IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT*, ENKRIPSI *RIJNDAEL*, DAN *BLUM-BLUM-SHUB*

SKRIPSI

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

Disusun Oleh:
Andreas Syahputra Sinurat
24010311140080

DEPARTEMEN ILMU KOMPUTER/INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2018

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Andreas Syahputra Sinurat

NIM : 24010311140080

Judul skripsi : Implementasi Steganografi Pada Citra Digital dengan Menggunakan Metode *Least Significant Bit,* Enkripsi Rijndael, dan *BlumBlumShub.*

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

Semarang, 3 Juli 2018

Andreas Syahputra Sinurat

NIM. 24010311140080

HALAMAN PENGESAHAN

Judul : Implementasi Steganografi Pada Citra Digital dengan Menggunakan Metode *Least Significant Bit,* Enkripsi Rijndael, dan *BlumBlumShub.*

Nama : Andreas Syahputra Sinurat

NIM : 24010311140080

Telah diujikan pada sidang tugas akhir pada tanggal 22 Juni 2018 dan dinyatakan lulus pada tanggal 22 Juni 2018.

Semarang, 3 Juli 2018

Mengetahui,
Ketua Departemen Ilmu Komputer/ Informatika
FSM Universitas Diponegoro

Dr. Retno Kusumaningrum, S.Si, M.Kom.
NIP. 198104202005012001

Panitia Penguji Tugas Akhir
Ketua

Ragil Saputra, S.Si, M.Cs
NIP. 198010212005011003

HALAMAN PENGESAHAN

Judul : Implementasi Steganografi Pada Citra Digital dengan Menggunakan Metode *Least Significant Bit,* Enkripsi Rijndael, dan *BlumBlumShub.*

Nama : Andreas Syahputra Sinurat

NIM : 24010311140080

Departemen : Ilmu Komputer/Informatika

Telah diujikan pada sidang tugas akhir pada tanggal 22 Juni 2018.

Semarang, 3 Juli 2018

Pembimbing

Drs. Eko Adi Sarwoko, M.Kom.

NIP. 196511071992031003

ABSTRAK

Data merupakan sumber informasi yang penting bagi manusia, terutama bagi organisasi, instansi, dan negara. Data tersebut dapat berupa dokumen, pesan, dan sebagainya. Data yang penting memerlukan sistematika pengamanan agar terhindar dari segala bentuk kejahatan yang mungkin dilakukan oleh orang lain. Oleh karena itu dibutuhkan pengamanan dengan cara menerapkan mekanisme kriptografi dan steganografi. Pada penelitian tugas akhir ini membahas tentang implementasi steganografi dengan menggunakan metode *Least Significant Bit* (LSB), algoritma *Advanced Encryption Standard* (AES) Rijndael, dan pembangkit bilangan acak semu *BlumBlumShub*. Algoritma AES Rijndael dipilih karena algoritma ini cukup aman dan tidak mudah dipecahkan. Metode LSB dipilih karena sangat sederhana dan perbedaan citra asli dan citra hasil penyisipan hampir tidak terlihat. PRNG *BlumBlumShub* dipilih karena sangat efektif dan sederhana secara kompleksitas teoritis dalam menghasilkan bilangan acak untuk posisi piksel dalam penyisipan pesan. Citra hasil dari proses enkripsi dan penyisipan menunjukkan nilai *Peak Signal to Noise Ratio* (PSNR) antara 40 dB sampai 80 dB yang berarti citra hasil penyisipan tidak jauh berbeda dengan citra sebelum disisipi. Berdasarkan pengujian yang dilakukan, pesan yang disisipkan kedalam citra tidak dapat diekstraksi jika pada citra hasil penyisipan dimanipulasi, seperti *grayscale, cropping,* atau kompresi.

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

ABSTRACT

Data are an important source of information for human, especially for organizations, agencies, and countries. Data can be documents, messages, etc. These important data require systematic security to avoid any form of crime that may be committed by others. Therefore, it is necessary to protect the data by applying cryptographic and steganographic mechanisms. This final project discussed the implementation of steganography using Least Significant Bit (LSB) method, Advanced Encription Standard (AES) Rijndael algorithm, and BlumBlumShub Pseudo Random Number Generator (PRNG). AES Rijndael algorithm was chosen because it is safe and not easily solved. The LSB method was chosen because it is simple and diifferences between original images and images after insertion are almost invisible. PRNG BlumBlumShub was chosen because it is effective and simple in theoretical complexity on generating random numbers for pixel positions in message insertions. Result images of the encryption and insertion process shows the value of Peak Signal to Noise Ratio (PSNR) between 40 dB to 80 dB which means images after the insertion were not much different from images before the insertion. Based on tests performed, messages inserted into images can not be extracted if images after insertion are manipulated, such as grayscaling, cropping or compressing.

Keywords : Steganography, Cryptography, Least Significant Bit (LSB), AES Rijndael, BlumBlumshub, Peak Signal to Noise Ratio (PSNR).

KATA PENGANTAR

Segala Puji bagi Tuhan Yang Maha Esa atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "Implementasi Steganografi Pada Citra Digital dengan Menggunakan Metode *Least Significant Bit,* Enkripsi Rijndael, dan *BlumBlumShub.*" ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Departemen Ilmu Komputer/ Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan laporan ini tentulah banyak mendapat bantuan dan dukungan dari berbagai pihak. Untuk itu pada kesempatan ini penulis mengucapkan rasa hormat dan terimakasih kepada :

1. Dr. Retno Kusumaningrum, S.Si, M.Kom. selaku Ketua Departemen Ilmu Komputer / Informatika FSM Universitas Diponegoro.
2. Helmie Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Departemen Ilmu Komputer / Informatika FSM Universitas Diponegoro.
3. Drs. Eko Adi Sarwoko, M.Kom. selaku dosen Pembimbing
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya 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, 3 Juli 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan dalam tugas akhir "*Implementasi Steganografi Pada Citra Digital dengan Menggunakan Metode Least Significant Bit, Enkripsi Rijndael, dan Blum-Blum-Shub*".

1.1. Latar Belakang

Pada era globalisasi sekarang ini, data merupakan sumber informasi yang penting bagi manusia, terutama bagi organisasi, instansi, dan negara. Data tersebut dapat berupa dokumen, pesan, dan sebagainya. Beberapa data dianggap penting bagi manusia karena isi ataupun kegunaan dari data tersebut. Data yang penting tersebut memerlukan sistematika pengamanan agar terhindar dari segala bentuk kejahatan yang mungkin dilakukan oleh orang lain. Kejahatan yang dapat terjadi pada data yaitu, pencurian data, perusakan data, pemalsuan data, dan penyadapan data.

Pengguna informasi semakin gencar mengembangkan suatu sistem pengamanan terhadap data. Berbagai macam teknik digunakan untuk melindungi data dari orang yang tidak berhak. Salah satu teknik yang sering digunakan adalah steganografi. Berbeda dengan kriptografi yang tujuannya mengacak pesan agar tidak dapat dimengerti orang lain, steganografi bertujuan untuk menyembunyikan pesan rahasia agar pihak lain tidak menyadari keberadaan dari pesan tersebut. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut.

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 informasi adalah media citra. Media citra dipilih sebagai media penyisipan karena seringnya penyampaian informasi dengan menggunakan citra pada perangkat digital. Penyisipan pesan dengan metode *Least Significant Bit* adalah metode penyembunyian pesan yang dilakukan dengan mengganti bit-bit terakhir dalam citra dengan bit-bit data rahasia (Munir, 2004). Konsep penyisipan pesan dengan menggunakan metode LSB ini adalah dengan mengubah nilai bit LSB dari setiap piksel pada citra sesuai dengan nilai biner pada pesan secara berurutan.

Penelitian pada jurnal yang berjudul "Analisa Kualitas Citra pada Steganografi untuk Aplikasi e-Government", modifikasi algoritma LSB dilakukan dengan menggunakan algoritma pembangkit bilangan acak semu (PRNG) untuk memilih posisi penyisipan pesan dengan pola tertentu. *Pseudorandom Number Generator* (PRNG) berfungsi untuk memperkuat teknik penyembunyian pesan, dimana bit-bit pesan tidak digunakan mengganti bit-bit dari piksel awal sampai piksel terakhir secara berurutan, namun dipilih susunan piksel secara acak (Male, Wirawan, & Setijadi, 2012).Piksel-piksel acak tersebut dapat dihasilkan dengan memanfaatkan algoritma *BlumBlumShub* yang efektif dan sederhana secara kompleksitas teoritis sebagai pembangkit bilangan acak semu (*Pseudorandom Number Generator /* PRNG).

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkripsi dan mendekripsi informasi tersebut dengan suatu kunci khusus. Algoritma kriptografi yang baik adalah algoritma yang dapat menjaga kerahasiaan pesan dan tidak mudah untuk dipecahkan oleh orang-orang yang tidak berkepentingan (kriptanalis).

Algoritma Rijndael merupakan salah satu algoritma kriptografi modern yang telah memenuhi standar keamanan AES (*Advanced Encryption Standard*). Menurut Delfianto pada jurnalnya yang berjudul "Studi dan Perbandingan Algoritma Rijndael dengan Algoritma Serpent", Rijndael memiliki *average clock cycle* 504, lebih cepat dibandingkan Serpent yang memiliki *average clock cycle* 2269 (diuji pada prosesor dengan arsitektur IA64). Hal tersebut dipengaruhi oleh operasi algoritma Rijndael lebih sedikit dibandingkan dengan Serpent (Rijndael = 10 operasi, Serpent = 32 operasi). Dalam hal desain, desain Rijndael lebih sederhana dibandingkan dengan Serpent karena menggunakan komponen yang sederhana. Desain Rijndael juga mendukung *parallel processing* yang sangat menguntungkan dimana perkembangan komputer saat ini adalah ke arah komputer dengan prosesor yang dapat mengeksekusi instruksi secara paralel (Delfianto, 2010).

Perangkat lunak komputer merupakan suatu perangkat program, prosedur, dan dokumen yang berkaitan dengan suatu sistem komputer. Suatu perangkat lunak dibutuhkan untuk melakukan operasi penyisipan teks digital pada suatu citra digital. Perangkat lunak tersebut perlu memiliki suatu kemampuan untuk mengenkripsi teks yang akan disisipkan untuk meningkatkan kerahasiaan teks yang disisipkan ke dalam citra digital.

Sebelumnya pernah dilakukan penelitian oleh Lutfiarani Safitri yang menghasilkan perangkat lunak untuk melakukan penyisipan berkas teks berformat .doc ke dalam citra

digital dengan konsep steganografi menggunakan metode LSB serta enkripsi pesan menggunakan algoritma AES Rijndael. Pada perangkat lunak tersebut proses penyisipan dilakukan berurut tanpa proses pengacakan lokasi piksel yang akan disisipi oleh bit informasi, dari berkas masukan yang telah terenkripsi. Kesimpulan yang dicapai pada penelitian tersebut menunjukkan bahwa metode pengacakan dirasa perlu untuk meningkatkan keamanan berkas yang disisipkan pada suatu citra digital. (Safitri, 2015)

Pada penelitian ini akan dikembangkan sebuah perangkat lunak yang dapat menyisipkan teks pada citra digital dengan konsep steganografi menggunakan metode LSB dan metode *Blum-Blum-Shub* dalam pengacakan lokasi penyisipannya, serta enkripsi pesan menggunakan algoritma AES Rijndael. Aplikasi ini diharapkan menjadi salah satu solusi penyembunyian informasi dari pihak yang tidak berkepentingan dan menjaga keamanan informasi agar lebih terjamin.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana membuat suatu aplikasi yang mengimplementasikan metode steganografi menggunakan metode *Least Significant Bit* untuk penyisipan pesan, algoritma kriptografi AES Rijndael untuk pengacakan informasi pesan, dan algoritma PRNG *BlumBlumShub* untuk pengacakan lokasi penyisipan.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah menghasilkan aplikasi yang mengimplementasikan metode steganografi menggunakan metode *Least Significant Bit* (LSB), algoritma kriptografi AES Rijndael, dan algoritma PRNG *BlumBlumShub* yang dapat menyisipkan informasi berupa pesan teks ke dalam citra digital dan mengetahui dampak serangan berupa kompresi, *grayscale,* dan *cropping* terhadap citra hasil penyisipan dan hasil ekstraksi.

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

1.4. Ruang Lingkup

Ruang lingkup dari penelitian tugas akhir ini adalah sebagai berikut:

1. Aplikasi berbasis desktop menggunakan bahasa C#.

2. Input berupa teks, citra sebagai media penampung, dan kunci enkripsi (maksimal 16 karakter).
3. Algoritma Kriptografi yang digunakan adalah algoritma Rijndael, algoritma PRNG yang digunakan algoritma *BlumBlumShub*, dan metode steganografi yang digunakan adalah metode *Least Significant Bit* (LSB).
4. Citra media penampung berupa citra digital berformat .bmp 24 bit.
5. Penilaian kualitas citra menggunakan penghitungan *Peak Signal to Noise Ratio* (PSNR).
6. Metode pengembangan yang digunakan yaitu metode *Unified Process* dengan satu kali iterasi. *Workflow* yang digunakan pada penelitian ini antara lain :
   a. *Requirement,* terdiri dari model bisnis atau deskripsi sistem, spesifikasi kebutuhan fungsional perangkat lunak, *business actor,* dan *business use case*.
   b. Analisis, terdiri dari *analysis class (boundary, control, entity)*, *use case realization-analysis*, dan *class responsibility and collaboration* (interaksi antar objek).
   c. Desain, terdiri dari *design class*, *use case realization-design*, *class diagram*, *sequence diagram*, *activity diagram*, dan perancangan sketsa antarmuka
   d. Implementasi, terdiri dari *implementation subsystem, implementation component,* dan *test subsystem*.
   e. *Test,* terdiri dari *black box* dan *test case.*

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 dasar teori yang berhubungan dengan topik tugas akhir. Dasar teori ini meliputi materi tentang Steganografi, *Least Significant Bit*, Kriptografi, Algoritma Rijndael, *Pseudo Random Number Generator*, *BlumBlumShub,* Citra Digital, *Peak Signal to*

Noise Ratio, bahasa *C#*, *Unified Modeling Language*, dan metode *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.