IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN METODE *LEAST SIGNIFICANT BIT* (LSB) UNTUK PENGAMANAN DAN PENYEMBUNYIAN *FILE*

SKRIPSI

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

Disusun Oleh:
LUTFIARANI SAFITRI
24010311130075

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

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

Semarang, 15 Desember 2015

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma *Advanced Encryption Standard* (AES) Dan Metode *Least Significant Bit* (LSB) Untuk Pengamanan Dan Penyembunyian *File*

Nama : Lutfiarani Safitri

NIM : 24010311130075

Telah diujikan pada sidang tugas akhir pada tanggal 15 Desember 2015 dan dinyatakan lulus pada tanggal 30 Desember 2015.

Semarang, 31 Desember 2015

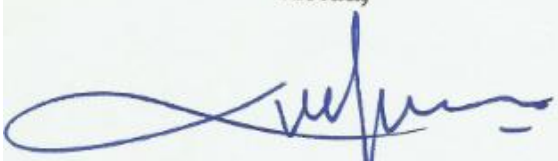
Mengetahui,

Ketua Jurusan Ilmu Komputer / Informatika
FSM UNDIP

Ragil Saputra, S.Si, M.Cs
NIP. 19801021 200501 1 003

Panitia Penguji Tugas Akhir

Ketua,



Nurdin Bahtiar, S.Si, M.T
NIP. 197907202003121002

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma *Advanced Encryption Standard* (AES) dan Metode *Least Significant Bit* (LSB) Untuk Pengamanan dan Penyembunyian *File*

Nama : Lutfiarani Safitri

NIM : 24010311130075

Telah diujikan pada sidang tugas akhir pada tanggal 15 Desember 2015

Semarang, 30 Desember 2015

Pembimbing

Drs. Suhartono, M.Kom

NIP. 195504071983031003

ABSTRAK

File berformat .doc merupakan salah satu *file* yang sering dipertukarkan melalui internet. Proses pertukaran ini tidak dapat menjamin bahwa *file* yang dikirimkan akan bebas dari pengaksesan oleh orang-orang yang tidak berwenang. *File* yang diakses oleh orang yang tidak berwenang dapat disalahgunakan sehingga akan merugikan pihak lain, oleh karena itu dibutuhkan pengamanan terhadap *file* yang dianggap penting sehingga orang-orang yang tidak berkepentingan tidak dapat mengakses *file* tersebut, dengan cara menerapkan mekanisme kriptografi dan steganografi. Tugas akhir ini membahas tentang implementasi Algoritma *Advanced Encryption Standard* (AES) dan Metode *Least Significant Bit* (LSB) untuk pengamanan dan penyembunyian *file* berformat .doc. Algoritma *Advanced Encryption Standard* (AES) dipilih karena dari algoritma ini cukup aman, tidak mudah dipecahkan, dan juga terhitung cepat dalam pemrosesannya. Metode *Least Significant Bit* (LSB) dipilih karena sederhana dan perbedaan antara citra asli dan citra hasil penyisipan hampir tidak terlihat sehingga memperkecil kemungkinan pihak tidak berwenang dapat menemukan *file* yang disembunyikan tersebut. Citra hasil dari proses enkripsi dan penyisipan menunjukkan nilai *Peak Signal to Noise Ratio* (PSNR) antara 39 dB sampai 59 dB yang berarti citra hasil penyisipan tidak jauh berbeda dengan citra sebelum disisipi. Nilai PSNR dipengaruhi oleh dimensi citra dan ukuran *file.* Semakin besar dimensi citra, citra dapat menampung *file* yang berukuran lebih besar. Berdasarkan pengujian yang dilakukan, *file* yang disisipkan kedalam citra tidak dapat diekstraksi jika citra hasil penyisipan diproses manipulasi citra seperti *grayscale, cropping*¸atau kompresi.

Kata Kunci : Kriptografi, *Advanced Encryption Standard* (AES), Steganografi, *Least Significant Bit* (LSB), *Peak Signal to Noise Ratio* (PSNR).

ABSTRACT

Doc file is one of the most frequently exchanged files via internet. This exchange process cannot guarantee that the files will be freely accessed by unauthorized people. Files which are accessed by unauthorized people can be abused to harm others. Therefore, it is necessary to protect important files, so that unauthenticated people cannot access the files, by applying the mechanism of cryptography and steganography. This final project discusses about the implementation of the Advanced Encryption Standard algorithm (AES) and the Least Significant Bit (LSB) method for security and hiding .doc files. Advanced Encryption Standard algorithm (AES) is selected because this algorithm is quite safe, not easily solved, and also fast in processing. Least Significant Bit (LSB) method is selected because it is simple and the changes between the image original and image result is not noticeable. The image results of the encryption process and the insertion show Peak Signal to Noise Ratio (PSNR) between 39 dB to 59 dB which means the image results are not much different from the image before it is inserted. PSNR value is influenced by dimensions of the image and the size of file. Larger dimensions of image, can accommodate larger file. Based on tests performed, file that inserted into image can not be extracted if image result get manipulation process such grayscaling, cropping, or compressing.

Keywords: Cryptography, Advanced Encryption Standard (AES), Steganography, Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR).

KATA PENGANTAR

Segala puji syukur bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan Tugas Akhir ini.

Laporan Tugas Akhir yang berjudul **"Implementasi Algoritma *Advanced Encryption Standard* (AES) dan Metode *Least Significant Bit* (LSB) untuk Pengamanan dan Penyembunyian *File*"** disusun sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada Jurusan Ilmu Komputer/Informatika Universitas Diponegoro. Penelitian Tugas Akhir ini mahasiswa dituntut untuk mengimplementasikan ilmu yang didapat di bangku perkuliahan untuk menyelesaikan suatu permasalahan yang ada dengan menggunakan teknik penelitian ilmiah.

Penyusunan laporan ini tentulah Penulis banyak mendapat bimbingan dan bantuan dari berbagai pihak. Kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada :

1. Prof. Dr. Widowati, M.Si, selaku Dekan Fakultas Sains dan Matematika (FSM) Universitas Diponegoro.
2. Ragil Saputra, S.Si, M.Cs, selaku Ketua Jurusan Ilmu Komputer/Informatika FSM UNDIP.
3. Helmie Arif Wibawa, S.Si, M.Cs selaku Dosen Koordinator Tugas Akhir Jurusan Ilmu Komputer/Informatika FSM UNDIP.
4. Drs. Suhartono, M.Kom selaku Dosen Pembimbing yang telah membantu dalam proses bimbingan hingga terselesaikannya laporan Tugas Akhir ini.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajian karena keterbatasan kemampuan dan pengetahuan Penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan.

Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya

Semarang, 15 Desember 2015

Penulis

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup penelitian tugas akhir mengenai implementasi Kriptografi Algoritma *Advanced Encryption Standard* (AES) dan Steganografi Metode *Least Significant Bit* (*LSB*) untuk pengamanan dan penyembunyian *file*.

1.1. Latar Belakang

Penyimpanan *file* di dalam komputer tidak dapat menjamin bahwa *file* disimpan akan bebas dari pengaksesan oleh pihak-pihak yang tidak berwenang. Begitupun dengan pengiriman *file* melalui internet. *File* yang disimpan ataupun dikirimkan lewat internet dapat disalahgunakan oleh penyerang untuk tujuan tertentu, misalnya penyerang ingin menangkap informasi penting dalam *file* yang disimpan atau dikirimkan, atau mengubah isi dari *file* sehingga mempunyai makna yang berbeda yang akan memberikan keuntungan bagi penyerang. Untuk mengatasi hal ini, dapat dikembangkan layanan keamanan jaringan yang diwujudkan dengan mekanisme keamanan jaringan. Mekanisme keamanan jaringan pada implementasinya menggunakan teknik penyandian yaitu kriptografi dan steganografi (Sadikin, 2012).

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkripsi informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkripsi dinamakan *plaintext*. Setelah dienkripsi dengan suatu kunci, dinamakan *ciphertext*. Steganografi (*Steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia (Munir, 2006). Steganografi membutuhkan dua properti yaitu media penampung dan data rahasia yang akan disembunyikan.

Algoritma kriptografi yang baik adalah algoritma yang dapat menjaga kerahasiaan pesan dan tidak mudah untuk dipecahkan oleh orang-orang yang tidak berkepentingan (kriptanalis). Algoritma *Advanced Encryption Standard* (AES) merupakan salah satu algoritma kriptografi modern. Pemilihan Algoritma *AES* dikarenakan dalam segi keamanan algoritma ini cukup aman, hal ini dibuktikan

dengan dilakukan uji ketahanan dengan menggunakan *exhaustive attack* membutuhkan waktu selama 5.4 x 10^{24} tahun untuk mencoba semua kemungkinan kunci (Septyandi K, 2014). Selain itu, dibandingkan dengan algoritma *Blowfish,* algoritma AES terbukti lebih cepat dalam pemrosesan (Riftadi, 2009).

Salah satu kriteria steganografi yang baik adalah perbedaan antara media sebelum disisipi pesan dan setelah disisipi pesan tidak dapat tertangkap oleh indera manusia. Salah satu media yang dapat digunakan untuk penyembunyian data adalah media citra. Media citra dipilih sebagai media penyisipan karena seringnya pertukaran data dengan menggunakan citra sehingga penyerang tidak akan curiga.

Penyisipan pesan dengan metode *Least Significant Bit* dianggap cukup aman karena kualitas citra sebelum disisipi pesan tidak jauh berbeda dengan kualitas citra setelah disisipi pesan. Metode *Least Significant Bit* adalah metode penyembunyian data yang dilakukan dengan mengganti *bit-bit* terahir dalam citra dengan *bit- bit* data rahasia (Munir, 2006). Penggantian *bit* terakhir ini akan mengakibatkan perubahan nilai *byte* satu lebih tinggi atau satu lebih rendah daripada sebelumnya, perubahan tersebut tidak mengubah citra secara berarti sehingga perbedaan yang terjadi tidak dapat tertangkap oleh mata manusia.

Dengan demikian, pengembangan aplikasi untuk pengamanan *file* yang mengimplementasikan Algoritma *Advanced Encryption Standard* (AES) dan Metode *Least Significant Bit* (*LSB*) ini diharapkan dapat mengamankan dan menyembunyikan informasi dalam bentuk *file* dari pihak yang tidak berkepentingan yang dapat mengakibatkan penyalahgunaan *file* tersebut.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi yaitu bagaimana membuat aplikasi yang mengimplementasikan Algoritma *Advanced Encryption Standard* (AES) dan Metode *Least Significant Bit* (*LSB*) untuk pengamanan dan penyembunyian *file*.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan aplikasi yang mengimplementasikan Algoritma *Advanced Encryption Standard* (AES) dan metode *Least Significant Bit* untuk pengamanan dan penyembunyian *file*.

Manfaat dari penelitian tugas akhir ini adalah aplikasi yang dikembangkan dapat membantu pengamanan dan penyembunyian *file* sehingga *file* tidak dapat diakses dan dideteksi keberadaannya oleh pihak yang tidak berwenang.

1.4. Ruang Lingkup

Ruang lingkup penelitian tugas akhir mengenai implementasi Kriptografi Algoritma *Advanced Encryption Standard (AES)* dan Steganografi Metode *Least Significant Bit* (LSB) untuk pengamanan dan penyembunyian *file* adalah sebagai berikut:

1. Aplikasi berbasis *desktop*
2. File yang dapat disisipkan hanya file berformat .doc
3. Citra sebagai media penampung adalah citra digital berformat .bmp 24-bit
4. Kunci enkripsi sepanjang maksimal 16 karakter
5. Algoritma Kriptografi yang digunakan adalah Algoritma *Advanced Encryption Standard (AES)* 128 *bit.*
6. Metode steganografi yang digunakan adalah metode *Least Significant Bit* (LSB).
7. Aplikasi dibuat dengan bahasa pemrograman C#
8. Penilaian kualitas citra menggunakan penghitungan *Peak Signal To Noise Ratio* (PSNR)

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Merupakan pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan.

BAB II LANDASAN TEORI

Berisi kumpulan studi pustaka yang berhubungan dengan topik tugas akhir. Dasar teori ini meliputi materi tentang Kriptografi, Algoritma *Advanced Encryption Standard* (AES), Steganografi, konsep Citra, metode *Least Significant Bit* (*LSB*), *Peak Signal To Noise Ratio* (PSNR), dan Metode Pengembangan *Unified Process*.

BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN

Membahas tahap definisi kebutuhan, analisis, dan tahap perancangan, serta hasil yang didapat pada ketiga tahap tersebut.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Membahas tahap implementasi dan rincian pengujian aplikasi yang dibangun dengan metode *black box*.

BAB V PENUTUP

Berisi kesimpulan yang diambil berkaitan dengan aplikasi yang dikembangkan dan saran-saran untuk pengembangan aplikasi lebih lanjut.