Dalgacık Dönüşümü ile Damgalama

Mustafa UÇAK
Kocaeli Üniversitesi
Elektronik Ve Haberleşme Mühendisliği Bölümü
İmge İşleme Laboratuarı
İzmit/Kocaeli
mustafa.ucak@emo.org.tr

ÖZETÇE

Sıkıştırma teknolojilerinin (JPEG,MPEG vb. imge kodlama standartları) gelişmesi ile çoklu ortam uygulamalarında bu yöntemler genişçe kullanım alanı buldu. Günümüzde sayısal belgeler WWW (World Wide Web) sayesinde çok fazla insana ulaşma imkanı bulmaktadır. Sayısal ortamların öneminin artması ile bunun sonucunda sayısal bilgilerin çoğaltılması ve işlenmesi gibi bir durum oluşmuştur. Bu da sayısal bilgilerin dağılımında bu sayısal bilginin (media,doküman vb.) kime ait olduğu konusunda bir güvenlik sorunu doğurmuştur. Damgalama (Watermarking) teknolojisi de bu sayısal ortamlara dışarıdan algılanamayan damgalar koyarak sayal sahiplerin; izinli kullanıcıların kimliklerinin bu ortamlara yerleştirilmesini sağlar[1].

Daha önce yapılan çalışmalar göstermiştir ki ; asıl imgenin önemli bölümünün (örneğin alçak frekans bileşenleri) değiştirilerek bilgi gömülmesi en güvenilir ve sağlam yoldur[2]. Buda Watermarking 'in gelişiminin frekans domeninde yapılmasında yol gösterici olmuştur.

Bir çok imge dönüşümü dikkate alınabilir. Bunlardan en önemlileri arasında ayrık kosinüs dönüşümü DCT(discreat cosine transform) ile bir çok watermark algoritmasının kullandığı ya blok bazlı yada global DCT[2] bulunur. Watermark için önerilen diğer dönüşümler DFT (discreat cosine transform) [3]; Fourier-Mellin Dönüşümü[4] bunlardan bazılarıdır. Bu çalışmada biz dalgacık uzayına yoğunlaşacağız.

Bu çalışmada sayısal veri olarak imge kullanılmakta ve kullanılan imgeler dalgacık dönüşümü katsayılarının bir telif imgesinin katsayıları ile işlenmesi sonucunda damgalanmıştır. Bu çalışmada telif imgesi olarak ikili imge şeklinde bir logo kullanılmıştır. Damgalanmış imge ile telif hakkı bulunan imge karşılaştırılarak bu imgenin içine gömülü logo sayesinde veri güvenliği sağlanmış olur.

1.Giriş

Watermarking' te amaç telif hakkının korunması için imgeye " damga(mark)" gömülerek bu sayede telif hakkını elinde tutan kişiyi tanımlayabilmektir [1]. Damga; tescil numarası, bir metin yada bir logo olabilir.

Sayısal damgalama algılanabilir yada algılanamayan bir şekilde olabilir. Algılanabilen damgalar genelde bir logo şeklinde ve imgeden izinsiz şekilde çıkarılması çok zor olan damgalar şeklinde olabilir. Biz bu çalışmada algılanamayan görünmez damgalamayla uğraştık.

Görünmeyen damgalamanın imge sıkıştırmasına (örneğin Jpeg), imge filtrelemesine ve imgede geometrik değişimlere dayanıklı olması gerekir. Bunda da damgada şifreleme tekniklerinin, pseudo-rasgele sayılarının istatistiği önemli bir rol oynar.Bu çalışmada sıkıştırmaya karşı dayanıklı bir damgalama üzerinde çalışılmıştır.

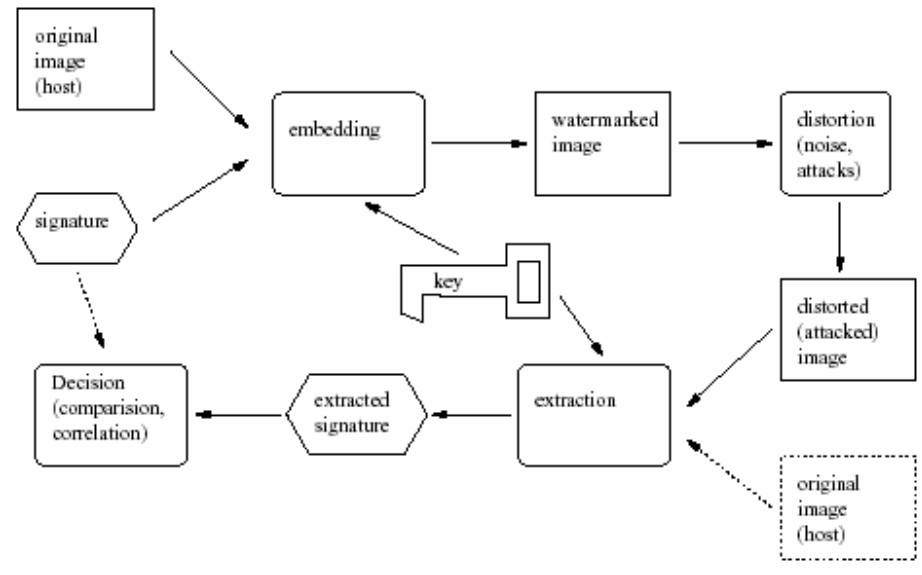
Watermarking'in telif hakkının korunmasının dışında başka bir kullanım alanı da bilgi gizlemedir. Bilgi gizleme yada steganografi görünmeyen ve maksimum kapasitede bilgiyi imgeye gömmeyi amaçlar. Bu şifrelenmiş mesajların iletiminde kullanılır.

Sayısal veriye göreceli küçük ölçekte bir sinyal olan *sayısal damga*nın eklenmesi[5] bize bugünlerde her türlü sayısal ortamın damgalanabileceğini göstermektedir. Bu yöntem ile sayısal veri üzerindeki herhangi bir işlem yapılsa dahi damganın korunması beklenir. Damganın duyu organları ile anlaşılamıyor olması damganın tespitini zorlaştırır ve orijinal veri ile damgalanmış verinin neredeyse aynı kalitede olmasını sağlar. Bu çalışmada sayısal veri olarak imgeler kullanılmıştır. Aşağıda kullanılan yöntem ile sonuçlara yer verilmiştir.

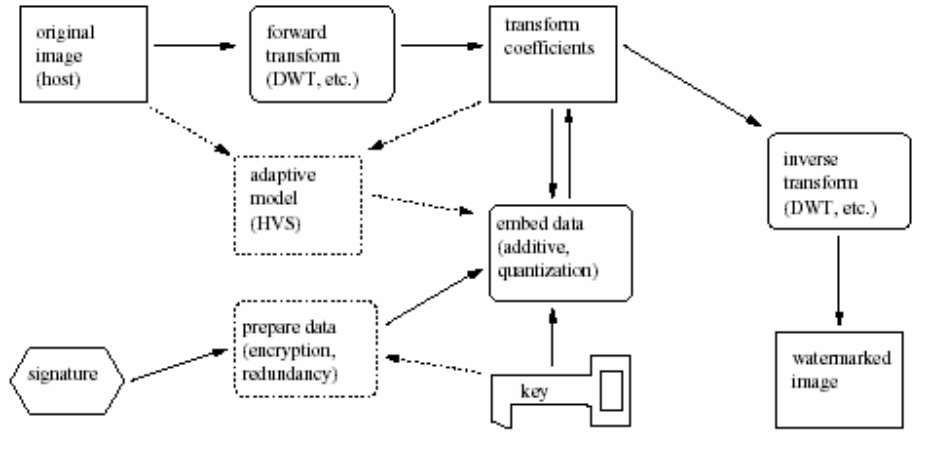
1.1 Damgalama Problemleri

İmge damgalama duyu organlarımız ile fark edilemeyen bilgileri ana imgeye gömmektir. Damgalamada genel olarak kullanılan bir işlem şekil 1.1 de verilmiştir. Orijinal imge , imza bilgisi ile değiştirilerek damgalanmış imge oluşturulur. Bu işlem sırasında bazı bozunumlar olacaktır. Burada gömülen bilginin şeffaf ve çok büyük miktarda bozunuma neden olmadığından emin olunması gerekir. Daha sonra dağılan bu imge bir çok bozunuma uğrayacaktır. Örneğin bu bozunumlar kayıplı imge sıkıştırma, yeniden örnekleme yada daha değişik saldırılar olabilir.

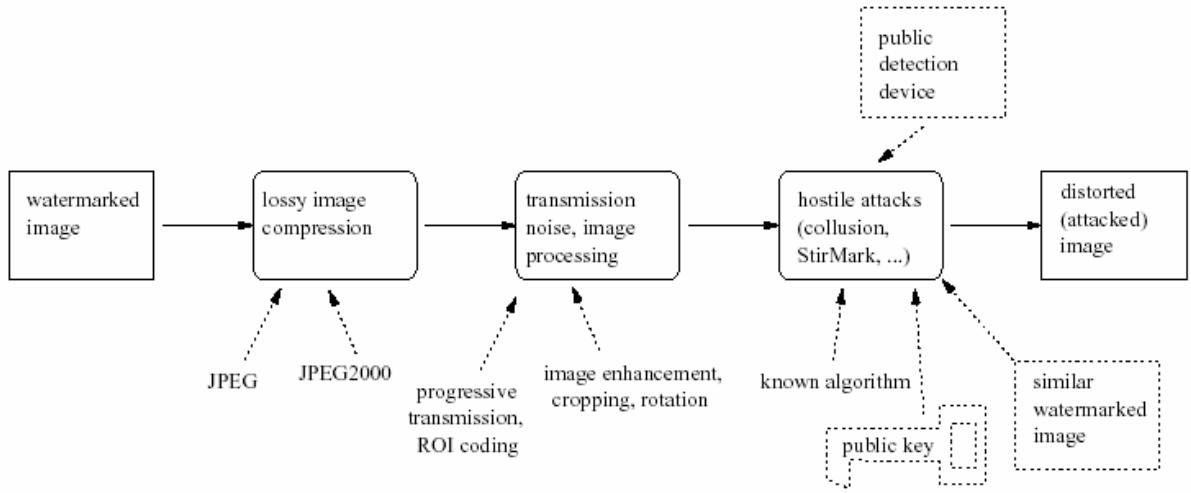
Damganın geri elde edilmesi sürecinde damgalama işleminin doğası gereği ana imgeye ihtiyaç duyulacaktır.Damga orijinal imge sayesinde geri oluşturulacaktır.



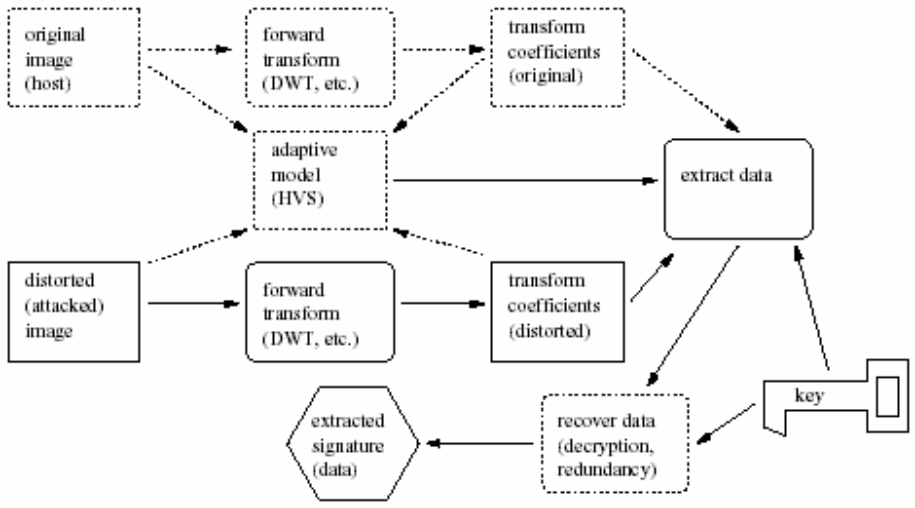
Şekil 1.1 – Bilgi gizleme modeli, genel bakış



Şekil 1.2 – Watermark gömme modeli



Şekil 1.3 – Damgalanmış imgenin dağılım modeli

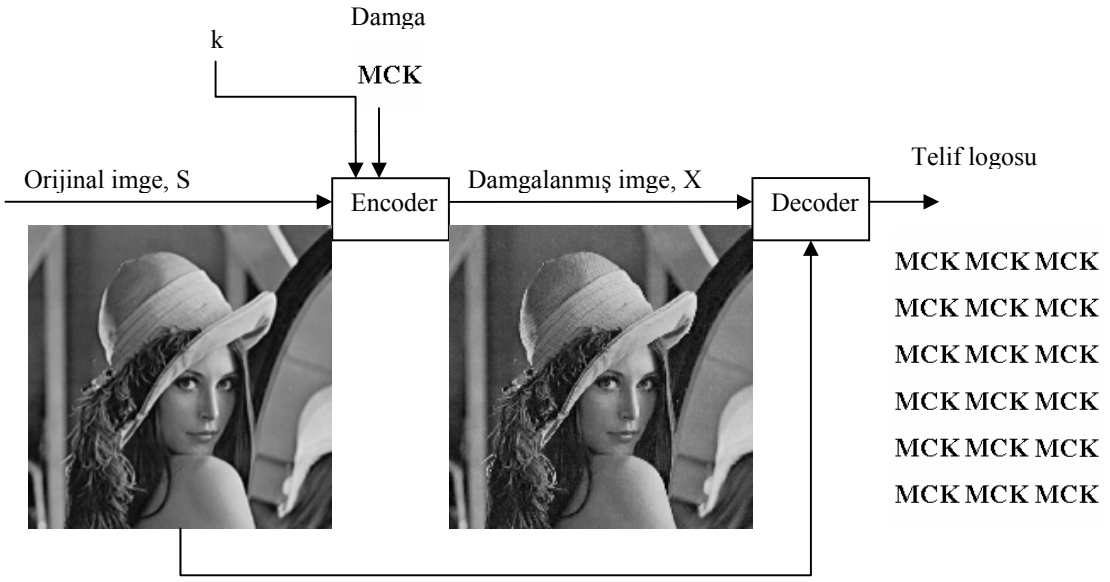


Şekil 1.4 – Damganın çıkarılması modeli

Yukarıda verilen modeller genel watermarking modelleridir. Bu modellerde şifreleme için private key ve public key kullanılmıştır. Bizim çalışmamızda herhangi bir şifreleme olmadığı için bu aşamalar bulunmamaktadır.

2.Yöntem

İmgelerin damgalanması, dalgacık dönüşümü katsayılarının üzerinde damga imgesinin katsayılarının işlenmesi ile oluşturulmaktadır.



Şekil 2.1 – Damgalama yöntemi

2.1 Damganın Eklenmesi

Damganın eklenmesi aşamasında öncelikle orijinal imgenin dalgacık dönüşümü katsayıları bulunmaktadır. Damga imgesi damgalanacak imge boyutunda çoğaltılarak damgalanmış imgeden damganın çıkartılması aşamasında belirli bir bölgede veri kaybı olsa dahi damganın geri elde edilebilmesi sağlanacaktır. Çoğaltılmış damgalardan oluşan yeni damga imgesi dalgacık dönüşümü katsayıları ile işleme sokularak orijinal imge üzerinde alçak frekans katsayılarına karşılık gelen değerlerin üzerine *k* katsayısı çarpanı ile eklenmiştir. *k* çarpanı damganın göz tarafından algılanmasını önleyecek şekilde ayarlanan bir çarpandır. Damga imgesinin dalgacık dönüşümü katsayıları ve k çarpanı ile orijinal imgenin dalgacık dönüşümü katsayıları üzerinde yapılan değişiklikler sonucu damgalanmış imge ters dalgacık dönüşümü yapılarak yeniden oluşturulur.

2.2 Damganın çıkarılması

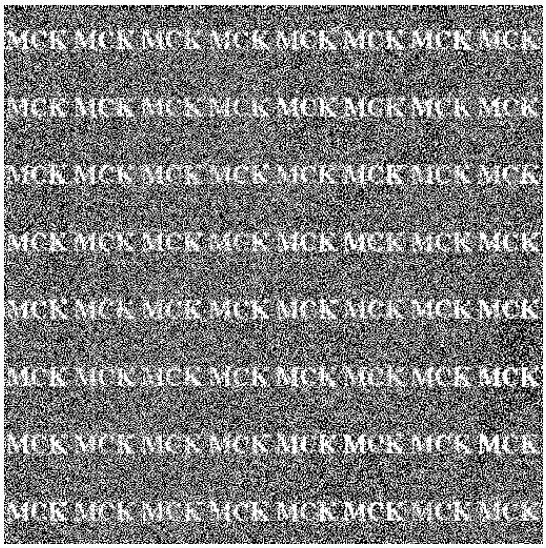
Damganın çıkarılması aşamasında telif hakkını elinde tuttuğunu iddia eden kişinin elindeki orijinal imge ile damgalandığı iddia edilen test imgesi üzerinde fark alma işlemleri yapılarak ;imge ;bazı imge sıkıştırma ve gürültü eklenme işlemlerine tabi olmuş olsa dahi; damga geri elde edilebilmektedir. Burada imgenin damgalı olup olmadığına karar verecek olan istatistiksel bir takım deneyler yerine, imgeden çıkarılan logoyu incelecek olan insandır.

3.Sonuçlar

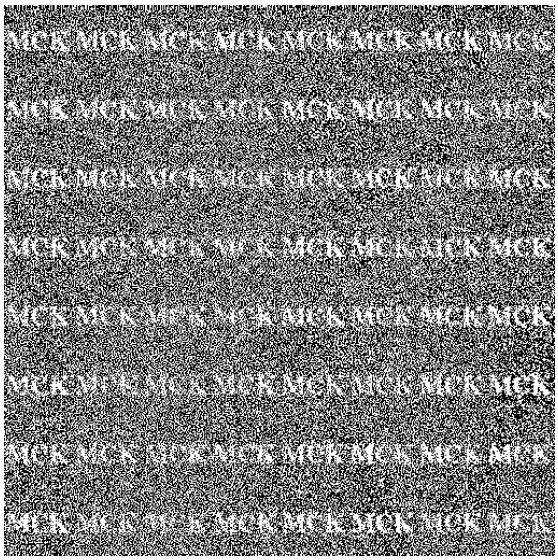
Bu çalışmada yukarıda anlatılan yöntemler kullanılarak oluşturulan damgalamanın JPEG sıkıştırma yöntemine ne kadar dayanıklı olduğu yapılan denemelerle gözlemlenemeye çalışıldı. Kullanılan JPEG sıkıştırma yöntemleri arasındaki farka bağlı olarak damganın tespiti değişiklik göstermektedir. MATLAB® ile yapılan JPEG sıkıştırma kullanılarak alınan sonuçlar incelenmiştir. Damga olarak "MCK" logosu kullanılmıştır. Yukarıda da bahsedildiği gibi burada imgenin damgalanıp damgalanmadığı,imgeden çıkarılan logoyu inceleyen kişiye kalmıştır. Alınan deneysel sonuçlar aşağıda verilmiştir.

a-Orjinal imge **b-**Damgalanmış imge

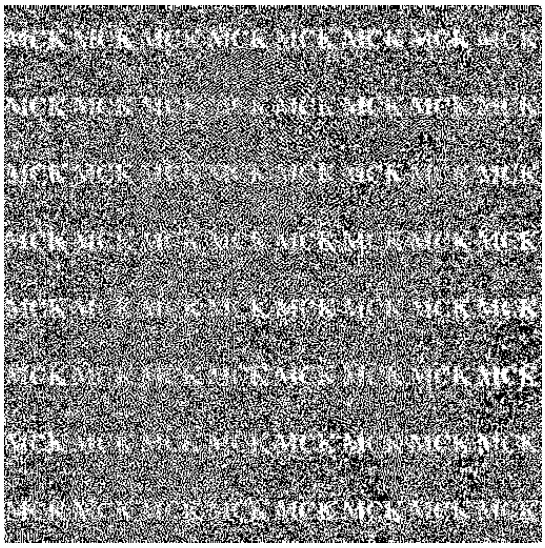
Şekil 3.1- Lena imgesi



a-Sıkıştırma kalitesi %90



b-Sıkıştırma kalitesi %80



c-Sıkıştırma kalitesi %60

d-Sıkıştırma kalitesi %50

Şekil 3.2 - Sıkıştırılmış imgelerden elde edilen logolar

Lena imgesinin içerisine saklanmış olan "MCK" logosu görüldüğü gibi damga çıkarılması yapıldıktan sonra belirli oranda JPEG sıkıştırması olmasına rağmen açık şekilde okunabilmektedir.
Sıkıştırma kalitesi daha da düşürüldüğünde artık "MCK" logosunun tespiti güçleşmiş hatta %50 kaliteden aşağısında neredeyse tespit edilemez hale gelmiştir.
Tabi ki kullanılan sıkıştırma metodlarına bağlı olarak logo tespiti insanın görüş açısına göre de değişecektir.

Kaynakça

[1]. Meerwald Peter; "Digital Image Watermarking in the Wavelet Transform Doamain", Sarlzburg, Janner 2001 http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/MasterThesis/wm_thesis.zip

[2]. Ingemar J. Cox,Joe Kilian, Tom Leighton, Talal G. Shamoon. Secure spread spectrum watermarking from multimedia. In *Proceedings of the IEEE International Conference on Image Processing, ICIP' 97, volume 6,* pages 1673-1687, Santa Barbara, California,USA,October 1997

[3]. Mahalingam Ramkumar, Ali N. Akansu, and A. Aydın Alatan. A robust data hiding scheme for images using DFT. In *Proceedings of the 6th IEEE International Conference on Image Processing, ICIP' 99*,pages 211-215, Kobe, Japan, October 1999

[4]. Joseph J. K. O'Ruanaidh and Thierry Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. Siganl Provessing, 66(3):303-317, May 1998

[5]. Guney N.; Anarım E.; "Dalgacık Dönüşümü ile İmge-uyumlu Damgalama", Siu2002_no226.

EK- Program Kodları:

Aşağıda verilen kodlar MATLAB® programı için yazılmıştır. *water.m* dosyası çalıştırıldıktan sonra damgalanacak imge seçilir. Damgalama işlemi bittikten sonra damgalanmış imge 'marked_image.bmp' olarak kayıt edilir. *watdet3.m* damgalanmış imge ile asıl imgeyi test ederek damganın geri alınmasını sağlar.

water.m – Ana program

```
%  -Watermarking in Wavelet Domain-
%
%  This program use wavelet transform for watermarking.
%  Wavelet Domain is more robust to image compression or additive noises.
%
%  This program benefit from "Image Adaptive & Fragile Watermarking;
%  Ebru Arısoy & Eda Ormancı,Bogazici University"

% Mustafa UCAK
% School of Electronic & Telecommunication Engineering
% University Of Kocaeli
% m_ucak@isnet.net.tr
% May 2005

clear all; close all; clc;

[filename1,pathname]=uigetfile('*.*','select the image');
image1=imread(num2str(filename1));
figure(1);
imshow(image1);title('original image');     % orginal image for watermarking
image1=double(image1);

[row,col]=size(image1);

imagew=imread('dmg2.tif');


[marked]=blockdwt2(image1,imagew);  % generates the watermarked image

markedmax = max(marked(:));
markscale = marked/markedmax*255;

figure(2);
colormap(gray(256));
image(marked);                                                  % shows the watermarked image
title('Watermarked image');
imwrite(marked,gray(256),'marked_image.bmp');     % saves the watermarked image as a bmp file
% figure(3);
%watermark=image1-marked;                          % image adaptive watermark
%watermark=watermark*255/max(watermark(:));
```

```
% colormap(gray(256));
% image(watermark);                                          % shows the image adaptive watermark
% title('watermark');
imwrite(marked,gray(256),'watermark.bmp');   % saves the image adaptive watermark as a bmp file
```

dmg.m – Damgalama logosunu üretir.

```
% Damga uretme
%
% imgew: Damga imgesi
% imge1: Orjinal imge
%
% Mustafa UCAK
% School of Electronic & Telecommunication Engineering
% University Of Kocaeli
% m_ucak@isnet.net.tr
% May 2005


function W=dmg(imgew,imge1);

[w h]=size(imgew');
[w1 h1]=size(imge1');
a=1;
b=1;
W=zeros(size(imge1'));

for i=1:w:w1
   for j=1:h:h1
      W(i:a*w,j:b*h)=imgew';
      b=b+1;
   end
   a=a+1;
   b=1;
end

   W=W';
```

blockdwt2.m – Wavelet uzatında damganın imgeye eklenmesi

```
% Mustafa UCAK
% School of Electronic & Telecommunication Engineering
% University Of Kocaeli
% m_ucak@isnet.net.tr
% May 2005


function [D]=blockdwt2(A,W);
```

```
[row,col]=size(A);

Tr=0;                % İnsan Görsel Sistemine göre damganın algılanmasını önleyen katsayılar.
k=0.027;

[ca,ch,cv,cd] = dwt2(A,'db1');   %Wavelet dönüşümü
c1 = [ch cv cd];

[h, w] = size(ca');
[m, n] = size(c1');

W=dmg(W,A); % damganın imge boyutunda oluşturulması


[caa chh cvv cdd]=dwt2(W,'db1');  %Wavelet dönüşümü
W=caa;
size(W);

% Adding watermark image.

for i=1:h
   for j=1:w
      if ca(i,j)>Tr
         Ca(i,j)=ca(i,j)+k*W(i,j);       % <--------k*abs(double(c1(i,j)))*W(i,j); de olabilir
      else
         Ca(i,j)=ca(i,j);                % Burada alçak frekans bileşenlerine damgalama yapılmakta
      end
   end
end

% CH1=C1(1:h,1:w);
% CV1=C1(1:h,w+1:2*w);
% CD1=C1(1:h,2*w+1:3*w);

D= double( idwt2(Ca,ch, cv, cd,'db1') ); % Ters Wavelet dönüşümü; imgenin geri oluşturulması
```

watdet3.m – Damganın kontrolü ve çıkarılması

```
% Mustafa UCAK
% School of Electronic & Telecommunication Engineering
% University Of Kocaeli
% m_ucak@isnet.net.tr
% May 2005

function W=watdet3(watermarkim,originalim);

a=marked-image1;
[ca ch cv cd]=dwt2(a,'db1');
imshow(ca);
```