PENYERANGAN PADA IMAGE WATERMARKING MENGGUNAKAN METODE MAULICIOUS ATTACK

TUGAS AKHIR

Diajukan sebagai salah satu syarat
Untuk memperoleh gelar Ahli Madya

Oleh :

LESTRI MAIJUNIATI
05 075 016

Program Studi Teknik Telekomunikasi Multimedia
Jurusan Teknik Elektro

POLITEKNIK UNIVERSITAS ANDALAS
2008

ABSTRAK

Watermarking merupakan sebuah teknik untuk menyisipkan informasi ke dalam sebuah *file digital* yang ditujukan untuk menjaga keaslian dari *file* tersebut. Penerapan *watermarking* ini dilakukan dalam banyak jenis *file digital* seperti gambar, video, dan audio. Salah satu yang menjadi perhatian lebih dalam makalah ini adalah *robustness*, yaitu bagaimana sebuah *watermarking* bisa bertahan dalam serangan-serangan yang dilakukan untuk membuka *watermark* yang disisipkan di sana.

Secara umum, ada empat jenis serangan yang digunakan di dalam menyerang *image watermarking*. Terdapat pengkategorian jenis serangan yaitu *Maulicious Attack dan Non Maulicious Attack*. *Maulicious attack* merupakan serangan terhadap *image watermarking* yang bertujuan agar *watermark* tidak dapat dideteksi atau dihilangkan dari gambar tersebut.

Kata kunci: *watermarking, maulicious attack*.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Produk digital pada saat ini merupakan sesuatu yang sangat populer dikarenakan perkembangan teknologi. Gambar, video, dan audio bisa ditransmisikan dari suatu tempat ke tempat lain tanpa kehilangan banyak kualitasnya. Akibatnya muncul masalah mengenai penggunaan produk tersebut secara ilegal seperti perekaman, manipulasi, atau menggunakannya untuk kepentingan komersial. Hal ini dapat menyebabkan pencipta dari produk digital tersebut mengalami kerugian.

Digital *watermarking* adalah teknik yang memungkinkan penyisipan itu terjadi. Informasi yang tersimpan itu disebut *watermark*. Informasi yang dimasukkan kedalam file dapat berupa teks, logo, data audio, hingga rangkaian bit yang tidak berarti. Tujuan dari *watermarking* adalah untuk mengkomunikasikan informasi. Salah satunya adalah robustness atau kekokohan dari penyimpanan informasi tersebut.

Kekokohan ini berkaitan dengan serangan terhadap *watermarking*. Jika sebuah penyisipan informasi dengan *watermarking* tersebut gampang dirusak, maka tujuan utama dalam *watermarking* akan sulit untuk tersampaikan. Serangan terhadap *watermark* adalah suatu proses untuk mendapatkan data yang telah disisipkan secara illegal, untuk kemudian akan dilakukan pengubahan isi dari *watermark* yang telah disisipkan. Serangan juga bisa berarti upaya penghilangan data yang disisipkan dalam sebuah image dengan cara merusak *watermark* asli nya, dengan harapan tidak bisa diungkap informasi yang sudah disembunyikan.

Maulicious attack merupakan serangan yang tujuan utamanya adalah menghilangkan atau membuat *watermark* tidak dapat dideteksi.

Sebuah sistem *watermark* dikatakan tangguh apabila komunikasi yang terjadi (pesan yang disisipkan) tidak bisa dirusak kecuali membuat data yang diserang menjadi tidak bermakna.

1.2 Tujuan pembuatan

Tujuan yang ingin dicapai dalam pembuatan tugas akhir ini adalah:

1. Melakukan penyerang terhadap *image watermarking* pada metoda LSB dan COX (Domain DCT)
2. Menganalisa hasil yang didapatkan setelah dilakukan penyerangan pada *image* tersebut untuk mengetahui tingkat *robustness* dari metoda LSB dan COX (Domain DCT) .

1.3 Rumusan Masalah

Implementasi dari teknik *watermarking* adalah untuk menciptakan pengamanan atau melindungi terhadap penyalinan data dan perlindungan hak cipta pada citra digital harus dilakukan sedemikian rupa sehingga tidak mudah disalah gunakan oleh orang lain.

Untuk itu, beberapa masalah yang harus diperhatikan sehubungan dari teknik *watermarking* salah satunya adalah *robustness* (Ketahanan watermark yang disisipkan apabila dilakukan penyerangan).

BAB V

PENUTUP

5.1 Kesimpulan

Setelah dilakukan pengujian dan analisa terhadap image watermarking dengan menggunakan metode LSB dan COX dapat ditarik kesimpulan sebagai berikut:

1. Template attack yang dilakukan pada metoda LSB dan COX terbukti bahwa watermark yang disisipkan tidak dapat dideteksi lagi.
2. Dimana kelemahan dari metoda LSB ini adalah sangat tidak tahan terhadap proses-proses yang mampu mengubah data citra terutama kompresi JPEG.
3. Metoda COX lebih tahan terhadap serangan kompresi JPEG, dimana watermark yang disisipkan masih dapat dideteksi setelah dilakukan kompresi.
4. Setelah melakukan dua kali *watermark* pada metode LSB, maka *watermark* kedua akan muncul menggantikan *watermark* pertama, hal ini menyebabkan sescorang yang memiliki image tersebut tidak akan bisa membuktikan keaslian *watermark* yang disisipkannya.ini membuktikan bahwa metode LSB dapat disisipkan dengan beberapa kali *watermark*.