VERIFIKASI KEPEMILIKAN CITRA MEDIS DENGAN KRIPTOGRAFI RSA DAN LSB *WATERMARKING*

SKRIPSI

Oleh :

Satya Sandika Putra

J2A 605 103

JURUSAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS DIPONEGORO

SEMARANG

2010

ABSTRAK

Di dalam dunia medis, penyembunyian informasi untuk perlindungan hak cipta sangat diperlukan. Teknik penyembunyian informasi biasa disebut dengan *watermarking*. Metode yang digunakan adalah dengan menyisipkan pesan teks ke dalam sebuah data citra medis. Perlindungan informasi di dalam data citra medis seorang pasien perlu dilakukan agar tidak terjadi kesalahan informasi kepemelikan data medis pasien satu dengan yang lainnya. Informasi yang disembunyikan di dalam citra medis berupa teks yang sebelumnya telah dilakukan enkripsi atau pengacakan pesan. Salah satu metode untuk menyembunyikan pesan teks adalah dengan memanfaatkan *Least Significant Bit* (LSB), yaitu dengan mengubah nilai bit terakhir pada citra medis. Karena hanya bit-bit terakhir yang diubah, maka citra medis yang telah tersisipi pesan sangat mirip dengan citra aslinya, perubahan nilai-nilai piksel pada citra medis tidak begitu terlihat. Untuk mengekstrak kembali pesan teks yang disisipkan menggunakan *private key* (kunci rahasia) yang sebelumnya telah ditentukan secara acak. Citra medis dan pesan teks hasil ekstrak sama dengan citra medis dan pesan teks sebelum dilakukan penyisipan.

Kata kunci : *watermarking*, citra medis, enkripsi, *private key, Least Significant Bit*

ABSTRACT

In medical world, hiding information to protect copy right is so necessary. Common hiding technique is called watermarking. Method that is used inserting text message in a medical image data. Information in medical image data's patient is necessary in order to reduce the error information about one data possesion to another. Information that is hidden in medical image formed disarranged text by encryption. Least Significant Bit (LSB) is a method to hide text message, it change last bit value in medical image. Because of only the last bit that is changed, medical image. Which has been inserted is so exactly with original image, the differ pixel amount in medical image is not significant. To extract inserted text message, it is used private key disarranged before effected. Medical image and text message by extraction is same with medical image and text message before insertion.

***Key word** : watermarking, medical image, encryption, private key, Least Significant Bit*

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era globalisasi saat ini teknologi komputasi berkembang dengan pesatnya. Berkembangnya teknologi komputer dan informasi selalu memilki dampak positif dan negatif. Terutama dalam dunia medis, salah satu dampak negatif yang terjadi adalah pencurian dan penyalahgunaan data medis, khususnya *image*. Dengan memanfaatkan kelemahan sistem penglihatan manusia, para penjahat digital melancarkan aksinya dan merugikan banyak pihak. Karena banyak kasus tersebut, dikembangkan teknologi untuk melindungi data-data medis. Dalam hal ini adalah citra medis. Salah satu teknologi itu adalah *watermarking.* (Putut, 2000).

Watermarking adalah teknik menyisipkan suatu informasi ke dalam data multimedia. Informasi tersebut dapat berupa data-data citra, audio, maupun video yang menggambarkan kepemilikan suatu pihak. Informasi yang disisipkan tersebut disebut *watermark*. Banyak metode yang bisa digunakan dalam *watermarking*, tergantung pada data-data apa yang akan di*watermark*. Misalnya, data citra, data audio, maupun data video. Salah satu metodenya adalah kriptografi kunci publik. (Brata, 2004).

Sistem kriptografi kunci publik adalah sebuah sistem yang menggunakan sepasang kunci kriptografi, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi diumumkan kepada publik sehingga dinamakan kunci publik,

sedangkan kunci untuk dekripsi bersifat rahasia sehingga dinamakan kunci privat. (Munir, 2004).

Dalam dunia medis diperlukan kebutuhan verifikasi untuk mengetahui keaslian dari sebuah citra medis. Contoh yang sering kita jumpai adalah ketika pihak medis yang memiliki citra digital berupa gambar dari bagian tertentu tubuh pasiennya dilakukan verifikasi citra medis sebelum dipublikasikan di media massa, sehingga pekerja di media massa yang mempunyai citra berupa fakta harus sesuai dengan citra yang diberikan oleh pihak medis. Jika tidak sesuai, berarti citra tersebut telah termanipulasi oleh pihak tertentu yang tidak bertanggung jawab dan hal tersebut bisa berbahaya jika untuk konsumsi publik. Di sini kebutuhan verifikasi citra sangat diperlukan. Kebutuhan lain yang muncul adalah kebutuhan otentikasi citra medis yaitu kebutuhan kepemilikan suatu citra digital dalam hal ini adalah pihak medis. Sehingga otentikasi ini dapat dilakukan publik tanpa perlu kehadiran pemilik citra tersebut.

Di sini *watermarking* dapat menjadi solusi untuk menyelesaikan masalah verifikasi dan otentikasi citra medis. Dengan cara menyisipkan suatu informasi ke dalam sebuah data, dalam hal ini berupa data citra medis yang menggambarkan kepemilikan suatu pihak.

Pada proses verifikasi dan otentikasi citra medis bisa menggunakan metode LSB *(Least Significant Bit)* dan Spread-Spectrum, dan algoritma yang bisa digunakan adalah algoritma RSA (Rivers Shamir Adleman), Elgamal, DSA, DES (Data Enkripsi Standar), MD5 (*Messages Digest* 5), DCT (*Descrete Cosine Transform*), SHA (*Secure Hash Algorithm*), DFT (*Descrete Fourier Transfom*), LUC. Metode dan algoritma tersebut memiliki keunggulan masing-masing

tergantung dari data informasi yang akan disisipkan. Untuk verifikasi dan otentikasi citra medis di atas menggunakan metode LSB dan algoritma RSA. Karena metode LSB merupakan metode yang menggunakan teknik domain spatial dan merupakan metode yang paling sederhana, cepat dan mudah. Metode ini akan mengubah nilai LSB komponen warna menjadi bit yang bersesuaian dengan bit label yang akan disembunyikan. Sehingga metode ini akan menghasilkan citra rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai bit terakhir dari data. Sedangkan algoritma RSA merupakan algoritma yang melibatkan ekspresi dengan fungsi eksponensial, algoritma ini paling mudah dimengerti cara kerjanya dan juga sangat kokoh untuk menyandi atau menterjemahkan sandi. RSA hanya menggunakan operasi pemangkatan. Bentuk operasi dasarnya adalah m^k **mod** n yang menghasilkan nilai relatif acak hubungan terhadap m sehingga algoritma ini susah dipatahkan. Dan sangat cocok diterapkan dalam *watermarking* sebuah citra.

Untuk itu penulis akan menerapkan metode LSB dan algoritma RSA di dalam proses verifikasi dan otentikasi citra medis. Hasilnya kemudian akan dilihat perbedaan kualitas citra sebelum dan sesudah dilakukan verifikasi dan otentikasi citra.

1.2 PERUMUSAN MASALAH

Permasalahan yang dibahas dalam tugas akhir ini adalah bagaimana melakukan proses verifikasi dan otentikasi pada citra medis dengan menggunakan

metode LSB dan algoritma RSA. Serta pembentukan skema *watermarking* untuk proses verifikasi dan otentikasi citra medis.

1.3 PEMBATASAN MASALAH

Agar fokus lebih jelas, maka dalam tugas akhir ini permasalahan dibatasi sebagai berikut :

1. Metode *watermarking* yang digunakan adalah LSB untuk otentikasi citra medis.
2. Algoritma kriptografi kunci publik yang digunakan adalah RSA untuk otentikasi citra medis. Algoritma ini sebagai fungsi tambahan pada proses penyisipan *watermark* dan ekstraksi *watermark*.
3. Format citra medis yang digunakan adalah BMP.
4. Pada tugas akhir ini menggunakan program bantu Matlab 7.1.

1.4 TUJUAN

Tujuan dari penulisan tugas akhir ini adalah :

1. Memahami penggunaan metode *watermarking* LSB dalam otentikasi sebuah citra medis.
2. Memahami penggunaan algoritma RSA dalam otentikasi sebuah citra medis.
3. Mengimplementasikan metode LSB dan algoritma RSA tersebut pada proses penyisipan *watermark* dan ekstraksi *watermark*.
4. Mendapatkan citra medis dan pesan teks hasil otentikasi yang mirip dengan citra medis dan pesan teks hasil verifikasi.

1.5 SISTEMATIKA PENULISAN

BAB I berisi latar belakang, perumusan masalah, pembatasan masalah, tujuan dan sistematika penulisan.

BAB II berisi dasar teori meliputi definisi citra digital, *watermarking*, kriptografi kunci publik, algoritma LSB, algoritma RSA, data flow diagram, dan MATLAB 7.1.

BAB III berisi analisis kebutuhan perangkat lunak yang digunakan, *context* diagram, desain antarmuka (*User Interface*), dan desain fungsi.

BAB IV berisi implementasi dan analisa hasil.

BAB V berisi penutup.

DAFTAR PUSTAKA