Erciyes Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 38, Sayı 1, 2022

Erciyes University
Journal of Institute of Science and Technology
Volume 38, Issue 1, 2022

Görüntü Kimlik Doğrulaması İçin Yeni Bir Ayrık Kosinüs Dönüşümü Tabanlı Kendinden Gömülü Kırılgan Damgalama Yöntemi

Ayhan Renklier*[1], Serkan Öztürk[2],

*[1] Kayseri Üniversitesi Develi Hüseyin Şahin Meslek Yüksekokulu Bilgisayar Teknolojisi Bölümü, Develi, KAYSERİ
[2] Erciyes Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği, KAYSERİ

(Alınış / Received: 12.02.2022, Kabul / Accepted: 14.04.2022, Online Yayınlanma / Published Online: 30.04.2022)

Anahtar Kelimeler
Görüntü Damgalama,
Görüntü Doğrulama,
Ayrık Kosinüs Dönüşümü

Öz: Son yıllarda görüntü paylaşımının hızla artması ile birlikte görüntü kimlik doğrulaması önemli bir konu haline gelmiştir. Görüntü kimlik doğrulaması için genellikle görüntü damgalama yöntemleri kullanılmaktadır. Bu yöntemlerde, görüntüden elde edilen damga bilgisi algılanamaz bir şekilde görüntüye eklenir. Damgalı görüntüye herhangi bir saldırı olup olmadığı görüntüden çıkarılan damga ile görüntüden elde edilen damga karşılaştırılarak gerçekleştirilir. Bu yöntemlerin çoğunda damga bilgisi blok tabanlı olarak elde edilir. Küçük boyutlu blok kullanan yöntemlerde damga görüntünün kalitesini düşürürken, büyük boyutlu blok kullanan yöntemlerde ise kurcalanmamış bölgeler saldırılmış olarak algılanabilir. Bu makalede görüntü kimlik doğrulaması için Ayrık Kosinüs Dönüşümü (AKD) tabanlı trigonometrik fonksiyon kullanan yeni bir kendinden gömülü kırılgan damgalama metodu önerilmiştir. İlk olarak gri seviyeli görüntü birbiriyle örtüşmeyen 4×4 boyutunda bloklara ayrılır. Ayrılan bloğa AKD uygulanarak, DC bileşeni seçilir. Seçilen değer, blok konum bilgisi ve güvenlik anahtarı kullanılarak, yeni trigonometrik formül ile kontrol bitleri oluşturulur. Üretilen bu kontrol bitleri bloğun ilk en az anlamlı bitlerine damga olarak saklanır. Önerilen yöntemin damgalı görüntünün şeffaflığını koruduğu ve görüntü üzerine yapılan bölgesel saldırıları tespit ettiği deneysel çalışmalarla gösterilmiştir.

A Novel Discrete Cosine Transform Based Self-embedded Fragile Watermarking Method For Image Authentication

Keywords
Image Watermarking,
Image Authentication,
Discrete Cosine Transform

Abstract: With the rapid increase in image sharing in recent years, image authentication has become an important issue. Image watermarking methods are generally used for image authentication. In these methods, the watermark information obtained from the image is imperceptibly embedded to the image. Whether there is any attack on the watermarked image is performed by comparing the watermark extracted from the image with the watermark obtained from the image. In most of these methods, watermark information is obtained on a block basis. While watermarking reduces the quality of the image in methods using small blocks, methods using large blocks may detect untampered regions as attacked. In this article, a new self-embedded fragile watermarking method based on Discrete Cosine Transform (DCT) with a trigonometric function is proposed for image authentication. First, the gray-level image is divided into non-overlapping 4×4 blocks. By applying DCT to the allocated block, the DC component is selected. Using the selected value, block position information and security key information, the control bits are generated with the new trigonometric formula. These generated control bits are embedded as watermark to the first least significant bits of the block. It has been shown

by experimental studies that the proposed method preserves the transparency of the watermarked image and detects regional attacks on the image.

*İlgili Yazar, email: ayhan@kayseri.edu.tr

1. Giriş

Son yıllarda internet, akıllı cihazlar ve sosyal medya araçlarının gelişmesi ile birlikte görüntü paylaşımı hızla yaygınlaşmıştır. Buna bağlı olarak kullanılan görüntülerin değiştirilmesi ve kopyalanması çok kolay hale gelmiştir. Bu sebepten dolayı görüntülerin doğrulanması, bütünlüğünün korunması ve sahteciliğin tespiti için askeri, medya ve adli tıp alanlarında çalışmalar yapılmaktadır. Görüntü kimlik doğrulaması için sayısal imzalama ve sayısal damgalama yaygın olarak kullanılmaktadır. Sayısal imzalama tekniklerinde görüntü içeriği görüntü sahibi tarafından imzalanmaktadır [1]. Bu yöntemler, görüntü bütünlüğünün korunmasında başarılı olmalarına rağmen, kurcalanan bölgelerin tespit edilmesini gerçekleştirememektedir. Sayısal damgalama tekniklerinde ise görüntü üzerine damga bilgisi algılanamaz bir şekilde eklenir. Sonrasında görüntüden çıkarılan damga ile orijinal damga karşılaştırılır ve görüntü doğrulanır [2].

Sayısal damgalama teknikleri, dayanıklı, yarı-kırılgan ve kırılgan olarak üçe ayrılır. Dayanıklı damgalama tekniklerinde saldırı yapılan damgalanmış görüntüden çıkartılan damganın görünür olması amaçlanmaktadır [3]. Yarı kırılgan damgalama tekniklerinde damga belirli saldırılar karşısında dayanıklı olmalıdır. Kırılgan damgalama tekniklerinde ise görüntü üzerinde yapılabilecek en ufak değişiklikte, damganın bozulması istenmektedir.

Literatürde kırılgan görüntü damgalama konusunda birçok çalışma bulunmaktadır. Walton görüntü kimlik doğrulaması işlemini damgalama tekniği ile gerçekleştiren ilk kişidir. Walton'un önerdiği yöntemde, görüntü 8x8 bloklara ayrılır ve en önemli yedi bitinin ortalaması alınarak rastgele seçilen piksellerin en önemsiz bitlerine yerleştirilir. Ancak bu yöntemde kurcalanmış bölgeler tam olarak tespit edilememektedir [4]. Chen ve Wang çalışmalarında blok tabanlı bir yapı önermişlerdir. Blokları birbirleri ile ilişkilendirmek için fuzzy c-means kümeleme tekniği kullanmışlardır. Bu yöntemde güvenli anahtar ile birlikte kimlik doğrulama bitleri, her görüntü bloğunun son iki bitine gömülmüştür [5]. Trivedy ve Pal piksel düzeyinde kurcalanmış alanların tespiti için bir kırılgan damgalama yöntemi önermişlerdir. Bu yöntemde, lojik haritadan üretilen kaotik sıralama kullanılarak damgalama bitleri elde edilmiştir. Damgalama bitleri, anahtar matris yardımı ile orijinal görüntü üzerinde saklanmıştır [6]. Gül ve Öztürk görüntü kalitesini ve güvenilirliği arttırmak amacıyla çalışmalarında SHA-256 temelli bir çalışma yapmışlardır. Çalışmalarında 32x32 boyutunda blok kullanmışlar ve elde edilen özet bilgisini görüntü bloğunun dörtte birine yerleştirmişlerdir [7]. Neena ve Shreelekshmi MD5 ve SHA-256 özet fonksiyonlarını kullanarak karma bir yöntem önermişlerdir [8]. Renklier ve Öztürk Frei-Chen temelli bir blok tabanlı yöntem geliştirmişlerdir. Bu yöntemde 3x3 boyutu her bir blok için Frei-Chen özellikleri, blok bilgisi ve güvenlik anahtarı kullanılarak doğrulama bitlerini oluşturmuşlardır [9].

Kırılgan görüntü damgalamada blok tabanlı ve piksel tabanlı metotların yanı sıra dönüşüm tabanlı metotlar da kullanılmaktadır. Qin ve arkadaşları 8×8 bloklara ayrık kosinüs dönüşümünü (AKD) rastgele uygulayarak doğrulama bitlerini oluşturmuşlardır [10]. Yeh ve Lee, görüntüyü 8×8 örtüşmeyen bloklara bölüp, bu bloklara AKD uygulamışlardır. Bu AKD uygulananmış blokların entropi değerlerinden kurtarma bitlerini elde etmişlerdir. Bu bitleri Toral otomorfizmi tekniği ile bloklar içerisine gizlemişlerdir [12]. Zang ve arkadaşları ise 8×8 ve 4×4 örtüşen bloklar üzerinde hızlı fraktal kodlama temelli bir metot önermişlerdir. Kurtarma bitlerini oluşturmak için fraktal kodlama, AKD ve bitlerin sola kaydırılmasından faydalanmışlardır [13]. Pred ve Vizireanu, JPEG sıkıştırma saldırılarına karşı bir yöntem sunmuşlardır. Bu yöntemde, bloklara uygulanan AKD ve kalite faktörü ile kurtarma bitlerini elde etmişlerdir. Oluşturulan bitleri niceleme indeks modülasyonu ile gizlemişlerdir. Görüntünün kurcalanıp kurcalanmadığını tespit etmek için ters AKD ile kalite faktörüne bağlı damga kontrolü yapmışlardır [14]. He ve arkadaşları dalgacık dönüşümü temelli bir damgalama metodu önermişlerdir. Bu metotta, dalgacık dönüşümü ve güvenlik anahtarı yardımı ile damga elde edilmiştir. Oluşan damga, görüntünün en anlamsız bitine eklenmiştir [15].

Literatürde bulunan çalışmaların çoğu blok tabanlıdır. Küçük boyutlu blok kullanan yöntemlerde damga görüntünün kalitesini düşürmektedir. Büyük blok boyutu kullanan yöntemler ise, kurcalanmamış bölgeleri saldırıya uğramış olarak algılayabilmektedir. Bu makalede, görüntü kimlik doğrulaması için AKD tabanlı trigonometrik fonksiyona kullanan yeni bir kendinden gömülü kırılgan damgalama metodu önerilmiştir. Bu metotta, kontrol bitlerini oluşturmak için; görüntü, örtüşmeyen 4×4 bloklara ayrılır. Bu bloğa AKD uygulanarak, DC bileşeni seçilir. Seçilen DC bileşen değeri, blok konum bilgisi ve güvenlik anahtarı kullanılarak trigonometrik fonksiyon yardımıyla kontrol bitleri oluşturulur. Kontrol bitleri bloğun, en az anlamsız bitlerine damga olarak eklenir. Görüntülere farklı saldırılar uygulanarak, yöntemin kurcalanan bölgelerin tespitindeki başarısı ortaya konulmuştur. Analiz sonuçları, önerilen metodun geometrik saldırılar, görüntü işleme saldırıları gibi bölgesel saldırıları tespit ettiğini gösterilmiştir.

Makalenin bu kısımdan sonraki organizasyonu şu şekildedir: Materyal ve metotlar Bölüm 2'de verilmiştir. Bölüm 3'te bulgular yapılan deneysel çalışmalarla desteklenmiştir. Bölüm 4'te ise makalenin genel değerlendirilmesi yapılmıştır.

2. Materyal ve Metot

Bu yöntemde, görüntü kimlik doğrulaması için yeni bir AKD tabanlı kendinden gömülü kırılgan damgalama yöntemi önerilmiştir. Orijinal gri seviyeli görüntü, 4×4 boyutunda örtüşmeyen bloklara bölünmüştür. 4×4 görüntü bloğunun kimlik doğrulama anahtarının elde edilmesi için AKD tabanlı blok özelliği ve güvenlik anahtarı kullanılmıştır. AKD verilerin uzaysal bölgeden frekans bölgesine blok tabanlı dönüşümünü sağlayan etkili yöntemlerden biridir. Görüntü bloğunun vektörünü yine aynı katsayı kümesine eşleyen doğrusal bir dönüşüm türüdür. Orijinal görüntü üzerine AKD uygulanması ile oluşan katsayı kümesi değerlerinden ilk değer olan DC bileşeni kullanılır. Blok anahtarı, AKD sonucunda elde ettiğimiz bu DC bileşen değerine, görüntü güvenlik anahtarına ve blok konum bilgisine bağlı oluşturduğumuz özel trigonometrik fonksiyon ile üretilir. Oluşturulan bu kimlik doğrulama anahtarı, her bir görüntü bloğunun en az anlamlı bitine gömülür.
Önerilen yöntem damga ekleme ve kurcalama tespiti olmak üzere iki aşamadan oluşmaktadır.

2.1. Damga Ekleme Yöntemi

Önerilen damga ekleme yönteminin akış şeması Şekil 1'de verilmiştir. Orijinal gri seviyeli görüntü, ilk aşamada 4×4 boyutunda birbiri ile örtüşmeyen bloklara bölünmektedir. Görüntü için damgayı oluşturmadan önce, blok piksel değerlerinin en az anlamlı bitleri sıfırlanır. Her bir bloğa AKD uygulanır ve elde edilen sonuçlardan hassasiyeti en yüksek değer olan DC bileşen değeri alınır. Blok kimlik doğrulama anahtarı; DC bileşen değeri $(G_n^{s,d}(1,1))$, güvenlik anahtarı (I_{key}) ve (i,j) blok konum bilgisi kullanılarak Denklem 1'e göre hesaplanır.

$$B_a^o(i,j) = Round\left(\left|\sin\left(i * G_n^{s,d}(1,1)\right) + \cos\left(j * G_n^{s,d}(1,1)\right)\right| \times I_{key}\right) \% \, 2^{16} \quad (1)$$

Oluşturulan kimlik doğrulama değeri ikili değere çevrilerek, bloktaki bulunan piksellerin en az anlamlı bitlerine eklenmektedir. Önerilen yöntemin damga ekleme adımları aşağıdaki gibidir:

1. BxB boyutundaki orijinal gri seviye görüntüyü, G^o, 4×4 boyutunda birbiriyle örtüşmeyen bloklara böl.
2. Görüntü bloğundaki piksellerinin en az anlamlı bitlerini(LSB) sıfırla ve $G^S(i,j)$'yi elde et.
3. 4×4 bloğa AKD uygula.

$$G_n^{s,d}(i,j) = AKD(G^S(i,j)) \quad (2)$$

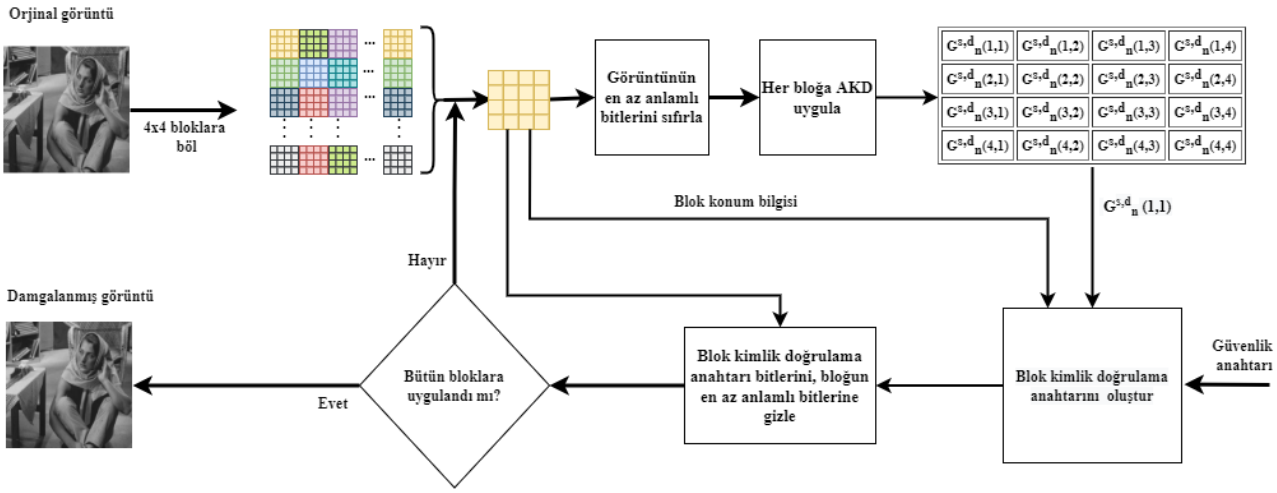
4. Blok konum bilgisi, güvenlik anahtarı ve DC bileşen değeri kullanılarak Denklem 1'e göre yeni bir blok anahtarı hesapla.
5. Blok anahtar değerini ikili sisteme çevir.

$$B_a^{o,b}(i,j) = Binary(B_a^o(i,j)) \quad (3)$$

6. Blok kimlik doğrulama bitlerini blok piksellerinin en az anlamlı bitlerine ekle.

$$G^w(i,j) = LSB(G^S(i,j) \oplus B_a^{o,b}(i,j) \quad (4)$$

7. Tüm bloklar için 2-6 arasındaki adımları tekrarla.
8. Damgalanmış görüntüyü elde et.



Şekil 1. Önerilen damga ekleme yönteminin akış şeması

2.2. Kurcalama Tespit Yöntemi

Şekil 2'de önerilen kurcalama tespit yönteminin akış şeması gösterilmektedir. Saldırıya uğramış görüntü 4×4 boyutunda birbiri ile örtüşmeyen bloklara bölünmektedir. Görüntünün içerisine eklenmiş olan damgayı çıkartmak için bloğun birinci en az anlamlı bitlerinden kimlik doğrulama değeri çıkarılır. Bu kimlik doğrulama değeri ile saldırıya uğramış görüntüden damga ekleme işlemine benzer bir şekilde oluşturulan kontrol damga değeri karşılaştırılır. Karşılaştırma sonucuna göre o bloğun kurcalanıp kurcalanmadığı ortaya çıkartılır.
Kurcalama tespiti için kullanılan adımlar aşağıdaki gibidir:

1. B×B boyutundaki orijinal gri seviye görüntüyü, S^o, 4×4 boyutunda birbiriyle örtüşmeyen bloklara böl.
2. Blok kimlik doğrulama bitlerini blok piksellerinin en az anlamlı bitinden çıkar.

$$K^{s,b}(i,j) = LSB(G^S(i,j)) \tag{5}$$

3. Görüntü bloğunun piksellerinin ilk en az anlamlı bitlerini sıfırla ve $S^S(i,j)$'yi elde et.
4. 4×4 bloğa AKD uygula.

$$S_n^{s,d}(i,j) = AKD(S^S(i,j)) \tag{6}$$

5. Blok konum bilgisi, güvenlik anahtarı ve DC bileşen değeri kullanılarak yeni bir blok anahtarı hesapla.

$$B_a^s(i,j) = Round\left(|\sin\left(i * S_n^{s,d}(1,1)\right) + \cos\left(j * S_n^{s,d}(1,1)\right)| \times I_{key}\right) \% \, 2^{16} \tag{7}$$

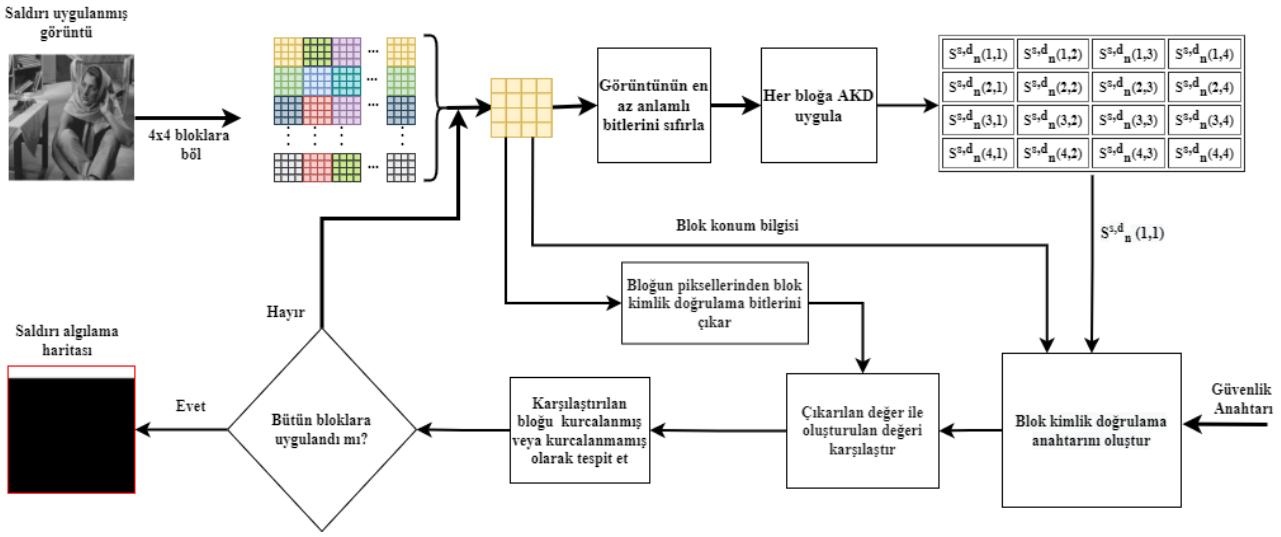
6. Blok anahtar değerini ikili sisteme çevir ve kontrol bitlerini oluştur.

$$B_a^{s,b}(i,j) = Binary(B_a^s(i,j)) \tag{8}$$

7. Blok kimlik doğrulama bitleri ile kontrol bitlerini karşılaştır:

$$K^{s,b}(i,j) =? \left(B_a^{s,b}(i,j)\right) \tag{9}$$

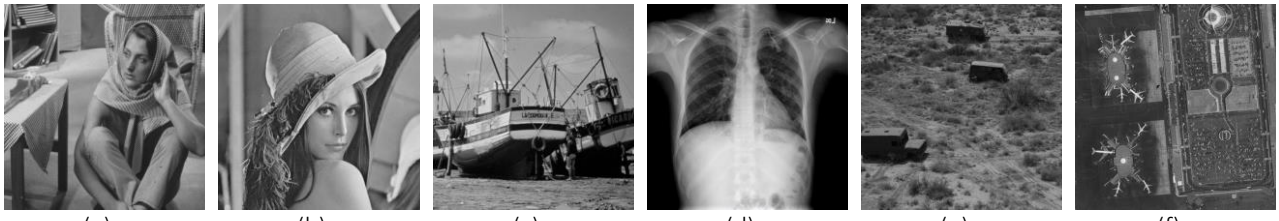
8. 4×4 blok için kurcalanmış veya kurcalanmamış olarak işaretle.
9. 2-8 adımları tüm 4×4 bloklar için uygula.



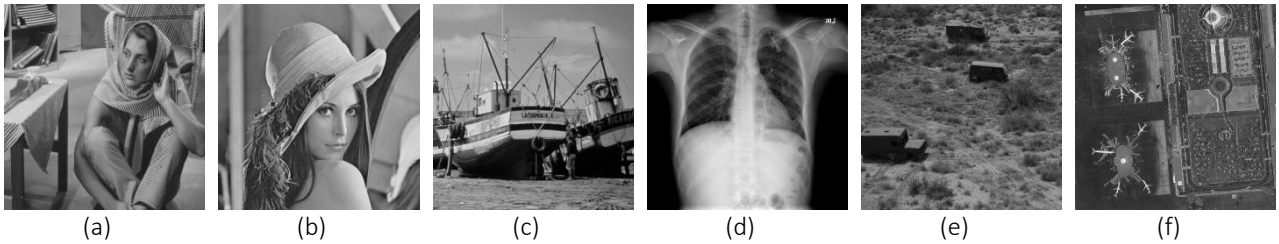
Şekil 2. Önerilen kurcalama tespit yönteminin akış şeması

3. Bulgular

Önerilen yöntemin başarımını değerlendirmek için deneysel çalışmalarda Şekil 3'de gösterilen gri seviyeli 512×512 boyutlarında "Barbara", "Lena", Boat", "X-Ray", "Truck" ve "Airport" görüntüleri kullanılmıştır. Önerilen yöntem kullanılarak damgalanmış olan bu görüntüler Şekil 4'de verilmiştir.



Şekil 3. Orijinal Görüntüler a) Barbara, b) Lena, c) Boat, d) X-ray, e) Truck, f) Airport



Şekil 4. Damgalanmış Görüntüler a) Barbara, b) Lena, c) Boat, d) X-ray, e) Truck, f) Airport

Damgalanmış görüntülerin kalitesinin korunduğu ve damganın algılanamazlığının sağlandığı Şekil 4 incelendiğinde anlaşılmaktadır. Deneysel sonuçlarda, damgalanmış görüntü ile orijinal görüntü arasındaki benzerliği ölçmek için Tepe Sinyal Gürültü Oranı (TSGO) ve Yapısal Benzerlik İndeksi (YBİ) değerleri kullanılmıştır. Genellikle orijinal görüntü ile damgalanmış görüntü arasındaki kalite değerini ölçmek için kullanılan TSGO aşağıdaki formül ile hesaplanır [16]:

$$TSGO(G^o, G^d) = 10log_{10}\left(\frac{255^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(G_{ij}^o - G_{ij}^d)}\right) \quad (10)$$

Burada M×N boyutundaki görüntü için G^o orijinal görüntüyü ve G^d damgalanmış görüntüyü ifade etmektedir. Ayrıca çalışmada diğer kalite ölçütü olarak YBİ kullanılmıştır. Wang ve arkadaşları tarafından geliştirilen ve insan görsel sistemi ile ilişkili olduğu düşünülen YBİ aşağıdaki formül ile hesaplanır [17]:

$$YBI(G^o, G^d) = \frac{(2\mu^{G^o}\mu^{G^d} + c_1)(2cov + c_2)}{((\mu^{G^o})^2 + (\mu^{G^d})^2 + c_1)((\sigma^{G^o})^2 + (\sigma^{G^d})^2 + c_2)} \tag{11}$$

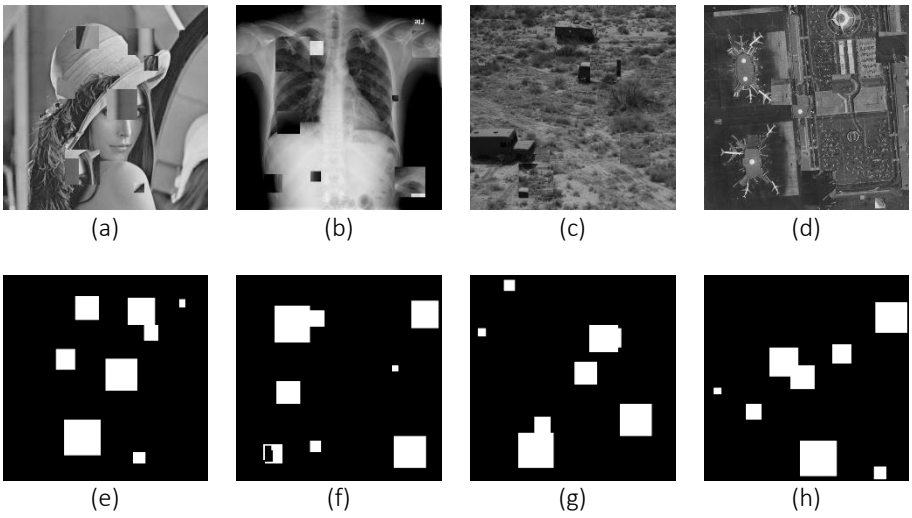
Burada G^o orijinal görüntüyü ve G^d damgalanmış görüntüyü, μ görüntülerin yerel ortalama değerlerini, σ standart sapma değerlerini, c_1 ve c_2 ise dengeleme için kullanılan değerleri göstermektedir. Yapılan çalışma sonucunda damgalanmış görüntülerin TSGO ve YBI değerleri Tablo 1' de verilmiştir.

Tablo 1. Damgalanmış görüntülerin TSGO ve YBI değerleri

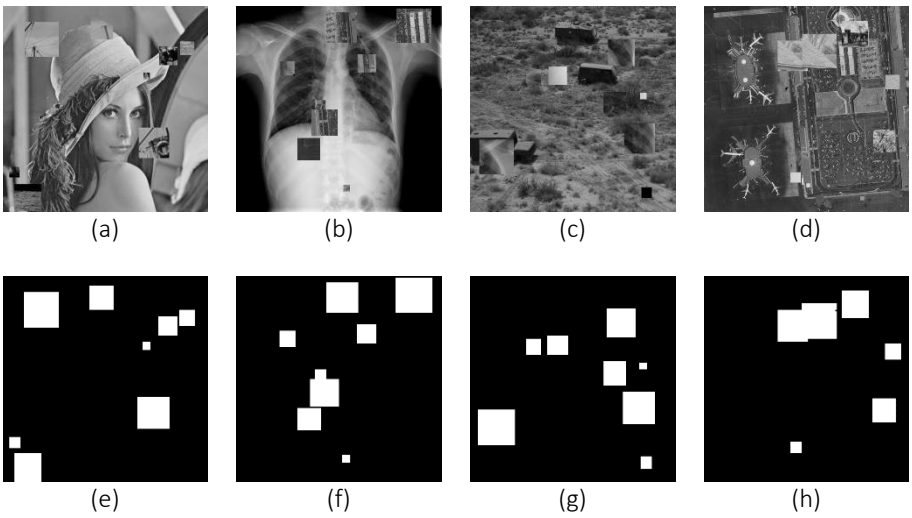
Görüntü	Barbara	Lena	Boat	X-ray	Truck	Airport
TSGO	51.2251	51.2427	51.2188	51.5710	51.2356	51.2304
YBI	0.9984	0.9978	0.9974	0.9940	0.9990	0.9986

TSGO ve YBI damgalanmış görüntülerin kalitesini ve damganın algılanamazlığını değerlendirmek için kullanılan objektif ölçütlerdir. Tablo 1'den görüntülerin TSGO ve YBI değerlerinin ortalamalarının sırasıyla 51.2872 ve 0.9975 olduğu görülmektedir. Sonuçlar, orijinal görüntüler ile damgalanmış görüntülerin birbirine kalite açısından yakın olduğunu göstermektedir. Kullanılan yöntemde her bir piksele eklenen veri olarak hesaplanan yük değeri 1bpp (piksel başına bit)'dir. Tablodaki sonuçlar incelendiğinde yöntemimizin damgalanmış görüntülerin kalitesini korunduğu ve damganın algılanamazlığını sağlandığı gözükmektedir.

Önerilen yöntemin saldırılara karşı başarımını değerlendirmek için damgalanmış görüntülere kopyala-taşı, ekleme ve metin ekleme gibi geometrik saldırılar ve keskinleştirme (1.0), ölçekleme ($2x \rightarrow x \rightarrow 2x$) ve tuz biber gürültüsü (0.1) gibi görüntü işleme saldırıları uygulanmıştır. Kopyala-taşı saldırıları görüntünün belirli bir bölgesinden seçilen alanın kopyalanarak görüntünün başka bir bölgesine taşınması olarak tanımlanır. Kopyala-taşı saldırısına uğramış görüntüler Şekil 5 (a-d)'de gösterilmektir. Saldırılar rastgele boyutlarda oluşturularak görüntüler üzerinde rastgele konumlara yapılmıştır. Önerilen kurcalama tespit yöntemi uygulandıktan sonra elde edilen sonuçlar Şekil 5 (e-h)'de gösterilmektedir. Şekilde tespit edilen saldırı yapılmış bölgeler beyaz olarak belirtilmiştir. Kopyala-taşı saldırısı sonuçlarına bakıldığında saldırıların net olarak tespit edildiği açıkça gözükmektedir. Ekleme saldırısı, diğer görüntülerden farklı boyutlarda görüntü alanlarının kopyalanarak damgalanmış görüntünün rastgele konumlarına yapıştırılması olarak tanımlanır. Ekleme saldırısı yapılmış görüntüler Şekil 6 (a-d)'de gösterilmektedir. Önerilen yöntem sonucunda elde edilen saldırı tespit haritaları Şekil 6 (e-h)'de gösterilmektedir.

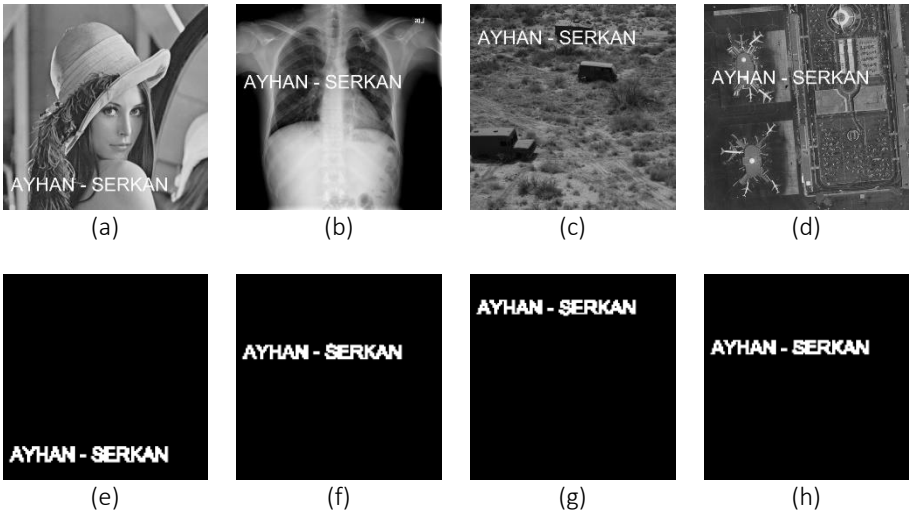


Şekil 5. Kopyala-taşı saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)



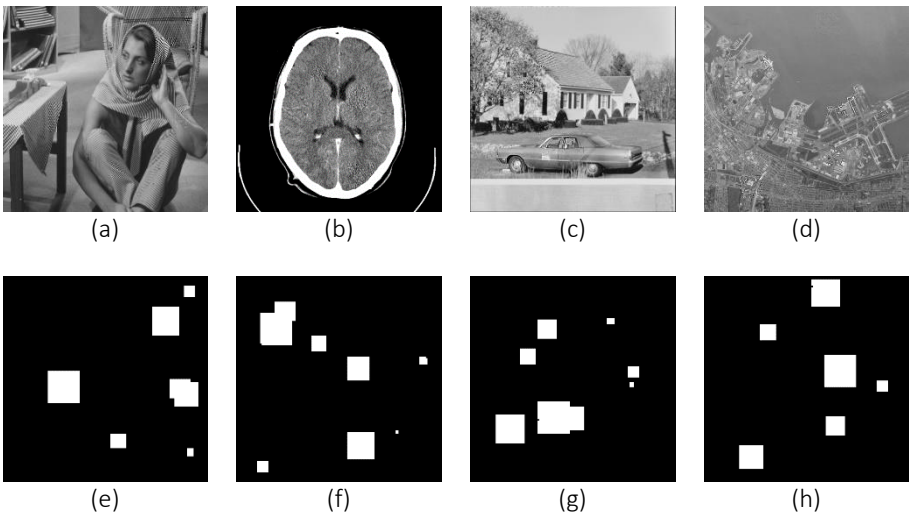
Şekil 6. Ekleme saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)

Ayrıca damgalanmış görüntüler üzerine Şekil 7 (a-d)'de gösterildiği gibi "AYHAN-SERKAN" metin ekleme saldırısı uygulanmıştır. Tespit edilen saldırı bölgeleri Şekil 7 (e-h)'de gösterilmektedir. Şekilden saldırı yapılan bölgelerin tam olarak tespit edildiği anlaşılmaktadır. Blok boyutunun 4x4 olmasından dolayı bir pikselde meydan gelen bozulmanın 4x4 boyutundaki bloğu etkilediği açıkça gözükmektedir.

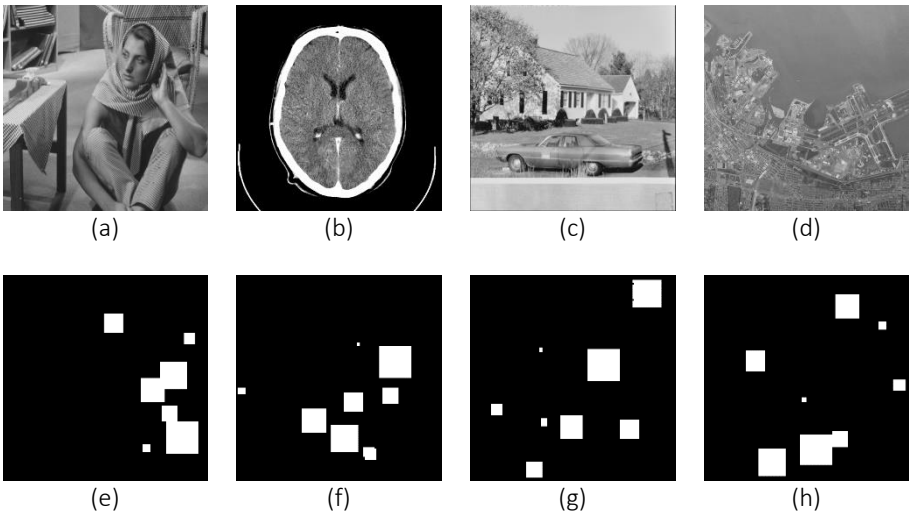


Şekil 7. Metin ekleme saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)

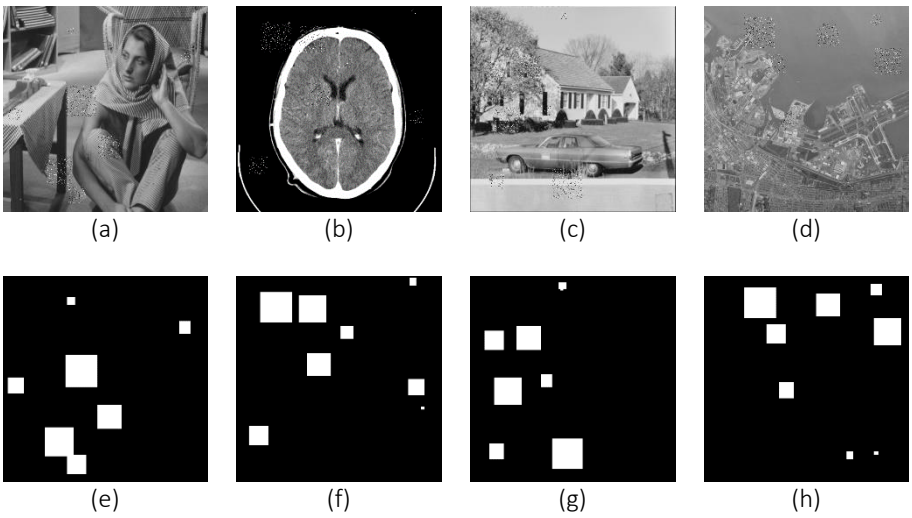
Damgalanmış "Barbara", "CT", "House" ve "San Francisco" görüntülerine yukarıda belirtilen görüntü işleme saldırıları uygulanmıştır. Bu saldırılar damgalanmış görüntüler üzerinde rastgele farklı bölgelere 10×10 ile 80×80 arasında rastgele boyutlarda uygulanmıştır. Şekil 8, 9, 10'da sırasıyla keskinleştirme, ölçekleme ve tuz biber saldırılarının uygulanmış görüntüleri ve önerilen metot sonucunda elde edilen saldırı bölgeleri gösterilmiştir. Önerdiğimiz yöntem ile kurcalanmış bölgelerin başarıyla tespit edildiği şekillerde açıkça gözükmektedir. Kurcalama tespit sonuçlarına bakıldığında sadece kurcalanmış bölgenin sınırları değil, saldırıların yapıldığı alanların tamamen belirlendiği anlaşılmaktadır.



Şekil 8. Keskinleştirme saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)



Şekil 9. Ölçekleme saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)



Şekil 10. Tuz biber saldırısı uygulanmış görüntüler (a)-(d), saldırı yapılmış bölgelerin haritası (e)-(h)

4. Tartışma ve Sonuç

Bu çalışmada, gri seviye görüntülerin bütünlüğünün korunması ve sahteciliğin tespiti için AKD tabanlı trigonometrik fonksiyon kullanan bir kendinden gömülü kırılgan damgalama yöntemi önerilmiştir. Bu yöntemde kimlik doğrulama anahtarı oluşturmak üzere görüntü 4×4 bloklara ayrılmıştır ve bu blokların en az anlamlı bitleri sıfırlanmıştır. Daha sonra bu bloklara AKD uygulanarak, DC bileşeni seçilmiştir. Seçilen değer, blok konum bilgisi ve güvenlik anahtarı kullanılarak, yeni bir AKD tabanlı trigonometrik formül ile kimlik doğrulama anahtarı meydana getirilmiştir. Üretilen bu kimlik doğrulama anahtarı görüntünün en az anlamlı bitlerine damga olarak saklanmıştır.
Önerilen yöntemin başarımını değerlendirmek için damgalanmış görüntüler üzerine farklı saldırılar uygulanmış ve saldırıya uğrayan bölgeler analiz edilmiştir. Deneysel sonuçlar, önerilen yöntem ile damgalanmış görüntülerin kalitesinin korunduğu ve damganın algılanamazlığının sağlandığını göstermektedir. Ayrıca, geometrik saldırılar, görüntü işleme saldırıları gibi farklı saldırı gruplarının neden olduğu yetkisiz görüntü ataklarını önerilen yöntemin tespit ettiği anlaşılmaktadır. Çalışmamızın en önemli katkısı, AKD ve trigonometrik fonksiyon kullanan yeni bir kendinden gömülü kırılgan damgalama yönteminin önerilmesidir.
Gelecekte, güçlü algılama başarımı sağlayacak ve damgalanmış görüntünün kalitesini en üst seviye çıkaracak kırılgan bir damgalama yöntemi için önerdiğimiz yöntemi geliştirmeyi çalışacağız. Blok tabanlı tekniklerin blok boyutundan kaynaklanan dezavantajlarını azaltmak için kurcalanmış alanı piksel ölçeğinde saptamak üzere piksel tabanlı yöntemlerin geliştirilmesi amaçlanmaktadır. Ayrıca, derin öğrenme ve yapay zekâ gibi modern ileri teknikler kullanılarak yeni yaklaşımlar ortaya konulması düşünülmektedir.

Kaynakça

[1] Sreenivas, K., Kamkshi Prasad, V. 2018. Fragile watermarking schemes for image authentication: a survey. Int. J. Mach. Learn. & Cyber. 9, (2018), 1193–1218. https://doi.org/10.1007/s13042-017-0641-4.

[2] Rathi, S.C. and Inamdar, V.S. 2012. Medical images authentication through watermarking preserving ROI, Health Informatics-An International Journal (HIIJ), (2012), 1,1.

[3] Ali, M., Ahn, C.W., and Pant, M. 2018. An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms, Multimedia Tools and Applications, 77(10),(2018),11751–11773.

[4] Walton, S. 1995. Information authentication for a slippery new age, Dr Dobb's J, 20(4),(1995),18–26.

[5] Chen, W.C., Wang, M.S. 2009. A fuzzy c-means clustering-based fragile watermarking scheme for image authentication, Expert Systems with Applications, 36(2),(2009),1300–1307.

[6] Trivedy, S., Pal AK. 2017. A logistic map-based fragile watermarking scheme of digital images with tamper detection, Iran J Sci Technol Trans Electric Eng, 41,(2017),103–113

[7] Gul, E., Ozturk, S. 2019. A novel hash function based fragile watermarking method for image integrity. Multimed Tools Appl, (2019), 78:1–18

[8] Neena Raj, NR., Shreelekshmi, R. 2019 Security analysis of hash based fragile watermarking scheme for image integrity. In: 2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT), vol 1. IEEE, (2019), 651–654.

[9] Renklier, A., Öztürk, S. 2022. A novel Frei-Chen based fragile watermarking method for authentication of an image. Concurrency and Computation: Practice and Experience, e6897.

[10] Qin, C., Chang, C-C., Chen, P-Y. 2012. Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism, Signal Process, 92,(2012),1137–1150.

[11] Li, C., Zhang, A., Liu, Z., Liao, L., Huang, D. 2015. Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication, Multimed Tools Appl 74,(2015),10581–10604.

[12] Yeh, FH., Lee, GC. 2006. Content-based watermarking in image authentication allowing remedying of tampered images. Opt Eng 45,7(2006),0770041–10.

[13] Zhang, X., Xiao, Y., Zhao, Z. 2014. Self-embedding fragile watermarking based on DCT and fast fractal coding. Multimed Tools Appl. ,(2014),doi:10.1007/s11042-014-1882-9.

[14] Pred, RO., Vizireanu, DN. 2015. Watermarking-based image authentication robust to JPEG compression. Electr Lett ,51,(2015),1873–1875.

[15] He, H., Zhang, J., Tai H-M. 2006. A wavelet-based fragile watermarking scheme for secure image authentication, IWDW 2006, LNCS 4283, 422–432.

[16] Horé, A., Ziou, D.2010. Image Quality Metrics: PSNR vs. SSIM,2010 20th International Conference on Pattern Recognition, (2010), 2366-2369.

[17] Wang, Z., Bovik, A. C, Sheikh, H. R., Simoncelli E. P.2004. Image quality assessment: from error visibility to structural similarity, IEEE Transactions on Image Processing, vol. 13, 4,(2004), 600-612.