İMGELERDE DWT İLE DAMGALAMA METODU

Dr.Ersin ELBAŞI

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
Kavaklıdere, Ankara

ersin.elbasi@tubitak.gov.tr

Özetçe

Yayın hakkını koruma amaçlı kullanılan damgalama (watermarking) metodunda en önemli özellik damgalanan çoklu ortam elemanının (imge, video, ses, vs.) saldırılara karşı dayanıklı olmasıdır. Bunu sağlamak amacıyla Ayrık Dalgalı Dönüşüm(Discrete Wavelet Transform) metodu kullanılarak çeşitli saldırılara karşı %100 başarı sağlayan bir algoritma geliştirdik. Bu algoritmada ayrık dalgalı dönüşüm yapılan imgenin sadece LL ve HH bantlarına damga ekledik ve detektör algoritmasında her iki banttan ayrı olarak logo çıkarttık. Gri, renkli ve video imgelerinde yaptığımız testlerde oldukça iyi sonuçlar elde edilmiştir.

1.Giriş

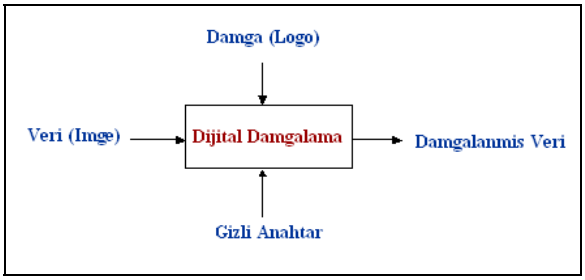
Bilgisayar teknolojisinin gelişmesi özellikle internetin yaygınlaşması ile birlikte resim, müzik, metin, grafik ve video gibi çoklu ortam elemanları daha hızlı ve kolay dağılmaya ve paylaşılmaya başlandı. Yayın hakkına sahip film stüdyoları ve müzik yapımcıları gibi şirketler için ise yasal olmayan kopyalama önemli bir sorun olmaya başladı. Bu sebepten "Damgalama" (Watermarking) son yıllarda yayın hakkını korumaktan, bilgi saklamaya kadar değişik alanlarda kullanılmak üzere ilgi çekmeye başlamıştır. Damgalama logo yada gürültü şeklindeki bit'lerin sayısal (digital) imge, video ve ses gibi çoklu ortam elemanlarına eklenerek sahibine ait bilgilerin saklanmasıdır [2].

Çoklu ortam elemanlarının güvenliği iki şekilde sağlayabiliriz.

a.Kriptografi
b.Damgalama

Kriptografi metodu sadece çoklu ortam elemanını bir ortamdan başka bir ortama aktarılırken koruma sağlar. Karşı taraf aldıktan sonra koruma bitmiş olur.Bu problemi çözmek için damgalama metodu kullanılmaktadır.

Damgalama metodunda en önemli özellikler: güvenilir olması, görünmez olması, kapasitesinin yüksek olması ve saldırılara karşı dirençli olmasıdır. Damgalanan imgenin kalitesinin orjinal imgeyle aynı olması yada yakın olması gerekir [3]. Damgalama yapıldıktan sonra damgayı yok etmek için çoklu ortam elemanına birçok saldırı olabilir. Uyguladığımız damgalama algoritmasının bu tür saldırılara karşı dayanıklı olması gerekir. Şekil 1 genel damgalama çalışma yapısını göstermektedir.



Şekil 1: Damgalama (watermarking) yapısı

Bu alanda uygulanan algoritmaları üç ana başlıkta toplayabiliriz.

a.Dönüşüm Alanında Damgalama
b.Uzamsal Alanda Damgalama
c.Sıkıştırılmış Alanda Damgalama

2.Damga Ekleme ve Çıkarma

Damga Ekleme: Damga gömme yada ekleme işlemi resim yada videoya logonun saklanması işlemidir. Eğer orjinal imgeye O, logomuza L dersek, E damgalama fonksiyonu, O ve L girdilerini alıp O* damgalanmış imgeyi çıkarır.

$$E(O,L)=O^*$$

Damga Çıkarma: Damgalanmış imgeden logonun çıkarılması işlemidir. İstatistiksel bir işlem olup bazı durumlarda sadece resim damgalı yada damgasız (detektör) diye sonuç bildirir.

$$D(O,O^*)=L$$

3. Damgalama metodları

Damgalama metodlarını çeşitli şekilde sınıflandırabiliriz [2].

Kriterya	Çeşitler
Döküman Çeşidine Göre	İmge, Video, Ses, Metin
İnsan Algılamasına Göre	Görünür, Görünmez
Çalışma Alanına Göre	Uzamsal, Dönüşüm
Logoya Göre	PRN, Görünür damga
Bilgi Çeşidine Göre	Kör-olmayan, Yarı-kör, Kör

Tablo 1. Çeşitli kriteryalara göre damgalama sınıflandırılması

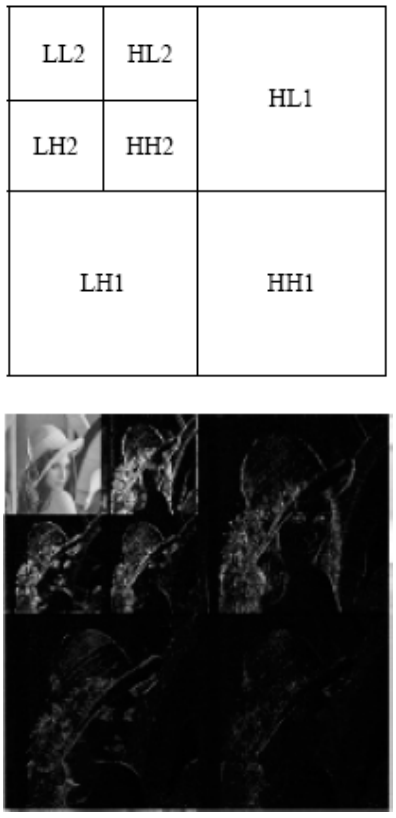
TV ekranında sağ üst köşede görmüş olduğumuz kanala ait logo gözle görülen logodur. Bunun yanında gözle göremediğimiz ancak detektör kullanarak göreceğimiz logolar vardır. Eğer damga cikarmada orjinal resmi kullanıyorsak buna kör olmayan damgalama diyoruz. Kör damgalamada orijinal resim ve damgaya ihtiyaç duyulmadan sadece gizli anahtar kulanılarak damga elde edilir. Yarı-kör damgalamada ise yine orijinal resme ihtiyaç duyulmadan sadece gizli anahtar ile damga kullanılarak damga cıkarılabilir[5].

İki türlü damga vardır. Birincisi gözle görülebilir logolar ikincisi ise rastgele(random) sayı sıralarıdır (PRN). Video damgalama araştırma açısından daha açık bir alandır. Özellikle zamana dayalı veri olduğu için çerçeve ortalama, çerçeve düşürme ve çerçeve değiştirme gibi saldırılar olmaktadır ve bu saldırılara karşı dayanıklı bir algoritma üretmek daha zordur.

Uzamsal alanlarda yapılan gömme işleminde logo direk olarak orjinal resme eklenir. Dönüşüm alanlarında yapılan gömme işleminde ise önce DWT,DCT yada DFT alanlarına çevrilen orjinal resim buradaki katsayılara eklenir. Video, ses gibi zamana bağlı elemanlarda ise sıkıştırılmış alanlarında (JPEG, MPEG v.b.) gömme yapılır.

DCT: Resim düşük, orta ve yüksek frekanslar olarak üç parçaya bölünür [4,6]. Algoritmaya baglı olarak bu parcalara gömme yapılır.

DWT: Resim 4 parçaya bölünür. LL, HL,LH ve HH bantları olmak üzere. LL bantı düşük, diğer 3 bant ise yüksek frekanslara sahiptir. Şekil 2 Lena imgesi için DWT iki katmanlı bantlarını göstermektedir [1].



Şekil 2.Lena imgesi ikinci katman ayrışmış DWT

Saldırılar: Damgalama algoritmamız saldırılara karşı dayanıklı olmalıdır. İki türlü saldırı vardır [6].

a.Direk olarak damgayı silmeye yada hasar vermeye yönelik saldırılar.

b.Algoritmayı çalışmaz hale getirmek için yapılan saldırılar.

Değerlendirme:

Damgalanmış imgenin kalitesini ölçmek için çeşitli değerlendirme metodları vardır.Bunlar:

a.MSE: (mean-square error)

$$MSE = \frac{\sum (f(i,j) - F(i,j))^2}{N^2}$$

b.PSNR: (Peak-signal-to noise ratio)

$$PSNR = 20 \times \log_{10}\left(\frac{255}{RMSE}\right)$$

c.M-SVD: (Measure of singular value decomposition)

$$M - SVD = \frac{\sum_{i=1}^{(k/n)\times(k/n)} (|\, D_i - D_{mid}\,|)}{(k/n)\times(k/n)}$$

d.SR: (Similarity ratio)

Dönüşüm alanlarında damgalama olarak birçok çalışma yapılmıştır. Bunlardan temel olanı Cox'in [4] yapmış olduğu DCT ile gri resimlere damgalama metotudur. Piva [6] aynı metodu logo yerine PRN ekleyerek yapmış ve başarılı sonuçlar almıştır. DWT olarak ilk çalışmayı Dugat [1] yapmıştır. 4 banta ayrılan resimlerde yüksek frekans olan HL,LH ve HH bantlarına gömme yapılmıştır. Dugat'in çalışması Piva'ya göre daha fazla gelecek vadetmektedir.

4.Yeni Damgalama Metodu

Dugat'ın algoritması sadece belirli bir grup saldırıya karşı dayanıklıdır. Biz ise bu algoritmayı geliştirerek farklı uygulamalardan çok daha iyi sonuçlar aldık. Geliştirdiğimiz algoritmayı şöyle özetleyebiliriz:

Ekleme:

1.*NxN* boyutlarındaki imge DWT'ye dönüştürülerek katsayılar hesaplanır.

2.Gizli anahtar kullanılarak bir PRN oluşturulur.

3.PRN katsayılarından T basamağından büyük olanlarına $T = \{t_i\}$, $t'_i = t_i + \alpha|t_i|x_i$, formülü kullanılarak LL ve HH bantlarına damga eklenir.

4. T katsayıları T' olarak değiştirilir.

5.DWT'den geriye imgeye dönülür. Böylelikle damgalama işlemi tamamlanmış olup I' elde edilmiş olur.

Detektör:

1.DWT katsayıları damgalanmış belkide saldırıya uğramış imge için hesaplanır.

2.T_2 basamağından büyük olan katsayılar bulunur.

3.Toplam $Z = \frac{1}{M}\sum_{i=1} y_i t_i^*$ hesaplanır.

4.Basamak $T = \frac{\alpha}{2M}\sum_{i=1} |\, t_i^* \,|$ hesaplanır.

5.Eğer Z>T ise damga var, aksi halde ise damga yok diye sonuç çıkartılır.

Haar süzgecinin kullanıldığı çalışmamızda oldukça başarılı sonuçlar alınmıştır. Sonuçlar göstermektedir ki:

a.Bir grup saldırı için (jpeg, resizing, gaussian noise,low pass filtering ve rotation) LL bantta damgalama yapmak;

b.Bir diger grup saldırı için (histogram equalization, contrast adjustment, gamma çorrection ve cropping) HH bantta damgalama yapmak saldırılara karşı daha başarılı sonuçlar vermektedir.

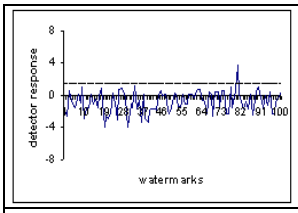
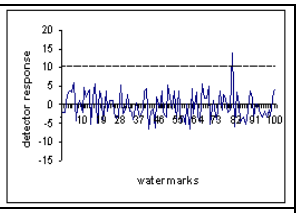
Original Lena | Damgalanmis Lena PSNR = 41.07 | Fark

Sekil 3. Damgalanmis Lena

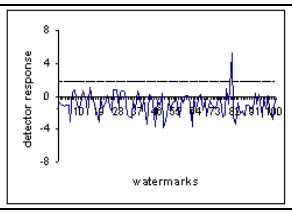
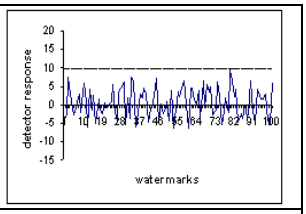
	
JPEG compression (Q=25)	Resizing (512→256→512)
	
Low pass filtering (window size=3x3)	Rotation (20^0)
	
Contrast adjustment ([l=0 h=0.8],[b=0 t=1])	Gamma correction (1.5)
	
Gaussian noise (mean = 0, variance =	Histogram equalization (automatic)

Şekil 4. Damgalanmış imgeye saldırılar

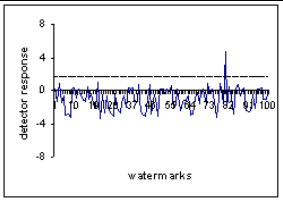
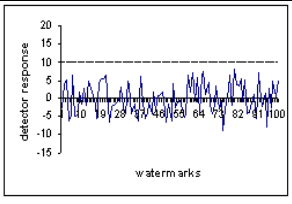
Şekil 3 orjinal imge ve damgalanmış imgeyi, şekil 4 ise damgalanmış imgeye yapılan ortak saldırıları göstermektedir. Sekil 5-14 ise detektör sonuçlarını gri, renkli ve video uygulamaları için vermektedir.

	
LL band (T=1.415)	HH band (T=10.236)

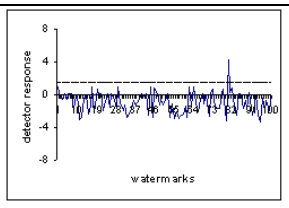
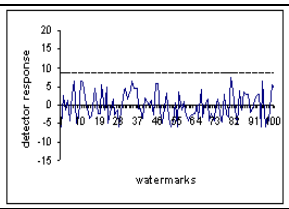
Şekil 5. Saldırıya uğramamış damgalı Lena için detektör sonuçları

	
LL band (T=1.752)	HH band (T=9.747)

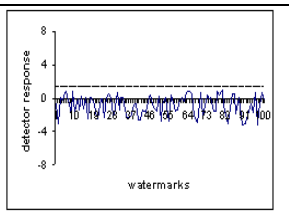
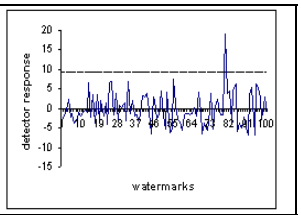
Şekil 6. JPEG Sıkıştırması için detektör sonuçları: Q=25

	
LL band (T=1.752)	HH band (T=9.997)

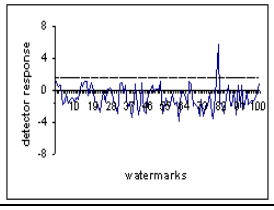
Şekil 7. Gaussian Gurultusu için detektör sonuçları

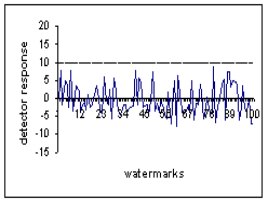
	
LL band (T=1.498)	HH band (T=8.703)

Şekil 8. Resizing için detektör sonuçları

	
LL band (T=1.462)	HH band (T=9.293)

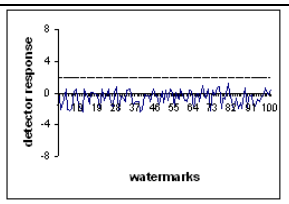
Şekil 9. Croping için detektör sonuçları

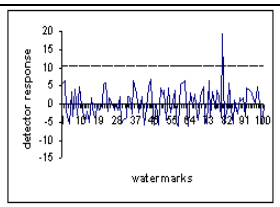




LL band (T=1.624)	HH band (T=9.812)

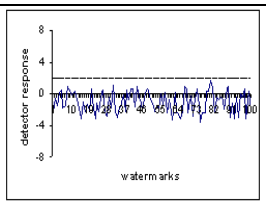
Şekil 10. Low pass süzgeçleri için detektör sonuçları

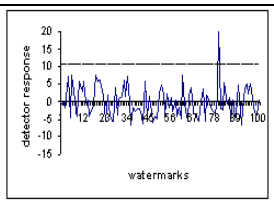




LL band (T=1.882)	HH band (T=10.455)

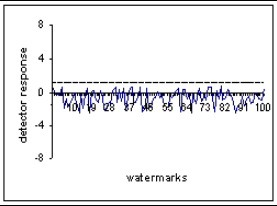
Şekil 11. Histogram Equalization için detektör sonuçları

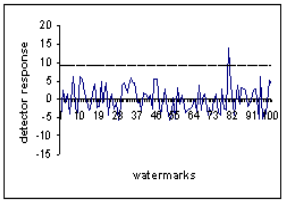




LL band (T=2.029)	HH band (T=10.748)

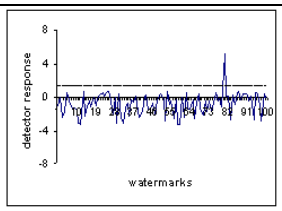
Şekil 12. Contract adjustment için detektör sonuçları

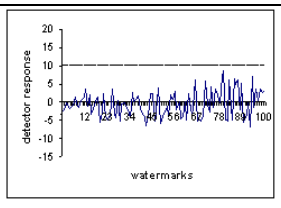




LL band (T=1.105)	HH band (T=9.138)

Şekil 13. Gamma çorrection için detektör sonuçları





LL band (T=1.126)	HH band (T=10.126)

Şekil 14. Rotation (20) için detektör sonuçları

5. SONUÇLAR

Dijital imge damgalama uygulama alanları bakımından önemli bir araştırma konusudur. Bu alanda birçok algoritma üretilmiş olmasına rağmen en önemli sorun bir takım saldırılardan sonra geliştirilen algoritmanın çalışmaması yada damgalanan logoların özelliğini kaybetmesidir. Bu bağlamda geliştirmiş olduğumuz DWT de hem LL hemde HH bantlara PRN ekleyerek saldırılara karşı daha dayanıklı damgalama yapılmıştır. Bazı saldırılara karşı LL bant bazı saldırılara karşı ise HH bant doğru sonuçlar vermiştir. Buradan sonuç olarak DWT de her iki bantta damgalama yapılması daha başarılı sonuçlar verdiği çıkartılabilir.

Teşekkür

Damgalama alanında yapmış olduğum çalışmalarda katkısından dolayı Prof.Dr.Ahmet Eskicioğlu'na teşekkür ederim.

Kaynaklar

[1] R. Dugad, K. Ratakonda, ve N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," *Proceedings of 1998 International Conference on Image Processing (ICIP 1998)*, Vol. 2, Chicago, IL, Ekim 4-7, 1998, pp. 419-423.

[2] E. Elbasi ve A. M. Eskicioglu, "A DWT-based Robust Semi-blind Image Watermarking Algorithm Using Two Bands," IS&T/SPIE's 18th Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, Ocak 15–19, 2006.

[3] C.-H. Lee ve Y.-K. Lee, "An Adaptive Digital Image Watermarking Technique for Copyright Protection," *IEEE Transactions on Consumer Electronics*,45(4), Kasim 1999, pp. 1005-1015.

[4] I. J. Cox, J. Kilian, T. Leighton ve T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, 6(12), Aralik 1997, pp. 1673-1687.

[5] W. Zhu, Z. Xiong ve Y.-Q. Zhang, "Multiresolution Watermarking for Images and Video," *IEEE Transactions on Circuits and Systems for Video Technology*, 9(4), Haziran 1999, pp. 545-550.

[6] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image, Proceedings of the 1997 International Conference on Image Processing (ICIP '97), Washington, DC, USA, Ekim 26-29, 1997.