Studi Dan Implementasi Steganografi Pada Citra JPEGDengan Metode Spread Spectrum

M. Luthfi Aksani [1] , Ignatius Fredrik Manurung [2]
Universitas Muhammadiyah Tangerang / Fakultas Teknik,
Program Studi Informatika
Jl. Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang TLP. 55793251, 55772949, 55793802, 55736926
e-mail: L13Fie@gmail.com , tem_nizz@yahoo.com

Abstrak

Informasi adalah sebuah data mentah yang telah dipilah sedemikian rupa sehingga memiliki manfaat informatif bagi sebagian maupun banyak pihak. Dan di era internet ini, transaksi informasi merupakan hal yang lumrah dilakukan di dunia maya. Hal yang sering dilupakan oleh para user internet adalah keamanan data. Dimana informasi di internet sifatnya adalah terbuka, dengan kemungkinan akses oleh user dari seluruh dunia. Dalam kasus yang sensitif, beberapa informasi ditujukan hanya untuk user atau pihak tertentu, dalam hal inilah diperlukan suatu proteksi untuk melindungi informasi dari pihak-pihak yang tidak berhak mengaksesnya. Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data-data digital semakin banyak digunakan. Disisi lain kemudahan tersebut telah memunculkan masalah di sekitar hak cipta dan hak kepemilikan materi digital. Teknik *hidden message* (steganografi), adalah suatu teknik yang mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain. Dengan kemampuan tersebut maka informasi hak cipta seperti identitas seorang pengarang, tanggal ciptaan, dan lain-lain dapat disisipkan/disembunyikan kedalam berbagai macam variasi jenis dokumen besar seperti: gambar, audio video, text atau file biner. Penelitian ini membahas steganografi dengan menggunakan Teknik Dynamic Cell Spreading yang merupakan teknik menyembunyikan atau menyisipkan data dengan bantuan buffer memori sebagai media penggabungan.

Kata kunci: *Perencanaan bisnis, teknologi informasi, percetakan online berbasis aplikasi web.*

PENDAHULUAN

1. Latar Belakang

Keamanan suatu informasi pada saat ini tidak akan ada habisnya jika dibahas karena telah menjadi suatu kebutuhan yang sangat penting. Kebutuhan keamanan akan semakin meningkat jika informasi tersebut mengandung nilai – nilai bisnis, privasi, ataupun kepentingan tertentu. Terlebih lagi, aksi penyalahgunaan informasi (hacking) dalam dunia maya semakin marak menyebabkan informasi tersebut harus dilindungi dari gangguan pihak – pihak yang tidak berkepentingan.

Salah satu cara yang paling sering digunakan adalah dengan mengenkripsi informasi – informasi tersebut, yang disebut dengan kriptogrfi. Metode lainnya yaitu dengan menyembunyikan data rahasia tersebut di dalam data yang lain. Teknik ini disebut dengan steganografi. Berbeda dengan teknik kriptografi yang dengan mudah dideteksi keberadaanya (walaupun sulit untuk dimengerti), steganografi menyamarkan keberadaan dari informasi (data) yang ingin disampaikan ke dalam media penyamar, misalnya media yang berbentuk berkas multimedia.

Masalah yang dapat dirumuskan dari latar belakang di atas adalah bagaimana membangun suatu aplikasi steganografi pada citra digital file gambar bitmap yang efisien, bagaimana mengeksploitasi keterbatasan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia, sehingga dengan keterbatasa

n tersebut manusia sulit menemukan gradasi penurunan kualitas warna file gambar yang telah disisipi pesan rahasia.

2. Tujuan

Tujuan yang di harapkan antara lain menganalisa teknik steganografi pada citra digital file gambar bitmap untuk menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya, sehingga pesan terlihat hanya seperti pesan biasa saja.

3. Metode

Metode steganografi yang digunakan adalah Spread Spectrum. Metode Spread Spectrum mentransmisikan sebuah sinyal pita informasi yang sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi. Penyebaran ini berguna untuk menambah tingkat redundansi. Besaran redundansi ditentukan oleh faktor pengali cr yang bernilai skalar. Panjang bit- bit hasil penyebaran ini menjadi cr kali panjang bit–bit awal.

Dalam makalah ini juga akan dibahas mengenai dampak perubahan dari audio yang dihasilkan setelah penyisipan, yang akan diukur secara subjektif dan objektif. Subjektif berarti dilakukan dengan pengamatan langsung, sedangkan objektif akan menggunakan metode PSNR (Peak Signal to Noise Ratio) yang mengukur tingkat perbedaan audio tersebut.

LANDASAN TEORI

Steganografi adalah 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. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan.

Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya “tersembunyi atau terselubung”, dan graphein, “menulis”. Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (*file*) komputer. Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya). Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya.

Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat di antara garis-garis yang kelihatan.Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula.

1. Metode Steganography Pada Teks

a. Metode Spasi Terbuka

Terdapat beberapa cara untuk memanfaatkan spasi terbuka dalam data text guna menyembunyikan informasi. Metode ini dapat berhasil karena buku bacaan pada umumnya menambahkan satu spasi tambahan pada akhir baris atau diantara dua kata sehingga tidak terbaca aneh. Bagaimanapun, metode spasi terbuka hanya dapat digunakan dengan memakai ASCII (*American Standard Character Interchange*) format. Bender et al memberikan tiga metode untuk mengungkap *white space* dalam proses penyembunyian.

Spasi terbuka antar kalimat akan menghasilkan nilai "0" apabila hanya terdapat sebuah spasi yang ditambahkan diantara kalimat tersebut. Dengan menambahkan dua spasi akan menghasilkan nilai "1". Metode ini dapat berhasil, tetapi membutuhkan data dalam jumlah besar untuk menyembunyikan sebuah informasi kecil. Dan juga terdapat banyak software *word-processing* yang akan secara otomatis membetulkan spasi antara kalimat, sehingga metode ini seringkali gagal.

Metode spasi *end-of-line* (EOL) mengutarakan white space pada akhir dari masing-masing baris. Data disembunyikan menggunakan jumlah spasi yang telah ditentukan sebelumnya dari akhir untuk masing- masing kalimat. Sebagai contoh dua spasi akan menyembunyikan satu bit, empat spasi akan menyembunyikan dua bit dan delapan spasi akan menghasilkan tiga bit dan seterusnya. Tehnik ini lebih baik dibandingkan metode spasi terbuka antar kalimat, karena dengan meningkatkan jumlah spasi akan dapat menyembunyikan lebih banyak data.

Salah satu kekurangan dari tehnik ini adalah dapat hilangnya informasi tersembunyi jika hard copy data yang diberikan Pada akhirnya, pemerataan kanan dari text dapat digunakan pula untuk menyembunyikan informasi rahasia pada data text. Penghitungan dan pengontrolan spasi diantara kata dapat menyembunyikan informasi dalam data text yang terlihat tidak penting. Sebuah spasi antara kata akan menghasilkan nilai "0" dan dua buah spasi akan menghasilkan nilai "1".

Bagaimanapun, pendekatan ini akan mempersulit untuk mengeluarkan informasi penitng dari media data text tersebut karena akan semakin tidak mungkin untuk membedakan sebuah spasi biasa dengan spasi yang berfungsi untuk penyembunyian data. Untuk mewujudkan hal ini, Bender et al menggunakan Manchester coding untuk mengelompokkan bit-bit. Sehingga "01" diinterpretasikan sebagai "1" dan "10" diinterpretasikan sebagai "0". Dimana "00" dan "11" akan dianggap sebagai null bit string.

b. Metode Syntactic

Metode Syntactic sebagaimana yang telah di sarankan oleh Bender et al, mengutarakan penggunaan punktuasi dan struktur text untuk menyembunyikan informasi tanpa secara signifikan mengubah arti dari pesan pembawa. Sebagai contoh terdapat dua frase "*bread, butter, and milk*" dan "*bread, butter and milk*" secara gramatikal benar tetapi berbeda dalam penggunaan koma. Salah satu dapat digunakan secara alternatif dalam pesan text guna mengintepretasikan nilai "1" apabila salah satu metode dipakai dan nilai "0" untuk metode lain yang dipakai.

c. Metode Semantic

Metode Semantic menggunakan dua sinonim sebagai nilai primer atau sekunder. Nilai tersebut akan diterjemahkan kedalam biner "1" atau "0". Bender et al menggunakan sebuah contoh dimana kata "big" berfungsi sebagai primer dan "large" berfungsi sebagai sekunder. Oleh karena itu, dalam menguraikan isi sebuah pesan akan menterjemahkan atas penggunaan primer sebagai "1" dan sekunder sebagai "0". Bender et al menyebutkan masalah yang dapat muncul dengan penggunaan metode ini adalah ketika sinonim tidak dapat digantikan karena dapat mengubah arti dari struktur kalimat. Sebagai contoh dalam memanggil seseorang dalam bahasa Inggris dengan "cool" mempunyai arti berbeda dibandingkan dengan memanggilnya "chilly".

2. Metode Steganography Pada Gambar

Sudah banyak metode yang digunakan untuk menyembunyikan pesan di dalam sebuah image tanpa mengubah tampilan image, sehingga pesan yang disembunyikan tidak akan terlihat. Berikut akan dibahas beberapa metode umum yang digunakan pada image steganography.

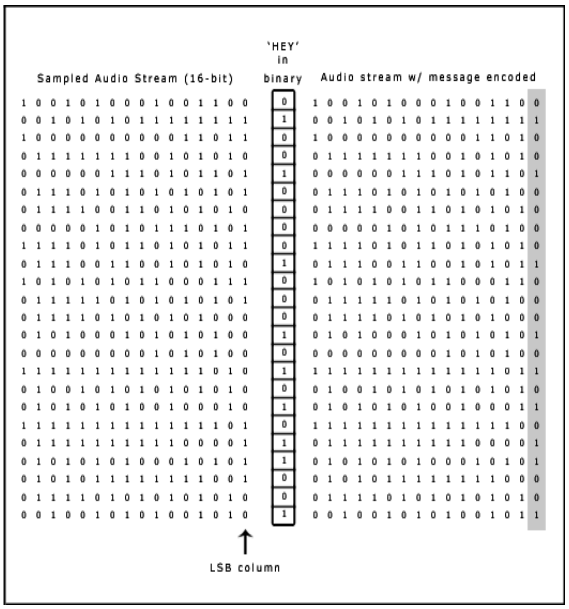
a. Penyisipan Least Significant Bit

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan *Least-Significant Bit* (LSB). 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 pikses 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)
jika diinginkan untuk menyembunyikan karakter A (10000001) dihasilkan :
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100110 11101001)
dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Jika digunakan image 8 bit color sebagai cover, hanya 1 bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan image harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra. Akan lebih baik jika image berupa image grayscale karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia.

Proses ekstraksi pesan dapat dengan mudah dilakukan dengan mengekstrak LSB dari masing-masing piksel pada stego secara berurutan dan menuliskannya ke output file yang akan berisi pesan tersebut. Kekurangan dari metode modifikasi LSB ini adalah bahwa metode ini membutuhkan "tempat penyimpanan" yang relatif besar. Kekurangan lain adalah bahwa stego yang dihasilkan tidak dapat dikompress dengan format lossy compression.



Gambar 2.1 Least Significant Bit

b. Masking dan Filtering

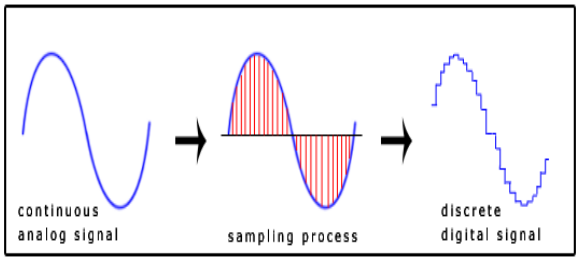
Teknik masking dan filtering ini biasanya dibatasi pada image 24 bit color atau image grayscale. Metode ini mirip dengan watermark, dimana suatu image diberi tanda (marking) untuk menyembunyikan pesan rahasia. Hal ini dapat dilakukan, misalnya dengan memodifikasi luminance beberapa bagian dari image. Walaupun metode ini akan mengubah tampilan dari image, dimungkinkan untuk melakukannya dengan cara tertentu sehingga mata manusia tidak melihat perbedaannya. Karena metode ini menggunakan aspek gambar (*image*) yang memang terlihat langsung, metode ini akan lebih "*robust*" terhadap kompresi (*terutama lossy compression*), *cropping*, dan beberapa image processing lain, bila dibandingkan dengan metode modifikasi LSB.

c. Transformation

Metode yang lebih kompleks untuk menyembunyikan pesan pada image ini dilakukan dengan memanfaatkan *Discrete Cosine Transformation* (DCT) dan *Wavelet Compression*. DCT digunakan, terutama pada kompresi JPEG, untuk metransformasikan blok 8x8 piksel yang berurutan dari image menjadi 64 koefisien DCT.

3. Metode Steganography Pada Suara

Cara untuk mengaplikasikan steganography pada file audio terdiri dari beberapa cara yang lazim digunakan dan prinsip kerja atau algoritma yang digunakan sama seperti pada metode steganography pada gambar. Audio digital berbeda dari suara analog tradisional dimana ini adalah sinyal diskrit dan bukan sinyal kontinu. Sinyal diskrit diciptakan dari sampling sinyal analog yang kontinu dengan rate tertentu. Sebagai contoh, sampling rate pada CD audo digital pada umumnya adalah 44 KHz (artinya dalam 1 detik ada sekitar 44000 sampel yang dimaninkan). Gambar berikut menggambarkan gelombang suara analog (kontinu) yang mengalami sampling untuk menghasilkan audio digital.



Gambar 2.2 Audio Digital

Berikut adalah beberapa teknik yang digunakan :

a. Low Bit Coding

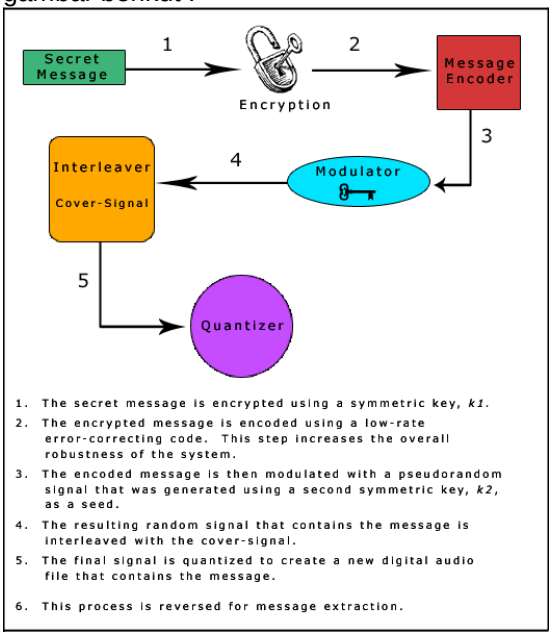
Cara ini lazim digunakan dalam teknik digital steganography yaitu mengganti LSB input setiap samplingnya dengan data yang dikodekan. Dengan metode ini keuntungan yang didapatkan adalah ukuran pesan yang disispkan relative besar, namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya noise.

b. Phase Coding

Metode kedua yang digunakan ini adalah merekayasa fasa dari sinyal masukan. Teori yang digunakan adalah dengan mensubstitusi awal fasa dari tiap awal segment dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari tiap awal segment ini dibuat sedemikian rupa sehingga setiap segmen masih memiliki hubungan yang berujung pada kualitas suara yang tetap terjaga. Teknik ini menghasilkan keluaran yang jauh lebih baik daripada metode pertama namun dikompensasikan dengan kerumitan dalam realisasinya.

c. Spread Spectrum

Metode-metode yang didasari oleh teknologi ini menyandikan pesan yang diinginkan agar tersembunyi. Untuk menyandikan, digunakan sebuah pseudorandom noise generator yang lebar untuk membuat sebuah barisan yang tersebar. Kemudian, sebuah skrema modulasi digunakan untuk memperluat spectrum yang sempit dari sebuat pesan dengan barisan yang tersebar, dengan demikian menyusun sinyal yang dibawa yang masuk ke dalam interleave dan ruang penyebar. Inner leaver juga dapat mempergunakan kunci untuk mendikte algoritma interleaving. Sinyal ini sekarang digabungkan dengan cover dari citra untuk menghasilkan citra stego, yang sudah dibagi-bagi dengan layak untuk memelihara dynamic range awal dari cover citra. Citra stego tersebut kemudian diteruskan kepada penerima pesan. Untuk lebih jelasnya, lihat gambar berikut :



Gambar 2.3 Spread Spectrum

d. Echo Hiding

Metode terakhir yang sering digunakan adalah menyembunyikan pesan melalui teknik echo. Teknik menyamarkan pesan ke dalam sinyal yang membentuk echo. Kemudian pesan disembunyikan dengan menvariasikan tiga parameter dalam echo yaitu besar amplitude awal, tingkat penurunan atenuasi, dan offset. Dengan adanya offset dari echo dan sinyal asli maka echo akan tercampur dengan sinyal aslinya, karena sistem pendengaran manusia yang tidak memisahkan antara echo dan sinyal asli. Keempat metode di atas memiliki kesamaan yaitu menggunakan kelemahan dari sistem pendengaran manusia. Maka dari itu teknik steganography dalam MP3 juga akan menggunakan kelemahan ini untuk menyembunyikan pesan.

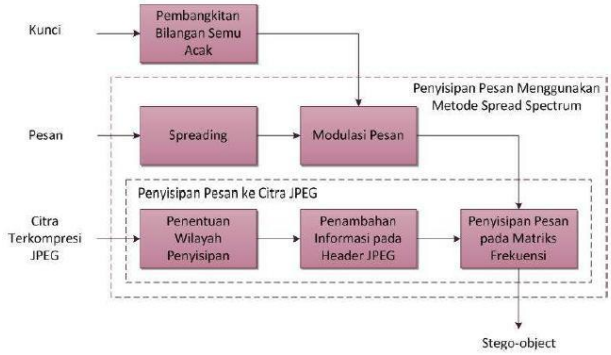
ANALIS DAN PEMBAHASAN

1. Analisis

Pada bagian ini akan dibahas mengenai proses penyisipan pesan, proses ekstraksi pesan, serta ukuran maksimum pesan yang dapat disisipkan. Terdapat juga analisis mengenai pembangkitan bilangan semu acak dan pengukuran kualitas dari citra.

a. Penyisipan Pesan

Sistem untuk menyisipkan pesan pada citra terkompresi JPEG membutuhkan masukan berupa citra terkompresi JPEG, pesan yang ingin disisipkan dan kunci yang akan digunakan untuk proses modulasi pesan. Skema penyisipan pesan dapat dilihat pada Gambar 1.



Gambar 3.1 Skema Penyisipan Pesan

Proses penyisipan pesan menggunakan metode Spread Spectrum ini terdiri dari tiga proses, yaitu spreading, modulasi, dan penyisipan pesan ke citra JPEG. Pada awalnya dilakukan proses spreading. Setelah itu dilakukan proses modulasi. Proses ini merupakan proses pengacakan pesan yang telah disebar dengan bilangan pseudonoise yang telah dibangkitkan menggunakan algoritma LCG. Panjang dari bilangan pseudonoise ini disesuaikan dengan panjang dari pesan.

Jika panjang pesan lebih kecil dari panjang bilangan pseudonoise, bilangan pseudonoise tersebut akan dipotong sesuai dengan ukuran pesan. Sebaliknya, jika panjang pesan lebih besar dari panjang bilangan pseudonoise, maka bilangan tersebut akan diulang sampai panjangnya sama dengan panjang pesan. Proses modulasi tersebut dilakukan dengan menggunakan fungsi XOR (Exclusive OR). Nilai yang dihasilkan dari proses modulasi inilah yang kemudian akan disisipkan ke dalam berkas JPEG.

Proses selanjutnya adalah penyisipan pesan ke dalam citra JPEG. Penyisipan pesan ke dalam citra terkompresi JPEG terdiri dari tiga proses, yaitu penentuan wilayah penyisipan, penambahan informasi pesan pada header JPEG, dan penyisipan pesan pada matriks frekuensi. Pada berkas JPEG terdapat matriks frekuensi berukuran 8 x 8 yang dapat disisipkan oleh pesan.

Setelah wilayah penyisipan didapatkan, selanjutnya dilakukan penambahan informasi pada header dari berkas JPEG yang dijadikan media penyisipan pesan. Informasi yang ditambahkan adalah nama berkas yang akan disisipkan, ukuran berkas yang akan disisipkan, wilayah penyisipan pesan, dan faktor bilangan pengali yang digunakan. Untuk keamanan, informasi tersebut dienkripsi sebelum ditambahkan pada header dari berkas JPEG. Informasi-informasi tersebut ditambahkan dengan menambahkan tag XML baru yang akan digunakan sebagai media penyimpanan informasi pada header berkas JPEG.

Setelah proses penambahan informasi selesai dilakukan, selanjutnya dilakukan

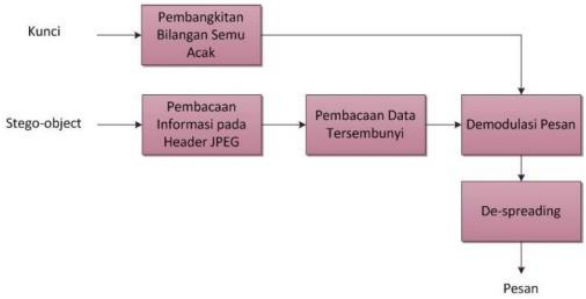
tahap terakhir dalam penyisipan pesan pada citra terkompresi JPEG. Tahap terakhir tersebut adalah penyisipan pesan pada matriks frekuensi. Pesan yang akan disisipkan dalam tahap ini adalah hasil dari proses modulasi yang telah dilakukan sebelumnya.

Penyisipan pesan pada matriks frekuensi dilakukan dengan cara menyisipkan bit pesan pada bit terakhir dari nilai yang terdapat di matriks frekuensi. Penyisipan tidak dapat dilakukan pada nilai 0, 1, dan 255 karena perubahan pada ketiga nilai tersebut dapat mengakibatkan berubahnya susunan matriks frekuensi. Penyisipan juga harus dilakukan sesuai dengan cara pembacaan matriks frekuensi, yaitu zig-zag.

Hal lain yang perlu diperhatikan dalam menyisipkan pesan pada matriks frekuensi adalah pembagian penyisipan yang merata pada seluruh matriks frekuensi yang terdapat pada berkas JPEG. Untuk itu penyisipan akan dilakukan secara selangseling berdasarkan jumlah matriks frekuensi yang ada pada berkas JPEG tersebut.

b. Ekstraksi Pesan

Sistem untuk mengekstraksi pesan pada citra terkompresi JPEG membutuhkan masukan berupa citra terkompresi JPEG yang telah disisipkan pesan dan kunci yang akan digunakan untuk proses demodulasi pesan. Skema penyisipan pesan dapat dilihat pada Gambar 2. Proses ekstraksi pesan menggunakan metode Spread Spectrum ini terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi, dan de- spreading.



Gambar 3.2 Skema Penyisipan Pesan

Proses pengambilan pesan dari matrks frekuensi diawalai dengan pembacaan informasi yang terdapat pada header JPEG ini dilakukan terhadap isi dari tag XML yang telah didefinisikan khusus sebelumnya. Adapun informasi yang didapatkan dari pembacaan ini adalah nama berkas yang disisipkan, ukuran berkas yang disisipkan, wilayah penyisipan pesan, dan faktor bilangan pengali yang digunakan.

Kemudian dilakukan pembacaan data tersembunyi dilakukan berdasarkan informasi wilayah penyisipan pesan yang didapatkan dari tahap sebelumnya, yaitu pembacaan informasi pada header JPEG. Pembacaan akan dilakukan secara berselang-seling pada matriks frekuensi yang terdapat pada citra dan berlangsung sampai data yang dibaca besarnya sama dengan informasi ukuran berkas yang disisipkan.

Setelah data tersembunyi berhasil dikumpulkan, dilakukan proses demodulasi terhadap data tersebut. Proses demodulasi ini melibatkan bilangan acak yang dibangkitkan dari kunci masukan menggunakan algoritma LCG. Adapun proses pembangkitan bilangan acak yang dilakukan pada tahap ekstraksi pesan sama seperti proses pembangkitan bilangan acak pada tahap penyisipan pesan.

Hasil dari proses demodulasi tersebut akan mengalami proses de-spreading. Proses dispreading ini adalah proses yang dilakukan untuk mendapatkan bit-bit dari pesan tersembunyi. Proses de-spreading ini bekerja menggunakan factor besaran pengali yang dimasukkan oleh pengguna pada proses penyisipan pesan.

c. Ukuran Maksimum Pesan yang Dapat Disisipkan

Pesan disisipkan kedalam LSB dari nilai yang terdapat pada matriks frekuensi. Ukuran pesan yang disisipkan bergantung pada 4 hal, yaitu banyaknya matriks frekuensi yang terdapat pada citra terkompresi JPEG yang menjadi media penyisipan pesan, banyaknya matriks yang merupakan header dari citra terkompresi JPEG, faktor besaran pengali -. yang dipilih, dan besar wilayah penyisipan pesan pada sebuah matriks frekuensi. Masing-masing berkas JPEG memiliki jumlah matriks frekuensi yang berbeda sesuai ukuran dari berkas JPEG tersebut, sedangkan factor besaran pengali -.

dapat diubah-ubah sesuai keinginan pengirim pesan.

d. Pembangkitan Bilangan Semu Acak

Pada steganografi, pembangkitan bilangan acak dapat digunakan untuk menentukan kunci penyisipan dan ekstraksi data dari berkas media. Komputer mampu menghasilkan bilangan semu acak (pseudorandom). Deret bilangan pseudorandom adalah deret bilangan bilangan yang kelihatan acak dengan kemungkinan pengulangan yang sangat kecil atau periode pengulangan yang sangat besar.

e. Pengukuran Kualitas Citra

Penilaian kualitas citra terkompresi JPEG dilakukan secara subjektif dan objektif. Penilaian subjektif dilakuan dengan cara melihat citra secara kasat mata. Penilaian objektif dilakukan dengan cara menghitung nilai PSNR (Peak Signal to Noise Ratio).

2. Pembahasan

Berdasarkan hasil analisis, perangkat lunak yang memiliki fungsi menyisipkan pesan dan ekstraksi pesan pada citra terkompresi JPEG menggunakan metode Spread Spectrum telah berhasil dikembangkan dengan baik. Selanjutnya, dilakukan pengujian untuk memeriksa kebenaran perangkat lunak serta menguji kinerja dari perangkat lunak tersebut. Untuk menguji kebenaran perangkat lunak dilakukan tiga buah kasus uji, yaitu menguji kebenaran proses penyisipan dan ekstraksi, menguji proses penggunaan kunci, dan menguji pengaruh dari penggunaan faktor bilangan pengali. Sedangkan untuk menguji kinerja perangkat lunak dilakukan pengujian terhadap dampak dari proses penyisipan pada citra.

a. Menguji kebenaran Proses Penyisipan dan Ekstraksi (Kasus 1)

Pengujian ini dilakukan dengan cara menyisipkan pesan ke dalam citra terkompresi JPEG, kemudian mengekstraksinya kembali. Citra yang menjadi media adalah citra pada Gambar 3 (stone.jpg). File pesan masukannya adalah sebuah file teks dan file gambar, yang isinya ditunjukkan pada Tabel 1. Kunci yang digunakan adalah 11, faktor bilangan pengali yang digunakan adalah 1 dan citra keluaran diberi nama baru yang sesuai dengan file pesan.

Gambar 3.3 Citra Media Penyisipan

Tabel 3.1 Isi File Penyisipan

Jenis File	Isi File
File Text	Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut
File Gambar	

Setelah proses penyisipan selesai, dilakukan proses ekstraksi dari masing-masing citra yang telah disisipkan pesan. Kunci dan faktor bilangan pengali yang digunakan sama dengan proses penyisipan, yaitu 11 dan 1, sehingga diharapkan pesan yang dihasilkan dari proses ekstraksi memiliki isi yang sama dengan pesan yang digunakan pada proses penyisipan. Isi dari file hasil ekstraksi dapat dilihat pada Tabel 2.

Tabel 3.2 Isi File Ekstraksi

Jenis File	Isi File
File Text	Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut
File Gambar	

Dari hasil pengujian terbukti bahwa perangkat lunak yang dibuat sudah berhasil menjalankan proses penyisipan dan ekstraksi dengan benar. Semua pesan yang menjadi masukan telah berhasil disisipkan, dan kemudian dapat diekstraksi dengan baik. Pesan yang diekstraksi sama dengan pesan yang asli, dan kunci yang digunakan pada proses penyisipan dan ekstraksi juga sama.

b. Menguji kebenaran Proses Penyisipan dan Ekstraksi (Kasus 2)

Pengujian ini dilakukan dengan cara melakukan ekstraksi dari citra hasil penyisipan pada kasus uji 1, namun dengan kunci yang berbeda, yaitu 22. Isi dari file hasil ekstraksi dapat dilihat pada Tabel 3.

Tabel 3.3 Isi File Ekstraksi dengan Kunci yang Salah

Jenis File	Isi File
File Text	뮲ぐl穎胠司볏□轡궝[□백 钌□齰즷譔員闐鼊'H用□柭張瘖 믿 [盰ゑ龠磡峅梵彨□햇힁
File Gambar	Gambar tidak dapat dimunculkan

Dari hasil pengujian, terbukti bahwa perangkat lunak yang dibuat dapat melakukan aspek penggunaan kunci dengan baik. Proses ekstraksi dengan kunci yang salah dapat ditangani, yaitu dengan menghasilkan pesan yang berbeda dengan pesan yang asli.

c. Menguji Pengaruh dari Penggunaan Faktor Bilangan Pengali (Kasus 3)

Pengujian ini dilakukan untuk menguji pengaruh dari penggunaan faktor bilangan pengali, yaitu dengan cara memasukkan faktor bilangan pengali yang berbeda dengan masukan pesan dan gambar yang sama dengan kasus uji 1. Pengujian akan berhasil apabila terdapat perbedaan ukuran maksimum pesan yang dapat disisipkan. Hasil dari pengujian ini dapat dilihat pada Tabel 4.

Jenis File	Faktor Bilangan Pengali	Isi File
File Text	1	stone_jpeg1.jpg
	2	stone_jpeg2.jpg
	3	stone_jpeg3.jpg
	4	Pesan tidak dapat disisipkan
File Gambar	1	stone_facebook1.jpg
	2	Pesan tidak dapat disisipkan

Tabel 4 Hasil Pengujian Kasus 3

Dari hasil pengujian, terbukti bahwa perangkat lunak yang dibangun penggunaan faktor bilangan pengali berpengaruh terhadap ukuran maksimum pesan yang dapat disisipkan. Semakin besar nilai dari faktor bilangan pengali, semakin kecil ukuran pesan yang dapat disisipkan. Hal ini dikarenakan pada proses penyisipan pesan dengan metode Spread Spectrum pesan akan digandakan sebanyak faktor bilangan pengali.

d. Menguji Dampak Penyisipan Pesan pada Citra (Kasus 4)

Pengujian ini dilakukan untuk menguji kualitas dari citra hasil penyisipan, yaitu dengan membandingkannya dengan citra yang asli. Pembandingan ini memakai masukan dari citra terkompresi JPEG yang telah melewati proses penyisipan pada Kasus uji 1, dan menggunakan dua cara perbandingan, yaitu subjektif dan objektif. Pengujian akan berhasil apabila dari masing-masing cara, didapatkan hasil seperti berikut:

1) Pada cara subjektif, citra dianggap mirip.
2) Pada cara objektif, nilai Peak Signal Noise Ration (PSNR) yang didapatkan berada diantara 30 dan 50. Hasil perhitungan nilai PSNR dapat dilihat pada Tabel 6.

Jenis File Pesan	Nilai PSNR (dB)
File Text	37.40943307
File Gambar	42.02490002

Pada cara subjektif, semua citra hasil penyisipan dianggap mirip dengan citra yang asli. Pada cara objektif, yaitu dari Tabel 5 dapat dilihat bahwa semua perbandingan memperoleh nilai Peak Signal $oise Ratio (PSNR) diantara 30 dan 50. Hal ini membuktikan bahwa proses penyisipan dengan metode Spread Spectrum ini tidak mengubah kualitas struktur citra secara signifikan.

KESIMPULAN

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut :

1. Telah berhasil dikembangkan perangkat lunak yang dapat melakukan steganografi pada citra terkompresi JPEG. Kebutuhan fungsional dari perangkat lunak, seperti proses penyisipan dan ekstraksi pesan, serta penggunaan kunci sudah dapat dilakukan dengan benar.
2. Metode Spread Spectrum sebagai metode penyisipan pesan sudah dapat dilakukan dengan benar, yaitu melakukan proses spreading terhadap pesan, modulasi pesan dengan kunci, dan penyisipan pesan dalam matriks frekuensi yang terdapat pada citra terkompresi JPEG.
3. Kualitas citra terkompresi JPEG yang dihasilkan bergantung dari besarnya ukuran pesan. Berdasarkan pengamatan yang dilakukan saat pengujian, citra JPEG yang disisipkan lebih banyak akan mengalami perubahan yang lebih besar.

DAFTAR REFERENSI

[1] Cole, Eric. 2003. *Hiding in Plainsight : Steganography and the Art of Covert Communication*. Wiley Publishing,Inc.

[2] Torrieri, Don. 2005. *Principles of Spread Spectrum Communications System*. Springer.