



## **Sayısal Görüntülerin Telif Hakkının Korunması İçin İris Tabanlı Biyometrik Damgalama Yaklaşımı**

### **Iris-Based Biometric Watermarking Approach for Copyright Protection of Digital Images**

**Şeyma Yücel Altay<sup>1\*</sup>**, **Güzin Ulutaş<sup>2</sup>**

<sup>1</sup> Atatürk Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Erzurum, TÜRKİYE

<sup>2</sup> Karadeniz Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Trabzon, TÜRKİYE

Sorumlu Yazar / Corresponding Author \*: seyma.yucel@atauni.edu.tr

Geliş Tarihi / Received: 29.07.2020

Araştırma Makalesi/Research Article

Kabul Tarihi / Accepted: 27.11.2020

DOI:10.21205/deufmd.2021236816

Atıf şekli/How to cite: ALTAY Ş.Y., ULUTAŞ G. (2021). Sayısal Görüntülerin Telif Hakkının Korunması İçin İris Tabanlı Biyometrik Damgalama Yaklaşımı. DEÜFMD 23(68), 531-546.

#### **Öz**

Modern teknolojik gelişmeler, görüntü, ses, video ve metin gibi multimedya verilerinin yasadışı kopyalarının üretilmesini çok kolay hale getirmiştir. Sayısal damgalama teknikleri, telif hakkı korumalı veri dosyalarının yasadışı kullanımını önlemek amacıyla telif hakkı bilgilerinin korunacak ortama sayısal olarak gömülmesini amaçlar. Bu çalışmada, biyometrik verilerle sayısal görüntünün damgalanması yöntemi ele alınmıştır. Geleneksel damga yerine biyometrik özelliklerin kullanımı damgalama şemasının güvenliğini artırır. Bu çalışmada daha güvenli olması ve kopyalanmasının daha zor olması sebebiyle iris biyometrik verisi tercih edilmiştir. Kişinin göz görüntüsünden üretilen iris şablonu ayrık kosinüs dönüşümü ile ikili koda dönüştürülür. Bu ikili kod, orijinal görüntüye yeniden dağıtılmış değişmez ayrık dalgacık dönüşümü ve Schur ayrıştırma yardımıyla gömülür. İkili kodun gömülmesi için kullanılan bloklar standart sapma değerlerine bağlı olarak seçilir. Deneysel sonuçlar önerilen yöntemin algısal kalitesinin yüksek olduğunu ortaya koymuştur. Ayrıca farklı görüntü işleme atakları ve geometrik ataklar karşısında dayanıklılığı oldukça yüksek bulunmuştur.

**Anahtar Kelimeler:** Biyometrik Damgalama, Yeniden Dağıtılmış Değişmez Ayrık Dalgacık Dönüşümü, Schur Ayrıştırma, Dayanıklılık

#### **Abstract**

Modern technological advances has made it very easy to produce illegal copies of multimedia data such as image, audio, video, or text. Digital watermarking techniques aim to digitally embed copyright information into the media to be protected in an attempt to prevent illegal use of copyright protected data files. In this study, the method of digital image watermarking with biometric data is discussed. The use of biometric features instead of traditional watermarks increases the security of the watermarking scheme. Iris biometric data is preferred in this study because it is more secured and more difficult to copy. The iris template produced from the eye image of the person is converted into binary code via discrete cosine transform. This binary code is embedded into the cover image with the help of the redistributed invariant discrete wavelet transform and Schur decomposition. The blocks used for embedding binary code are selected based on their standard deviation values. Experimental results revealed that the perceptual quality of the proposed method is high. In addition,

it is found to be highly robust against different types of image processing attacks as well as geometrical attacks.

**Keywords:** *Biometric Watermarking, Redistributed Invariant Discrete Wavelet Transform, Schur Decomposition, Robustness*

## 1. Giriş

Son yıllarda sayısal verileri çoğaltmak ve değiştirmek için kullanılabilen gelişmiş kopyalama/çoğaltma araçlarının kullanımı oldukça yaygınlaşmıştır. Görüntü, ses, video ve metin gibi çoklu ortam verilerinin kalite kaybı olmadan sayısız kopya edilmesi ve internet üzerinden kolayca dağıtılması telif haklarının korunması ile ilgili endişeleri de beraberinde getirmektedir. Bu noktada, kriptografi ve diğer alternatiflerle birlikte, sayısal damgalama, bunu başarmanın popüler yollarından biri olarak devreye girmektedir. Sayısal damgalama, telif hakkı sahipliğini kanıtlamak için bir taşıyıcı (orijinal) sinyale görünmez bir sayısal model yerleştirmeyi hedefler. Sayısal damgalama metodlarında damga ya bir sözde rasgele sayı dizisinden ya da kaotik dizi veya ikili görüntülerden (logo) oluşur. Bu durumda sayısal damganın aidiyetini kanıtlamak zor olacaktır. Bu göz önüne alındığında aidiyeti kanıtlamak için damganın daha güvenli bir şekilde tanınması gerekmektedir. Bu sebeple, yetkili ve yetkisiz kullanıcılar arasında ayırım yapabilme kabiliyeti nedeniyle bir kullanıcının benzersiz, ölçülebilir fizyolojik ve davranışsal özelliklerini kullanan biyometrik tabanlı güvenlik şemaları, geleneksel telif hakkı koruma ve kimlik doğrulama şemalarına sağlam bir alternatif oluşturmaktadır [1].

İris tanıma en güvenli biyometrik teknolojilerden biridir. Yüz tanıma, ses tanıma ve el geometrisi elverişsiz olmamasına rağmen, bu biyometrik yöntemlerin tümü iris tanıma ile karşılaştırıldığında nispeten güvenilmezlerdir. Ayrıca parmak izi ile karşılaştırıldığında da iris tarama daha güvenlidir [2]. Parmak izi tarayıcıları oldukça yaygındır ve iris tarayıcılara göre nispeten daha ucuzdur, ancak parmak izi sahteciliğine kıyasla, irisi oluşturan desenlerin kopyalanması daha zordur. [2]'ye göre iki irisin tamamen aynı olacağına dair istatistiksel olasılık 1072'de 1 olarak tahmin edilmektedir, bu nedenle bu çalışmada aidiyeti kanıtlamak için göz görüntülerinden çıkarılan iris kodu damga olarak kullanılmış ve doğal görüntülere gizlenmiştir.

Görüntü damgalama şemaları, damga çıkarma aşamasında orijinal görüntüye ihtiyaç duyulup, duyulmamasına bağlı olarak 3 sınıfa ayrılır. Bunlar kör olmayan (non-blind), yarı kör (semi-blind) ve kör (blind) damgalama sistemleridir. **Kör olmayan damgalamada** orijinal görüntü damga çıkarma aşamasında gerekliken, **kör damgalamada** damganın çıkarılması orijinal görüntünün mevcut olup olmamasına bağlı değildir. Kör olmayan damgalama sistemleri, tespit sırasında orijinal görüntünün kullanılabilirliği nedeniyle kör damgalama sistemlerinden daha dayanıklıdır, ancak bazı uygulamalarda işe yaramaz hale gelebildiği için uygulama alanı sınırlıdır [3, 4]. **Yarı kör damgalama teknikleri** ise damga çıkarma adımıyla orijinal görüntüyü gerektirmezler, ancak orijinal görüntünün bazı özelliklerine ihtiyaç duyarlar [5]. Kör damgalama sistemleri, damganın tespitinde ne orijinal görüntüyü ne de damganın kendisini gerektirdiğinden daha popüler bir tekniktir. Ayrıca kör damgalama, orijinal görüntülerin depolanması için gerekli maliyet ve bellek yükünü azaltır [3] ve yarı kör ve kör olmayan damgalama sistemlerine kıyasla daha güvenlidir [5].

Sayısal görüntü damgalama teknikleri, damgalamanın gerçekleştiği alana bağlı olarak uzaysal alan (spatial domain) ve dönüşüm alanı (transform domain) teknikleri olmak üzere iki ayrı sınıfta incelenebilir. **Uzaysal alan teknikleri**, orijinal görüntüye doğrudan damga eklemek için tasarlanmıştır. Uzaysal alanda damgalamada, damga, orijinal görüntünün görünüşünde belirgin bir bozulmaya neden olmayacak şekilde direk olarak seçili pikseli değiştirerek gömülür. Bu teknikler dönüşüm alanındaki algoritmalara göre daha az karmaşık olsa da, farklı sinyal işleme saldırılarına (gürültü, filtreleme, sıkıştırma gibi) ve geometrik ataklara (dönme gibi) karşı zayıftır. Bunlar arasında en yaygın kullanılan teknik En Anlamsız Bit (Least Significant Bit) tekniğidir. **Dönüşüm alanı teknikleri**, algısal özelliklerden yararlanmak için, orijinal görüntülerin dönüşüm alanına bir damga yerleştirmeyi hedeflemiştir. Bu tür damga düzenleme şemaları, JPEG sıkıştırma, filtreleme ve gürültü ilavesi gibi en yaygın sinyal

işleme manipülasyonlarına karşı iyi bir dayanıklılık performansına sahiptir. Ayrık Fourier Dönüşümü (AFD) (Discrete Fourier Transform), Ayrık Kosinüs Dönüşümü (AKD) (Discrete Cosine Transform), Ayrık Dalgacık Dönüşümü (ADD) (Discrete Wavelet Transform) en yaygın kullanılan dönüşüm alanı tekniklerindedir.

Sayısal damgalamanın temel iki gereksinimi algılanamazlık ve dayanıklılıktır. Algılanamazlık, yalnızca telif hakkı koruma uygulamalarında değil, tüm görünmez damgalama uygulamalarında önemli olan bir gereksinimdir. Uygulamada, algılanamazlık şartı, damgalanmış görüntülerin algısal kalitesinin yüksek tutulması gerektiği anlamına gelir. Taşıyıcı görüntünün orijinali ile damgalanmış hali arasındaki görsel benzerlik ve orijinal sinyalin algısal kalitesi, damganın yerleştirilmesiyle fark edilmeden dönüştürülmelidir. En yaygın olarak ölçülen özelliklerden bir diğeri ise, sayısal damgalama sistemlerinin, döndürme, ölçekleme, görüntü çevirme gibi çeşitli saldırılara ve JPEG sıkıştırma, filtreleme, gürültü ekleme gibi yaygın sinyal işleme işlemlerine makul derecede dayanıklı olması gerektiğidir [6].

Dayanıklı sayısal damgalama şeması iyi algısal şeffaflığa sahip olmakla birlikte, sinyal işleme saldırılarına karşı sağlam olmalıdır. Bu parametreler söz konusu olduğunda son zamanlarda, dönüşüm alanı tekniklerinden dalgacık tabanlı (wavelet-based) damgalama şemaları daha fazla dikkat çekmeye başlamıştır. Dalgacık dönüşümü, tersinir, kayıpsız bir dönüşüm tekniğidir. Bir sinyali yansıtmak için dalgacık adı verilen sınırlı süreli ve değişken frekanslarda küçük dalgalar kullanır. İki boyutlu ADD, görüntüleri çok ölçekli bir çerçevede analiz etmek ve hem uzay hem de frekans alanlarında yerleştirilmiş görüntü ayrıntılarını yakalamak için etkili bir araçtır. Dalgacık alanına damga yerleştirmenin nedenlerinden biri, iyi uzaysal-frekans lokalizasyonu (spatial-frequency localization) özelliğidir [7]. Çok ölçekli temsiller olarak da bilinen uzaysal-frekans görüntü dönüşümleri, bir görüntüyü, görüntü ayrıntılarını ve yapılarını birden çok ölçekte ve birden çok yönde gösteren bir dizi alt görüntüye ayırır. Her alt görüntü, bir frekans alt bandına yani görüntü spektrumunun yerleştirilmiş bir bölümüne karşılık gelir. Bunun dışında, üstün insan görsel sistemi (Human Visual System) modellemesi ve düşük hesaplama maliyetine

sahip olmasından dolayı da dalgacık tabanlı yaklaşımlar öne çıkmıştır [7].

Literatürde ADD tabanlı farklı yöntemler önerilmiştir. [8]'de Kaldıran Dalgacık Dönüşümüne dayalı bir kör yöntem önerilmiştir. Burada düşük frekanslı alt banda gömme yapıldığı için yöntemin algısal kalitesi çok yüksek değildir; ancak dayanıklılığı yüksektir. Bir başka Kaldıran Dalgacık Dönüşümüne dayalı yöntemde, düşük frekanslı katsayılarla birlikte regresyon ağacı damga gömmek için kullanılır [9]. Çalışmanın dezavantajı, döndürme ve gürültü ataklarına karşı dayanıklılığının düşük olmasıdır. ADD alanında yapılan bir başka çalışma [10], damgalama için AKD ve Tekil Değer Ayrıştırmanın (TDA) (Singular Value Decomposition) birleşiminden yararlanmıştır. Bu çalışma yaygın sinyal işleme ataklarına karşı güçlü bir performans sergilemiştir.

Pratikte, bir damga dalgacık alanına gömülecekse, aralarından seçim yapabilecek birçok dalgacık tabanı vardır. Bazı araştırmacılar Haar dalgacığının görüntü damgalama için uygun olduğunu bulmuşlardır [11]. Bu nedenle Haar dalgacık dönüşümüne dayalı, aynı zamanda geometrik ataklara da nispeten dayanıklı bir yöntem olan Yeniden Dağıtılmış Değişmez Ayrık Dalgacık Dönüşümünden (YDDADD) (Redistributed Invariant Discrete Wavelet Transform) bu çalışmada yararlanılmıştır.

Bu yöntemde damgalama yapmak için YDDADD ile birlikte kullanılan bir dönüşüm alanı tekniği ise Schur ayrıştırmasıdır. YDDADD ile alt bantlarına ayrılan görüntünün düşük frekanslı alt bandı (LL bant) öncelikle bloklara ayrılır. Düşük frekanslı alt banttaki her bir bloğun yapısından dolayı damgalama başarısına farklı etkisi vardır. Bu bloklar arasından en uygun olanlar standart sapma değerlerine bağlı olarak seçilir. Seçilen bloklara Schur ayrıştırma uygulanır. Schur ayrıştırma sonucu elde edilen birimsel matrisin birinci sütun vektörü üzerindeki elemanlar arasındaki korelasyon bu çalışmada yeni bir yaklaşımla ele alınarak damganın gömülmesinde kullanılmıştır.

Çalışmanın geri kalanı şu şekilde düzenlenmiştir: Bölüm 2'de ilişkili çalışmalar anlatılmıştır. Bölüm 3'de kullanılan teorik kavramlar açıklanmış ve önerilen sistem tanımlanmıştır. Bölüm 4'te araştırma bulgularına değinilirken, Bölüm 5'te tartışma ve sonuca yer verilmiştir.

## 2. İlişkili Çalışmalar

Literatürde biyometrik damgalama için birçok yöntem önerilmiştir. Bu yöntemler, konuşma sinyali, imza, parmak izi, yüz, el geometrisi ve iris gibi çeşitli özellikleri kullanmışlardır. Biyometrik damgalama yöntemlerinden bazılarında tek bir biyometrik özellik kullanılarak damgalama yapılırken, bazıları birden fazla biyometrik özelliği kullanarak (çok modellenli) damgalama yapmışlardır.

Sadece iris verisinin kullanıldığı bir çalışmada, göz görüntüsünden çıkarılan iris kodunu doğal görüntülere gömmek için Haar Dalgacık Dönüşümü kullanılmıştır [12]. İris biyometrik verisi kullanan bir başka yöntemde iris şablonunun AKD sonucu elde edilen DC değeri ikili koda çevrilir [13]. Ardından örten görüntüye ADD ve TDA yöntemi uygulanır ve ikili damga örten görüntünün tekil değerlerine gömülür. Çalışmada kör olmayan damgalama yöntemi kullanıldığı için, şemanın algısal kalitesi yüksektir, ancak dayanıklılığı test edilmemiştir. Bir başka iris tabanlı çalışmada göz görüntüsünden AKD yardımıyla elde edilen ikili iris kodu, AKD-TDA tabanlı yöntemle orijinal görüntüye gömülür [14]. Bu çalışma algısal kalite ya da dayanıklılık sonuçlarını rapor etmemiştir. [15]'te yazarlar, iris kodunu orijinal görüntüye uzaysal alanda gömen bir yöntem önermişlerdir. Burada En Anlamsız Bit tekniğiyle damga gizlenmiştir. Damga uzaysal alanda gömüldüğü için algısal kalitesi yüksektir, ancak sadece tuz ve biber gürültüsü, Gaussian filtreleme ve kırpmaya karşı dayanıklılık sonuçları verilmiştir.

Çok modellenli biyometrik damgalama şemalarından birinde, parmak izi ve iristen çıkarılan öznitelikler, kör olmayan damgalama yöntemiyle doğal görüntünün AKD katsayılarına gömülür [16]. Çalışmanın özellikle filtreleme ataklarına karşı dayanıklılık performansı düşük çıkmıştır. İris ve yüz görüntülerinin kullanıldığı bir biyometrik damgalama şemasında, artımlı ADD ve TDA tabanlı bir yöntem önerilmiştir [17]. Parmak izi ve iris görüntüsünün kullanıldığı bir başka çalışmada [1], damga Bağımsız Bileşenler Analizi (BBA) ile gömülmüştür. Burada parmak izi ve iris BBA ile ayrıştırılan görüntünün farklı bileşenlerine gömülmüştür. Parmak izi ve iris görüntüsünün damga olarak kullanıldığı bir başka çalışmada taşıyıcı görüntü olarak yüz görüntüsü kullanılmıştır [18]. Parmak izi ve iris görüntüsü şifrelenerek yüz görüntüsüne Slantlet

dönüşümü ve TDA yardımıyla gömülür. Çalışma, gürültü ataklarına karşı çok güçlü olmasa da filtreleme ataklarına karşı dayanıklıdır.

## 3. Materyal ve Metot

### 3.1. Yeniden dağıtılmış değişmez ayrık dalgacık dönüşümü

Bir damgalama sisteminin başarılı olabilmesi için çeşitli olası saldırılara karşı dayanıklı olması gerekir. Genelde damgalama sistemine karşı ataklar, ortak görüntü işleme işlemleri ve geometrik bozulmalar olarak sınıflandırılabilir. Her ne kadar ADD'ye dayalı mevcut damgalama şemalarının ortak görüntü işlemeye karşı etkili olduğu gösterilmiş olsa da, geometrik bozulmalarla karşı karşıya kaldığında hala yetersizdir [7]. Bunun nedeni, ADD katsayılarının geometrik dönüşümler altında değişmez olmamasıdır. Görüntü damgalama tekniklerinde ADD'nin yaygın kullanımı göz önüne alındığında, dalgacık tabanlı görüntü damgalama şemalarının geometrik bozulmalara karşı sağlamlığını artırmanın yollarını belirlemek yararlı olacaktır. Bu çalışmada, [7] tarafından önerilen ve damgalamanın geometrik bozulmalara dayanıklı alanda yapıldığı YDDADD'den yararlanılmıştır. YDDADD görüntünün piksellerinin konumlarını değiştiren ancak değerlerini değiştirmeyen 90°'nin katları ve görüntü çevirme gibi bazı geometrik bozulmalara karşı dayanıklıdır.

Bir  $M \times N$  boyutlu  $I$  görüntüsü için 90° ve katları döndürme ve görüntü çevirmede değişmezlik elde etmek amacıyla, aşağıda bahsedilen bir takım süreçlere uygulanır [7].

Orijinal görüntü dört ( $2 \times 2$ ), eşit boyutlu alt görüntüye bölünür ve ortalama yoğunluk matrisi şu şekilde hesaplanır:

$$mean = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, a, b, c, d \geq 0 \quad (1)$$

Normalizasyon matrisi  $S$  ortalama yoğunluk matrisine bağlı olarak şu şekilde elde edilir:

$$S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} = \begin{pmatrix} a + b + c + d & a + b - c - d \\ a - b + c - d & a - b - c + d \end{pmatrix} \quad (2)$$

Burada  $S_{11}$ ,  $S_{12}$ ,  $S_{21}$  ve  $S_{22}$ 'nin hiç birinin 0'a eşit olmadığını ve  $|S_{21}| \neq |S_{12}|$  koşulunun sağlandığını varsayıyoruz ki; doğal görüntülerde

bu zaten sağlanır. Burada belirtilen  $|\cdot|$ , mutlak değeri ifade etmektedir.

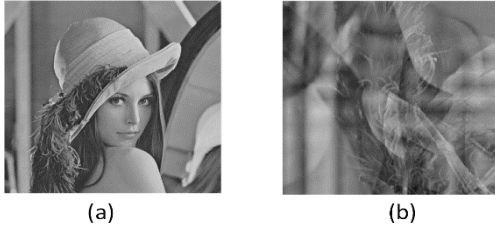
Normalizasyon matrisinin işaret matrisi şu şekilde hesaplanır:

$$Sign = \begin{pmatrix} Sg_{11} & Sg_{12} \\ Sg_{21} & Sg_{22} \end{pmatrix}, Sg_{ij} \in \{-1, +1\} \quad (3)$$

Görüntü yeniden dağıtılır. Yeniden dağıtılmış görüntü  $NI$  Denklem 4 ile elde edilir. Şekil 1’de standart gri seviye “Lena” görüntüsü ve bu görüntünün yeniden dağıtılmış sürümü görülmektedir.

$$\begin{aligned} NI(2i-1, 2j-1) &= I(i, j), 1 \leq i \leq M/2, 1 \leq j \leq N/2 \\ NI(2i-1, 2j-N) &= I(i, 3N/2-j+1), 1 \leq i \leq M/2, N/2 < j \leq N \\ NI(2i-M, 2j-1) &= I(3M/2-i+1, j), M/2 < i \leq M, 1 \leq j \leq N/2 \\ NI(2i-M, 2j-N) &= I(3M/2-i+1, 3N/2-j+1), M/2 < i \leq M, N/2 < j \leq N \end{aligned} \quad (4)$$

Yeni görüntü  $NI$  1 seviyeli Haar dalgacık dönüşümü ile Şekil 2’deki gibi alt bantlarına ayrılır.



Şekil 1. (a) Orijinal “Lena” görüntüsü, (b) Yeniden dağıtılmış “Lena” görüntüsü

Bu alt bantlar düşük frekans katsayılarını içeren LL bant, yatay detayları içeren HL bant, dikey detayları içeren LH bant ve köşegen detayları içeren HH banttır. Dönüştürülen alt bant işaret matrisiyle çarpılır ve  $B$  matrisi elde edilir.

$$\begin{aligned} B &= \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \\ &= \begin{pmatrix} Sg_{11} \times A_{11} & Sg_{12} \times A_{12} \\ Sg_{21} \times A_{21} & Sg_{22} \times A_{22} \end{pmatrix} \end{aligned} \quad (5)$$

Eğer  $|S_{21}| < |S_{12}|$  ise  $B$  matrisi şu şekilde güncellenir:



Şekil 2. Yeniden dağıtılmış görüntünün 1 seviye ayrıştırılmış matrisi [7]

$$B = \begin{pmatrix} B_{11}^T & B_{21}^T \\ B_{12}^T & B_{22}^T \end{pmatrix} \quad (6)$$

Burada  $B_{ij}^T, B_{ij}$  matrisinin devrik matrisini ifade eder.  $B$ , değişmez dalgacık alanıdır.

### 3.2. Schur ayrıştırma

Schur ayrıştırma sayısal lineer cebirde önemli bir araçtır. Gerçek bir  $A$  matrisi, Denklem 7’deki gibi Schur ayrıştırma ile  $U$  ve  $V$  matrislerine ayrıştırılabilir [19].

$$[U, V] = schur(A) \quad (7)$$

Burada  $U$ , birimsel (üniter) matristir. Yani, sütunları (ve satırları) ortonormal olan karmaşık bir kare matristir ve tersi, eşlenik devriğine (conjugate transpose) eşittir. Eğer  $A$  matrisinin girişlerinin tümü gerçek sayı ise  $U$  matrisin ortogonal olduğu söylenebilir.  $V$  ise, diyagonal elemanları gerçek öz değerlere sahip bir üst üçgen matristir. Denklemde yer alan  $schur(\cdot)$  ifadesi Schur ayrıştırma fonksiyonunu temsil eder. Ayrıştırılmış matrislerden orijinal  $A$  matrisi Denklem 8 ile yeniden elde edilebilir.

$$A = U \times V \times U^T \quad (8)$$

$U^T$  birimsel  $U$  matrisinin eşlenik devriğini belirtir. Schur, matematikte matris üstel değerlerini hesaplamak için kullanılır, çünkü Schur ayrıştırmadaki birimsel matris, hesaplama matrisi işlevlerini daha kolay ve daha az karmaşık hale getirir. Bunun yanı sıra, Schur ayrıştırma, simetrik olmayan matrisleri öz değerlerine ayrıştırma probleminde de kullanılır [20]. Tüm matrisler gerçek simetrik matrisler gibi köşegenleştirilemez. Ancak, Schur ayrıştırma simetrik olmayan matrislerin köşegenleştirilebilmesi için iyi bir alternatiftir. Schur ayrıştırma, TDA’da önemli bir ara adımdır [21] ve TDA’da gerekli olan hesaplamalardan çok daha az sayıda hesaplama gerektirir.

$U$  matrisinin birinci sütun vektörü ( $U_1$ ) elemanları arasında güçlü bir ilişki vardır.  $U_1$ ’in tüm elemanlarının işaretleri aynıdır ve değerleri birbirlerine çok yakındır.  $U$  matrisinin ilk sütununun bu özelliği damga bitlerinin yerleşimi için onu cazip hale getirmiştir [19]. Bu nedenle iris damga verilerinin gizlenmesi için bu alan tercih edilmiştir.

### 3.3. İris görüntüsünden ikili damganın elde edilmesi

İris verilerini damga olarak kullanmak için Bath Üniversitesinden elde edilen göz görüntülerine ait veri tabanından yararlanılır [22, 23]. 40 farklı göz ve her bir göze ait 10 ayrı görüntü ele alındığından 400 farklı görüntüden elde edilen iris kodları deneylerde kullanılmıştır.

Herhangi bir göz görüntüsünde, irisin yanı sıra göz bebeği, sklera ve göz kapağı da yer almaktadır. İris kodunu elde etmeden önce bu olumsuz faktörlerin göz görüntüsünden çıkarılması için görüntü normalleştirilmelidir. Bu faktörleri ortadan kaldırmak için göz görüntüsüne minimum sınırlı izotetik dikdörtgen (MBIR) formatı uygulanır. Böylece, Şekil 3'te görüldüğü gibi MBIR formatında  $120 \times 200$  piksel boyutuna normalize edilmiş dikdörtgen iris şablonları elde edilir [2, 24]. Normalize edilmiş  $120 \times 200$  boyutlu iris görüntüsüne,  $1 \times 200$  boyutunda piksel kümesi elde etmek için sütun bazında, bir boyutlu AKD uygulanır ve her bir sütunun DC değeri tutulur. Daha sonra, bu  $1 \times 200$  boyutlu DC değerleri gömülen damganın yükünü hafifletmek için bir anahtar değere bölündükten sonra,  $8 \times 200$  boyutlu bit formatı olan ikili dizeye kodlanır.

### 3.4. Damga gömme süreci

İristen elde edilen ikili damgayı standart test görüntüsüne gömmek için gerekli adımlar şu şekildedir:

1.  $512 \times 512$  boyutlu gri seviye görüntüye (I) 'haar' filtre ile YDDADD uygulanır ve dört ayrı bant elde edilir.

$$[LL, LH, HL, HH] = YDDADD(I) \quad (9)$$

2. LL bant  $4 \times 4$  boyutlu örtüşmeyen bloklara ayrılır.
3. Her bloğa 1 bit gömülmesi durumunda damga boyutundan daha fazla blok elde edilir. Bu durumda damganın gömüleceği uygun blokları seçmek için, öncelikle tüm bloklar standart sapma değerlerine bağlı olarak artan sırada sıralanır. Damga gömme adımında standart sapma değeri en düşük olan bloklardan yararlanılır ve bu blokların indeksleri çıkarma adımında kullanılmak üzere bir vektörde saklanır (*gizli anahtar 1*).
4. Seçilen bloğa Schur ayrıştırma uygulanır.

5. Elde edilen U bileşenin ilk sütununun 2. elemanına damga gömmek için Denklem 10'dan yararlanılır. Burada T damgalamanın ölçekleme faktörünü ifade eder ve deneyler sonucu 0.02 olarak bulunmuştur.  $U(:,1)$  ise U matrisinin 1. sütun elemanlarını gösterir.

$$U_{2,1} = \begin{cases} \text{sign}(U_{2,1}) \times (\max(|U(:,1)|) + T), & w_{m_i} = 1 \\ \text{sign}(U_{2,1}) \times (\min(|U(:,1)|) - T), & w_{m_i} = 0 \end{cases} \quad (10)$$

6. Modifiye edilmiş U matrisi ve V matrisi kullanılarak ters Schur ayrıştırma ile damgalanmış blok elde edilir.

$$\text{blok}^* = U \times V \times U' \quad (11)$$

7. Seçilen tüm bloklar için 4-6 arası adımlar uygulanır. Tüm damgalanmış bloklar birleştirildikten sonra, modifiye edilmiş LL bant ( $LL^*$ ) elde edilir. Bu alt bant, diğer alt bantlarla ( $LH, HL, HH$ ) birleştirilip ters YDDADD uygulanarak damgalanmış görüntü ( $I^*$ ) elde edilir.

$$I^* = YDDADD^{-1}(LL^*, LH, HL, HH) \quad (12)$$

8. *gizli anahtar 1*, çıkarma adımına iletilir.

### 3.5. Damga çıkarma süreci

$512 \times 512$  boyutlu gri seviye damgalanmış test görüntüsünden damga çıkarmak için gerekli adımlar şu şekildedir:

1. Damgalanmış ve bozulmuş görüntüye (WI) "haar" filtre ile YDDADD uygulanır.

$$[LL, LH, HL, HH] = YDDADD(WI) \quad (13)$$

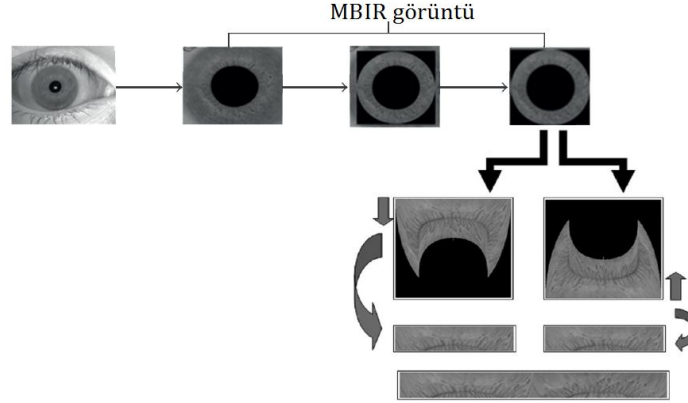
2. LL bant  $4 \times 4$  boyutlu örtüşmeyen bloklara ayrılır.
3. *gizli anahtar 1* ile belirtilen her bir bloğa Schur ayrıştırma uygulanır.
4. Her bir bloğa gömülen damga Denklem 14-17 ile belirtilen kurallara göre çıkarılır.

$$\text{abs}U_{21} = |U_{2,1}| \quad (14)$$

$$\text{diffMin} = |\text{abs}U_{21} - \min(|U(:,1)|)| \quad (15)$$

$$\text{diffMax} = |\text{abs}U_{21} - \max(|U(:,1)|)| \quad (16)$$

$$w_{m_i}^* = \begin{cases} 1, & \text{diffMax} < \text{diffMin} \\ 0, & \text{diffMax} \geq \text{diffMin} \end{cases} \quad (17)$$



Şekil 3. Bir iris görüntüsünün normalizasyon süreci

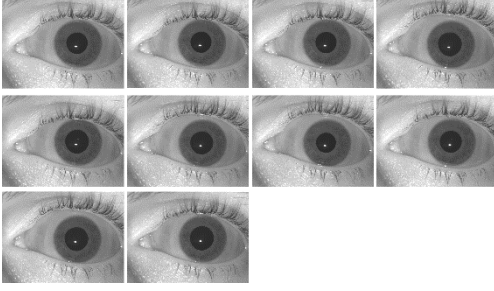
#### 4. Bulgular

Bu bölümde, önerilen YDDADD-Schur ayrıştırma tabanlı yöntemin deneysel sonuçları ayrıntılı olarak açıklanmaktadır. Yöntem, Matlab R2017b yazılımı kullanılarak Intel (R) Core™ i7 2.50 GHz, 16 GB RAM'e sahip kişisel bir bilgisayarda gerçekleştirilmiştir. Önerilen sistemde, iris görüntüleri  $512 \times 512$  gri seviye test görüntülerine gizlenmektedir. Tablo 1, iris veri tabanlarını, bu veri tabanlarını kullanan biyometrik damgalama çalışmalarını, göz görüntülerine ait boyut ve renk bilgisini içermektedir. Her veri tabanındaki görüntülerin özellikleri (boyut, iris yarı çapı, göz bebeği yarı çapı vs.) farklı olduğu için literatürdeki çalışmalar, seçmiş oldukları belirli bir veri tabanı üzerinden sonuçlar vermeye yönelmişlerdir. Bu çalışmada da Bath Üniversitesi veri tabanından alınan iris verileri damga olarak kullanılmaktadır. Şekil 4'te veri tabanındaki bir göze ait farklı görüntüler gösterilmiştir. Her bir görüntü aynı göze ait olsa da kısmi farklılıklar olduğu için üretilen damga bilgisi birebir aynı olmamaktadır. Bu nedenle veri setini genişletmek amacıyla, hem farklı kişilerden hem de aynı kişiye ait farklı görüntülerden elde edilen iris kodları damga olarak kullanılmıştır. Bu nedenle, her bir göze ait 10 farklı görüntünün yer aldığı ve 40 ayrı gözün kullanıldığı, toplamda 400 görüntü üzerinden elde edilen iris kodları ile çalışma ayrı ayrı test edilmiştir. Performans hem algılanamazlık hem de dayanıklılık açısından ölçülmüştür. Algılanamazlık için Tepe Sinyali Gürültü Oranı (Peak Signal to Noise Ratio-PSNR) ölçütü olarak kullanılmıştır. Dayanıklılığı hesaplamak amacıyla, her orijinal görüntünün 1 tane sadece damgalanmış ve 40 tane de damgalanmış ve ardından saldırıya uğramış

türevlerinden damga bilgisi çıkarılır. Burada bahsi geçen saldırılar, farklı yoğunluklardaki tuz ve biber gürültüsü, Poisson gürültüsü, farklı varyanslarda benek gürültüsü, farklı varyanslarda Gaussian gürültüsü, sol üst köşeden ve merkezden  $100 \times 100$  boyutlu bölgenin ayrı ayrı kırılması, farklı kalite faktörlerinde JPEG sıkıştırma, farklı maske boyutlarında Gaussian filtreleme ve ortanca filtreleme, ortalama filtresi, keskinleştirme filtresi, histogram eşitleme, yeniden ölçekleme, gamma düzeltmesi, 90, 180 ve 270° döndürme, görüntüyü yatayda ve dikeyde çevirme, görüntüden rasgele 20 satır ve 20 sütun silme, Wiener filtresi ve dalgacık sıkıştırma olarak sıralanabilir. Çıkarılan damga bilgisi ve gömülen damga bilgisi arasındaki Normalize Edilmiş Korelasyon (Normalized Correlation-NC) ve Bit Hata Oranı (Bit Error Rate-BER) hesaplanarak yöntemin saldırılara karşı direnci ölçülmüştür.

Tablo 1. Literatürde kullanılan iris veri tabanları.

Veri Tabanı	Boyut	Kullanıldığı Çalışmalar	Renk
Bath Üniversitesi	1280x960	[13, 14]	Gri Seviye
CASIA V1	320x280	[16]	Gri Seviye
CASIA-Iris-Twins	640x480	[18]	Gri Seviye
ICE-Right	640x480	[15]	Gri Seviye
SDUMLA-HMT	768x576	[1, 17]	Gri Seviye



Şekil 4. Bir kişiye ait farklı göz görüntüleri

Gri seviyede görüntülerde PSNR değerinin hesaplanması Denklem 18'de verilmiştir [8]. PSNR ne kadar yüksek olursa damgalanmış görüntünün görsel kalitesinin o kadar iyi olduğu söylenebilir.

$$= 10 \times \log_{10} \frac{PSNR}{Maxf^2} \quad (18)$$

$$\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [f(i,j) - g(i,j)]^2$$

Burada  $Maxf$  görüntünün maksimum parlaklık değerini belirtirken,  $M$  ve  $N$  görüntünün boyutunu,  $f(i,j)$  orijinal görüntünün  $(i,j)$  pikselinin parlaklık değerini,  $g(i,j)$  ise damgalanmış görüntünün  $(i,j)$  pikselinin parlaklık değerini ifade eder.

Gömme şemasının dayanıklılığını kanıtlamak için kullanılan NC ve BER değerleri sırasıyla Denklem 19 ve 20'de ifade edilmektedir [8]. NC, gömülü damga ile çıkarılan damga arasındaki benzerliği hesaplar. NC değeri 1'e yaklaştıkça, çıkarılan damganın kalitesi artar. BER ise çıkarılan damganın bit hatasını gösterir. BER ne kadar düşük olursa damgalamanın kalitesi de o kadar iyi olur.

$$NC = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (w_{i,j} \times w_{i,j}^*)}{\sum_{i=1}^{N1} \sum_{j=1}^{N2} w_{i,j}^2} \quad (19)$$

$$BER = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (w_{i,j} \otimes w_{i,j}^*)}{N1 \times N2} \quad (20)$$

Burada  $w$  orijinal damgayı ifade ederken,  $w^*$  çıkarılan damgayı ifade eder.

#### 4.1. Algılanamazlık

Algılanamazlık (imperceptibility) damgalama sistemlerinde önemli bir gereksinimdir ve damgalanmış içeriğin algısal kalitesini ifade

eder. Yani, damgalanmış içeriğin aslına (orijinaline) uygunluğunun bir ölçütüdür. Kör olmayan damgalama sistemleri, tespit sırasında orijinal görüntüye ihtiyaç duyduğu için kör damgalama sistemlerine göre daha sağlamdır [3, 4]. Ancak kör damgalama, orijinal görüntülerin depolanması için maliyet ve bellek yükünü azaltması [3] ve daha güvenli olması [5] sebebiyle bu çalışmada tercih edilmiştir. Kör damgalamayı gerçekleştirirken istenilen dayanıklılığı elde etmek için algılanamazlığın kör olmayan damgalama sistemine göre bir miktar düşük olması kaçınılmazdır. Tablo 2'de farklı test görüntüleri ve bu görüntüler taşıyıcı görüntü olarak kullanıldığında elde edilen PSNR değerleri verilmiştir. Bu altı test görüntüsü için ortalama PSNR değeri **37.4714 db** olarak bulunmuştur ki; bu değer algısal kalite açısından oldukça iyidir. Şekil 5'te önerilen sistem tarafından elde edilen damgalanmış "Lena" görüntüleri verilmiştir. Şekil 5'ten de görüldüğü üzere damgalanmış görüntülerde damganın varlığı kesinlikle hissedilmemektedir.

#### 4.2. Dayanıklılık

Damgalama şemalarında dayanıklılık (robustness), damganın, damgalanmış içerik saldırıya uğramış olsa bile hala hayatta kalması yani, kurtarılabilir olması anlamına gelmektedir. İyi bir damgalama sisteminin gürültü ilavesi, filtreleme işlemi, JPEG sıkıştırma, geometrik dönüşümler gibi saldırılara karşı direnç göstermesi gerekmektedir. Önerilen yöntemin dayanıklılığı daha önce bahsi geçen 41 farklı atak karşısında test edilmiştir. Dayanıklılığı test etmek için hem NC hem de BER değerleri ölçülmüştür. Tablo 3 "Lena" görüntüsü kullanıldığında ataklar karşısında elde edilen NC ve BER değerlerini göstermektedir.

Tablo 3 incelendiğinde atak yokken NC 1 ve BER 0 bulunmuştur. Gürültü ataklarında tuz ve biber gürültüsü (yoğunluk 0.02 ve 0.03) ve Gaussian gürültüsü (varyans 0.009) dışında NC değerleri 0.9'un üstündedir. BER değerleri de NC ile tutarlı bulunmuştur. NC'nin düşük olduğu yukarıdaki gürültülerde BER değeri de 0.1'in üstüne çıkmıştır. Diğer durumlarda dayanıklılık oldukça iyidir.

Kırpma atağında, damganın gömüldüğü bloklar art arda değil de blokların standart sapmasına göre seçildiğinden yöntem oldukça başarılı bulunmuştur. Farklı kalite faktörlerinde (KF) test edilen JPEG sıkıştırmada da yöntem çok



yüksek bir dayanıklılığa sahiptir. KF 50 iken bile NC 0.9555 olarak ölçülmüştür.

Önerilen yöntem filtreleme ataklarına karşı oldukça başarılı bulunmuştur. Özellikle Gaussian filtreleme ve Keskinleştirme filtresinde NC 1 ve BER 0 ya da 0'a oldukça yakın bulunmuştur.

Yöntem histogram eşitleme, yeniden ölçekleme ve gamma düzeltmesi ataklarına da oldukça dayanıklıdır. NC değeri çoğu durumda 1 iken BER değeri 0 bulunmuştur.

YDDADD'nin doğası gereği, yöntemin görüntü çevirme ve 90° ve katlarında döndürmeye karşı dayanıklılık performansı üst seviyededir. Bu ataklarda NC 1 iken BER 0 bulunmuştur.

Önerilen damgalama sisteminin diğerlerine kıyasla nispeten daha az başarılı olduğu durum rasgele 20 satır ve 20 sütun silme atağına karşıdır. Bu atak karşısında NC değeri 0.9184 ve BER değeri 0.1256 olarak bulunmuştur. Son olarak dalgacık sıkıştırma atağı incelendiğinde (piksel başına bit, bpp, 3.5 ve 8) yöntem yine çok başarılı bir performans sergilemiştir. NC ve BER değerleri sırasıyla 1 ve 0 olarak bulunmuştur.

### 4.3. Sonuçların kıyaslanması

Elde edilen deneysel sonuçlar hem geleneksel damgalama şemaları [8-10] ile hem de iris verisini kullanan biyometrik damgalama şemaları [17, 18] ile kıyaslanmıştır. Geleneksel yöntemlerden kaldırma dalgacık dönüşümüne dayalı kör yöntem [8], kaldırma dalgacık dönüşümü - regresyon ağacına dayalı kör yöntem [9] ve ADD-AKD-TDA'ya dayalı kör yöntem [10] ile çalışma kıyaslanmıştır.





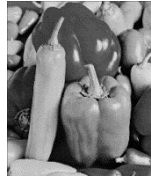

Tablo 4 damga tipi, damga boyutu ve PSNR açısından önerilen sistemin referans çalışmalarla kıyaslamasını içermektedir. Tablo 4'ten görüldüğü üzere önerilen sistem

algılanamazlık açısından daha avantajlıdır. Bu çalışmada ıristen elde edilen ikili damga boyutu 1600 bittir. [8], [9] ve [10]'daki çalışmalar daha az boyuttaki (1024 bit) ikili damgayı gömdüğü halde bu dört çalışmanın PSNR değeri birbirine yakın çıkmıştır. Ayrıca önerilen sistem biyometrik veri kullandığı için de bu geleneksel yöntemlere kıyasla daha güvenlidir. Biyometrik şemalarla algılanamazlık açısından bir karşılaştırma yapılmamasının sebebi, referans çalışmaların çoklu biyometrik veri kullanmaları ve bundan ötürü sağlıklı bir kıyaslanmanın söz konusu olamayacağındandır.

Tablo 5'te, biyometrik sistemlerle ataklar karşısındaki dayanıklılık performansı karşılaştırılmıştır. [17]'de artımlı ADD ve TDA'ya dayalı yüz ve iris biyometrik verilerini kullanan bir damgalama şeması önerilmiştir. [18]'de ise Slantlet dönüşümü ve TDA'ya dayalı iris ve parmak izi verisini kullanan çok modellen bir damgalama şeması sunulmuştur. Tablo 5'ten görüldüğü üzere önerilen sistem, rasgele 20 satır ve 20 sütun silme atağı dışında [17]'deki çalışmadan daha üstündür. Çalışma [18] ile karşılaştırıldığında ise atak yokken, tuz ve biber gürültüsüne karşı, kırpma atağına karşı, Gaussian filtreleme, keskinleştirme filtresi ve histogram eşitlemeye karşı daha yüksek performans sergilemiştir.

Tablo 6 ve 7'de geleneksel damgalama şemalarına karşı NC ve BER değerleri kıyaslanmıştır. Atak olmadığında bu dört çalışmanın da sonuçları aynı bulunmuştur. Gürültü ataklarında, önerilen sistem ve [8] ve [9]'da verilen sistemler genellikle birbirlerine yakın sonuçlar elde etse de [8] tarafından önerilen çalışma nispeten daha iyidir. Ancak [10]'da önerilen sistemin performansının daha kötü olduğu görülmektedir.

**Tablo 2.** Farklı test görüntülerine ait PSNR değerleri.

Boat	Cameraman	Couple	Lena	Peppers	Pirate
36.6101 db	38.527 db3	36.8114 db	37.9105 db	37.6677 db	37.3012 db
					



**Şekil 5.** Damgalanmış ve atak uygulanmış “Lena” görüntüleri: a) Atak yok b) Tuz ve biber gürültüsü ( $d=0.03$ ) c) Poisson gürültüsü d) Benek gürültüsü ( $v=0.009$ ) e) Gaussian gürültüsü ( $v=0.009$ ) f) Kırpma (Sol-Üst) g) Kırpma (Merkez) h) JPEG Sıkıştırma (KF=75) i) JPEG Sıkıştırma (KF=50) j) Gaussian filtre (3x3) k) Ortalama filtre (3x3) l) Ortanca filtresi (3x3) m) Keskinleştirme filtresi n) Histogram eşitleme o) Yeniden ölçekleme (512-256-512) p) Gamma düzeltmesi r) Döndürme (90 derece) s) Döndürme (180 derece) t) Görüntü çevirme (sütunlar) u)Görüntü çevirme (satırlar) v) Rasgele 20 satır ve 20 sütun silme y) Wiener filtre z) Dalgacık sıkıştırma (bpp=3.5)

**Tablo 3.** "Lena" görüntüsü için ataklar karşısında NC ve BER değerleri.

Ataklar	NC	BER	Ataklar	NC	BER
Atak yok	1	0	Gaussian filtre (maske boyutu=3x3)	1	0.0131
Tuz ve biber gürültüsü (d=0.005)	0.9666	0.0344	Gaussian filtre (maske boyutu=5x5)	1	0.0131
Tuz ve biber gürültüsü (d=0.01)	0.9147	0.0638	Gaussian filtre (maske boyutu=9x9)	1	0.0131
Tuz ve biber gürültüsü (d=0.02)	0.8962	0.1144	Ortalama filtresi (maske boyutu=3x3)	0.9481	0.0631
Tuz ve biber gürültüsü (d=0.03)	0.8294	0.1588	Ortanca filtresi (maske boyutu=2x2)	0.9926	0.0188
Poisson gürültüsü	1	0	Ortanca filtresi (maske boyutu=3x3)	0.9555	0.0538
Benek gürültüsü (v=0.001)	1	0	Keskinleştirme filtresi	1	0
Benek gürültüsü (v=0.005)	0.9876	0.0106	Histogram eşitleme	1	0
Benek gürültüsü (v=0.009)	0.9456	0.0506	Yeniden ölçekleme (512-256-512)	0.9889	0.0131
Gaussian gürültüsü (v=0.001)	0.9938	0.0056	Yeniden ölçekleme (512-1024-512)	1	0
Gaussian gürültüsü (v=0.005)	0.9011	0.1019	Gamma düzeltmesi (gamma değeri=0.2)	1	0
Gaussian gürültüsü (v=0.009)	0.8517	0.1644	Döndürme (90 derece)	1	0
Kırpma (sol-üst)	1	0	Döndürme (180 derece)	1	0
Kırpma (merkez)	0.9876	0.0063	Döndürme (270 derece)	1	0
JPEG sıkıştırma (KF=100)	1	0	Görüntü çevirme (sütunlar)	1	0
JPEG sıkıştırma (KF=90)	1	0	Görüntü çevirme (satırlar)	1	0
JPEG sıkıştırma (KF=85)	1	0	Rasgele 20 satır ve 20 sütun silme	0.9184	0.1256
JPEG sıkıştırma (KF=80)	1	0	Wiener filtre	0.9604	0.0375
JPEG sıkıştırma (KF=75)	1	0	Dalgacık sıkıştırma (bpp=3.5)	1	0
JPEG sıkıştırma (KF=60)	0.9815	0.0169	Dalgacık sıkıştırma (bpp=8)	1	0
JPEG sıkıştırma (KF=50)	0.9555	0.0475			

Kırpma atağında sol-üst kırpma atağına karşı önerilen çalışmanın sonuçları daha iyidir. Merkezi kırpmada ise [9]'da elde edilen sonuçların daha etkili olduğu gözlenmiştir. JPEG sıkıştırmaya karşı performans [8] ve [9]'da önerilen yöntemlerdekiyle benzerdir. KF, 75

olduğunda önerilen sistem ve [8]'in NC değeri 1, [9]'un ise 0.9977 olarak verilmiştir. [10]'da önerilen yöntem ise KF, 70 olduğunda 0.9859 olarak bulunmuştur. Dolayısıyla, önerilen sistem [10]'a kıyasla JPEG sıkıştırma atağına karşı nispeten daha başarılıdır.

**Tablo 4.** Önerilen sistemin var olan çalışmalarla PSNR açısından karşılaştırılması.

	Önerilen sistem	[8]	[9]	[10]
Damga tipi	Biyometrik damga	İkili damga	İkili damga	İkili damga
Damga boyutu	<b>1600 bit</b>	1024 bit	1024 bit	1024 bit
PSNR ("Lena" için)	37.91	37.98	38.89	<b>40.07</b>

Filtreleme ataklarına gelince Gaussian filtrelemede önerilen çalışma, [8] ve [9]'un NC değerleri aynı iken, BER değeri referans çalışmalarda daha iyi bulunmuştur. Ancak aradaki fark oldukça azdır. Ortalama filtresine karşı [9]'da önerilen çalışmanın sonucu daha iyi iken, ortanca filtresine karşı [10] nispeten daha başarılıdır. Keskinleştirme filtresi ve histogram eşitlemede önerilen sistem ve [8] ve [9] tarafından önerilen yöntemler üst seviyede performans sergilemişlerdir.

Yeniden ölçeklemeye karşı benzer sonuçların yer aldığı tabloda asıl fark yaratan husus döndürmeye karşı dayanıklılıktır. [8] ve [9]'un döndürmeye karşı performansı oldukça kötüdür. Şöyle ki; NC referans çalışmalarda yaklaşık 0.1 iken BER yaklaşık 0.5 olarak verilmiştir. Bizim çalışmamızda NC ve BER değerleri sırasıyla 1 ve 0 olarak bulunmuştur. [10]'da ise döndürmeye karşı dayanıklılık test edilmemiştir. Ayrıca referans çalışmalarda verilmeyen görüntü çevirme ve dalgacık sıkıştırma atağına karşı dayanıklılık da bu yöntemin en önemli üstünlüğüdür.

Sonuç olarak bakıldığında önerilen sistem biyometrik damga kullandığı için güvenlik açısından ikili damga kullanan çalışmalara göre daha avantajlıdır. Ayrıca bu çalışmada kullanılan damga boyutu referans çalışmalardakilerden çok daha fazla olmasına rağmen PSNR değerleri yakın bulunmuştur. Çalışmalar çoğu atak karşısında yakın sonuçlar vermesine rağmen asıl fark döndürmeye karşı performansta öne çıkmıştır. Referans çalışmaların döndürmeye karşı performansı oldukça kötü olmasına rağmen, önerilen sistem döndürmeye karşı değişmezdir. Ayrıca YDDADD'nın yapısından dolayı satır ve sütun bazında görüntü çevirmeye karşı önerilen yöntem diğer yöntemlerin aksine

dayanıklısıdır. Yine referans çalışmalarda verilmeyen dalgacık sıkıştırma atağına karşı performansta da bizim çalışmamız gömülen damgayı hatasız olarak çıkarabilmiştir.

## 5. Tartışma ve Sonuç

Bu çalışmada sayısal görüntülerin telif hakkı koruması için YDDADD-Schur ayrıştırma tabanlı kör bir damgalama yöntemi önerilmiştir. YDDADD, geleneksel dalgacık dönüşümünden farklı olarak 90° katlarında döndürme ve görüntü çevirmeye karşı dayanıklı bir tekniktir. YDDADD sonucu elde edilen düşük frekanslı alt bant önce örtüşmeyen bloklara ayrılır. Ardından en uygun bloklar standart sapma değerlerine bağlı olarak sıralandıktan sonra seçilir. Seçilen bloklara Schur ayrıştırma uygulandıktan sonra damga gömülür. Schur ayrıştırma TDA'ya göre daha az hesaplama gerektirmesi sebebiyle avantajlı bir tekniktir. Schur ayrıştırma sonucu elde edilen U matrisinin birinci sütun elemanları arasındaki ilişki den damga gömme aşamasında yararlanılmıştır.

Çalışmada damga olarak eşsiz bir özellik olan iris verisi kullanılmıştır. Damganın biyometrik özelliklerden seçilmesi damgalamanın güvenliğini artırır. İris şablonu hem kopyalanması zor olduğundan hem de birçok biyometrik özelliğe kıyasla daha güvenli olduğundan bu çalışmada tercih edilmiştir. İris şablonunun AKD yardımıyla ikili koda dönüştürülmesi ile elde edilen damga YDDADD-Schur ayrıştırma tabanlı yaklaşımla orijinal görüntüye gizlenmiştir.

Elde edilen deneysel sonuçlar incelendiğinde damgalanmış görüntülerde damganın varlığı kesinlikle hissedilmemektedir. Ayrıca 41 farklı saldırı karşısında dayanıklılık test edildiğinde, damga bu bozulmuş görüntülerden başarılı bir şekilde çıkarılmıştır. Önerilen yöntem referans çalışmalara kıyaslandığında, algılanamazlık açısından performansının daha üstün olduğu görülmektedir. Nitekim bu çalışmada referans çalışmalara göre daha fazla sayıda bit kullanılmasına rağmen, elde edilen PSNR değeri referans çalışmalardakine oldukça yakındır. Bunun yanı sıra, çalışma hem iris tabanlı hem de geleneksel damgalama şemalarıyla dayanıklılık açısından karşılaştırıldığında, özellikle geometrik ataklarda ve dalgacık sıkıştırmada oldukça yüksek bir performansa sahip olduğu görülmektedir.

**Tablo 5.** Çıkarılan iris kodunun NC değerinin mevcut biyometrik çalışmalarla kıyaslanması.

	<b>Önerilen Sistem</b>	<b>[17]</b>	<b>[18]</b>
<b>Kullanılan teknik</b>	YDDADD+Schur Ayırıştırma	Artımlı ADD + TDA	Slantlet Dönüşümü + TDA
<b>Kullanılan veri tabanı</b>	Bath Üniversitesi	SDUMLA-HMT	CASIA-Iris-Twins
<b>NC</b>			
<b>Atak yok</b>	<b>1</b>	--	0.9994
<b>Tuz ve biber gürültüsü</b>	<b>0.9147</b> (d=0.01)	0.8277 (d belirtilmemiş)	0.8829 (d belirtilmemiş)
<b>Kırpma</b>	<b>1</b> (Sol-üst)	--	0.9974
<b>Gaussian filtresi</b>	<b>1</b>	0.8868 (maske boyutu belirtilmemiş)	0.9992
<b>Ortalama filtresi (maske boyutu=3x3)</b>	0.9481	--	<b>0.9991</b>
<b>Ortanca filtresi (maske boyutu=3x3)</b>	0.9555	--	<b>0.9986</b>
<b>Keskinleştirme filtresi</b>	<b>1</b>	0.8903	0.9988
<b>Histogram eşitleme</b>	<b>1</b>	0.9836	0.9787
<b>Yeniden ölçekleme (512-256-512)</b>	0.9889	0.8582	<b>0.9985</b>
<b>Döndürme</b>	<b>1</b>	0.7933 (derece belirtilmemiş)	--
<b>Görüntü çevirme (sütunlar)</b>	<b>1</b>	0.9860	--
<b>Görüntü çevirme (satırlar)</b>	<b>1</b>	0.8952	--
<b>Rasgele 20 satır ve 20 sütun silme</b>	0.9184	<b>0.9193</b> (silinen satır ve sütun sayısı belirtilmemiş)	--

**Tablo 6.** "Lena" görüntüsüne ait NC değerlerinin geleneksel şemalarla kıyaslanması.

Ataklar	Önerilen Sistem	[8]	[9]	[10]	Ataklar	Önerilen Sistem	[8]	[9]	[10]
Atak yok	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	JPEG sıkıştırma (KF=75)	<b>1</b>	<b>1</b>	0.9977	0.9859 (KF=70)
Tuz ve biber gürültüsü (d=0.01)	0.9147	<b>0.9609</b>	0.9317	0.8817	Gaussian filtre (maske boyutu= 3x3)	<b>1</b>	<b>1</b>	<b>1</b>	--
Tuz ve biber gürültüsü (d=0.02)	0.8962	0.8776	<b>0.9016</b>	0.8386	Gaussian filtre (maske boyutu= 5x5)	<b>1</b>	<b>1</b>	<b>1</b>	--
Tuz ve biber gürültüsü (d=0.03)	0.8294	<b>0.8454</b>	0.8374	--	Ortalama filtresi (maske boyutu=3x3)	0.9481	0.9727	<b>0.9932</b>	0.9641
Poisson gürültüsü	<b>1</b>	<b>1</b>	<b>1</b>	--	Ortanca filtresi (maske boyutu=3x3)	0.9555	0.9013	0.9909	<b>0.9967</b>
Benek gürültüsü (v=0.001)	<b>1</b>	<b>1</b>	0.9955	--	Keskinleştirme filtresi	<b>1</b>	<b>1</b>	<b>1</b>	0.9993
Benek gürültüsü (v=0.005)	0.9876	<b>0.9975</b>	0.9662	--	Histogram eşitleme	<b>1</b>	<b>1</b>	<b>1</b>	0.9953
Benek gürültüsü (v=0.009)	0.9456	<b>0.9825</b>	0.8982	--	Yeniden ölçekleme (512-256-512)	0.9889	<b>1</b>	<b>1</b>	0.9987
Gaussian gürültüsü (v=0.001)	0.9938	<b>1</b>	0.9842	--	Yeniden ölçekleme (512-1024-512)	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>
Gaussian gürültüsü (v=0.005)	0.9011	<b>0.9195</b>	0.8199	0.8470	Döndürme (90 derece)	<b>1</b>	0.1084	0.1187	--
Gaussian gürültüsü (v=0.009)	<b>0.8517</b>	0.8097	0.6887	--	Döndürme (180 derece)	<b>1</b>	0.1015	0.1200	--
Kırpma (sol-üst)	<b>1</b>	0.9850	0.9433	--	Döndürme (270 derece)	<b>1</b>	--	--	--
Kırpma (merkez)	0.9876	0.9625	<b>0.9955</b>	--	Görüntü çevirme (sütunlar)	<b>1</b>	--	--	--
JPEG sıkıştırma (KF=80)	<b>1</b>	<b>1</b>	<b>1</b>	--	Görüntü çevirme (satırlar)	<b>1</b>	--	--	--

**Tablo 7.** “Lena” görüntüsüne ait BER değerlerinin geleneksel şemalarla kıyaslanması.

Ataklar	Önerilen Sistem	[8]	[9]	[10]	Ataklar	Önerilen Sistem	[8]	[9]	[10]
Atak yok	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	JPEG sıkıştırma (KF=75)	<b>0</b>	<b>0</b>	0.0010	0.0205 (KF=70)
Tuz ve biber gürültüsü (d=0.01)	0.0638	<b>0.0156</b>	0.0293	0.1650	Gaussian filtre (maske boyutu= 3x3)	0.0131	<b>0</b>	<b>0</b>	--
Tuz ve biber gürültüsü (d=0.02)	0.1144	0.0498	<b>0.0430</b>	0.2217	Gaussian filtre (maske boyutu= 5x5)	0.0131	<b>0</b>	<b>0</b>	--
Tuz ve biber gürültüsü (d=0.03)	0.1588	<b>0.0635</b>	0.0723	--	Ortalama filtresi (maske boyutu=3x3)	0.0631	0.0107	<b>0.0029</b>	0.0518
Poisson gürültüsü	<b>0</b>	<b>0</b>	<b>0</b>	--	Ortanca filtresi (maske boyutu=3x3)	0.0538	0.0391	0.0039	<b>0.0049</b>
Benek gürültüsü (v=0.001)	<b>0</b>	<b>0</b>	0.0020	--	Keskinleştirme filtresi	<b>0</b>	<b>0</b>	<b>0</b>	0.0010
Benek gürültüsü (v=0.005)	0.0106	<b>0.0010</b>	0.0146	--	Histogram eşitleme	<b>0</b>	<b>0</b>	<b>0</b>	0.0068
Benek gürültüsü (v=0.009)	0.0506	<b>0.0068</b>	0.0439	--	Yeniden ölçekleme (512-256-512)	0.0131	<b>0</b>	<b>0</b>	0.0020
Gaussian gürültüsü (v=0.001)	0.0056	<b>0</b>	0.0068	--	Yeniden ölçekleme (512-1024-512)	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>
Gaussian gürültüsü (v=0.005)	0.1019	<b>0.0322</b>	0.0811	0.2100	Döndürme (90 derece)	<b>0</b>	0.5205	0.4785	--
Gaussian gürültüsü (v=0.009)	0.1644	<b>0.0791</b>	0.1455	--	Döndürme (180 derece)	<b>0</b>	0.5156	0.5000	--
Kırpma (sol-üst)	<b>0</b>	0.0059	0.0244	--	Döndürme (270 derece)	<b>0</b>	--	--	--
Kırpma (merkez)	0.0063	0.0146	<b>0.0020</b>	--	Görüntü çevirme (sütunlar)	<b>0</b>	--	--	--
JPEG sıkıştırma (KF=80)	<b>0</b>	<b>0</b>	<b>0</b>	--	Görüntü çevirme (satırlar)	<b>0</b>	--	--	--

**Kaynakça**

- [1] Wójtowicz, W., Marek, R. O. 2016. Digital Images Authentication Scheme Based on Bimodal Biometric Watermarking In An Independent Domain, *Journal of Visual Communication and Image Representation*, Cilt. 38, s. 1-10.
- [2] Majumder, S., Singh, A. D., & Mishra, M. 2009. A GUI Based Iris Authentication System For Secured Access. *Int. Conf. Systemics, Cybernetics, Informatics (ICSCI-2009) under Pentagon Research, Hyderabad held, January, 7-10.*
- [3] Singh, P., Chadha, R. S. 2013. A Survey of Digital Watermarking Techniques, Applications and Attacks, *International Journal of Engineering and Innovative Technology (IJEIT)*, Cilt. 2(9), s. 165-175.
- [4] Zaiane, O., Mario, N., Stanley, O. 2002. *Digital Watermarking: Status, Limitations and Prospects.*
- [5] Naderahmadian, Y., Hosseini-Khayat, S. 2014. Fast and Robust Watermarking In Still Images Based on QR Decomposition, *Multimedia Tools and Applications*, Cilt. 72(3), s. 2597-2618.
- [6] Tao, H., Chongmin, L., Zain, J. M., Abdalla, A. N. 2014. Robust Image Watermarking Theories and Techniques: A review, *Journal of Applied Research and Technology*, Cilt. 12(1), s. 122-138.
- [7] Li, L., Xu, H. H., Chang, C. C., Ma, Y. Y. 2011. A Novel Image Watermarking in Redistributed Invariant Wavelet Domain. *Journal of Systems and Software*, Cilt. 84(6), s. 923-929.
- [8] Kazemivash, B., Moghaddam, M. E. 2017. A Robust Digital Image Watermarking Technique Using Lifting Wavelet Transform and Firefly Algorithm, *Multimedia Tools and Applications*, Cilt. 76(20), s. 20499-20524.
- [9] Kazemivash, B., Moghaddam, M. E. 2018. A Predictive Model-based Image Watermarking Scheme Using Regression Tree and Firefly Algorithm, *Soft Computing*, Cilt. 22(12), s. 4083-4098.
- [10] Kang, X. B., Zhao, F., Lin, G. F., & Chen, Y. J. 2018. A Novel Hybrid of DCT and SVD in DWT Domain for Robust and Invisible Blind Image Watermarking with Optimal Embedding Strength, *Multimedia Tools and Applications*, Cilt. 77(11), s. 13197-13224.
- [11] Liu, J. F., Huang, D. R., Hu, J. Q. 2003. The Orthogonal Wavelet Bases for Digital Watermarking, *Journal of Electronics and Information Technology*, Cilt. 25(4), s. 453-459.
- [12] Hassanien, A. E. 2006. Hiding Iris Data for Authentication of Digital Images Using Wavelet Theory, *Pattern Recognition and Image Analysis*, Cilt. 16(4), s. 637-643.
- [13] Majumder, S., Devi, K. J., & Sarkar, S. K. 2013. Singular Value Decomposition and Wavelet-based Iris Biometric Watermarking, *IET Biometrics*, Cilt. 2(1), s. 21-27.
- [14] Lu, J., Qu, T., & Karimi, H. R. 2014. Novel iris biometric watermarking based on singular value decomposition and discrete cosine transform, *Mathematical Problems in Engineering*, 2014.
- [15] Umar, M. M., Mehmood, A., Song, H., & Choo, K. K. R. 2017. I-Marks: An Iris Code Embedding System for Ownership Identification of Multimedia Content, *Computers & Electrical Engineering*, Cilt. 63, s. 209-219.
- [16] Paunwala, M., & Patnaik, S. 2014. Biometric Template Protection with DCT-Based Watermarking, *Machine Vision and Applications*, Cilt. 25(1), s. 263-275.
- [17] Singh, P., Raman, B., & Roy, P. P. 2017. A Multimodal Biometric Watermarking System For Digital Images in Redundant Discrete Wavelet Transform, *Multimedia Tools and Applications*, Cilt. 76(3), s. 3871-3897.
- [18] Tarif, E. B., Wibowo, S., Wasimi, S., & Tareef, A. 2018. A Hybrid Encryption/Hiding Method for Secure Transmission of Biometric Data in Multimodal Authentication System, *Multimedia Tools and Applications*, Cilt. 77(2), s. 2485-2503.
- [19] Su, Q., Niu, Y., Liu, X., Zhu, Y. 2012. Embedding Color Watermarks in Color Images Based on Schur Decomposition, *Optics Communications*, Cilt. 285(7), s. 1792-1802.
- [20] Karajeh, H., Khatib, T., Rajab, L., Maqableh, M. 2019. A Robust Digital Audio Watermarking Scheme Based on DWT and Schur Decomposition, *Multimedia Tools and Applications*, Cilt. 78(13), s. 18395-18418.
- [21] Su, Q., Chen, B. 2017. An Improved Color Image Watermarking Scheme Based on Schur Decomposition, *Multimedia Tools and Applications*, Cilt. 76(22), s. 24221-24249.
- [22] Monro, D. M., Zhang, Z. 2005. An Effective Human Iris Code with Low Complexity. *IEEE International Conference on Image Processing 2005, September, 277-280.*
- [23] Rakshit, S., Monro, D. M. 2006. Effects of Sampling and Compression on Human Iris Verification. *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, May, 337-340.*
- [24] Kalita, R., Majumder, S., Hussain, M. A. 2010. Multidimensional Multimetric Novel and Simple Techniques for Iris Recognition System, *Int. J. Recent Trends Eng. Cilt. 3(3)*, s. 161-166.