KEAMANAN BERLAPIS STEGANOGRAFI DENGAN METODE LSB DAN ENKRIPSI XOR DI MATLAB

Achmad Aditya A. U[1], Meta Sanjaya[2]

Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1]achmad.aditya@gmail.com, [2]metasanjaya@gmail.com

ABSTRAK

Hal yang menjadi prioritas dalam penggunaan steganografi adalah keamanan dalam berkomunikasi. Bagaimana seseorang dapat menyampaikan pesan melalui suatu media tanpa diketahui oleh orang lain selain orang yang diinginkan. Dalam hal ini adalah pesan digital yang dikirimkan melalui media transmisi. Pesan digital tersebut disisipkan ke dalam sebuah media dengan tidak mengubah integritas media tersebut. Media yang dipakai adalah media gambar atau citra digital. Media gambar adalah media yang paling populer dalam menyembunyikan pesan rahasia. Teknik yang dipakai dalam menyembunyikan pesan disini adalah metode LSB (Least Significant Bit) atau menyisipkan bit pesan pada bit rendah atau bit paling kanan. Namun, metode LSB ini juga mudah ditembus karena algoritmanya yang sederhana. Untuk itulah ditambahkan enkripsi XOR untuk menambah tingkat keamanan pesan. Metode XOR ini dijadikan kunci yang akan membuka pesan rahasia. Kunci ini bebentuk file citra asli atau sampul dari citra yang disisipkan pesan. Penerima pesan akan dikirimkan dua buah file citra dengan waktu yang berbeda sebagai cara untuk meningkatkan keamanan. File gambar tersebut adalah file citra yang berisi pesan rahasia dan file citra yang menjadi kunci pembuka pesan rahasia.

Kata Kunci: *steganografi, pesan rahasia, LSB, enkripsi, XOR*

I. PENDAHULUAN

Internet memudahkan penyebaran data dan informasi antar komputer yang saling terhubung. Pengguna komputer dapat dengan mudah bertukar data dan informasi darimanapun mereka berada tanpa terkendala oleh batasan jarak dan waktu. Hampir segala jenis informasi dapat diperoleh, baik informasi yang valid maupun informasi yang tidak dapat dipertanggungjawabkan kebenarannya. Informasi yang diperoleh langsung dari sumbernya maupun informasi yang didapat dari pihak lain, dan itu semua bisa didapatkan dengan sebuah komputer yang terhubung dengan dunia maya ini (Internet).

Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data digital semakin populer dan digunakan didalam banyak kebutuhan. Ada beberapa hal yang membuat data digital (seperti audio, citra, video, dan teks) tersebut semakin banyak digunakan, di antaranya:

a. Mudah diperbanyak atau diduplikasi dengan hasil sama seperti asli.
b. Biaya yang dibutuhkan untuk memperbanyak sangat kecil.
c. Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut.
d. Mudah disebarluaskan, baik dengan media disk maupun melalui jaringan seperti Internet.

Kemudahan-kemudahan tersebut disatu sisi menimbulkan keuntungan, tapi disisi lain menimbulkan kerugian, salah satunya dalam masalah hak cipta dan hak kepemilikan data digital. Setiap data digital yang telah tersebar sangat mungkin untuk menjadi "hak" milik setiap orang. Selain itu, masalah kerahasiaan dalam berkomunikasi menjadi sudah tidak rahasia, karena internet diakses oleh semua orang.

Karena itulah kemudian muncul sejumlah ide tentang bagaimana cara melindungi hasil pekerjaan dalam bentuk data digital, cara untuk mencegah aktivitas penduplikasian oleh pihak yang yak berhak serta teknik untuk melacak penyebaran data digital tersebut, hingga cara untuk mengirim pesan secara rahasia tanpa diketahui orang yang bukan tujuan dari pesan tersebut.

Steganografi muncul sebagai salah satu teknik dalam memecahkan masalah di atas melalui pesan tersembunyi. Steganografi yaitu suatu teknik yang memungkinkan pengguna, dalam hal ini pemilik data digital untuk menyembunyikan suatu pesan di dalam data tersebut. Dengan Steganografi maka pemilik data dapat menyembunyikan informasi hak ciptanya seperti identitas pembuat, tanggal dibuat, hingga pesan kepada seseorang. Steganografi ini menyembunyikan informasi ke dalam berbagai jenis data seperti: gambar, audio, video, text atau file biner.

Steganografi itu sendiri dianggap sebagai seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia di dalamnya. Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi Steganografi. Hari

ini, teknologi jaringan dan komputer menyediakan cara yang lebih mudah untuk menggunakan Steganografi. Istilah Steganografi pun melebar termasuk penyembunyian data digital dalam berkas-berkas (file) komputer. Pada umumnya, pesan steganografi disisipkan pada media lain seperti citra, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan rahasia ini menyatu atau disamarkan dengan media yang disisipinya.

Dalam prakteknya, sebenarnya pesan yang disembunyikan akan membuat perubahan tipis terhadap data digital yang disisipinya. namun karena perubahan itu sulit dilihat dengan mata, maka data tersebut tidak akan menarik perhatian dari orang yang tidak berhak untuk membaca pesan tersebut. Sebagai contoh di bawah ini ada sebuah gambar tidak mengandung pesan rahasia, dan di bawahnya ada gambar yang mengandung pesan rahasia.

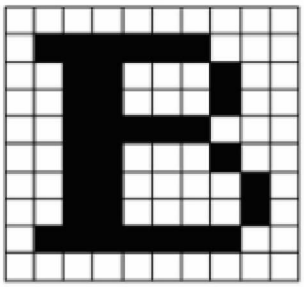
Gambar 1. Contoh gambar sebelum disisipi pesan

Gambar 2. Contoh gambar sesudah disisipi pesan

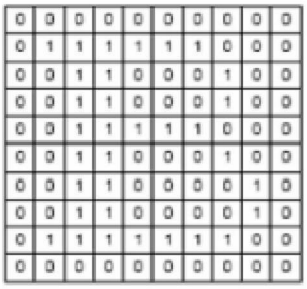
Secara kasat mata, kedua gambar di atas tidak ada bedanya. Tapi jika digunakan aplikasi pengolah gambar bisa diketahui perbedaan melalui warna jika kedua gambar diperbesar hingga beberapa kali. Prioritas utama dari Steganografi adalah bagaimana orang lain tidak menyadari bahwa ada pesan rahasia pada suatu data digital.

Pada dasarnya citra digital (diskrit) dihasilkan dari citra analog (kontinu) melalui
digitalisasi. Digitalisasi citra analog terdiri atas *sampling* dan kuantisasi (*quantization*). *Sampling* adalah pembagian citra ke dalam elemen-elemen diskrit (piksel), sedangkan kuantisasi adalah pemberian nilai intensitas
warna pada setiap piksel dengan nilai yang berupa bilangan bulat[1]. Berdasarkanwarna-warna penyusunnya, citra digital dapat dibagi menjadi tiga macam[2], yaitu:

a. Citra biner, yaitu citra yang hanya terdiri atas dua warna, yaitu hitam dan putih. Setiap piksel pada citra biner cukup direpresentasikan dengan 1 bit.



Gambar 3. Citra Biner

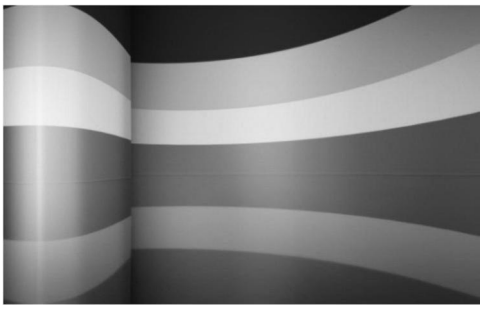


Gambar 4. Representasi Citra Biner

Representasi citra biner terlihat pada gambar 4. Dimana bilangan biner 1 menunjukkan warna hitam, sebaliknya putih ditunjukkan dengan bilangan 0.
Citra biner memiliki sejumlah keuntungan sebagai berikut:

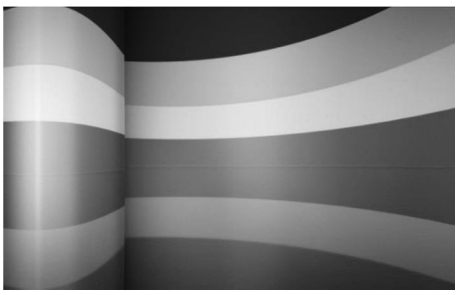
1) Hanya memerlukan memori yang kecil, karena cukup direpresentasikan dengan 1 bit.
2) Waktu proses lebih cepat, karena tidak memerlukan data banyak.

b. Citra grayscale, yaitu citra yang memiliki lebih banyak warna, namun merupakan kombinasi dari warna hitam dan putih. Dimana nilai intensitas paling rendah adalah warna hitam dan nilai intensitas paling tinggi adalah warna putih.



Gambar 5. Citra Grayscale

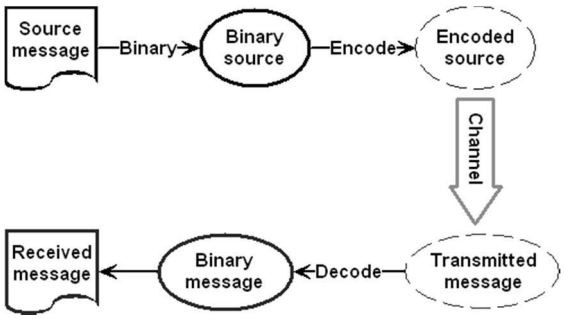
c. Citra berwarna, yaitu citra yang mempunyai warna-warna selain hitam dan putih. Banyaknya warna yang digunakan bergantung kepada kedalaman piksel citra yang bersangkutan. Citra berwarna direpresentasikan dalam beberapa kanal (channel) yang menyatakan komponen-komponen warna penyusunnya.



Gambar 6. Citra Berwarna

II. KONSEP STEGANOGRAFI

Metode Steganografi sedemikian rupa dalam menyembunyikan isi suatu data di dalam suatu sampul mediaatau data digital lain yang tidak dapat diduga oleh orang biasa sehingga tidak menimbulkan kecurigaan kepada orang yang melihatnya. Gambar 7 adalah ilustrasi dasar dari konsep Steganografi.



Gambar 7. Ilustrasi Dasar Konsep Steganografi

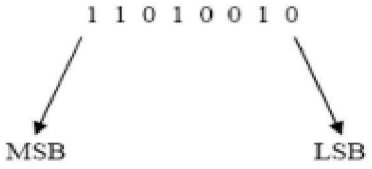
Sebuah pesan yang akan dikirimkan diubah terlebih dahulu menjadi kode biner dan dimasukkan ke dalam kode biner data lain yang menjadi media atau sampulnya. Lalu kedua kode biner tersebut dikodekan sehingga menjadi satu kesatuan tanpa mengubah integritas media yang ditumpangi. Selanjutnya data tersebut dikirimkan dan diterima oleh si penerima pesan. Penerima pesan lalu mengkodekan kembali pesan tersebut sehingga pesan bisa dibaca.

Sebagai contoh, pengirim pesan mulai dengan berkas citra biasa, lalu mengatur warna setiap piksel ke-50 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

III. METODOLOGI LSB

Sebuah program steganografi dibutuhkan untuk melakukan hal-hal implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan, seperti menemukan kelebihan bit dalam dokumen yang dapat digunakan untuk menyembunyikan pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyembunyikan data dan melakukan penyembunyian data dalam bit yang telah dipilih sebelumnya.

Terdapat dua langkah dalam sistem Steganografi yaitu proses penyembunyian dan pengambilan data dari media yang disisipi. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen gambar dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode modifikasi LSB (*Least Significant Bit Modification*). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti *(least significant bit* atau LSB).



Gambar 8. Bit pada MSB dan LSB

Metode *Least Significant Bit Insertion* (LSB) adalah metoda yang digunakan untuk menyembunyikan pesan dengan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data piksel yang menyusun file tersebut. Pada citra bitmap 24 bit, setiap piksel (titik) pada citra tersebut terdiri dari tiga susunan warna, yaitu merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111.

Dengan demikian, pada setiap piksel citra bitmap 24 bit kita dapat menyisipkan 3 bit data. Kekurangan dari metode LSB ini adalah dapat secara drastis mengubah unsur pokok warna dari piksel jika tidak tepat dalam mengganti bit atau pesan yang dimasukkan terlalu panjang. Sehingga dapat menunjukkan perbedaan yang nyata dari gambar asli dengan

gambar yang telah disisipkan pesan. Sementara kelebihan dari metode LSB adalah algoritma yang dipakai cepat dan mudah. Karena bit yang diganti adalah bit rendah, maka perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil. Misalkan segmen data citra sebelum perubahan:

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0
1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1

Segmen data gambar setelah '0 1 1 1' disembunyikan:

0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1
1 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1

Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Misalnya jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka byte yang diganti bit LSB-nya dipilih secara acak, misalkan byte nomor 36, 5, 21, 10, 18, 49.
Bilangan acak dapat dibangkitkan dengan algoritma pseudorandom number generator. Pseudorandom number generator menggunakan kunci rahasia untuk membangkitkan posisi piksel yang akan digunakan untuk menyembunyikan bit-bit. Pseudorandom number generator dibangun dalam sejumlah cara, salah satunya dengan menggunakan algoritma kriptografi berbasis blok (block cipher). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi.

Ukuran data yang akan disembunyikan bergantung pada ukuran gambar penampung. Pada citra 24-bit yang berukuran 256x256 pixel terdapat 65536 piksel, setiap piksel berukuran 3 byte (komponen RGB), berarti seluruhnya ada 65536x3=196608 byte. Karena setiap byte hanya bisa menyembunyikan satu bit di LSB-nya, maka ukuran data yang akan disembunyikan di dalam gambar maksimum adalah: 196608/8 = 24576 byte. Ukuran data ini harus dikurangi dengan panjang nama dokumen, karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama dokumennya. Semakin besar data disembunyikan di dalam gambar, semakin besar pula kemungkinan data tersebut rusak akibat manipulasi pada gambar penampung.

III. ENKRIPSI XOR

1. ENKRIPSI

Untuk meembuat keamanan berlapis, ditambahkan enkripsi di dalam steganografi. Enkripsi sendiri adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa "kunci" yang telah ditentukan sebelumnya. Enkripsi banyak digunakan dalam kepentingan militer maupun agen pemerintah yang memang bertujuan untuk menjaga kerahasiaan informasi. Namun saat ini enkripsi telah digunakan untuk kebutuhan yang lebih luas, seperti pembayaran online untuk situs *e-commerce*.

Enkripsi mempunyai algoritma untuk mengenkripsi data. Data yang telah terenkripsi disebut sebagai *ciphertext*. Rumus ini memerlukan sebuah variabel untuk mengembalikan data tersebut kembali ke bentuk asal. Variabel ini biasa disebut kunci. Tanpa kunci, seseorang sangat sulit bahkan hampir tidak mungkin, untuk dapat memecahkan kode enkripsi tersebut. Maka kunci ini memegang peranan vital di dalam enkripsi.

Enkripsi terbagi menjadi dua: simetris dan asimetris (juga disebut sebagai *public key*). Enkripsi simetris memungkinkan sebuah file dijalankan melalui program dan membuat sebuah kunci untuk mengacak file tersebut. Kemudian file terenkripsi dan kunci dikirimkan secara terpisah kepada penerima. Penerima menjalankan aplikasi enkripsi yang sama dan menggunakan kunci yang diberikan untuk menyatukan kembali file yang telah diacak. Kelebihan enkripsi simetris adalah sangat mudah dan sangat cepat dalam penggunaannya, tetapi tidak seaman enkripsi asimetris, karena jika kunci tersebut jatuh ke tangan orang lain, maka mudah untuk menyatukan file.

Berbeda dengan enkripsi simetris, enkripsi asimetris lebih rumit tapi lebih aman. Hal ini dikarenakan dibutuhkan dua kunci yang saling berhubungan untuk membuka file. Kunci tersebut adalah kunci publik dan kunci pribadi. Kunci publik disediakan bagi siapa saja yang ingin dikirimkan informasi yang terenkripsi. Namun, kunci tersebut hanya dapat digunakan untuk mengkodekan data. Jika ingin mendekodekan data, maka dibutuhkan kunci pribadi yang disimpan oleh pemilik kunci. Kelebihan dari enkripsi asimetris adalah tingkat keamanannya sangat tinggi, tapi kekurangannya adalah dibutuhkan proses dan waktu yang lebih banyak untuk mengenkripsi dan mendekripsi data.

2. OPERASI XOR

Operasi XOR merupakan operasi logika bitwise yang bekerja dengan membandingkan dua buah bit yang apabila pada salah satu bit nya bernilai Benar, maka hasil akhir operasi XOR tersebut adalah benar. Namun, bila kedua bit yang akan dibandingkan bernilai Salah atau keduanya bernilai Benar maka hasil akhir operasi XOR tersebut adalah Salah.

Tabel 1. Tabel Kebenaran Operasi XOR

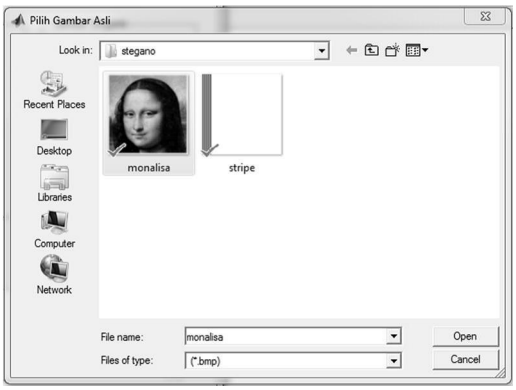
X	Y	X^Y
1	1	0
1	0	1
0	1	1
0	0	0

Ide penggunaan enkripsi XOR dalam steganografi ini adalah tidak mungkin untuk membalikkan operasi tanpa mengetahui nilai awal dari salah satu dari dua argumen. Jika dua variabel dikenai operasi XOR dari nilai yang tidak diketahui, maka tidak bisa diketahui dari hasil operasi apa nilai-nilai variabel tersebut. Misalnya, jika dilakukan operasi XOR pada variabel A dan B, dan hasil operasinya adalah TRUE, maka tidak dapat diketahui apakah variabel A bernilai FALSE dan B bernilai TRUE, atau apakah B bernilai FALSE dan A bernilai TRUE. Bahkan jika operasi tersebut mengembalikan nilai FALSE, tidak bisa dipastikan jika kedua variabel bernilai TRUE atau keduanya bernilai FALSE.

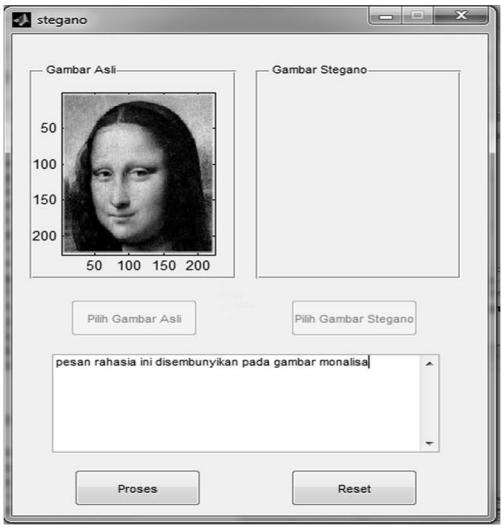
IV. IMPLEMENTASI

Menggabungkan teknik LSB dalam steganografi dengan enkripsi XOR untuk mendapatkan tingkat keamanan yang lebih tinggi pada citra digital ini dilakukan dengan menggunakan aplikasi MatLab 2012. Tahapan untuk menyisipkan pesan rahasia ke dalam citra digital ditunjukkan melalui gambar 9 hingga 12.

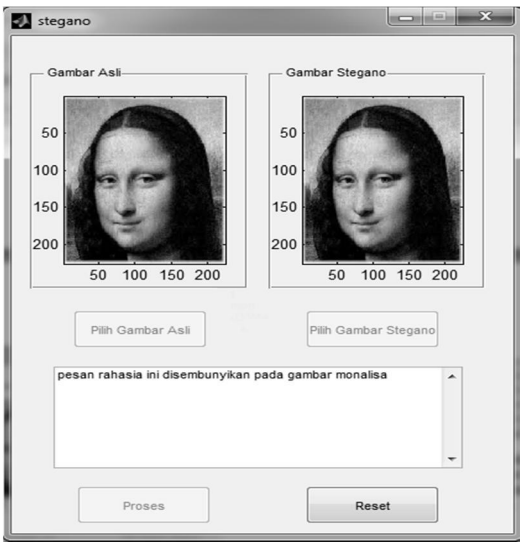
Gambar 9. Tampilan Awal Program



Gambar 10. Tampilan Mencari Citra untuk disisipkan pesan



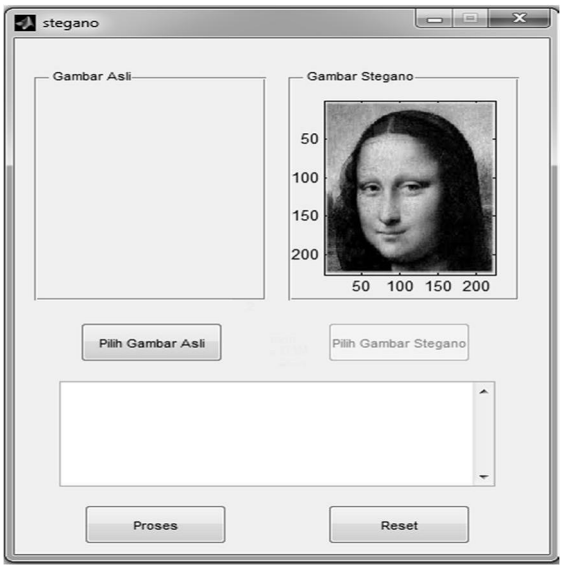
Gambar 11. Tampilan Menuliskan Pesan yang akan disisipkan



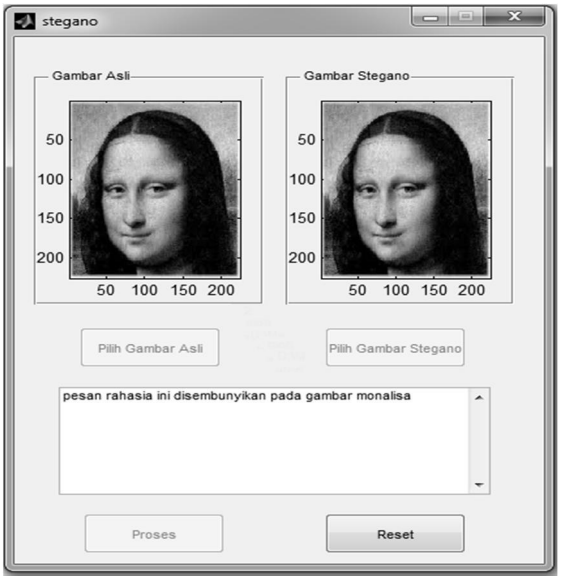
Gambar 12. Tampilan Akhir Proses Penyisipan Pesan

Pada gambar 12, diperlihatkan citra digital yang asli atau belum disisipkan pesan (sebelah kiri) dengan citra digital yang telah disisipkan pesan. Sekilas tidak tampak perbedaan antara keduanya. Semakin panjang pesan yang akan disisipkan, semakin terlihat perbedaan antara citra asli dengan citra yang sudah disisipkan.

Selanjutnya pada gambar 13 dan 14 ditunjukkan tampilan ketika proses pengambilan pesan atau dilakukan.



Gambar 13. Tampilan Memasukkan Kunci untuk Mengambil Pesan. Kunci berupa citra digital asli.



Gambar 14. Tampilan Hasil Pengambilan Pesan

Saat ini program hanya mampu memproses citra digital yang berformat BMP.

V.KESIMPULAN

Strategi keamanan berlapis pada steganografi dengan menggunakan metode LSB dan enkripsi XOR telah meningkatkan keamanan informasi atau data yang disisipkan pada citra digital. Berikut kelebihan dari keamanan berlapis ini:

a. Pesan rahasia disembunyikan dengan metode LSB dengan tingkat kesulitan yang tidak bisa dibilang mudah
b. Citra digital yang telah disisipi pesan dengan metode LSB, lalu dienkripsi dengan metode XOR sehingga menjadi lebih sulit untuk membukanya.
c. Dibutuhkan kunci untuk mendekodekan enkripsi XOR.
d. Kunci untuk mendekodekan enkripsi XOR berupa citra digital asli sebelum disisipi pesan, sehingga tidak menimbulkan kecurigaan.
e. Kunci dikirim secara terpisah kepada penerima, sehingga jika salah satunya jatuh ke tangan orang yang tidak berhak, tetap sulit untuk mengetahui pesan rahasia yang ada di dalamnya.

DAFTAR PUSTAKA

[1] Awcock, G.W. 1996. *Applied Image Processing.* Singapore. McGraw-Hill Book.

[2] Chandra, Marvin. 2007. *Pengolahan citra digital menggunakan matlab.* Bandung. Penerbit Informatika Bandung.

[3] Pengertian dan Jenis Enkripsi, Shvoong, http://id.shvoong.com/

[4] Enkripsi Sederhana Menggunakan XOR, Raitosun, http://raitosun.blogspot.com

[5] Steganography - Technique to hide information within image file, Programmer2Programmer, http://www.programmer2programmer.net

[6] Popa, Richard, (1998), "An Analysis of Steganographic Techniques", *Journal from University Politehnica Timisoara.*

[7] Provos, Niels, Honeyman. Peter. (2003), "Hide And Seek: An Introduction To Steganography", *IEEE Computer Society.*