UJI KETAHANAN WATERMARKING PADA DOMAIN WAVELET DAN FREKUENSI TERHADAP SERANGAN *MOTION BLUR* DAN KOMPRESI JPEG

Hendry H. Wahid, Aris Sugiharto, Beta Noranita
Jurusan Matematika FMIPA UNDIP
Jl. Prof. Soedarto, Kampus UNDIP Tembalang, Semarang

Abstrak: *Watermarking* merupakan salah satu metode yang dikembangkan guna melindungi citra digital dari upaya penggandaan secara illegal. Beberapa metode watermarking telah dilakukan pada domain wavelet dan frekuensi. Pada penelitian ini dikaji tentang ketahanan watermarking pada kedua domain dari serangan (*attack*) berupa pengkaburan (*blurring*) dan kompresi JPEG. Sebagai tolak ukur ketahanannya digunakan NC (*Normalized Cross correlation*) dengan membandingkan watermark terekstrak dengan watermark asli.

Kata Kunci : watermarking, kompresi JPEG, *motion blur*, NC.

PENDAHULUAN

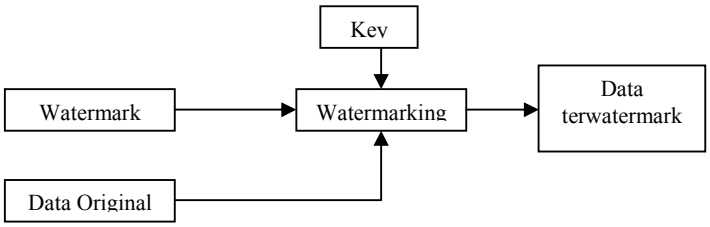
Data digital pada era sekarang ini mengalami perkembangan yang sangat pesat. Banyak data digital dipertukarkan untuk berbagai kepentingan. Mulai dari kepentingan yang positif hingga kepentingan yang negatif. Salah satunya adalah adanya penggandaan secara illegal seperti pembajakan CD, konflik kepemilikan citra digital dan sebagainya. Hal inilah yang mengakibatkan data digital menjadi salah satu pusat perhatian karena kemudahan data ini untuk digandakan tanpa takut atau khawatir akan adanya penurunan kualitas [2]. Sehingga banyak upaya atau metode yang dikembangkan guna melindungi data digital dari upaya penggandaan di atas.

Watermarking hadir sebagai salah satu alternatif untuk melindungi data digital dari usaha orang-orang yang tidak bertanggung jawab yang dengan seenaknya tanpa memperhatikan hak atas kekayaan intelektual (HAKI) dengan melakukan upaya manipulasi dan penggandaan tanpa ijin. Akan tetapi watermarking dalam kenyataannya juga sangat sering mengalami berbagai serangan. Serangan ini dapat berupa serangan alamiah seperti pemrosesan citra pada umumnya seperti proses rotasi, translasi, maupun cropping serta serangan yang benar-benar hanya bertujuan untuk menghilangkan watermark. Diantaranya serangan berupa pemrosesan citra digital seperti pengkaburan citra (*blurring*) dengan *Motion blur* dan kompresi JPEG. Pada penelitian ini diinginkan untuk mengetahui seberapa jauh efek serangan ini terhadap keutuhan watermark.

TINJAUAN PUSTAKA

Watermarking

Watermarking merupakan sebuah metode yang relatif baru yang dimanfaatkan untuk melindungi data digital dari upaya penggandaan atau manipulasi lainnya secara illegal. Watermarking atau tanda air berbeda dengan tanda air pada uang kertas. Tanda air pada uang kertas masih dapat dilihat dengan mata telanjang (pada posisi tertentu), tetapi watermarking pada data digital disini tidak akan dirasakan kehadirannya oleh manusia tanpa menggunakan alat bantu mesin pengolah digital seperti komputer dan sejenisnya. Jadi watermarking dapat diartikan sebagai suatu teknik menyembunyikan data atau informasi "rahasia" ke dalam suatu data lain untuk "ditumpangi", tetapi orang lain tidak menyadari akan kehadiran adanya data tambahan pada hostnya. Sehingga seolah - olah tidak ada perbedaan antara data host sebelum dan sesudah proses watermarking [4].



Gambar 1. Sistem Watermarking

Beberapa aplikasi watermarking yang sering digunakan adalah :

a. *Owner Identification* (tanda pengenalan kepemilikan)
   Pada aplikasi ini pemilik data dapat menanamkan informasi hak cipta pada data host, sehingga usaha untuk menghilangkan informasi hak cipta akan berdampak menurunnya kualitas data host.
b. *Proof of ownership* (Bukti kepemilikan)
   Selain digunakan sebagai tanda pengenalan pemilikan, watermarking juga dapat digunakan sebagai bukti kepemilikan. Pembuktian ini diperlukan bilamana terjadi perselisihan hak kepemilikan atas data digital.
c. *Authentication* (Keaslian)
   Watermarking dapat juga digunakan sebagai teknik untuk membuktikan keaslian suatu data digital. Hal ini disebabkan, watermark akan selalu melekat pada data host. Sehingga jika data host mengalami perubahan baik di crooping atau diubah ke dalam format lainnya maka watermarknya akan selalu bersama dengan data host.
d. *Fingerprinting*
   Fingerprinting digunakan untuk menelusuri penggandaan ilegal terhadap data host. Pemilik data host dapat menananmkan watermark berbeda ke data host yang akan didistribusikan ke pelanggan yang berbeda. Dengan cara ini maka penggandaan ke pihak ketiga akan dapat dideteksi, karena adanya watermark yang berbeda untuk pelanggan yang berbeda.
e. *Medical safety*
   Pada aplikasi ini, watermark yang berupa data pasien (nama, tanggal) dapat ditanamkan ke data host (medical image) sehingga dapat meminimalisir adanya kesalahan data.
f. *Broadcast Monitoring*
   Pada aplikasi ini watermark ditanamkan ke dalam tiap video maupun suara sebelum ditayangkan oleh stasiun televisi atau radio. Untuk itu diperlukan stasiun pengamat otomatis yang akan menerima tayangan tersebut sehingga akan dapat mengekstrak informasi watermark yang dibawa dan sekaligus mencatat informasi tayangan yang muncul.

Motion Blur

Pengkaburan citra sering digunakan dalam proses pelembutan citra yang bertujuan untuk menekan gangguan (*noise*) pada citra. Gangguan pada citra umumnya berupa variasi intensitas suatu *pixel* yang tidak berkolerasi dengan *pixel-pixel* tetangganya. Secara kasat mata, gangguan mudah dilihat oleh mata, karena tampak berbeda dengan *pixel* tetangganya.

Pengkaburan citra didapatkan dengan mengkonvolusikan citra dengan sebuah penapis (filter). Penapis ini disebut juga penapis lolos-rendah (low-pass filter), karena menekan komponen yang berfrekuensi tinggi dan meloloskan yang berfrekuensi rendah.

$g(x,y) = f(x,y) * h(x,y)$

$h(x,y)$: fungsi penapis

Aturan untuk mendapatkan penapis lolos-rendah, adalah :

1) Semua koefisien penapis harus positif.
2) Jumlah semua koefisien harus sama dengan 1

Pengkaburan citra dengan *motion* blur merupakan efek yang disebabkan karena perpindahan objek atau bisa juga karena pergerakan kamera pada saat pengambilan gambar [6].

Fungsi penapis *motion blur* dihasilkan dengan menggunakan fungsi yang sudah ada pada software Matlab7.1 dengan menentukan parameter radius pengakaburan dan sudut yang dibentuk.

Kompresi JPEG

Data digital terutama citra memiliki ukuran file yang cukup besar. Hal ini mengakibatkan adanya beberapa permasalahan yang sering terjadi pada pemrosesan citra. Dengan ukuran file yang cukup besar memberi dampak pada ruang penyimpanan dan waktu transfer data. Untuk itu diperlukan upaya kompromi dengan menggunakan kompresi. Sebenarnya kompresi merupakan upaya dilematis. Disatu sisi menguntungkan karena berkurangnya ukuran file tetapi disisi lain merugikan karena menurunnya kualitas citra.

Kompresi dibedakan menjadi dua jenis, yakni *lossless* dan *lossy*. Pada kompresi *Lossless* diperuntukkan ketika terdapat suatu persyaratan bahwa informasi asli tetap utuh. Pesan asli direkontruksi kembali seperti aslinya. Contoh tipe kompresi in adalah citra GIF dan BMP. Sedangkan kompresi *Lossy* juga menyimpan tempat, tetapi integritas citra asli tidak terjaga. Contoh metode ini terdapat pada citra JPG dan hasil kompresi sangat baik [8].

JPEG adalah salah satu standar kompresi citra yang dikembangkan oleh *Joint Photograpic Expert Group*, yang didesain untuk kompresi citra *full-colour* atau *gray-scale*. JPEG menggunakan metode *lossy* ada

informasi yang hilang, tetapi masih dapat ditolerir oleh persepsi mata. JPEG memanfaatkan keterbatasan mata manusia dalam melihat warna. Mata manusia tidak sensitif terhadap perubahan warna yang kecil, dibandingkan dengan perubahan kecerahan (*brightness*) yang kecil. Tetapi, jika dianalisis menggunakan komputer, akan terlihat kualitas citranya. Kompresi ini sangat cocok sekali diaplikasikan pada foto-foto digital *(Digital Images*).

Untuk mengetahui kualitas citra hasil kompresi, maka dikenal besaran PSNR (*peak signal to noise ratio*). PSNR memiliki satuan *decibel* (dB) yang dihitung untuk mengukur perbedaan antara citra semula dengan citra hasil kompresi dengan rumus [8] :

$$rms = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j) - f'(i,j)]^2}$$

$$PSNR = 20 * \log 10\left(\frac{b}{rms}\right)$$

dimana :

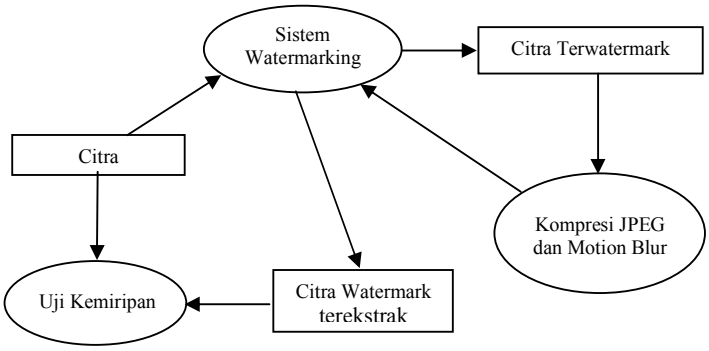
f'(i,j) : *pixel* citra kompresi
f(i,j) : *pixel* citra semula.
b : 255 (nilai maksimum derajat keabuan)
M, N : Lebar dan Tinggi citra

Dari persamaan diketahui, PSNR berbanding terbalik dengan rms. Nilai rms yang rendah yang menyiratkan bahwa citra hasil kompresi tidak jauh berbeda dengan citra semula, akan menghasilkan PSNR yang tinggi. Semakin tinggi nilai PSNR-nya, maka kualitas citra akan semakin bagus, yang artinya bahwa proses kompresi tidak menurunkan kualitas citra, sebaliknya jika nilai PSNR-nya semakin kecil, maka proses kompresi menyebabkan penurunan kualitas citra.

PEMBAHASAN

Metode

Pada penelitian ini digunakan adalah citra digital yang sudah ditanami *watermark* pada domain wavelet dan frekuensi. Metode yang digunakan dapat digambarkan sebagai berikut :



Gambar 2. Metode kompresi JPEG dan Uji kemiripan

Pada tahap awal, citra asli dan citra watermark dengan sistem watermarking [2] dilakukan proses penanaman sehingga diperoleh citra terwatermark. Selanjutnya citra terwatermark dikenakan serangan kompresi JPEG dengan menggunakan parameter quality tertentu dan *Motion Blur* dengan parameter radius dan sudut tertentu. Kemudian citra terwatermark yang telah terkena serangan dengan menggunakan sistem watermarking diekstrak untuk memperoleh citra watermark terekstrak. Citra watermark terekstrak inilah yang akan diuji kemiripannya dengan citra watermark asli. Pengujian dilakukan dengan menggunakan rumus *Normalized Cross Correlation* (NC) [3]

$$NC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sum_i \sum_j [w_{ij}]^2} \quad \text{..... (2)}$$

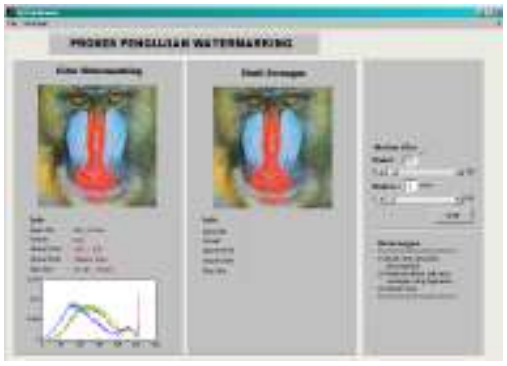
Hasil

Citra yang disimulasikan adalah citra mandrilRGB dengan ukuran 256 x 256 berjenis RGB 24 bit, yang telah ditanami *watermark* pada domain wavelet Daubechies 4 dengan alpa 0.1, 0.5, 1.0, 1.5, 2.0 dan untuk domain frekuensi pada nilai K 10, 50, 100, 150, 200. dan citra watermarknya merupakan citra biner dengan ukuran 20 x 50.

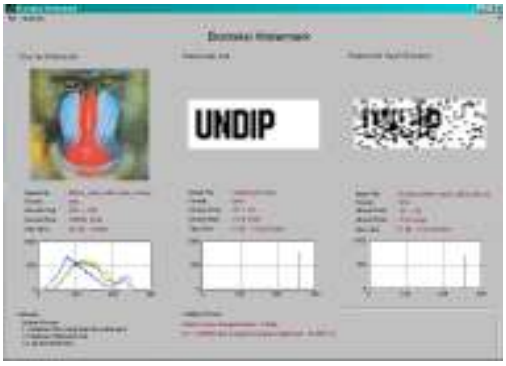
(a) (b)

Gambar 3. (a) Citra mandrilRGB.bmp 256 x 256 yang telah disisipi watermark.
(b) Citra watermark1.bmp 20x50.

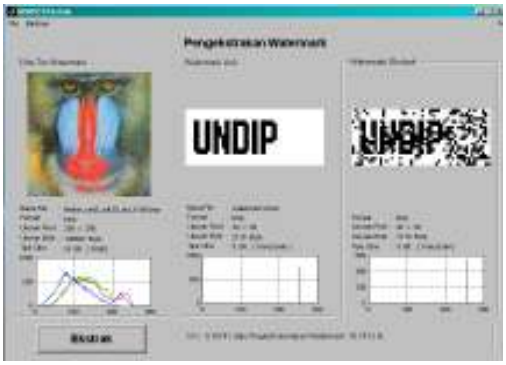
Data - data di atas kemudian disimulasikan dalam simulasi pengujian [7] dan pengekstrakan [10, 11] dengan menggunakan program aplikasi Graphical User Interface (GUI) Matlab 7.1 yang diperlihatkan pada gambar 4.



(a)



(b)

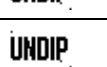
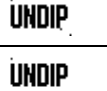


(c)

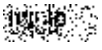
Gambar 4. (a) Pengujian watermark. (b) Pengekstrakan watermark pada domain wavelet, (c) Pengekstrakan watermark pada domain frekuensi

Mula-mula citra mandrillRGB yang telah ditanami *watermark* dilakukan ekstraksi terlebih dahulu untuk mendapatkan nilai NC sebelum dilakukan serangan untuk masing-masing domain pada konstanta alpha dan K yang telah ditentukan. Pada Gambar 5.a diberikan serangan yang berupa *motion blur* pada nilai radius 5 dan sudut 30 atau kompresi JPEG pada nilai kualitas 20. Kemudian citra hasil serangan tersebut diekstrak kembali sesuai dengan domain penanamannya sehingga diperoleh *watermark* terekstrak hasil serangan. dengan nilai NC-nya. Secara lengkap dari beberapa percobaan yang dilakukan diperlihatkan pada beberapa tabel berikut:

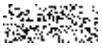
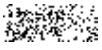
Tabel 1. Hasil Ekstraksi Sebelum Dilakukan Pengujian

HASIL EKSTRAKSI *WATERMARK* PADA DOMAIN WAVELET DAN FREKUENSI					
ALPHA	**Wavelet**		**K**	**Frekuensi**	
	NC	**Watermark Ekstrak**		**NC**	**Watermark Ekstrak**
0.1	0.807		**10**	1	
0.5	0.953		**50**	1	
1.0	0.994		**100**	1	
1.5	0.996		**150**	1	
2.0	0.997		**200**	1	

Tabel 2. Hasil pengujian *watermark* pada serangan *motion blur*

PENGUJIAN *WATERMARK* DENGAN *MOTION BLUR* PADA RADIUS 5 DENGAN SUDUT 30					
Wavelet DB4			**Frekuensi**		
ALPHA	**NC**	**Watermark Ekstrak**	**K**	**NC**	**Watermark Ekstrak**
0.1	0.740		**10**	0.576	
0.5	0.818		**50**	0.655	
1.0	0.856		**100**	0.707	
1.5	0.893		**150**	0.732	
2.0	0.910		**200**	0.748	

Tabel 3 Hasil pengujian *watermark* pada serangan kompresi JPEG

PENGUJIAN *WATERMARK* DENGAN KOMPRESI JPEG PADA NILAI KUALITAS 20					
Wavelet DB4			**Frekuensi**		
ALPHA	**NC**	**Watermark Ekstrak**	**K**	**NC**	**Watermark Ekstrak**
0.1	0.741		**10**	0.576	
0.5	0.774		**50**	0.775	
1.0	0.808		**100**	0.930	
1.5	0.828		**150**	0.995	
2.0	0.852		**200**	0.999	

KESIMPULAN

Dari pembahasan yang telah dilakukan dengan melalui beberapa eksperimen diperoleh kesimpulan bahwa semakin tinggi nilai skala alpha dan K, maka kemiripan atau nilai NC juga semakin tinggi. Untuk serangan *motion blur*, dilihat dari perbedaan nilai NC sebelum dan sesudah dilakukan serangan, untuk domain wavelet perbedaannya tidak terlalu jauh jika dibandingkan domain frekuensi, hal ini menandakan domain wavelet lebih tahan serangan ini daripada domain frekuensi. Untuk serangan kompresi JPEG, dilihat dari nilai NC-nya, ternyata domain frekuensi memberikan hasil yang lebih baik daripada domain wavelet, ini terlihat dari nilai NC yang semakin naik yang mendekati nilai NC awalnya, hal ini menunjukkan pada domain frekuensi untuk serangan ini lebih tahan daripada domain wavelet.

DAFTAR PUSTAKA

[1]. Acharya, Tinku and Ajoy K. Ray, *Image Processing Principles and Application*, John Wiley and Sons Inc., New Jersey, 2005.

[2]. Aris S, *Watermarking Citra Digital dengan Transformasi Wavelet Diskrit*, Tesis Magister Ilmu Komputer, UGM Yogyakarta, 2004.

[3]. Aris S, Helmie A. W., Ketahanan Watermarking terhadap Kompresi JPEG, *Jurnal Matematika dan Ilmu Komputer,* Jurusan Matematika FMIPA UNDIP Semarang, Vol. 8, pp. 13 -18, 2005.

[4]. Bandemer Bernd, *Course Project 4 ECE 642,* http://www.stud.tuilmenau.de/~beba-ii/docs, html, 2003.

[5]. Chio-Ting Hsu and Ja-Ling Wu, Multiresolution Watermarking for Digital Images, *IEE Trans Circuit & System II : Analog & Digital Signal Processing,* Vol. 45, No.8, pp. 1097 – 1101, 1998.

[6]. Cox, I.J., et. al., Watermarking Applications and Their Properties*, Proceedings of the Conf. Information Technology*, 2000.

[7]. Hendry H.W, *Uji Ketahanan Watermarking pada Domain Wavelet dan Frekuensi Terhadap Serangan Pemrosesan Digital dan Kompresi Jpeg*, Tugas akhir S1 Matematika, FMIPA UNDIP.

[8]. Munir Rinaldi, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Penerbit Informatika bandung, 2004.

[9]. Potmesil, Michael, Indranil C., *Modelling Motion Blurr in Computer-Generated Images* , http://www.cs.sunysb.edu/~mueller/ papers/motionBlurPts.pdf

[10]. Priyoyudo,Ady, *Teknik Pembuktian Kepemilikan Citra Digital dengan Watermarking pada Domain Wavelet*, Tugas akhir S1 Matematika, FMIPA UNDIP, 2006.

[11]. Rahmatulloh, Zaki, *Watermarking pada Domain Frekuensi untuk Memberikan Identitas (Watermark) pada Citra Digital*, Tugas akhir S1 Matematika, FMIPA UNDIP, 2006.