SAYISAL İMGELER İÇİN AYRIK KOSİNÜS DÖNÜŞÜMÜ ESASLI VERİ GİZLEMENİN ATAKLARA DAYANIKLILIĞI

Murat YEŞİLYURT[*], Ahmet Turan ÖZCERİT[**], Yıldıray YALMAN[*] ve İsmail ERTÜRK[*]

(*) *Turgut Özal Üniversitesi, Bilgisayar Mühendisliği Bölümü, ANKARA*

(**) *Sakarya Üniversitesi, Elektronik ve Bilgisayar Eğitimi Bölümü, SAKARYA*

myesilyurt@turgutozal.edu.tr, aozcerit@sakarya.edu.tr, yyalman@turgutozal.edu.tr, ierturk@turgutozal.edu.tr

Özet: Sıkıştırılmış sayısal imgeler özellikle internet ortamında yaygın bir biçimde kullanılmaktadır. Bu durum, telif hakkı ihlallerinin önlenmesi ve sıkıştırılmış imgelerin gizli haberleşme ortamı olarak kullanılması açılarından yeni çalışmaların da çıkış noktası olmuştur. Damgalama ve veri gizleme olarak adlandırılan her iki durumda da sayısal imgelere çeşitli yöntemlerle gizli veriler (damga, kişisel bilgi, kritik bilgi vb.) gömülür. Bu imgelerin iletişim ortamındayken değişik saldırılara ve bozulmalara maruz kalma ihtimali, taşınılan gizli bilgilerin kaybolmaması amacıyla dayanıklı veri gizleme yöntemlerinin geliştirilmesi ve kullanımı önem arz etmektedir. Bu bildiride sunulan çalışmada, **A**yrık **K**osinüs **D**önüşümü (**AKD**) esaslı görünmez damgalama/veri gizleme yöntemi kullanılarak elde edilen taşıyıcı imgelerin, çeşitli saldırılar (sıkıştırma, parlaklık değiştirme, tekdüze gürültü) sonucunda içerdiği gizli bilgiyi muhafaza etme yeterliliği incelenmektedir. AKD bloklarına ait katsayıların veri gizleme için kullanılması ve ikili damganın her bir bitinin ayrı bir bloğa gömülmesi ile ataklar sonucunda gizli bilgide oluşan bozulmanın minimize edilebildiği gösterilmektedir.

Anahtar Kelimeler: Görünmez Damgalama, Veri Gizleme, Ayrık Kosinüs Dönüşümü, Bilgi Güvenliği

ROBUSTNESS OF DIGITAL IMAGE DATA HIDING METHODS BASED ON DISCRETE COSINE TRANSFORM AGAINST ATTACKS

Abstract: Compressed digital images are often used because they have relatively small sizes and can be easily transmitted over the internet. This fact naturally brings up copyright issues to be handled as well as enables utilizing compressed images as an important medium for transferring secret information. In both cases, watermarks or secret data are hidden in digital images by using various data embedding methods. However, any attack from a third party may lead to loss of hidden data carried in the stego images. In this paper, robustness of **D**iscrete **C**osine **T**ransform (**DCT**) based data hiding or blind watermarking methods for digital images against well-known attacks (jpeg compression, sharpen noise, uniform noise, etc.) is examined. The method focused on in this work is based on the fact that each bit of the binary watermark is embedded in a different DCT block. Thus, carrier deterioration is minimized, achieving a high invisibility. The results show that, this method can be safely used for binary watermarks. After the data hiding or watermarking processes, stego images is corrupted by using JPEG compression, sharpen and uniform noise attacks in order to analyze the changes on the watermark/hidden data.

Keywords: Invisible Watermarking, Data Hiding, Discrete Cosine Transform, Information Security

1. Giriş

Hızla gelişen bilgisayar teknolojisi ile birlikte artan internet kullanımı imge, video, ses, yazı gibi çoklu ortam elemanlarının serbestçe kullanılmasına olanak sağlamıştır [1]. Sayısal çoklu ortam dosyalarını korumak için günümüze kadar birçok veri gizleme yöntemi geliştirilmiş olup, bunlardan en çok kullanılanları; Steganografi Algoritmaları, Damgalama Algoritmaları ve diğer veri gizleme algoritmalarıdır [2].

Damgalama yöntemleri genel olarak damgalama algoritmasının oluşturduğu düzleme göre iki ana grupta incelenmektedir:

- Uzamsal Alan (Spatial Domain): Damgalama işlemi için imgenin piksel değerleri kullanılır.
- Frekans Alanı (Frequency Domain): Damgalama, Ayrık Kosinüs Dönüşümü (AKD), Ayrık Fourier Dönüşümü (AFD) veya Ayrık Dalgacık Dönüşümü (ADD) gibi dönüşümler sonucunda elde edilen katsayılar kullanılarak gizlenir [3].

Bu dönüşümlerden AKD, birçok çalışmada görüntü damgalama yöntemi olarak tercih edilmiş Frekans Alanı aracıdır [4].

İmgelerin damgalanması konusunda son yıllarda oldukça başarılı çalışmalar yapılmış, özellikle logo ya da gürültü şeklindeki damgalar imgelere gömülmüştür. Uzamsal alanlarda yapılan çalışmalar "Cox" ile başlamış, ancak bazı saldırılar karşısında dayanaksız olan bu algoritmalar ilk olarak "Piva"nin AKD alanında yapmış olduğu çalışmalarla birlikte frekans uzayında yaygın olarak yapılmaya başlanmıştır [5].

Bu bildiride sunulan çalışmada, Ayrık Kosinüs Dönüşümü (AKD) esaslı görünmez bir damgalama yöntemi kullanılarak elde edilen yeni imgelerin, çeşitli saldırılar (sıkıştırma, parlaklık değiştirme, tekdüze gürültüsü) sonucunda, içerdikleri gizli bilgiyi muhafaza etme yeterlikleri incelenmektedir.

Bildirinin izleyen bölümleri şöyle organize edilmiştir: Bölüm 2'de imge sıkıştırma hakkında genel bilgiler verilerek, alt bölümlerde YCbCr renk uzayı ve AKD anlatılmaktadır. Uygulanan görünmez damgalama yöntemi ve ataklara karşı taşıyıcı imgelerin dayanıklılığı Bölüm 3'te detaylandırılırken, son bölümde ise sonuçlar ve genel bir değerlendirme sunulmaktadır.

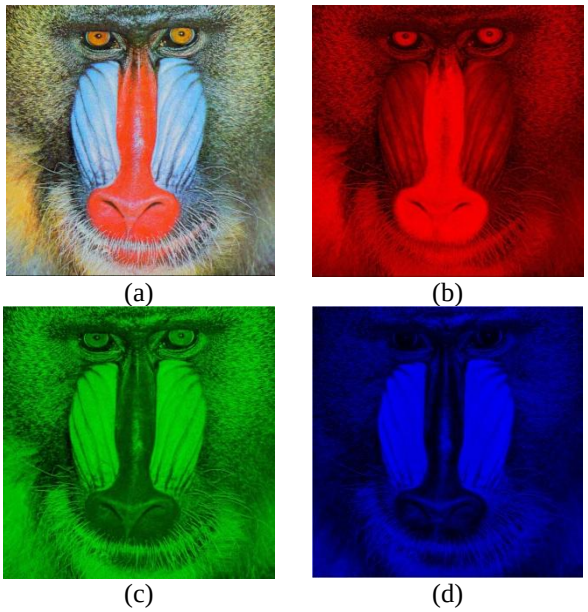
2. İmge Sıkıştırma Temelleri

Veri sıkıştırma yöntemleri, verilerin depolama ortamlarında daha az yer kaplamaları ve bir iletişim ağı üzerinden daha hızlı transfer edilebilmeleri için günümüzde yaygın olarak kullanılmaktadırlar. Sıkıştırma yöntemleri kayıpsız ve kayıplı sıkıştırma olarak iki alt başlıkta incelenirler. Kayıpsız sıkıştırmada orijinal veri sıkıştırma işleminden sonra istendiğinde tamamen elde edilebilirken, sıkıştırma oranları düşük kalmaktadır. Kayıplı sıkıştırmada ise orijinal veride kayıplar meydana gelmekle birlikte kapladıkları alan ya da iletimde ihtiyaç duyulan band genişliği azalmakta ve sıkıştırma oranına bağlı olarak görüntüde meydana gelen bozulma İnsan Görme Sistemi (İGS) tarafından algılanamamaktadır. Kayıplı sıkıştırma yöntemlerinde en çok kullanılan JPEG algoritmasında, öncelikle YCbCr dönüşümü yapılır ve sonra AKD (DCT) dönüşümü gerçekleştirilir.

Şekil 1'de JPEG sıkıştırma algoritmasının genel şeması görülmektedir [6].

2.1. RGB ve YCbCr Renk Uzayları

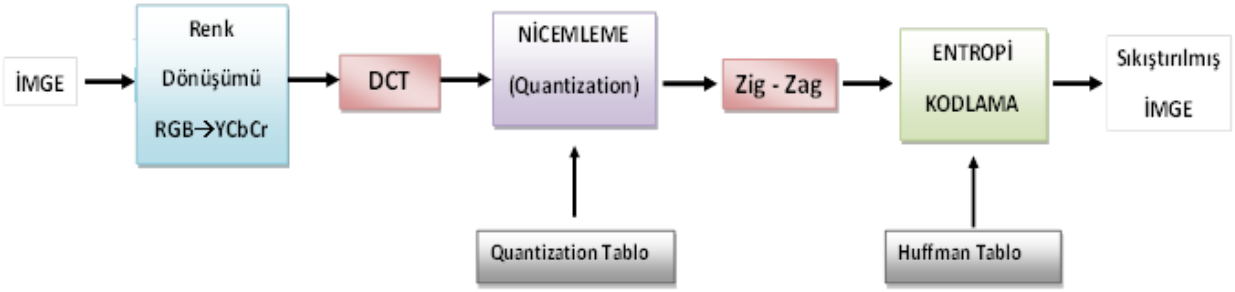
Birçok çalışmada imgelerin renk değerleri veri gizleme ve damgalama algoritmalarında kullanılmaktadır. Sayısal imgelerde RGB (Red, Green, Blue) (Şekil 2). MPEG (Motion Pictures Expert Group) ve JPEG formatlarında YUV (Y: Luminance, U: Chrominance1 (blue), V: Chrominance2 (red)) ve YCbCr (Y: Luminance, Cb: Chrominance1 (blue), Cr: Chrominance2 (red)) renk uzayları kullanılmaktadır [7].



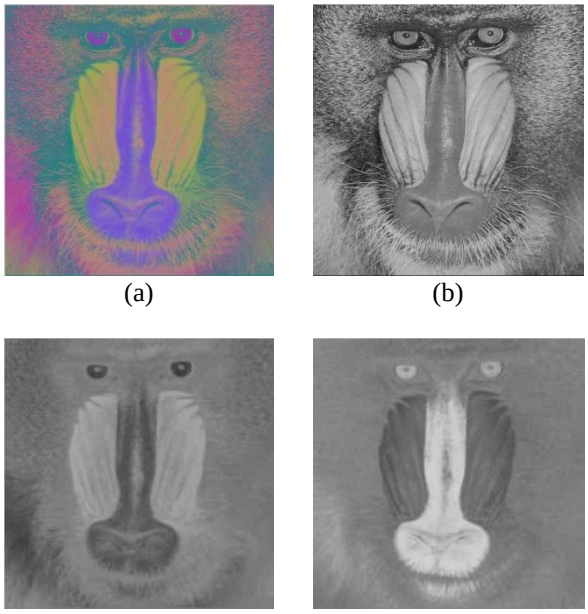
Şekil 2. RGB imge (a) ve R (b), G (c), B (d) renk kanalları.

RGB renk uzayında renkler her biri 8 bitlik üç ayrı kanalda tanımlanmaktadırlar. Bu renk uzayında renk (hue), doygunluk (saturation) ve parlaklık (brightness) değerleri bulunmamaktadır.

YCbCr renk uzayında ise biri parlaklık (Y) olmak üzere iki renk (Cb, Cr) kanalı bulunmaktadır (Şekil 3). Bu renk kanallarında parlaklık değeri 4 bit, renk değerleri ise ikişer bitle ifade edilmektedir.



Şekil 1. JPEG imge sıkıştırma şeması.



(a) (b)

(c) (d)

Şekil 3. YCbCr imge (a) ve Y (b), Cb (c), Cr (d) renk kanalları.

Denklem (1)'de ITU−R BT.601 standardına göre RGB renk uzayından YCbCr renk uzayına dönüşüm gösterilmektedir [8].

$$Y = 0.257R + 0.504G + 0.098B + 16$$

$$Cb = -0.148R - 0.291G + 0.439B + 128 \quad (1)$$

$$Cr = 0.439R - 0.368G - 0.071B + 128$$

2.2. Ayrık Kosinüs Dönüşümü (AKD)

Ayrık Kosinüs Dönüşümü, frekans alanında en uygun enerji dağılımını sağlaması sebebiyle, Jpeg, Mpeg ve H.26x serileri de dahil olmak üzere bir çok kodlama sisteminde, başarıyla kullanılmaktadır [9].

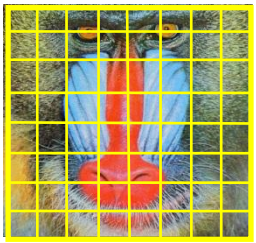
Damgalama işlemlerinde AKD'nin orta bandında (middle band) yer alan katsayıların kullanılmasının sebebi sıkıştırmalar karşısında oldukça dayanıklı bir yapıda olmasıdır. Denklem (2)'de N×M boyutlu bir f(x,y) imgesinin AKD formülü görülmektedir [10].

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16} \quad (2)$$

$$C(u), C(v) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } u, v = 0 \\ 1 & \text{diğer durumlar} \end{cases}$$

3. Kullanılan AKD Esaslı Damgalama Yöntemi

Frekans Uzayı, literatürde yer alan birçok görünmez damgalama uygulamasında kullanılmıştır. Özellikle JPEG sıkıştırma saldırısına maruz kalan imgelerde, damga bilgisini korumak amacıyla AKD esaslı yöntemler tercih edilmektedir [11]. AKD ile yapılan damgalama uygulamalarında imge, her biri 8×8 boyutunda olan bloklara bölünür ve her bloğun frekansları ayrı ayrı hesaplanır (Şekil 4). Değişikliklerin yapılacağı frekansların seçiminde, JPEG kayıplı sıkıştırmasının etkisi ve imgede oluşacak bozulmanın İGS tarafından fark edilemeyecek kadar küçük bir seviyede tutulması önemli rol oynamaktadır. Bunun için orta frekans bandının seçilmesi literatürde genel kabul gören bir yaklaşımdır [10, 11].



RGB-YCbCr Dönüşümü

Y

445.934	-6.6754	5.3726	0.5681	-0.0985	0.0174	0.0695	-0.3180
-30.9788	-4.8906	-3.1945	-0.4683	0.0383	-0.2661	-0.3175	0.0401
-3.2713	0.2034	0.1755	-0.3423	0.5511	-0.2608	-0.1245	-0.1105
-3.9521	-0.0811	0.3795	-0.3701	0.1156	-0.3607	-0.0522	-0.0848
0.1815	0.1242	0.1137	-0.1951	-0.4638	0.0993	0.4411	0.3049
-0.1355	-0.2939	0.2242	-0.1713	-0.7617	0.0421	-0.2898	-0.2869
-0.1425	-0.2790	-0.8220	0.0637	0.1492	0.2753	-0.0200	0.0850
0.2897	-0.0765	-0.0933	0.0985	-0.0915	-0.1031	-0.0444	0.3496

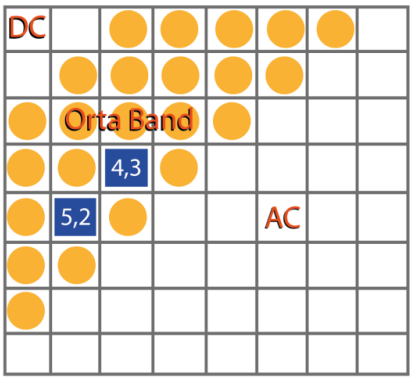
Şekil 4. İmgenin (Y) kanalı için örnek AKD katsayıları.

AKD kullanılarak gerçeklenen damgalama uygulamalarının ataklara dayanıklılığını test edebilmek için örnek bir yöntem kullanılmış olup, takip eden alt bölümde ilgili yöntemin detayları anlatılmaktadır.

3.1. Damganın İmgeye Gömülmesi

Sunulan örnek uygulamada, 2000×2000 çözünürlükteki 24 bitlik örtü verisinin RGB renk değerleri YCbCr renk değerlerine dönüştürülmekte, elde edilen Y (Luminance − Parlaklık) değeri için AKD dönüşümüne tabi tutulmaktadır (Şekil 4). Ortaya çıkan AKD blok katsayılarından, bloğun orta bandında yer alan (5, 2) ve (4, 3) hücreleri damgalama için seçilmiştir (Şekil 5).

Gömü verisinin "1" olduğu durumlarda AKD (5, 2) katsayısının büyük olması istenmekte, "0" olduğu durumlarda ise bu katsayının küçük olması istenmektedir [12].



Şekil 5. Damgalama için kullanılan AKD frekans bileşenleri.

Gömü verisi "1" olduğu halde AKD (5, 2) < AKD (4, 3) ise, değerler birbirleriyle yer değiştirilir. Bu işlemin ardından AKD katsayılarının birbirlerine çok yakın olmasından dolayı damganın (Şekil 6) en az kayıpla geri döndürülmesini sağlamak amacıyla bir güçlülük sabiti (***n***) tanımlanmıştır [13, 14, 15].

Eğer gömü verisi = 1 ise

$$\begin{aligned} AKD(5,2) &= AKD(5,2) + \boldsymbol{n} \\ AKD(4,3) &= AKD(4,3) + \boldsymbol{n} \end{aligned} \tag{3}$$

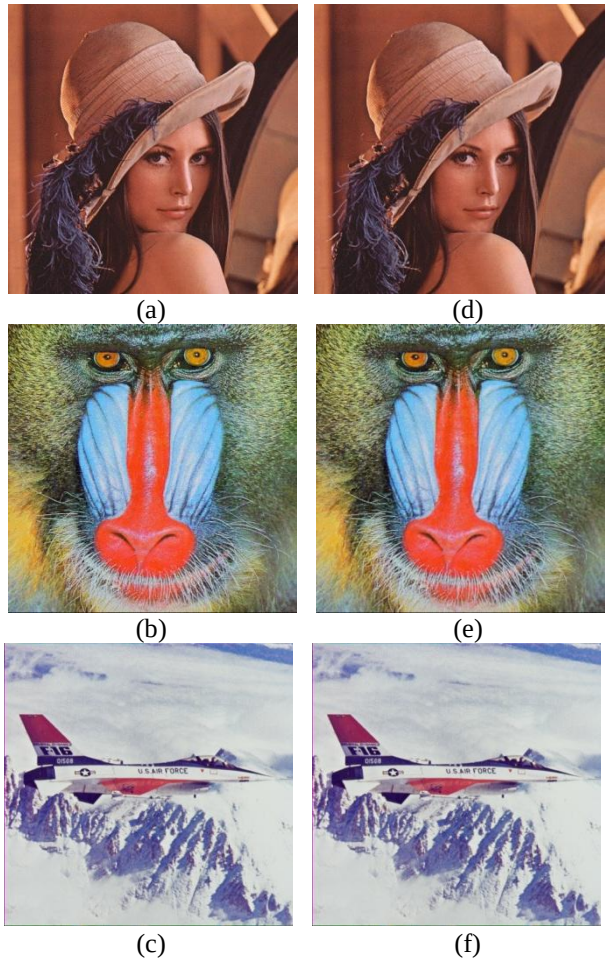
Bu sabit, gömü verisinin geri dönüşümünde belirleyici rol oynamaktadır. Yapılan deneysel çalışmalar sonucunda en iyi sonucu veren ***n*** değeri 12 olarak belirlenmiştir. Bu noktada dikkat edilecek husus, kullanılan damgalama yönteminde AKD katsayılarına gömü verisi değerlerinin herhangi bir şekilde eklenmediğidir.

Şekil 6. 200×200 boyutlarındaki gömü verisi.

Damga eklenen imgelerde (Şekil 7) oluşan bozulmalar uygulanan veri gizleme/damgalama yöntemin başarımını belirlemek için büyük önem taşımaktadır. Bu bozulmalar literatürde yaygın kabul gören Tepe Sinyal Gürültü Oranı (PSNR: Peak Signal to Noise Ratio) ile ölçülmektedir. Kullanılan damgalama yönteminin üç imge için PSNR başarımı oldukça yüksek olup kabul edilebilir seviyededir (Tablo 1).

Tablo 1. Uygulanan AKD esaslı yöntemin başarımı.

İmgeler (2000×2000)	**PSNR (dB)**
Lena	47,78
Baboon	44,24
Airplane	48,10



Şekil 7. Damgalamada kullanılan orijinal imgeler (a, b, c) ve damgalanmış imgeler (d, e, f).

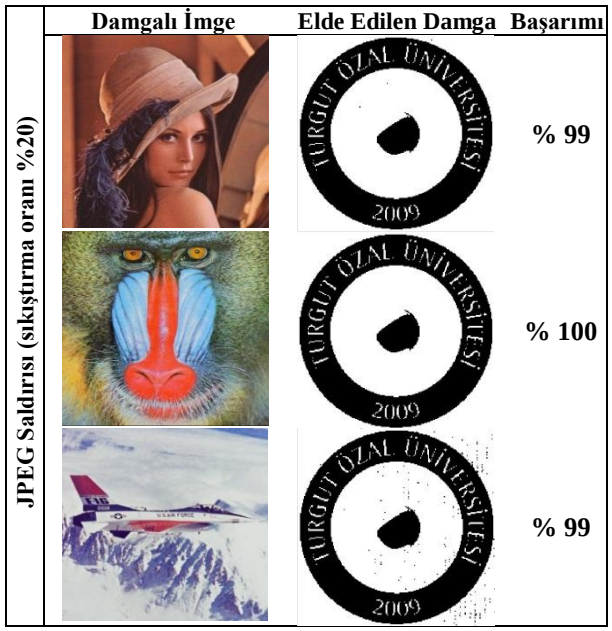
3.2. Damganın Taşıyıcı İmgeden Çıkarılması

Kullanılan örnek yöntemde damganın örtülü veriden elde edilmesi, damgalama işlemlerine oranla daha kolay yapılmaktadır. Öncelikle, damgayı taşıyan taşıyıcı imgeye, damgalama işleminde olduğu gibi RGB−YCbCr renk dönüşümü uygulanır ve parlaklık değerlerinin AKD katsayıları elde edilir. Damgalama sırasında kullanılan (5,2) ve (4,3) katsayılarının değerleri dikkate alınarak gömü verisi (1 veya 0) değeri tekrar elde edilir. Gömü verisi ***v*** olmak üzere incelenen blokta,

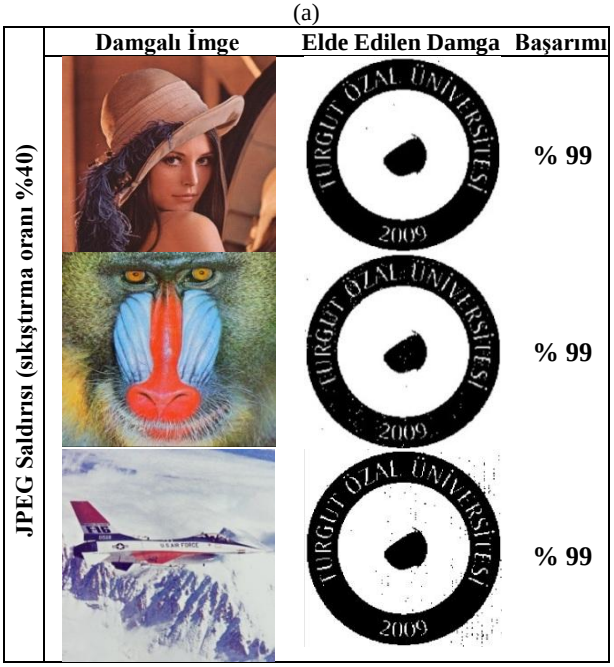
$$\boldsymbol{v} = \begin{cases} 1 & AKD(5,2) > AKD(4,3) \\ 0 & AKD(5,2) < AKD(4,3) \end{cases} \tag{4}$$

denklemi ile damgalanmış veri tespit edilmektedir. Bu işlem gömü verisi kadar blok için uygulanır. Tarama işlemi bittiğinde damga tekrar elde edilmiş olur. Damganın, imgeye ait AKD katsayılarına gömülmesinin ardından kuantalama işlemi yapılıp, kaydedilmesi sürecinde bazı kayıplar meydana gelmektedir. Oluşan bu kayıplara ek olarak, imgenin üçüncü kişilerce ataklara maruz bırakılması ihtimali, damganın sağlıklı şekilde elde edilmesinin önüne geçmektedir. Şekil 8 ve 9'da damgalanmış imgelere bazı atakların yapılmasının ardından, damgada oluşan bozulmalar görülmektedir.

Şekil 8'de, damgalı imgelerin % 20 ve % 40 oranında sıkıştırılması sonucunda, çıkartılan damgalardaki bozulmanın çok düşük seviyelerde olduğu görülmektedir. Şekil 9'da görülen imgelerde ise parlaklaştırma ve tekdüze dağılımlı gürültüye maruz bırakılan imgelerden elde edilen damgalarda da oldukça başarılı sonuçlar elde edilmiştir. Bu noktada öne çıkan en önemli sonuç, AKD esaslı bir yaklaşımla kodlanan ilgili damganın üçüncü kişilerin yapacağı saldırılardan en düşük seviyede etkilenmesi, dolayısıyla damganın imgeden çıkarılmasının ardından anlaşılabilir olmasıdır.

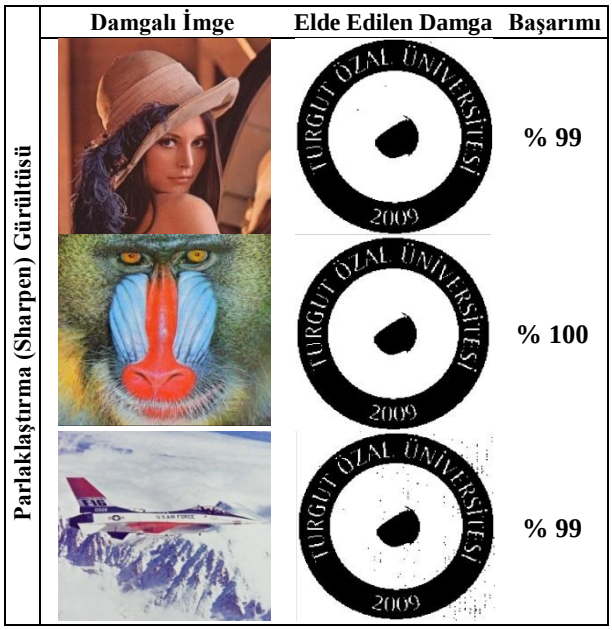


(a)

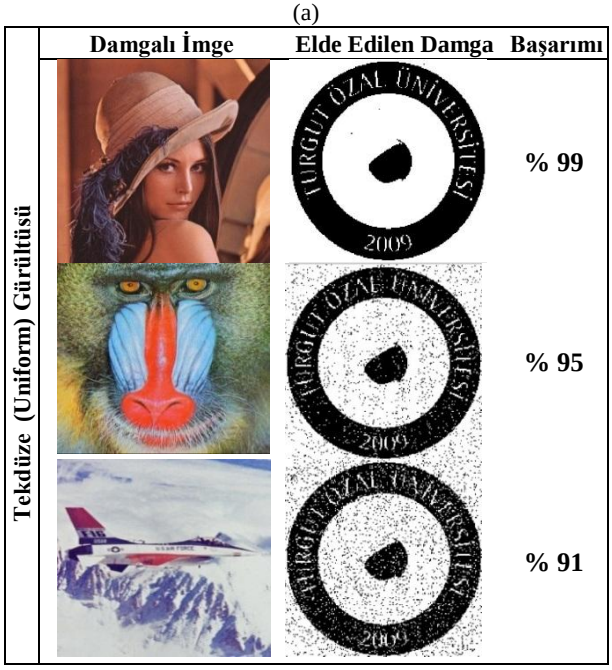


(b)

Şekil 8. Farklı oranlarda JPEG sıkıştırma saldırılarına uğratılmış imgeler, elde edilen damgaların görünümleri ve kurtarılma oranları.



(a)



(b)

Şekil 9. Parlaklaştırma (a) ve tekdüze (b) gürültüleri ile atak yapılan imgeler, elde edilen damgaların görünümleri ve kurtarılma oranları.

4. SONUÇ

Sunulan çalışma, ikili logoların sıkıştırılmış sayısal imgelere gizlenmesi/damgalanması uygulamalarında, AKD yönteminde kullanılan orta bant katsayılarının hem damganın saldırılara karşı dayanıklılığını artırdığı hem de imgeler üzerinde oldukça düşük bozulmalara sebep olduğunu göstermektedir.

Damgalama işleminde örtü verisi olarak kullanılan 24 bit RGB imgelerin YCbCr dönüşümü yapılarak parlaklık (Y) değeri üzerinde gizleme işlemi uygulanmaktadır. Jpeg ve Mpeg standartlarının renk değerlerinden ziyade, yüksek yoğunluklu Y değerini kullanmaları damganın yapılan saldırılara karşı daha güçlü olmasını sağlamaktadır.

Literatürde yer alan diğer çalışmalar incelendiğinde, çok küçük boyutlu ikili resimlerin damga olarak kullanılmış olduğu görülmektedir. Bu bildiride sunulan ve değerlendirilen yöntemin örnek uygulamasında ise 40000 bitten oluşan nispeten büyük bir veri/damga kullanılmış olmasına rağmen, damganın imge içerisine gömülmesi ve çıkarılması işlemleri oldukça basit ve başarılı bir şekilde gerçekleştirilebilmektedir.

Damganın ataklara karşı dayanıklılığını değerlendirmek amacıyla yapılan örnek saldırılar (kayıplı sıkıştırma, parlaklaştırma ve tekdüze dağılımlı gürültü) sonucunda, damgada oluşan bozulmaların kabul edilebilir seviyelerde oldukları görülmüştür. Sonuç olarak, AKD esaslı veri gizleme/damgalama yöntemlerinin gizli haberleşme ve telif hakkı ihlali önleme uygulamalarında kullanımının yerinde bir yaklaşım olacağı öngörülmektedir. Önerilen bu yaklaşımın, sadece sıkıştırılmış imgelerde değil yapılacak geliştirme ile sıkıştırılmış video (Mpeg) ortamlarında da etkin şekilde kullanımının mümkün olduğu değerlendirilmektedir.

KAYNAKLAR

[1] 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), pp. 545−550, 1999.

[2] O. Cetin, A. T. Ozcerit, A new steganography algorithm based on color histograms for data embedding into raw video streams, Computers & Security, 28, 670−682, 2009.

[3] C. T. Hsu, J. W. Wu, Hidden Digital Watermarks in Images, IEEE Transaction on Image Processing, 8 (1), 58−68, 1999.

[4] Q, Wang, S. Sun, DCT−Based Image Independent Digital Watermarking, 5th International Conference on Signal Processing, 2, 942−945, 2000.

[5] S.Aydın, M. Memiş, E. Elbaşı, Dijital İmgelerde Çok Katmanlı DWT ile Damgalama Metodu, SIU 2008, Aydın, 2008.

[6] A. Mesut, Veri Sıkıştırmada Yeni Yöntemler, Ph.D. Thesis, Trakya University, 2006.

[7] S. K. Singh, S. K. D. Agarwal, A. Gambhir, S. Kumar, Colour Space Entropy Based Lossy and Lossless Colour Image Compression System, International Journal of Computer Science and Network Security, 9 (3), 327-336, 2009.

[8] R. Lukac, K. N. Plataniotios, Color Image Processing: Methods and Applications, Taylor & Francis Group, LLC, New York, 2007.

[9] Y.Y. Chen, Medical Image Compression Using DCT-based Subband Decomposition and Modified SPIHT Data Organization, International Journal of Medical Informatics, Elsevier, 76 (2007) 717–725, 2006.

[10] P. Zhengjun, A. G. Rust, H. Bolouri, Image Redundancy Feduction for Neural Network Classification Using Discrete Cosine Transforms, IEEE−INNS−ENNS International Joint Conference, 3(3), 149−154, 2000.

[11] A. Koschan, M. Abidi, Digital Color Image Processing, Wiley Interscience, Canada, 50−51, 2008.

[12] Yesilyurt, M., Yalman, Y., Erturk, I., Ozcerit, A.T., A DCT based Invisible Watermarking Application for Compressed Images, 8th International Conference on Electronics and Computer Technologies (IKECCO'2011), December 18–20, Kazakhstan, 2011.

[13] F. A. P. Petitcolas, Watermarking Schemes Evaluation, IEEE Signal Processing Magazine, 17, 58−64, 2000.

[14] C. T. Hsu, J. L. Wu, Multiresolution Watermarking for Digital Images, IEEE Transactions on Circuits and Systems − II: Analog and Digital Signal Processing, 45(8), 1097−1101, 1998.

[15] V. Saxena, J. P. Gupta, Collusion Attack Resistant Watermarking Scheme For Colored Images Using DCT, IAENG International Journal of Computer Science, 34(2), 2007.