APLIKASI STEGANOGRAFI PESAN TEKS PADA MEDIA AUDIO MP3 MENGGUNAKAN METODE PENYISIPAN *LEAST SIGNIFICANT BIT* DAN *ADVANCED ENCRYPTION STANDARD*

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
pada Jurusan Ilmu Komputer / Informatika

Disusun Oleh :

ILHAM FIRMAN ASHARI

24010311130032

JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini,

Nama : Ilham Firman Ashari

NIM : 24010311130032

Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Dengan ini saya menyatakan bahwa dalam tugas akhir atau skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 31 Agustus 2015

Ilham Firman Ashari

24010311130032

HALAMAN PENGESAHAN

Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Nama : Ilham Firman Ashari

NIM : 24010311130032

Telah diujikan pada sidang tugas akhir pada tanggal 20 Agustus 2015 dan dinyatakan lulus pada tanggal **31 Agustus 2015**.

Semarang, 1 September 2015

Mengetahui,
Ketua Jurusan Ilmu Komputer / Informatika
FSM UNDIP

Nurdin Bahtiar, S.Si, M.T
NIP. 19790720 200312 1 002

Panitia Penguji Tugas Akhir
Ketua,

Sukmawati Nur Endah, S.Si, M.Kom
NIP. 19780502 200501 2 002

HALAMAN PENGESAHAN

Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Nama : Ilham Firman Ashari

NIM : 24010311130032

Telah diujikan pada sidang tugas akhir pada tanggal 20 Agustus 2015

Semarang, 1 September 2015
Dosen Pembimbing,

Aris Sugiharto, S.Si, M.Kom
NIP. 19710811 199702 1 004

ABSTRAK

Perkembangan teknologi informasi telah berkembang sangat pesat, sehingga memberikan kemudahan dalam mengakses dan mendapatkan data informasi. Dampak negatifnya adalah masalah keamanan dan munculnya berbagai macam teknik yang digunakan oleh berbagai pihak untuk mendapatkan informasi yang bersifat rahasia. Oleh karena itu, keamanan informasi merupakan aspek penting untuk menjaga kerahasian suatu informasi. Salah satu metode keamanan yang dapat digunakan untuk mengamankan pesan rahasia tanpa dapat dipersepsi adalah dengan menggabungkan metode kriptografi dan steganografi. Dalam penelitian ini, metode kriptografi yang digunakan adalah *Advanced Encryption Standard* (AES) dan metode Steganografi yang digunakan adalah *Least Significant Bit* (LSB) dengan media audio MP3. Pada awalnya pesan teks akan di dilakukan enkripsi menggunakan AES, kemudian hasil *ciphertext*nya akan disisipkan ke dalam audio MP3 dengan menggunakan metode LSB untuk mendapatkan file MP3Stego. Tahapan terakhir untuk mendapatkan file pesan adalah melakukan ekstraksi pada MP3Stego dan melakukan dekripsi dengan menggunakan AES untuk mendapatkan pesan asli. Hasil akhir dari aplikasi ini berupa audio MP3 stego yang telah memuat pesan yang disisipkan. Audio MP3 stego mempunyai ukuran dan bentuk yang sama persis seperti audio MP3 aslinya. Meskipun bit-bit audio MP3 sudah mengalami perubahan akibat penyisipan, namun perubahan itu tidak begitu signifikan, sehingga audio MP3Stego tidak menimbulkan kecurigaan. Berdasarkan pengujian terhadap *Signal Noise to Ratio* (SNR) maka didapatkan nilai SNR berbanding terbalik dengan ukuran pesan yang disisipkan, semakin besar ukuran pesan yang disisipkan maka nilai SNR semakin kecil.

Kata Kunci : Steganografi, Kriptografi, AES, LSB

ABSTRACT

The development of information technology has been growing very rapidly, so as to provide easy access and obtain information data. The negative impact of security problems and the emergence of a wide range of techniques used by the various parties to obtain secret information. Therefore, information security is an important aspect for maintaining the confidentiality of the information. One of the security methods that can be used to secure the secret message without perceptible is to combine methods of cryptography and steganography. In this study, the method used is AES cryptography and steganography method used is LSB with MP3 audio containers. At first text message will be carried out using the AES encryption, then the results will inserted into MP3 audio by using LSB method to obtain Stego.MP3 file. The last stage to get the message file is doing extracting the MP3Stego and perform decryption using the AES to get the original message. The end result of this application in the form of audio MP3stego contains messages that have been inserted. MP3 audio stego have the same size and shape exactly as the original MP3 audio. Although the MP3 audio bits have changed as a result of the insertion, but the change was not so significant, so the MP3 audio Stego not to arouse suspicion. Based on the testing of the SNR then obtained SNR value is inversely proportional to the size of the message is inserted.

Key*word*s : Steganography, Cryptography, AES, LSB

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah Subhanahu wa Ta'ala yang telah melimpahkan segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini yang mempunyai judul "Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* dan *Advanced Encryption Standard*".

Skripsi ini dibuat dengan tujuan sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada Jurusan Ilmu Komputer/Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.

Dalam pelaksanaan tugas akhir serta penyusunan dokumen skripsi ini, penulis menyadari banyak pihak yang membantu sehingga akhirnya dokumen ini dapat diselesaikan. Oleh karena itu, melalui kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Prof. Dr. Widowati, S.Si, M.Si, selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
3. Indra Waspada, S.T, M.TI, selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
4. Aris Sugiharto, S.Si, M.Kom, selaku dosen pembimbing yang telah membantu dalam membimbing dan mengarahkan penulis hingga selesainya skripsi ini.

Penulis menyadari bahwa dokumen skripsi ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang membangun sangat penulis harapkan. Akhir kata, semoga skripsi ini dapat bermanfaat bagi semua pihak.

Semarang, 20 Agustus 2015

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

BAB I
PENDAHULUAN

Bab pendahuluan ini menjelaskan tentang latar belakang dari pemilihan tema dan judul tugas akhir ini, rumusan masalah dalam pelaksanaan tugas akhir, tujuan dan manfaat yang dapat diperoleh, ruang lingkup yang menjadi batasan-batasan dari tugas akhir, dan sistematika penulisan dokumen tugas akhir ini.

1.1. Latar Belakang

Perkembangan teknologi sekarang ini yang tumbuh semakin pesat terutama di bidang internet dan multimedia telah memberikan kemudahan kepada masyarakat. Perkembangan ini tentu memberikan dampak positif dan dampak negatif. Dampak positif dari perkembangan teknologi internet antara lain adalah memberikan kemudahan dalam mendapatkan pesan atau data informasi. Sayangnya dengan berkembangnya teknologi ini tentu memberikan dampak negatif. Berbagai teknik yang *modern* banyak digunakan oleh orang yang tidak bertanggung jawab untuk dapat memperoleh data atau informasi yang bukan haknya, maka dari itu dengan semakin bekembangnya teknologi informasi ini juga harus berbanding lurus dengan perkembangan pengamanan data informasi.

File audio yang telah dikenal masyarakat umumnya antara lain MIDI, WAV, FLAC,dan MP3. Saat ini dokumen audio yang sering digunakan ialah audio MP3. Menurut (Arubusman, 2007), format kompresi audio MP3 saat ini menjadi yang terpopuler dan merupakan kompresi audio yang jauh lebih baik dari segi kapasitas dan kualitas, ditunjukkan dengan meluasnya penggunaan MP3 oleh banyak orang. Akan tetapi bukan hal yang mustahil, bahwa MP3 dapat digunakan untuk aplikasi keamanan informasi. MP3 memiliki ukuran yang relatif lebih besar daripada dokumen citra, sehingga memungkinkan lebih banyak data yang bisa disembunyikan dalam media ini. Dengan begitu, dalam beberapa waktu ke depan MP3 tidak hanya berfungsi sebagai media audio saja tetapi dapat berfungsi lebih banyak, salah satunya sebagai alternatif media penyimpanan pesan rahasia.

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,

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.

Metode steganografi yang digunakan adalah metode *Low Bit Encoding* atau biasa dikenal dengan nama *Least Significant Bit* (LSB). LSB adalah sebuah teknik steganografi dengan mengganti bagian tertentu dari bit-bit yang kurang berpengaruh dengan bit-bit informasi yang disisipkan. Penggunaan metode ini populer dikarenakan implementasinya yang sederhana dan dapat menyisipkan informasi lebih banyak dibandingkan dengan metode audio steganografi yang lain seperti *spread spectrum*, *echo hiding* ataupun *phase coding*. Namun pada perkembangannya diketahui bahwa penggunaan metode LSB pada audio steganografi rentan terhadap serangan analisis statistik dan proses steganalisis (Djebbar, 2010).

Untuk menjaga keamanan data lebih lanjut maka sebelum digunakan metode LSB untuk penyisipan pesan maka data dienkripsi terlebih dahulu. Enkripsi adalah proses pengubahan suatu pesan teks ke dalam bentuk kode atau sandi untuk mengamankan data dari pencurian (Ariyus, 2008), sehingga meskipun data yang disisipkan dapat diekstraksi, data yang diekstraksi masih aman karena masih dalam kondisi terenkripsi. Metode enkripsi yang digunakan adalah metode AES karena metode ini lebih fleksibel dan memiliki faktor keamanan yang lebih baik dari segi kunci maupun ukuran blok dibandingkan metode lain seperti Blowfish, Twofish, RC4, DES ataupun Triple DES dan untuk memecahkan kunci AES-128 bit maka terdapat $2^{128} = 3{,}4 \times 10^{38}$ kemungkinan kunci.

Riset terdahulu terkait dengan steganografi audio dengan LSB telah dilakukan oleh Aminah Rizki Lubis(2012). Aminah Rizki membuktikan suatu teknik penyembunyian pesan rahasia di dalam media audio MP3 dengan menggunakan metode penyisipan LSB. Hasil file keluaran yang dihasilkan mengalami perubahan rendah, hal ini dapat terlihat dari rata-rata nilai *Peak Signal To Noise Ratio* sebesar 99.5 % yang artinya bahwa hanya terjadi kerusakan audio 0.5 % dalam setiap file hasil keluaran yang dibandingkan dengan file asli yang menjadi masukkannya.

Pada penelitian ini diterapkan sebuah aplikasi perangkat lunak yang dapat menyisipkan teks dengan konsep steganografi menggunakan metode LSB dan enkripsi pesan menggunakan algoritma AES ke dalam *file 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.

1.2. Rumusan Masalah

Melihat latar belakang yang ada, dapat dirumuskan permasalahannya yaitu bagaimana menghasilkan suatu aplikasi steganografi menggunakan metode LSB dan algoritma AES yang memiliki output berupa stego file audio MP3 yang dapat menyimpan data informasi berupa pesan text dan dapat menampilkan kembali pesan informasi.

1.3. Tujuan dan Manfaat

Tujuan tugas akhir mengenai pembangunan aplikasi steganografi dan enkripsi dengan AES ini adalah :

1. Penelitian ini bertujuan untuk membangun sebuah sistem yang dapat menyisipkan pesan teks dengan menggunakan enkripsi AES ke dalam media audio MP3 dan memunculkan kembali pesan teks yang telah disisipi.
2. Penelitian ini bertujuan untuk mengetahui perubahan yang terjadi pada berkas audio MP3 setelah terjadinya proses penyisipan pesan dilihat dari :
    a. Aspek *fidelity*, pengukuran menggunakan parameter SNR.
    b. Aspek *recovery*, pengukuran menggunakan parameter nilai CER.
    c. Aspek *robustness*, pengujian dilakukan dengan melakukan manipulasi terhadap sinyal MP3*(Bitrate, Mode Channel, Frequency Sampling)*
    d. Aspek *security*, pengujian dilakakukan dengan mencoba menggunakan kunci yang sesuai dan tidak sesuai *(AES)*.

Manfaat dari penelitian tugas akhir ini adalah aplikasi steganografi audio MP3 ini diharapkan dapat dapat dimanfaatkan sebagai salah satu solusi dalam mengamankan pesan rahasia.

1.4. Ruang Lingkup

Pada tugas akhir ini terdapat beberapa pembatasan ruang lingkup agar nantinya pengerjaan tugas akhir ini tidak keluar dari target yang diharapkan, diantaranya adalah sebagai berikut.

1. Media penampung yang digunakan adalah file audio MP3.
2. File yang disisipkan berupa pesan teks dengan ukuran lebih kecil dibandingkan file pembawanya.
3. Key yang digunakan terbatas sebanyak 16 karakter untuk AES 128 bit, 24 karakter untuk AES 192 bit, dan 32 karakter untuk AES 256 bit .
4. Bahasa pemrograman yang digunakan adalah Java dengan bantuan IDE Netbeans.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dokumen tugas akhir ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan tentang hal-hal yang melatar belakangi dari pembuatan tugas akhir ini, rumusan permasalahan yang dikerjakan, tujuan dan manfaat yang diharapkan, ruang lingkup yang membatasi, dan sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang keseluruhan dari teori-teori yang digunakan dalam pengerjaan tugas akhir ini.

BAB III FASE *INCEPTION* DAN FASE *ELABORATION*

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan *Unified Process*. Pada Bab ini disajikan dua fase awal yaitu *Inception* dan *Elaboration.*

BAB IV FASE *CONSTRUCTION* DAN *FASE TRANSITION*

Bab ini membahas mengenai tahapan akhir dari pembangunan perangkat lunak untuk model pengembangan *Unified Process*. Pada Bab ini disajikan fase *Construction* yaitu fase untuk melakukan implementasi dan fase *Transition* untuk melakukan pengujian sistem.

BAB III PENUTUP

Bab ini berisi tentang kesimpulan dari pengerjaan tugas akhir ini, beserta dengan saran yang dapat diajukan guna pengembangan sistem ini ke depannya.