

PERBANDINGAN WATERMARKING CITRA DENGAN ALIHRAGAM WAVELET DAN DISCRETE COSINE TRANSFORM

B. Yudi Dwiandiyanta

Program Studi Teknik Informatika Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta
Jl. Babarsari 43 Yogyakarta Telp 0274487711
Email: yudi-dwi@mail.uajy.ac.id

Abstrak

Watermarking merupakan salah satu metode proteksi hak cipta yang bertujuan untuk menanggulangi penyebaran karya seseorang secara ilegal. Pada dasarnya, watermarking adalah proses penandaan suatu citra dengan pesan hak cipta atau signature yang secara rahasia disisipkan dalam citra namun tidak terlihat perbedaan antara citra asli dengan citra yang telah ditandai. Pada penelitian ini akan dilakukan perbandingan algoritma watermarking yang dilakukan pada kawasan wavelet dan Discrete Cosine Transform (DCT). Sebagai obyek penelitian digunakan citra warna sebagai citra host, sedangkan sebagai citra watermark digunakan citra biner dengan ukuran 1/16 citra host. Proses embedding dilakukan berdasarkan Human Visual System (HVS), sehingga diharapkan diperoleh watermark yang tidak kelihatan (invisible watermark). Proses embedding dilakukan dengan algoritma aditif. Pada kedua alihragam yang dikembangkan, watermark disisipkan pada komponen frekuensi tinggi citra. Wavelet yang digunakan dalam penelitian ini adalah wavelet db4. Sedangkan alihragam DCT yang digunakan adalah operasi blok 4x4, yang diharapkan dapat mengurangi beban komputasi. Berdasarkan pengujian yang dilakukan terhadap algoritma watermarking, menunjukkan bahwa kedua algoritma watermarking yang dikembangkan secara umum tahan terhadap pemberian derau, operasi geometris citra dan operasi-operasi pengolahan citra. Algoritma watermarking yang dikembangkan kurang dapat bertahan terhadap serangan-serangan tapis lolos-bawah dan tapis median. Kedua algoritma watermarking yang dikembangkan mempunyai unjuk kerja yang sangat baik terhadap serangan tapis lolos-atas.

Kata kunci: *alihragam Discrete Cosine Transform (DCT); alihragam wavelet; Human Visual System (HVS); watermarking citra*

Pendahuluan

Dewasa ini perkembangan teknik pengolahan citra sudah sangat pesat. Perkembangan itu didukung pula oleh komputer dengan kapasitas memori yang besar, sehingga memungkinkan untuk melakukan komputasi dalam waktu yang relatif singkat. Banyak aplikasi yang terdapat dalam teknik pengolahan citra, diantaranya adalah peningkatan citra (*image enhancement*), pemulihan citra (*image restoration*), analisis citra (*image analysis*), sistem kompresi data citra (*image compression*), dan sistem keamanan data citra.

Diantara sekian banyak aplikasi pengolahan citra, bidang yang banyak menarik perhatian adalah sistem keamanan data citra. Metode pengamanan data yang telah banyak dilakukan antara lain adalah steganografi, enkripsi, dan *fingerpint*. Saat ini, seiring dengan berkembangnya teknologi informasi, publikasi elektronik, dan sistem distribusi video/citra digital melalui internet, maka diperlukan suatu teknik yang dapat digunakan untuk melakukan proteksi terhadap hak cipta. *Watermarking* merupakan salah satu metode proteksi hak cipta yang bertujuan untuk menanggulangi penyebaran karya seseorang secara ilegal. Pada dasarnya, *watermarking* adalah proses penandaan suatu citra dengan pesan hak cipta atau *signature* yang secara rahasia disisipkan dalam citra namun tidak terlihat perbedaan antara citra asli dengan citra yang telah ditandai. Pesan hak cipta yang disisipkan dapat berupa nomor register (seperti UPC: *Universal Producer Number*) yang sering dijumpai dalam CD, pesan teks, gambar atau logo perusahaan, citra tanda tangan atau sidik jari seseorang ataupun citra foto seseorang.

Teknik *watermarking* yang berkembang saat ini masih memiliki kekurangan dalam hal ketahanan terhadap operasi-operasi pengolahan citra (misalnya penapisan, operasi modifikasi aras keabuan), ketahanan terhadap serangan derau, ketahanan terhadap operasi-operasi geometris (misalnya pemotongan, penyekalaan dan rotasi citra), dan ketahanan terhadap operasi kompresi citra.

Istilah steganografi atau menyembunyikan informasi sejarahnya telah dimulai sejak jaman Yunani kuno ketika seorang raja hendak mengirimkan pesan rahasia yang harus melewati daerah musuh. Raja tersebut memanggil budak kepercayaannya untuk kemudian mentato pesannya diatas kulit kepala. Begitu rambut budak tersebut tumbuh, budak tersebut kemudian dikirim hingga ke tujuannya. Teknik demikian terus berkembang hingga pada abad ke-20,

ketika tentara Jerman menyembunyikan informasi dengan cara menulis pesan dengan tinta yang tidak bisa dilihat. Begitu sampai di tujuan, pesan tersebut diolah sedemikian rupa hingga tulisannya muncul.

Saat ini, seiring dengan kemajuan komputer, teknik steganografi berkembang ke arah bentuk menempelkan logo dalam informasi yang dapat dilihat (*watermarking* tampak), atau logo yang tidak dapat dilihat (*watermarking* tidak tampak) yang disimpan dalam citra digital. *Watermarking* dapat digunakan sebagai bukti kepemilikan dalam persidangan (Langelaar, 2000).

Berdasarkan kawasan penyisipan *watermark*, terdapat dua cara untuk melakukan *watermarking*, yaitu *watermarking* pada kawasan spasial dan *watermarking* pada kawasan frekuensi (Meerwald, 2001). *Watermarking* pada kawasan spasial (Tirkel et. al, 1996; Yeung et. al, 1997; Bartollini et. al, 2001; Queluz et. al. 2000) mudah diimplementasikan dan tidak memerlukan citra asli (*host*) untuk mendeteksi *watermark*. Keunggulan penggunaan *watermarking* pada kawasan spasial adalah beban komputasi yang relatif lebih sedikit, sehingga dapat diimplementasikan untuk aplikasi *real time*. Kelemahan penggunaan *watermarking* pada kawasan spasial adalah kegagalan untuk mendeteksi *watermark* apabila citra telah diolah misalnya dengan penapisan, operasi geometris (*cropping*, penyekalaan citra), dan kompresi. Kelemahan yang lain adalah terjadinya penurunan kualitas citra karena *watermarking* diterapkan langsung pada piksel citra (Wang et. al., 1998).

Watermarking pada kawasan frekuensi dapat dilakukan pada kawasan *Discrete Cosine Transform* (DCT), *Discrete Fourier Transform* (DFT), dan *Discrete Wavelet Transform* (DWT). Cox et al. (1997) dan Koch et al. (1994) telah melakukan penelitian *watermarking* yang dilakukan pada kawasan DCT. Ramkumar et al. (1999) melakukan penelitian *watermarking* yang dilakukan pada kawasan DFT. Penelitian *watermarking* pada kawasan DWT telah banyak dilakukan. Penggunaan keluarga *wavelet* Daubechies dan kode Hamming membuat citra yang telah disisipi *watermark* lebih tampak seperti aslinya (Wang et. al., 1998). Kanai et al. (1998) menggunakan citra poligon sebagai citra *host*, sehingga dapat digunakan untuk melakukan proteksi hak cipta terhadap model-model geometris 3-dimensi. Pereira et al. (1999) menitikberatkan pada optimisasi proses *embedding* dengan menggunakan *linear programming*. *Watermarking* pada kawasan DWT dapat juga dilakukan dengan menggabungkan dengan algoritma kompresi HS (*Hierarchical Segmentation*) dan menggunakan citra medis ROI (*Region of Interest*) sebagai citra *host* (Wakatani, 2002). *Watermarking* dapat digunakan untuk tujuan *image authentication* dengan menggunakan teknik kuantisasi optimal (Paquet, 2002).

Penelitian *watermarking* dengan menggunakan *wavelet* sudah banyak diteliti. *Watermarking* dapat dilakukan dengan menggunakan *wavelet* hingga level ke-3 (Sharma et. al., 2013; Kasyap et. al., 2012). *Watermarking* dengan menggunakan *wavelet* dapat dikembangkan secara robust apabila penyisipan dilakukan pada bagian tepi citra (Razafindradina, et. al., 2013). *Watermarking* yang robust dapat digunakan untuk perlindungan hak cipta (Hemeed et. al., 2006). *Watermarking* dapat juga dilakukan dengan cara menggabungkan *Discrete Wavelet Transform* dan *Discrete Cosine Transform* (Ram, 2013). Penyisipan *watermarking* pada kawasan *wavelet* dapat dilakukan dengan menggunakan metode *alpha blending* (Singh et. al, 2009). Untuk lebih membuat *watermarking* mempunyai sifat *invisible* dan *robust*, maka penyisipan *watermark* dapat dilakukan berdasarkan *Human Visual System* (HVS) (Reddy et. al., 2010). *Wavelet biorthogonal* dapat juga digunakan untuk proses *watermarking* (Prasad et. al, 2012). Agar proses ekstraksi *watermark* tidak membutuhkan citra *host*, maka seringkali dikembangkan teknik *blind-watermarking* (Abdallah et. al, 2011).

Watermarking pada kawasan frekuensi secara umum memberikan perlindungan yang lebih terhadap pengolahan terhadap citra yang telah disisipi *watermark* (Meerwald, 2001). Akan tetapi *watermark* pada kawasan frekuensi umumnya membutuhkan citra asli (*host*) untuk mendeteksi *watermark*. Diantara ketiga jenis kawasan transformasi tersebut, kawasan DWT memiliki kelebihan dalam hal ketelitian analisis terhadap isyarat transformasi (Meerwald, 2001). Koefisien transformasi hasil DWT selanjutnya digabungkan dengan data *watermark* yang telah dipersiapkan guna penggabungan.

Pada penelitian ini akan dilakukan perbandingan algoritma *watermarking* yang dilakukan pada kawasan *wavelet* dan DCT. Diharapkan akan diperoleh perbandingan kedua algoritma terhadap operasi-operasi pengolahan citra, serangan derau, operasi-operasi geometris citra. Proses *embedding* pada kawasan *wavelet* dan DCT dilakukan berdasarkan *Human Visual System* (HVS) dengan obyek berupa citra warna, sehingga diharapkan diperoleh *watermark* yang tidak kelihatan (*invisible watermark*).

Metode Penelitian

Dalam penelitian ini dilakukan tahap-tahap berikut:

1. Pengumpulan bahan

Pengumpulan bahan bertujuan untuk memperoleh literatur yang lengkap tentang bahan yang sedang diteliti. Pengumpulan bahan dilakukan dengan mencari buku, jurnal, tesis yang berhubungan dengan bahan yang sedang diteliti. Pengumpulan bahan dapat memanfaatkan perpustakaan yang sudah ada dan mengakses situs-situs internet yang telah mempublikasikan hasil penelitian. Berdasarkan bahan-bahan yang sudah diperoleh kemudian dilakukan pengembangan terhadap algoritma *watermarking* yang akan diteliti.

2. Perancangan perangkat-lunak

Pada tahap ini dilakukan penyusunan *flowchart* berdasarkan algoritma yang dikembangkan. Penyusunan *flowchart* bertujuan untuk mempermudah penyusunan perangkat-lunak.

3. Pembuatan perangkat-lunak

Hasil rancangan *flowchart* kemudian diimplementasikan dengan menggunakan bahasa pemrograman Matlab. Pembuatan perangkat-lunak dilakukan dalam tahap sbb.

(i) Pembuatan perangkat-lunak proses *embedding*

Proses *embedding* watermark meliputi beberapa fungsi/prosedur sbb.

- Prosedur alihragam wavelet dan DCT
- Prosedur alihragam *wavelet* untuk citra biner
- Prosedur permutasi *pseudo-random*
- Prosedur pemilihan koefisien *wavelet* dan DCT
- Prosedur penyisipan *watermark*
- Prosedur alihragam balik wavelet dan DCT

(ii) Pembuatan perangkat-lunak proses ekstraksi watermark

Proses ekstraksi *watermark* meliputi beberapa fungsi/prosedur sbb.

- Prosedur alihragam wavelet dan DCT
- Prosedur mengekstraksi tiap-tiap subbidang
- Prosedur alihragam balik permutasi *pseudo-random*
- Prosedur rekonstruksi citra *watermark*

4. Pengujian perangkat-lunak

Perangkat lunak yang sudah jadi kemudian diuji dengan menggunakan data citra yang sesungguhnya. Pada tahap ini dilakukan pengujian apakah perangkat-lunak sudah bekerja sesuai dengan yang diinginkan. Revisi perangkat-lunak dapat dilakukan jika program tidak bekerja sesuai dengan yang diinginkan.

(i) Pengujian terhadap pengaruh perubahan *embedding strength*

Pengujian dilakukan bertujuan untuk mengetahui pengaruh perubahan *embedding strength* terhadap algoritma *watermarking* yang dikembangkan.

(ii) Pengujian ketahanan algoritma *watermarking* terhadap serangan

Pada percobaan ini akan digunakan citra *stego* yang sudah mengalami gangguan, yaitu: Operasi-operasi pengolahan citra, misalnya penapisan dan peningkatan kontras citra, pemberian efek derau terhadap citra dan operasi geometris terhadap citra (*cropping* dan *rescaling*).

Alihragam wavelet

Alihragam *wavelet* mempunyai penerapan yang luas pada aplikasi pengolahan isyarat dan pengolahan citra. Ide dasar alihragam *Discrete Wavelet Transform* (DWT) 1-dimensi adalah seperti berikut. Isyarat dibagi menjadi dua bagian, frekuensi tinggi dan frekuensi rendah. Bagian frekuensi rendah dibagi lagi menjadi isyarat frekuensi tinggi dan rekuensi rendah. Proses ini diulang sampai isyarat tidak dapat didekomposisikan lagi atau sampai pada level yang telah ditentukan pengguna. Beberapa aplikasi pengolahan citra secara umum tidak memerlukan lebih dari 5 level dekomposisi (Meerwald, 2001). Isyarat asli dapat dipulihkan dengan menerapkan invers DWT (IDWT) pada isyarat yang telah didekomposisi.

Embedding dengan algoritma aditif

Pada *watermarking* dengan algoritma aditif, data *watermark* disisipkan ke dalam citra *host* dengan menggunakan persamaan:

$$f'(m,n) = f(m,n)(1 + \alpha w_i) \quad (1)$$

dengan $f(m,n)$ adalah koefisien data *host* yang sudah dimodifikasi, α adalah faktor *embedding strength*, $f(m,n)$ adalah koefisien citra *host*, dan w_i adalah citra *watermark*. Alternatif yang lain, *embedding* dapat dilakukan dengan menggunakan persamaan:

$$f'(m,n) = f(m,n) + \alpha w_i \quad (2)$$

Ekstraksi *watermark* dapat dilakukan dengan menggunakan informasi citra *host* dan informasi citra *stego* yang ada. Ekstraksi dapat dilakukan dengan menggunakan persamaan:

$$w_i^* = \frac{f^*(m,n) - f(m,n)}{\alpha f(m,n)} \quad (3)$$













dengan w_i^* adalah citra *watermark* hasil ekstraksi dan $f^*(m,n)$ adalah citra yang diterima.

Hasil dan Pembahasan







Pada simulasi komputer digunakan citra *host* berupa citra warna dengan ukuran 512x512 dan citra *watermark* berupa citra biner dengan ukuran 128x128. Penggunaan citra biner sebagai *watermark* karena citra biner umumnya

berukuran kecil dan dapat dengan mudah disisipkan ke citra *host* secara tak terlihat. Informasi mengenai logo perusahaan, logo universitas, tandatangan, ataupun *barcode* sudah sangat mencukupi jika direpresentasikan menggunakan citra biner. Citra biner juga lebih tahan terhadap serangan yang ingin melemahkan atau membuang *watermark*. Citra biner yang mengalami kehilangan informasi, secara pola masih dapat dikenali. Berbeda kalau digunakan teks sebagai *watermark*, perubahan yang terjadi hanya pada satu bit teks akan mengubah informasi *watermark* secara signifikan. Beberapa contoh hasil penelitian dapat dilihat pada Tabel 1 dan Tabel 2.

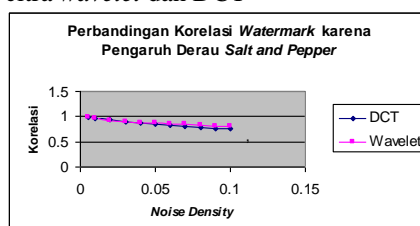
Tabel 1. contoh hasil *watermarking* menggunakan alihragam *wavelet*

Jenis Serangan	Citra Stego	Citra <i>Watermark</i> Hasil Ekstraksi
Derau <i>Salt and Pepper</i> dengan densitas 0,01		
Derau Gaussian dengan varians derau 0,005		
Pemotongan sebesar 25%		
Tapis Lolos-Atas		
Perubahan nilai <i>brightness</i> sebesar +50		
Perentangan Kontras menggunakan <i>Histogram Equalization</i>		

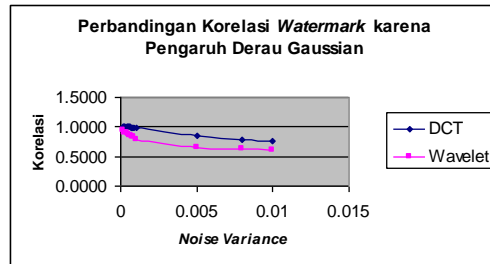
Tabel 2. Contoh Hasil *Watermarking* menggunakan Alihragam DCT

Jenis Serangan	Citra Stego	Citra <i>Watermark</i> Hasil Ekstraksi
Derau <i>Salt and Pepper</i> dengan densitas 0,01		PS2 TEUGM Yogya
Derau Gaussian dengan varians derau 0,005		PS2 TEUGM Yogya
Pemotongan sebesar 25%		PS2 TEUGM Yogya
Tapis Lolos-Atas		PS2 TEUGM Yogya
Perubahan nilai <i>brightness</i> sebesar +5		PS2 TEUGM Yogya
Perentangan Kontras menggunakan <i>Histogram Equalization</i>		PS2 TEUGM Yogya

Berdasarkan penelitian yang dilakukan, terdapat beberapa persamaan karakteristik antara strategi *embedding* yang dilakukan pada subbidang detail citra *wavelet* dan DCT

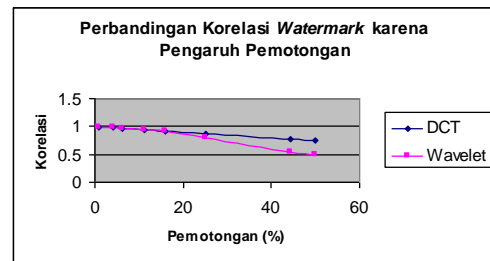


Gambar 1. Grafik perbandingan korelasi *watermark embedding* pada kawasan *wavelet* dan DCT karena pengaruh derau *salt and pepper*



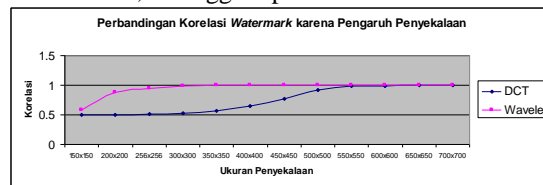
Gambar 2. Grafik perbandingan korelasi watermark embedding pada kawasan wavelet dan DCT karena pengaruh derau Gaussian

Berdasarkan grafik pada Gambar 1, embedding yang dilakukan pada kawasan wavelet lebih kebal terhadap derau saltandpepper. Sebaliknya (Gambar 2) embedding dilakukan pada kawasan DCT lebih kebal terhadap derau Gaussian. Jumlah level dekomposisi akan berpengaruh terhadap ketahanan sistem watermarking terhadap derau Gaussian dan saltandpepper. Pada embedding yang dilakukan pada subbidang detail citra, pemilihan embeddingstrength dapat dipilih dengan nilai yang lebih besar, sehingga diperoleh watermarking yang lebih tahan terhadap serangan derau.



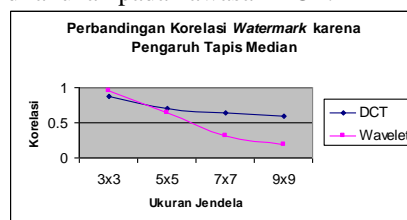
Gambar 3. Grafik perbandingan korelasi watermark embedding pada kawasan wavelet dan DCT karena pengaruh pemotongan citra

Berdasarkan Gambar 3, terlihat bahwa semakin besar pemotongan citra maka akan semakin kecil korelasi watermark yang diperoleh. Hal ini disebabkan proses pemotongan citra akan menghilangkan informasi watermark yang ada. Pada embedding yang dilakukan pada subbidang detail citra, pemotongan yang dilakukan pada daerah yang halus akan menghasilkan korelasi watermark yang lebih baik dibandingkan pemotongan yang dilakukan pada daerah yang tajam/detail citra. Hal ini disebabkan sifat embedding yang dilakukan pada frekuensi tinggi akan menyembunyikan informasi watermark pada detail citra. Jika pemotongan dilakukan pada detail citra, maka akan banyak menghilangkan informasi watermark, sehingga diperoleh korelasi watermark yang lebih rendah.

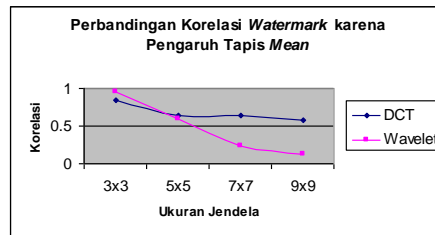


Gambar 4. Grafik perbandingan korelasi watermark embedding pada kawasan wavelet dan DCT karena pengaruh penyekalaan citra

Berdasarkan Gambar 4, terlihat bahwa semakin besar perbedaan ukuran penyekalaan terhadap citra asli maka akan semakin kecil korelasi watermark yang diperoleh. Hal ini disebabkan proses penyekalaan akan menghilangkan informasi watermark yang ada. Terhadap penyekalaan citra, terlihat penyisipan pada kawasan wavelet lebih unggul dibandingkan dengan penyisipan yang dilakukan pada kawasan DCT.



Gambar 5. Grafik perbandingan korelasi watermark embedding pada kawasan wavelet dan DCT karena pengaruh tapis median



Gambar 6. Grafik perbandingan korelasi *watermark embedding* pada kawasan *wavelet* dan DCT karena pengaruh tapis *mean*

Berdasarkan grafik pada Gambar 5 dan 6, *embedding* yang dilakukan pada kawasan DCT lebih kebal terhadap serangan tapis *mean* dan tapis median. Rendahnya nilai korelasi *watermark* disebabkan penyisipan *watermark* dilakukan pada frekuensi tinggi atau bagian detail citra, sedangkan sifat tapis median adalah menghaluskan citra atau menghilangkan titik-titik yang terisolasi yang kebanyakan berkontribusi komponen frekuensi tinggi citra. Dengan berkurangnya komponen frekuensi tinggi citra, maka informasi *watermark* yang disisipkan pada kawasan frekuensi tinggi citra secara otomatis akan berkurang juga.

Kesimpulan

Operasi-operasi pengolahan citra (penapisan, perubahan *brightness* dan penyamaan histogram) akan menyebabkan turunnya nilai korelasi *watermark* yang diurai. *Watermarking* citra yang dilakukan dengan alihragam *wavelet* dan DCT mempunyai keunggulan lebih kebal terhadap serangan-serangan tapis lolos-atas, perubahan *brightness* dan penyamaan histogram, namun kurang dapat bertahan terhadap serangan-serangan tapis lolos-bawah dan tapis median.

Pemberian derau terhadap citra *stego* akan menyebabkan turunnya nilai korelasi *watermark* yang diurai. Semakin banyak derau akan semakin turun nilai korelasi *watermark* yang diperoleh. *Embedding* yang dilakukan pada kawasan *wavelet* lebih kebal terhadap derau *saltandpepper*. Sebaliknya *embedding* dilakukan pada kawasan DCT lebih kebal terhadap derau Gaussian.

Proses pemotongan dan penyekalaan citra akan menyebabkan turunnya nilai korelasi *watermark* yang diurai. Semakin besar pemotongan citra maka akan semakin turun nilai korelasi *watermark* yang diperoleh. Semakin berbeda ukuran penyekalaan terhadap ukuran citra asli maka nilai korelasi *watermark* yang diperoleh juga akan semakin turun. Terhadap penyekalaan citra, terlihat penyisipan pada kawasan *wavelet* lebih unggul dibandingkan dengan penyisipan yang dilakukan pada kawasan DCT.

Daftar Pustaka

- Abdallah, H.A., Hadhoud, M.M., Shaalan, A.A., dan El-Samie F.E.A., (2011), "Blind Wavelet-Based Image Watermarking", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 4, No. 1, March 2011, pp. 15 – 28.
- Bartollini, F., A. Tefas, M. Barni, and I. Pitas, (2001), "Image Authentication Techniques for Surveillance Application", *Proceedings of the IEEE*, Vol. 89, No. 10, pp. 1403-1418.
- Cox, I.J., J. Kilian, F.T. Leighton, and T. Shamoon, (1997), "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transaction on Image Processing*, Vol. 6, No. 12, pp. 1673-1687.
- Hameed, K., Mumtaz, A., dan Gilani S.A.M., (2006), "Digital Image Watermarking in the Wavelet Transform Domain", *World Academy of Science, Engineering and Technology* 13, pp. 86 – 89.
- Kanai, S., H. Date, and T. Kishinami, (1998), "Digital Watermarking for 3D Polygon using Multiresolution Wavelet Decomposition", Department of Systems Engineering, Hokkaido University, Sapporo, Japan.
- Kasyap, N., dan Sinha G.R., (2012), "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", *I.J.Modern Education and Computer Science*, Vol 3, pp. 50-56
- Koch, E., J. Rindfrey, and J. Zhao, (1994), "Copyright Protection for Multimedia Data", *Proc. Int. Conf. Digital Media and Electronic Publishing*.

- Langelaar, G.C., (2000), “*Real Time Watermarking Techniques for Compressed Video Data*”, Master Thesis, Delft University of Technology, Universal Press, Veenendaal.
- Meerwald, P., (2001), “*Digital Image Watermarking in the Wavelet Transform Domain*”, Master Thesis, Computer Science, University of Salzburg, Austria.
- Paquet, A.H. and R.K. Ward, (2002), “*Wavelet Based Digital Watermarking for Image Authentication*”, University of British Columbia, Department of Electrical and Computer Engineering, Canada.
- Pereira, S., S. Voloshynovskiy, and T. Pun, (1999), “*Optimized Wavelet Domain Watermark Embedding Strategy Using Linear Programming*”, University of Geneva – CUI, Geneva, Switzerland.
- Prasad, B.R., Kota, K.V., Reddy, B.M., (2012), “Biorthogonal Wavelet Transform Digital Image Watermarking”, *International Journal of Advanced Computer Research*, Vol 2, No 3, pp. 84 – 89.
- Queluz, M.P. and P. Lamy, (2000), “Spatial Watermark for Image Verification”, *SPIE Conference on security and Watermarking of Multimedia Contents II*, Vol. 3971, pp. 120-130.
- Ram, B., (2013), “Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform”, *International Journal of Advancements in Research & Technology*, Volume 2, Issue4, April-2013 pp.19 – 27.
- Ramkumar, M., A.N. Akansu, and A.A. Alatan, (1999), “A Robust Data Hiding Scheme for Images Using DFT”, in *Proceedings of the 6th IEEE International Conference on Image Processing ICIP 99*, pp. 211-215.
- Razafindradina , H.B., dan Karim, A.M., (2013), “Blind And Robust Images Watermarking Based On Wavelet And Edge Insertion”, *International Journal on Cryptography and Information Security (IJCIS)*, Vol.3, No. 3, pp. 23 – 30.
- Reddy, V.P., dan Varadarajan, S., (2010), “An Effective Wavelet-Based Watermarking Scheme Using Human Visual System for Protecting Copyrights of Digital Images”, *International Journal of Computer and Electrical Engineering*, Vol. 2, No. 1, February, (2010), pp. 32-40.
- Sharma, P. dan Swami, S., (2013), “Digital Image Watermarking Using 3 level Discrete Wavelet Transform”, *Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013)*, pp. 129 - 133.
- Singh, A.P., dan Mishra, A., (2009), “Wavelet Based Watermarking on Digital Image”, *Indian Journal of Computer Science and Engineering*, Vol 1, No 2, pp. 86-91.
- Tirkel, A.Z., C.F. Osborne, and R.G. Schyndel, (1996), “Image Watermarking a Spread Spectrum Technique”, *IEEE 4th International Symposium on Spread Spectrum Techniques and Applications*, Vol. II, pp. 785-789.
- Wakatani, Akiyoshi, (2002), “Digital Watermarking for ROI Medical Images by using Compressed Signature Image”, *Proceedings of the 35th Hawai International Conference on System Sciences*.
- Wang, Houngh-Jyh Mike, Su, Po-Chyi and C. Jay Kuo, (1998), “*Wavelet-based Digital Image Watermarking*”, Department of Electrical Engineering-Systems University of Southern California, Los Angeles.