Penerapan Keamanan Penyampaian Informasi Melalui Citra dengan Kriptografi Rijndael dan Steganografi LSB

Information Security Through Imagery with Rijndael Cryptography and Steganography LSB

Bonifacius Vicky Indriyono
Sekolah Tinggi Manajemen Informatika dan Komputer Kadiri (STMIKKA) Kediri
E-mail: **bonifaciusvicky@gmail.com**

Abstrak

Komunikasi telah menjadi bagian dari kehidupan manusia dan menjadi hal yang sangat penting seiring dengan berjalannya waktu. Dalam proses komunikasi, banyak terjadi kegiatan pertukaran informasi. Ada kalanya informasi yang dipertukarkan tersebut bersifat penting dan rahasia sehingga keberadaannya tidak boleh diketahui oleh pihak yang tidak berkepentingan. Dengan berkembangnya teknologi informasi, banyak cara yang dilakukan agar kerahasiaan informasi tersebut dapat terjaga agar tidak jatuh ke tangan pihak-pihak yang tidak berkepentingan. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan dan meningkatkan aspek keamanan informasi. Selain menggunakan teknik kriptografi, menjaga kerahasiaan informasi juga dapat dilakukan dengan menggunakan metode steganografi, dimana dalam metode ini informasi yang akan dikirimkan disisipkan melalui sebuah media (gambar, musik, suara, video).

Dalam penelitian ini, peneliti merancang sebuah aplikasi dengan menerapkan kombinasi steganografi teknik Least Significant Bit untuk menyisipkan informasi pesan dalam media gambar bitmap 24 bit dan kriptografi Rijndael yang digunakan untuk melakukan enkripsi terhadap gambar bitmap sehingga informasi pesan dapat diamankan dari pihak-pihak yang tidak berkepentingan.

Kata Kunci *— Kriptografi, Steganografi, LSB, Rijndael*

Abstract

Communication has been a part of human life and become very important over time. In the process of communication, a lot going on information exchange. There are times when the information exchanged is important and so secret that its existence should not be known by unauthorized parties. With the development of information technology, many ways in which the confidentiality of the information that can be maintained in order not to fall into the hands of parties who are not interested. Cryptography is the study of science and art to keep a message and to improve aspects of the security of information. In addition to using cryptographic techniques, confidential information can also be done by using steganography, which in this method of information to be transmitted is inserted through a media (images, music, sound, and video).

In this study, researchers designed an application by applying a combination of Least Significant Bit steganography techniques to insert messages in the media information 24 bit bitmap images and Rijndael cryptography is used to encrypt the message bitmap image so that information can be secured from the parties who are not interested.

Keywords *— Cryptography, Steganography, LSB, Rijndael.*

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Komunikasi telah menjadi bagian dari kehidupan manusia dan menjadi hal yang sangat penting seiring dengan berjalannya waktu. Dalam berkomunikasi, ada kalanya informasi yang akan disampaikan bersifat penting dan rahasia sehingga keberadaanya tidak boleh diketahui oleh pihak yang tidak berkepentingan. Oleh karena itu dibutuhkan teknik pengamanan data yang tepat agar keamanan dan kerahasiaan informasi yang akan disampaikan tersebut tetap terjaga. Untuk menjaga keamanan dan kerahasiaan informasi yang akan disampaikan, maka diperlukan teknik untuk melindungi informasi tersebut. Hal ini dilakukan agar informasi penting tidak sampai jatuh ke pihak yang tidak berkepentingan. Kriptografi dan steganografi merupakan teknik yang dikembangkan untuk meningkatkan perlindungan dan keamanan data. Kriptografi merupakan salah satu teknik pengamanan data yang digunakan untuk tujuan menjaga kerahasiaan data, keaslian data serta originalitas [1], sedangkan steganografi adalah teknik yang digunakan untuk menyembunyikan informasi ke dalam sebuah media, bisa berupa media gambar, suara ataupun video [2]. Pada steganografi media gambar dikenal sebuah teknik yang dinamakan *Least Significant Bit* (LSB). Metode penyisipan LSB (*Least Significant Bit*) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan.

Pada penelitian ini akan dibangun sebuah aplikasi dengan kombinasi teknik kriptografi dan steganografi yang dapat dimanfaatkan untuk mengatasi masalah keamanan dalam penyampaian informasi yang bersifat. Teknik Kriptografi yang digunakan dalam penelitian ini adalah AES (*Advanced Encryption Standards*) *Rijndael* karena algoritma kriptografi ini selain aman juga efisien dalam implementasinya [3]. Untuk teknik steganografi, digunakan teknik *Least Significant Bit* (LSB). Pemilihan teknik ini didasarkan pada asumsi bahwa teknik LSB merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu [4]. Format citra yang digunakan sebagai media penampung pesan informasi adalah gambar bitmap 24 bit karena dalam steganografi, format yang diperbolehkan adalah yang bersifat *losslessimage format* (24-bit BMP, 32-bit BMP) sehingga diperlukan suatu media pembawa yang dapat menyimpan bit-bit data tanpa menghilangkan suatu bagian dari bit-bit data tersebut.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, maka dapat dirumuskan beberapa hal berikut ini:

1. Bagaimanakah implementasi algoritma steganografi LSB dalam proses penyisipan informasi ke dalam media gambar?
2. Bagaimanakah proses dan kecepatan enkripsi dengan *AES Rijndael* untuk mengenkripsi gambar?
3. Bagaimanakah implementasi kombinasi teknik kriptografi *AES Rijndael* dan steganografi *Least Significant Bit* (LSB) dalam mengamankan penyampaian informasi melalui media gambar?

1.3. Batasan Variabel Penelitian

Agar pembahasan dalam penelitian ini bisa terarah dan tidak melebar dari konsep yang dikerjakan, maka diberikan beberapa batasan sebagai berikut:

1. Citra yang digunakan sebagai media untuk menampung informasi pesan adalah gambar dengan format bitmap (.bmp) 24 bit.
2. Informasi yang akan disisipkan adalah dalam bentuk teks.
3. Menggunakan teknik steganografi *Least Significant Bit* (LSB).
4. Penelitian ini tidak membahas masalah kelemahan LSB maupun *AES Rijndael*.

5. Menggunakan teknik kriptografi *AES Rijndael* 128 bit untuk mengenkripsi gambar bitmap.
6. Uji coba implementasi menggunakan *compiler* Delphi 2010.

1.4. Tujuan Penelitian

Beberapa tujuan yang ingin dicapai dalam penelitian ini antara lain sebagai berikut:

1. Untuk lebih mengetahui konsep dan algoritma steganografi teknik LSB dalam proses penyisipan informasi melalui media gambar.
2. Memperdalam pengetahuan tentang algoritma kriptografi *AES Rijndael*.
3. Dapat menerapkan teknik kriptografi *AES Rijndael* dan steganografi LSB ke dalam sebuah aplikasi yang dapat digunakan untuk menyampaikan informasi melalui media gambar bitmap 24 bit.

1.5. Ulasan Penelitian Sebelumnya

Bagian ulasan penelitian sebelumnya ini digunakan untuk mempelajari dan melihat hasil dari beberapa penelitian yang dilakukan oleh peneliti sebelumnya yang relevan dengan topik penelitian yang dilakukan peneliti sekarang. Pada bagian ini juga dituliskan perbedaan dengan penelitian yang dilakukan saat ini. Beberapa penelitan terdahulu tentang pemanfaaatan steganografi *Least Significant Bit* (LSB) dan kriptografi *AES Rijndael* diantaranya:

1. Basuki Rakhmat dan Muhammad Fairuzabadi [5] yang membahas tentang Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan RC4.
2. Pada penelitian mereka, proses steganografi yang dilakukan dikombinasikan dengan algoritma Vigenere dan RC4, sedangkan yang dilakukan peneliti sekarang proses steganografi dikombinasikan dengan algoritma kriptografi AES Rijndael 128 bit. Bagus Satrio Waluyo Poetro, Aris Sugiharto dan Sukmawati Nur Endah [6] membahas tentang Kriptografi Citra Digital Dengan Algoritma Rijndael Dan Transformasi Wavelet Diskrit Haar. Perbedaan penelitan ini terletak pada media uji coba dimana pada penelitian yang dilakukan oleh penelitia sebelumnya menggunakan dua komposisi warna yakni RGB dan *Grayscale*, sedangkan yang dilakukan peneliti sekarnag hanya menggunakan citra dengan warna RGB.
3. Bangun Wijayanto dan Retantyo Wardoyo [7] membahas masalah pengacakan citra menggunakan algoritma Catmap-Rijndael. Pada penelitian sebelumnya, citra yang akan diolah berasal dari citra yang dihasilkan melalui *webcam*, sedangkan citra yang digunakan oleh peneliti sekarang adalah gambar bitmap 24 bit yang tidak hanya berasal dari pengolahan *webcam*.
4. Shinta Puspita Sari, Winarno, Dodick Z. Sudirman [8] membahas masalah Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard. Perbedaan dengan penelitian sekarang terletak pada format citra yang digunakan. Penelitian sebelumnya menggunakan format .PNG sedangkan penelitian sekarang menggunakan format .BMP.
5. R. Kristoforus JB dan Stefanus Aditya BP [9] tentang Implementasi Algoritma Rijndael Untuk Enkripsi dan Dekripsi Pada Citra Digital. Pada penelitian sebelumnya lebih membahas pada kecepatan proses enkripsi dan dekripsi Rijndael, sedangkan pada penelitian sekarang lebih membahas pada bagaimana efek citra stego setelah di enkripsi dengan Rijndael dan bagaimana cara mendapatkan kembali pesan stego.
6. Za'imatun Niswati [10] membahas masalah Steganografi Berbasis Least Significant Bit (LSB) Untuk Menyisipkan Gambar Ke Dalam Citra Gambar. Perbedaan dengan penelitian sekarang terletak pada apa yang disisipkan ke gambar. Jika pada penelitian sebelumnya yang disisipka adalah gambar, maka pada penelitian sekarang ini yang disisipkan adalah pesan teks.
7. Zulhadi Hasibuan [11] tentang Perancangan Aplikasi Steganografi Dengan Metode Least Significant Bit (LSB) Untuk Data Terenkripsi Dari Algoritma Hill Cipher. Perbedaan dengan

penelitian sekarang terletak pada teknik enkripsi data. Pada penelitian sebelumnya menggunakan algoritma *Hill Chiper* sedangkan pada penelitian sekarnag menggunakan algoritma AES Rijndael 128 bit.

8. Fadhilah Hanifah [12] membahas tentang penerapan algoritma Rijndael dengan kunci 128 bit untuk mengamankan citra digital atau foto. Perbedaan dengan penelitian sekarang terletak pada warna citra yang digunakan. Penelitian sebelumnya hanya menggunakan *grayscale*, sedangkan penelitian sekarang dapat menggunakan RGB dan *grayscale* untuk citra / gambarnya.

2. METODE PENELITIAN

2.1. Metode Penelitian

Dalam penelitian ini metode yang digunakan adalah deskriptif analitik. Langkah yang dilakukan adalah mengumpulkan bahan penelitian, studi literatur, mempelajari algoritma steganografi dan kriptografi, melakukan perancangan dan implementasi sistem. Selain itu, dalam penelitian ini juga digunakan metode steganografi teknik LSB dan kriptografi *AES Rijndael* untuk menguji serta menemukan gambaran dari keamanan sistem yang telah dibuat. Secara umum, langkah-langkah implementasi yang dilakukan dalam penelitian ini adalah sebagai berikut:

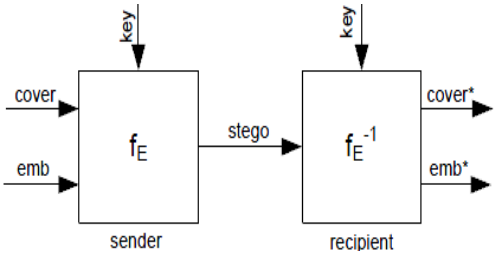
1. Melakukan pemilihan gambar bitmap 24 bit.
2. Menulis pesan/informasi.
3. Menyisipkan informasi ke gambar bitmap 24 bit dengan steganografi teknik LSB.
4. Melakukan enkripsi gambar bitmap 24 bit dengan teknik kriptografi *AES Rijndael*.
5. Mendekripsi gambar dan menampilkan informasi yang berada dalam gambar bitmap 24 bit.

2.2. Metode Analisis Data

Dalam mengimplementasikan keamanan penyampaian pesan informasi dengan menggunakan kombinasi steganografi LSB dan algoritma Rijndael, maka dalam penelitian ini akan dibangun sebuah perangkat lunak aplikasi untuk melakukan proses penyisipan informasi dalam gambar, enkripsi gambar dan dekripsi gambar sampai diperoleh kembali informasi yang berada dalam gambar. Pada saat melakukan proses enkripsi diperlukan sebuah kunci. Kunci tersebut akan digunakan kembali untuk mendekripsi gambar sehingga informasi yang berada dalam gambar akan dapat ditampilkan kembali. Data yang dapat mengalami proses enkripsi maupun dekripsi adalah gambar bitmap. Seluruh rangkaian enkripsi maupun dekripsi menggunakan blok data 128 bit.

2.2.1. Analisis Data Dengan Steganografi Least Significant Bit (LSB)

Steganografi (*steganography*) adalah suatu teknik yang digunakan untuk menyembunyikan data rahasia di dalam sebuah wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain. Gambar 1 di bawah ini menunjukkan alur sistem algoritma steganografi :



Gambar 1. Alur Sistem Algoritma Steganografi

Dalam steganografi dikenal teknik *Least Significant Bit* (LSB). Metode steganografi LSB (*Least Significant Bit*) dipergunakan untuk menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam *cover* dengan bit-bit data rahasia. Untuk menyembunyikan suatu gambar dalam LSB pada setiap *byte* dari gambar 24-bit, dapat disimpan 3 *byte* dalam setiap *pixel* [13]. *Least Significant Bit* terletak paling kanan dari barisan bit. Sebagai contoh *byte* 1101001**0**, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya [14]. Sebagai ilustrasi, terdapat segmen *pixel-pixel* citra/gambar awal sebagai berikut:

00110011 10100010 11100010 10101011 00100110
10010110 11001001 11111001 10001000 10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi (digaris bawahi):

00110011 10100011 11100011 10101010 00100110
10010111 11001000 11111001 10001001 10100011

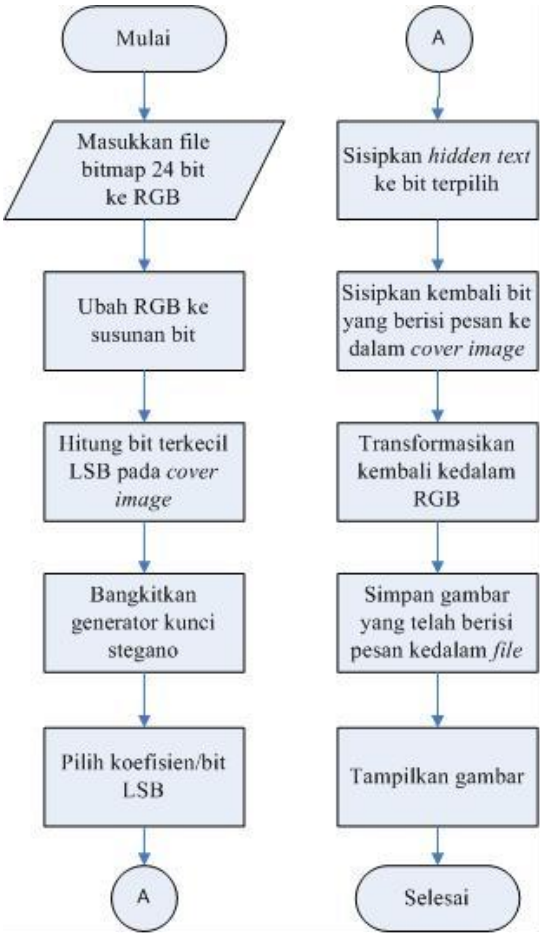
Dalam teknik LSB, terdapat dua proses utama yakni proses *embedding* dan proses *extraction.* Proses *embedding* adalah proses penyisipan pesan rahasia ke dalam suatu media, sedangkan proses *extraction* adalah proses pengambilan pesan rahasia dari suatu media. Algoritma yang dijalankan untuk proses *embedding* ini adalah sebagai berikut [15]:

1. Menentukan citra gambar yang akan menjadi media penyisipan *ciphertext* (*cover image*)
2. Memasukkan pesan informasi sebagai *ciphertext* untuk disisipkan
3. Menentukan *key file* yang akan digunakan sebagai *password* dalam proses *extract*
4. Penyisipan *file* ke dalam gambar
5. Memetakan menjadi citra baru

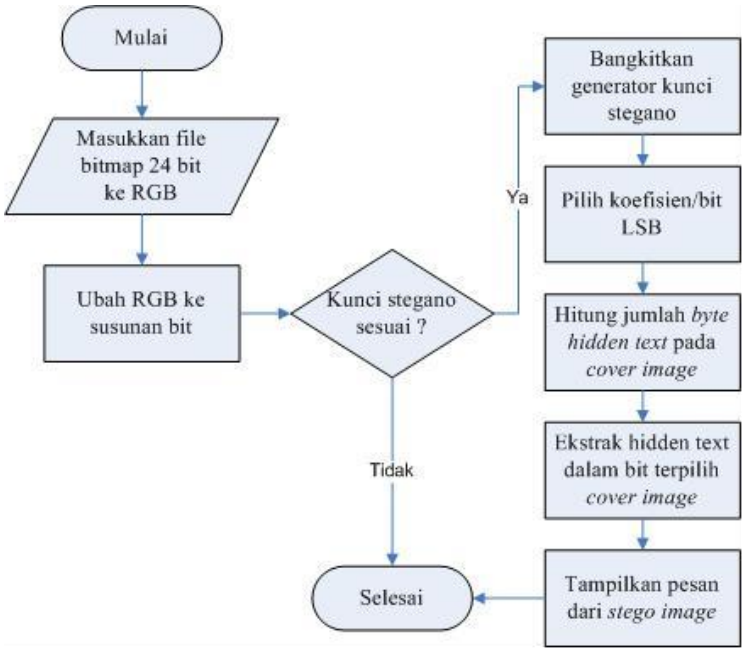
Adapun untuk proses *extract* (pembacaan pesan), algoritma yang dijalankan adalah sebagai berikut [15]:

1. Memilih file gambar atau *covert image* yang akan di-*extract*
2. Memasukan *key file*
3. Menampilkan hasil pembacaan pesan

Adapun alur proses *embedding* dan *extraction* diperlihatkan pada Gambar 2 dan Gambar 3 di bawah ini:



Gambar 2. Diagram alir proses *embedding*



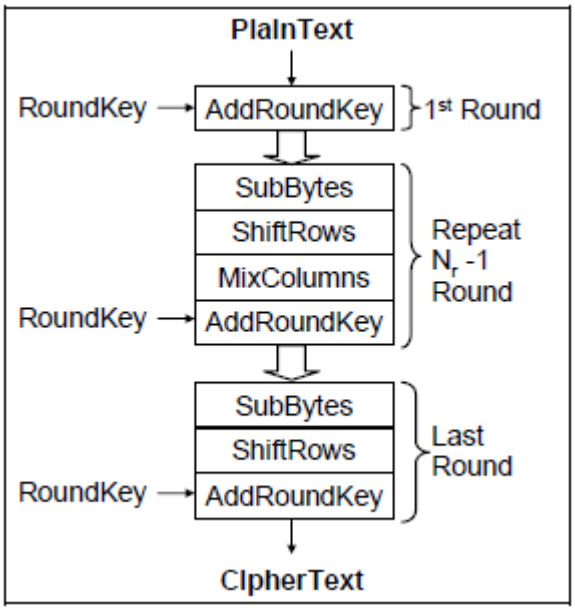
Gambar 3. Diagram alir proses *extraction*

2.2.2. Analisis Data Dengan Algoritma Kriptografi AES Rijndael

Kriptografi adalah ilmu dan seni yang digunakan untuk menjaga keamanan pesan (*Chriptography is the art an science of keeping message secure*)[16]. Definisi lain, kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi [17]. Dalam perkembangannya, ada 2 jenis algoritma kriptografi yakni algoritma enkripsi kunci simetris dan algoritma enkripsi kunci publik. *Rijndael* termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu [3].

Algoritma *Rijndael* bekerja menggunakan substitusi dan permutasi, serta sejumlah putaran (*cipher* berulang). Setiap putarannya menggunakan kunci internal yang berbeda (kunci setiap putaran disebut *round key*). *Rijndael* beroperasi dalam orientasi *byte*. [18]. Algoritma *Rijndael* mempunyai 3 (tiga) parameter: (1). *Plaintext* adalah array yang berukuran 16 *byte*, yang berisi data masukan. (2). *Ciphertext* adalah array yang berukuran 16 *byte*, yang berisi hasil enkripsi. (3). Kunci adalah array yang berukuran 16 *byte*, yang berisi kunci *cipher* (disebut juga *chiper key*).

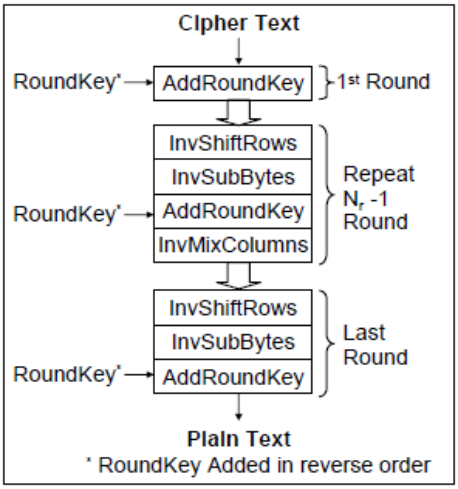
Proses enkripsi pada algoritma *AES* 128 *Rijndael* terdiri dari 4 jenis transformasi *byte* yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses, masukkan yang telah berbentuk *array state* akan mengalami transformasi *AddRoundKey ()*. Selanjutnya *array state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey* secara berulang sebanyak Nr. Proses ini dinamakan dengan *round function*. Gambar 4 di bawah ini memperlihatkan alur proses enkripsi *Rijndael*:



Gambar 4. Alur proses enkripsi *Rijndael* [19]

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers *cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*.

Gambar 5 di bawah ini menunjukkan alur proses dekripsi *Rijndael*:



Gambar 5. Alur proses dekripsi Rijndael [19]

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi [3]. Tabel 1 di bawah ini menunjukkan perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan.

Tabel 1. Jumlah proses berdasarkan bit blok dan kunci

Panjang Kunci (Nk) Dalam words	Ukuran Blok Data (Nb) dalam words	Jumlah Proses (Nr)
4	4	10
6	4	12
8	4	14

3. HASIL DAN PEMBAHASAN

Uji coba terhadap perangkat lunak yang dihasilkan dalam penelitian ini bertujuan untuk mengetahui apakah perangkat lunak aplikasi sudah berjalan sesuai dengan rancangan/desain sistem yang dibangun baik untuk proses penyisipan pesan dalam gambar bitmap 24 bit maupun proses enkripsi gambar bitmap dengan *AES Rijndael.* Pada bagian ini dijelaskan tentang desain sistem proses penyisipan pesan dalam gambar, proses enkripsi gambar dan dekripsi gambar sampai dengan menampilkan kembali pesan stego yang dilakukan dalam penelitian ini. Desain sistem ini meliputi rancangan proses penyisipan pesan dalam gambar, enkripsi gambar, dekripsi gambar, proses baca pesan dan implementasi antar muka dari keseluruhan proses tersebut. Berikut ini penjelasan dari proses yang dilakukan:

3.1. Rancangan Proses Penyisipan Pesan

Gambar 5 dibawah ini memperlihatkan jalannya proses penyisipan pesan ke dalam gambar bmp 24 bit yang dilakukan dalam penelitian ini:

Gambar 6. Alur proses penyisipan pesan ke gambar bmp 24 bit

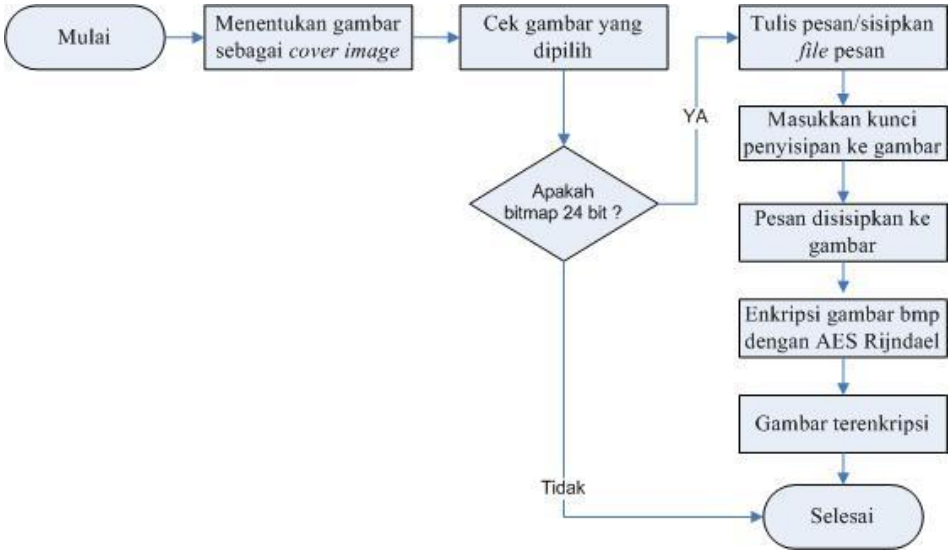
3.2. Implementasi Antar Muka Penyisipan Pesan

Dari rancangan seperti pada Gambar 6 di atas, maka selanjutnya rancangan tersebut diimplementasikan ke aplikasi. Gambar 7 di bawah ini memperlihatkan tampilan antar muka untuk proses penyisipan pesan ke dalam gambar bmp 24 bit:

Gambar 7. Antar muka proses penyisipan pesan ke gambar bmp 24 bit

3.3. Rancangan Proses Enkripsi Gambar dengan Rijndael

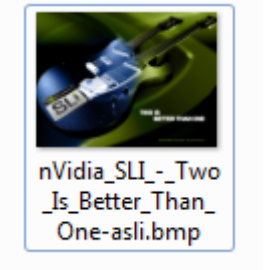
Dalam penelitian ini, gambar *stego* (gambar yang berisi pesan) akan dienkripsi dengan *AES Rijndael* 128 bit. Pada saat proses enkripsi, sistem akan meminta kunci enkripsi. Rancangan jalannya proses ini diperlihatkan pada Gambar 8.



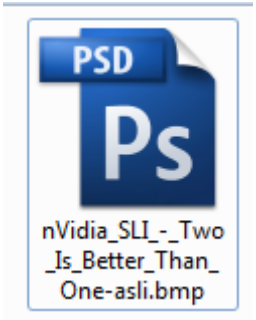
Gambar 8. Desain proses enkripsi gambar dengan Rijndael

3.4. Implementasi Enkripsi AES Rijndael

Hasil dari rancangan sistem proses enkripsi gambar bitmap 24 bit dengan *AES Rijndael* adalah pada waktu pesan berhasil disisipkan dalam gambar, maka gambar *stego* (gambar yang berisi pesan) akan langsung terenkripsi. Gambar 9 dan Gambar 10 di bawah ini memperlihatkan tampilan awal saat gambar belum dienkripsi dan setelah gambar dienkripsi:



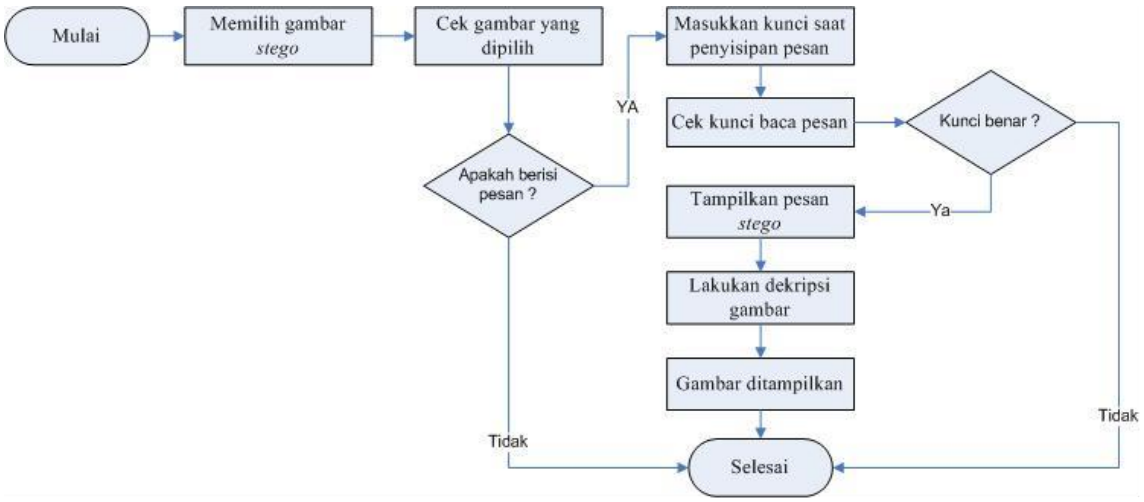
Gambar 9. Tampilan asli gambar



Gambar 10. Tampilan gambar setelah enkripsi

3.5. Rancangan Proses Baca Pesan dan Dekripsi Gambar

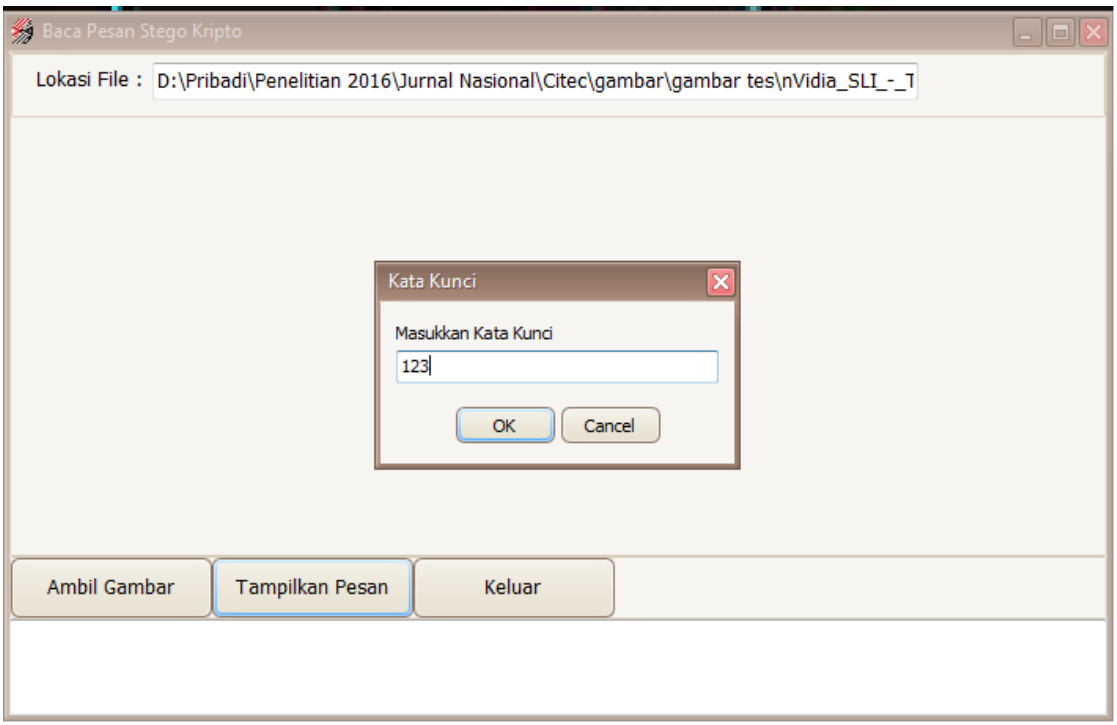
Pada tahap ini, akan dilakukan proses dekripsi gambar. Proses dekripsi dilakukan dengan memasukkan kunci enkripsi terlebih dahulu. Jika kunci benar, maka gambar dapat terdekripsi dan informasi yang berada dalam gambar dapat ditampilkan kembali. Rancangan sistem dekripsi gambar dan *extraction mesaage* (proses baca pesan) diperlihatkan pada Gambar 11 dibawah ini:



Gambar 11. Desain proses baca pesan dan dekripsi gambar

3.6. Rancangan proses baca pesan dan dekripsi gambar

Hasil dari rancangan tersebut diimplementasikan kedalam sebuah antar muka baca pesan seperti terlihat pada Gambar 12 dan Gambar 13 di bawah ini. Pada saat pesan berhasil terbaca, maka secara otomatis gambar bmp yang semula terenkripsi menjadi terbaca/terlihat kembali.



Gambar 12. Antar muka proses baca pesan

Gambar 13. Hasil proses baca pesan

4. KESIMPULAN

Dari hasil pembahasan yang meliputi perancangan desain sistem dan uji coba implementasi aplikasi, maka dapat ambil kesimpulan sebagai berikut:

1. Penerapan algoritma steganografi *Least Significant Bit* dilakukan dengan menggantikan *bit-bit* pesan rahasia pada *bit* terakhir tiap komponen warna piksel citra. Dalam metode ini kualitas citra tidak berubah setelah mengalami proses penyisipan pesan, pesan tidak dapat diketahui secara indrawi akan tetapi pesan dapat diekstrak kembali tanpa adanya kerusakan.
2. Citra bitmap 24 bit yang dienkripsi dengan *AES Rijndael* mengalami 4 proses transformasi yakni: *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Kecepatan proses enkripsi maupun dekripsi tergantung dari panjangnya *key* atau kunci yang digunakan. Pada metode Rijndael (AES128), tipe file diperlakukan sama sebagai arsip biner. Waktu proses enkripsi lebih lama dari proses dekripsi, hal ini dikarenakan pada proses dekripsi pengecekan panjang maksimum kunci (*Key Max Size*) ditiadakan.
3. Kombinasi penerapan algoritma steganografi LSB dan kriptografi AES 128 Rijndael dapat diimplementasikan dalam sebuah aplikasi baik berbasis *desktop* maupun *web*. Penerapan kombinasi ini bertujuan agar pesan benar-benar terlindungi dengan aman.

5. SARAN

Adapun saran-saran yang dapat penulis berikan untuk pengembangan dan perbaikan sistem ini bagi penelitian selanjutnya adalah sebagai berikut:

1. Hasil dari penelitian ini dapat dikembangkan dengan menerapkan beberapa metode steganalisis yang lain sehingga pendeteksian keberadaan pesan tersembunyi pada sebuah gambar bisa lebih akurat.
2. Media yang digunakan untuk menampung pesan dalam penelitian ini masih dalam bentuk gambar bitmap 24 bit, sehingga untuk pengembangan ke depan dapat digunakan media

penampung pesan yang lain seperti gambar dengan format selain bmp, music, video dan lain sebagainya.

3. Aplikasi hasil penelitian ini dapat dikembangkan dengan mengganti metode kriptografi *AES Rijndael* 128 bit dengan metode yang lain agar semakin menguatkan hasil analisis keamanan data.

6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada keluarga tercinta yang telah dengan sabar mendampingi penulis selama proses penulisan laporan penelitian ini. Penulis juga menyampaikan terima kasih kepada Tim LP2M STMIKKA Kediri yang telah memberikan banyak dukungan terhadap setiap kegiatan penulisan laporan penelitian yang penulis lakukan. Dan tidak lupa pula terima kasih penulis sampaikan kepada pengelola dan editor jurnal CITEC yang telah memberikan kesempatan kepada penulis untuk berkontribusi dalam jurnal CITEC.

DAFTAR PUSTAKA

[1] Tumanggor, S. F., 2009, Studi Enkripsi Dan Dekripsi File Dengan Menggunakan Algoritma Twofish, *Skripsi*, Fakultas Matematika Dan Ilmu Pengetahuan Alam, Program Studi Sarjana Matematika, Universitas Sumatera Utara, Medan.

[2] Firmansyah, R., 2011, Implementasi Kriptografi dan Steganografi Pada Media Gambar Dengan Menggunakan Metode DES dan Region Embed Data Density, *Tesis*, Program Pasca Sarjana Teknik Informatika, Institut Teknologi Sepuluh Nopember, Surabaya.

[3] Surian, D., 2006, Algoritma Kriptografi AES Rijndael, *Jurnal Teknik Elektro*, No. 2, Vol. 8, Hal 97 – 101.

[4] Alatas, P., 2009, Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital, *Skripsi*, Jurusan Sistem Informasi, Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Gunadarma, Jakarta.

[5] Rakhmat, B., Fairuzabadi, M., 2010, Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan RC4, *Jurnal Dinamika Informatika*, No. 2, Vol. 5, Hal 1-17.

[6] Poetro, B. S. W., Sugiharto, A., Endah, S. N., 2010, Kriptografi Citra Digital Dengan Algoritma Rijndael Dan Transformasi Wavelet Diskrit Haar, *Seminar Nasional Ilmu Komputer Universitas Diponegoro*, Semarang, 7 Agustus 2010.

[7] Wijayanto, B., Wardoyo, R., 2011, An Implementation of Catmap-Rijndael (AES) Algorithm For Image Security (Case Study on A Software For Making Students Card At Universitas Jenderal Soedirman), *IJCCS*, Vol 5, No 1, Hal 1-8.

[8] Sari, S. P., Winarno, Sudirman, D. Z., 2012, Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard, ULTIMATICS, Vol IV, No 1

[9] Bendi., R. K. J., Aditya, S. B. P., 2012, Implementasi Algoritma Rijndael Untuk Enkripsi dan Dekripsi Pada Citra Digital, *Seminar Nasional Aplikasi Teknologi Informasi 2012 (SNATI 2012)*, Yogyakarta, 15-16 Juni 2012.

[10] Niswati, Z., 2012, Steganografi Berbasis Least Significant Bit (LSB) Untuk Menyisipkan Gambar Ke Dalam Citra Gambar, *Faktor Exacta*, No. 2, Vol. 5, Hal 181-191.

[11] Hasibuan, Z., 2014, Perancangan Aplikasi Steganografi Dengan Metode Least Significant Bit (LSB) Untuk Data Terenkripsi Dari Algoritma Hill Cipher, *Pelita Informatika Budi Darma*, No. 2, Vol. 6, Hal 150-154.

[12] Hanifah, F., 2012, Aplikasi Algoritma Rijndael Dalam Pengamanan Citra Digital, *Skripsi*, Fakultas Matematika Dan Ilmu Pengetahuan Alam, Program Studi Sarjana Matematika, Universitas Indonesia, Jakarta.

[13] Cahyadi, T., 2012, Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG, *TRANSIENT*, Vol 1, No 4, Hal 282.

[14] Lubis, A. R., Lidya, M. S., Budiman, A., 2012, Perancangan Perangkat Lunak Steganografi Audio MP3 Menggunakan Metode Least Significant Bit (LSB) Dengan Visual Basic 6.0, *Jurnal Dunia Teknologi Informasi*, No. 1, Vol. 1, Hal 63-68.

[15] Husein, M., 2014, Implementasi Caesar Cipher Untuk Penyembunyian Pesan Teks Rahasia Pada Citra Dengan Menggunakan Metode Least Significant Bit., *Pelita Informatika Budi Darma*, No. 2, Vol. VII, Hal 116-122.

[16] Schneier, B., 1996, *Applied Chriptography, protocols, Algorithms and Source Code in C*, John Wiley & Sons, Inc, New York.

[17] Kromodimoeljo, S., 2009, *Teori & Aplikasi Kriptografi*, SPK IT Consulting, Jakarta. ok

[18] Silva, L. D., Dessyanto B.P., Heriyanto, 2013, Aplikasi Enkripsi Dan Dekripsi File Dengan Menggunakan AES (Advanced Encryption Standard) Algoritma Rijndael Pada Sistem Operasi Android, *Telematika*, No. 1, Vol. 10, Hal 33 – 42.

[19] Stalling, W., 2005, *Cryptography and Network Security Priciples and Practices, Fourth Edition*, Prentice Hall, New Jersey.