JURNAL MATEMATIKA DAN KOMPUTER
Vol. 7. No. 3, 18 - 25, Desember 2004, ISSN : 1410-8518

WATERMARKING PADA BEBERAPA KELUARGA WAVELET

Aris Sugiharto, Eko Adi Sarwoko
Jurusan Matematika FMIPA Universitas Diponegoro

Abstrak

Teknik Watermarking banyak digunakan untuk melindungi data digital dari upaya pembajakan dalam bentuk penggandaan secara illegal. Banyak metode yang sudah dikembangkan baik dalam domain spasial, frekuensi maupun domain wavelet. Dalam tulisan ini sistem watermarking yang dibahas adalah domain wavelet dengan menggunakan transformasi wavelet diskrit (discrete wavelet transform) yang diujikan pada beberapa keluarga wavelet dengan menggunakan faktor skala yang berbeda.

Kata kunci : *watermarking, wavelet, skala*

1. PENDAHULUAN

Saat ini hampir tidak ada orang yang tidak mengenal komputer. Komputer telah dipakai dalam hampir segala aspek kehidupan. Komputer sebagai alat pengolah digital saat ini hampir dimiliki oleh setiap keluarga yang memiliki taraf kehidupan menengah ke atas. Seperti halnya televisi, komputer saat ini juga banyak digunakan sebagai media hiburan. Dengan perkembangan komputer, data - data dalam bentuk digital semakin banyak digunakan, karena memang komputer yang berkembang saat ini merupakan peralatan elektronik yang menggunakan dan mengolah data dalam bentuk digital. Penggunaan data digital baik berupa teks, suara, citra maupun video sangat pesat dengan adanya komputer , apalagi dengan perkembangan teknologi jaringan antar komputer didunia yang disebut dengan internet, yang memungkinkan pertukaran data digital semakin mudah dilakukan.

Penggunaan data digital selain mudah dalam hal penyebaran, juga disebabkan akan kemudahan dan murahnya biaya penggandaan (peng-copyan) serta penyimpannya untuk digunakan di kemudian hari. Dampak kemudahan inilah yang disalah gunakan tanpa memperhatikan aspek hak cipta (Intelectual Property Right), sehingga perlu dipikirkan adanya perlindungan terhadap hak cipta. Banyak cara yang sudah dilakukan untuk memberikan perlindungan data

digital seperti enkripsi, copy-protection, visible marking, header marking dan lainnya. Tetapi cara tersebut di atas memiliki kelemahan masing - masing. Satu dekade terakhir muncul pemakaian steganography untuk mengatasi masalah perlindungan hak cipta ini pada data digital yang lebih dikenal dengan istilah watermarking.

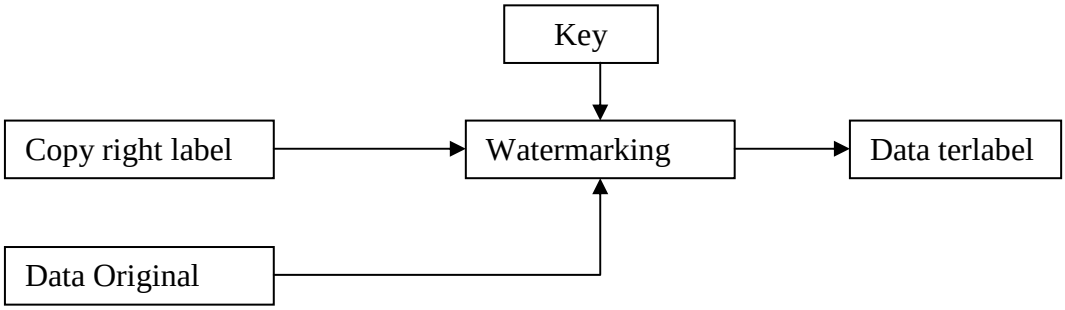
2. TINJAUAN PUSTAKA

Watermarking merupakan salah satu cabang ilmu steganography. Steganography sendiri merupakan suatu cabang ilmu yang mempelajari tentang teknik menyembunyikan suatu informasi (data) "rahasia" di dalam suatu informasi lainnya. Steganography dan cryptography memiliki sejarah yang hampir sama dan keduanya banyak dipakai pada era peperangan. Sedangkan perbedaan dari keduanya terletak pada bagaimana proses menyembunyikan data dan hasil akhir dari proses tersebut. Pada cryptography data asli mengalami proses pengacakan dengan menggunakan teknik enkripsi tertentu sehinga data asli benar-benar berbeda dengan data yang telah terenkripsi. Sedangkan pada steganography suatu data asli disembunyikan dalam suatu data lain yang akan ditumpangi tanpa mengubah data yang ditumpangi (host) tersebut.

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. Jadi seolah - olah tidak ada perbedaan antara data host sebelum dan sesudah proses watermarking [Cox, 2000].

Pada proses watermarking (gambar 1), kunci memegang peranan yang sangat penting. Kunci ini digunakan untuk mencegah adanya usaha penghapusan secara langsung oleh pihak-pihak yang tidak bertanggung jawab, dengan

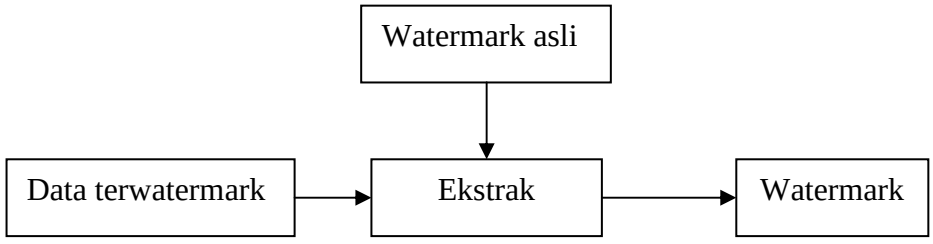
menggunakan teknik enkripsi yang sudah ada. Sedangkan ketahanan terhadap proses - proses pengolahan lainnya itu tergantung pada metode watermarking yang digunakan.



Gambar 1. Proses watermarking

Dari berbagai penelitian yang telah dilakukan belum ada suatu metode watermarking yang ideal sehingga bisa memungkinkan tahan terhadap semua proses pengolahan data digital yang mungkin. Secara umum sistem watermariking memiliki 2 sub bagian yaitu :

1. Proses penyembunyian watermark (gambar 1)
2. Menghasilkan kembali watermark dari data yang telah terwatermark baik menggunakan watermark asli atau tidak.



(a)

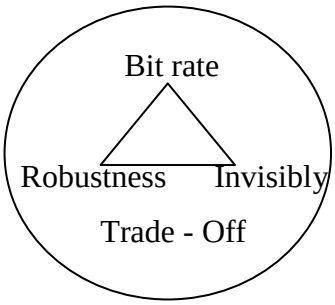
(b)

Gambar 2. (a). Proses ekstraksi dengan watermark asli
(b). Proses ekstraksi tanpa watermark asli

Setiap aplikasi dari watermarking menuntut hal-hal (parameter) yang berbeda dari penerapan metode watermarking. Beberapa parameter yang perlu diperhatikan adalah :

a. jumlah data (bitrate) yang akan disembunyikan.
b. Ketahanan (robustness) terhadap proses pengolahan sinyal.

Trade-off yang terjadi adalah antara kedua parameter (bitrate dan robustness) dengan invisibly (tidak nampak) dapat dilihat pada gambar 3.



Gambar 3. Trade-off Watermarking

Bila diinginkan robustness yang tinggi maka bitrate akan menjadi rendah, sedangkan jika diinginkan invisible yang tinggi maka diperoleh tingkat robustness yang menurun. Sehingga harus dipilih nilai - nilai dari parameter tersebut agar memberikan hasil yang sesuai dengan diinginkan (sesuai aplikasi).

3. PEMBAHASAN

Seperti telah diketahui bahwa pada sistem watermarking umumnya terdiri dari proses penanaman watermark dan pengekstrakan watermark.

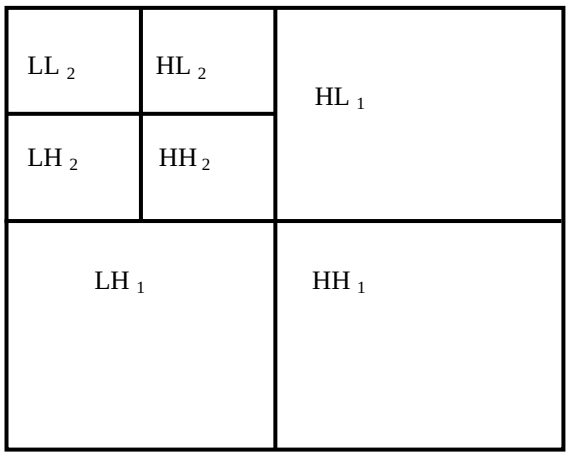
3.1 Penanaman watermark

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, dipilih daerah penanaman [Tokur, 2003] yaitu :

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

.



Gambar 4. Pembagian frekuensi citra hasil transformasi wavelet level 2

Untuk memperoleh citra terwatermark dilakukan proses pembalikan dengan menggunakan invers DWT.

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

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

3.2 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 koefisen-koefisien wavelet baik koefisen aproksimasi cA, maupun koefisen 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 , 1998] :

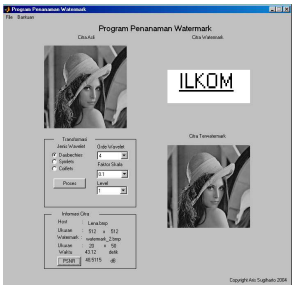
$$NC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sum_i \sum_j [w_{ij}]^2} \qquad (3)$$

3.3 Hasil

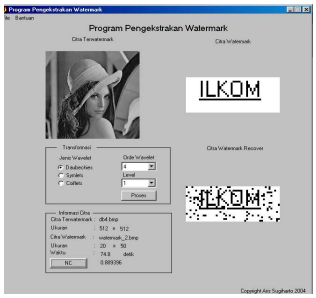
Citra yang akan disimulasikan adalah citra lena dengan ukuran 512 x 512 dalam skala abu-abu 256 dan citra watermarknya merupakan citra biner dengan ukuran 20 x 50. Sedangkan keluarga wavelet yang digunakan untuk transformasi dapat ditentukan sesuai pilihan. Misalnya dipilih daubechies 4 , symlet 2 dan coiflet 3.

Gambar 5. (a) Citra lena.bmp 512x512 (b) Citra watermark_2.bmp 20x50

Semua data di atas kemudian disimulasikan dalam sistem watermarking yang telah dibuat sebelumnya dengan menggunakan program aplikasi Graphical User Interface (GUI) matlab 6.5 [Aris S, 2004].



(a)



(b)

Gambar 6. (a). Simulasi penanaman watermark
(b). Simulasi pengekstrakan watermark

Secara lengkap diperoleh hasil sebagai berikut :

Skala α	PSNR	NC
0.1	48.5115	0.889396
0.5	37.5498	0.996579
1	31.671	1
1.5	28.1887	1
2	25.7236	1

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

Skala α	PSNR	NC
0.1	48.5018	0.871152
0.5	37.5741	0.997719
1	31.7007	1
1.5	28.2180	1
2	25.7575	1

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

Skala α	PSNR	NC
0.1	48.5235	0.887115
0.5	37.5658	0.997719
1	31.6859	1
1.5	28.2055	1
2	25.7391	1

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

4. KESIMPULAN

Dari hasil simulasi sebelumnya dan pembahasan yang telah dilakukan menunjukkan bahwa pemilihan keluarga wavelet yang digunakan pada transformasi tidak memberikan perbedaan 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 perbedaan hasil yang signifikan.

DAFTAR PUSTAKA

Aris S, 2004, "*Watermarking Citra Digital dengan Transformasi Wavelet Diskrit*", Tesis Magister Ilmu Komputer, UGM Yogyakarta

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

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

Yuksel Tokur, Ergun Ercelebi, 2003, *"Wavelet-Based Digital Image Watermarking for Copyright Protection"*, International XII Turkish Symposium on Artificial Intelligence and Neural Networks.