

**TUGAS AKHIR**

**WATERMARKING PADA CITRA MAMMOGRAM  
MENGUNAKAN METODE LSB ( LEAST SIGNIFICANT BIT)**

*Diajukan Sebagai Salah Satu Syarat untuk Menyelesaikan Pendidikan Tahap  
Strata I di Jurusan Teknik Elektro Fakultas Teknik Universitas Andalas*

Oleh :

**INA MUTIA**

No.BP : 06 975 014

Pembimbing :

**DR.Eng.RAHMADI KURNIA**

NIP : 132 176 861



**JURUSAN TEKNIK ELEKTRO  
FAKULTAS TEKNIK  
UNIVERSITAS ANDALAS  
PADANG  
2009**



## ABSTRAK

Watermarking merupakan solusi untuk melindungi citra digital dari masalah kepemilikan, *copyright*, otentifikasi, *fingerprinting*, dan sebagainya. Watermarking (tanda air) disebut juga sebagai suatu teknik penyembunyian data. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Penelitian watermarking ini dilakukan dengan menggunakan *Citra Mammogram* dalam bentuk *bitmap* sebagai media penampung pesan dengan menggunakan metoda LSB (*least Significant Bit*) sehingga didapatkan gambar *bitmap* yang telah disisipkan pesan. Gambar hasil *watermarking* ini dapat dilihat kualitasnya melalui perhitungan MSE dan PSNR. Dari penelitian ini didapatkan kualitas gambar hasil *watermarking* yang baik bila ukuran file yang disembunyikan (*hidtext*) lebih kecil dari file gambar.

**Kata Kunci :** *Watermarking, Citra Mammogram, LSB, MSE, PSNR*

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi digital serta internet saat ini telah memberi kemudahan untuk melakukan akses serta mendistribusikan berbagai informasi dalam format digital. Beberapa faktor yang membuat data digital (seperti audio, citra, video dan text) banyak digunakan antara lain :

- Mudah diduplikasi dan hasilnya sama dengan aslinya.
- Murah untuk penduplikasian dan penyimpanan.
- Mudah disimpan dan kemudian untuk diolah atau diproses lebih lanjut.
- Serta mudah didistribusikan, baik dengan media disk maupun melalui jaringan seperti internet.

Kemudahan tersebut akhirnya dapat digunakan secara "negatif" tanpa memperhatikan aspek hak cipta (*Intellectual Property Right*). Perlindungan hak cipta terhadap data digital memang sudah menjadi perhatian orang-orang sejak dulu.

Banyak cara yang sudah ditempuh untuk memberikan atau melindungi data digital, seperti: *encryption*, *copy protection*, *visible marking*, *header marking*, dan sebagainya, tetapi semua cara tersebut memiliki kelemahannya masing-masing. Proses *encryption* mengkodekan data menjadi bentuk tertentu yang mana hasilnya tidak bisa dibaca lagi, untuk membaca hasil disebut dengan proses *desryption*. Dalam proses *desryption* ini menggunakan algoritma dan kunci. Ada berbagai jenis algoritma dan kunci pada proses *desryption* antara lain:



AES dan DES. Kelemahan dari proses *encryption* harus menggunakan algoritma yang panjang dan memerlukan kunci. *Copy Protection* hanya berfungsi untuk mencegah data agar tidak dapat disalin, tetapi data tetap bisa dibaca. *Visible marking*; dengan menggunakan program pengolahan citra, *visible marking* dapat dihapus, sedangkan pada *header marking* lebih mudah dibaca karena letaknya khusus, tidak tercampur dengan data inti.

Teknologi *watermarking* merupakan suatu solusi didalam melindungi hak cipta kepemilikan terhadap data-data digital, yang akhir-akhir ini dikembangkan para peneliti, yang memiliki sifat-sifat *invisibility* dan *robustness* yang dapat diatur serta data yang ter*watermark* dapat diduplikasi seperti layaknya data digital. Ide awal teknologi *watermarking* muncul pada tahun 1990, dan pada tahun 1993 Tirkel et al mulai menggunakan kata '*watermark*' dalam *paper*nya.

*Watermarking* ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Jadi *watermaking* merupakan suatu cara untuk menyembunyikan atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) kedalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera), dan mampu menghadapi proses-proses pengolahan sinyal digital yang tidak merusak kualitas data yang ter-*watermark* sampai pada tahap tertentu

Disamping itu data yang ter-*watermark* harus tahan (*robust*) terhadap serangan-serangan baik secara sengaja maupun tidak sengaja untuk menghilangkan data *watermark* yang terdapat didalamnya.

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan hasil pengujian sistem dan analisis yang telah dilakukan maka beberapa kesimpulan yang dapat diambil adalah :

1. Algoritma dan flowchart yang telah dibuat dalam langkah awal pengerjaan proyek akhir dapat berjalan dengan baik sehingga informasi dapat disisipkan dan diambil kembali isinya dari suatu media gambar . Gambar yang besar lebih tahan terhadap eror akibat penambahan teks dibandingkan dengan gambar yang lebih kecil.
2. Kualitas dari file gambar sangat ditentukan pada ukuran file yang disembunyikan dan ukuran file pembawa. Semakin besar ukuran file yang disembunyikan , maka semakin besar pula noise yang ditimbulkan.

#### 5.2 Saran

*Watermarking* pada gambar bitmab ini ini dibuat untuk melakukan penyisipan file dalam file dan penulis hanya melakukan uji coba dengan file media mammogram ekstensi bitmab dengan bahasa pemrograman visual C ++ 6 . Oleh karena itu harapan kami agar aplikasi ini dapat dikembangkan lebih lanjut dengan menggunakan bahasa pemrograman yang lebih memberikan kedinamisan dalam jenis file media yang dipakai maupun pesan rahasia yang dimasukkan dan pengembangan aplikasi sehingga dapat menggunakan berbagai jenis file media lainnya dan juga dengan menggunakan metoda *Watermarking* lainnya.



## DAFTAR PUSTAKA

- Arnold, Michael; Martin Schumucker; Stephen D Walthusen." *Techniques and Applications of Digital Watermarking and Content Protection*". Boston, Mass.[u.a]:Artech House, ©2003
- Budiono." *Digital Image Watermarking pada Mobile Device*" Departemen Teknik Informatika. Institut Teknologi Bandung, 2004
- Castleman, Kenneth R. " *Digital Image Processing*". Englewood Cliffs, NJ:Prentice-Hall. ©1979
- Cox, Ingemar J; Mather L Miller, Jeffrey A Bloom. " *Digital Watermarking: Principles and Practice*". San Francisco, Calif; Morgan Kaufman; London: International Thomson, 2002
- Furht, Borko; Darko Kirovski. " *Multimedia Security Handbook*". CRC Press, 2004
- Kurnia, Rahmadi. " *Simulasi Edge Detection Pada Citra Mamography dengan Bantuan Transformasi Wavelet*". Thesis, Universitas Indonesia, 1998
- Lai, Chun-Shien. " *Multimedia Security: Steganography and digital Watermarking Techniques for Protection of Intellectual Property*". Hershey, Pa. [u.a]: Idea, 2005
- Munir, Rinaldi. " *Steganografi dan Watermarking*" Departemen Teknik Informatika Institut Teknologi Bandung, 2004
- Pan, Jeng-Shyang; Hsiang-Cheh Hang; LC Jain. " *Intelligent Watermarking Techniques*". River Edge, NJ: World Scientific. ©2004
- Petitcolas, Fabien; Hyoung Joong Kwon. " *Digital Watermarking*". Berlin; London: Springer, 2003
- Pratt, William K. " *Digital Image Processing*". New York: Wiley. ©1978
- Seitz, Juergen. " *Digital Watermarking for Digital Media*". Hershey, PA: Information Science Pub. ©2005

[http://images.google.co.id/images?hl=id&client=firefox-a&channel=s&rls=org.mozilla:enUS:official&q=citra+mammogram&um=1&ie=UTF8&ei=yv4XSiHNEiSSKAWUkU&saa=X&oi=image\\_result\\_group&resnum=1&ct=title](http://images.google.co.id/images?hl=id&client=firefox-a&channel=s&rls=org.mozilla:enUS:official&q=citra+mammogram&um=1&ie=UTF8&ei=yv4XSiHNEiSSKAWUkU&saa=X&oi=image_result_group&resnum=1&ct=title)