STEGANOGRAFI PADA MEDIA VIDEO DIGITAL DENGAN MENGGUNAKAN METODE FFT (*FAST FOURIER TRANSFORM*) DAN LSB (*LEAST SIGNIFICANT BIT*)

Oleh :

RIZKI AYUS GUSMAYUDA
(10103150)

gusmayuda@yahoo.com

Pembimbing I : Santi Novani, S.Si.,M.T.
Pembimbing II : Irfan Maliki, S.T.

Fakultas Teknik dan Ilmu Komputer
Jurusan Teknik Informatika
Universitas Komputer Indonesia

Abstrak

Perkembangan teknologi saat ini tidak hanya dimanfaatkan untuk keperluan positif. Hal ini sejalan dengan semakin berkembang pula kejahatan sistem informasi. Dengan berbagai cara, banyak yang mencoba mengakses informasi yang bukan hak mereka. Contohnya seperti pengiriman data rahasia yang harus melalui berbagai tangan terlebih dahulu, tentu saja data tersebut harus disembunyikan. Oleh karena itu, diperlukan pula pengamanan sistem informasi yang tangguh.

Salah satu teknik yang digunakan untuk melindungi informasi dari orang yang tidak berhak adalah steganografi. Steganografi adalah suatu cara untuk melindungi informasi dengan cara menyembunyikan data digital pada media digital lainnya sehingga keberadaan informasi rahasia tersebut tidak diketahui oleh indera manusia. Media pembawanya dapat berupa teks, suara, gambar, video, dan lainnya. Kebutuhan penyembunyian data dalam jumlah besar membutuhkan media pembawa yang cukup besar juga. Maka pemilihan file video sebagai media steganografi merupakan langkah yang tepat untuk mengakomodasi kebutuhan tersebut.

Kata kunci: steganografi, video.

BAB I PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi saat ini tidak hanya dimanfaatkan untuk keperluan positif. Hal ini sejalan dengan semakin berkembang pula kejahatan sistem informasi. Dengan berbagai cara, banyak yang mencoba mengakses informasi yang bukan hak mereka. Contohnya seperti pengiriman data rahasia yang harus melalui berbagai tangan terlebih dahulu, tentu saja data tersebut harus disembunyikan. Oleh karena itu, diperlukan pula pengamanan sistem informasi yang tangguh.

Salah satu teknik yang digunakan untuk melindungi informasi dari orang yang tidak berhak adalah steganografi. Teknik steganografi digunakan pertama kali oleh bangsa Yunani kuno. Steganografi adalah suatu cara untuk melindungi informasi dengan cara menyembunyikan data digital pada media digital lainnya sehingga keberadaan informasi rahasia tersebut tidak diketahui oleh indera manusia.

Keterbatasan kemampuan indera manusia dimanfaatkan dalam steganografi untuk menyembunyikan data. Media pembawanya dapat berupa teks, suara, gambar, video, dan lainnya. Kebutuhan penyembunyian data dalam jumlah besar membutuhkan media pembawa yang cukup besar juga. Maka pemilihan *file* video sebagai media steganografi merupakan langkah yang tepat untuk mengakomodasi kebutuhan tersebut.

1.2 Identifikasi masalah

Bedasarakan latar belakang masalah di atas dapat diidentifikasi bagaimana membangun suatu aplikasi steganografi pada media video dengan menggunakan metode *(FFT) Fast Fourier Transform* dan *(LSB) Least Significant Bit*.

1.3 Maksud dan tujuan

Maksud dari penulisan tugas akhir ini adalah untuk membuat aplikasi yang dapat menyisipkan suatu data digital penting kedalam media video, dan mengekstrak kembali data digital tersebut, sedangkan tujuan dari penulisan tugas akhir ini adalah untuk menyembunyikan suatu data penting atau rahasia kedalam suatu media video tanpa menyebabkan perubahan besar pada kualitas media pembawanya sehingga tidak mudah terlihat oleh mata manusia.

1.4 Batasan masalah

Dalam penulisan tugas akhir ini diberikan batasan masalah agar dalam penjelasannya nanti akan lebih mudah, tidak keluar dan menyimpang, terarah, dapat dipahami dan sesuai dengan yang diharapkan serta terorganisasi dengan baik.

Adapun batasan masalah perancangan dan pembangunan tugas akhir ini antara lain :

1. Sistem hanya melibatkan proses penyisipan dan pengekstrakan.
2. Penyimpanan informasi dalam video ini dilakukan pada kumpulan gambar yang bergerak saja, tidak melibatkan audio
3. *File* masukan dan keluaran untuk perangkat lunak berupa *file* video jenis Microsoft AVI
4. Ukuran data yang disisipkan lebih kecil dari ukuran media pembawa, kurang lebih perbandingannya 1 bit sisip untuk 1 byte pembawa.
5. Metode yang digunakan adalah *(FFT) Fast Fourier Transform* untuk merubah data yang akan disispkan.
6. Metode yang digunakan untuk menyisipkan data yang sudah dirubah adalah *(LSB) Least Significant Bit*

1.5 Metodologi penelitian

Metodologi penelitian yang dipakai dalam penyusunan tugas akhir ini dan sebagai penunjang dalam membangun aplikasi ini adalah sebagai berikut:

1. Tahap pengumpulan data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Wawancara

Wawancara adalah salah satu cara mengumpulkan data dengan cara mewawancarai sumber informasi. Tujuan dari wawancara ini adalah untuk mendapatkan data yang akurat dari sumbernya secara langsung.

b. Studi Pustaka

Studi pustaka ini tujuannya adalah untuk mendapatkan referensi mengenai tugas akhir dari buku lain, jurnal, situs, dan paper sebagai sumber untuk landasan teori.

2. Tahap pembangunan perangkat lunak

Teknik analisis data dalam pembuatan tugas akhir ini menggunakan metode *waterfall*, yang meliputi beberapa proses diantaranya:

a. Analisis

Merupakan tahap menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek.

b. Design

Tahap penerjemahan dari data yang dianalisis kedalam bentuk yang mudah dimengerti oleh user.

c. Coding

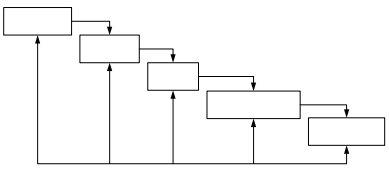
Tahap penerjemahan data atau pemecahan masalah yang telah dirancang keadalam bahasa pemrograman tertentu.

d. Pengujian

Merupakan tahap pengujian terhadap aplikasi yang dibangun.

e. Maintenance

Tahap akhir dimana suatu aplikasi yang sudah selesai dapat mengalami perubahan–perubahan atau penambahan sesuai dengan permintaan *user*.



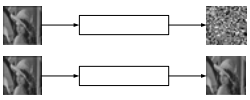
Gambar 1.1 *Waterfall model*

BAB II LANDASAN TEORI

2.1 Steganografi

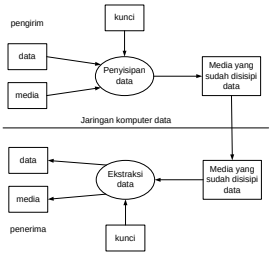
Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata steganorafi berasal dari Bahaya Yunani yang berarti “tulisan tersembunyi” (*covered writing*). Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi berbeda dengan kriptografi, di

mana pihak ketiga dapat mendeteksi adanya data (*chipertext*), karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan, tetapi dapat dikembalikan ke bentuk semula. Ilustrasi mengenai perbedaan kriptografi dan steganografi dapat dilihat pada gambar 2.2.



Gambar 2.2. Ilustrasi kriptografi dan steganografi pada citra digital.

Steganografi membahas bagaimana sebuah pesan dapat disisipkan ke dalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem indera manusia seperti mata dan telinga. Dengan adanya keterbatasan inilah, metoda steganografi ini dapat diterapkan pada berbagai media digital. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi di sini sebatas oleh kemampuan indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya. Ilustrasi mengenai proses steganografi dapat dilihat pada gambar 2.3.



Gambar 2.3. Diagram Sistem Steganografi

Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Sedangkan data rahasia yang disembunyikan dapat berupa berkas apapun. Media yang telah disisipi data disebut stegomessage. Proses penyembunyian data ke dalam media disebut penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi. Proses tersebut dapat dilihat pada gambar 2.4. Penambahan kunci yang bersifat opsional dimaksudkan untuk lebih meningkatkan keamanan.



Gambar 2.4. Proses penyisipan dan ekstraksi dalam steganografi

2.1.1. Steganografi pada video

Seperti dikatakan sebelumnnya, video merupakan kumpulan dari image yang “bergerak”, jadi sebagian besar metode yang digunakan pada image steganography dapat digunakan pada video steganography. Dapat dikatakan bahwa video steganography merupakan turunan dari image steganography. Pada video steganography ini, menggunakan metode transformasi Fast Fourier Transform. Hal ini dikarenakan modifikasi LSB akan mengasilkan stego yang berukuran sangat besar sedangkan metode masking dan filtering akan mengubah tampilan visual dari video secara langsung.

Untuk menyembunyikan pesan pada cover video, prinsipnya sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image cover video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan diganti dengan bit-bit data pesan yang akan disembunyikan. Setelah seluruh pesan di-embed, koefisien tadi ditransformasi balik untuk menghasilkan stego video. Untuk mengekstrak pesan dari stego video, prinsipnya juga sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image stego video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan merupakan bit-bit data pesan yang telah disembunyikan dan akan ditulis ke file output yang berisi pesan yang disembunyikan tersebut.

Keuntungan dari video steganography adalah banyaknya data yang dapat disembunyikan di dalamnya, serta fakta bahwa video merupakan “streams” dari image-image menyebabkan adanya distorsi pada salah satu frame image tidak akan dilihat dengan mudah dengan mata manusia. Akan tetapi, semakin banyak data pesan yang disembunyikan, bukan hal yang mustahil jika perubahan pada video menjadi semakin mudah terlihat.

2.1.2. FFT (*Fast Fourier Transform*)

Citra pada umumnya digambarkan dalam dimensi spasial antara amplitude dengan posisi spasial dua dimensi. Dalam operasi analisis citra, seringkali dilakukan operasi konvolusi pada matriks (citra) yang berdimensi besar. Hal ini menjadi salah satu penghambat karena ketika dilakukan operasi konvolusi, maka dibutuhkan resource computer yang sangat besar

Agar operasi analisis citra dapat dilakukan dengan efisien, maka sebaiknya citra dirubah dahulu kedalam dimensi frekuensi. Hal ini sangat penting dilakukan terlebih dalam operasi yang mengunakan konvolusi karena konvolusi dalam dimensi spasial berarti perkalian produk

(dot product) dalam dimensi frekuensi. mempercepat waktu proses. Untuk melakukan transformasi dari dimensi spasial menjadi dimensi frekuensi, salah satunya adalah dengan menggunaka transformasi Fourier. Inti dari transformasi Fouries adalah memecah signal (citra) menjadi gelombang-gelombang sinusoidal dimana jumlahnya sama dengan signal asalnya.

Algoritma DFT standar tidak bagus jika digukanan pada citra berukuran besar, karena proses komputasinya memakan waktu yang lama. Untuk mempercepat proses transformasi, digunakan algoritma FFT (Fast Fourier Transform). Algoritma ini sangat cepat mengerjakan matriks yang berukuran besar. Perbedaan kompleksitas waktu DFT dengan FFT adalah

$$0(N^2) : 0(N^2 \log N)$$

Dengan FFT proses komputasi biasa direduksi dari N2 menjadi N log2N. Misalnya dengan menggunakan DFT kita akan melakukan transformasi sebanyak N=1024 titik, maka kita memerlukan perkalian sebanyak N2 =1.048.567. Sedangkan dengan menggunakan FFT perkalian yang diperlukan sebanyak N log2N = 5120 perkalian.

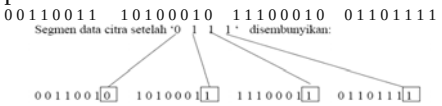
2.2. LSB *(Least Significant Bit)*

LSB (Least Significant Bit) Coding. Metoda ini merupakan metoda yang sederhana. Metoda ini akan mengubah nilai LSB (*Least Significant Bit*) komponen luminansi atau warna menjadi *bit* yang bersesuai dengan *bit* label yang akan disembunyikan. Memang metoda ini akan menghasilkan video rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai *bit* terakhir dari data. Metoda ini paling mudah diserang, karena bila orang lain tahu maka tinggal membalikkan nilai dari LSB-nya maka data label akan hilang seluruhnya.

1. Penyembunyian data dilakukan dengan mengganti *bit-bit* data di dalam segmen citra dengan *bit-bit* data rahasia. Metode yang paling sederhana adalah metode **LSB** (*Least Significant Bit Modification*).
2. Pada susunan *bit* di dalam sebuah *byte* (1 *byte* = 8 *bit*), ada *bit* yang paling berarti (*most significant bit* atau *MSB*) dan *bit* yang paling kurang berarti (*least significant bit* atau *LSB*).
3. Perhatikan contoh sebuah susunan *bit* pada sebuah *byte*:

   MSB → 11010010 ← *LSB LSB = Least Significant Bit*
   MSB = Most Significant Bit

   Bit yang cocok untuk diganti adalah *bit LSB*, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan 6 *byte* tersebut menyatakan warna merah, maka perubahan satu *bit* LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil.
4. Misalkan segmen data citra sebelum perubahan:

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

BAB III ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis masalah

Steganografi bertujuan untuk menyisipkan suatu data rahasia kedalam media digital agar data rahasia tersebut tidak bisa dilihat oleh pihak ketiga ataupun untuk identifikasi hakcipta dari suatu data digital. Kebanyakan steganografi diterapkan pada media text ataupun image yang ukurannya relatif kecil. Masalah yang timbul adalah bagaimana jika data rahasia tersebut berukuran besar, tentunya akan membutuhkan media pembawa yang relatif besar juga dan waktu yagn cukup lama untuk proses penyisipan tersebut. Pada sistem yang akan direalisaikan ini akan mengatasi masalah tersebut, yaitu menyisipkan file video dengan waktu yang singkat.

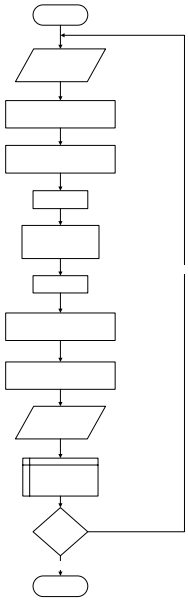
3.2. Cara Kerja Sistem

Sistem ini secara garis besar bekerja dengan tiga proses, yaitu proses penyisipan , pengekstrakan dan perhitungan nilai *Peak Signal-to-noise ratio* (PSNR). Karena penyisipan dilakukan pada domain frekuensi maka harus

dilakukan proses transformasi dari domain waktu ke domain frekuensi terlebih dahulu dengan menggunakan metode *FFT (Fast Fourier Transform).* Setelah proses transformasi, proses penyisipan dapat dilakukan, dalam sistem ini penyisipan menggunakan metode *LSB (Least Significant Bit).*

3.3.1. ProsesPenyisipan

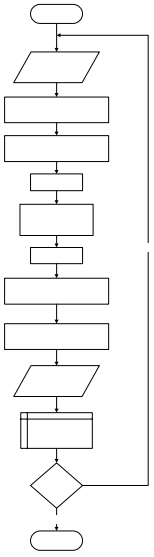
Proses dimulai dengan memasukan dua buah inputan, yang pertama video pembawa dan yang kedua video sisip, kemudian kedua video tersebut di pecah manjadi kumpulan frame yang berupa image, dengan catatan jumlah frame video sisip lebih kecil dari jumlah frame video pembawa, begitu juga dengan ukuran pixelnya. Kemudian tiap frame tersebut dibagi menjadi blok-blok. setelah itu blok video pembawa di transform dari domain waktu ke domain frekuensi menggunakan metode *Fast Fourier Transform (FFT)*, kemudian setiap blok video sisip disisipkan kedalam setiap blok video pembawa dengan mengunakan metode *Least Significant Bit (LSB).* Setelah semua blok dsisipkan kemudian di invers kembali dengan FFT, di gabungkan menjadi sebuah frame yang kemudian kumpulan frame tersebut digabungkan kembali sehingga menjadi video stego.



Gambar 3.1. Proses penyisipan

3.3.2. Proses Pengekstrakan

Proses ekstraksi dimulai dengan memasukan video hasil steganografi (sudah disisipi data video), kemudian video stego tersebut dipecah menjadi frame dalam bentuk image, dari image tersebut di rubah menjadi blok-blok yang akan ditransform menjadi domain frekuensi, setelah itu proses ekstraksi dimulai dengan mencari setiap frame yang telah memiliki data tersembunyi dan mengeluarkan data tersebut dengan mengembalikan nilai biner blok-blok frame pembawa tersebut ke asal. Kemudian semua frame yang telah dikeluarkan di invers transform dan di gabungkan kembali menjadi sebuah video ekstrak.



Gambar 3.6. Proses ekstraksi

BAB IV IMPLEMENTASI DAN PENGUJIAN

1.1 Implementasi

Pada tahap implementasi sistem, merupakan kegiatan yang dilakukan setelah tahap perancangan dibuat, tujuan yang ingin dicapai pada tahap ini agar dapat mengoperasikan hasil perancangan sistem yang telah dibuat serta mengetahui bagimana kinerja sistem yang dibangun setelah melalui proses pengujian.

Pada tahap ini, pengujian sistem dilakukan untuk mengetahui bagaimana sistem yang dibangun sesuai dengan yang direncanakan, seperti bagaimana proses penyisipan data rahasia dan pengekstrakan yang berupa video pada video pembawa dan video hasil penyisipan, serta membandingkan bagaimana hasil dari video yang asli dengan video yang telah disisipi sebuah data, analisa dapat dilihat dari segi kualitas warna, dan ukuran file video tersebut, selain itu tentunya bagaimana dengan pengoperasian dari sistem yang dibangun.

Aplikasi ini dibangun dengan menggunakan bahasa *visual Delphi 7.0*, dengan menggunakan sistem operasi *windows xp sp2*.

4.2 Pengujian

Pengujian yang dilakukan terhadap lima video sebagai media pembawa dan empat video yang disisipkan, hasil dari analisis terhadap pengujian yang telah dilakukan antara lain :

1. Ukuran file, resolusi dan jumlah frame video yang akan disisipkan harus lebih kecil dari video pembawanya.
2. Perbandingan video pembawa dan video sisipan agar proses penyisipan berhasil adalah 1 bit sisip untuk 1 byte pembawa.
3. Kecepatan dan keberhasilan proses penyisipan tergantung pada kemampuan hardware.
4. Format video yang bisa diproses hanya format microsof t AVI.
5. Proses penyisipan ini dapat menjamin kerahasiaan dari video, karena perubahan terhadap video yang telah mengalami penyisipan tidak terlalu besar sehingga tidak akan terlihat oleh mata manusia.

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisa dan pembahasan yang telah diuraikan pada bab-bab sebelumnya, maka penulis dapat menarik beberapa buah kesimpulan sebagai berikut :

1. Proses penyisipan dan pengekstrakan pada media video (Microsoft AVI) dengan metode *FFT* dan *LSB* berhasil dilakukan.
2. Video hasil penyisipan tidak mengalami perubahan kualitas yang *significant*, sehingga tidak dapat terlihat oleh mata manusia dan aman untuk berpindah tangan selama tangan yang tidak berhak tersebut tidak memiliki aplikasi steganografi yang di bangun ini.
3. Untuk melakukan penyisipan, ukuran *file*, resolusi dan jumlah *frame* video yang akan disisipkan harus lebih kecil dari video pembawanya, perbandinganya 1 bit sisip untuk 1 byte pembawa.
4. Proses penyisipan dan ekstraksi dipengaruhi oleh kemampuan *Hardware* dan *Software* yang dimiliki.

5.2 Saran

Saran-saran yang penulis kemukakan diharapkan dapat lebih meningkatkan hasil yang telah didapatkan. Berikut beberapa saran yang disampaikan oleh penulis :

1. Jika memungkinkan dalam melakukan pemerosesan tidak memerlukan memori yang besar.
2. Pengembangan lebih lanjut disarankan dapat menggunakan format video lain sebagai video media yang akan disisipkan maupun video sebagai bahan penyisipan.
3. Diharapkan ukuran video hasil dari penyisipan tidak terlalu besar dan tidak jauh berbeda dengan video pembawa sebelum penyisipan.
4. Tidak hanya melibatkan video tanpa audio.

DAFTAR PUSTAKA

[1] Suhono H. Supangkat, Juanda, Riwut Libinuko, "*Proteksi Citra Digital dengan Informasi yang tidak kelihatan"*, ITB, 2000.

[2] Christian Cachin, "Digital Steganography", Switzerland, 2004.

[3] *http://www.wikipedia.org* Diakses pada hari Sabtu, 15 Desember 2007

[4] *http://www.ilmukomputer.org* Diakses pada hari Sabtu, 15 Desember 2007

[5] *http://en.wikipedia.org/wiki/peak-signal-to-noise-ratio* Diakses pada hari Senin, 10 September 2007

[6] Linda, Agustina., "Penerapan *Region of Interest* (ROI) pada Metode Kompresi JPEG2000", ITB, 2003.

[7] http://en.wikipedia.org/wiki/Fast_Fourier_Transform, *Fast Fourier Transform*. Diakses pada hari Selasa, 4 September 2007.

[8] http://en.wikipedia.org/wiki/Discrete_Fourier_Transform, *Discrete Fourier Transform*. Diakses pada hari Selasa, 4 September 2007.

[9] Alex Lestari, Desi, "IMPLEMENTASI TEKNIK WATERMARKING DIGITAL PADA DOMAIN DCT UNTUK CITRA BERWARNA", Yogyakarta, 2003.

[10] Elsiawaty, "Partial Watermarking", ITB, 2004.