Aplikasi Watermarking Citra Digital Pada Mobile Device Menggunakan J2ME

[1]Marlina Septiani
[1] Jurusan Teknik Informatika Fakultas Teknologi Industri, Universitas Gunadarma
(boelan_69@yahoo.com)

ABSTRAK

Skripsi ini membahas mengenai pembuatan aplikasi *watermarking* dari sebuah citra pada *mobile device* yang mendukung fitur kamera. *Watermarking* citra digital merupakan salah satu jenis w*atermarking* untuk melindungi kepemilikan (*copyright*) dari sebuah citra. Sedangkan *Watermarking* merupakan bagian dari ilmu kriptografi dengan metode menyisipkan sebuah informasi ke dalam media tertentu. Implementasi *watermarking* citra digital dalam skripsi ini meliputi penerapan penggunaannya pada *mobile device* untuk citra yang diambil dari kamera *watermark*.

Sebuah perangkat lunak yang bernama Marza akan dibangun pada sebuah *mobile device* untuk mendukung implementasi dari *watremarking citra* digital. Aplikasi ini dikembangkan dengan menggunakan bahasa pemograman JAVA khusunya J2ME yang menyediakan berbagai *interface* untuk melakukan pengambilan citra melalui kamera *mobile device*. Aplikasi ini juga dapat menghitung lamanya waktu untuk proses penyisipan dan pendeteksian sebuah file citra.

Penulis menggunakan PSNR untuk membandingkan hasil citra sebelum dan sesudah diwatermark. Hasil pengujian menunjukkan bahwa *mobile device* memiliki kemampuan untuk melakukan proses digital *image wateramarking* pada sebuah citra yang diambil dari fitur kameranya tanpa menurunkan kualitas dari citra tersebut. Selain itu, implementasi dari digital *image watermarking* pada *mobile device* ini memiliki keterbatasan dalam melakukan proses algoritma penyisipan *watermark* dan ekstrasi atau deteksi *watermark* dari citra yang dihasikannya dikarenakan keterbatasan melakukan komputasi dan kapasitas memori dari *mobile device* tersebut.

Kata Kunci : *Watermarking*, citra digital, J2ME, *moble device*, ekstraksi/deteksi, Marza.

PENDAHULUAN

Saat ini kebutuhan akan teknologi *mobile* semakin meningkat di kalangan masyarakat. Salah satunya adalah penggunaan fitur kamera yang terdapat dalam perangkat *mobile*. Dengan semakin banyaknya telepon seluler yang mendukung teknologi 3G, foto-foto yang dihasilkan dari perangkat *mobile* dapat dengan mudah di*upload* secara langsung ke internet dan dikonsumsi oleh masyarakat secara luas. Hal ini menimbulkan pertanyaan akan originilitas dari setiap gambar yang ada di internet. Bahkan tidak sedikit saat ini kasus-kasus hak cipta mengenai hasil foto

kamera diperdebatkan. Akhirnya, muncul keraguraguan dari pihak pemilik perangkat *mobile* untuk meng*upload* foto mereka secara *online* di internet.

Untuk itu, perlu adanya suatu teknologi yang dapat melindungi hak cipta dari setiap foto yang dihasilkan dari perangkat *mobile* ini. Salah satu solusinya adalah dengan menerapkan teknologi Digital *Image Watermarking.* Pada umumnya kita mengetahui teknologi digital image watermarking hanya diterapkan dan dijalankan pada sebuah komputer pc saja. Sejauh ini, penulis belum menemukan perangkat *mobile* seperti telepon selular yang telah dilengkapi dengan fasilitas teknologi *watermarking* tersebut. Oleh karena itu pada penulisan skripsi ini, penulis akan mencoba membuat sebuah aplikasi watermarking yang dapat diterapkan pada perangkat *mobile* seperti telepon selular.

TINJAUAN PUSTAKA

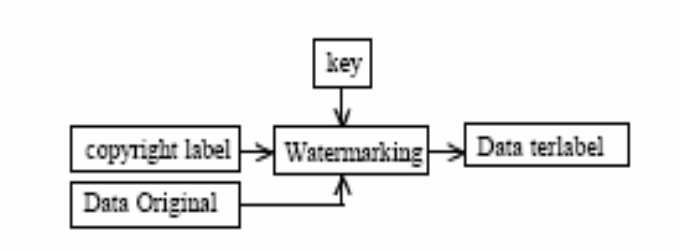
Digital watermarking atau *watermarking* adalah teknik untuk menyisipkan informasi tertentu ke dalam data digital yang disebut *watermark* (tanda air). *Watermark* dapat berupa teks seperti informasi *copyright*, gambar berupa logo, data audio, atau rangkaian bit yang tidak bermakna. Penyisipan *watermark* dilakukan sedemikian sehingga *watermark* tidak merusak data digital yang dilindungi. Selain itu *watermark* yang telah disisipkan tidak dapat dipersepsi oleh indra manusia, tetapi dapat dideteksi oleh komputer dengan menggunakan kunci yang benar. *Watermark* yang telah disisipkan tidak dapat dihapus dari dalam data digital sehingga jika data digital tersebut disebar dan diduplikasi maka otomatis *watermark* di dalamnya akan ikut terbawa. *Watermark* di dalam data digital harus dapat diekstraksi kembali. *Watermarking* berguna untuk membuktikan kepemilikan, *copyright, protection*, *authentication*, *fingerprinting tamper profing*, dan *distribution tracing*.

- **Tujuan *Watermarking***

  Berikut beberapa tujuan penggunaan teknologi watermarking, antara lain :

  1. Menjaga sedemikian rupa agar dokumen-dokumen elektronik yang berisi transaksi elektronik yang otentik sehingga tetap terjaga kualitas legal dan bobot buktinya.
  2. Untuk aplikasi perlindungan hak cipta, tanda yang disisipkan pada dokumen (gambar, teks, atau audio) digunakan sebagai identifier yang menunjukkan hak kepemilikan.

- **Proses *Watermarking***



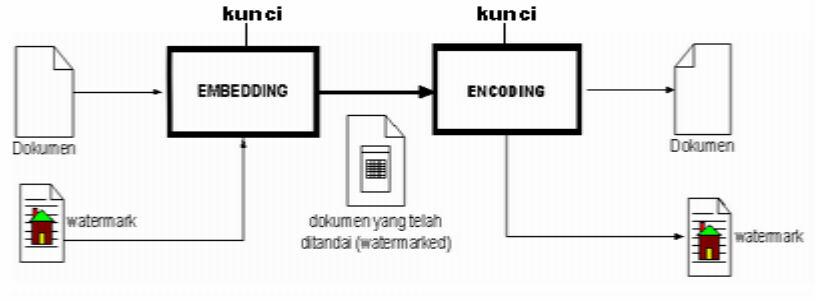
Gambar 1. Proses Watermarking
Sumber : (Rodiah, 2004)

Pada Gambar 1 proses *watermarking* diatas, terdapat komponen (key), key ini digunakan untuk mencegah penghapusan secara langsung oleh pihak tak bertanggung jawab, dengan menggukan metoda enkripsi yang sudah ada. Sedangkan ketahanan terhadap proses-proses pengolahan lainnya, itu tergantung pada metoda *watermarking* yang digunakan.

Tetapi dari berbagai penelitian yang sudah dilakukan belum ada suatu metoda *watermarking* ideal yang bisa tahan terhadap semua proses pengolahan digital yang mungkin. Biasanya masing-masing penelitian menfokuskan pada hal hal tertentu yang dianggap penting. Penelitian dibidang *watermarking* ini masih terbuka luas dan semakin menarik, salah satunya karena belum ada suatu standar yang digunakan sebagai alat penanganan masalah hak cipta ini.

- **Cara kerja *Watermarking***

Pada watermark digital, sebuah sinyal *low-energy* disisipkan ke sinyal utama sebagai cover signal untuk menyembunyikan sinyal *low-energy* tadi.



Gambar 2: Prinsip kerja watermark
Sumber : (Rodiah, 2004)

Pada gambar 2 diilustrasikan sinyal *low-energy* adalah *watermark*, dan cover signal-nya adalah dokumen, yang dapat berupa gambar, video, suara, atau teks dalam format digital.

- **Aplikasi *Watermarking***

Berikut beberapa aplikasi dari *watermarking*, antara lain :

Broadcast Monitoring

Watermarking dapat digunakan dalam *broadcast monitoring* dengan menambahkan *watermark* yang unik kedalam tiap video ataupun suara sebelum ditayangkan oleh stasiun televisi atau disiarkan oleh stasiun radio.

Owner Identification

Watermarking dapat digunakan sebagai tool untuk *owner identification*, karena informasi hak cipta tersebut diletakan didalam data *host*-nya dan merupakan bagian dari data *host* tersebut, sehingga usaha untuk menghilangkan informasi hak cipta tersebut dapat menurunkan kualitas data *host*nya.

Copy Control

Penggunaan *watermark* sebagai *copy control* hampir sama dengan copy protection yang digunakan pada disket-disket (*disk-protection*) beberapa tahun yang lampau. Penerapan *watermarking* sebagai *copy control* harus disertai dengan penanaman *watermarking detector* pada perangkat *hardware* untuk membaca data digital tersebut. Bila *detector* mendeteksi adanya *watermark* pada data digital yang akan dibacanya, maka beberapa proses yang dapat dilakukan hardware tersebut misalnya peng-*copy*-an akan di-*disable*-kan.

- **Jenis Digital *Watermarking***

1. ***Visible Watermark***
   Watermarking jenis ini merupakan *watermarking* yang memiliki tujuan untuk meningkatkan perlindungan akan hak cipta. Selain itu, *watermarking* jenis ini juga digunakan untuk mengidentifikasi kepemilikan dari sebuah karya (originalitas).
2. ***Invisible Robust Watermark***
   Watermarking jenis ini untuk mendeteksi ketidaktepatan dari sebuah citra. Selain itu, jenis ini biasanya digunakan untuk menerangkan kemepilikan.
3. ***Invisible Fragile Watermark***
   Watermarking jenis ini digunakan oleh perangkat kamera yang cukup handal. Dan proses *watermarking* dilakukan ketika pengambilan gambar.

Berdasarkan berbagai jenis dari *watermarking* tersebut, skripsi ini akan sesuai dengan jenis *watermarkingInvisible Fragile Watermark.* Berikut adalah Karakteristik *Invisible Fragiles Watermarking* yang Baik :

- *Invisible Watermarking* harusnya tidak dapat diketahui oleh *viewer* dan tidak menurunkan kualitas dari konten yang sebenarnya.

- *Invisible Fragiles Watermarking* harusnya dapat dimodifikasi ketika ada suatu niai *pixel* gambar yang diubah.
- Untuk gambar yang berkualitas, jumlah *pixel* yang dimodifikasi harus sekecil mungkin.

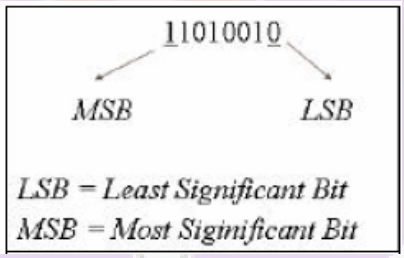
- **Serangan Pada *Watermark*s**

Citra ber-*watermark* biasanya diselewengkan untuk kepentingan tertentu, beberapa penyelewengan yang dilakukan secara sengaja adalah kompresi dan transmisi bunyi dan hal-halseperti pemotongan (*cropping*), *filtering*, dan lain-lain.

- Kompresi Lossy : Banyak skema kompresi seperti JPEG dan MPEG yang kemungkinan besar dapat menurunkan kualitas data melalui kehilangan sejumlah data yang tidak dapat dikembalikan.
- Distorsi Geometric : Distorsi *Geometric* lebih spesifk pada citra video termasuk beberapa operasinya antara lain memutar (*rotation*), *translation*, *scalling*, dan pemotongan (*cropping*).

- **Teknik Image *Watermarking***

Jumlah dari teknik algoritma untuk *image watermarking* sangat sedikit. Salah satunya adalah metode spasial. Metode ini menyisipkan *watermark* langsung pada nilai *byte* dari pixel citra. Metode ini dapat dilakukan dengan melakukan pergantian bit LSB dengan bit data.



Gambar 3 LSB dan MSB

Pada Gambar 3 terdapat sebuah gambar yang menjelaskan tentang salah satu teknik watermarking yaitu metode spasial, yang dapat berupa penggantian bit LSB atau MSB. Jika kita ingin mengubah bit LSB, maka hanya perlu mengubah nilai byte lebih tinggi atau satu lebih rendah dari nilai sebelumnya.

Dikarenakan implementasi image watermarking pada perangkat mobile memiliki keterbatasan melakukan komputasi, maka dalam penulisan skripsi akan menerapakan metode spasial. Selain metode spasial, terdapat juga metode transformasi.

- **Prinsip Kerja (Algoritma) LSB**

Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen suatu data dengan bit-bit data rahasia. Salah satu metode penyembunyian data yang sederhana adalah LSB.

Perhatikan contoh sebuah susunan bit pada sebuah byte:

11010010

MSB LSB

LSB = Least Significant Bit

MSB = Most Siginificant 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 byte tersebut menyatakan warna keabuan tertentu, maka perubahan satu bit LSB tidak mengubah warna keabuan tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil.

Misalkan segmen data sebelum perubahan:

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1

Segmen data setelah ’0 1 1 1 ’ disembunyikan:

0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1

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.

- **BMP (Bitmap Image)**

Bitmap adalah representasi atau gambaran yang terdiri dari baris dan kolom pada titik image graphics di komputer. Nilai dari titik disimpan dalam satu atau lebih data bit. Format file ini merupakan format grafis yang fleksibel untuk platform Windows sehingga dapat dibaca oleh program grafis manapun. Format ini mampu menyimpan informasi dengan kualitas tingkat 1 bit samapi 24 bit.

Tampilan dari bitmap atau raster, menggunakan titik-titik berwarna yang dikenal dengan sebutan pixel. Pixel-pixel tersebut ditempatkan pada lokasi-lokasi tertentu dengan nilai-nilai warna tersendiri, yang secara keseluruhan akan membentuk sebuah tampilan gambar. Tampilan bitmap mampu menunjukkan kehalusan gradasi bayangan dan warna dari sebuah gambar, karena itu bitmap merupakan media elelktronik yang paling tepat untuk gambar-gambar dengan perpaduan gradasi warna yang rumit seperti foto dan lukisan digital.

- ***Peak Signal to Noise Ratio***

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan desibel. Pada penulisan skripsi ini, PSNR digunakan untuk mengetahui kualitas (validasi) dari citra hasil watermark.

- **JAVA 2 MICRO EDITION**

Seperti disebutkan sebelumnya, J2ME dirancang untuk dapat menjalankan program pada perangkat-perangkat semacam telepon genggam dan PDA, yang memiliki karakteristik yang berbeda dengan sebuah komputer biasa, misalnya jumlah kecilnya jumlah memori pada telepon genggam dan PDA. J2ME terdiri atas komponen-komponen sebagai berikut :

- Java Viritual Machine (JVM)
  Komponen ini untuk menjalankan program-program Java. Pada emulator atau *handheld devices*.
- Java API (Application Programming Interface)
  Komponen ini merupakan kumpulan library untuk menjalankan dan mengembangkan program Java pada *handheld devices*.
- *Tools* lain untuk pengembangan aplikasi Java, semacam emulator *Java Phone*, emulator Motorola.

METODE PENELITIAN

Metode penulisan yang digunakan oleh penulis adalah :

a. Studi Pustaka, dimana penulis mendapatkan bahan-bahan untuk penulisan ini dari buku-buku dan membuat aplikasi dengan menggunakan J2ME.
b. Studi Lapangan, dimana penulis mengambil langsung citra-citra yang akan disisipkan *watermark* melalui kamera telepon seluler.

Ada beberapa tahapan-tahapan dalam membuat metode penulisan skripsi ini diantaranya adalah :

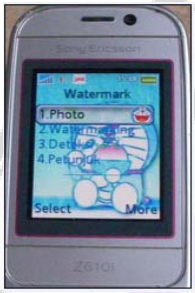
1. Analisis, penulis melakukan Studi Pustaka dan Studi lapangan dalam mengumpulkan data yang berkaitan dengan masalah-masalah yang dihadapi selama penyusunan penulisan skripsi ini.
2. Perancangan, dimana penulis merancang tampilan aplikasi ini dengan struktur navigasi sehingga terlihat jelas arah untuk melakukan penelusuran.
3. Pembuatan, penulis membuat aplikasi ini menggunakan J2ME untuk menulis kode programnya.
4. Generasi kode program, dimana penulis membuat kode programnya dalam J2ME.
5. Pengujian, dimana penulis mencoba menguji menggunakan emulator *Java Phone.*

6. Implementasi, penulis membuat aplikasi ini dan diimplementasikan pada telepon seluler.

HASIL DAN PEMBAHASAN

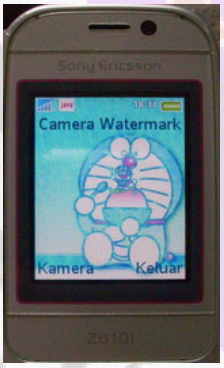
Tampilan Aplikasi Marza

1. Tampilan Menu Utama



2. Tampilan Menu Save As

3. Tampilan Kamera Watermark

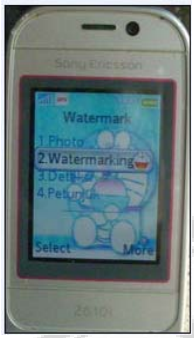


4. Tampilan Video kamera Watermark

5. Tampilan Citra yang Telah Di ambil

6. Tampilan Hasil Proses

7. Tampilan Menu Watermarking



8.Tampilan Tulis Watermark

9. Tampilan Input Kode PIN

10. Tampilan Direktori

11. Tampilan Folder

12. Tampilan File Citra.BMP

13. Tampilan Peringatan

14. Tampilan Hasil Proses Penyisipan Watermark

15.Tampilan Menu Deteksi

16. Tampilan Watermark yang Terdeteksi

17. Tampilan Menu Petunjuk

18. Tampilan Petunjuk Penggunaan

- **Hasil Uji Coba Aplikasi Watermarking yang Dijalankan Pada *Handphone* Sony Ericsson seri Z610i dan Nokia seri N-73.**

Tabel 2: Penyisipan dan Pendeteksian Watermark Pada *Handphone* Sony Ericsson seri Z610i Untuk Watermark yang Berbeda

No	Nama File	Watermark	Kode PIN	SaveAS	Waktu (detik)		Ukuran Citra (KB)
					Penyisipan	Deteksi	
1	EJA JELEK	LINA PINK	36985	EJA JELEK1	59.11	16.16	900
2	LATIHAN1	LUVUMARZA BANGET DEH	6969	COBA_SATU	59.69	16.51	900
3	ELIAS1	ELIAS SEMANGAT	14189	ELIAS2	58.28	16.75	900
4	Sapiqu	Ini namanya KJATA	4508	KJATA	59.52	16.66	900
5	SABAR	SABARRRR	89561	SABAR AJA	59.14	16.55	900
6	MooOo	SAPI	17845	MO	59.44	17.28	900
7	KAMPUS D	KAMPUS D GEDUNG 4	444	KMPSD	01.00.02	16.31	900
8	POHON	LIHAT KEBUNKU	80563	PHN1	59.18	17.60	900
9	ANDRE	ANDRE GRANDONG	78965	GRANDONG	01.00.36	17.48	900
10	FOTO1	LINA LAGE NONTON TV NEH!!	10	TVQU	59.09	17.43	900
Waktu Rata-rata					59.38	16.87	

Tabel 3 : Penyisipan dan Pendeteksian Watermark Pada *Handphone* Sony Ericsson seri Z610i Untuk Watermark yang Sama

Watermark : Smoga Skripsiqu Cpt DiAcc

No	Nama File	Kode PIN	SaveAS	Waktu (detik)		Ukuran Citra (KB)
				Penyisipan	Deteksi	
1	ANDRI	1234	ANDRI1	59.50	17.25	900
2	LPK1	29081	CONVEYER	58.06	16.45	900
3	LPK2	93176	PRAKTIKAN	57.45	16.32	900
4	LPK3	40593	ASTN	59.84	16.23	900
5	PUNCAK1	19860	BARU1	58.91	16.30	900
6	GUNUNG LAGI	70184	JALANBLK	59.51	17.00	900
7	LIBURAN 1	65718	IJOBIRU	57.71	16.15	900
No	**Nama File**	**Kode PIN**	**SaveAS**	**Waktu Penyisipan (detik)**	**Waktu Deteksi (Detik)**	**Ukuran Citra (KB)**
8	NIGHTMARE	36827	VIEW	59.52	16.22	900
9	BANDUNG3	59310	DANAU	57.83	15.43	900
10	BANDUNG1	61094	CIATER	55.20	16.81	900
Waktu Rata-Rata				58.35	16.41	

Tabel 4: Penyisipan dan Pendeteksian Watermark Pada Handphone Nokia seri N-73 dengan Watermark yang Berbeda

No	Nama File	Watermark	Kode PIN	SaveAS	Waktu (detik)		Ukuran Citra (KB)
					Penyisipan	Deteksi	
1	POHOND	POHON	74325	PHN TGI	28.47	09.45	900
2	MOBIL IJO	INI MOBIL WARNANYA IJO	85271	IJO1	29.31	10.38	900
3	SEPATU	SEPATU PUTIH	508	SEPATU 1	28.87	09.88	900
4	BACA KORAN	HOBIQU BACA KORAN	5	KORAN	27.04	07.15	900
5	IBU	IBU LIA YG DUNK2	11522	LIA DUNK2	27.37	08.14	900
6	DIAN	DIAN LPK	85417	DIAN	27.79	10.01	900

				DUNK2			
7	TONG SAMPAH	TONG SAMPAH YG KEREN	7412	TONG	28.32	07.78	900
8	GEDUNG 2	GEDUNG 2 DI D	47831	GDG2	29.49	07.38	900
9	NORMAN	NORMAN	3652	NORMAN1	28.16	09.88	900
10	SEPATU HITAM	SEPATUQU BAGUS SEKALI	66914	SPATU PTH	29.55	09.21	900
Waktu Rata-Rata					28.48	08.93	

Tabel 5 :Penyisipan dan Pendeteksian Watermark Pada Handphone Nokia seri N-73 dengan Watermark yang Sama

Watermark : Smoga Skripsiqu Cpt DiAcc

No	Nama File	Kode PIN	SaveAS	Waktu (detik)		Ukuran Citra (KB)
				Penyisipan	Deteksi	
1	BOBO	36908	OMKIPLI2	28.96	10.90	900
2	GAZEBO	78541	GAZEBO2	29.12	10.38	900
3	SANDAL	58207	SANDAL2	30.43	09.88	900
4	HP	14325	HP2	29.98	07.15	900
5	MOPINKY	80421	MOPINKY2	28.78	08.14	900
6	AIR	52930	AIR2	29.41	10.01	900
7	RUANG	42318	RUANG2	28.30	07.78	900
8	NGASAL	63251	NGASAL2	28.89	07.38	900
9	TAS	21185	TAS2	29.20	09.88	900
10	SEPATU KEREN	96740	SEPATU KEREN2	28.58	09.21	900
Waktu Rata-Rata				29.17	09.08	

Tabel 6 : Hasil perbandingan Citra menggunakan PSNR pada hanndphone Sony Ericsson seri Z610i

No	Nama File	Nama File Setelah Terwatermark	Nilai PSNR (dB)
1	ANDRI	ANDRI1	56.0226
2	LPK1	CONVEYER	46.1347
3	LPK2	PRAKTIKAN	49.9756
4	LPK3	ASTN	52.2866
5	PUNCAK1	BARU1	45.265
6	GUNUNGLAGI	JALANBLK	44.9916
7	LIBURAN1	IJOBIRU	46.7619
8	NIGHTMARE	VIEW	44.05
9	BANDUNG3	DANAU	49.3588
10	BANDUNG1	CIATER	44.5761
11	EJA JELEK	EJA JELEK1	50.0928
12	LATIHAN1	COBA_SATU	45.6277
13	ELIAS1	ELIAS2	48.3418
14	Sapiqu	KJATA	44.9824
15	SABAR	SABAR AJA	49.1546
16	MOoOo	MO	52.0298
17	KAMPUS D	KMPS D	52.3214
18	POHON	PHN1	49.6376
19	ANDRE	GRANDONG	48.2746
20	FOTO1	TVQU	49.7895
Nilai Rata-Rata PSNR			48.4838

Tabel 7: Tabel Hasil Perbandingan Citra Menggunakan PSNR Pada Handphone Nokia seri N-73

No	Nama File	Nama File Setelah Terwatermark	Nilai PSNR (dB)
1	POHON D	PHN TGI	51.5839
2	MOBIL IJO	IJO1	52.7311
3	SEPATU	SEPATU1	50.3067
4	BACA KORAN	KORAN	44.5386
5	IBU	LIA DUNK2	56.8752
6	DIAN	DIAN DUNK2	49.8169
7	TONG SAMPAH	TONG	50.0938
8	GEDUNG 2	GDG2	50.0353

No	Nama File	Nama File Setelah Terwatermark	Nilai PSNR (dB)
9	NORMAN	NORMAN1	47.3987
10	SEPATU HITAM	SPATU PTH	47.7286
11	BOBO	OMKIPLI2	44.8152
12	GAZEBO	GAZEBO2	54.7532
13	SANDAL	SANDAL2	52.0857
14	HP	HP2	49.8019
15	MOPINKY	MOPINKY2	43.4291
16	AIR	AIR2	45.5461
17	DYAH	DI	52.9062
18	NGASAL	NGASAL2	52.0982
19	TAS	TAS2	48.2746
20	SEPATU KEREN	SEPATU KEREN2	48.0575
Nilai rata-rata PSNR			49.6439

KESIMPULAN DAN SARAN

KESIMPULAN

Kesimpulan yang dapat diambil dari aplikasi *watermarking* citra digital pada *mobile device* ini adalah sebagai berikut :

1. Sebuah aplikasi *watermarking* citra digital, telah berhasil penulis ciptakan dengan menggunakan bahasa pemrograman J2ME.
2. Citra-citra yang telah di*watermark* tersebut telah berhasil dihitung nilai kualitasnya menggunakan metode PSNR
3. Waktu yang diperlukan untuk melakukan proses *watermarking* lebih lama dibandingkan waktu untuk ekstraksi atau deteksi dari citra yang telah ter*watermark.*
4. Kecepatan melakukan proses *watermarking* tergantung dari kemampuan dari *mobile device* untuk melakukan proses komputasi.
5. Nilai yang dihasilkan oleh PSNR membuktikan bahwa kualitas citra yang ter*watermark* adalah cukup baik, yaitu rata-rata diatas 40 db.

SARAN

Pada aplikasi *watermarking* citra digital ini, dirasakan masih terdapat kekurangan diantaranya adalah citra yang dihasilkan oleh kamera *watermark* hanya terbatas pada format file bitmap dan untuk menjaga keamanan hak cipta citra pada aplikasi ini, hanya digunakan kode pin saja. Penulis harapkan pada kesempatan yang lain akan ada pengembangan dari aplikasi *watermarking* citra digital pada *mobile device* ini sehingga kamera *watermark* ini dapat menghasilkan format citra yang lain seperti

JPEG, PNG dan lainnya. Jika sudah dapat menghasilkan beragam tipe format file, diharapkan dengan mudah diaplikasikan pada tipe-tipe *handphone* lainnya. Sementara itu untuk memperkuat keamanan hak cipta, diharapkan akan ada metode-metode lainnya yang dapat diterapkan pada algoritma pada aplikasi ini. Sehingga tidak hanya kode pin yang digunakan untuk menjaga keamanan hak cipta pada aplikasi ini.

Selain itu pada skripsi ini pembuatan PSNR tidak di ikutsertakan kedalam aplikasi *Watermarking* tersebut. Semoga pada kesempatan lainnya aplikasi ini dapat disempurnakan sehingga mampu menampilkan nilai PSNR, tampa harus menghitung menggunakan program lainnya.

DAFTAR PUSTAKA

1. Antonius Rahmat, et al, 2005, *Diktat Kuliah multimedia*, Fakultas Teknik Informatika, Universitas Kristen Duta Wacana.
2. Budi Insan, http://budi.insan.co.id/courses/el7010/2003/ msw-report.pdf./ articles/ *Watermarking*.
3. David Kahn, *"Codebreakers : Story of Secret Writting"*, Macmillan, 1987.
4. Hal Berghel, "WatermarkingCyberspace", *Communications of theACM*, Nov.1997, Vol.40, No.11, pp.19-24.
5. Kejariwal Arun, et al., *Energy Analysis of Multimedia Watermarking on Mobile Handheld Device*, 1989.
6. Munir, Rinaldi, 2006, *Diktat Kuliah Kriptografi*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung.
7. P. Mohanty Saraju, *Digital Watermarking*, Departement of Computer Science and Engineering, 2000.
8. Rodiah, 2004. *Makalah Watermarking Sebagai Teknik Penyembunyian Label Hak Cipta Pada Data Digital Menggunakan Algoritma DCT (Discrete Cosinus Transform)*, Universitas Gunadarma, Jakarta.
9. S.P.Mohanty, et al., A Dual Watermarking Technique for Images , Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.
10. Tim Task Force E-Government, *Panduan sistem manajemen kerahasiaan, dan keamanan dokumen elektronik*, Kementerian Komunikasi dan Informasi Republik Indonesia, 2002, draft.
11. W. Bendor, et. al., "*Techniques for Data Hiding*", *IBM Systems Journal*, Vol.35, No.3 and 4, pp. 313-336, 1996. July 1999, pp.1208-1227.