Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES

Syaiful Anwar
Magister Ilmu Komputer, Universitas Budi Luhur
Jl. Ciledug Raya, Pertukangan Utara, Jakarta Selatan, 12260
sa060586@gmail.com

Abstract - Security and confidentiality are two important aspects of data communications. In maintaining the security and confidentiality of an important message to be delivered, the first message is encrypted and hidden into a medium. Media used in this study is a digital image with a color depth of 24 bits. This research aims to develop a system that can be used to enhance the security of data in the form of important and confidential messages. Cryptographic algorithms used for encryption was aes algorithm and steganography by modifying the method of least significant bit (LSB) which was used to save the message in the image. Modified LSB used in this research was by inserting bits of the ciphertext into a diagonal matrix of pixel color components in the image. The system was developed using the programming language c #. Tests conducted in this study were to look at aspects of imperceptibility and recovery of the method modified LSB. This study confirms that the combination of the aes algorithm and modified LSB can be used to improve data security.
Keywords: Cryptography, Steganography, AES, modified LSB, imperceptibility

***Abstrak* - Keamanan dan kerahasiaan merupakan dua aspek penting dalam komunikasi data. Dalam menjaga keamanan dan kerahasiaan suatu pesan penting yang akan dikirimkan, pesan terlebih dahulu dienkripsi dan disembunyikan ke dalam suatu media. Media yang digunakan dalam penelitian ini adalah citra digital dengan kedalaman warna 24 bit. Penelitian ini bertujuan untuk membangun suatu sistem yang dapat digunakan dalam meningkatkan keamanan data yang berupa pesan-pesan penting dan rahasia. Algoritma kriptografi yang digunakan untuk melakukan enkripsi adalah algoritma aes dan steganografi dengan memodifikasi metode least significant bit (LSB) digunakan untuk menyimpan pesan ke dalam citra. Modified LSB yang digunakan dalam penelitian ini yaitu dengan menyisipkan bit-bit cipherteks ke dalam diagonal matriks pixel komponen warna pada citra. Sistem ini dikembangkan dengan menggunakan bahasa pemrograman c #. Pengujian yang dilakukan pada penelitian ini yaitu dengan melihat aspek imperceptibility dan aspek recovery pada metode modified LSB. Penelitian ini menegaskan bahwa kombinasi dari algoritma aes dan modified LSB dapat digunakan dalam meningkatkan keamanan data.**
***Kata Kunci:* kriptografi, steganografi, AES, modified LSB, imperceptibility**

I. PENDAHULUAN

Perkembangan teknologi informasi semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media. Komunikasi yang melibatkan pengiriman dan penerimaan pesan dengan memanfaatkan kemajuan teknologi informasi rentan terhadap pelaku kejahatan komputer yang memanfatkan celah keamanan untuk mendeteksi dan memanipulasi pesan.

Keamanan dan kerahasiaan menjadi aspek yang sangat penting bagi pengguna teknologi informasi. Untuk menghindari pesan yang dikirimkan jatuh pada pihak-pihak yang tidak berkepentingan dan terjadi penyalahgunaan terhadap pesan, maka dilakukan enkripsi terhadap pesan asli dan penyisipan pesan ke dalam suatu media dengan menerapkan ilmu kriptografi dan steganografi.

Untuk meningkatkan keamanan digunakan kombinasi antara kriptografi dan steganografi, dimana pesan rahasia dienkripsi terlebih dahulu, kemudian ciphertext disembunyikan di dalam media lain sehingga pihak-pihak yang tidak berkepentingan tidak menyadari keberadaan pesan.

Berdasarkan latar belakang masalah, proses pertukaran pesan memerlukan jaminan keamanan dan kerahasiaan. Diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik pada pesan rahasia, dan menjaga kerahasiaan pesandengan menyembunyikannya ke dalam media lain (gambar) agar keberadaan pesan rahasia tidak diketahui.

Adapun tujuan yang ingin dicapai adalah merancang sebuah aplikasi yang dapat mengenkripsi dan mendekripsi pesan teks menggunakan algoritma kriptografi aes dan juga merancang sebuah aplikasi yang dapat menyisipkan dan mengekstrak cipherteks berupa blok-blok integer dalam media berupa citra digital menggunakan algoritma LSB.

II. LANDASAN TEORI

Tinjauan Studi

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya

Khalil Challita dan Hikmat Farhat [1] melakukan penelitian mengenai *Combining Steganografi And Cryptography: New Directions Dengan Kombinasi Algoritma MCO (Multiple Cover Object).* Membuat kesepakatan antara pengirim dan penerima pesan dalam informasi password yang digunakan sebagai kata kunci.

Kavita Kadam, Ashwini Koshti dan Priya Dunghav [2] melakukan penelitian mengenai steganography using least signicant bit algorithm dengan kombinasi algoritma dct (discrete cosine trabsformations). Menyisipkan pesan rahasia edalam gambar yang dilindungi dengan password pribadi yang terenkripsi.

M. Anggrie Andriawanm, Solikin dan Setia Juli Irzal Ismail [3] melakukan penelitian mengenai implementasi steganografi pada citra digital file gambar bitmap (bmp) menggunakan java dengan penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit. Menyembunyikan pesan rahasia dengan metode LSB untuk mengeksploitasi keterbatasan sistem penglihatan manusia.

Steganografi

Steganografi berasal dari bahasa yunani yang terdiri dari dua kata, yaitu *steganos* dan *graphia*. Steganos berarti tersembunyi dan graphia artinya tulisan. Dengan demikian, steganografi adalah ilmu atau seni untuk menyembunyikan pesan [4]. Pesan tersebut disembunyikan dengan tujuan agar tidak diketahui oleh orang lain. Yang mengetahuinya adalah dirinya sendiri dan orang lain yang dikehendaki. Steganografi membahas cara untuk menyamarkan dan menyembunyikan pesan.

Teknik steganografi terus berkembang sejalan dengan perkembangan zaman dan teknologi yang ada. Di antara contohnya adalah penggunaan *watermarking* (tanda air). Steganografi di masa sekarang ini telah melibatkan pula teknologi komputer. Dalam teknologi komputer pengamanan data dengan steganografi dapat dilakukan dengan dua cara [5]. Cara pertama melibatkan satu file saja sebagai file media atau file carrier. Dan cara kedua dengan cara melibatkan dua file, yaitu file yang memuat data rahasia yang akan disembunyikan dan file lain adalah file media atau carrier.

Ada beberapa kriteria yang harus diperhatikan dalam steganografi[6], yaitu :

Imperceptibility. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra covertext-nya. Jika covertext berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio stegotext-nya.

Fidelity. Mutu stegomedium tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra covertext-nya. Jika covertext berupa audio, maka audio stegotext tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.

Recovery. Pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu pesan rahasia di dalam stegotext harus dapat diambil kembali untuk digunakan lebih lanjut.

Metode LSB *(Least Significant Bit)*

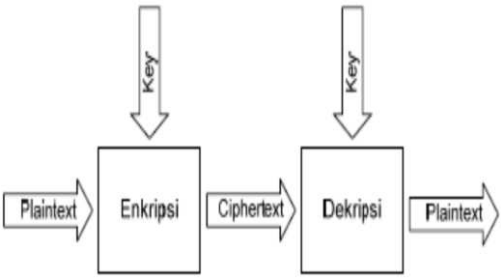
Metode LSB *(Least Significant Bit)* merupakan salah satu teknik substitusi pada steganografi. Dimana tiap bit terendah pada byte-byte media citra akan digantikan dengan bit-bit pesan yang akan disisipkan. Pada file citra 24 bit setiap pixel pada citra terdiri dari susunan tiga warna, yaitu merah, hijau dan biru (rgb) yang masingmasing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Informasi dari warna biru berada pada bit 1sampai bit 8, dan informasi warna hijau berada pada bit 9 sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24.

Metode LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya, sehingga perubahan yang terjadi tidak begitu berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan kecil yang terjadi tersebut.

Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa yunani *cryptós (secret)* dan *gráphein (writing).* Jadi, kriptografi berarti *secret writing* (tulisan rahasia). Kriptografi merupakan ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi adalah sebuah cara yang efektif dalam mengamankan informasi-informasi penting baik yang tersimpan dalam media penyimpanan maupun yang ditransmisikan melalui jaringan komunikasi[7]. Orang yang melakukan penyandian ini disebut kriptografer, sedangkan orang yang mendalami ilmu dan seni dalam membuka atau memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut kriptanalis.

Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia *(ciphertext). Ciphertext* inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut:



Gambar 1. Proses enkripsi dan dekripsi

Algoritma AES *(Advanced Encryption Standard)*

Sejak tahun 1976, *data encryption standard* (DES) dipilih sebagai standar kriptografi yang dipakai pada pemerintahan Amerika Serikat. Namun pada tahun 1990, panjang kunci DES dianggap terlalu pendek, dan pada tahun 1998 DES berhasil dipecahkan dalam waktu 96 hari, kemudian di tahun 1999 dapat dipecahkan dalam waktu 22 hari.

Karena alasan tersebut maka kemudian diadakan kompetisi oleh NIST (*National Institute of Standard and Technology*) untuk mencari pengganti des. Nist mengundang peserta dari seluruh dunia untuk berpartisipasi dengan mengajukan algoritma baru untuk menggantikan des [7].

Citra Digital

Semua citra digital yang ditampilkan di layar komputer adalah sederetan atau sekumpulan pixel (*picture element)*. Citra tersebut dikatakan sebagai citra digital karena bentuk representasinya yang berupa bilangan. Oleh komputer akan dikenal dalam urutan '0' dan '1'.

Ada beberapa format citra digital, antara lain: bmp, png, jpg, gif, pxc, dan sebagainya. Masing-masing format mempunyai perbedaan satu dengan yang lain terutama pada header file-nya. Namun ada beberapa yang memiliki kesamaan yaitu penggunaan *pallete* untuk penentuan warna pixel.

Representasi citra digital dalam sebuah file dapat dianalogikan seperti halnya ketika kita ingin melukis, maka kita harus mempunyai palet dan kanvas. Di mana palet adalah kumpulan warna yang dapat membentuk citra, seperti palet warna yang berisi berbagai warna cat. Lalu setiap warna yang berbeda di dalam palet tersebut diberi nomor. Kemudian kita dapat melukiskan warna-warna tersebut di atas sebuah kanvas. Kanvas tersebut berupa matriks yang setiap elemen matriksnya dapat diisi dengan sebuah warna yang berasal dari palet warna. Kumpulan angka (mewakili warna) dalam bentuk matriks inilah yang disebut dengan citra. Sementara informasi mengenai palet (korespondensi antara warna dengan angka) disimpan di dalam komputer melalui aplikasi untuk membuka citra seperti, photoshop dan paint

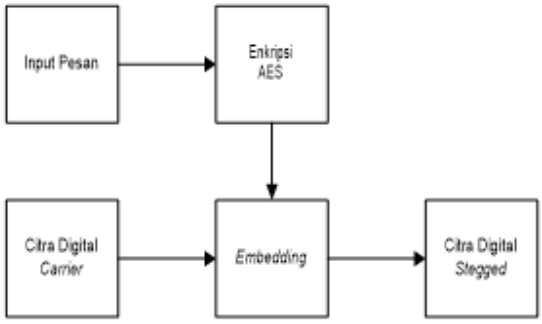
III. ANALISIS DAN PERANCANGAN

Analisis sistem

Secara umum proses steganografi pada sistem ini ada dua, yaitu proses penyisipan pesan (*embedding*) dan proses pengungkapan pesan (ekstraksi).

Proses Embedding Pesan

Ada dua tahap yang dilakukan dalam proses embedding, yaitu enkripsi aes yang mentransformasikan pesan asli (plaintext) menjadi teks acak (ciphertext) , selanjutnya dilakukan penyisipan (embedding) dalam citra digital pembawa (carrier). Ilustrasi dari proses embedding dapat dilihat pada Gambar 2.



Gambar 2. Proses embedding

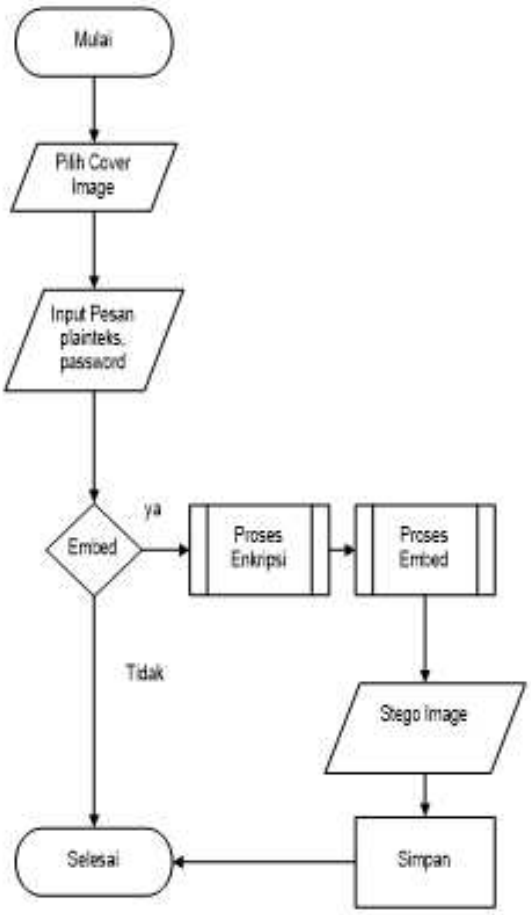
Proses Ekstraksi Pesan

Dalam proses ekstraksi ada dua tahap yang dilakukan yaitu seperti pada Gambar 3.

Gambar 3. Proses ekstraksi

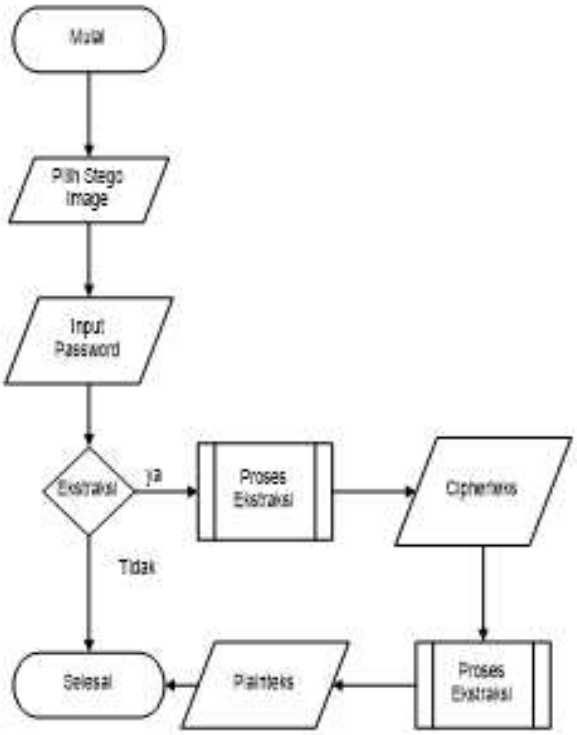
Perancangan System

Untuk menyisipkan *cipherteks* ke dalam *cover image* penyembunyian pesan dilakukan dengan menggunakan metode *modified* LSB yang mengganti diagonal-diagonal byte komponen warna merah pada citra. Proses penyembunyian pesan tersebut dapat digambarkan dengan flowchart di Gambar 4.



Gambar 4. Flowchart proses embedding

Ekstraksi dilakukan untuk memisahkan cipherteks yang tersembunyi dari *stego image*. Flowchart untuk proses ekstraksi diperlihatkan pada Gambar 5.



Gambar 5. Flowchart proses ektraksi

Implementasi Sistem

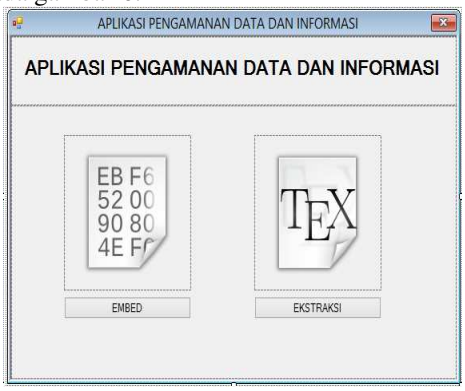
Implementasi Antarmuka Sistem

Dalam proses ini, penulis menggunakan microsoft visual studio 2010 sebagai alat pengembangan untuk menerapkan kriptografi dan steganografi dengan menggunakan c # sebagai bahasa pemrograman. Proses ini akan menerapkan coding fungsi dan mengintegrasikan fungsi ke dalam GUI (*graphical user interface).*

Implementasi dari hasil tahapan analisis dan perancangan dapat dilihat dari tampilan antarmuka sistem sebagai berikut:

1. Tampilan Halaman Menu Utama

Halaman menu utama merupakan halaman awal yang akan ditampilkan saat sistem dijalankan. Tampilan halaman menu utama ditunjukkan pada gambar 6.



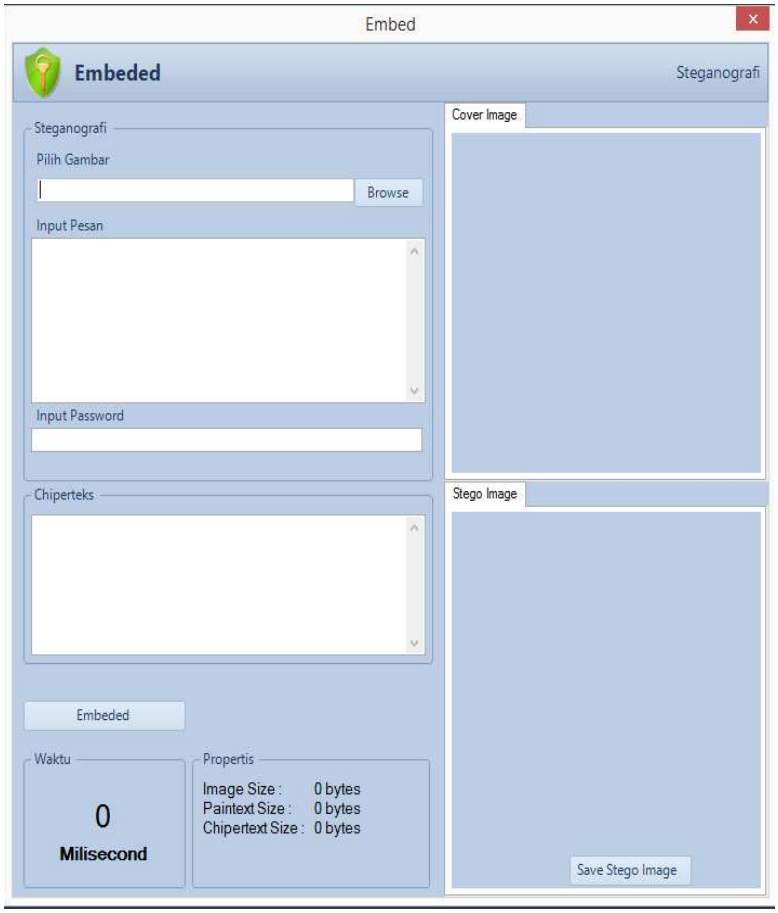
Gambar 6. Halaman menu utama

2. Halaman *Embe*d

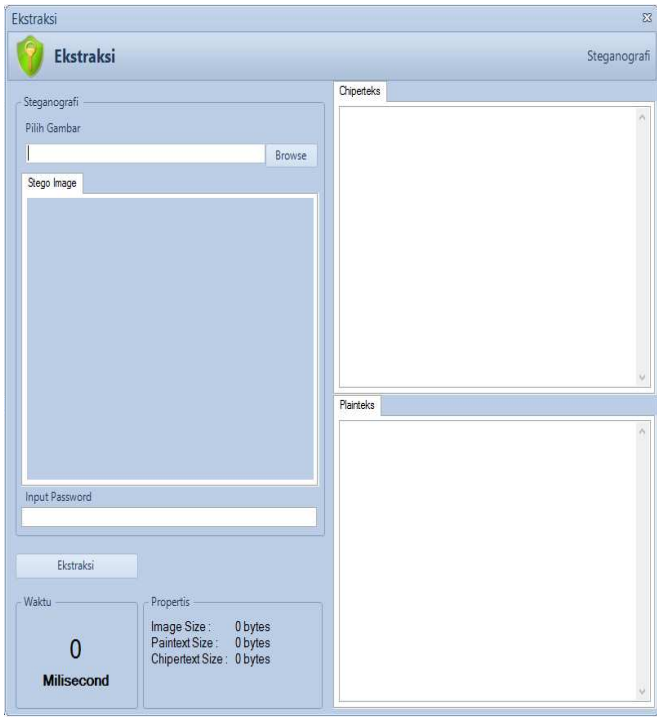
Halaman e*mbe*d merupakan halaman untuk proses enkripsi pesan menjasi cipherteks dan penyisipan bit – bit cipherteks dan penyisipan bit bit cipherteks kedalam cover image, proses tersebut terjadi pada pihak pengirim pesan. Pada halaman embed ini, user atau pengirim pesan akan menginputkan pesan yang akan dikirimkan kepada penerima pesan dan juga memilih cover image. Gambar 6 menampilkan halaman embed.

3. Tampilan Halaman Ektraksi

Halaman ekstraksi merupakan halaman tempat berlangsungnya proses ekstraksi pesan dari stego image dan dekripsi cipherteks ke plainteks agar dapat dibaca oleh penerima pesan. Untuk dapat mendekripsikan cipherteks, penerima pesan membutuhkan password yang sama, yang sebelumnya digunakan untuk melakukan enkripsi pesan oleh pengirim pesan. Gambar 8 adalah tampilan halaman ekstraksi.



Gambar 7. Halaman embed



Gambar 8. Halaman ekstraksi

Pengujian sistem

1. Aspek I*mperceptibility*

Seperti yang telah dijelaskan pada bab sebelumnya, aspek *imperceptibility* merupakan salah satu aspek/ kriteria yang harus diperhatikan dalam penyembunyian pesan pada proses steganografi. Aspek imperceptibility menekankan bahwa algoritma steganografi yang baik membuat keberadaan pesan rahasia pada stego object tidak dapat dipersepsi oleh inderawi. Dalam penelitian ini, cover object yang digunakan adalah berkas digital, sehingga diharapkan pentisipan pesan dalam cover image akan menghasilkan stego object yang sukar dibedakan oleh mata dengan cover object nya. Penentuan apakah keberadaan pesan rahasia dapat dipersepsikan atau tidak ditentukan dari penglihatan manusia atau indra mata.

Pengujian diberikan terhadap beberapa cover image yang telah disisipi pesan terlebih dahulu untuk membuktikan apakah algoritma modified LSB telah memenuhi aspek imperceptibility atau tidak. Dari penyisipan pesan tersebut akan dihasilkan stego image. Dimana aspek imperceptibility akan terlihat dari perbandingan antara kedua berkas citra digital tersebut tidak dapat dilihat secara kasat mata, maka dapat ditarik kesimpulan bahwa algoritma modified LSB yang digunakan untuk menyembunyikan pesan telah memenuhi aspek imperceptibility.

Pengujian untuk kriteria yang telah ditentukan sebelumnya ditampilkan padaGambar 9.

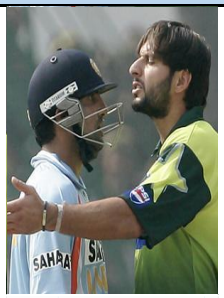
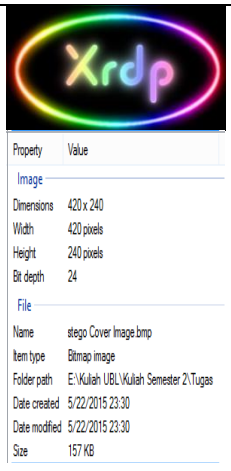
Gambar 9. Hasil proses enkripsi dan embed.

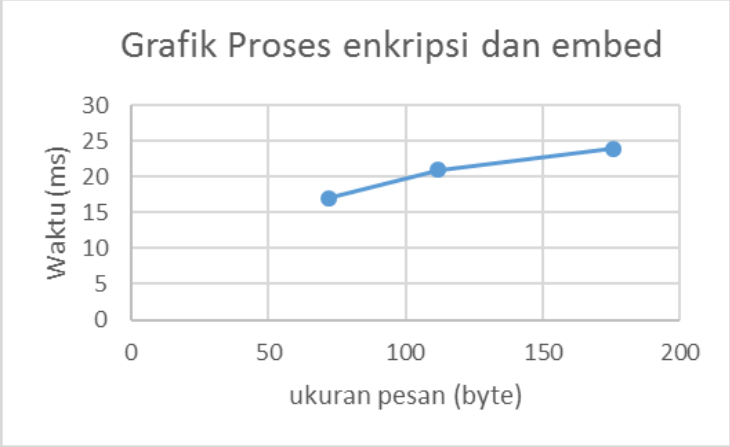
Beberapa pengujian lain untuk masukan yang berbeda beda akan terlihat pada Tabel 1.

Dari beberapa pengujian yang telah dilakukan terlihat bahwa cover image dengan stego image telah berisi cipherteks secara kasat mata terlihat sama dan tidak terlihat perbedaan sedikitpun, tidak hanya itu ukuran citra dan juga dimensi citra sebelum dan sesudah disisipkan pesan tidak mengalami perubahan. Hal ini disebabkan perubahan byte-byte diagonal komponen warna pada citra hanya akan menghasilkan perubahan 1 byte lebih tinggi atau lebih rendah, pergantian tersebut tidak akan menampilkan perubahan yang berarti pada stego image. Dengan demikian metode modified LSB telah memenuhi aspek imperceptibility sebagai salah satu kriteria algoritma steganografi yang baik.

Dapat dilihat pula dari hasil pengujian berdasarkan waktu lama proses, maka semakin besar ukuran pesan yang akan disisipkan gambar maka semakin lama proses enkripsi dan embed. Bisa dilihat dalam Gambar 10.

TABEL 1
HASIL PENGUJIAN PADA BEBERAPA COVER IMAGE

No	Plainteks / size	Kunci	Cipherteks/size	Cover image	Stego image	Waktu (ms)
1.	Gambar ini telah disisipi pesan yang harus di jaga kerahasiaan. (62 bytes)	Qwerty!@ #$%	Eaaaak+arhpa7nv6h8fjzptlyscggroyxamwqgbg9v5kzneczour84r8u8jx2ozkoixi89hbpc/tat4jrkt0v0a/d3gzfkd/8isqf7wnqy4+pbk+ (112 bytes)			21
2.	Abcdefghijklmnopqrstuvwxyz (26 bytes)	1234567890	Eaaaaly2bwm4a8j58vz/ds6ev8tqbiufpgc4y2wkhrvabk3wo9tvywb4qhndk8+b1khemq== (72 bytes)			17
3.	Setelah aplikasi ini melewati proses tahap coding, maka tahap selanjutnya adalah tahap pengujian. (98 bytes)	Asdfghjkl	Eaaaajuldk9zyqxmm6i2ihlg37msxyffooj19taar9cenuwugmmyqqzu67xecvzw4ewsaz5ptj1jatzyp9mcgzw0dqvw8ce7kehci9wdxpaeda4ldc1ko959i2vbfp2z0bvadiuu96zkbrrnb3vuoofe2pr4dagca34ytmjbgh5dy21g (176 bytes)			24



Gambar 10. Grafik Proses Enkripsi Dan Embed

2. Aspek *Recovery*

Aspek *recovery* menyatakan bahwa pesan yang disembunyikan dalam stego object harus dapat diungkap kembali. Untuk mengatur keberhasilan aspek recovery dalam algoritma modified LSB, dapat dilihat dari kesesuaian cipherteks yang berhasil diektraksi dari stego image dengan cipherteks hasil dari proses enkripsi.

Hasil pengujian terhadap aspek recovery untuk contoh masukan stego image hasil embedding pada pengujian sebelumnya ditunjukan Tabel 2.

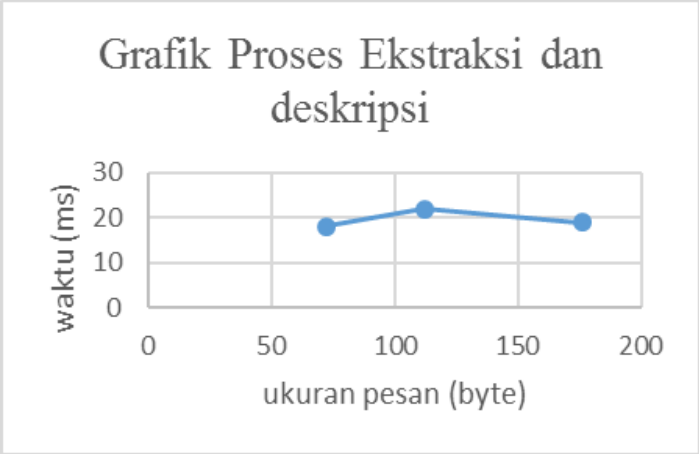
TABEL 2
HASIL PENGUJIAN PADA BEBERAPA STEGO IMAGE

No	Stego image	Cipherteks Sebelum	Cipherteks Sesudah	Password	Plainteks Hasil	Waktu (ms)
1.		Eaaaak+arhpa7nv6h8fjzptlyscggroyxamwqgbg9v5kzneczour84r8u8jx2ozkoixi89hbpc/tat4jrkt0v0a/d3gzfkd/8isqf7wnqy4+pb+ (112 bytes)	Eaaaak+arhpa7nv6h8fjzptlyscggroyxamwqgbg9v5kzneczour84r8u8jx2ozkoixi89hbpc/tat4jrkt0v0a/d3gzfkd/8isqf7wnqy4+pbk+ (112 bytes)	Qwerty!@#$%	Gambar ini telah disisipi pesan yang harus di jaga kerahasian. (62 bytes)	22
2.		Eaaaaly2bwm4a8j58vz/ds6ev8tqbiufpgc4y2wkhrvabk3wo9tvywb4qhndk8+b1khemq== (72 bytes)	Eaaaaly2bwm4a8j58vz/ds6ev8tqbiufpgc4y2wkhrvabk3wo9tvywb4qhndk8+b1khemq== (72 bytes)	1234567890	Abcdefghijklmnopqrstuvwxyz (26 bytes)	18
3.		Eaaaajuldk9zyqxmm6i2ihlg37msxyffooj19taar9cenuwugmmyqqzu67xecvzw4ewsaz5ptj1jatzyp9mcgzw0dqvw8ce7kehci9wdxpaeda4ldc1ko959i2vbfp2z0bvadiuu96zkbrrnb3vuoofe2pr4dagca34ytmjbgh5dy21g (176 bytes)	Eaaaajuldk9zyqxmm6i2ihlg37msxyffooj19taar9cenuwugmmyqqzu67xecvzw4ewsaz5ptj1jatzyp9mcgzw0dqvw8ce7kehci9wdxpaeda4ldc1ko959i2vbfp2z0bvadiuu96zkbrrnb3vuoofe2pr4dagca34ytmjbgh5dy21g (176 bytes)	Asdfghjkl	Setelah aplikasi ini melewati proses tahap coding, maka tahap selanjutnya adalah tahap pengujian. (98 bytes)	19

Dari beberapa pengujian yang dilakukan dapat dilihat bahwa hasil ekstraksi dari stego image menghasilkan cipheteks yang sesuai dengan cipherteks hasil enkripsi, dan untuk proses dengan kunci yang tepat akan

menghasilkan plainteks sama seperti yang diinputkan semula. Dengan demikian, algoritma modified LSB yang digunakan dalam penelitian ini telah memenuhi aspek recovery.

Dapat dilihat pula dari hasil pengujian berdasarkan waktu lama proses, maka semakin lama proses ektraksi dan dekripsi maka semakin besar ukuran pesan yang disisipkan. Bisa dilihat dalam Gambar 11.



Gambar 11. Grafik Proses Ekstraksi Dan Deskripsi

IV. KESIMPULAN

Dari hasil percobaan yang telah dilakukan, maka dapat disimpulkan bahwa implementasi algoritma kriptografi aes dan steganografi dengan metode lbs cukup berhasil.

Pengujian terhadap beberapa sample membuktikan bahwa metode modified LSB memenuhi aspek imperceptibility, dimana keberadaan pesan rahasia pada citra digital sulit untuk dipersepsi oleh inderawi. Hal ini karena perubahan yang terjadi tidak begitu berarti dan tidak menghasilkan perbedaan yang mencolok terhadap stego object. Pengujian terhadap aspek recovery menunjukkan bahwa cipherteks dapat diekstraksi dengan tepat menggunakan metode modified LSB

Pengimplementasian teknik kriptografi aes dan steganografi dengan metode lbs pada data citra rgb berhasil dan berjalan dengan baik. Semakin besar ukuran pesan semakin lama proses enkripsi dan embed.

REFERENSI

[1] Khalil challita, hikmat farhat, combining steganografi and cryptography : new directions dengan kombinasi algoritma mco (multiple cover object), 2012
[2] Kavita kadam, ashwini koshti dan priya dunghav, steganography using least signicant bit algorithm dengan kombinasi algoritma dct (discrete cosine trabsformations), 2012
[3] M. Anggrie andriawanm, solikin dan setia juli irzal ismail, implementasi steganografi pada citra digital file gambar bitmap (bmp) menggunakan java dengan penyisipan pesan ke dalam bit terendah (lsb) bitmap 24 bit.
[4] Chandraleka, h. Mengamankan data pribadi ala agen rahasia. Jakarta: elex media komputindo 2009.
[5] Ariyus, d. 2006. Kriptografi keamanan data dan komunikasi. Yogyakarta: graha ilmu.
[6] Munir, r. Kriptografi. Informatika Bandung: bandung 2006.
[7] Ariyus, d. Pengantar ilmu kriptografi teori, analisis, dan implementasi. Yogyakarta: andi offset 2008.
[8] Ariyus, d. Keamanan multimedia. Yogyakarta : penerbit andi 2007.
[9] Nechvatal j. Et al. Report on the development of the advanced encryption standard (aes). Computer security division information technology laboratory national institute of standards and technology administration u.s. department of commerce 2000.
[10] Edition. New jersey: pearson education. Stallings, w.. Cryptography and network security principles and practice. Third 2003
[11] Daemen, j. & rijmen, v. 1999. Aes proposal: rijndael.http://csrc.nist.gov/archive/aes/rijndael/rijndael-ammended.pdf (18 mei 2015).