# DAYANIKLI SAYISAL RESİM DAMGALAMA

**Chasan CHOUSE**[1] **Songül ALBAYRAK**[2]

[1,2]Bilgisayar Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
Yıldız Teknik Üniversitesi, 80750, Beşiktaş, İstanbul

[1]e-posta: chasanc@yahoo.com [2]e-posta: songul@ce.yildiz.edu.tr

*Anahtar sözcükler: Damgalama, Telif Hakkı, İçerik Doğrulama*

## ABSTRACT

*This paper presents a robust digital image watermarking technique. The proposed technique uses a circularly symmetric watermark to embed it into an image. Watermark is embedded in the middle frequencies of DFT domain. To make watermark less visible in spatial domain multiplicative embedding rule is used. This method is resistant to JPEG compression, filtering, noise addition and cropping. Results prove the robustness of this method against the above-mentioned attacks.*

## 1. GİRİŞ

Son yirmi yıldaki en büyük teknolojik gelişmeler, günlük yaşantımızın tüm alanlarını etkisi altına alan sayısal kitle iletişim araçlarında olmuştur. Sayısal resim/film/ses ve çokluortam uygulamaları günlük hayatımızın bir parçası haline gelmiştir. Özellikle internet aracılığıyla sayısal ürünlere çok kolay bir şekilde erişilebilmesi buna sebep olarak gösterilebilir.
Resimlerin sayısal ortamda saklanması ve klasik yöntemlere göre çok rahat bir şekilde iletilebilmesi beraberinde telif hakkı problemlerini getirmiştir. Telif hakkı(copyright) sahipleri çalışmalarını kullanan kişilerden yaptıkları işin bedelini almak ve çalışmalarının izinsiz kullanılmadığından emin olmak isteyebilirler. Sayısal ortamın yukarıda belirtilen özelliklerinden dolayı telif hakkı koruma ve içerik doğrulama(authentication) çok zor bir hal alır. Problemin çözümüne yönelik yöntemlerden biri resmin şifrelenmesi olmakla birlikte tam anlamı ile koruma sağlayamamaktadır. Resim bir defa deşifre edildiğinde istenildiği kadar kopya edilebilmekte ve dağıtılabilmektedir.

Son yedi yıldır sayısal teknolojiden kaynaklanan telif hakkı problemlerinin giderilmesi konusunda çalışan pek çok bilim adamı bulunmaktadır. Bulunan çözüm güvenilir ve geleceği olan bir yöntem olan resmin içine bilgi gizleme olmuştur. Bilgi gizlemek için her çeşit sayısal veri(resim, ses, video, yazı vs.) kullanılabilir. Biz bu çalışmamızı resme bilgi gizleme ile sınırlandıracağız. Bilgi gizleme tekniğinin en önemli özelliği, içine yerleştirilen bilginin resme bakan bir kişi tarafından farkedilmemesidir.

Hiçbir zaman bilgi gizleme tekniklerinin tümünün sağlaması gereken genel bir tanımlama yoktur. Bu çalışmada telif hakkı korumak için bilgi gizleme yöntemiyle ilgileneceğiz ve kullanacağımız terim damgalama(watermarking) olacaktır.

## 2. DAMGALAMA TEKNİKLERİNİN KULLANIM ALANLARI

Farklı ihtiyaçları ve sınırları olan değişik uygulama alanlarındaki damgalama teknikleri şu şekilde özetlenebilir[1]:

- Telif hakkı ve parmak izi onayı: Resme eklenmiş bilgi, telif hakkı iddia eden kişi tarafından kanıt olarak veya bilgiyi izinsiz kullanan kişinin izini sürmek için kullanılabilir.
- Doğruluğunu veya uygunsuz kullanıldığını belgelemek: Klasik bilgi doğrulama yöntemlerinden checksum, CRC üretimi kullanılabilir. Fakat resimdeki ufak bir değişiklik bu yöntemleri kullanılmaz hale getirir.
- Gizli iletişim: Resmin içine resme bakan kişi tarafından algılanamıyacak şekilde bilgi eklenebilir. Bu tür uygulamalarda karşı tarafa iletilmesi gereken gizli bilginin fazla olması internet ortamının çok fazla kullanılmasına sebep olur.
- Resim hakkında bilgi: Resim içine örneğin tıbbi bir resim hakkında açıklayıcı bilgiler saklanabilir.

## 3. TELİF HAKKI KORUMAK İÇİN DAMGALAMA

Son yıllarda işaret işleme literatürüne çok fazla damgalama teknikleri eklenmiştir. Her damgalama şemasında üç temel bölüm bulunmaktadır. Damga üretme, ekleme ve algılama bu üç bölümü oluşturmaktadır. Damga üretme, resme bağlı damga şablonu elde etmeyi hedefler. Damga ekleme işlemi, orijinal resmin farklı bir katmanına damga şablonunu ekleme olarak düşünülebilir. Damga algılama ise genellikle damga benzerliği veya varsayım testi ile gerçekleştirilir.

## 3.1 DAMGALAMA TEKNİKLERİ

Damgalama teknikleri farklı özelliklerine göre dört değişik kategoride sınıflandırılabilir.

- Bir grup damglama tekniği, algılama esnasında orijinal resme ihtiyaç duyar. Bununla birlikte geometrik bozulmalara karşı(kesmek, boyut büyültmek/küçültmek, döndürmek) dayanıklıdır. Fakat internette otomatik arama gibi uygulamalarda hatlarda yoğunluğu arttırması, bellek miktarının yetmemesi gibi sebepler dolayısıyla bu yöntem çok başarılı değildir.

- Bir diğer grup damgalama da damga sinyalini farklı bölgede ekler. Bazı teknikler görünen bölgede(spatial domain)[2] piksellerin yoğunluğunu ayarlayarak bilgiyi resme ekler. Bazıları da DCT[3], DFT[4] veya DWT[5] bölgelerinde damga işaretini resme ekler.

- Diğer bir teknik ise resmin karakteristiğine bağlı psiko-görsel (Humen Visual System)[6] maskeleme özelliğinden yararlanır.

- Sonuncu olarak sınırlandırılmış şifreli damgalama tekniklerinden bahsedilebilir. Bu yöntemde damgalanmış resimdeki bilgi sadece bilgiyi resme ekleyen kişi tarafından tekrar elde edilebilir veya damgayı herkes okuyabilir fakat sadece şifreyi bilen damgayı değiştirebilir ya da silebilir.

## 3.2 SALDIRILAR

Özel tasarlanmış birtakım saldırılar damga eklenmiş resimlerden bilgiyi silebilir veya resimdeki bilgiyi bozabilir. Bu yöntemlerden bazılarında resme basit ve hemen hemen hiç görünmeyen ufak bozulmalar eklenir (resmi bulandırdıktan sonra çok az bir şekilde geometrik bozulma eklemek) ve damga saptanamaz hale gelir.

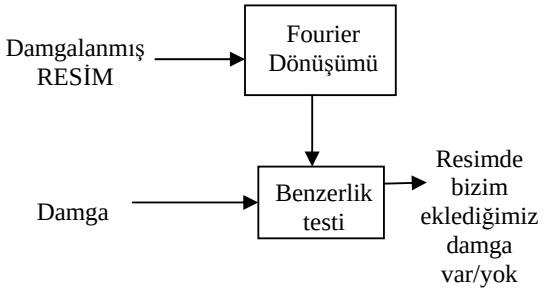
Saldırılar arasında en çok bilineni SWICO(Single Watermarked Image Counterfeit Original)[7] yöntemidir. Orijinal resim **I** 'dan damgalı resim $\hat{\mathbf{I}}$ 'ni elde etmek için **W** damgasını bir resme eklediğimizi düşünelim. Bir saldırgan orijinal resmin sahtesini ($\hat{\mathbf{I}}'$) başka bir $\hat{\mathbf{I}}$ 'nden $\mathbf{W}'$ damgasını çıkararak elde eder.

Saldırgan $\hat{\mathbf{I}}'$ 'nin asıl ve $\hat{\mathbf{I}}$ 'nin de damgalanmış resim olduğunu söyleyebilir. Bu durumda **I**, $\mathbf{W}'$ 'nden elde edilebilir.

## 4. DAYANIKLI RESİM DAMGALAMA

Damga ekleme yönteminin blok diagramı Şekil-1'de görülmektedir. Orijinal resmin fourier dönüşümü alınır ve frekans bölgesinde(domain) üretilen dairesel simetrik damga yine aynı bölgede resme eklenir. Ters Fourier dönüşümü ile damgalanmış resim elde edilir.

Damga varlığının testi için damgalandığı varsayılan resmin Fourier dönüşümü elde edilir. Tekrar üretilen damga ile Fourier dönüşümü yapılmış resim benzerlik testinden geçirilerek damganın varlığı için karar aşamasına geçilir. Şekil-2.'de sistemin blok diagramı görülmektedir.




Şekil-2. Damga bulma yöntemi

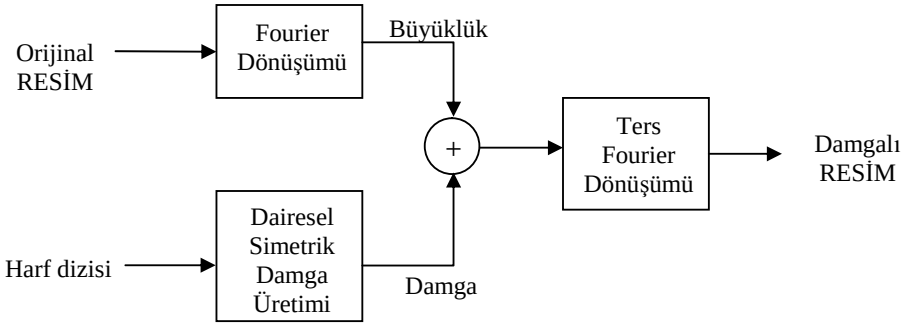
## 4.1 DAMGA ÜRETİMİ

Damga üretiminde kullanılacak karakter dizisi $T_{xt}$ olsun. Karakterlerin sayısı S ise damgada S adet dairesel simetrik halka olur. $R_1$ ilk dairenin yarıçapı ve $R_2$ de son dairenin yarıçapı olsun. Buna göre damgadaki bit sayısı:

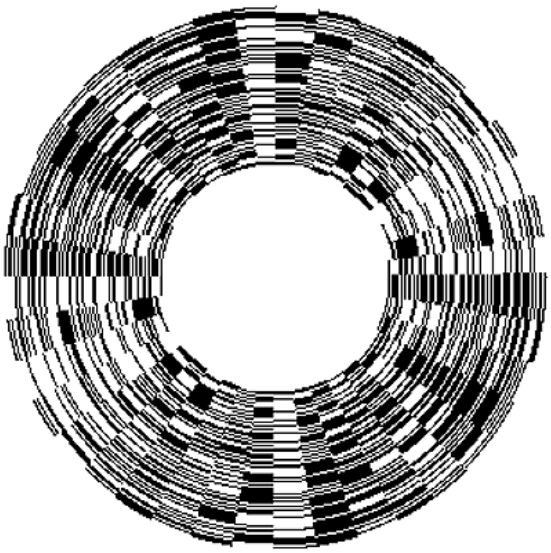
$$L = S \cdot (R_2 - R_1) \qquad (1)$$

olur[9].

Damga üretiminde $T_{xt}$ 'deki her karakterin karşılığı olarak 20-bit ve her sayı için '0' ve '1' lerin adedi eşit olan sayılar kullanılır. '0' yerine '-1' yazarak damgayı kullanabileceğimiz formata çevirmiş oluruz. Dairenin 0°-180° aralığına 20-bit sayının karşılığı olan bitler yerleştirilir. Aynı bitler, aynı yönde 180°-360° arasına yerleştirilir. Şekil-3 'de $T_{xt}$ için üretilmiş örnek bir damga görülmektedir.




Şekil-1. Damgalama yöntemi



Şekil-3. $T_{xt}$ için üretilen damga

$T_{xt}$ = "COPYRIGHT® BY YTU ELEKTRIK ELEKTRONIK FAKULTESI BILGISAYAR BILIMLERI MUHENDISLIGI BOLUMU"
olarak alınırsa üretilen dairesel simetrik damganın bit sayısı:

$$L = 2 \cdot S \cdot (R_2 - R_1) = 2 \cdot 88 \cdot 88 = 15488$$

olur.

Kullandığımız damgada 20-bit 180° yer kaplar ve her bit damga dairesinde 9° 'lik bir yer kaplar. Damgayı oluşturan dairelerin bir matriste olduğunu düşünelim. Bu durumda dairenin matrisde karşılığı olan noktalar

$$x = r \cdot \cos(q) \quad (2)$$

$$y = r \cdot \sin(q) \quad (3)$$

bağıntısından bulunur.

## 4.2 DAMGALAMA

Damgalama frekans bölgesinde bilgi ifade eden +1 ve -1 'ler kullanılarak yapılır. Damgada +1 ve -1 'lerin sayısı eşittir. Dolayısıyla damganın ortalaması sıfırdır. Frekans bölgesinde resmin düşük frekanslarına yapılacak herhangi bir uygulama resmin görünen yüzünde gözle görülür değişikliklere sebep olur. Resmin sıkıştırılması(JPEG vs. gibi) ise frekans bölgesinde yüksek frekansları etkiler. Bu durumda damga orta frekanslara eklenmelidir. Damganın dikkatli bir şekilde tasarlanması durumunda hem filtrelere karşı dayanıklı hem de görünmez olacaktır. Sıfır frekansı $I(0,0)$ 'ın bölgesinde merkez olduğunu düşünürsek damganın orta frekansları içine alan bir daireye eklenmesi gerekir.

$$q = \arctan\left(\frac{b}{a}\right) \quad (4)$$

$$M = r = \sqrt{a^2 + b^2} \quad (5)$$

$$W(r,q) = \begin{cases} 0, & r < R_1 \,\&\, r > R_2 \\ \pm 1, & R_1 \le r \le R_2 \end{cases} \quad (6)$$

a : Resmin frekans bölgesinde pikselin gerçek kısmı.
b : sanal kısmı.
M : büyüklüğü(magnitude).
$q$ : fazı(phase).

Daire, yarıçapı $r \in [R_1, R_2]$ olan $R_2$-$R_1$ adet aynı merkezli S adet daireden oluşur. Her dairedeki damganın değeri aynıdır(+1 veya -1).

$M'(x,y)$ değiştirilmiş büyüklük ve $I'(x,y)$ de damgalanmış resim olsun. $M(x,y)$ orjinal resmin büyüklüğü, $W(x,y)$ damga ve $\alpha$ da damganın dayanıklılığını belirleyen katsayı olmak üzere damgalama formulü:

$$M'(x,y) = M(x,y) + a \cdot M(x,y) \cdot W(x,y) \quad (7)$$

olur[9]. Gerçek resmin ters frekans bölgesi kompleks özelliğe sahiptir. $M'(x,y)$ 'nin ters bölgesinin gerçek olduğundan emin olmak için damganın aşağıdaki simetriyi koruması gerekir:

$$W(x,y) = W(N-x, N-y), \forall x, y \in [1, N] \quad (8)$$

Matristeki her noktanın frekans bölgesindeki karşılığı $z = a + ib$ şeklindedir. $a$ gerçek kısım ve $b$ de sanal kısımdır. Büyüklük $M$ ve faz $q$ olsun.

$$M = r = \sqrt{a^2 + b^2} = |a + ib| \quad (9)$$

$$q = \arctan\left(\frac{b}{a}\right) \quad (10)$$

olur.

Ters frekans bölgesi dönüşümü için $\theta$ ve $M'$ değerlerinden faydalanabiliriz.

$$a' = M' \cdot \cos(q) \text{ ve } b' = M' \cdot \sin(q) \quad (11)$$

$$z' = a' + ib' \quad (12)$$

$$i'(x,y) = IDFT(z') \quad (13)$$

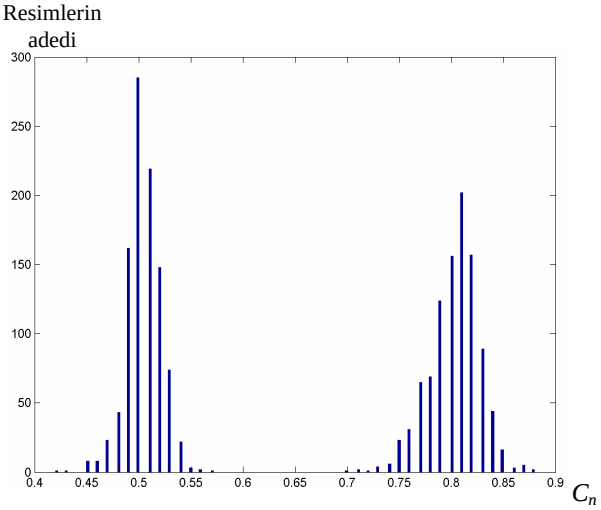
Damgalanmış resim $i'(x,y)$ 'dir. Son değerler 1 byte sınırını aşabileceğinden $i'(x,y)$ 'yi [0,255] aralığına çekilmesi gerekir. Ayrıca damganın görünmezliğini arttırmak için maskeleme tekniklerinden biri kullanılabilir[10].

## 4.3 BENZERLİK TESTİ İLE DAMGANIN TESPİTİ

$I'$ muhtemel damgalanmış resmin frekans bölgesindeki karşılığı ve $M'$ de büyüklüğü olsun. Muhtemel damgalanmış resmin $M'$ katsayıları ile

damga $W$ arasındaki benzerlik $\{c\}$, damganın varlığının test edilmesinde kullanılır. Şayet $I'$, $W$ ile damgalanmış resim ise benzerlik Eşitlik 14'de görülmektedir. *W* ve *M'* 'nin birbirinden bağımsız ve benzer şekilde rastgele dağıtılmış değişkenler olduğunu varsayarsak, *W* 'nin ortalama değeri sıfır olur. Resimde kullanılan *W* 'nin ortalama değerini hernekadar sıfır olarak varsaysak da *sin*/*cos* dönüşümünden kaynaklanan hatalar dolayısıyla genellikle ortalama değer sıfır olmaz. Bu problemi gidermek için yukardaki formul, normalleştirilmiş benzerlik $c_n$ olarak Eşitlik 15 'deki gibi değiştirilmesi gerekir.

*T* 'nin eşik değeri olduğunu varsayarsak Şekil-4 'ten faydalanarak *T* = 0.57 diyebiliriz. Yapılan testlerde her damgalanmış resmin benzerlik değeri $c_n$, *T* değerinden büyük ya da eşit çıkmıştır.




Şekil-4. 1000 adet damgalanmış(sağ bölge) ve damgasız(sol bölge) resmin dağılım eğrisi

$$c = \sum_{x=1}^{N}\sum_{y=1}^{N}\left(W(x,y)\cdot M'(x,y) + a\cdot W^2(x,y)\cdot M'(x,y)\right) \tag{14}$$

$$c_n = \left(\frac{\sum_{M'\in M'_+} M'}{N_+} - \frac{\sum_{M'\in M'_-} M'}{N_-}\right)\cdot\frac{N_+ + N_-}{2f(M',a)} = \left(\frac{\sum_{M'\in M'_+}\left(M' + f_+(M',a)\right)}{N_+} - \frac{\sum_{M'\in M'_-}\left(M' - f_-(M',a)\right)}{N_-}\right)\cdot\frac{1}{2m_{f(M',a)}} \tag{15}$$

Damgalanmış ve damgasız resimlerin normalleştirilmiş benzerlik $c_n$ 'i farklıdır. $c_n$ benzerlik özelliğini damganın varlığının testinde kullanabilmek için damgasız resimlerden oluşan 1000 adet resmin $c_n$'i ve damgalanmış 1000 adet resmin $c_n$'i hesaplanırsa Şekil-4 'te görülebilen bir dağılım grafiği elde edilir.

Damga tespiti:

$H_0$: Şayet $c_n \geq T$ ise $I'$, W ile damgalanmıştır.

$H_1$ : Şayet $c_n < T$ ise $I'$, W ile damgalanmamıştır.

$N_+$: Damgadaki +1'lerin sayısı.

$N_-$: Damgadaki -1'lerin sayısı.

$M' : M'(x,y)$

$M'_+ : \{M'(x,y); W(x,y) = +1\}$

$M'_- : \{M'(x,y); W(x,y) = -1\}$

$m_{f(M',a)} = m_{f_+(M',a)} + m_{f_-(M',a)}$

$f(M',a) = a\cdot M'(x,y)$

$f_+(M',a) = \{a\cdot M'(x,y); W(x,y) = +1\}$

$f_-(M',a) = \{a\cdot M'(x,y); W(x,y) = -1\}$

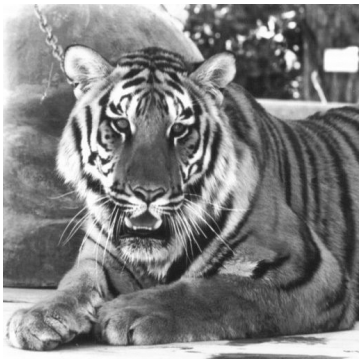
## 5. SONUÇ

Yapılan testlerde dairesel simetrik damgalama ile şu sonuçlara ulaşılmıştır:

- Damgalanmış resimlerde görünen bir bozulma olmamıştır. Bunun sebebi frekans bölgesinde orta frekanslarda resme eklenen damganın resmin görünen bölgesine(spatial domain) etki etmemesidir. Tablo-1 'de bazı test sonuçları görülmektedir.
- Damgalanmış resim ile damgasız resim arasındaki fark Şekil-6'da görülmektedir. Buradan resmin damgalandığı sonucu çıkarılabilir.
- $I$ resmine $W_1$ damgası uygulanıp $I'$ resmi elde edilmiş olsun. Yine $I$ resmine $W_2$ damgası uygulanıp $I''$ resmi elde edilmiş olsun. Damgalı resim $I'$, $W_2$ damgası ile test edildiğinde algoritma damganın olmadığı sonucuna varmaktadır. Yine damgalı resim $I''$, $W_1$ damgası ile test edildiğinde algoritma damganın olmadığı sonucuna varmaktadır. Bu bize kullanılan yöntemin yanlış damga tespitine karşı yeterince güvenli olduğunu göstermektedir.
- Damga işareti $W$ yi oluşturan +1 yerine -1 ve -1 yerine +1 konularak tersi alınmış olsun.

Oluşan damga işaretine $W'$ diyelim. Damgalanmış resim $I'$, damga $W'$ uygulandığında resimden damganın silindiği ve resmin görünen bölgesine etki eden bozulmaların yok olduğu tespit edilmiştir.

- Aynı resme farklı damgalar uygulandığında dağılım eğrisinin eşit aralıkta sağa veya sola doğru kaydığı görülmüştür. Bu çalışmadaki damgalama yönteminin frekans bölgesinde orta frekansa etki etmeyen filtrelere karşı dayanıklılığı gösterilmiştir. Örneğin gürültü ekleme oranını %10'dan daha yüksek olarak alırsak resmin frekans bölgesinde orta frekanslara etki etmeye başladığı ve bu nedenle damganın tespitinin imkansızlaştığı görülmüştür.



Şekil-5 Orijinal resim

Şekil-6. Damgalanmış resim

Şekil-6. Damgalanmış resim ile damgasız resim arasındaki fark.

Tablo-1. Sınır değeri $c_n = 0.57$ alınarak yapılan test sonuçları

| Efektler | $c_n$ |
|---|---|
| Gaussian Blur | 0.62 |
| Mosaic 2x2 | 0.58 |
| Gürültü %10 | 0.59 |
| Median | 0.61 |
| JPEG 1:37.7 | 0.61 |
| Kırpma | 0.62 |

**Kaynakça**


[1] N. Nikolaidis and I. Pitas, "Digital Image Watermarking: An Overview". *ICMCS 99*, Volume 1, Florence, Italy, pp 1-6.

[2] N. Nikolaidis, I. Pitas, "Robust image watermarking in the spatial domain". *Signal Processing*, v. 66, no. 3 (May 98), pp 385-403.

[3] M. Swanson, B. Zhu, A.. Tewfik, "Transparant robust image watermarking". Proc. 1996, *IEEE Int. Conference on Image Processing*, vol III, pp 211-214.

[4] S. Pereira, J. J. K. Ó Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, "Template Based Recovery of Fourier-Based Watermarks Using Log-polar and Log-log Maps", *IEEE ICMCS99*, Florence, Italy, June 1999.

[5] C-S. Lu, S-K. Huang, C-J. Sze, H-Y. M. Liao, *IEEE Trasactions on Multimedia*, vol. 2 no. 4, December 2000.

[6] J. F. Delaigle, C. De Vleeschouwer, B. Macq, "Watermarking Algorithms Based on a Human Visual Model", *Signal Process*, vol. 66, pp. 319-336, 1998.

[7] S. Craver, N. Memon, B. Yeo, "Resolving Rightful Ownership with Invisible Watermarking Techniques:Limitations, Attacks and Implications", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp 587-593, May 1998.

[8] P. Bourke, 2 Dimensional FFT, http://astronomy.swin.edu.au/~pbourke/analysis/fft2d/, July 1998.

[9] V. Solachidis and I. Pitas. "Circularly symmetric watermark embedding in 2-D DFT domain". *In Proceedings of ICASSP99*, Volume 6, pages 3469-3472, Phenix, Arizona, USA, March 15-19 1999.

[10] F. Bernolini, M. Barni, V. Cappelini, and A. Piva. "Mask building for perceptually hiding frequency embedded watermarks". *In Proc. of ICIP'98*, volume I, pages 450-454, Chicago, USA, 4-7 October 1998.