

WATERMARKING CITRA DIGITAL DENGAN TRANSFORMASI WAVELET DISKRIT

Digital Images Watermarking with Discrete Wavelet Transform

Aris Sugiharto¹, Agus Harjoko²

Program Studi Ilmu Komputer
Program Pascasarjana Universitas Gadjah Mada

ABSTRACT

At present digital data is used widely for all kind of applications. It is caused by the progress of digital technology. By the digital data can modified easily through all kinds of media especially internet. This ease can be used by the irresponsible party without regard to property right.

Watermarking is a sufficient technique that promises for the proof of possession of digital data. In this research a technique of watermarking digital image using wavelet as transformation media (DWT) is developed. In this technique host image is transformed using wavelet into four frequenci areas LL, LH, HL and HH. To increase the robustness from JPEG compression attack, watermark bits are embedded to LH and HL areas.

The experimental results using three wavelet families daubechies, symlets and coiflet showed that scale factor α has more effect over the type of wavelet. The results also showed that the watermarking technique presented here is robust to JPEG compression.

Keywords : *watermarking, wavelet, DWT, watermark, JPEG compression.*

¹ Fakultas MIPA Universitas Diponegoro, Semarang

² Fakultas MIPA Universitas Gadjah Mada, Yogyakarta

PENGANTAR

Komputer saat ini mengalami perkembangan yang sangat pesat dengan ditunjang kemajuan teknologi IC yang semakin kecil (baik ditinjau dari ukuran dan daya listrik yang digunakan) dan cepat. Dengan perkembangan ini maka data-data dalam bentuk digital semakin banyak digunakan. Sejalan dengan itu, teknologi digital memperlihatkan kemajuan yang pesat pula. Teknologi ini menawarkan berbagi keuntungan, antara lain kemudahan dalam penyebaran tanpa kehilangan kualitas secara signifikan, juga kemudahan dan kemurahan dalam penggandaan serta penyimpanannya untuk digunakan lagi pada saat diperlukan. Kemudahan inilah yang dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab sehingga tidak lagi memperhatikan hak cipta (*Intellectual Property Right*). Untuk itu upaya perlindungan hak cipta terhadap data digital menjadi perhatian serius sehingga banyak cara yang ditempuh untuk memberikan perlindungan data digital.

Watermarking merupakan proses penanaman data (*watermark*) atau label ke dalam suatu objek. Objek bisa berupa teks, citra, audio, dan video. Beberapa karakteristik teknik *watermarking* (Cox et al., 2000) yang harus dipenuhi adalah sebagai berikut.

1. Robustness

Robust artinya *watermark* di dalam *host* data harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti pengkonversian dari digital ke analog atau sebaliknya, kompresi terutama kompresi *lossy*.

2. Tamper Resistance

Yaitu ketahanan sistem *watermarking* terhadap kemungkinan adanya serangan atau usaha untuk menghilangkan, merubah bahkan memberikan *watermark* palsu terhadap suatu *host* data.

3. Fidelity

Yang dimaksud dengan *fidelity* disini adalah derajat degradasi *host* data sesudah diberikan *watermark* dibandingkan dengan sebelum diberikan *watermark*. Biasanya bila *robustness* dari *watermark* tinggi maka memiliki *fidelity* yang rendah sebaliknya *robustness* yang rendah dapat membuat *fidelity* yang tinggi.

4. Computational Cost

Ada beberapa aplikasi yang menuntut proses *watermarking* baik penyisipan maupun pengambilan bekerja secara *real time*, ada juga yang mengharapkan salah satu baik pengambilan atau penyisipan saja yang *real time* ataupun keduanya boleh tidak *real time*.

Penelitian *watermarking* telah banyak dilakukan antara lain pada *domain spasial* (Murinto, 2004), secara sederhana menyisipkan suatu *watermark* ke dalam *the least significant bits* secara random. Sedangkan pada domain frekuensi citra ditransformasi ke dalam domain frekuensi dengan DCT (Handoko, 2003), ataupun DWT.

Dalam penulisan ini akan dibahas bagaimana cara menanamkan *watermark* kedalam citra asli dan mengekstrak *watermark* tersebut dengan menggunakan transformasi DWT. Untuk menguji ketahanan citra ter*watermark* terhadap serangan digunakan kompresi JPEG dengan *quality* yang bervariasi.

CARA PENELITIAN

Teknik *watermarking* dengan menggunakan transformasi DWT memiliki dua tahapan, yaitu :

a. penanaman Watermark

Pada tahapan penanaman *watermark*, citra asli ditransformasikan kedalam koefisien-koefisien *wavelet* sehingga diperoleh empat koefisien *wavelet* yaitu koefisien aproksimasi cA , dan koefisien detil cH, cV, cD . Sedangkan pada citra *watermark* dilakukan proses vektorisasi sehingga diperoleh elemen 0 dan 1. Selanjutnya dilakukan pembangkitan bilangan random dengan menggunakan kunci sebagai *state*. Penanaman *watermark* dilakukan jika vektor *watermark* berisi bit 0. Untuk meningkatkan ketahanan citra *watermark* dari serangan, maka dipilih daerah penanaman (Tokur and Ercelebi, 2003) yaitu :

$$I_{Wuv} = \begin{cases} W_i + \alpha |W_i| x_i & u, v \in HL, LH \\ W_i & u, v \in HH, LL \end{cases} \quad (1)$$

LL ₂	HL ₂	HL ₁
LH ₂	HH ₂	
LH ₁		HH ₁

Gambar 1. Pembagian frekuensi citra hasil transformasi *wavelet* level 2

Untuk memperoleh citra *terwatermark* dilakukan proses pembalikan dengan menggunakan IDWT. Untuk mengetahui kualitas citra *terwatermark* jika dibandingkan dengan citra asli akibat adanya proses penanaman ini, digunakan tolak ukur nilai PSNR (*Peak Signal to Noise Ratio*) yang dirumuskan :

$$PSNR = \frac{XY \max_{x,y} P^2_{xy}}{\sum_{xy} (P_{xy} - \bar{P}_{xy})^2} \quad (2)$$

Secara lengkap tahapan yang dilakukan adalah :

1. Baca citra asli
2. Baca citra watermark
3. Merubah citra watermark menjadi vektor watermark dengan elemennya bit 0 dan 1
4. Menentukan faktor skala
5. Menentukan kunci (state / seed)
6. Generate Random #
7. Transformasi Wavelet Diskrit (DWT) untuk citra asli berdasarkan jenis dan orde wavelet.
8. Kerjakan dari awal sampai panjang vektor watermark
9. Tentukan matriks random horizontal dengan elemen -1, 0, 1
10. Tentukan matriks random vertikal dengan elemen -1, 0, 1
11. Jika elemen vektor watermark = 0

12. Tambahkan matriks horizontal hasil transformasi DWT dengan faktor skala kali matriks horizontal hasil randomisasi.
13. Tambahkan matriks vertikal hasil transformasi DWT dengan faktor skala kali matriks vertikal hasil randomisasi.
14. Citra *terwatermark* diperoleh dengan mentransformasi balik menggunakan IDWT.
15. Konversi citra *terwatermark*.
16. Simpan file citra *terwatermark*
17. Tampilkan citra *terwatermark*.

b. pengekstrakan *Watermark*

Proses pengekstrakan *watermark* digunakan untuk mendapatkan kembali citra *watermark* dari citra yang telah *terwatermark*. Pada langkah ini diperlukan citra *terwatermark* dan citra *watermark* asli yang digunakan untuk menentukan ukuran citra *watermark* yang akan diekstrak. Langkah ini diawali dengan mentransformasi citra *terwatermark* sehingga diperoleh koefisien-koefisien *wavelet* baik koefisien aproksimasi cA, maupun koefisien detail masing-masing cH, cV, dan cD. Kemudian dilakukan proses pseudorandom berdasarkan kunci yang sama pada proses penanaman *watermark*. Langkah selanjutnya adalah menentukan korelasi matriks cH dan cV dengan matriks hasil *pseudorandom*, kemudian dilakukan penghitungan rata-rata kedua korelasi. Rata-rata korelasi ini digunakan untuk mendeteksi adanya *bit watermark* terekstrak. Jika korelasi matriks cH > rata-rata korelasi matriks cH dan korelasi matriks cV > rata-rata korelasi matriks cV maka *bit watermark* terekstrak diberi nilai 0 dan diberi nilai 1 untuk yang lainnya.

Untuk mengetahui kesamaan antara citra *watermark* asli dengan citra *watermark* terekstrak digunakan ukuran kemiripan NC (*Normalized Cross-Correlation*) yang dapat dirumuskan (Hsu and Whu, 1998) :

$$NC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sum_i \sum_j [w_{ij}]^2} \quad (3)$$

Secara lengkap tahapan pengekstrakan *watermark* adalah :

1. Baca citra *terwatermark*
2. Baca citra *watermark* (asli)

3. Merubah citra watermark menjadi vektor watermark yang memiliki elemen-elemen bit 0 dan 1.
4. Menentukan kunci state (harus sama dengan kunci pada proses penanaman)
5. Generate random #
6. Transformasi Wavelet Diskrit (DWT) untuk citra terwatermark berdasarkan jenis dan orde wavelet.
7. Kerjakan dari awal sampai panjang vektor watermark
8. Tentukan matriks random horizontal dengan elemen $-1, 0, 1$
9. Tentukan matriks random vertikal dengan elemen $-1, 0, 1$
10. Menghitung korelasi antara matriks random horizontal dengan koefisien horizontal hasil transformasi langkah 8.
11. Menghitung korelasi antara matriks random vertikal dengan koefisien vertikal hasil transformasi langkah 9.
12. Menghitung rata-rata korelasi horizontal
13. Menghitung rata-rata korelasi vertikal
14. Buat vektor watermark terekstrak sepanjang watermark (asli) dan diisi dengan angka 1.
15. Kerjakan dari awal sampai panjang vektor watermark
16. Jika korelasi matriks horizontal $>$ rata-rata korelasi horizontal dan korelasi matriks vertikal $>$ rata-rata korelasi vertikal.
17. Isi 0 pada vektor watermark terekstrak
18. Ubah vektor watermark terekstrak menjadi matriks watermark terekstrak dengan ukuran watermark (asli).
19. Tampilkan citra watermark terekstrak.

HASIL DAN PEMBAHASAN

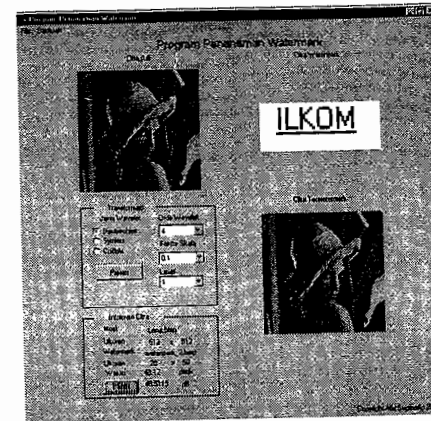
Dalam penelitian ini citra asli yang digunakan adalah citra gray level 256 yang mempunyai ukuran 512×512 serta watermark yang disisipkan berupa citra biner dengan ukuran 50×20 . Gambar 2. memperlihatkan citra asli, sedangkan Gambar 3. merupakan citra watermark.



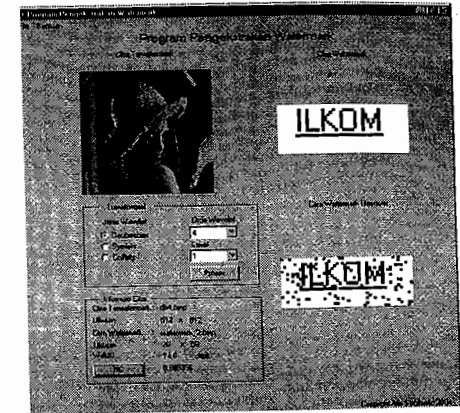
Gambar 2. Citra Asli
Lena 512 x 512

ILKOM

Gambar 3. Citra Watermark
ILKOM 50 x 20



Gambar 4. Tampilan Program
Penanaman Watermark



Gambar 5. Tampilan Program
Pengekstrakan
Watermark

Setelah dilakukan eksperimen dengan menggunakan keluarga wavelet yang berbeda serta nilai faktor skala yang bervariasi diperoleh hasil seperti terlihat pada Tabel 1. dimana wavelet yang digunakan adalah *daubechies 4* watermark ILKOM dan level 1, Tabel 2. menggunakan wavelet *symlets 2* watermark ILKOM dan level 1, dan Tabel 3. menggunakan wavelet *coiflet 3* watermark ILKOM dan level 1.

Tabel 1. Hasil pengujian watermarking dengan menggunakan wavelet *daubechies 4*, watermark_2 dan level 1.

Host : Lena.bmp [512 x 512]
Watermark : ILKOM [20 x 50]
Wavelet : Daubechies 4
Level : 1

Skala	PSNR	Normalized Cross Correlation (NC)				
		Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	48.5115	0.889396	0.783352	0.781072	0.803877	0.893957
0.5	37.5498	0.996579	0.833523	0.86203	0.940707	0.996579
1	31.671	1	0.872292	0.95553	0.989738	1
1.5	28.1887	1	0.931585	0.986317	0.986317	1
2	25.7236	1	0.979475	0.995439	1	1

Tabel 2. Hasil pengujian watermarking dengan menggunakan wavelet Symlet 2, watermark_2 dan level 1.

Host : Lena.bmp [512 x 512]
 Watermark : ILKOM [20 x 50]
 Wavelet : Symlets2
 Level : 1

Skala	PSNR	Normalized Cross Corelation (NC)				
		Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	48.5018	0.871152	0.759407	0.781072	0.77081	0.871152
0.5	37.5741	0.997719	0.803877	0.859749	0.904215	0.997719
1	31.7007	1	0.86317	0.938426	0.992018	0.99886
1.5	28.2180	1	0.91106	0.982896	1	1
2	25.7575	1	0.963512	0.99886	1	1

Tabel 3. Hasil pengujian watermarking dengan menggunakan wavelet Coiflet 3, watermark_2 dan level 1.

Host : Lena.bmp [512 x 512]
 Watermark : ILKOM [20 x 50]
 Wavelet : Coiflet3
 Level : 1

Skala	PSNR	Normalized Cross Corelation (NC)				
		Normal	JPEG25	JPEG50	JPEG75	JPEG100
0.1	48.5235	0.887115	0.779932	0.781072	0.795895	0.882554
0.5	37.5658	0.997719	0.810718	0.871152	0.939567	0.997719
1	31.6859	1	0.858609	0.95439	0.994299	1
1.5	28.2055	1	0.924743	0.992018	1	1
2	25.7391	1	0.970353	0.997719	1	1

Dari tabel-tabel di atas dapat dilihat bahwa jika digunakan faktor skala yang lebih besar akan mengakibatkan penurunan nilai PSNR. Hal ini disebabkan karena nilai *bit watermark* yang ditanamkan akan menjadi lebih besar. Sebaliknya jika digunakan faktor skala yang lebih kecil maka diperoleh nilai PSNR yang tinggi, karena semakin kecil nilai faktor skala akan semakin kecil pula *bit* yang ditanamkan sehingga *noise* yang terdapat pada citra juga semakin sedikit. Hal ini

berbeda dengan nilai NC yang digunakan untuk mengetahui tingkat kemiripan antara citra *watermark* asli dengan citra *watermark* terekstrak. Jika digunakan faktor skala yang lebih besar maka akan diperoleh nilai NC yang lebih besar pula. Sedangkan sebaliknya jika digunakan nilai faktor skala yang lebih kecil maka semakin kecil pula nilai kemiripannya. Sehingga untuk memperoleh teknik *watermarking* yang baik, harus benar-benar dipilih komponen faktor skala yang tepat dengan mempertimbangkan nilai PSNR dan NC.

KESIMPULAN DAN SARAN

Dari hasil penelitian dan pembahasan yang telah dilakukan menunjukkan bahwa pemilihan keluarga *wavelet* yang digunakan pada transformasi tidak memberikan hasil yang signifikan, hal ini bisa dilihat dari nilai PSNR yang tidak terlalu berbeda jika diberikan citra *host*, *watermark*, dan level yang sama. Sebaliknya pemilihan faktor skala α menunjukkan hasil yang signifikan.

Terdapat *trade off* antara kualitas citra terwatermark dengan kemiripan citra *watermark* setelah diekstrak, hal ini dapat dilihat dari nilai PSNR dan NC yang mempunyai kecenderungan (*trend*) berlawanan untuk nilai faktor skala α yang bervariasi.

Secara umum algoritma *watermarking* yang digunakan tahan terhadap serangan kompresi lossy JPEG. Hal ini dapat dilihat dari nilai NC citra *watermark* yang diekstrak cukup tinggi.

SARAN

Teknik *watermarking* masih sangat menantang untuk diteliti lebih lanjut, khususnya yang menggunakan transformasi wavelet diskrit. Penelitian lebih lanjut dapat difokuskan pada penggunaan keluarga wavelet yang lain misalnya *meyer*, *shanon*, *bior* (biortogonal), *mexihat* dan lainnya, sehingga diharapkan akan diperoleh teknik *watermarking* yang benar-benar tahan terhadap segala serangan.

DAFTAR PUSTAKA

Cox, I.J., Kilian, J., Miller, M.L., and Bloom, J.A., 2000, *Watermarking applications and their properties*, Proceedings of the Conf. Information Technology.

- Handoko, T., 2003, *Watermarking pada citra digital dengan Discrete Cosine Transform (DCT)*, tesis Magister Ilmu Komputer, Program Pascasarjana Universitas Gadjah Mada Yogyakarta.
- Hsu Chio-Ting and Wu Ja-Ling, 1998, "Multiresolution Watermarking for Digital Images", *IEE Trans Circuit & System II : Analog & Digital Signal Processing Vol 45 No.8 pp 1097 - 1101*.
- Tokur Y., and Ercelebi, E., 2003, "Wavelet-Based Digital Image Watermarking for Copyright Protection", *International XII Turkish Symposium on Artificial Intelligence and Neural Networks*.