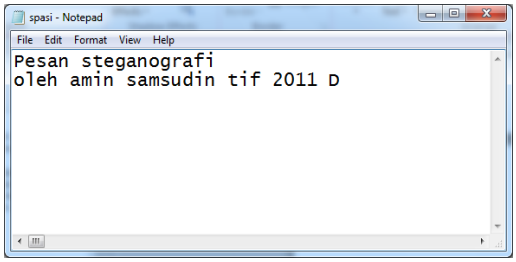
Berdasarkan hasil embedding analisa waktu proses dilakukan untuk mengetahui berapa lama waktu yang dibutuhkan untuk embedding data file audio,dan pada grafik dibawah ini menunjukan bahwa waktu proses

embedding tergantung ukuran pesan yang dimasukan kedalam audio, semakin besar pesan yang dimasukan kedalam file audio semakan lama waktu proses ekstraksi.



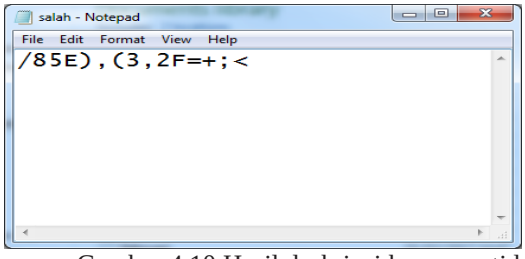
Gambar 4.9 Diagram waktu proses ekstraksi

1. Hasil Deskripsi file stego audio Key yang cocok
Hasil deskripsi pada gambar dibawah ini merupakan hasil dari kleuaran pesan yang ada didalam file audio yang disisipi pesan apabila key atau kata kunci cocok.



Gambar 4.10 Hasil deskripsi key yang cocok

2. Hasil deskripsi file stego audio Key yang cocok
Dari gambar dibawah ini merupakan hasil proses ekstraksi atau deskripsi dari file audio MP3 dimana dalam uji coba ini peneliti menguji file media yang telah distego dan di deskripsi dengan menggunakan kata kunci atau key yang tidak cocok.



Gambar 4.10 Hasil deskripsi key yang tidak cocok

KESIMPULAN

Berdasarkan uraian tersebut diatas, maka dapat diambil beberapa kesimpulan, diantaranya adalah :

1. Penelitian berhasil menunjukan implementasi steganografi dengan menggunakan metode *least significant bit* dan penambahan fitur enkripsi untuk meningkatkan keamanan. Kualitas yang dimiliki aplikasi AudioSteganografi baik karena telah memenuhi kriteria steganografi berdasarkan ukuran.
2. Ukuran akhir memiliki ukuran yang sama dengan *cover file*. Karena pesan hanya disisipkan dengan cara mengganti bit terakhir *cover file* bukan menambahkan kedalam *cover file*. Ini menunjukkan pada metode LSB ukuran pesan yang dimasukkan tidak akan merubah pukuran *cover file*.
3. Setiap *cover file* yang digunakan mempunyai batasan dalam hal menampung besarnya ukuran *file* yang dapat disisipkan dengan sempurna,. Jadi, semakin besar ukuran *file* yang akan disisipkan maka ukuran *file* mp3 yang dibutuhkan semakin besar.

Kualitas *audio* yang dihasilkan bergantung pada ukuran *file* yang disisipkan ke dalam *cover file*. Semakin besar ukuran *file* yang disisipkan maka akan semakin besar pula *penurunan* kualitas audio.MP3 yang disebabkan.

DAFTAR PUSTAKA

[1] Agus Prawoto, 2016, *HadiCharacter Encoding ASCII*, website : http://jagowebdev.com/character-set-dan-character-encoding/characterset-ascii.html diakses tanggal : 16 Februari 2017.

[2] Aminah Rizki Lubis, Maya Silvi Lidya, B.Sc.M.Sc, M. Andri Budiman, S.T.,M. Comp.Sc.M.E.M , 2012, : *Perancangan Perangkat Lunak Steganografi Audio MP3 Menggunakan Metode Least Significant Bit* (LSB) Vol. 1, No. 1, (2012) 63-68.

[3] Alatas Putri. 2009, *Implementasi Teknik Steganografi Denganmetode LSB Pada. Citra Digital*, Tugas Akhir, Universitas Gunadarma.San Maria.2007. Transparent Digisec-9 VPN.Indianapolis: Rehearsal Studio. Jakarta.

[4] Citra Dewi Astuti Br Tarigan, 2014, STMIK Budidarma, :*Steganografi Pada File Audio Mp3 Untuk pengamanan Data Menggunakan Metode Least Significant Bit (LSB)* 4 (4), 2301-9425.

[5] Prasetyo Fahri. 2010, *Steganografi Menggunakan Metode LSB dengan*

Software Matlab, Tugas Akhir, Universitas Islam Negri Syarif Hidayatullah, Fakultas Saint Dan Teknologi.Jakarta.

[6] Krisnawati , *2008*, Metode *Least Significant Bit* (LSB) Pada Teks Kedalam Citra , *1979-2328.*

[7] Muhamad Fitra Syawal , Deddy Chandra Fikriansyah , Nazori Agani ,2012 :*Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB*, Vol. 4 ,No.3 Mei (2016).

[8] Noto, Mark, 2014, *MP3Stego Hiding text in MP3 Files*, website : http://www.securitydocs.com/library/2159 ,diakses tanggal : 19 Desember 2016.

[9] Putu H. Arjana, Tri Puji Rahayu ,Yakub, Hariyanto , *2012*, *STMIK Dharma Putra Tangerang :Implementasi Enkripsi Data Algoritma Vigenere Chiper 6 (2), 2089-981*.

[10] Rachmansyah Budi Setiawan, 2015, Institut Teknologi Bandung, : *Penggunaan kriptografi dan steganografi dalam mengamankan pesan, (*2015:13).

[11] Raissi, 2002,*Struktur file MP3 dan Karakteristik gelombang suara*, website : http://Library.binus.ac.id/eColls/ethesisdoc/bab2html/2012100780IF/page18.html ,diakses tanggal : 12 Januari 2017.

[12] Suharja,2009, STMIK Budidarma : *Karakteristik gelombang suara* (2009, p16).

[13] *Yus Gias Vembrina*, 2006, Institut Teknologi Bandung, :*Spread Spectrum Steganography 2006 : 304*).