Implementasi Teknik Steganografi dengan Menggunakan Metode *Least Significant Bit* Pada Citra Digital

Danna Saputra
Mahasiswa Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia, 12260
danna.saputra22@gmail.com

Warsudi
Mahasiswa Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan,Indonesia, 12260
Warsudi.nurhakim27@gmail.com

Abstrak—Steganografi adalah suatu ilmu dan seni menyembunyikan data pada suatu media. Steganografi tercipta sebagai salah satu cara yang digunakan untuk mengamankan data dengan cara menyembunyikannya dalam media lain agar "tidak terlihat". Penyisipan LSB dilakukan dengan memodifikasi bit terakhir dalam satu byte data. Penggunaan teknik steganografi banyak diaplikasikan sebagai cara untuk mengamankan kerahasian sebuah data baik itu berupa gambar, teks, ataupun video saat di transmisikan melalui jaringan intenet. Pada steganografi data rahasia disembunyikan ke dalam media lain dalam bentuk gambar, teks, suara ataupun video. Penelitian ini dilakukan dengan menggunakan metode LSB (Least Significant Bit) untuk menyembunyikan sebuah gambar di dalam gambar [1].dan ,penelitian ini juga membukikan bagaimana kualitas gambar yang telah digabungkan sesuai dengan alokasi atau banyaknya bit untuk gambar yang telah disembunyikan. Alokasi banyaknya bit tersebut dapat diatur sesuai dengan keinginan melalui aplikasi yang digunakan pada penelitian LSB Steganografi ini. Aplikasi tersebut dibuat dengan aplikasi Visual Basic .NET 2008 untuk sistem operasi berbasis Windows 7. Tak hanya gambar dengan ektensi .JPG, aplikasi ini juga dapat memproses data dengan format .BMP, .PNG, .TIFF, dan .GIF. Dari sisi ukuran gambar yang dicoba, tak hanya gambar beresolusi rendah saja yang dapat diproses, gambar yang memiliki resolusi yang sangat tinggi dapat diproses oleh aplikasi ini.

Kata Kunci—Steganografi, Keamanan data, Least Significant Bit, Visual Basic

I. PENDAHULUAN

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Namun demikian, informasi yang dikirimkan dapat disadap ditengah jalan oleh pihak yang tidak diinginkan [2]. Ada banyak teknik untuk mencegah informasi yang dikirimkan melalui jaringan publik seperti internet. Hal ini menjadi sangat berbahaya, bila informasi yang dikirimkan tersebut dinilai sensitif, seperti rahasia Negara atau perusahaan. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan sistem informasi.

Untuk mencegah jatuhnya informasi penting ke tangan yang salah, maka digunakanlah teknik kriptografi, yaitu proses mengubah (encrypt) suatu informasi (plaintext) dengan suatu algoritma khusus (cipher) dengan tujuan agar informasi tersebut tidak dapat dibaca (decrypt) tanpa bantuan kunci (key) khusus [3]. Teknik enkripsi memiliki beberapa kelemahan, salah satunya yaitu mengundang perhatian [4].

Steganografi adalah seni dan ilmu untuk menyembunyikan pesan dalam sebuah pesan. Seni dan ilmu ini telah diterapkan sejak dahulu oleh orang Yunani kuno yang menyembunyikan pesan dengan cara membuat tato di kepala pembawa berita yang dibotaki dan menunggu sampai rambutnya tumbuh. Teknik steganografi lainnya adalah dengan menggunakan "invisible ink" (tinta yang tidak tampak). Tulisan yang ditulis dengan menggunakan *invisible ink* ini hanya dapat dibaca jika kertas tersebut diletakkan di atas lampu atau diarahkan ke matahari. Ketika perang dunia pertama, orang Jerman menyembunyikan pesan dalam bentuk "microdot", yaitu titik-titik yang kecil. Agen dapat membuat foto kemudian mengecilkannya sampai sekecil titik di tulisan dalam buku. Buku ini kemudian bisa dibawa-bawa tanpa ada yang curiga bahwa tanda titik di dalam tulisan di buku itu berisi pesan ataupun gambar.

Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama sehingga digunakan metode steganografi. Dengan metode steganografi, pesan yang ingin disampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut.

Dengan menggabungkan teknik enkripsi dan steganografi, maka diharapkan informasi yang penting dapat dikirimkan dengan lebih aman.

A. Rumusan Masalah

Rumusan masalah yang dibahas dalam karya tulis ini adalah sebagai berikut:

1. Bagaimana perubahan dan pengaruh terhadap gambar yang digunakan sebagai media file steganografi?
2. Bagaimana mengimplementasikan metode LSB (*Least Significant Bit)* terhadap file yang akan disembunyikan ke dalam gambar?
3. Bagaimana implementasi Steganografi pada sebuah gambar sehingga gambar yang telah disembunyikan benar-benar terjaga kerahasiannya.

B. Batasan Masalah

Agar karya tulis ini dapat mencapai tujuan yang ingin dicapai, maka batasanmasalah disusun sebagai berikut:

1. Karya tulis ini menitikberatkan pada pembuatan sebuah aplikasi pengamanangambar atau citra yang disisipkan ke dalam sebuah gambar.
2. Cara menyisipkan informasi ke dalamsebuah gambar menggunakan teknik *LeastSignificant Bit* (LSB).
3. Menggunakan berbagai format gambar untuk menyembunyikan sebuah gambar.

C. Metode Penelitian

Metode penelitian yang digunakan dalam penulisan karya tulis ini adalah sebagai berikut:

1. Studi pustaka, yaitu dengan membaca beberapa literatur-literatur dan referensi mengenai steganografi yang diperoleh dari buku-buku dan informasi yang ada di internet.
2. Analisis dan desain, yaitu menganalisa kebutuhan program dan melakukan perancangan antarmuka dari aplikasi yang akan dibuat.
3. Pemrograman, yaitu melakukan pengkodean terhadap rancangan-rancangan yang telah didefinisikan.
4. Implementasi, yaitu mengevaluasi kemampuan program dengan melakukan perbandingan terhadap perubahan ukuran gambar asli dengan gambar yang disembunyikan dan melakukan perbandingan terhadap perubahan yang dialami oleh gambar yang telah disisipkan.

II. LANDASAN TEORI

A. Steganografi

Kata Steganografi pada awalnya berasal dari bahasa Yunani yaitu Steganos sendiri sebenarnya merupakan kata dari bahasa Yunani [5]. Kata Steganos memiliki arti penyamaran atau penyembunyian dan graphein atau graptos memiliki arti tulisan, sehingga secara keseluruhan artinya adalah “tulisan yang disebunyikan”.

Secara umum steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat JPEG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan file tersebut memilik bit-bit data redundan yang dapat dimodifikasi. Setelah dimodifikasi file media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya.

Pengertian steganografi yang cukup sering digunakan dalam pembelajaran dengan metodologi sejarah adalah menulis tulisan yang tersembunyi atau terselubung. Jadi secaraharfiah dan dalam pengertian yang didewasakan steganografi dapat diartikan sebagai seniuntuk menyamarkan atau menyembunyikan pesan rahasia tertulis ke dalam pesan lainnyadengan segala cara sehingga selain orang yang dituju, orang lain tidak akan tahu pesanrahasia apa yang sebenarnya ingin disampaikan.

B. Tujuan Steganografi

Saat ini dalam dunia digital, teknik steganografi banyak digunakan untukmenyembunyikan informasi rahasia dengan berbagai maksud. Salah satu tujuan dari steganografi adalah mengirimkan informasi rahasia melalui jaringan tanpa menimbulkan kecurigaan. Disamping itu steganografi juga dapat digunakan untuk melakukan autentikasi terhadap suatu hasil karya sebagaimana pemanfaatan watermarking. Namun steganografi juga bias digunakan sebagai sarana kejahatan yang dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan lainnya.

C. Cara Kerja Steganografi

Steganografi memerlukan setidaknya dua properti. Properti pertama adalah wadah penampung *(cover)* dan yang kedua adalah data atau pesan yang disembunyikan. Untuk meningkatkan tingkat keamanan data yang disimpan, dapat dilakukan dengan menambahkan properti kunci *(key)* rahasia. Properti kunci ini dapat berupa kunci simetris maupun kunci public atau privat. Berkas hasil dari proses steganografi sering disebut sebagai berkas stego *(stego file)* atau stego objek.

Properti wadah *(cover)* yang mungkin digunakan untuk menyimpan pesan dalam steganografi sangat beragam. Medium wadah tersebut antara lain citra, suara, video ataupun teks. Adapun data yang disimpan juga dapat berupa audio, citra, video maupun teks. Pertimbangan pemilihan penggunaan kunci dari segi tipe (simetris, *public/privat*) serta panjang kunci adalah suatu hal yang juga berperan penting dalam pengamanan data yang tersimpan dalam steganografi, disamping

menjadi pertimbangan tingkat kemudahan saat ekstraksi data.

Steganografi berbeda dengan kriptografi. Jika dalam kriptografi pesan yang dirahasiakan tidak disembunyikan, seorang kriptanalis dapat membaca pesan dalam format yang terenkripsi dan juga melakukan dekripsi data, maka dalam steganografi yang pertama kali harus dilakukan oleh seorang steganalis adalah menemukan stego objek terlebih dahulu, hal ini karena pesan yang dirahasiakan disembunyikan (tidak nampak) dalam medium lain *(cover).*

Proses penyimpanan data atau informasi yang ingin disembunyikan disimpan dalam sebuah wadah *(cover)* dapat dilakukan dengan suatu algoritma steganografi tertentu (misalnya metode LSB). Untuk menambah tingkat keamanan data, dapat diberikan kunci, agar tidak semua orang mampu mengungkapkan data yang disimpan dalam berkas wadah (cover). Hasil akhir dari proses penyimpanan data ini adalah sebuah berkas stego *(stego data/stego file).*

Pengungkapan data atau informasi dari berkas stego dapat dilakukan dengan mengekstrak berkas stego tersebut dengan memasukkan kunci yang sesuai. Hasil ekstraksi ini adalah berupa data atau informasi dan wadah *(cover)* awal. Proses pengungkapan informasi dari berkas stego digambarkan pada gambar berikut ini.

Pada dasarnya, terdapat tujuh teknik yang digunakan dalam steganografi, yaitu:

1. *Injection*
   Merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut *Embedding.*
2. *Substitusi*
   Data normal digantikan dengan data rahasia. Biasanya hasil teknik itu tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bias menurunkan kualitas media yang ditumpangi.
3. *Transform domain*
   Teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada "*transform space*". Akan sangat lebih efektif bila teknik ini diterapkan pada file berekstensi Jpeg (gambar).
4. *Spread Spectrum*
   Sebuah teknik pentransmisian menggunakan *pseudo-noise code,* yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi *(bandwdith)* yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika*pseudo-noise code* tersinkronisasi.
5. *Statistical Spectrum*
   Teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistic walaupun hanya 1 bit. Perubahan statistic ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. *Distortion*
   Metode ini menciptakan perubahan atas benda yang ditumpangi oleh datarahasia.
7. *Cover Generation*
   Metode ini lebih unik daripada metode lainnya karena *cover object* dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah Spam Mimic.

D. Steganografi yang baik

Penyembunyian data di dalam steganografi dapat dilakukan menggunakan wadah berupa citra, audio, teks, ataupun video dengan berbagai format. Adapun kriteria yang perlu diperhatikan dalam penyembunyian data, yaitu:

1. *Fidelity*
   Setelah penambahan data rahasia, mutu citra penampung tidak jauh berubah, citra steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
2. *Robustness*
   Data yang disembunyikan harus tahan (robust) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras, penajaman, kompresi, perbesaran gambar, pemotongan gambar (cropping), dan sebagainya. Data yang disembunyikan seharusnya tidak rusak dan tetap valid jika diekstraksi kembali.
3. *Recovery*
   Data yang disembunyikan harus dapat diungkapkan kembali (reveal). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

E. Teknik Steganografi LSB

Least Significant Bit (LSB)Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan Least-Significant Bit (LSB). Pada citra digital pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah

atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna 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.

Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format lossless compression, karena metode ini menggunakan bit-bit pada setiap piksel pada image. Jika digunakan format lossy compression, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan image 24 bit color sebagai cover, sebuah bit dari masing-masing komponen Red, Green, dan Blue, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia. Misalnya, di bawah ini terdapat 3 piksel dari image 24 bit color:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Untuk menyembunyikan karakter A (10000001) akan dihasilkan:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

F. Bitwise Operation

Operasi bitwise adalah operasi matematika yang berproses pada level bit/digit dari sebuah bilangan bulat (integer) [6]. Penggunaan operasi bitwise sendiri lebih banyak pada konteks operasi logika. Bit/digit dari sebuah bilangan juga dikenal sebagai bilangan biner (binary) atau bilangan basis 2.

Operator	Description	Example
&	Binary AND Operator copies a bit to the result if it exists in both operands.	(A & B) will give 12 which is 0000 1100
|	Binary OR Operator copies a bit if it exists in eather operand.	(A | B) will give 61 which is 0011 1101
^	Binary XOR Operator copies the bit if it is set in one operand but not both.	(A ^ B) will give 49 which is 0011 0001
~	Binary Ones Complement Operator is unary and has the efect of 'flipping' bits.	(~A) will give -60 which is 1100 0011
<<	Binary Left Shift Operator. The left operands value is moved left by the number of bits specified by the right operand.	A << 2 will give 240 which is 1111 0000
>>	Binary Right Shift Operator. The left operands value is moved right by the number of bits specified by the right operand.	A >> 2 will give 15 which is 0000 1111

a. Operator AND

Operator bitwise AND dilambangkan dengan '&'. Pada dasarnya operasi AND akan menghasilkan nilai 1 apabila dalam kedua operan mengandung bit bernilai 1. Sedangkan nilai yang lain akan menghasilkan nilai 0. Berikut ini adalah contoh penggunaannya di dalam actionscript:

0101 (decimal 5)
AND 0011 (decimal 3)
= 0001 (decimal 1)

b. Operator OR

Operator bitwise OR menggunakan simbol '|'. Pada daasarnya operasi bitwise OR akan menghasilkan nilai 1 apabila salah satu dari bit operan bernilai 1 atau kedua-duanya bernilai 1. Sedangkan juga kedua-duanya bernilai 0, maka operasi ini menghasilkan nilai 0.Berikut ini contoh penggunaannya di dalam actionscript:

0101 (decimal 5)
OR 0011 (decimal 3)
= 0111 (decimal 7)

c. Operator XOR

Operasi bitwise XOR (eXclusive OR) menggunakan simbol '^' Pada dasarnya operasi bitwise XOR akan menghasilkan nilai 1 apabila salah satu bit operan bernilai 1. Jika kedua bit yang dioperasikan bernilai 0 atau kedua2nya bernilai 1 maka operasi XOR akan menghasilkan nilai 0.Berikut ini contoh penggunaannya di dalam actionscript:

0101 (decimal 5)
XOR 0011 (decimal 3)
= 0110 (decimal 6)

d. *Operator NOT*

Berbeda dengan bitwise AND, OR dan XOR yang kesemuanya membutuhkan 2 operan untuk memberikan hasil, operasi bitwise NOT hanya membutuhkan 1 operan untuk memberikan hasil. Operasi NOT mempunyai simbol '~'. Berikut ini adalah contoh penggunaanya di dalam actionscript:

0111 (decimal 7)
NOT = 1000 (decimal 8)

E. Bitmask Operation

Dalam ilmu komputer, mask adalah data yang digunakan untuk operasi bitwise, khususnya di bilangan bit [7].

a. Mask bit to 1

Untuk mengaktifkanbittertentu, bitwiseORoperasi dapatdigunakan, mengikutiprinsip bahwaYOR1=1danYOR0=Y.Oleh karena itu, untuk memastikansebuah bit ituaktif,ORdapat

digunakandengan1.Untuk membiarkan sebuat bit tidak berubah, maka ORdigunakandengan0.Contoh: menyalakan 4 bit

10011101 10010101
OR 00001000 00001000
= 10011101 10011101

b. Mask bit to 0

Tidak ada carauntuk mengubahsebuat bit dari on menjadi offmenggunakanoperasi OR. Sebaliknya, bitwiseANDdigunakan. Ketikanilai yang di ANDdengan1, hasilnya adalahhanyanilai asli, seperti dalam: YDAN1=Y.Namun, meng-AND nilaidengan0dijaminuntuk mengembalikan0, sehingga memungkinkanuntuk mengubahsedikitoffdengan meng AND kan dengan0: Y=0AND0. Untukmeninggalkanbitlainnyasaja, dengan meng AND merekadengan1dapat dilakukan.Contoh: menyalakan 4 bit

10011101 10010101
AND 11110111 11110111
= 10010101 10010101

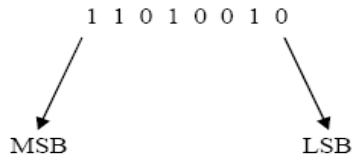
III. ANALISA DAN PERANCANGAN

A. ANALISA

a. Metode LSB yang digunakan

Untuk menyembunyikan sebuah pesan di dalam gambar, bit dari pesan tersebut dapat disisipkan ke dalam digit bit paling belakang yang merupakan least significant bit (LSB). Dengan menyisipkannya ke dalam LSB, tak hanya teks, gambar pun dapat disisipkan ke dalam sebuah gambar.Pasalnya, least significant bit yang berada di paling belakang tidak berpengaruh banyak pada gambar aslinya. Tanpa kasatmata, perbedaan antara gambar polos dan gambar yang sudah disisipkan pesan tidak dapat dibedakan.

Contohnya, jika komponen piksel warna merah terdiri dari 255 bit, lalu dialokasikan satu bit terakhir untuk menyisipkan pesan atau gambar sehingga tinggal 254 bit, maka gambar aslinya pun tidak akan jauh berbeda dengan sebelumnya.



Tak hanya satu bit terakhir saja, mengalokasikan beberapa LSB pun tidak membuat gambar aslinya banyak berubah. Semakin banyak alokasi bit yang dapat digunakan, maka semakin banyak pula ruang untuk menyembunyikan pesan di dalam sebuah gambar.

Berbeda dengan LSB, Most Significant Bit (MSB) sangat berpengaruh pada sebuah gambar. Jika diubah, MSB yang terletak di jajaran bit paling depan akan membuat gambar berubah secara signifikan sehingga gambar aslinya tidak terlihat lagi. Walaupun hanya mengubah satu bit, perubahan yang terjadi cukup banyak.

Contohnya, bilangan 255 dengan biner 1111 1111 pada saat diubah menjadi 0111 1111 nilai bilangannya akan menjadi 127. Dengan kata lain, ada selisih sebesar 128 antara 255 dan 127 sehingga membuat gambar aslinya pun tak nampak lagi.

a.

b. Cara Kerja Program

Melalui program yang dibuat dengan menggunakan Microsoft Visual Basic .NET, LSB dari gambar asli dapat dialokasikan untuk menyimpan MSB dari gambar yang ingin disembunyikan. Dengan kata lain, bit pixel yang termasuk dalam LSB pada gambar asli akan digunakan untuk bit pixel yang termasuk dalam MSB untuk menyembunyikan sebuah gambar.

Dengan menggunakan metode tersebut, nilai pixel pada gambar asli pun tidak banyak bertambah sehingga kedua gambar tersebut dapat menyatu tanpa kasat mata. Gambar asli pun dapat menutupi keberadaan gambar yang disembunyikan.
Contohnya ketika ingin menggunakan 3 bit terakhir yang merepresentasikan pixel warna merah untuk menyembunyikan gambar. Misalkan pixel berwarna merah pada gambar asli memiliki biner 10110101. Sedangkan pixel berwarna merah pada gambar yang ingin disembunyikan memiliki biner 01010011. Untuk menggunakan 3 bit terakhir (LSB) untuk menyembunyikan gambar, 3 bit terakhir (LSB) pada gambar asli dapat dibuang lalu diganti dengan bit yang paling signifikan (MSB) dari gambar yang ingin disembunyikan.

Dalam contoh ini, gambar asli memiliki biner **10110101** dan gambar yang ingin disembunyikan memiliki biner **01010011**. Itu berarti gambar asli yang memiliki gambar tersembunyi di dalamnya akan memiliki bilangan biner **10110~~101~~** + **010~~10011~~** = 10110**010**.
Setelah gambar dikombinasikan, untuk mengetahui seberapa besar perubahan yang terjadi pada gambar, bilangan biner pada gambar asli dan gambar yang sudah dikombinasikan dapat dibandingkan. Gambar asli memiliki bilangan biner 10110101. Jika dikonversikan ke dalam bilangan desimal berarti 181. Sedangkan gambar yang sudah dikombinasikan memiliki bilangan biner 10110010. Dalam bilangan desimal berarti 178.

Jika diselisihkan antara 181 dan 178, hasilnya adalah 3. Kecilnya selisih tersebut membuat gambar yang sudah dikombinasikan pun nampak seperti gambar aslinya saat belum dikombinasikan. Hal tersebut terjadi karena tidak banyak perubahan

yang terjadi mengingat perubahan binernya pun sangat kecil.

Untuk memulihkan kembali gambar yang tersembunyi, 3 bit terakhir (LSB) dari gambar yang sudah tergabung dapat diekstraksi dan digunakan sebagai MSB. Dalam contoh sebelumnya, 10110**010** merupakan bilangan biner dari gambar yang sudah tergabung. Bilangan biner tersebut bisa diekstraksi sehingga dapat menghasilkan gambar asli serta gambar yang tersembunyi. Setelah diekstraksi, bilangan biner yang dihasilkan adalah 10110000 untuk gambar asli. Sedangkan untuk gambar yang tersembunyi bilangan binernya adalah 01000000.

Jika dibandingkan dengan bilangan biner asalnya, baik pada gambar asli maupun gambar yang disembunyikan, bilangan biner yang dihasilkan setelah diekstraksi dari gambar yang sudah tergabung pun berbeda. Meski begitu, bilangan biner yang dihasilkan tidak terlalu jauh dari aslinya sehingga masih dapat digunakan kembali.

c.Alur Program

Pertama-tama, user menentukan berapa banyak bit yang ingin digunakan melalui objek "NumericUpDown1". Setelah itu, user pun dapat menekan tombol "Eksekusi". Tombol tersebut akan memanggil fungsi "Sembunyikan Gambar" untuk menyembunyikan gambar yang ada di dalam objek "PictureBox2" ke dalam gambar yang ditampilkan pada objek "PictureBox1". Setelah itu, fungsi "SembunyikanGambar" pun menampilkan hasil dari penggabungan kedua gambar pada objek "PictureBox3".

Kemudian fungsi "KembalikanGambar" dipanggil untuk mengekstraksi gambar yang tersembunyi dan menampilkan hasilnya pada objek "PictureBox4"

B. RANCANGAN SISTEM

a. KebutuhanSistem

Sebagai aplikasi yang berbasis desktop, untuk menjalankan program steganografi ini dibutuhkan dua hal, yakni perangkat keras (hardware) dan perangkat lunak (software). Hardware merupakan wujud perangkat secara fisik yang terdiri dari prosesor, hard disk, monitor, RAM, power supply, mainboard, serta keyboard dan mouse. Sedangkan software digunakan untuk memerintahkan hardware agar dapat memproses dan menjalankan data sehingga aplikasi pun dapat berjalan dengan sempurna.

b. SpesifikasiKebutuhanHardware

Agar program tersebut dapat berjalan, setidaknya dibutuhkan komputer maupun notebook dengan spesifikasi hardware sebagai berikut:

1. CPU berkecepatan 1,6 GHz atau lebih tinggi.
2. Harddisk minimal 50 GB
3. Monitor berresolusi 1024 x 768 pixel.
4. Memori RAM yang digunakan minimal 384 MB.

c. Spesifikasi Kebutuhan Software

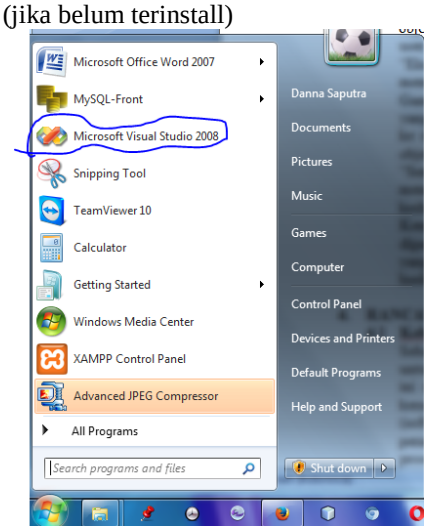
Beberapa software yang dibutuhkan untuk dapat menjalankan program tersebut adalah:

1. Microsoft Visual Basic 2008
2. Sistem operasi Windows XP (32 bit atau 64 bit) atau lebih tinggi

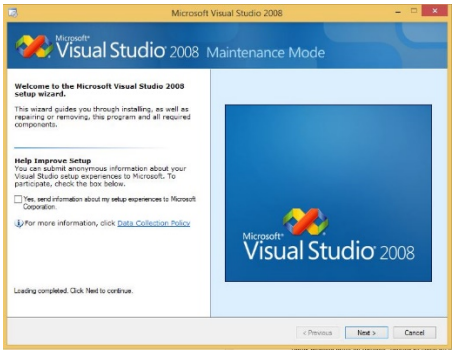
d. ImplementasidanPengujian

Untuk mengimplementasikan dan menguji metode LSB dari program yang dibuat, ada beberapa langkah yang harus dilakukan. Di antaranya adalah:

1. Melakukan instalasi Microsoft Visual Basic 2008 (jika belum terinstall)

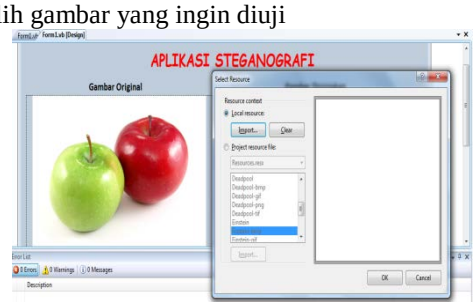


2. Membuka program steganografi dengan menggunakan Microsoft Visual Basic 2008



3. Membuka Aplikasi Steganografi

4. Memilih gambar yang ingin diuji



5. Menjalankan program steganografi

e. Spesifikasi Hardware yang Digunakan

Untuk menguji program tersebut, spesifikasi hardware yang digunakan adalah:

1. CPU Intel i3 M380 berkecepatan 2,53 GHz
2. VGA ATI Mobility Radeon HD 5610 1GB
3. Harddisk WD Black 3,5" SATA III berkapasitas 500GB
4. Monitor ViewSonic VA1932 dengan resolusi 1.366 x 768 pixel.
5. RAM DDR3 N-Gen 4GB(2x2GB)
6. Mainboard Toshiba L645
7. Power Supply Thermaltake ThoughPower 750W

f. Spesifikasi Software yang Digunakan

Untuk menguji program tersebut, spesifikasi software yang digunakan adalah:

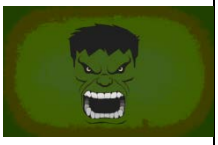
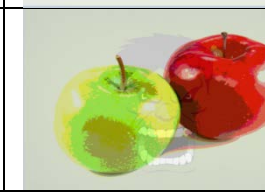
1. Windows 7 32Bit
2. Microsoft Visual Studio 2008

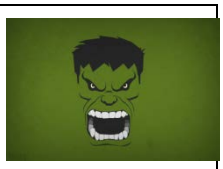
g. Pengujian yang digunakan

Penulis melakukan empat uji coba dengan kombinasi gambar yang berbeda-beda dari sisi ukuran (resolusi) dan komposisi warna. Keempat percobaan tersebut dilakukan dengan delapan gambar dengan format .JPG. Masing-masing percobaan dilakukan dengan mengalokasikan LSB pada gambar sebanyak 0-8 secara berturut-turut.

Pengujian pertama dilakukan dengan file "Apel.jpg" dan "Hulk.jpg". File "Apel.jpg" memiliki ukuran 506 KB. Sedangkan file "Hulk.jpg" memiliki ukuran 594 KB. Kedua gambar tersebut memiliki resolusi yang sama, yakni 180 x 180 bit depth 24.

	
Apel.jpg	Hulk.jpg

Bit LSB	Gambar Gabungan	Gambar Setelah Diekstraksi
0		
1		
2		
3		
4		
5		
6		

7		
8		

Jika gambar yang ditampilkan dilihat secara seksama, gambar yang sudah dikombinasikan sangat mirip dengan gambar asli yang belum dikombinasikan. Tak hanya itu, hasil gambar yang diekstraksi dari gambar yang sudah dikombinasikan pun sangat mirip dengan gambar yang ingin disembunyikan sebelum digabungkan. Semakin tinggi pengalokasian bit LSB pada gambar asli akan membuat gambar yang sudah dikombinasikan nampak seperti gambar yang ingin disembunyikan.

Penulis juga sempat menguji coba program tersebut dengan berbagai format gambar. Tak hanya format .JPG, format gambar lainnya seperti .BMP, .GIF, .PNG, dan .TIFF juga dapat diproses.

h. Evaluasi Program

Evaluasi program merupakan salah satu hal yang perlu dilakukan dalam setiap pengembangan aplikasi guna menganalisa dan mengetahui hasil yang telah dicapai oleh aplikasi yang dikembangkan tersebut. Demikian juga pada aplikasi steganografi yang dikembangkan ini, maka dilakukan evaluasi program untuk menganalisa hasil yang dicapai pada aplikasi ini. Dan dalam evaluasi tersebut ditemukan beberapa kelebihan dan kekurangan program yang dilihat dari beberapa kondisi dan situasi. Adapun kelebihan dan kekurangan pada aplikasi yang dikembangkan adalah sebagai berikut:

a) Kelebihan program

- Program dapat dengan mudah dioperasikan oleh user, karena memiliki user interface (tampilan antar muka) yang baik dan user friendly.
- Dapat dioperasikan di komputer yang memiliki spesifikasi rendah karena program aplikasi ringan ketika dijalankan.
- Tidak memerlukan database dalam pengoprasiannya.
- Integritas data dari file yang disisipi tetap dapat terjaga.
- Lebih banyak pesan yang dapat disimpan kedalam gambar karena pesan tersebut dikompresi terlebih dahulu sebelum disisipkan kedalam gambar.

b) Kekurangan Program

- Hanya dapat memuat pesan berupa text saja, karena memang hanya dirancang untuk pesan berupa text
- Hanya dapat memuat Gambar saja untuk melakukan konfersi Bit, karena memang hanya dirancang untuk pesan berupa text
- Dalam beberapa kasus, jumlah bit yang dihasilkan setelah melakukan kompresi bisa menjadi lebih besar dari sebelumnya. Hal ini dikarenakan dalam penyisipan pesan disertakan juga tabel huffmannya.
- Stego image bisa berubah isi pesannya jika terjadi perubahan pada pixel-pixel yang disisipkan pesan.
- Stego image tidak dapat dibaca jika telah terjadi perubahan pada header data, atau dengan kata lain pixel-pixel yang mengandung header pesan telah berubah bit nya.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari pengujian yang dilakukan, ada beberapa hal yang dapat disimpulkan. Di antaranya adalah:

1. Setelah kedua gambar digabungkan, lalu gambar yang disembunyikan diekstraksi kembali, ada penurunan kualitas gambar. Hal tersebut disebabkan oleh tidak utuhnya bit pada gambar yang disembunyikan ketika diekstraksi. Dengan kata lain, tidak semua bit yang ada pada gambar yang disembunyikan dapat dikembalikan ketika diekstraksi.
   Meski begitu, secara keseluruhan, gambar dapat dikembali dalam bentuk semula. Hanya saja, terdapat degradasi warna ketika diekstraksi. Degradasi warna cukup terasa pada saat mengalokasikan kurang dari lima bit LSB untuk gambar asli. Sedangkan pada saat mengalokasikan lebih dari empat bit LSB, degradasi warna tidak terlalu terlihat.
2. Pada saat mengalokasikan sebanyak 0 bit LSB, hasil ekstraksi dari gambar yang disembunyikan hanya menampilkan warna hitam. Hal ini disebabkan oleh tidak adanya alokasi bit sama sekali untuk gambar yang ingin disembunyikan. Hal ini juga membuktikan bahwa gambar yang ingin disembunyikan tidak disisipkan ke dalam gambar pertama ketika mengalokasikan 0 bit untuk LSB.
3. Pada saat mengalokasikan 8 bit LSB, gambar asli tak nampak lagi. Gambar yang ingin disembunyikan justru nampak tanpa adanya penurunan kualitas. Dengan kata lain, gambar aslinya tidak ditampilkan sama sekali. Hal ini disebabkan oleh tidak adanya alokasi bit untuk gambar asli. Pada saat proses penggabungan,

seluruh digit bit yang ada dialokasikan untuk gambar yang ingin disembunyikan.

4. Mengalokasi 2-3 bit LSB merupakan angka yang ideal untuk menyembunyikan gambar di dalam gambar. Pasalnya, konfigurasi tersebut membuat gambar yang disisipkan tidak terlihat pada gambar aslinya. Namun untuk gambar yang memiliki warna polos, mengalokasikan 3 bit dapat membuat gambar yang disisipkan sedikit tampak pada gambar asli.

5. Pada saat gambar yang disembunyikan memiliki resolusi yang lebih besar, gambar asli tidak dapat menyembunyikan seluruh bagian gambar. Hal ini membuat gambar yang disembunyikan tidak dapat kembali normal (terpotong) pada saat diekstraksi dari gambar asli.
6. Ketika memproses gambar yang memiliki resolusi besar, seperti Full HD (1.920 x 1.080), waktu yang dibutuhkan untuk menggabungkan dan mengekstraksi gambar menjadi lebih banyak. Semakin besar resolusi gambar, maka semakin lama pula proses penggabungan gambarnya.
7. Program aplikasi *steganography* ini membatasi akses dari orang yang tidak berhak atas pesan atau data rahasia, karena informasi disisipkan kedalam *file image* dengan key berupa password dan disembunyikan dengan baik ke dalam *file image* tersebut.Selain itu dalam hal kompresi jika pesan yang ingin disisipkan panjang, maka pengimplementasian kompresi pesan akan sangat berguna dalam mengkompresi pesan sebelum masih ke dalam file image. Sedangkan untuk konsistensi data, data pesan akan terjaga selama tidak terjadi perubahan citra gambar pada pixel-pixel yang mengandung pesan, dan juga perubahan citra tersebut tidak merubah header pesannya.
8. Untuk pengembangan aplikasi *steganography* dengan kompresi data kedepannya bisa ditambahkan metode enkripsi di dalamnya, dan juga dilakukan pengecekan apakah terjadi perubahan pada citra atau tidak, sehingga dapat memastikan konsistensi data pesan. Seperti halnya bisa dilakukan pengecekan dengan menggunakan *checksum* terlebih dahulu sebelum data pesan dibaca dari gambar.

B. Saran

Beberapa saran dari penulis yang dapat diberikan kepada pembaca antara lain:

1. Aplikasi steganografi ini dapat dikembangkan sehingga memiliki beragam fitur.

2. Dibuat dengan menggunakan Microsoft Visual Basic .NET membuat aplikasi steganografi ini memiliki extension .EXE yang hanya dapat berjalan pada sistem operasi Windows. Oleh karena itu, aplikasi ini dapat dikembangkan untuk berbagai sistem operasi seperti Linux, macOS, dan FreeBSD.

3. Aplikasi steganografi ini menggunakan metode LSB untuk menyembunyikan gambar di dalam gambar. Pengembangan lainnya dengan menggunakan objek berbeda pun dapat dilakukan. Seperti menyembunyikan teks di dalam gambar, menyembunyikan teks di dalam file audio, dan lain-lain.

DAFTAR PUSTAKA

[1] Wayan Firdaus Mahmudy Steganografi Pada File Citra Bitmap 24Bit Untuk Pengamanan Data *MenggunakanMetode Least Significant Bit(LSB) Insertion*. Matematika, FMIPA Universitas Brawijaya Malang. 2006

[2] Prasetyo, Tyo,*Jurnal Steganografi Gambar dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online.*Fakultas Sainsdan Teknologi UIN Sunan Gunung Djati Bandung, 2012

[3] Naufal, Muhammad. 2013. *Implementasi Steganografi Dan Kriptografi Untuk Keamanan Data Dengan Metode Rc2 Pada Citra Bitmap*. Triguna Dharma

[4] Cahyad Tri, Rizal R, Handoyo, *Makalah Seminar TugasAkhirimplementasiSteganografiLsbDengan EnkripsiVigenere Cipher Pada Citra Jpeg*.TeknikElektroFakultasTeknikUniversitasDi ponegoro, 2012

[5] http://en.wikipedia.org/wiki/Steganography, 20 Oktober 2015