DIGITAL IMAGE WATERMARKING (DIW) YANG TAHAN TERHADAP TRANSFORMASI GEOMETRIS

DIGITAL IMAGE WATERMARKING (DIW) *ROBUST TO GEOMETRIC TRANSFORMATIONS*

Yoiceta Vanda[1], Setyawan Ary Cahyono[2]
Program Studi Teknik Elektronika, Akademi Teknologi AUB Surakarta
Jl. M.W. Maramis No.29 Nusukan, Banjarsari, Surakarta, Jawa Tengah, Indonesia.
[2] Program Studi Teknik Elektronika,Akademi Teknologi AUB Surakarta,
Jl. M.W. Maramis No.29 Nusukan, Banjarsari, Surakarta, Jawa Tengah, Indonesia.
E-mail : yoiceta@yahoo.com

Abstract

Digital images can be easily copied and distributed illegally using widely available software tools. Watermarking methods that embed side information into images with the aim of protecting copyright have been proposed. So far, these methods have been defeated by simple attacks such as rotation, translation and scaling. In this research, a novel digital image watermarking system that takes advantage of the Wavelet Transform properties to embed a spread spectrum circular symmetric watermark in an image is proposed. Watermark robustness against translation, rotation and scaling attacks is achieved by the proposed method. Successful experiments showing the performance of the method to geometric.

Key words: *watermarking, mark, wavelet, spread spectrum circular symmetric*

1. PENDAHULUAN

Dengan perkembangan komputer digital dan perangkat-perangkat lainnya yang serba digital, telah membuat data digital banyak digunakan. Ada beberapa faktor yang membuat data digital (seperti audio, citra, video, dan teks) banyak digunakan, antara lain:

- Mudah diduplikasi dan hasilnya sama dengan aslinya
- Murah untuk penduplikasian dan penyimpanan
- Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut
- Serta mudah didistribusikan, baik dengan media disk maupun melalui jaringan seperti internet.

Dengan adanya Internet sebagai sistem jaringan terluas di dunia yang menghubungkan hampir seluruh komputer-komputer dunia, membuat semua komputer di dunia ini semakin mudah untuk bertukar data.

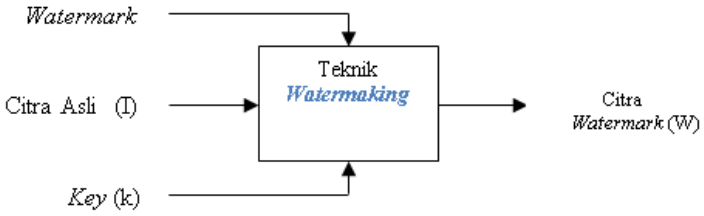
Akibat dari perkembangan internet yang begitu pesat, memungkinkan orang untuk mengakses semua jenis informasi dengan bebas tanpa ada batasan. Apalagi untuk data yang berbentuk digital, seperti citra, video, dan MP3 mudah sekali untuk diggandakan, dan disebarkan sesuai keinginan kita. Kadang hal tersebut membuat kita mudah untuk mendapatkan sebuah data untuk kepentingan kita, tapi lain halnya jika digunakan untuk hal negatif.

Dalam bentuk digital, penyebaran karena pengkopian sangat sulit dihentikan ataupun dibawa ke pengadilan, karena hasil kopian tersebut sama persis dengan yang asli. Untuk itu diperlukan teknik tertentu untuk menjaga hak cipta sebagai *'intellectual property"* pada keaslian atau keotentikasian berkas data dan penyebaran secara ilegal tersebut dapat dilacak.

Untuk mengatasi masalah tersebut, diperlukan suatu teknik lainnya agar data dapat dilacak asal – usulnya, yang dikenal dengan teknik pengamanan *Watermarking*. Tujuan teknik *watermarking* adalah untuk proteksi *copyright* dengan menambahkan 'mark', yang umumnya berguna untuk mengidentifikasi pemilik yang sah. Mark dapat berupa nomor register (seperti UPC : *Universal Producer Number*) yang dijumpai dalam CD, pesan teks, atau gambar berupa logo. Sedangkan data yang hendak diberi *watermark* umumnya berupa citra.

ISBN 978-602-99334-4-4

Citra yang telah disisipi *mark* akan diberi serangan atau biasa disebut *attack*. Serangan ini biasanya adalah serangan yang biasa dilakukan pada pengolahan citra, yaitu transformasi geometris seperti rotasi, penskalaan, dan pemotongan. Juga akan dilakukan kompresi, *filter adaptif*, dan *filter median*.



Gambar 1.1 Konsep *Watermarking*

Komponen *key* pada gambar diatas digunakan untuk mencegah penghapusan secara langsung oleh pihak yang tidak bertanggung jawab. Jadi *watermarking* merupakan teknik untuk penyembunyian atau penanaman data tertentu ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia, dan mampu menghadapi proses – proses pengolahan sinyal digital pada tahap – tahap tertentu. Dalam *watermarking*, proses – proses pengolahan sinyal digital disebut dengan istilah serangan dalam teknik *watermarking*. Apabila citra yang sudah ter-*watermark* dikenai serangan, dan hasilnya tidak mengalami perubahan, maka dikatakan *watermark* tahan terhadap serangan.

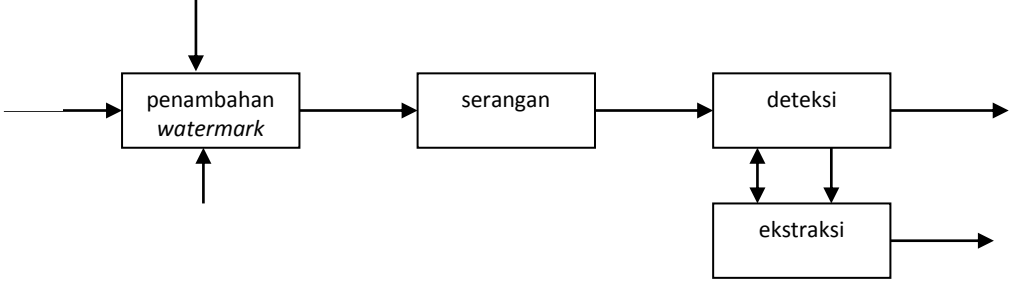
Penelitian yang telah dilakukan pertama kali oleh Bruyndonckx dkk [2], yang mengusulkan dasar kalsifikasi piksel *region*, penelitian ini dilakukan dalam domain spatial. *Frequency Domain Watermarking* diperkenalkan oleh Cox dkk [4] dan Bolland [5]. Pendekatan Cox menggunakan teknik penyebaran spektrum untuk mengabungkan bit tunggal dalam citra. Bagaimanapun teknik ini membutuhkan gambar asli untuk membaca kode *watermark*. Smith dkk [6] mengacu pada pendekatan – pendekatan diatas (ketika gambar asli dibutuhkan dalam proses pembacaan kode). Koch dkk melaporkan teknik domain DCT yang efisien dan tahan terhadap kompresi JPEG.

Pendekatan yang diharapkan akhirnya diusulkan oleh Ruanaidh dkk [8], dimana *watermark* disembunyikan dalam *Fourier – Merlin transform domain*. Penyembunyian *watermark* dalam domain ini, akan membuat *watermark* tersebut tahan terhadap rotasi, penskalaan, dan translasi. Satu kelemahan dari metode ini adalah pemetaan spektrum *Fourier* dalam koordinat *Log – Polar* yang terkadang bisa menurunkan kualitas citra yang di-*watermark.*

Pitas dkk [20] mengajukan metode penempatan *watermark* ganda sepanjang pusat sirkulasi dalam frekuensi nol dari *magnitude fourier transform* dari citra. Metode ini ditunjukkan sebagai metode yang efisien terhadap serangan rotasi tidak lebih dari 3^0 dan begitu juga dengan penskalaan dan translasi.

1.1 Model Sistem Watermarking Secara Umum

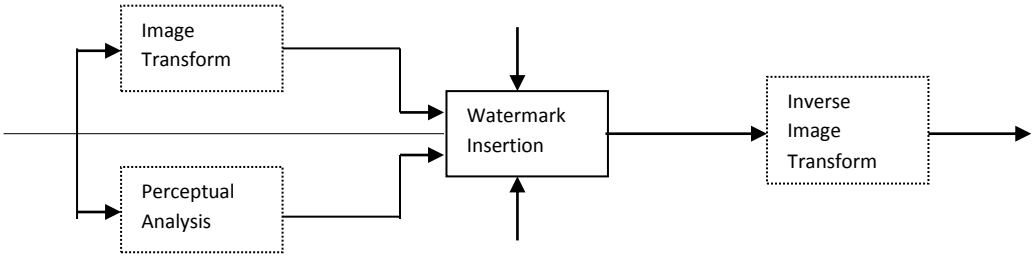
Heileman dkk [15] mengusulkan tentang model umum untuk sistem *watermarking*, yang direpresentasikan dengan sedikit modifikasi seperti yang tampak pada gambar 1.2. *I* adalah citra asli. *W* sebagai *watermark* yang disisipkan dalam *I* menggunakan kunci khusus *k* dan I_ω sebagai citra *watermarked* yang mengandung *watermark*. Citra *watermarked* setelah mendapatkan serangan kita lambangkan dengan $\hat{I}_\omega$. Ini merupakan tujuan dari proses ekstraksi dengan menambahkan *watermark* dalam W dari I_ω atau $\hat{I}_\omega$. Hal ini dimungkingkan dilakukan dengan tujuan ada atau tidaknya *watermark* dalam menganalisa citra. Hal ini dilakukan dalam proses deteksi.



Gambar 1.2 Model Sistem *Watermarking* secara umum

1.2 Proses Penyisipan

Proses penyisipan *watermarking* ditunjukkan dalam gambar 1.3. Seperti yang telah disebutkan sebelumnya bahwa *watermark* dapat disisipkan melalui domain spatial ataupun domain frekuensi dari sebuah citra. Pertimbangan ini diambil dengan menjumlahkan model – model yang ada. Kita juga dapat menyisipkan *watermark* dalam komponen yang signifikan dari image untuk menambahkan kekuatan pada *watermark.*



Gambar 1.3 Proses Penyisipan *Watermark*

Gambar diatas menunjukan garis tidak putus – putus yang menunjukkan proses penyisipan *watermark*. Garis putus – putus menunjukkan operasi pilihan. Yaitu model – model secara umum yang dapat disisipi *watermark* baik dalam domain frekuensi ataupun domain spatial. Analisis perceptual dipilih, dan metode yang digunakan untuk penyisipan *watermark* biasanya mudah, dan penelitian dilakukan untuk menutupi kekurangan dari penglihatan manusia.

1.3 Serangan Dalam Watermarking

Serangan atau gangguan dalam teknik *watermarking* adalah segala upaya yang dilakukan untuk menghilangkan data *mark* [Licks, 1999]. Setelah data mark dapat dihilangkan, selanjutnya dapat mengkopi citra tersebut dan mendistribusikannya. Serangan umum dalam teknik *watermarking* yaitu transformasi geometris (penskalaan, rotasi, pemotongan, dan kompresi).

1.3.1 Penskalaan

Penskalaan sumbu dalam kawasan spatial menyebabkan kebalikan penskalaan dalam kawasan *wavelet*, yaitu untuk dua skalar a dan b, dinyatakan sebagai berikut:

$$I(ax,by) \leftrightarrow \frac{1}{|ab|} F\left(\frac{u}{a},\frac{v}{b}\right) \tag{1.1}$$

1.3.2 Rotasi

Bila pasangan SWT dan ISWT dipresentasikan dalam koordinat polar [Licks, 1999] sebagai berikut:

$$x = r\cos\theta,\ y = r\sin\theta$$
$$u = w\cos\phi,\ v = w\sin\phi \tag{1.2}$$

maka bentuk notasi I(x,y) dan F(u,v) menjadi I(r,θ) dan F(W,ϕ). Rotasi citra dengan sudut θ_0 menyebabkan *watermarking* berotasi dengan sudut sama, yaitu:

$$I(r,\theta+\theta_0) \leftrightarrow F(w,\phi+\theta_0) \tag{1.3}$$

1.3.3 Pemotongan

Bila F(u,v) dan I(x,y) merupakan fungsi periodis dengan periode N, maka terdapat relasi sebagai berikut:

$$F(u,v) = F(u+N,v+N) \tag{1.4a}$$
$$I(x,y) = I(x+N,y+N) \tag{1.4b}$$

Lebih lanjut dalam kesimetrisan konjugasi, diperlihatkan bahwa lF(u,v)l = lF(-u,-v)l, sehingga untuk pemotongan berlaku hubungan:

$$I(x-N,y-N) \leftrightarrow F(u-N,v-N) \tag{1.5}$$

1.3.4 Kompresi JPEG

Dari kenyataan tersebut, kompresi dapat dianalogikan dengan proses penskalaan. Untuk alihragam *wavelet*, berlaku hubungan:

$$I(a_m x_i, b_n y_j) \leftrightarrow \frac{1}{|a_m b_n|} F\left(\frac{u_i}{a_m},\frac{v_j}{b_n}\right) \tag{1.6}$$

ISBN 978-602-99334-4-4

2. METODOLOGI

2.1 Bahan Penelitian

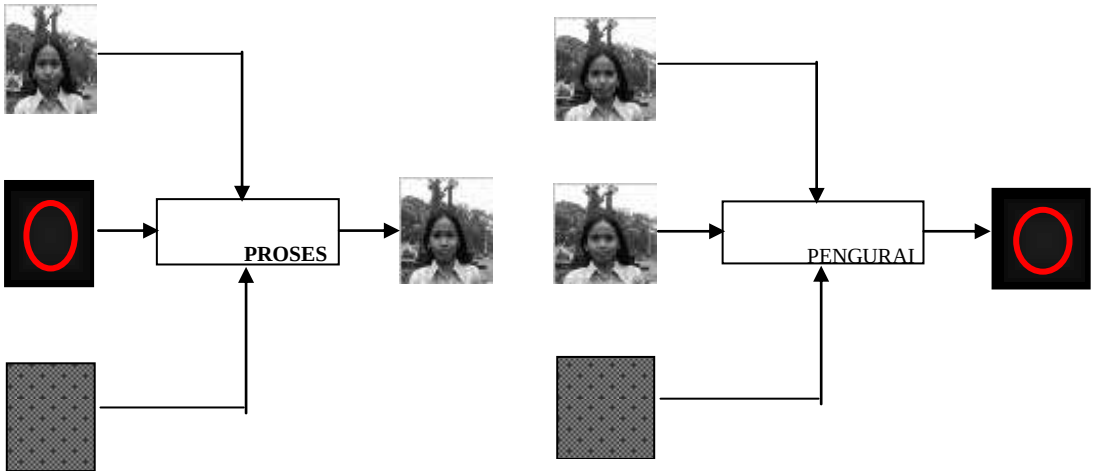
Bahan penelitian yang digunakan adalah citra asli: kiddy2.jpeg, ary71.jpeg, kid3.jpeg, kidir2.jpeg, kidin3.jpeg, kidjem2.jpeg. Citra – citra tersebut diperoleh dari hasil pengambilan dengan kamera digital, yang kemudian dipotong – potong menjadi 256 x 256 piksel.

2.2 Metode Penelitian

Terhadap citra hasil proses *watermarking* akan diterapkan penilaian kuantitatif dan penilaian secara kualitatif (subyektif). Penilaian secara kuantitatif berdasar pada statistika citra, dan penilaian kualitatif didasarkan pada persepsi mata manusia atas citra. Kedua hasil penilaian akan didampingkan dengan metoda komparatif.

2.3 Proses Penelitian

Beberapa citra yang dihasilkan dari proses *editing Adobe Photoshop* dirubah nilai *map*-nya dari citra warna ke citra *grayscale*, menggunakan program *Matlab* dengan memberikan nilai RGB sebagai berikut: R(*red*)=0,2290, G(*green*)=0,5870, dan B(*blue*)=0,1140.Citra *grayscale* dalam Matlab dengan bentuk nilai matriks. Citra dengan ukuran 256 x 256 piksel adalah bentuk matrik dengan ukuran 256 baris x 256 kolom. Sedangkan data teks berupa kumpulan huruf karakter dari a hingga z, 0 – 9, dan beberapa bentuk tanda baca yang umum digunakan serta spasi. Karakter yang dipilih selanjutnya diubah dalam untaian huruf biner 0 dan 1, dengan pengkodean satu karakter digantikan oleh 6 bit. Citra asli diurai dengan *wavelet transform* yang menghasilkan nilai aproksimasi dan 3 detail (vertikal, horisontal, dan diagonal). Selanjutnya dalam *wavelet transform* ini disisipkan data *mark* dan data pengaman, inilah sesungguhnya yang dinamakan proses *watermarking* seperti yang terlihat pada Gambar 2.1.(a). Setelah bergabung menjadi satu, kemudian disimpan untuk dijadikan sebagai hasil akhir *watermarking*. Dihitung nilai korelasi antara citra asli dengan citra *watermarking*. Bila perubahan yang terjadi tidak begitu kelihatan pada penampilannya, maka dikatakan proses *watermarking* berhasil dilakukan. Setelah penggabungan ini berhasil dilakukan, selanjutnya dilakukan proses kebalikan dengan mengurai kembali gambar yang disisipkan dalam citra *watermarking* untuk memperoleh kembali data *mark* yang disisipkan, yang terlihat pada Gambar 2.1.(b).



Gambar 2.1.(a) Proses *Watermarking;* (b) Pengurai *Watermarking*

3. HASIL

Untuk menentukan bentuk data *mark* yang akan dibuat, maka kita harus menentukan nilai R yaitu nilai *radian* yang harus dicari agar data *mark* sesuai dengan yang diiginkan. Kemudian dicari nilai konstanta penguat (*Alpha)*, digunakan untuk memperbaiki bentuk tampilan data *mark*, dan jumlah maksimal karakter yang dapat dituliskan. Dari beberapa percobaan yang dilakukan, diperoleh nilai R yang tepat ada disekitar nilai 100, nilai alpha yang tepat yaitu 12000, dan jumlah karakter yang dapat dituliskan adalah 32. Kemudian data *mark* yang sudah dibuat disisipkan ke dalam citra asli.

(a)

(b)

Gambar 3.1. (a) Citra asli, (b) Citra *Watermarking*

Tabel 3.1. Nilai Korelasi citra asli dengan citra *watermarking* dalam menentukan derajat dekomposisi SWT

4. KESIMPULAN

1. *Digital Image Watermarking* (DIW) dengan memanfaatkan keuntungan dari transformasi *wavelet*, menghasilkan suatu teknik *watermarking* yang paling baik dengan nilai korelasi mendekati 1 (0.9999) adalah pada saat nilai dekomposisi 26 menggunakan SWT2 (*Stationary Wavelet Transform* 2).
2. Pada proses penskalaan, menyebabkan penurunan kualitas citra *watermarking* saat citra diubah ke bentuk yang lebih besar, juga saat citra diubah ke bentuk yang lebih kecil, jadi

Dekomp.	Rekons.	Corr W	Corr M	SNR W	PSNR W	SNR M	PSNR M
1	1	0.9418	0.7324	8.8493	57.0141	-3.2011	44.5698
7	7	0.9982	0.9766	25.6346	73.1458	-3.1256	44.5689
9	9	0.9989	0.9751	27.8085	75.1236	-3.1478	44.4561
11	11	0.9992	0.9737	29.2356	77.1235	-3.5698	44.9652
13	13	0.9994	0.9701	30.2589	79.1041	-3.1234	45.1236
19	19	0.9998	0.9632	67.0258	82.0145	-3.1258	44.9400
20	20	0.9998	0.9588	34.1236	82.0148	-3.4569	45.6321
21	21	0.9998	0.9581	34.0189	83.1258	-3.1245	44.7890
23	23	0.9998	0.9853	36.1258	84.1270	-3.2258	44.1258
24	24	0.9998	0.9507	36.9986	84.6952	-3.1698	44.7769
26	26	0.9999	0.9497	37.5556	86.2356	-3.1478	44.9631

   teknik *watermarking* dalam transformasi *wavelet* ini, tahan terhadap serangan penskalaan.
3. Secara umum proses rotasi tidak menyebabkan perubahan kualitas citra *watermarking*. Jadi dapat dikatakan bahwa teknik *watermarking* dalam transfomasi *wavelet* ini, tahan terhadap serangan rotasi.
4. Dalam proses pemotongan terjadi penurunan kualitas citra *watermarkin*g. Dalam proses pemotongan ini, data *mark* yang disisipkan akan terpotong dan hasil dari ekstraksi *mark* hanya ada beberapa karakter saja, tergantung dari besar pemotongan. Bisa dikatakan teknik *watermarking* yang dibuat dalam kawasan *wavelet* ini, tahan terhadap serangan pemotongan.
5. Citra *watermarking* yang dikenai proses filter median ini, akan mengalami penurunan kualitas saat menggunakan blok [5 5] dan seterusnya, seiring dengan meningkatnya besar blok. *Watermark* yang disisipkan akan semakin hilang karakternya satu per satu. Untuk filter Adaptif, dengan besar blok [2 2] citra *watermarking* memiliki bentuk yang sama dengan citra asli. Sehingga dapat dikatakan bahwa penyembunyian *watermark* dalam kawasan *wavelet* tahan terhadap serangan filter adaptif, tapi citra hasil *watermarking* akan mempunyai kualitas yang semakin menurun dengan meningkatnya besar blok yang digunakan. Tapi *watermark* yang disisipkan tidak terpengaruh dengan peningkatan besar blok.
6. Proses kompresi menyebabkan penurunan kualitas *watermark*, tapi untuk kualitas citra *watermarking* tidak begitu terlihat hingga nilai *quality* 10. Bisa dikatakan teknik *watermarking* yang dibuat dalam kawasan *wavelet* ini, tahan terhadap serangan kompresi.

ISBN 978-602-99334-4-4

5. DAFTAR PUSTAKA

1. 1. A. Tirkel, G. Rankin, R. van Schyndel, W. Ho, N. Mee, and C. Osborne, "*Electronic water mark*", in Proc. DICTA 1993, Dec. 1993, pp. 666-672.
2. O. Bruyndonckx, J.J. Quisquater, and B. Macq, "*Spatial method for copyright labeling of digital images*", In Proc. IEEE Workshop Nonlinear Signal and Image Processing, Halkidiki, Greece, June 1995.
3. M. Kutter, "*Watermarking resisting to translation, rotation and scaling*", in http://ltssg3.epfl.ch:1248/kutter/watermarking/#publications
4. I. Cox, J. Kilian, T. Leighton and T. Shamoon, "*Secure Spread Spectrum Watermarking for Multimedia*", Technical Report 95-10, NEC Research Institute.
5. F.M. Boland, J.J.K. Ó.Ruanaidh and W.J. Dowling, "*Watermarking digital images for copyright protection*", IEE Proceedings on Vision, Signal and Image Processing, 143, 4, pp. 250-256, August 1996.
6. J. Smith and B. Comiskey, "*Modulation and information hiding in images*", in Proc. First International Workshop on Information Hiding, Lecture Notes on Computer Science, Cambridge, UK, pp. 207-226, June 1996.
7. E. Koch and J. Zhao, "*Toward robust and hidden image copyright labeling*", in Proc. Workshop Nonlinear Signal and Image Processing, Marmaros, Greece, June 1995.
8. J.J.K.O. Ruanaidh and T. Pun, "*Rotation, scale and translation invariant spread spectrum digital image watermarking*", Signal Processing, vol. 66, no.3, pp. 303-318, May 1998.
9. J.J.K.O. Ruanaidh and T. Pun "*Rotation, Scale and Translation Invariant Digital Image Watermarking*", IEEE International Conference on Image Processing, pp. 536-539, Santa Barbara, October 1997.
10. S. Pereira, J.J.K.O. Ruanaidh, T. Pun, "*Secure Robust Digital Watermarking Using the Lapped Orthogonal Transform*", In
11. http://cuiwww.unige.ch/~vision/Publications/postscript/99/
12. G. Voyatzis and I. Pitas, "*The Use of Watermarks in the Protection of Digital Multimedia Products*", in Proc. IEEE, vol. 87, no. 7, pp. 1197-1207, July 1999.
13. F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "*Information Hiding – A Survey*", in Proc. IEEE, vol. 87, No. 7, July 1999, pp. 1062-1078.
14. F. Hartung and M. Kutter, "*Multimedia Watermarking Techniques*", In Proc. IEEE, vol 97, No. 7, July 1999, pp. 1079-1107.
15. M.Kutter and F.A.P. Petitcolas, "*A fair benchmark for image watermarking systems*", Electronic Imaging '99 – Security and Watermarking of Multimedia Contents, vol. 3657, January 1999, San Jose, United States.
16. G.L. Heileman, C.E. Pizano and C.T. Abdallah, "*Image Watermarking for Copyright Protection*", In Lecture Notes in Computer Science 1619, Algorithm Engineering and Experimentation: International Workshop ALENEX'99, Springer-Verlag, Berlin, pp. 226-245, 1999.
17. R.L.Pickholtz, D.L. Schilling and L.B. Milstein, "*Theory of Spread-Spectrum Communications – A Tutorial*", In IEEE Trans. Comm., vol. COM-30, no. 5, pp. 855-884, May 1982.
18. J. œ Ruanaidh, W.J. Dowling and F.M. Boland "*Phase watermarking of digital images*", In Proceedings of ICIP'96, vol. III, pp. 239-242, Lausanne, Switzerland, September 1996.
19. R.C. Gonzalez, R.E. Woods Digital Image Processing, Massachusetts: Addison-Wesley, 1993.
20. R.J. Anderson and F.A.P. Petitcolas, "*Information Hiding – An Annotated Bibliography*", in http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography