Jurnal Sains dan Matematika Vol. 19 (3): 75-81 (2011)

Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermarking

[1]Satya Sandika Putra, [2]Priyo Sidik Sasongko, and [2]Nurdin Bahtiar
[1]Jurusan Matematika, [2]Jurusan Ilmu Komputer / Informatika
Fakultas Sains dan Matematika Universitas Diponegoro

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 miripdengan 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

PENDAHULUAN

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 **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.

GAMBARAN UMUM SISTEM

Analisis kebutuhan software diperlukan untuk menganalisa pendukung sistem, penganalisaan yang baik akan mengetahui kekurangan dan kelebihan dari perangkat pendukung maupun *software* yang dibuat. Analisis sistem menjelaskan tentang data context diagram dan analisis sistem LSB watermarking. Desain sistem menjelaskan tentang antarmuka (user interface), desain fungsi.

Kebutuhan perangkat lunak guna mengimplementasikan pembuatan program adalah sebagai berikut:

- Sistem Operasi Windows 98 / NT / 2000 / XP.
- Software Matlab 7.1

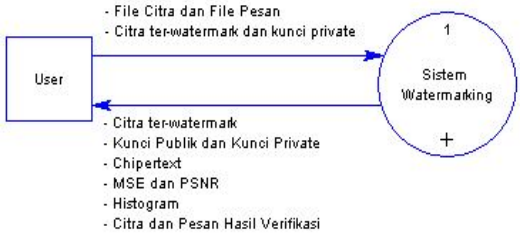
Kebutuhan perangkat keras guna mengimplementasikan pembuatan program adalah sebagai berikut:

- Processor Pentium(R) M processor 1,50 GHz.
- VGA mampu menampilkan 32 bit atau dengan resolusi 1024 x 768. RAM 256 MB.
- Free space harddisk minimum 2,5 GB
- Keyboard dan Mouse.

PEMODELAN FUNGSIONAL

1. Data Context Diagram

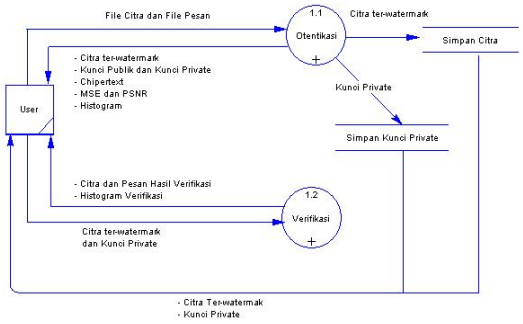
Data Context Diagram (DCD) pada gambar 1 merupakan data arus awal. Dimana, user melakukan inputan file citra medis dan file pesan untuk dilakukan otentikasi sehingga user mendapatkan hasil citra otentikasi. Sedangkan untuk melakukan proses verifikasi, user harus menginputkan citra hasil otentikasi dan kunci private untuk mendapatkan citra dan pesan hasil verifikasi. DCD disebut juga sebagai DFD level 0.



Gambar 1. DCD Aplikasi

2. DFD Level 1

DFD Level 1 di Gambar 2 merupakan *breakdown* dari Gambar 1.

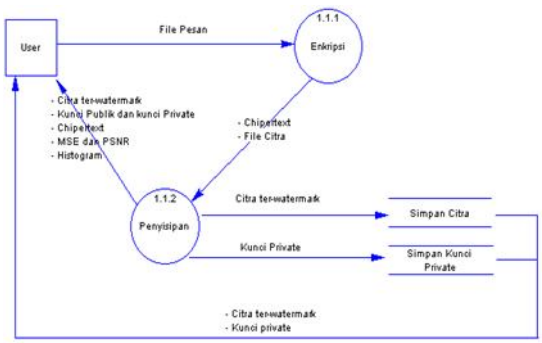


Gambar 2. DFD Level 1

DFD level 1 pada gambar 2 merupakan penjabaran dari DCD. Pada DFD level 1 ini menjelaskan jalannya proses otentikasi dan verifikasi yang merupakan penjabaran dari proses sistem *watermarking* pada DCD. Untuk melakukan proses otentikasi (Penyisipan) *user* melakukan inputan file citra medis dan file pesan untuk diproses sehingga menghasilkan file citra ter-*watermark* atau bisa disebut juga file citra otentikasi, kemudian file citra otentikasi disimpan ke dalam format BMP dan untuk selanjutnya dapat ditampilkan. Sedangkan untuk proses verifikasi, *user* menginputkan citra otentikasi dan kunci private untuk diproses sehingga didapatkan citra medis dan pesan hasil verifikasi. Apabila *user* melakukan otentikasi, maka yang didapatkan *user* adalah citra hasil otentikasi, kunci public dan kunci private, MSE, PSNR, dan histogram. Jika *user* melakukan verifikasi, maka *user* mendapatkan citra medis, pesan hasil verifikasi, dan histogram.

3. DFD Level 2 Proses 1

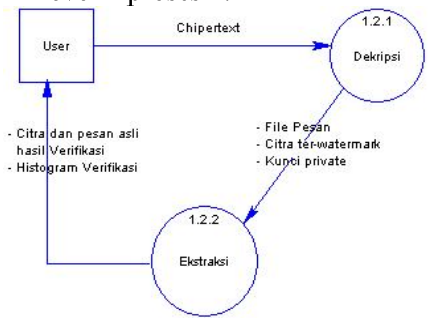
Pada DFD level 2 proses 1 merupakan penjabaran dari proses otentikasi pada DFD level 1. Di dalam proses otentikasi terdapat dua proses, yaitu proses enkripsi dan proses penyisipan. Untuk melakukan enkripsi, *user* menginputkan file pesan untuk diproses sehingga menghasilkan *chipertext* (pesan terenkripsi). Kemudian, *user* melakukan penyisipan *chipertext* ke dalam file citra medis dan dihasilkan file citra ter-*watermark*, kunci publik, kunci private, MSE, PSNR, dan histogram. Hasil citra otentikasi (Citra ter-*watermark*) dan kunci *private* disimpan, untuk selanjutnya dapat ditampilkan. Gambar 3 adalah gambar dari DFD level 2 proses 1.



Gambar 3. DFD Level 2 Proses 1

4. DFD Level 2 Proses 2

DFD level 2 proses 2 merupakan penjabaran dari proses verifikasi pada DFD level 1. Di dalam proses verifikasi terdapat dua proses, yaitu proses dekripsi dan proses ekstraksi. *User* menginputkan *chipertext* untuk didekripsi sehingga didapat file pesan. Selanjutnya, masukkan cita ter-*watermark* dan kunci *private* untuk diekstrak dan dihasilkan citra dan pesan asli hasil ekstraksi. Proses verifikasi dinyatakan berhasil apabila citra medis dan pesan hasil ekstraksi sama seperti citra medis dan pesan sebelum diotentikasi. Gambar 4 adalah gambar dari DFD level 2 proses 2.



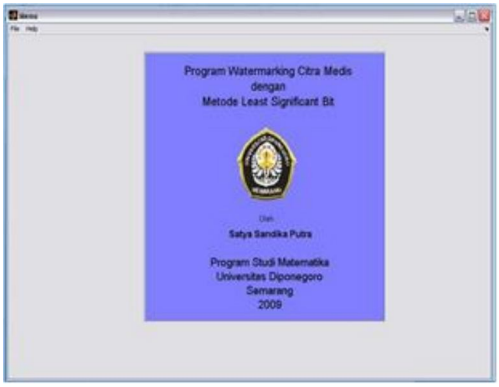
Gambar 4. DFD Level 2 Proses 2

Secara spesifik beberapa hal yang dipaparkan dalam analisis sistem pada LSB *watermarking* antara lain:

1) Input citra medis yang digunakan berformat BMP, yang selanjutnya akan disebut dengan citra asli.
2) Pembentukan kunci publik dan kunci rahasia dipilih secara random.
3) Panjang pesan yang diinputkan maksimal 100 huruf.
4) Dengan metode LSB, sistem dapat menunjukkan hasil citra setelah pesan berhasil disisipkan ke dalam citra asli. Kemudian disebut dengan citra watermark.
5) Proses ekstraksi (Verifikasi) yang dilakukan adalah pemisahan data citra asli dan data pesan. Citra watermark atau citra asli yang telah tersisipi sebuah pesan akan dipisahkan kembali dengan menggunakan sebuah kunci, yaitu kunci privat yang sebelumnya telah ditentukan.
6) Verifikasi dikatakan berhasil apabila citra hasil ekstraksi sama dengan citra asli yang diinputkan. Begitu juga pesan hasil ekstraksi, hasilnya sama dengan pesan yang diinputkan.

IMPLEMENTASI SISTEM

Implementasi antarmuka *watermarking* dibuat dengan menggunakan *Software Graphical User Interface* (GUI) Matlab 7.1 dan terdiri atas tiga bagian, yaitu bagian muka/cover yang merupakan tampilan dari *form* menu, bagian *watermarking* yang merupakan tampilan dari *form* otentikasi, dan bagian ekstraksi yang merupakan tampilan dari *form* verifikasi.



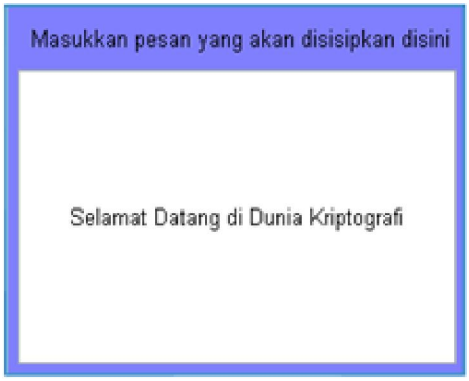
Gambar 5. Form Utama

Gambar 6. Tampilan bagian watermarking (form Otentikasi)

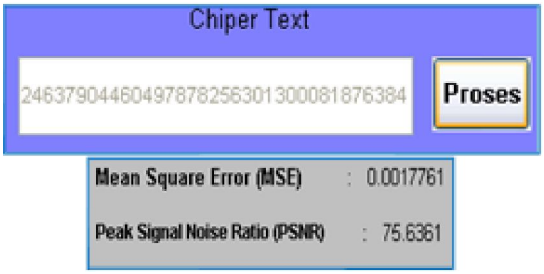
Gambar 7. Tampilan Form Verifikasi

Gambar 8. Tampilan Citra Medis telah terinput

Gambar 9. Tampilan Public Key dan Private Key telah terinput



Gambar 10. Pesan teks yang disisipkan



Gambar 11. Push button Proses setelah diklik

Gambar 12. Citra medis telah ter-watermark

ANALISIS HASIL

Pada analisa hasil ini menjelaskan penentuan hasil otentikasi citra medis setelah disisipkan sebuah pesan teks di dalamnya. Hasil implementasi program diperoleh tingkat kualitas citra otentikasi / ter-watermark yang mirip dengan citra medis sebelum dilakukan otentikasi.

Implementasi program digunakan citra RGB Rontgen.bmp sebagai citra medis yang akan disisipi pesan. Dan pesan teks yang disisipkan bertuliskan "Selamat Datang di Dunia Kriptografi".

Gambar 13. Rontgen.bmp

Hasil implementasi pada gambar 13 menyatakan bahwa penyisipan pesan teks ke dalam citra medis tidak menyebabkan terjadinya perubahan citra secara signifikan, terlihat pada histogram yang secara sepintas terlihat sama. Hal ini terjadi karena proses penyisipan yang dilakukan hanya pada nilai bit terakhir di dalam citra, sesuai dengan metode penyisipan yang digunakan yaitu Least Significant Bit.

Untuk mengukur perbedaan kualitas citra medis sebelum dengan sesudah dilakukan penyisipan pesan teks digunakan parameter PSNR (Peak Signal to Noise Ratio). Nilai PSNR diperoleh dengan membandingkan citra asli dengan citra ter-watermark. Semakin tinggi nilai PSNR menunjukkan bahwa penyisipan pesan teks ke dalam citra medis tidak mengakibatkan penurunan kualitas citra. Sebaliknya, jika nilai PSNR semakin kecil maka terjadi penurunan kualitas citra medis dikarenakan proses penyisipan pesan.

Untuk mengetahui nilai PSNR, terlebih dahulu harus menghitung nilai MSE citra medis tersebut. MSE (Mean Square Error) yaitu tingkat kesalahan nilai-nilai piksel dari citra ter-watermark terhadap citra asli. Nilai MSE sangat mempengaruhi nilai PSNR yang dihasilkan. Semakin tinggi nilai MSE maka nilai PSNR citra tersebut semakin rendah. Jadi jika tingkat kesalahan nilai-nilai piksel dari citra ter-watermark semakin sedikit maka kualitas citra semakin baik. Tingkat kualitas citra/tingkatan nilai PSNR dapat diketahui pada tabel 1. (Constant, 2007).

Tabel 1. Nilai PSNR

PSNR (dB)	Kualitas Citra
60	Sangat baik, tidak ada noise
50	Baik, masih terdapat noise kecil
40	Kurang baik, terdapat noise cukup besar
30	Tidak baik, terdapat noise besar
20	Citra tidak dapat digunakan

Dari hasil beberapa citra medis yang dilakukan proses penyisipan menghasilkan nilai MSE dan PSNR yang berbeda. Nilai PSNR yang dihasilkan diatas 60 dB dan itu berarti kualitas citra medis hasil penyisipan sangat baik, tidak terdapat noise. Terlihat pada tabel 2.

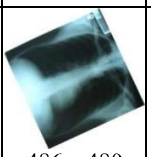
Tabel 2. Nilai MSE dan PSNR

Citra Medis	**Proses Watermarking**	
	MSE	**PSNR**
	**0.0017818**	**75.6361**

	**0.0026841**	**73.8427**
	**0.003458**	**72.7426**
	**0.0031895**	**73.0936**

Untuk menguji citra ter-watermark apakah tahan terhadap serangan atau tidak, maka dilakukan cropping, compressing, rotation, resize, dan brightness. Terlihat pada tabel 3.

Tabel 3. Uji Citra Ter-watermark

Citra ter-*watermark*	Pengujian	Pesan ter-ekstrak	Ket
 486 x 480	 486 x 480	" Selamat Datang di Dunia Kriptografi "	Berhasil
 486 x 480	*Cropping*  360 x 204	–	Tidak berhasil, karena *cropping* merubah ukuran piksel citra dari ukuran semula sehingga pesan yang tersembunyi
 486 x 480 (.BMP)	*Compressing*  238 x 235 (.JPEG)	–	Tidak berhasil, karena *compressing* merubah format dan kualitas pada citra , pesan yang tersembunyi akan hilang.
 486 x 480	 486 x 480	–	Tidak berhasil, karena *rotation* merubah posisi panjang dan lebar citra sehingga pesan menjadi hilang.
 486 x 480	 486 x 480	–	Tidak berhasil, karena brightness merubah tingkat kecerahan citra menjadi lebih tinggi, dan

KESIMPULAN

Otentikasi yaitu penyisipan sebuah pesan teks ke dalam citra medis yang menghasilkan citra ter-watermark. Citra ter-watermark tersebut dapat diekstrak kembali untuk mendapatkan pesan teks yang disisipkan. Kemudian dilakukan verifikasi, yaitu mengekstrak pesan teks yang terdapat di dalam citra medis terwatermarkdengan menggunakan kunci rahasia untuk keamanan pesan teks.

Secara umum, dari hasil yang diperoleh dalam implementasi dapat disimpulkan bahwa :

1) Proses watermarkingcitra medis menghasilkan citra ter-watermark yang mirip dengan citra asli.
2) Kualitas citra medis yang ter-watermarktergolong dalam kategori sangat baik karena nilai PSNR yang dihasilkan lebih dari 60 dB yaitu 75,6361.
3) Hasil verifikasi adalah citra medis RGB dan pesan teks yang sama seperti citra medis dan pesan teks sebelum dilakukan proses otentikasi.
4) Watermarking dengan metode LSB (Least Significant Bit) tidak tahan terhadap serangan seperti cropping, compressing, rotation, dan brightness.

DAFTAR PUSTAKA

[1] Away, Gunaidi Abdia. 2006. The Shortcut of MATLAB Programmimg. Bandung: Informatika.

[2] Brata, Angga Indra. 2004. Watermarking dengan Algoritma Kunci Publik untuk Verifikasi dan Otentikasi Citra. ITB.
[3] Constant, Mike. 2007. Signal to Noise Ratio. Diakses tanggal 18 Februari 2010. www.cctv-information.co.uk/ constant2/ sn_ratio.html
[4] Gultom, Bernardus Surya Perdana. 2006. Analisis Kinerja Algoritma RSA Dalam Pengacakan Citra Watermark. STTTELKOM Bandung.
[5] Hestiningsih, Idhawati. 2007. Pengolahan Citra.
[6] Ladjamudin, Al Bahra Bin. 2006. Rekayasa Perangkat Lunak. Graha Ilmu.
[7] Mukodim, Didin. 2002. Tinjauan Tentang Enkripsi Dan Dekripsi Suatu Teknik Pengamanan Data Dengan Penyandian RSA. Universitas Gunadarma.
[8] Munir Renaldi, Riyanto Bambang, Sutikno Sarwono. 2004. Penerapan Sistem Kriptografi Kunci-Publik Untuk Membentuk Skema Publik-Key Watermarking, ITB.
[9] Ping Wah Wong. 2004. A Public Key Watermark for image Verification and Authentication. Hawlett Packard Company. Diakses tanggal 19 April2009. http://www.tsi.enst.fr/~maitre/tatouage/icip98/ mall_07.pdf
[10] Putri, Dwitya. 2008. Membandingkan Steganographi Dan Watermarking Pada Keamanan File Grafik. Universitas Gunadarma.
[11] Putut, Dwidy. 2000. Metode Least Significant Bit. STTTELKOM Bandung.
[12] Rivest, R.L. , Shamir, A. , and Adleman, L. 1997. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. ACM.
[13] Riyanto, M. Zaki, Ardhi Ardhian. 2008. Kriptografi Kunci Publik Sandi RSA. Kelompok Studi Sandi. Yogyakarta. Diakses tanggal 23 Mei 2009. http://sandi.math.web.id
[14] Semarajana, Gede. 2007. Analisis Dan Simulasi Bblind Watermarking Dengan Transformasi Wavelet Pada Citra Digital. STTTELKOM. Bandung.
[15] Sugiharto, Aris. 2006. Pemrograman GUI dengan MATLAB. Yogyakarta: ANDI.
[16] Supriyono. 2008. Pengujian Sistem Enkripsi-Dekripsi Dengan Metode RSA Untuk Pengamanan Dokumen. STT Nuklir. Yogyakarta.
[17] Wibowo, Inu Laksito. 2001. Aplikasi Algoritma RSA Pada Sistem Pengaman Data Yang Menjamin Keaslian Dan Kerahasiaan Data. ITS.
[18] Wijaya, Marvin Ch dan Agus Prijono. 2007. Pengolahan Citra Dijital Menggunakan MATLAB. Bandung: Informatika.