STUDI DAN IMPLEMENTASI STEGANOGRAFI METODE ALGORITMA DAN TRANSFORMASI PADA CITRA JPEG

Timothy John Pattiasina, ST., M.Kom.*

ABSTRAK

Steganografi adalah seni dan ilmu menulis atau menyemhunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. lstilah steganografi termasuk penyemhunyian data digital dalam komputer Ada beberapa metode steganografi, salah satunya adalah metode Algorithms and Transformation. Metode menyembunyikan data dalam fungsi matematika yang disebut algoritma *compression*. Dua fungsi tersebut adalah *Discrete Cosine Transformation* (DCT) dan *Wavelet Transformation*. Fungsi DCT dan Wavelet yaitu untuk mentransformasikan data dari satu tempat (domain) ke tempat (domain) yang lain. Fungsi DCT yaitu mentransformasi data dari tempat spatial (spatial domain) ke tempat fiekuensi (frequency domain).

Kata Kunci: Steganografi, DCT (Discrete Cosine Transform), Wavelet Transform, Algoritma dan Transformasi.

1. PENDAHULUAN

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak mengaksesnya, salah satunya adalah teknik steganografi. Teknik steganografi dilakukan dengan cara menyembunyikan pesan rahasia agar bagi orang awam tidak menyadari keberadaan dari pesan yang disembunyikan. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Pada penelitian kali ini, akan dijabarkan bagaimana jika steganografi diimplementasikan pada citra JPEG.

1.1. Latar Belakang

Teknik-teknik penyembunyian suatu file atau data saat ini berkembang pesat. Dahulu, orang mengenal teknik kriptografi, dimana istilah ini berasal dari akar kata Yunani kryptos dan gráphō, yang mempunyai arti "tulisan tersembunyi", dan telah ada hampir sepanjang kata-kata tertulis.

Steganografi sendiri 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”. Steganografi membutuhkan dua properti, yaitu media penampung dan data rahasia yang akan

* Staf Pengajar Program Studi S1-Teknik Informatika IKADO

disembunyikan, media penampung steganografi dapat berupa Image, Audio, ataupun Video.

Walaupun steganografi dapat dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda. Semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasiaan komunikasinya bukan pada datanya.

1.2. Perumusan Masalah

Perumusan masalah untuk penerapan steganografi dalam implementasinya dengan citra JPEG adalah sebagai berikut:

1. Bagaimana menyisipkan pesan atau informasi ke dalam sebuah *file image* agar tidak mudah diketahui oleh yang tidak berhak, tetapi mudah dibuka oleh yang berwenang?
2. Bagaimana menyisipkan pesan ke dalam sebuah *file image* dengan menggunakan metode Algoritma dan Trasformasi?
3. Apakah pengiriman pesan atau informasi dengan menggunakan teknik steganografi dapat lebih memaksimalkan tingkat keamanannya?
4. Bagaimana proses kompresi pada *file image JPEG?*
5. Bagaimana proses transformasi *image* setelah mengalami proses kompresi?

1.3. Batasan Masalah

Batasan-batasan masalah pada penelitian ini adalah sebagai berikut :

1. Objek penelitian difokuskan pada kerahasiaan komunikasinya bukan pada pesan atau data informasinya.
2. Media komunikasi yang dipakai adalah file *image JPEG.*
3. Metode yang dipakai adalah Algoritma dan Transformasi

1.4. Tujuan dan Manfaat Penelitian

Penelitian ini bertujuan untuk mempelajari cara menyisipkan data atau pesan pada *file image,* menganalisa dan mengetahui proses pengiriman pesan melalui file *image* dengan menggunakan metode Algoritma dan Transformasi, mengetahui tingkat keamanan pengiriman data atau pesan dengan menggunakan teknik steganografi, menganalisa dan mengetahui teknik kompresi *JPEG, serta m*enganalisa dan mengetahui proses transformasi *image* setelah mengalami kompresi.

Sedangkan manfaat yang didapatkan melalui penelitian ini adalah dapat ditingkatkannya keamanan dalam pengiriman suatu data atau pesan dalam berbagai aspek kehidupan yang menggunakan komputer sebagai mediatornya.

2. TINJAUAN PUSTAKA

Telah diketahui pada latar belakang penelitian ini, tentang latar belakang lahirnya steganografi. Untuk mengenal lebih lanjut mengenai steganografi, apa kaitannya dengan dunia pengolahan citra digital, serta metode algoritma dan transformasi pada citra JPEG, akan dibahas pada bab ini.

2.1. Pengolahan Citra Digital

Pengolahan citra digital dapat didefinisikan sebagai proses memperbaiki kualitas citra agar mudah diinterpretasi oleh manusia atau komputer. Teknik pengolahan citra dengan mentrasformasikan citra menjadi citra lain, contoh : pemampatan citra *(image compression).* Pengolahan citra merupakan proses awal *(preprocessing)* dari komputer visi.

Beberapa operasi pengolahan citra diantaranya adalah:

- Perbaikan Kualitas Citra
  - Tujuan dari perbaikan citra ini adalah memperbaiki kualitas citra dengan memanipulasi parameter-parameter citra.
- Pemugaran Citra (*Image Restoration*)
  - Tujuan dari pemugaran citra ini adalah untuk menghilangkan cacat pada sebuah citra. Operasi pemugaran citra dapat dilakukan dengan cara menghilangkan kesamaran *(debluring)* dan menghilangkan derau *(noise)* pada sebuah citra
- Pemampatan Citra (*Image Compression*)
  - Tujuan dari pemampatan citra ini adalah untuk merepresentasikan citra dalam bentuk yang lebih kecil sehingga, sehingga kebutuhan memori lebih sedikit namun dengan tetap mempertahankan kualitas gambar (misalnya dari *BMP* menjadi *,IPEG).*
- Segmentasi Citra (*Image Segmentation*)
  - Tujuan dari segmentasi citra adalah untuk memecah suatu citra ke dalam beberapa segmen dengan suatu kriteria tertentu. Biasanya segmentasi citra sangat erat hubungannya dengan pengenalan pola.
- Pengorakan Citra (*Image Analysis*)
  - Tujuan dari pengorakan citra adalah menghitung besaran kuntitatif dari citra untuk menghasilkan deskripsinya. Hal ini diperlukan untuk melokalisasi objek yang diinginkan dari sekelilingnya. Operasi pengorakan citra biasanya dilakukan cara pendeteksian tepi objek *(edge detection),* ekstraksi batas dan representasi daerah *(region).*
- Rekonstruksi Citra (*Image Reconstruction*)
  - Tujuan dari rekonstrukdi citra adalah untuk membentuk ulang objek dari beberapa citra hasil proyeksi.

2.2. Steganografi

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi 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 *steganography (steganografi)* berasal dari bahasa Yunani *steganos,* yang artinya "tersembunyi atau terselubung", dan *graphein,* "menulis".

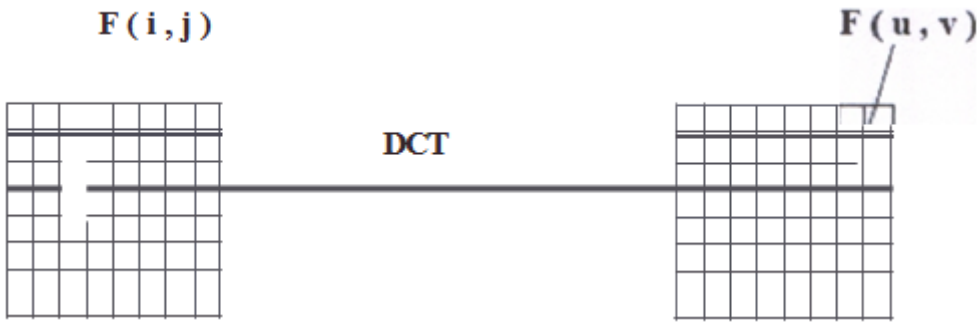
Kini, istilah steganografi termasuk penyembunyian data digital dalam *file- file* komputer. Contohnya, si pengirim mulai dengan *file* gambar biasa, lalu mengatur warna setiap *pixel* ke-100 untuk menyesuaikan suatu huruf dalam *alphabet* (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika isi tidak benar-benar memperhatikannya).

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format *file* digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan diantaranya:

- Format image : bitmap (bmp), gif, pcx, jpeg, dll.
- Format audio : way, voc, mp3, dll.
- Format lain : teks file, html, pdf, dll

Ada beberapa metode steganografi, salah satunya adalah metode *Algorithms and Transformation*. Metode menyembunyikan data dalam fungsi matematika yang disebut algoritma *compression.* Dua fungsi tersebut adalah *Discrete Cosine Transformation (DCT)* dan *Wavelet Transformation.* Fungsi *DCT* dan *Wavelet* yaitu mentransformasi data dari satu tempat *(domain)* ke tempat *(domain)* yang lain. Fungsi *DCT* yaitu mentransformasi data dari tempat *spatial (spatial domain)* ke tempat frekuensi *(frequency domain).*



Gambar Diagram DCT

Jangan terlalu khawatir jika tidak mengerti fungsi tersebut atau tepatnya bagaimana transformasinya. Pikirkan saja mereka dalam cara yang berbeda dari manipulasi dan mempresentasikan data. Ide dari semua ini berkenaan dengan *steganography* yaitu menyembunyikan *bit* data dalam *least significant* koefisien.

3. METODE ANALISA

Pada bab ini, akan dijabarkan metode yang digunakan di dalam penelitian ini, serta prosedur-prosedur dalam pengumpulan dan analisa data. Pada bab ini pulaakan diungkapkan hasil dari penelitian tersebut.

3.1. Metode Analisa

Penelitian tentang teknik penyembunyian pesan pada *image* yang difokuskan pada *image JPEG* (steganografi) dilakukan dengan cam mengumpulkan beberapa *paper* dari internet. Kumpulan *paper* yang diambil dari Internet tersebut kemudian dipelajari, dianalisa dan dirangkum sebagi bahan penelitian

Selain itu, teknik memperoleh data juga diambil dan berbagai *e-book* berformat *PDF* yang membahas tentang teknik kompresi *image* dan steganografi. Dart *e-hook* tersebut dipelajari dan diambil teori-teori teknik penyembunyian pesan (steganografi) yang menggunakan metode algoritma dan transformasi.

Variabel-variabel yang terkait pada penelitian ini adalah perbedaan proses penyandian *(encode* data tersembunyi) dan pembacaan sandi *(decode* data tersembunyi) yang merupakan proses penjabaran dari steganografi dengan metode algoritma dan transformasi. Dari variabel tersebut dapat diketahui bagaimana perbedaan proses *encoding* dan *decodingnya* walaupun perbedaan prosesnya tidak mengalami perbedaan yang signifikan.

Batas-batas penelitian ini adalah sebagai berikut :

1. Cara kerja penyandian *(encode)* steganografi dengan metode algoritma dan transformasi menggunakan *image JPEG.*
2. Cara kerja pembacaan sandi *(decoding)* steganografi dengan metode algoritma dan transformasi menggunakan *image JPEG.*

Poin-poin yang disebutkan di atas telah cukup mencakup cara kerja teknik penyembunyian pesan melalui *image JPEG* dengan metode algoritma dan transformasi secara keseluruhan karena pembahasan mengenai teknik kompresi *JPEG* dan steganografi sudah dapat dijelaskan secara keseluruhan

3.2. Prosedur Pengumpulan Data

Penelitian ini menggunkan prosedur pengumpulan data yang dijabarkan pada poin-poin di bawah ini :

a) Mencari artikel-artikel yang membahas segala sesuatu tentang teknik steganografi terutama yang membahas tentang metode algoritma dan transformsi. Artikel-artikel dicari pada internet, karena algoritma ini tidak dijabarkan dalam artikel-artikel majalah dan sebagainya.
b) Mencari buku-buku yang membahas tentang teknik penyembunyian pesan (steganografi) khusunya yang membahas tentang metode algoritma dan transformasi. Buku yang dicari berupa *e-book* yang format *PDF* tetapi tidak engurangi isi *e-book* dengan isi dari buku aslinya. Hal ini dilakukan karena buku-buku tentang teknik penyembunyian pesan pada *image* terutama dengan metode algoritma dan transformasi sangat sulit untuk dicari. Kebanyakan buku tentang steganografi pada *image* pembahasannya ditekankan pada metode *LSB.*
c) Bertanya kepada pembuat artikel-artikel tersebut melalui forum tanya jawab. Forum tanya jawab dilakukan di intenet melalui situs dimana kita mengunduh *(Men-download)* artikel tersebut.

4. ANALISIS ALGORITMA

Pada bab analisa algoritma ini menjelaskan secara detail mengenai algoritma yang dipakai dalam steganografi dengan metode algoritma dan transformasi. Karena media yang digunakan adalah *Image .IPEG* maka sebelumnya perlu dijelaskan teknik kompresi *image JPEG.*

4.1. Kompresi Citra/*Image*

Kompresi citra adalah aplikasi kompresi data yang dilakukan terhadap citra digital dengan tujuan untuk mengurangi redundansi dari data-data yang terdapat dalam citra sehingga dapat disimpan atau ditransmisikan secara efisien.

Ada dua teknik dalam teknik kompresi citra/ *image*, diantaranya adalah :

1. *Lossy Compression:* Teknik ini dilakukan dengan tujuan untuk merubah ukuran *file* agar menjadi lebih kecil dengan cara menghilangkan beberapa informasi dalam citra asli. Teknik ini mengubah detail dan warna pada *file* citra menjadi lebih sederhana tanpa terlihat perbedaan yang mencolok dalam pandangan manusia, sehingga ukurannya menjadi lebih kecil. Biasanya digunakan pada citra foto atau *image* lain yang tidak terlalu memerlukan detail citra, dimana kehilangan *bit rate* foto tidak berpengaruh pada citra.
2. *Loseless Compression*
   Teknik kompresi citra dimana tidak ada satupun informasi citra yang dihilangkan. Biasa digunakan pada citra medis. Metode *loseless* meliputi *Run Length Encoding, Entropy Encoding (Huffman, Aritmatik),* dan *Adaptive Dictionary Based (LZW).*

Ada hal-hal penting yang harus diperhatikan dalam teknik kompresi citra, diantaranya adalah:

a) Scalability/ Progressive Coding/ Embedded Bitstream
   Scalability adalah kualitas dari hasil proses pengkompresian citra karena manipulasi *bitstream* tanpa adanya dekompresi atau rekompresi. Biasanya dikenal pada *loseless codec*. Contohnya pada saat *preview image* sementara *image* tersebut *di-download.* Semakin baik *scalability,* makin bagus *preview image*

b) Region of Interest Coding
   Region of interest coding adalah daerah-daerah tertentu *di-encode* dengan . kualitas yang lebih tinggi daripada yang lain.

c) Meta Information
   Meta information adalah *image* yang dikompresi juga dapat memiliki *meta information* seperti statistik warna, tekstur, *small preview image,* dan *author* atau *copyright information.*

Dalam kompresi *image* terdapat standar pengukuran *error (Galat)* kompresi. yang pertama disebut *MSE (Mean Square Error)* yaitu sigma dari jumlah *error* antara citra hasil kompresi dan citra asli. *MSE,* dapat dirumuskan sebagai berikut :

$$MSE = \frac{1}{NxM} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2$$

Rumus Means Square Error

Dimana:

- I(x,y) adalah nilai *pixel* di citra asli
- I'(x,y) adalah nilai *pixel* pada citra hasil kompresi
- M,N adalah dimensi *image*

Dan yang kedua yaitu *Peak Signal to Noise Ratio (PSNR),* untuk menghitung *peak error*. Untuk menghitung *PSNR* dapat dirumuskan sebagai berikut:

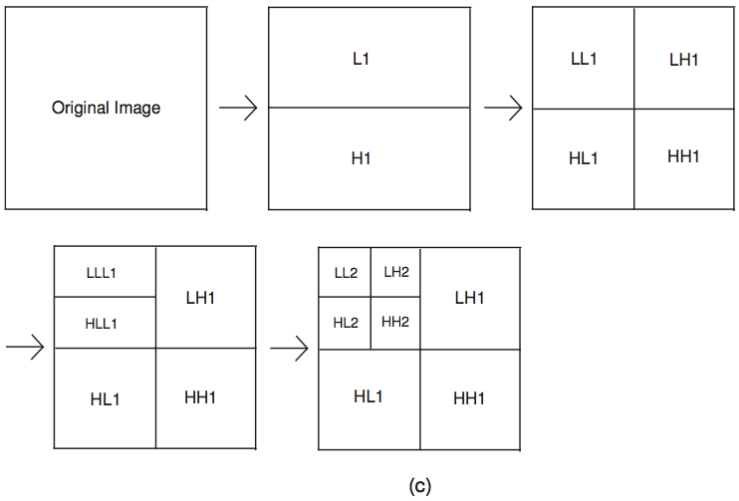
$$PSNR = 20 \log_{10} \left(\frac{255}{RMSE} \right),$$

$$RMSE = \sqrt{\frac{\sum_{x=1}^{512} \sum_{y=1}^{512} [f(x, y) - g(x, y)]^2}{512^2}}$$

Rumus *Peak Signal to Noise Ratio*

Nilai *MSE* yang rendah akan lebih baik, sedangkan nilai *PSNR* yang tinggi juga akan lebih baik.

Algoritma umum untuk melakukan kompresi *image* adalah menentukan *bitrate* dan toleransi *distorsi image* dari inputan *user* kemudian melakukan pembagian data *image* ke dalam bagian-bagian tertentu sesuai dengan tingkat kepentingan yang ada *(classifying)* yaitu menggunakan salah satu teknik: *DWT (Discreate Wavelet Transform)* yang akan mencari frekuensi nilai *pixel* masing-masing, menggabungkannya menjadi satu dan mengelompokkannya, seperti terlihat pada gambar berikut:



(c)

Dimana

LL : Low Low Frequency (most importance)
HL : High Low Frequency (lesser importance)
LH : Low High Frequency (more lesser importance)
HH : High High Frequency (most less importance)

Setelah melakukan *classifiying* kemudian dilakukan Pembagian bit-bit di dalam masing-masing bagian yang ada *(bitallocation).* Setelah itu dilakukan proses kuantisasi. Proses kuantisasi sendiri terbagi menjadi dua macam yaitu kuantisasi *scalar* dan kuantisasi *vector*. Kuantisasi *scalar* dilakukan dengan cara data-data yang tersedia dikuantisasi sendiri-sendiri sedangkan kuantisasi *vector* dilakukan dengan cara data-data dikuantisasi sebagai suatu himpunan nilai-nilai *vector* yang diperlukan sebagai nilai kesatuan. Dan langkah terakhir dalam proses kompresi *image* adalah melakukan pengkodingan untuk masing-masing bagian yang sudah dikuantisasi tadi dengan menggunakan teknik *entropy coding (Huffman dan aritmatik)* dan menuliskan ke dalam file hasil

4.2. Steganografi menggunakan Metode Algoritma dan Transformasi

Kunci dari metode ini adalah seperti pada kompresi *file* gambar berformat *JPEG*. *File* gambar berformat *JPEG* memiliki kualitas gambar yang relatif tinggi namun dengan ukuran *file* yang tidak terlalu besar karena telah melalui proses kompresi dengan sebuah algoritma dan transformasi matematis, sehingga informasi gambar tersebut dapat disimpan dengan ukuran *file* yang kecil dengan tetap mempertahankan kualitasnya. Algoritma kompresi dan transformasi matematis *JPEG* ini memungkinkan sebuah informasi disimpan sebaik dan seefisien mungkin. Sebuah *file* rahasia dapat disisipkan ke dalam sebuah *file* gambar yang tidak melalui proses kompresi seperti format *TIFF,* misalnya dengan menggunakan algoritma *JPEG* ini. Sehingga setelah melalui proses ini akan didapatkan *file* gambar berformat *TIFF* tadi berubah menjadi berformat *JPEG* dengan disertai "sesuatu" di dalamnya.

4.2.1. Embedding Data

Data embedded, yang tersembunyi kedalam suatu gambar membutuhkna dua *file.* Pertama adalah gambar asli yang belum modifikasi yang akan menangani informasi yang tersembunyi, yang disebut *cover image. File* kedua adalah informasi pesan yang disembunyikan. Suatu pesan bisa berupa *plaintext, chipertext,* gambar yang lain, atau apapun yang dapat di tempelkan kedalam *bit stream.* Ketika dikombinasikan, *cover image* dan pesan yang ditempelkan membuat *stego-image.* Suatu *stego-key* (suatu *password* khusus) juga bisa digunakan secara tersembunyi, pada saat *decode* selanjutnya dari pesan.

Kebanyakan *software steganography* tidak mendukung atau tidak direkomendasi menggunakan gambar *JPEG,* tetapi sebagai gantinya direkomendasikan menggunakan gambar *lossless 24-bit* seperti *BMP.* Alternatif terbaik berikutnya untuk gambar *24-bit* adalah 256 warna atau gambar *gray scale.* Secara umum ditemukan pada interne atau file *GIF.*

4.2.2. Rahasia Didalam Gambar Digital

Banyak cara untuk menyembunyikan informasi di dalam gambar. Untuk menyembunyikan informasi, penyisipan pesan yang langsung bisa *meng-encode* setiap *bit* dari informasi dalam gambar atau menempelkan pesan secara selektif dalam area *"noisy"* yang menggambarkan area yang kurang diperhatikan, dimana ada banyak variasi warna natural. Pesan bisa juga terserak secara acak sepanjang gambar. Pola redundansi *encoding "wallpapers"* menutup gambar dengan pesan.

Sejumlah cara yang ada untuk menyembunyikan informasi dalam gambar digital dengan pendekatan yang umum termasuk:

a. Penyisipan Least Significant Bit (LSB)

   Penyisipan *Least Significant Bit (LSB)* adalah umum, pendekatan yang sederhana untuk menempelkan informasi didalam suatu file *cover.* Sayangnya, hal itu sangat peka untuk kejadian yang melalaikan manipulasi gambar. Mengkonvert suatu gambar dari format *GIF* atau *BMP ,* yang merekonstruksi pesan yang sama dengan yang asli *(lossless compression)* ke *JPEG* yang *lossy compression,* dan ketika dilakukan kembali akan menghancurkan informasi yang tersembunyi dalam *LSB.*

b. Masking dan Filtering

Tehnik *masking dan filtering*, selalu hanya terbatas ke gambar *24-bit* dan *gray-scale*, informasi disembunyikan dengan menandai suatu gambar dalam cara sama *paper watermark.* Tehnik *watermarking* bisa di aplikasikan dengan resiko rusaknya gambar dalam kaitannya dengan *lossy compression* sebab mereka lebih menyatu ke dalam gambar.

c. Algoritma dan Transformasi

Metode Algoritma dan transformasi adalah salah satu metode untuk memanipulasi *LSB.* Cara ini cepat dan mudah untuk menyembunyikan informasi tetapi sangat peka untuk perubahan hasil yang kecil dari pemerosesan gambar atau *lossy compression.* Seperti kompresi yang merupakan kunci keuntungan dari gambar *JPEG* yang mempunyai kelebihan dari format yang lain. Gambar dengan kualitas warna yang tinggi dapat disimpan dalam *file* yang *relative* kecil menggunakan metode kompresi *JPEG,* sehingga gambar *JPEG* menjadi lebih berlimpah pada Internet.

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.* Dengan menggunakan rumus sebagai berikut:

$$F(u,v) = 0.25 * C_u C_v \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos\left(\frac{(2x+1)\,u\,\pi}{16}\right) \cos\left(\frac{(2y+1)\,v\,\pi}{16}\right)$$

Where:

$$C_u = \frac{1}{\sqrt{2}} \text{ for } u = 0 \text{ otherwise } C_u = 1$$

$$C_v = \frac{1}{\sqrt{2}} \text{ for } v = 0 \text{ otherwise } C_v = 1$$

Rumus Menghitung Koefisien DCT

Setelah koefisien-koefisien diperoleh, dilakukan proses kuantisasi.

Sebagai contoh, berikut merupakan algoritma sederhana untuk menyembunyikan pesan di dalam *image JPEG* dengan menggunakan *DCT:*

Pseudo Code* Steganografi dengan *DCT

```
1: WHILE (masih ada data untuk di-embed) do
2:    ambil koefisien DCT selanjutnya dari cover image
      (DCT)
3:    IF koefisien < nilai treshold then
4:       ambil bit selanjutnya dari pesan
5:       ganti bit koefisien DCT dengan bit pesan
         tersebut
6:    END IF
7:    masukkan DCT ke stego (invers DCT)
8:    END WHILE
```

Dari potongan *pseudo code* di was dapat dianalisa menjadi beberapa poin sebagai berikut:

1. Ambil koefisien *DCT* dari *image* asli
2. Selanjutnya dibandingkan antara koefisien *DCT* dengan nilai *threshold* pada *image* asli
3. Apabila nilai koefisien *DCT* lebih kecil daripada koefisien *threshold,* maka akan diambil *bit* dari pesan. Selanjutnya *bit* dari pesan itu digunakan untuk menggantikan koefisien *DCT*. Penggantian *bit* dari pesan dilakukan sampai nilai koefisien *DCT* tidak ada yang lebih kecil dari nilai *Threshold*
4. Proses ini dilakukan sampai data sudah tidak ada yang bias di *embedding*.
5. Terbentuklah *file Stego (image* yang sudah disisipi pesan).

5. UJI COBA

Pada bab uji coba ini dilakukan pegujian steganografi dari bermacam-macam segi. Namun tidak semua dijelaskan dalam bab ini. Hal-hal yang perlu diuji secara detail meliputi, tampilan visual antara *cover data* dan *stego data,* perbandingan ukuran *cover data* dan *stego* data dan lain sebaginya.

5.1. Membandingkan Tampilan Visual Cover Stego dan Stego Data

Perbandingan tampilan gambar pada antara *stego data* dengan *cover data* dapat dilihat pada gambar di bawah ini:

Gambar Stego Data dan Cover Data

Secara kasat mata, kedua gambar tersebut tidak memiliki perbedaan. Apabila gambar pada *stego data* dan *cover data* dibesar sampai 8x pada area yang sama, hasilnya akan terlihat seperti pada gambar berikut ini:

Gambar Cover dan Stego Zoom 8x

Dengan melakukan perbesaran beberapa kali maka tampak perbedaan visual walaupun tidak terlalu mencolok. Hal ini menunjukkan steganografi dengan naenggunakan metode algoritma dan transformasi terbukti aman.

5.2. Membandingkan Ukuran Antar File Stego dan File Cover Data

Setelah menguji melalui tampilan visual .*JPEG* memiliki ukuran *file* sebesar 49,168 bytes. Sedangkan *cover data* memiliki ukuran sebesar 48,558 *bytes.* Hal ini menunjukan bahwa terdapat perubahan atau manipulasi terhadap *cover-data* sehingga terdapat pertambahan sebesar 610 *bytes* pada *stego data.* Selama pihak lain memiliki *file* gambar yang asli maka hal ini akan menimbulkan kecurigaan. Hasil uji secara lengkap dapat dilihat pada tabel di bawah ini :

Tabel Uji Berdasarkan Ukuran File

Cover Data	Pesan Rahasia	Ukuran Stego Data	Ukuran Cover Data
Way	Jpeg	217672	217672
Way	Way	217672	217672
Jpeg	Txt	49168	48558
Jpeg	Jpeg	49288	48558
Jpeg	Way	49320	48558
Bmp	Jpeg	1368890	136890

Melalui tabel tersebut dapat terlihat bahwa perbedaan ukuran *file* hanya terjadi pada kasus ketika *cover data* yang digunakan berformat *jpeg.* **Oleh** karena itu dapat disimpulkan bahwa *steghide* (proses steganografi) lulus uji 2 hanya untuk *cover data* berformat *jpeg. Jpeg* merupakan *file* gambar terkompresi. Setelah dilakukan proses *stego system* dan kemudian hasil proses dituliskan pada *file, steghide* perlu melakukan kompresi sehingga didapatkan ukuran *file* yang mendekati *file* aslinya, sesuai karakteristik dari *file jpeg.* Hanya saja, proses kompresi tidak dilakukan secara sempurna sehingga terjadi perubahan ukuran file.

5.3. File Txt yang Diselipkan pada File JPEG

Pengujian dilakukan terhadap *file* tesF2jpeg. Proses ekstraksi *file* **sebelum** dikenakan manipulasi akan menghasilkan *file* teks bernama daftarpustaka2.txt. *File* teks tersebut seharusnya memiliki isi yang sama denganfi/e daftarpustaka.txt. Berikut perintah yang digunakan pada steghide untuk melakukan ekstraksi :

```
steghide extract -sf tesF2.jpg -xf

daftarpustaka2.txt -v
```

Maksud perintah tersebut adalah file tesF2.jpg diekstrak untuk mendapatkan pesan rahasia. Pesan tersebut disimpan ke dalam sebuah *file* teks bernama daftarpustaka2.txt.

-v digunakan agar Steghide menampilkan informasi proses secara detail. Keluaran yang diperoleh melalui perintah tersebut adalah :

```
reading stego files "tesF2.jpg"...done

extracting data ...done

checking crc32 checksum... ok

writing extracted data to

"daftarpustaka2.txt"_done
```

Berikut isi file daftarpustaka2.txt yang sama dengan pesan rahasia yang disembunyikan pada file tesF2.jpeg :

1 Ross J. Anderson. Stretching the Limits of • Stegaziography. Iii Ross J. Anderson, editor. Information Hidutg. First Interzia ti on al 1.Vorkshop. x-o inane- 1174 of Lecture Notes in Computer Science. pages 39-48 Springer. 1996.
2. Rainer B oluue and Andreas 'Westfeld. Exploiting Preserved Statistics *for* Stegamilysis. 1tx Jessica J. Fridrich. editor. Information Hiding. 6th International NVorkshop. s-tillime 3200 *of* Lecture Notes in Computer Science. Springer. *2004*.
3. Elke Franz. Steganography Preserving Statistical Properties. In F.A.P. Petitcolas. editor. Information Hiding. 5th International 'Workshop. volume 2578 of Lecture Notes in Computer Science. pages 278-294. Springer. 2003.
•. Jessica Fridrich_ /s/lirc>slax- Circ iljatra. and Dam id Souk al. Higher—order statistical stegtmalysis of palette images In Proceedings of the Elecnonic Imaging SPIE Santa Clara_ CA. **January** 2003. pages 17S-190. 2003.

Picture File TestF2.Jpeg

Gambar Image dan Text File yang Disembunyikan

6. KESIMPULAN DAN SARAN

Dari penelitian tentang penyembunyian pesan pada *image* (steganografi) dengan metode algoritma dan transformasi dapat diambil beberapa kesimpulan dan saran.

6.1. Kesimpulan

Dari pembahasan pada bab-bab sebelumnya, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. *File* yang disisipkan dalam sebuah *image* tidak akan tampak oleh kasat mata dan sangat sulit terdeteksi karena *cover image* dan *stego* image tidak tampak adanya perbedaan.
2. *File JPEG* merupakan *file* yang tepat untuk metode algoritma dan transformasi karena hasil *file* yang telah dikompresi tidak mengalami penurunan kualitas *image* sehingga kerahasiaan dalam megirimkan pesan tersembunyi akan semakin kuat.

6.2. Saran

Adapun saran dari penelitian ini dapat dijabarkan sebagai berikut:

1. *Media yang digunakan* (image) *yang digunakan adalah* image *dengan format* JPEG. *Hal ini dikarenakan kualitas* image *yang tidak berubah meskipun habis ditransformasi*.
2. Pesan yang disisipkan lebih baik berupa *file teks* atau *image* karena proses pengidentifikasian bagi yang berkepentingan bisa dilakukan dengan lebih mudah dan lebih terjamin kerahasiaannya.

7. DAFTAR PUSTAKA

Ariyus, Deny. *Kriptografi Keamanan Data dan Komunikasi*. Graha Ilmu, 2006

Lisa Marvel, Charles Bocelet, and Charles Retter, *"Spread Spectrum image Steganography". 2005*

Munir, Rinaldi. *Kriptografi: text.* Informatika. 2006

Sayood, Khalid, *Lossless Compression Handbook,* Academic Press, 2003

http://id.wikipedia.org/wiki/Steganografi, *Wikipedia "Steganografi"* (diakses pada: 12 April 2009, pukul 15.55 WIB)

http://www.indoskripsi.com , *"Pembuatan Aplikasi Steganografi"* (diakses pada: 14 April 2009, pukul 18.05 WIB)

http://www.whatis.com **,** *"What is Steganography ?"* (diakses pada: 20 April 2009, pukul 10.38 WIB)