KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

İRİS BİYOMETRİSİNİ KULLANAN DAYANIKLI DAMGALAMA YÖNTEMİ

DOKTORA TEZİ

Şeyma YÜCEL ALTAY

MAYIS 2021
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

İRİS BİYOMETRİSİNİ KULLANAN DAYANIKLI DAMGALAMA YÖNTEMİ

Şeyma YÜCEL ALTAY

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"DOKTOR (BİLGİSAYAR MÜHENDİSLİĞİ)"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 21 / 04 /2021
Tezin Savunma Tarihi : 28 / 05 /2021

Tez Danışmanı : Doç. Dr. Güzin ULUTAŞ

Trabzon 2021

ÖNSÖZ

İnternet teknolojilerinin hızlı bir şekilde gelişmesiyle birlikte görüntü, video, ses vb. çoklu ortam verileri, bilgi aktarımı için önemli bir araç haline gelmiştir. Bu durum, sayısal içeriklerin yetkisiz olarak bulundurulması, değiştirilmesi, kullanılması ve dağıtılması tehdidini beraberinde getirir. Sayısal damgalama, sayısal içeriklerin telif haklarının korunması için etkili bir çözüm sunar. Bu tez çalışmasında, gri seviye ve renkli sayısal görüntüler üzerinde telif hakkı koruma amacıyla, yeni yöntemler ortaya konarak, dayanıklı damgalama sistemleri tasarlanmıştır.

Çalışmalarım süresince bilgi, görüş ve önerileriyle bana yardımcı olan çok değerli danışman hocam Sayın Doç. Dr. Güzin ULUTAŞ'a teşekkürü bir borç bilirim. Ayrıca değerli görüş ve katkılarını esirgemeyen tez jüri üyelerim Sayın Prof. Dr. Vasif Vagifoğlu NABİYEV ve Sayın Prof. Dr. İsmail Hakkı ALTAŞ'a şükranlarımı sunarım.

Yaşadığı müddetçe her zaman yanımda olan ve öğrenim hayatımda beni hep destekleyen rahmetli babama, tez çalışmam süresince ilgilerini her daim hissettiğim eşime ve aileme, ayrıca bu süreçte onu birçok kez ihmal etmek zorunda kaldığım kızıma sonsuz teşekkürlerimi sunarım.

Şeyma YÜCEL ALTAY

Trabzon 2021

TEZ ETİK BEYANNAMESİ

Doktora Tezi olarak sunduğum "İris Biyometrisini Kullanan Dayanıklı Damgalama Yöntemi" başlıklı bu çalışmayı baştan sona kadar danışmanım Doç. Dr. Güzin ULUTAŞ'ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı / yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 28/05/2021

Şeyma YÜCEL ALTAY

İÇİNDEKİLER

Sayfa No

Doktora Tezi

ÖZET

İRİS BİYOMETRİSİNİ KULLANAN DAYANIKLI DAMGALAMA YÖNTEMİ

Şeyma YÜCEL ALTAY

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Güzin ULUTAŞ
2021, 148 Sayfa

Tez kapsamında sayısal görüntülerin telif haklarının korunması için dayanıklı damgalama sistemlerine değinilmiştir. Bu amaçla dalgacık dönüşümüne dayalı farklı ayrıştırma teknikleri kullanan yeni damgalama yöntemleri önerilmiştir. Ayrık Dalgacık Dönüşümü ve Tekil Değer Ayrıştırma tekniklerinin kullanıldığı ilk yaklaşımda birbirleriyle çelişen algılanamazlık ve dayanıklılığı dengede tutmak için Ateş Böceği Algoritmasının yeni bir sürümü olan Kendinden Uyarlanabilir Adımlı Ateş Böceği Algoritmasından ilk kez yararlanılmıştır. Bu algoritma her ateş böceğinin bir sonraki adımını mevcut durumuna ve geçmiş bilgilerine bağlı olarak belirlediğinden, çözüm uzayının global olarak araştırılmasını sağlar. Bir diğer yaklaşımda, gömülen damganın aidiyetinin kanıtlanması hususunda etkili bir çözüm sunan iris kodu renkli görüntülere gizlenmiştir. Burada Ayrık Dalgacık Dönüşümünün geometrik ataklar karşısındaki dayanıklılık problemini çözmek için Yeniden Dağıtılmış Değişmez Ayrık Dalgacık Dönüşümü'nden yararlanılmıştır. Bu dönüşüm tekniği ile birlikte Ateş Böceği Algoritması / Kendinden Uyarlanabilir Adımlı Ateş Böceği Algoritması ile optimize edilmiş Tekil Değer Ayrıştırma, Schur Ayrıştırma ve QR Ayrıştırmaya dayalı farklı yaklaşımlar önerilmiştir. Bu yaklaşımlar arasından algılanamazlık, dayanıklılık ve kimlik doğrulama hassasiyeti bakımından en uygun yöntem belirlenmeye çalışılmıştır. Araştırma bulguları hem geleneksel hem de biyometrik tabanlı damgalama sistemlerinin algısal şeffaflık ve dayanıklılık açısından etkinliğini kanıtlamıştır. Ayrıca biyometrik damgalamaya yönelik çalışmanın kimlik doğrulama performansı incelendiğinde sonuçların oldukça tatmin edici olduğu gözlenmiştir.

Anahtar Kelimeler: Sayısal görüntü damgalama, Biyometrik damgalama, Ayrık dalgacık dönüşümü, Tekil değer ayrıştırma, QR ayrıştırma, Schur ayrıştırma.

PhD. Thesis

SUMMARY

ROBUST WATERMARKING METHOD USING IRIS BIOMETRICS

Şeyma YÜCEL ALTAY

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Assoc. Prof. Güzin ULUTAŞ
2021, 148 Pages

In this study, robust watermarking systems for copyright protection of digital images have been mentioned. For this purpose, new watermarking methods using different decomposition techniques based on wavelet transform have been proposed. In the first approach using Discrete Wavelet Transform and Singular Value Decomposition methods, a new version of the Firefly Algorithm, the Self-Adaptive Step Firefly Algorithm, has been used for the first time to balance the conflicting imperceptibility and robustness. Since this algorithm determines the next step of each firefly based on its present situation and historical information, it enables a global exploration of the solution space. In other approach, the iris code, which presents an effective solution for proving the ownership of the embedded watermark is hidden into color images. Here, Redistributed Invariant Discrete Wavelet Transform has been used to solve the robustness problem of the Discrete Wavelet Transform against geometric attacks. With this transform technique, different approaches based on Singular Value Decomposition, Schur Decomposition and QR Decomposition optimized by Firefly Algorithm/Self-Adaptive Step Firefly Algorithm are proposed. Among these approaches, the most appropriate method with regard to imperceptibility, robustness and authentication accuracy has been tried to determine. Research findings prove the effectiveness of both traditional and biometric-based watermarking systems in terms of perceptual transparency and robustness. In addition, when the authentication performance of the biometric watermarking study is examined, it is observed that the results are quite satisfactory.

Key Words: Digital image watermarking, Biometric watermarking, Discrete wavelet transform, Singular value decomposition, QR decomposition, Schur decomposition.

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

AADD	Artımsal Ayrık Dalgacık Dönüşümü (RDWT)
ABA	Ateş Böceği Algoritması (FA)
ADD	Ayrık Dalgacık Dönüşümü (DWT)
AFD	Ayrık Fourier Dönüşümü (DFT)
AKD	Ayrık Kosinüs Dönüşümü (DCT)
BBA	Bağımsız Bileşenler Analizi (ICA)
BCH	Bose, Chaudhuri, and Hocquenghem
BDO	Bit Doğrulama Oranı (BCR)
BHO	Bit Hata Oranı (BER)
CD	Contourlet Dönüşümü (CT)
DAD	Döngüsel Artıklık Denetimi (CRC)
DE	Diferansiyel Evrim
EAB	En Anlamsız Bit (LSB)
EHO	Eşit Hata Oranı (EER)
FLD	Fibonacci Lucas Dönüşümü (FLT)
GA	Genetik Algoritma
GBD	Görsel Bilgi Doğruluğu (VIF)
GKA	Guguk Kuşu Arama (CS)
GKO	Gerçek Kabul Oranı (GAR)
HD	Hough Dönüşümü
HU	Hamming Uzaklığı
İGS	İnsan Görsel Sistemi (HVS)
KDD	Kaldıran Dalgacık Dönüşümü (LWT)
KFD	Kesirli Fourier Dönüşümü
KKO	Karınca Kolonisi Optimizasyonu (ACO)
KUAABA	Kendinden Uyarlanabilir Adımlı ABA (SASFA)
LP	Laplacian Piramidi
MSİD	Minimum Sınırlı İzotetik Dikdörtgen (MBIR)
NK	Normalleştirilmiş Korelasyon (NC)
NMH	Normalleştirilmiş Mutlak Hata (NAE)

OAB	Orta Derecede Anlamlı Bit (ISB)
OKH	Ortalama Karesel Hata (MSE)
PSO	Parçacık Sürüsü Optimizasyonu
RA	Regresyon Ağacı (RT)
SGO	Sinyal Gürültü Oranı (SNR)
TBA	Temel Bileşenler Analizi (PCA)
TDA	Tekil Değer Ayrıştırma (SVD)
TDD	Tamsayı Dalgacık Dönüşümü (IWT)
TSGO	Tepe Sinyal Gürültü Oranı (PSNR)
YAK	Yapay Arı Kolonisi (ABC)
YBİ	Yapısal Benzerlik İndeksi (SSIM)
YDDADD	Yeniden Dağıtılmış Değişmez Ayrık Dalgacık Dönüşümü (RIDWT)
YFB	Yönlü Filtre Bankaları (DFB)
YKO	Yanlış Kabul Oranı (FAR)
YRO	Yanlış Reddetme Oranı (FRR)

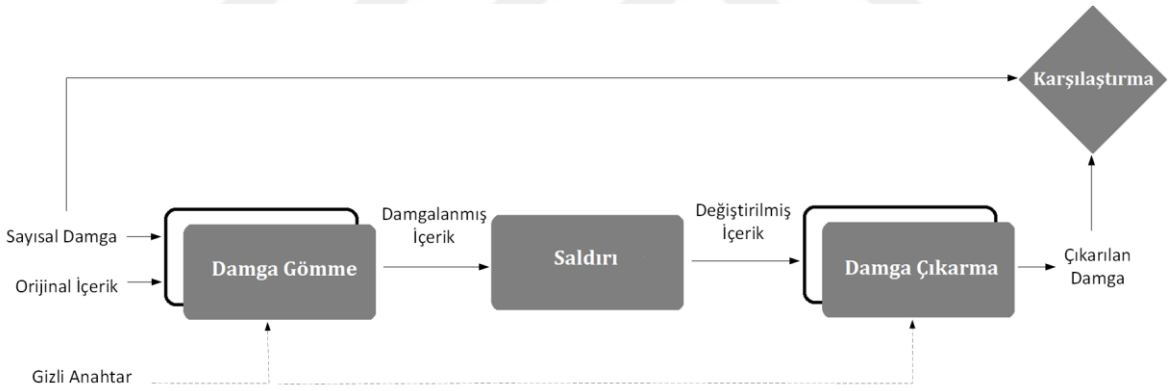
1. GENEL BİLGİLER

1.1. Giriş

Son yıllarda sayısal ağ sistemlerinin hızla gelişmesi, sayısal belgelerin hiç bilgi kaybı olmadan ve ücretsiz olarak çok sayıda insana kopyalanabilmesi ve dağıtılabilmesini mümkün kılmıştır. İnsanlar ses, görüntü ve video gibi çoklu ortam dosyalarını indirebilir, bunları paylaşabilir veya orijinal içeriklerini değiştirebilirler. Çoklu ortam içeriğinin korunması, tüketicilerin fikri mülkiyet hakkına yeterince hâkim olmamaları nedeniyle son zamanlarda önemli bir konu haline gelmiştir. Yasadışı bulundurma, çoğaltma ve yaymaya karşı savunmasız oldukları için sayısal biçimde temsil edilen içerikleri korumak amacıyla sayısal damgalama algoritmaları geliştirilmiştir. Sayısal damgalama, logo, imza veya metin gibi bilgileri görüntü, video veya ses dosyası gibi çoklu ortam verilerine gizleyerek fikri mülkiyet ve telif haklarını korumak için etkili bir çözüm sunmaktadır.

Sayısal cihazları kullanarak ve bunları internete bağlayarak, kişiler telif hakkıyla korunan materyalleri yasal içerik sahiplerine iade etmeden kaydedebilir ve dağıtabilirler. Yasal mülk sahipleri açısından kendilerine ait sayısal içeriği korumak adına kullanılan en yaygın yöntem kriptografidir. Bu teknolojiyle, ürünler satılmadan önce şifrelenir ve yalnızca bunları satın alan kişiler şifrelenmiş dosyalara tam olarak erişmek için şifre çözme anahtarına sahiptir. Şifrelenmiş dosyalar internet üzerinden de kullanılabilir hale getirilebilir. Maalesef satıcılar, şifre çözüldükten sonra yasal bir müşterinin içeriği nasıl işlediğini izleyemez. Orijinal kopya satıldıktan sonra, bir korsan gerçekten ürünü satın alabilir, korumasız kopya içeriği elde etmek için şifre çözme anahtarını kullanabilir ve ardından yasadışı dağıtım için birden fazla kopya çoğaltabilir. Dolayısıyla, kriptografi sınırlı bir koruma ölçüsü sağlar. Şifresi çözülen içerik müşteriye ulaştığında başka bir koruma olmayacaktır. Bu nedenle, şifresi çözüldükten sonra bile içeriğin daha fazla korunmasına ihtiyaç vardır. Sayısal damga, sahibinin telif hakkı korumasını yerine getirmek için kullanılabilecek, gelecek vaat eden bir teknolojidir. Sayısal damgalamada bilgiler içeriklerin içinde saklanır ve sıkıştırma, sayısaldan analoğa dönüştürme ve dosya biçimi değişiklikleri gibi farklı saldırı türleri karşısında hayatta kalabilir. Sayısal damgalama, telif hakkı koruma, kimlik doğrulama, parmak izi, kopya kontrolü, yayın izleme ve dış müdahale algılama gibi farklı amaçlarla kullanılabilir.

Sayısal damgalama, damga adı verilen sayısal bilgilerin çoklu ortam içeriğine gömülmesi (veya gizlenmesi) ve daha sonra sayısal içeriğin telif hakkını korumak, yasadışı kopyalanmasını önlemek veya herhangi bir tahrife karşı direnç sağlamak gibi çeşitli amaçlarla gömülü verilerin, yetkisiz kişiler tarafından fark edilemeyen ve çıkarılması zor olan damgalanmış içerikten çıkarılabilmesi veya tespit edilebilmesi sürecidir. Sayısal damgalamada tanımlanması gereken üç önemli kavram vardır. Taşıyıcı sinyal (ya da orijinal içerik), damga bilgisini içerecek olan sayısal ses, görüntü, metin veya video sinyalidir. Damganın kendisi, bir orijinal içerik aracılığıyla depolanacak veya iletilecek olan, genellikle ikili biçimdeki veri kümesi olarak tanımlanır. Damga, tek bit kadar küçük veya orijinal içeriğin kendisindeki örnek sayısı kadar büyük olabilir. Bunun yanı sıra, telif hakkı bildirimi, gizli mesaj veya başka herhangi bilgi olabilir. Son olarak, taşıyıcı sinyale damgayı yerleştirmek için anahtar gerekli olabilir ve bu anahtar daha sonra damga verilerinin çıkarılması aşamasında kullanılabilir [1]. Şekil 1.1'de sayısal damgalamanın temel şeması yer almaktadır.



Şekil 1.1. Sayısal damgalama şeması

Sayısal damgalamada kullanılan taşıyıcı içeriğin türüne göre damgalama teknikleri sayısal metin damgalama, görüntü damgalama, ses damgalama ve video damgalama olarak sınıflandırılabilir.

- Sayısal metin damgalama: Metin verileri, kelime, cümle, satır, paragraf ve noktalama işareti vb. gibi farklı anlamsal varlıklardan oluşur. Metin damgalama farklı türlerde yapılabilir [2, 3]. Format ve yapısal tabanlı damgalamada metnin düzeni damga bitlerini gizlemek için değiştirilir. Genelde, cümle kaydırma, sözcük aralığı ve satır aralığı biçimleri arasındaki

küçük farklılıklara dayanan ve belge yapısını hafiften değiştiren damgalamadır. Dilbilimsel damgalamada söz dizimsel ve anlamsal olmak üzere iki farklı yaklaşım ele alınır. Söz dizimsel damgalamada, kümedeki kelimeler verileri gizlemek için manipüle edilir. Damga mesajını gizlemek için metin içeriğinin fiilleri, isimleri, sıfatları, zamirleri, edatları ve diğer gramer özellikleri kullanılır. Bu dilbilgisi değişiklikleri, metnin orijinal anlamını etkilemeden yapılır. Cümlelerdeki kelimelerin sırası da bitleri gizlemek için yeniden düzenlenebilir. Bu, metinin yapısını değiştirerek yapılabilir. Örneğin zarf ifadesinin yeri değiştirilebilir, özne eklenebilir veya cümle aktiften pasife çevrilebilir. Anlamsal tabanlı damgalamada, eşanlamlı kelimelerin değiştirilmesi veya cümlelerin dönüştürülmesi gibi anlamsal değişiklikler ile damga gömülür. Görüntü tabanlı yaklaşımda, bazı araştırmacılar, taranan metin belgeleri için metin damgalama algoritmalarını uygulamışlardır. Böyle bir durumda metnin görüntüsü damgalama işlemi sırasında kullanılır ve damgalama, uzaysal alanda yürütülür.

- Görüntü damgalama: Sayısal görüntü damgalamada sayısal damga, orijinal görüntünün içine yerleştirilir. Damga, metni, sahip adını veya ticari marka sembolü veya logosunu temsil eden bit dizisi olabilir. Gri seviye veya renkli görüntü damgalama için, damga gömme teknikleri, damgayı doğrudan parlaklık veya renk bileşenleri gibi orijinal görüntü verilerine veya algısal özelliklerden veya belirli sinyal manipülasyonlarına karşı dayanıklılıktan yararlanmak için orijinal verilerin bazı dönüştürülmüş sürümlerine eklemek için tasarlanmıştır.
- Ses damgalama: Ses damgalama üzerine yapılan araştırmaların çoğu, ya ses sinyalinin doğrudan damgalanması ya da sesin sıkıştırılmış bir formatta temsil edildiği bit akışı gömme üzerine odaklanmıştır. Algısal modellerin kullanımı ses için etkili ve kabul edilebilir damgalama şeması oluşturmada önemli bir bileşendir. Ses damgalama için gereksinimler, algılanamazlık (duyulmama) ve sıkıştırma, filtreleme ve A/D ve D/A dönüşümü gibi sinyal değişikliklerine karşı dayanıklılıktır [4].
- Video damgalama: Video damgalama, videoyu yasa dışı kopyalamadan korumak ve manipülasyonları tanımlamak için bir video dizisine damga yerleştirmeyi ifade eder. Video damgalama üzerine çalışmalar, sıkıştırılmış

alanda, uzaysal alanda ve dönüşüm alanında damgalama yapan teknikler şeklinde sınıflandırılabilir [5, 6]. Sıkıştırılmış alan damgalama tekniklerinde damga, MPEG-2, MPEG-4, H.264/AVC, H.265/HEVC gibi standartlar ile uyumlu kodlayıcılar kullanılarak oluşturulan kodlanmış bit akışına gömülür. Sıkıştırılmış video damgalamada çoğu zaman damganın, önemli ölçüde karmaşıklık ve ek gecikme sağlayan tam bir kod çözme, damgalama ve yeniden kodlama adımından geçmeden doğrudan sıkıştırılmış bit akışına gömülebilmesi arzu edilir [4]. Uzaysal alanda damga gömme, bir video çerçevesinin gömme kanalının piksel değerlerinin doğrudan değiştirilmesiyle elde edilir. Bu teknikler En Anlamsız Bit (EAB) tabanlı, blok tabanlı, istatistiksel tabanlı ve özellik noktası tabanlı yaklaşımlar şeklinde sınıflandırılabilir. Dönüşüm alanında damgalamada, damgayı yerleştirmeden önce, bir video dizisindeki bilgisayar çerçevesi yeni bir alana dönüştürülür. Damga gömme işlemi sırasında, dönüşüm alanı katsayıları damga tarafından değiştirilir ve ardından bu değiştirilmiş katsayılara ters dönüşüm uygulanarak damgalanmış çerçeve oluşturulur.

Sayısal damgalama giriş bölümünde genel hatlarıyla tanıtıldıktan sonra, bir sonraki bölümde sayısal damgalamanın hangi amaçlarla uygulandığına değinilmiştir.

1.2. Sayısal Damgalama Uygulamaları

Sayısal damgalama, son yıllarda yaygınlaşmış yeni bir alandır. Sayısal damga bilgileri metin, logo, kaotik dizi veya sayı dizisi olabilir. Bu damga bilgileri aşağıda detayları verilen telif hakkı koruma, kimlik doğrulama, parmak izi, kopya kontrolü, yayın izleme, dış müdahale algılama ve yerini belirleme gibi farklı uygulama alanlarında kullanılabilir [7, 8].

1.2.1. Telif Hakkı Koruma

Sayısal damgalamanın yaygın kullanım alanlarından biri, metin, resim, video ve ses ortamında telif hakkı koruma amacıyla gerçekleştirilmiş olanıdır. Telif hakkı koruma uygulamalarında sayısal damga, menşe, sahip, zaman damgası ve hatta bir logo veya ticari marka gibi telif hakkıyla ilgili bilgileri tanımlamak için tasarlanmıştır. Böylece içerik

güvenilmeyen ağ üzerinde dağıtıldığında, sahibinin haklarını korur. Bu tür telif hakkı koruması, damgalanmış içerikte meydana gelebilecek bozulmalar karşısında gömülü damganın çıkarılabilmesini mümkün kılmak için yüksek düzeyde dayanıklılık gerektirir. Ayrıca, damga gömüldüğünde içeriği, insan duyuları tarafından algılanamayacak şekilde değiştirmeli ve yetkisiz kullanıcılar tarafından dayanıklı damganın kasıtlı olarak kaldırılması içeriğin kalitesinde ciddi bozulmaya neden olmalıdır [9].

1.2.2. Kimlik Doğrulama

Bilgisayar teknolojisindeki ilerlemelerle, sayısal çoklu ortam içeriğinin manipülasyonu daha kolay hale gelmiştir ve buna bağlı olarak içeriğin orijinalliğinin belirlenmesi zorlaşmıştır. Damgalamada kimlik doğrulama, damgalanmış verilerin bütünlüğünü doğrulama ve verilerin tahrif edilmediğinden emin olma prosedürüdür. Bir içerik modifiye edilmemişse otantiktir denilebilir [10].

1.2.3. Parmak İzi

Parmak izi uygulamasında, damgalama yoluyla gömülen veriler, çoklu ortam dosyasının belirli bir kopyasının kaynağını veya alıcılarını izlemek için kullanılır. İnsanları ayırt etme bağlamında biyometrik özelliklerin benzersizliğini referans alan bu uygulamada, sayısal belgelere parmak izi ilkesi uygulanmıştır. Sayısal içeriği kötü niyetli saldırılardan korumak, sahte sayısal içeriği tespit etmek ve güvenli aktarımı sağlamak için damga şeklindeki sayısal parmak izleri uygulanabilir. Örneğin, farklı seri veya kimlik numaraları taşıyan sayısal damgalar, çok sayıda alıcıya dağıtılmadan önce çoklu ortam bilgilerinin farklı kopyalarına yerleştirilir. Parmak izi uygulamalarında uygulanan algoritmaların görünmez olması ve kasıtlı saldırılara ve kayıplı sıkıştırma veya filtreleme gibi sinyal işleme değişikliklerine karşı dayanıklı olmasının yanı sıra çarpışma saldırısına karşı da dirençli olmalıdır [11]. Yani, orijinal içeriğe birden fazla kimlik numarası gömmek imkânsız olmalıdır ki; farklı parmak izleri içeren aynı çoklu ortam dosyasına sahip bir kullanıcı grubu, parmak izini gizlice ele alıp doğrulayamasın. Bu tür damgalar ayrıca kriptografik yöntemlerle korunmalıdır [7].

1.2.4. Kopya Kontrolü

Burada ana fikir, sayısal formattaki veriyi yasadışı kopyalama ve çoğaltmaya karşı korumaktır. Kopya koruması için, damga bilgileri içeriğe gömülmeli ve bu içeriğin telif hakkıyla korunup korunmadığı tespit edilmelidir [12]. Sayısal çok yönlü disklere (DVD), ortamın görüntülenmesine izin verirken kaydedilmesini engellemek amacıyla yerleştirilen sayısal damga, hak sahibinin uygulamak istediği kullanım ve kopyalama kuralları hakkında bilgi içerir [13]. Bunlar genellikle "Asla kopyalanamaz", "Serbestçe kopyalanabilir", "Bir kez kopyalanabilir" veya "Artık kopyalanamaz" gibi basit kurallar olacaktır. [12]'de belirtildiğine göre kullanıcıların böyle bir ortamdaki sayısal veriyi kopyalayabilmesi için, uyumlu cihazlar önce kopya kontrol bilgilerini denetlerler. Ardından, damga "Serbestçe kopyalanabilir" ve "Bir kez kopyalanabilir" ise, buna izin verirler. Ancak "Bir kez kopyalanabilir" kuralına sahip içeriğin yasal kopyasının "Artık kopyalanamaz" durumunda olması gerekir. "Asla kopyalanamaz" ve "Artık kopyalanamaz" şartlarının geçerli olduğu ortamlarda ise çoğaltmaya müsaade edilmez.

1.2.5. Yayın İzleme

Bu tür izleme, özellikle reklamlarda, reklamını yaptıran müşterinin reklamlarının gerçekten doğru zamanda ve doğru sürede yayınlanıp yayınlanmadığını izlemek istediği durumlarda kullanılabilir. Bunun yanı sıra müzisyenler ve oyuncular, performanslarının yayınları hususunda doğru telif hakkı ödemeleri almak için veya telif hakkı sahipleri, mülklerinin korsan istasyonlar tarafından yasadışı olarak yeniden yayınlanmamasını sağlamak için yayın izlemeyi kullanabilirler [14]. Yapım şirketlerinin yasadışı yeniden yayın faaliyetlerini önlemesi önemlidir. Bu durumda, yayından önce her videoya veya ses klibine koyulan benzersiz bir damga yayın izleme için kullanılabilir. Otomatik izleme istasyonları daha sonra yayınları alıp bu damgaları arayarak her bir klibin ne zaman ve nerede göründüğünü belirleyebilir.

1.2.6. Dış Müdahale Algılama ve Yerini Belirleme

Dış müdahale algılama uydu görüntüleri veya tıbbi görüntüler gibi oldukça hassas verileri içeren bazı uygulamalar için çok önemlidir. Bu uygulama kimlik doğrulamayla yakından ilişkilidir. Eğer bir görüntüde dış müdahale algılanırsa, görüntünün orijinal olmadığı sonucuna varılır. Bundan sonraki aşama tahrif edilen bölgenin belirlenmesidir [10].

Yukarıda bahsedilen uygulamaların dışında sayısal damgalama iletişim iyileştirme, medya açıklaması, sayısal adli bilimi gibi uygulamalarda da kullanılmaktadır.

Şu ana kadar çeşitli çoklu ortam verilerinde sayısal damgalama uygulamalarına yer verilmiştir. Tez kapsamında, sayısal görüntüler taşıyıcı içerik olarak kullanıldığından bir sonraki bölümde sayısal görüntü damgalamaya değinilmiştir.

1.3. Sayısal Görüntü Damgalama

Sayılar matrisi olarak tanımlanabilen sayısal görüntüler ikili görüntü, gri seviye görüntü ve renkli görüntü olmak üzere sınıflandırılabilir. İkili görüntüler her bir pikselin 1 bit ile temsil edildiği siyah beyaz görüntülerdir. Gri seviye görüntüler grinin tonlarını içerir. Gri seviyelerin sayısı 2^n ile temsil edilir ki; burada n görüntünün bit derinliğini ifade eder [8]. Renkli görüntüler, her piksel için renk bilgilerini içeren sayısal görüntülerdir. Bir rengi temsil etmek için çoğu renk alanı üç bileşen kullanırken, üçten fazla özellik kullanan renk uzayları da mevcuttur. Üç bileşen ile rengin temsil edildiği RGB, YIQ, YCbCr, YUV gibi renk uzayları kullanıldığında, renkli pikseli temsil etmek için her kanal başına sekiz bit, dolayısıyla toplamda 24 bit gerekir. Sayısal görüntü damgalama sistemleri genellikle gri seviye ve renkli görüntüler üzerinde gerçekleştirilir.

Sayısal görüntü damgalama, tipik olarak iki ana süreçten meydana gelir: Kodlayıcı adı verilen damga gömme süreci ve kod çözücü adı verilen damga çıkarma süreci. Damga gömme sürecinde girişler orijinal görüntü, sayısal damga ve güvenlik anahtarıdır. Kodlayıcı, makine tarafından okunabilir kodu (damga), damga gömme algoritmaları yardımıyla görüntülere ekler. Neredeyse tüm damgalama prosedürleri, damga bilgisini uygun şekilde çıkarmak ve temel güvenliği garanti etmek için gömme ve çıkarma prosedürüne atanan özel anahtarlarla kontrol edilir [11]. Damga gömme sürecinin çıktısı, güvenlik anahtarı ve damgalanmış görüntüdür. Bir damga çıkarma süreci gömülü damgayı, damga içeren sinyalden çıkarır ve çıkarılan damga, orijinali ile karşılaştırılır.

Bir damgayı sayısal görüntü ile birleştirip damgalanmış görüntü (I^w) elde etmek için, orijinal görüntüye (I), gizlenecek veriye ait bilgileri içeren sayısal damgaya (W), güvenlik anahtarına (K) ve kodlama algoritmasına (E) ihtiyaç duyulur. Kodlayıcı, damgayı ve orijinal görüntüyü alır ve damgalanmış görüntüyü (1.1)'deki gibi oluşturur:

$$I^w = E(I, W, K) \tag{1.1}$$

Damga çıkarma algoritmasının girişleri, I^{wc} (damgalanmış ve muhtemelen bozulmuş görüntü) ve K'dir. I ve W'nun kullanımı ise damga çıkarma durumuna bağlı olarak belirlenir. (1.2)'de damga çıkarma prosedürü tanımlanmıştır. Burada $e(\cdot)$ damga çıkarma algoritmasını, W^* çıkarılan damgayı temsil eder.

$$W^* = e(I^{wc}, K, \dots) \tag{1.2}$$

Bu bölümde sayısal görüntü damgalama, genel hatlarıyla tanıtılmıştır. Sonraki bölümde ise sayısal görüntü damgalama sisteminde dikkate alınması gereken temel özelliklere değinilecektir.

1.4. Sayısal Görüntü Damgalama Gereksinimleri

Sayısal damgalama şemasını tasarlamak için bazı gereksinimlerin ya da özelliklerin göz önünde bulundurulması gerekir. Bu temel gereksinimler, istenen amaca ve uygulamaya bağlı olarak değişmektedir.

1.4.1. Algılanamazlık

Sayısal damgalama şeması için algılanamazlık ya da algısal şeffaflık (imperceptibility), uygulama amacına bağlı olmayan temel bir özelliktir [15]. Damgalanmış içerik ve orijinal içerik arasındaki benzerlik miktarı olarak tanımlanabilir. Sayısal damganın gömülmesi, orijinal içeriğin algısal kalitesini etkilememelidir. Görünmez damgalama uygulamalarında, gömülen veriler, orijinal içerikte hafif bozulmalara sebep olsa bile, insan gözü tarafından mümkün olduğunca fark edilemez olmalıdır.

Bir damgalama sisteminin algılanamazlığı çeşitli değerlendirme metrikleriyle ölçülebilir. Tepe Sinyal Gürültü Oranı (TSGO), bu ölçütlerden biridir. Damgalanmış görüntü ve orijinal görüntü arasındaki benzerlik arttıkça, TSGO da artar. TSGO'nun birimi dB'dir ve [16]'da ifade edildiğine göre, damgalanmış görüntünün TSGO değeri 30 dB'nin üzerindeyse insan gözü için kabul edilebilirdir. Gri seviye görüntüler için TSGO'nun hesaplanması (1.3)'te verilmektedir.

$$TSGO = 10\log_{10}\frac{MaksI^2}{OKH} \tag{1.3}$$

Burada $MaksI$, görüntünün maksimum parlaklık değeridir. OKH ise Ortalama Karesel Hatayı ifade etmektedir ve (1.4)'teki gibi hesaplanmaktadır.

$$OKH = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(\mathrm{i},\mathrm{j}) - \mathrm{I}^{w}(\mathrm{i},\mathrm{j})]^2 \tag{1.4}$$

Burada M ve N orijinal görüntünün boyutunu temsil ederken, I orijinal görüntüyü, I^w damgalanmış görüntüyü ifade eder.

Algılanamazlığı değerlendirmede kullanılan bir diğer metrik, Yapısal Benzerlik İndeksidir (YBİ). YBİ, her iki görüntünün yerel parlaklığını, kontrastını ve yapısını ayrı ayrı değerlendirir ve ardından genel değerlendirmeyi elde etmek için tüm yerel değerlendirmelerin ortalamasını alır [17]. YBİ aralığı [0, 1]'dir ve 1 değeri, orijinal ve referans görüntülerin aynı olduğu anlamına gelir. YBİ, (1.5)'teki gibi hesaplanır.

$$YB\dot{I} = \frac{(2\mu_I\mu_{I^w} + C_1)(2\sigma_{II^w} + C_2)}{(\mu_I^2 + \mu_{I^w}^2 + C_1)(\sigma_I^2 + \sigma_{I^w}^2 + C_2)} \tag{1.5}$$

Burada I ve I^w sırasıyla orijinal ve damgalanmış görüntüleri temsil etmektedir. μ_I ve $\mu_I w$, I ve I^w'ya ait ortalama parlaklık değerini; σ_I ve $\sigma_I w$, I ve I^w'ya ait standart sapmayı; $\sigma_{II}w$, I ve I^w arasındaki kovaryansı ve C_1 ve C_2, 1'den çok küçük sabit değerleri ifade etmektedir.

İnsan Görsel Sisteminin (İGS) özelliklerine dayalı bir görüntü değerlendirme metriği ise Görsel Bilgi Doğruluğudur (GBD). GBD, referans görüntü (I) ile bozulmuş görüntü (I^w)

arasındaki karşılıklı bilgiyi referans görüntüde bulunan bilgilere göre nicelleştiren bilgi doğruluğu kriteri olarak modellenmiştir [18]. GBD, ilk olarak görüntüyü birkaç alt bant halinde ayrıştırır ve her alt bandı bloklara ayırır. Daha sonra GBD, her blokta ve her alt bantta farklı modellerde karşılıklı bilgileri hesaplayarak görsel bilgileri ölçer. Son olarak, görüntü kalitesi değeri, tüm bloklar ve tüm alt bantlar için görsel bilgilerin entegre edilmesiyle ölçülür [19]. GBD indeksi aralığı [0,1]'dir. Bu değer arttıkça görüntünün kalitesi de artmış olacaktır.

1.4.2. Dayanıklılık

Bir damgalama sisteminin dayanıklılığı (robustness), damganın dışarıdan yapılabilecek çeşitli saldırılara karşı direnme yeteneği olarak ifade edilebilir. Bu saldırılar arasında ölçekleme, döndürme, görüntü çevirme gibi geometrik ataklar, kayıplı sıkıştırma, filtreleme, gürültü ekleme, histogram eşitleme gibi yaygın sinyal işleme atakları yer almaktadır. Damgalanmış görüntü, bu saldırılara maruz kalsa bile damganın damgalanmış içerikten başarılı bir şekilde çıkarılması gerekmektedir. Kırılgan olması için özel olarak tasarlanmış damgalar dışında, dayanıklılık önemli bir konudur. Bir damgalama sisteminin dayanıklılık performansı çeşitli metriklerle ölçülebilir. Bunlar arasında Normalleştirilmiş Korelasyon (NK), Bit Hata Oranı (BHO), Bit Doğrulama Oranı (BDO) yer almaktadır. NK, orijinal damga ve çıkarılan damga arasındaki benzerliği ölçmek için kullanılır. Herhangi bir damgalama şemasının dayanıklılığı, NK değeri 1'e yaklaştıkça artar. NK, (1.6) yardımıyla hesaplanır.

$$NK = \frac{\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left(W(i,j)\times W^{*}(i,j)\right)}{\sqrt{\sum_{i=1}^{N1}\sum_{j=1}^{N2}W(i,j)^{2}}\sqrt{\sum_{i=1}^{N1}\sum_{j=1}^{N2}W^{*}(i,j)^{2}}} \tag{1.6}$$

Burada N1 ve N2 gömülen damga boyutunu, W gömülen damga bilgisini, W^{*} ise çıkarılan damga bilgisini ifade etmektedir.

BHO, damga bilgisinin ikili formatta olduğu durumda kullanılır. Yanlış çıkarılan bit sayısının gömülen toplam bit sayısına oranıdır. Değeri 0'a yaklaştıkça çıkarılan damga bitlerinin doğruluğu artar.

$$BHO = \frac{\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left(W(i,j)\oplus W^{*}(i,j)\right)}{N1\times N2} \tag{1.7}$$

BDO, da BHO gibi gömülen damganın ikili formatta olduğu durumlarda kullanılır. (1.8)'de verildiği gibi tanımlanan BDO, çıkarılan damganın doğruluk oranını ölçmek için kullanılır.

$$BDO = \frac{\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left(\overline{W(i,j)\oplus W^{*}(i,j)}\right)}{N1\times N2} \tag{1.8}$$

1.4.3. Güvenlik

Damgalama gereksinimlerinden bir diğeri de güvenliktir. Güvenli bir damgalama sistemi, damga gömme ve çıkarma algoritması bilgisine sahip olmayan, yetkisiz bir tarafın damga bilgisine erişmesini engellemelidir. Diğer bir deyişle, damgalama sistemine yönelik düşmanca ataklara karşı direnebilmelidir [20]. Düşmanca ataklar, damganın yetkisiz kaldırılması, yetkisiz algılanması ve yetkisiz gömülmesi şeklindeki ataklar olarak sınıflandırılabilir. Bunlar arasında, yetkisiz kaldırma ve yetkisiz gömme orijinal içeriği değiştirmesi dolayısıyla aktif atak iken, yetkisiz algılama pasif atak olarak tanımlanabilir.

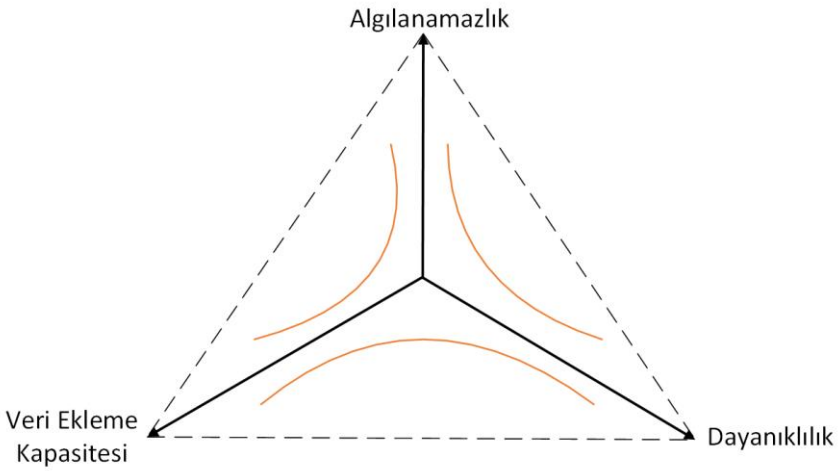
1.4.4. Hesaplama Maliyeti

Bir orijinal görüntüye damga yerleştirmenin ve damgalanmış görüntüden damgayı çıkarmanın hesaplama maliyeti minimum olmalıdır [21]. Hesaplama maliyetini düşürmek için, bir damgalama yöntemi daha az karmaşık olmalıdır. Yüksek karmaşık algoritmalara sahip damgalama yöntemleri, daha fazla donanım kaynağı gerektirmesinin yanı sıra damga gömme ve çıkarma için gereken zamanı da artıracaktır. Hesaplama basitliği, genellikle mobil cihazlar gibi kaynakların sınırlı olduğu ortamlarda tercih edilir [10].

1.4.5. Kapasite

Bir damgalama sisteminde veri yükleme kapasitesi, orijinal içeriğe eklenebilecek maksimum veri miktarıdır [22]. Kapasite, damgayı ekledikten sonra taşıyıcı görüntünün taşıdığı bit sayısı ile tanımlanır ve uygulamaya bağlı olarak değişebilir. Örneğin, kopya koruma uygulamalarında, genellikle az miktarda verinin gömülmesi yeterli olurken, kırılgan veya yarı kırılgan yapıya sahip olan bütünlük kontrolü damgalama şemaları yüksek gömme kapasitesi gerektirir.

Şekil 1.2'de gösterildiği gibi dayanıklılık, algılanamazlık ve veri ekleme kapasitesi damgalama şemalarının uyumsuz üç özelliğidir. Şöyle ki bu üç gereksinimden birinin iyileştirilmesi diğer ikisinin kötüleşmesine sebep olacaktır. Örneğin, bitlerin orijinal içeriğe gömülmesi, orijinal içeriğin bazı özelliklerinin değiştirilmesini gerektirdiğinden, algılanamazlığı etkilemektedir. Özellikle gömme kapasitesi fazla olan bir sistem tasarlamak genellikle damgalanmış görüntüde daha fazla bozulmaya neden olur ve bu nedenle çoğu zaman yüksek algılanamazlığı sağlamayı zorlaştırır. Bunun yanı sıra damganın büyük boyutlu olması saldırılar karşısındaki dayanıklılığı olumsuz etkilemektedir. Bu nedenle algılanamazlık şartını minimum düzeyde sağlayacak, dayanıklılığı azaltmayacak ve yüksek oranda veri eklemeye izin verecek şekilde bir sistem tasarlanmalıdır.



Şekil 1.2. Algılanamazlık, dayanıklılık ve kapasite arasındaki ödünleşim üçgeni

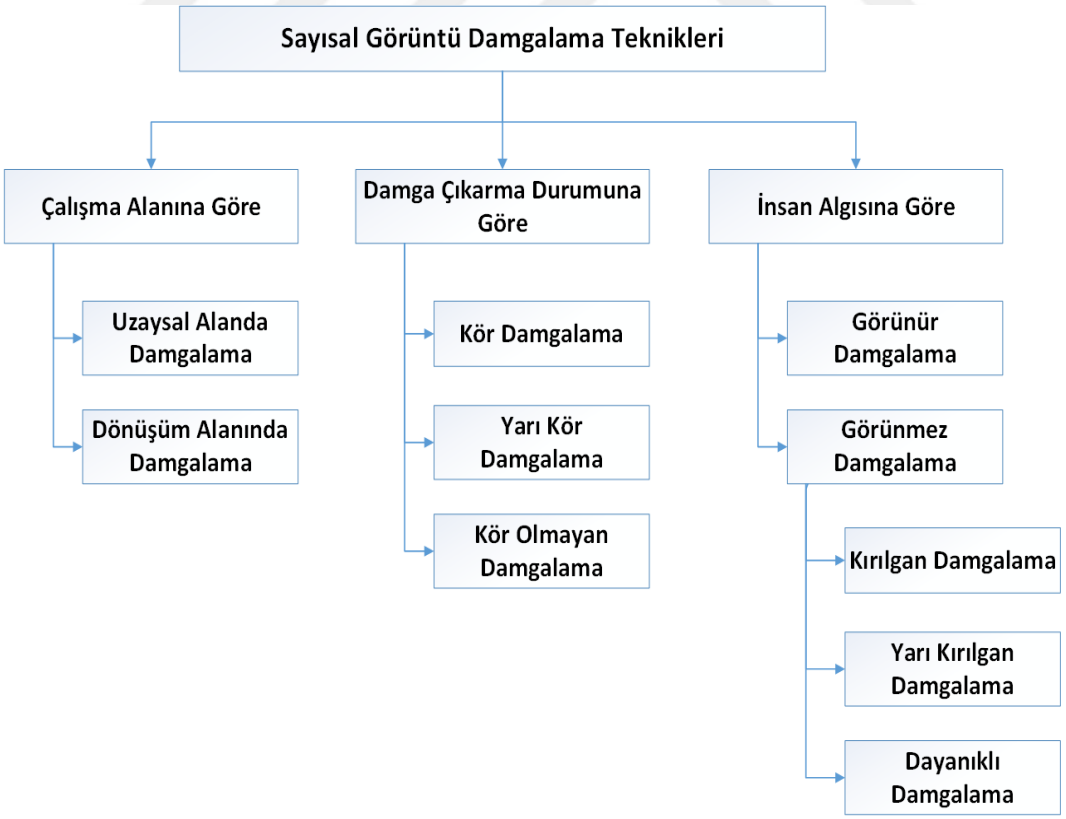
Bu bölümde temel sayısal görüntü damgalama gereksinimleri tanıtılmıştır. Sonraki bölümde ise sayısal görüntü damgalama teknolojilerinin farklı alanlara göre sınıflandırılması ele alınmaktadır.

1.5. Sayısal Görüntü Damgalama Tekniklerinin Sınıflandırılması

Sayısal görüntü damgalama, sayısal görüntüleri yetkisiz erişim ve değişikliklerden korumak için kullanılan bir tekniktir. Bu teknikler çalışma alanına, damga çıkarma durumuna ve insan algısına göre Şekil 1.3'te gösterildiği gibi farklı sınıflara ayrılır [23, 24].

1.5.1. Çalışma Alanına Göre Sınıflandırma

Sayısal görüntü damgalama teknikleri damgalamanın gerçekleştiği alana göre uzaysal alanda damgalama ve dönüşüm alanında damgalama olmak üzere iki sınıfa ayrılır.



Şekil 1.3. Sayısal görüntü damgalama tekniklerinin sınıflandırılması

1.5.1.1. Uzaysal Alanda Damgalama

Bir görüntünün uzaysal temsili x ve y koordinatlarını içeren uzayın bir fonksiyonudur. Uzaysal alanda damgalama teknikleri direk olarak taşıyıcı görüntünün x ve y koordinatlarında yer alan piksel değerleri üzerinde çalışır. Damga piksel değerlerinin değiştirilmesiyle gömülebilir. Dolayısıyla herhangi bir görüntüye kolayca uygulanabilir. Bu tekniklerin üstünlüğü, uygulamasının kolay olması, çok düşük hesaplama maliyetine sahip olması, daha az karmaşıklık gerektirmesi ve daha az zaman alması şeklinde sıralanabilir [25]. Bu sınıftaki yöntemlerin ilgi odağı olmasının sebebi, dayanıklılık, kapasite ve algılanamazlık arasında optimum ödünleşimin nasıl elde edileceğine dair daha iyi bir sezgi sağlamasıdır [11, 21]. Söz konusu tekniğin en ciddi problemi ise, dayanıklılığının zayıf olmasıdır.

Uzaysal alanda damgalama için çeşitli yöntemler kullanılmaktadır. Bunlar arasında renkli veya gri tonlamalı bir görüntüdeki belirli piksellerin parlaklık değerlerinin en düşük sıralı bitine damganın gömüldüğü EAB tekniği, en yaygın olarak kullanılan [21] ve görünmez sayısal damgalama için en basit [25] olanıdır. Gömülecek verinin her bir biti, orijinal görüntünün her pikselindeki en anlamsız bit ile değiştirilir ve damgalanmış görüntü elde edilir. Damga çıkarma da yine aynı yolla yapılır. En anlamsız bitler, daha önemsiz bilgileri taşır ve bu nedenle, orijinal görüntünün kalitesini çok etkilemez. Orijinal görüntü üzerinde ihmal edilebilir bir etki ile yüksek algısal şeffaflık sağlar. Ancak bu algoritma istenmeyen gürültü, kırpma, kayıplı sıkıştırma ve benzeri saldırılardan etkilenebilir ve bir bilgisayar korsanı tarafından tüm en anlamsız bitler 1 yapılarak, gömülü damga herhangi bir zorluk çekilmeden kolayca saldırıya uğrayabilir [21]. Şekil 1.4 gizli mesajın EAB tekniği ile bir görüntü bloğundaki piksellere gömülmesini göstermektedir. Şekilden de görüldüğü üzere piksel parlaklık değeri ikili forma dönüştürüldüğünde en anlamsız bit, o piksele gömülecek damga biti ne ise onunla değiştirilir. İkili piksel değerleri orijinal formuna tekrar dönüştürüldüğünde damgalanmış görüntü elde edilir. Bu damgalanmış görüntü, iletişim kanalı üzerinden alıcı uca iletilir. Alıcı uçta gizlenmiş mesaj en anlamsız bitlere bakılarak çıkarılabilir.

Şekil 1.4. EAB'nin gömme süreci

EAB tekniği ataklar karşısında dayanıklılığı garanti etmediği için alternatif bir yöntem olarak Orta Derecede Anlamlı Bit (OAB) tekniği damgalama sisteminin sağlamlığını artırmak ve kalitesini korumak için geliştirilmiştir. OAB farklı algoritmalar kullanılarak gerçekleştirilebilir. Bunlardan biri, bit düzlemi aralığının ortası ve kenarı arasında en iyi piksel değerini bularak klasik EAB tekniğini bu piksel üzerinde uygular. Bu yöntemde, damgalanmış görüntü çeşitli saldırılardan korunur ve damgalanmış görüntünün değiştirilmesi ihtimali en aza indirilir [26]. Başka bir çalışma [27], orijinal görüntünün her pikseline damga görüntüsünün seçilen iki bitinin gömüldüğü ve diğer altı bitin, orijinal pikseli doğrudan asimile edecek şekilde değiştirildiği ikili orta anlamlı bit modeline odaklanmıştır. Önerilen model, EAB yöntemlerine kıyasla daha yüksek görsel kaliteye sahiptir.

Yama işi (patchwork) tekniği, sözde rasgele istatistiksel modele dayanmaktadır [25]. Sözde rasgele seçim yardımıyla, görüntü iki parçaya bölünür ve biri A, diğeri B olarak adlandırılır. Yama A'daki bir nokta bir birim parlak yapılırken, yama B'deki nokta bir birim karartılır. Görüntüde dokunulması gereken noktaları belirlemek için, hem verici hem de alıcı tarafından paylaşılan gizli bir anahtarla beslenen sözde rasgele sayı üreteci kullanılır ki; kod çözme algoritması gömülü verileri çıkarmak için aynı sırayla aynı noktaları ziyaret edebilsin. Bu yöntem, rastgele doku içeren geniş alanlar için uygundur ancak metin görüntüleri için uygun değildir [21].

1.5.1.2. Dönüşüm Alanında Damgalama

Uzaysal alanda damgalama dayanıklılık, kapasite ve algılanamazlık arasında optimal bir dengenin nasıl elde edileceği konusunda daha iyi sezgi sağladığı için ilgi çekicidir [11].

Ancak, uzaysal alan tekniklerinin en ciddi sorunu, dayanıklılığın zayıflığıdır. Verileri daha etkili bir şekilde gizleyebilen dönüşüm alanında (frekans alanı olarak da bilinir) damgalama teknikleri ise, Ayrık Kosinüs Dönüşümü (AKD), Ayrık Fourier Dönüşümü (AFD), Ayrık Dalgacık Dönüşümü (ADD) gibi farklı dönüşüm yöntemlerini kullanarak bir görüntüyü öncelikle farklı bir alana taşır. Ardından, orijinal görüntünün dönüşüm alanı katsayılarını değiştirerek damgayı gömer. Damgalanmış görüntü ters dönüşüm yardımıyla elde edilir. Dönüşüm alanında yaygın olarak kullanılan teknikler ve damgalamada yararlanılan matris dönüşümleri aşağıda alt başlıklar halinde incelenmektedir.

1.5.1.2.1. Ayrık Kosinüs Dönüşümü

AKD, sayısal sinyal işlemede en yaygın kullanılan doğrusal dönüşümlerden biri olan ortogonal dönüşüme dayanır [28]. AKD algoritması, orta düzeyde karmaşıktır ve enerji sıkıştırma konusunda iyi bir yeteneğe sahiptir. AKD alanında damgalama, gürültü, sıkıştırma, keskinleştirme ve filtreleme gibi saldırılara karşı dirençlidir. Standart JPEG sıkıştırmaya dayalıdır. AKD'nin özellikleri, katsayıların yüksek oranda ilintili olması ve bilgi içeriğinin büyük kısmının düşük frekans katsayılarında olmasıdır [29]. Bu özellikler hem gereksiz hem de alakasız bilgilerin azaltılmasını destekler. AKD bahsi geçen karakteristiğinden dolayı çoğu çalışma için tercih edilen dönüşüm olmuştur.

AKD, bir görüntünün farklı frekans bantlarına ayrıştırılmasına izin vererek damga bilgilerinin görüntünün frekans bantlarına gömülmesini kolaylaştırır. Gömme için genellikle orta frekans bantları tercih edilir. Bu durum, daha yüksek frekansları bozabilen saldırılara karşı dayanıklılığı artırır. Ayrıca, görüntünün enerjisinin çoğu düşük frekans katsayılarında yoğunlaştığından orta frekans bandı seçilerek, damgalanmış görüntünün görsel kalitesinde meydana gelebilecek bozulmanın indirgenmesi sağlanır. $M \times N$ boyutlu bir görüntü için, 2 boyutlu AKD şu şekilde ifade edilir:

$$F(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \qquad (1.9)$$

$$c(u)=\begin{cases}\dfrac{1}{\sqrt{2}}, & u=0\\ 1, & u=1,2,\ldots,M-1\end{cases} \tag{1.10}$$

$$c(v)=\begin{cases}\dfrac{1}{\sqrt{2}}, & v=0\\ 1, & v=1,2,\ldots,N-1\end{cases} \tag{1.11}$$

Ters AKD ise (1.12)'de verildiği gibi ifade edilmektedir:

$$f(x,y)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}c(u)c(v)F(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{1.12}$$

1.5.1.2.2. Ayrık Fourier Dönüşümü

AFD, örneklenmiş bir sinyalde bulunan frekansları analiz etmek için sinyal işlemede ve ilgili alanlarda yaygın olarak kullanılır [8]. Bir görüntüye AFD uygulandığında, genlik ve faz gösterimi elde edilir. Hem genlik hem de faz katsayıları damgayı gömmek için kullanılabilir. AFD'nin önemli bir özelliği, ötelemeye karşı değişmez olmasıdır [30]. Uzaysal kaymalar faz bileşenini etkilese de genliği etkilemez. Uzaysal alanda görüntünün dairesel olarak ötelenmesi AFD genliğini etkilemediği için, damganın bu alana gömülmesi ötelemeye karşı değişmezlik sağlayacaktır [22]. AFD'nin bir başka avantajı da, kırpma ataklarına karşı etkili olmasıdır [30]. $M \times N$ boyutlu bir $f(x,y)$ görüntüsünün AFD ve ters AFD denklemleri sırasıyla (1.13) ve (1.14)'teki gibi hesaplanır:

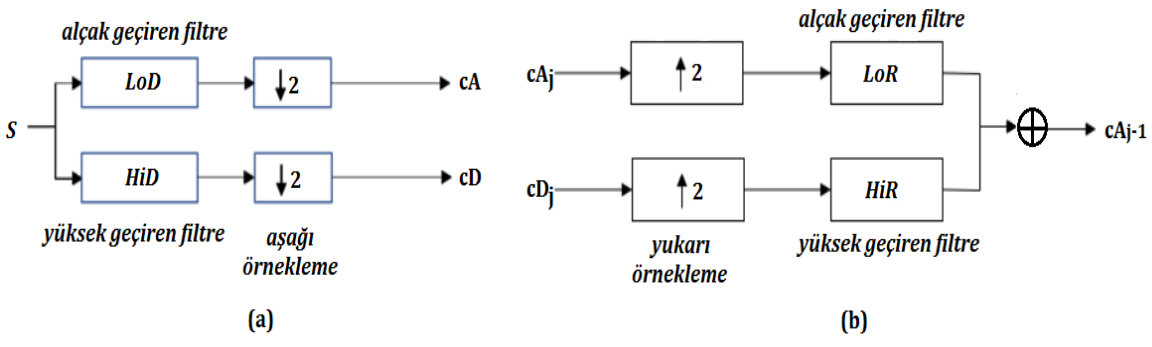
$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)e^{-2\pi j\left(\frac{ux}{M}+\frac{vy}{N}\right)}=R(u,v)+jI(u,v) \tag{1.13}$$

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)e^{2\pi j\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{1.14}$$

Burada, $R(u,v)$ ve $I(u,v)$ sırasıyla Fourier dönüşümünün reel ve sanal kısmını ifade etmektedir. AFD'nin çıktısının karmaşık değerler içermesi ve hesaplama verimliliğin düşük olması bu tekniğin temel dezavantajıdır.

1.5.1.2.3. Ayrık Dalgacık Dönüşümü

Dalgacık Dönüşümü, bir sinyalin zaman-frekans temsilini veren bir dönüşümdür [31]. Dalgacık Dönüşümü, farklı frekansların farklı çözünürlüklerle analiz edildiği çoklu çözünürlük tekniğini kullanır [31]. Alt bant kodlamaya dayanan ADD ise, hızlı bir dalgacık hesaplaması sağlamaktadır. ADD, çoklu çözünürlük özellikleri, üstün İGS modellemesi ve mükemmel zaman frekansı analizi nedeniyle diğer teknikler arasında en iyi dönüşüm alanı tekniği olarak kabul edilebilir ve sinyal işleme amaçları için geniş ölçekte kullanılır [31, 32]. ADD, bir giriş sinyali S'yi iki katsayılı kümeye ayırır. ADD'nin merkezinde bir çift filtre vardır: Alçak geçiren ve yüksek geçiren filtre. Alçak geçiren filtrede sinyalin geçirilmesiyle yakınlık katsayıları cA (düşük frekanslar) üretilir. cD katsayıları (yüksek frekanslar) ise yüksek geçiren filtre boyunca sinyalin geçirilmesinin ardından aşağı örnekleme işlemi yapılarak üretilir. Ters ADD işlemi, bu bileşenleri kullanarak bilgi kaybı olmadan orijinal sinyali yeniden oluşturur veya sentezler [33]. Şekil 1.5'te bir-boyutlu sinyalin bir-seviye ADD ile ayrıştırılması ve ayrıştırılan sinyalden orijinal sinyalin oluşturulması aşaması resmedilmiştir.

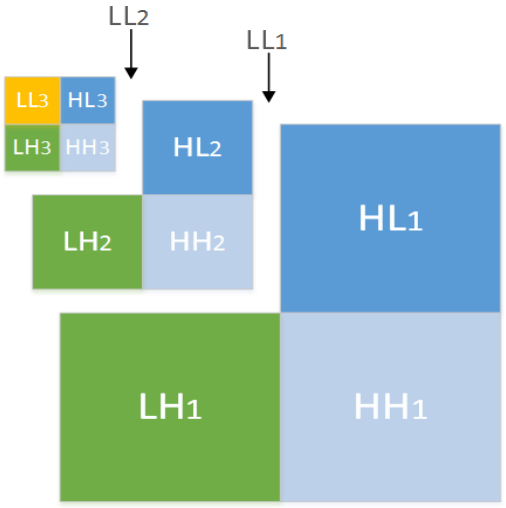


Şekil 1.5. ADD ve ters ADD şeması: a) 1-seviyeli ADD ile bir sinyalin ayrıştırılması b)Ters ADD ile bir sinyalin yeniden oluşturulması

Çoğu doğal görüntüde, düzgün renk değişimleri ve bunlar arasında yer alan ve keskin kenarlar olarak gösterilen ince detaylar mevcuttur. Teknik olarak, görüntüdeki düzgün renk

değişimleri düşük frekans bileşenleri, keskin değişimler ise yüksek frekans bileşenleri olarak adlandırılabilir. Düşük frekans bileşenleri bir görüntüyü tanımlayan en önemli kısımları temsil ederken, yüksek frekans bileşenleri daha az önemli olan detay katsayılarını içerir. İki-boyutlu dalgacık dönüşümünde ilk olarak, alçak geçiren filtre her veri satırı için uygulanır, böylece satırın düşük frekanslı bileşenleri elde edilir. Ancak alçak geçiren filtre yarım bantlı bir filtre olduğundan, çıkış verileri yalnızca orijinal frekans aralığının ilk yarısındaki örnekleri içerir. Ardından, yüksek geçiren filtre her veri satırı için uygulanır ve yüksek geçiş bileşenleri ayrıştırılır. Tüm satırlar için bu işlemler tamamlandıktan sonra, üretilen düşük frekanslı ve yüksek frekanslı verilerin her sütunu için filtreleme yapılır. Böylece iki-boyutlu giriş görüntüsünden LL (düşük-düşük), HL (yüksek-düşük), LH (düşük-yüksek) ve HH (yüksek-yüksek) olarak etiketlenmiş dört alt bant elde edilir. LL bant bir kez daha aynı şekilde ayrıştırılabilir ve böylece daha fazla alt bant üretilebilir. Şekil 1.6 iki boyutlu bir sinyalin 3-seviye ADD ile ayrışmasını göstermektedir.

Bir görüntü dalgacık dönüşümüne tabi tutulduğunda, her bir ayrışma seviyesinde, ADD katsayılarının genliği düşük frekanslı bantta (LL), diğer üç banda (LH, HL ve HH) kıyasla daha büyüktür. Görüntü enerjisinin çoğu düşük frekanslı alt bantta yoğunlaştığından damgayı düşük frekanslı alt bantlara gömmek, görüntüde algısal değişikliklere neden olur ancak dayanıklılığı artırır. Yüksek frekanslı alt bantlara gömmek ise damganın dayanıklılığını olumsuz etkiler.



Şekil 1.6. 2-boyutlu 3-seviye ADD ile sinyalin alt bantlarına ayrıştırılması

1.5.1.2.4. Contourlet Dönüşümü

Contourlet Dönüşümü (CD), pürüzsüz konturları ve dokuları içeren 2D sinyalleri verimli bir şekilde temsil edebilir ve konturun pürüzsüzlüğünü tanıyamayan dalgacık dönüşümünün dezavantajının üstesinden gelebilir [34-36]. CD aynı zamanda çoklu ölçek, zaman-frekans lokalizasyonu gibi dalgacık dönüşümüne benzer özelliklere de sahiptir. CD iki ana adıma ayrılabilir: Laplacian Piramidi (LP) ayrışması ve Yönlü Filtre Bankaları (YFB) ayrışması. LP şeması, alçak geçiren filtreleme ve aşağı örnekleme kullanılarak çok ölçekli bir ayrıştırma elde etmek için kullanılır [35]. Bir görüntü LP ayrıştırma ile alçak geçişli görüntüye ve bant geçişli görüntüye ayrıştırıldıktan sonra her bant geçiş görüntüsü YFB adımıyla daha da ayrıştırılır [34]. YFB, yüksek frekans bilgilerini içeren pürüzsüz konturlar ve yönlü kenarları yakalamak için tasarlanmıştır. Çok çözünürlüklü ve çok yönlü ayrıştırma, alçak geçişli görüntü için yukarıda belirtilen aynı adımların tekrarlanmasıyla elde edilebilir.

1.5.1.2.5. Matris Dönüşümleri

Bu bölümde, sayısal damgalamada yararlanılan matris dönüşümlerinden Tekil Değer Ayrıştırma (TDA), QR Ayrıştırma ve Schur Ayrıştırma detaylı olarak incelenmiştir.

1.5.1.2.5.1. Tekil Değer Ayrıştırma

TDA, birçok uygulamada tercih edilen sayısal analiz tekniğidir. Görüntü damgalama, görüntü gizleme, görüntü sıkıştırma ve gürültü azaltma gibi görüntü işleme uygulamalarında yaygın olarak kullanılmaktadır [37, 38]. A, $M \times N$ boyutlu bir görüntü olsun. Bu görüntünün TDA'sı şu şekildedir:

$$A = U \times S \times V^T \tag{1.15}$$

$$U = [u_1, u_2, \ldots, u_M] \tag{1.16}$$

$$V = [v_1, v_2, \ldots, v_N] \tag{1.17}$$

$$S = \begin{bmatrix} s_1 & 0 & \cdots & 0 \\ 0 & s_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & s_n \end{bmatrix} \tag{1.18}$$

Burada U ve V, sırasıyla $M \times M$ boyutlu ve $N \times N$ boyutlu ortogonal matrislerdir. U ortogonal matrisinin sütunları sol tekil vektörü temsil eder. V'nin sütunları ise sağ tekil vektörü temsil eder. Sol tekil vektörler AA^T'in öz vektörleri, sağ tekil vektörler A^TA'nın öz vektörleridir. S ise $M \times N$ boyutlu tekil değerlerin tutulduğu diyagonal matristir. TDA'nın görüntü işlemede genişçe kullanılması onun aşağıda belirtilen özelliklerinden kaynaklanmaktadır [37-39].

- Bir görüntünün tekil vektörleri (U ve V) görüntünün geometrisini belirler. Sol tekil vektör yatay detayları temsil ederken, sağ tekil vektör dikey detayları temsil eder. Bunun yanı sıra, tekil değerler görüntünün cebirsel özelliklerini, parlaklığını (luminance) belirler.
- Tekil değerlerdeki hafif değişimler görüntünün algısal kalitesini değiştirmez.
- Tekil değerler azalan sırada sıralanmıştır ve birinci tekil değerle kıyaslandığında onların çoğu çok küçük kalmaktadır. Yeniden oluşturma adımında bu küçük değerleri göz ardı etmek ya da güncellemek görüntü kalitesinde çok hafif ve önemsiz değişimlere sebep olur.
- TDA, kare ve dikdörtgen matrislere uygulanabilir.

1.5.1.2.5.2. QR Ayrıştırma

Bir matrisin QR Ayrıştırması (QR çarpanlarına ayırma olarak da adlandırılır), matrisin ortogonal bir matrise ve üçgensel bir matrise ayrıştırılmasıdır [40]. Reel sayılardan oluşan bir kare matris A'nın QR Ayrıştırması şu şekilde formüle edilir:

$$A = QR \tag{1.19}$$

Burada Q ortogonal matristir (yani $Q^TQ = I$) ve R üst üçgensel bir matristir. A tekil değilse, bu çarpanlara ayırma benzersizdir.

QR Ayrıştırmayı hesaplamak için çeşitli yöntemler vardır. Bu yöntemlerden biri Gram-Schmidt sürecidir. Gram-Schmidt işlemi, ortogonal olmayan bir temelden ortogonal bir temel bulmak için kullanılır. Ortogonal bir temel, daha fazla hesaplama ve genişletme için arzu edilen birçok özelliğe sahiptir. Aşağıdaki gibi n sütun vektörü içeren A matrisi düşünülsün:

$$A = [a_1 \mid a_2 \mid \ldots \mid a_n] \tag{1.20}$$

Burada, a_n, matrisin doğrusal olarak bağımsız bir sütun vektörüdür. Gram-Schmidt işlemi, her sütun vektörü a_n için ortogonal bir projeksiyon (q_n) bulur ve daha sonra yeni projeksiyonları, önceki projeksiyonları (q_i) çıkararak oluşturur. Elde edilen vektör daha sonra birim vektör üretmek için bu vektörün uzunluğuna bölünür. Gram-Schmidt işlemi, önce birinci sütun vektörü a_1'in ortogonal projeksiyonunu bularak sürece devam eder.

$$u_1 = a_1,\ e_1 = \frac{u_1}{\|u_1\|} \tag{1.21}$$

a_1 ilk sütun vektörü olduğundan, çıkarılacak önceki projeksiyon yoktur. u_2 ikinci sütun a_2'den sütun vektörü üzerindeki bir önceki projeksiyonun çıkarılmasıyla elde edilir.

$$u_2 = a_2 - proj_{u_1}(a_2) = a_2 - (a_2 \cdot e_1)(e_1), e_2 = \frac{u_2}{\|u_2\|} \tag{1.22}$$

Süreç n. sütun vektörüne kadar devam eder. Burada her artımlı adım k + 1 şu şekilde hesaplanır:

$$u_{k+1} = a_{k+1} - (a_{k+1} \cdot e_1)(e_1) \ldots - (a_{k+1} \cdot e_k)(e_k), e_{k+1} = \frac{u_{k+1}}{\|u_{k+1}\|} \tag{1.23}$$

Denklemde $\|\cdot\|\ L_2$ normu ifade etmektedir: Böylece A matrisi QR matrisine aşağıdaki gibi ayrıştırılır:

$$A=[a_1\,|\,a_2\,|\ldots|\,a_n]=[e_1\,|\,e_2\,|\ldots|\,e_n]\begin{bmatrix} a_1\cdot e_1 & a_2\cdot e_1 & \ldots & a_n\cdot e_1 \\ 0 & a_2\cdot e_2 & \cdots & a_n\cdot e_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n\cdot e_n \end{bmatrix}=QR \tag{1.24}$$

Burada, "$\cdot$" iç çarpımı ifade eder. QR Ayrıştırma sonucu elde edilen R matrisinin iyi bir özelliği A'nın sütunları birbiriyle ilişkili olduğunda, ilk satırının elemanlarının mutlak değerinin diğer satırlardaki elemanların mutlak değerinden muhtemelen çok büyük olmasıdır [41]. Bir görüntüdeki küçük boyutlu blokların sütunları da genellikle birbiriyle ilişkili olduğundan, R matrisinin sadece ilk satırının değeri vardır. Diğerleri neredeyse 0'dır. Damgayı gömmek için başka satırların seçilmesi, damgalanmış görüntüde uygun olmayan önemli görsel bozulmaya sebep olacaktır. Dolayısıyla, algısal kalite açısından damganın R matrisinin ilk satır elemanlarına yerleştirilmesi avantaj sağlayacaktır.

1.5.1.2.5.3. Schur Ayrıştırma

Schur Ayrıştırma sayısal lineer cebirde önemli bir araçtır. Elemanları reel sayılardan oluşan A kare matrisi, (1.25)'teki gibi Schur Ayrıştırma ile U ve V matrislerine ayrıştırılabilir [42].

$$\begin{aligned} &A=U\times V\times U^T \\ &A=\begin{bmatrix} \vdots & & \vdots \\ b_1 & \cdots & b_n \\ \vdots & & \vdots \end{bmatrix}\times V\times\begin{bmatrix} \vdots & & \vdots \\ b_1 & \cdots & b_n \\ \vdots & & \vdots \end{bmatrix}^T \end{aligned} \tag{1.25}$$

Burada, U üniter matrisi ifade eder. V ise üst üçgensel matristir ve diyagonal elemanları gerçek öz değerlerden oluşmaktadır.

Schur Ayrıştırmada üniter matris, hesaplama matrisi işlevlerini daha kolay ve daha az karmaşık hale getirir [43]. Bundan dolayı, Schur Ayrıştırma matematikte matris üstel

değerlerini hesaplamak için kullanılır. Ayrıca, simetrik olmayan öz değerlerin ayrışmasını hesaplamak için de yararlanılır. Schur Ayrıştırma, TDA'da önemli bir ara adımdır [44]. [45]'te Schur Ayrıştırma tabanlı damgalama şemalarının, TDA tabanlı sayısal damgalama algoritmalarının tüm avantajlarına sahip olduğu ifade edilmektedir. Ayrıca, Schur Ayrıştırma, TDA için gereken hesaplama sayısının yaklaşık üçte birini gerektirir [45]. Ancak, toplam hesaplama sayısındaki azalmanın aynı olması beklenmemelidir. Bunun temel nedeni, gömme ve çıkarma prosedürlerinin Schur Ayrıştırmanın yanı sıra başka işlemleri de içermesinden dolayıdır.

Sütun vektörü b_1'in elemanları arasında güçlü korelasyon vardır. b_1'in tüm elemanlarının işaretleri aynıdır ve değerleri birbirine çok yakındır. Bu durum, V matrisinin ilk sütununun her zaman maksimum öz değerlere sahip olduğu öncülüne dayanır. U matrisinin ilk sütunu, bu özelliğinden dolayı damga verilerinin gizlenmesi için cazip hâle gelmiştir [42].

1.5.2. Damga Çıkarma Durumuna Göre Sınıflandırma

Damgalama şemaları, damga çıkarma moduna göre 3 ayrı sınıfa ayrılır. Bunlar kör olmayan, yarı kör ve kör damgalama sistemidir. Kör olmayan (non-blind) bir damgalama sistemi, damga bilgisini çıkarmak için orijinal içeriğin kod çözme aşamasında mevcut olmasını gerektirir. Dolayısıyla daha iyi dayanıklılık garanti eder, daha düşük hata olasılığına ve daha yüksek kapasiteye sahiptir [46, 47]. Ancak, gerçek dünyada orijinal verilerin her zaman garanti edilmediği göz önünde bulundurulursa, uygulama alanı kısıtlıdır [48]. Kör olmayan damgalama sisteminin bir başka dezavantajı da birden fazla sahiplik iddiasına yol açabilmesidir [47].

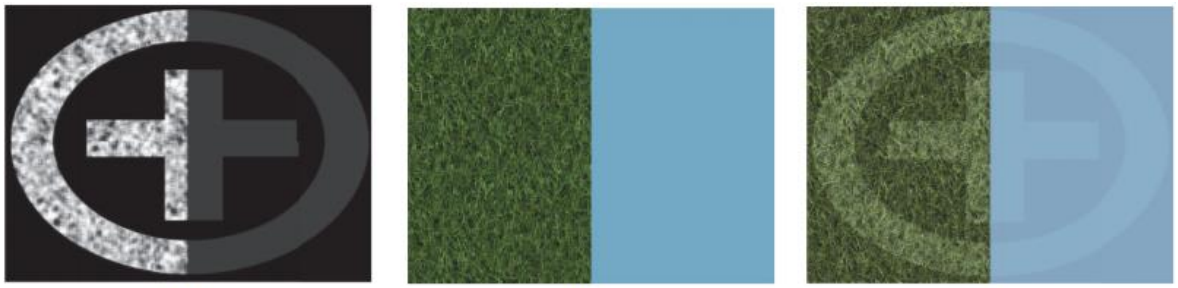
Yarı kör (semi-blind) damgalama yöntemleri, damga çıkarma adımında orijinal görüntüyü gerektirmezler ancak orijinal görüntünün bazı özelliklerine ihtiyaç duyarlar [49]. Bu tür damgalama sahiplik kanıtlama ve kopya kontrolü amacıyla kullanılabilir [48].

Kör (blind) damgalama sistemleri, orijinal görüntüyü ve damganın kendisini damga çıkarma aşamasında gerektirmediğinden daha popülerdir. Kör damgalama, orijinal görüntülerin depolanmasına ihtiyaç duymadığından, kör olmayan sistemlere kıyasla daha az maliyete ve bellek yüküne sahiptir [50]. Kör damgalamanın dezavantajı, damgalanmış görüntü ciddi şekilde yok edildiğinde, damganın tespitinin çok zor hale gelmesidir [47].

1.5.3. İnsan Algısına Göre Sınıflandırma

Sayısal damgalama sistemleri insan algısına göre görünür (visible) ve görünmez (invisible) damgalama sistemleri olmak üzere sınıflandırılabilir. Görünür damgalama, damganın bir gözlemci tarafından algılanabileceği şekilde taşıyıcı içeriğe gömülmesi işlemidir. Örneğin, sahiplik ile ilgili bir logonun insanların fark edeceği şekilde orijinal görüntüye yerleştirilmesiyle, telif hakkı koruması daha doğrudan ve anında gerçekleştirebilir [51]. Böylece, gizli anahtarlara veya ekstra bilgilere ihtiyaç duymadan içeriğin sahipliğini görsel olarak kanıtlamaya izin verir [52]. Görünür damgalamanın bazı özellikleri şöyle sıralanabilir [51]: i) Doku, kenar gibi orijinal görüntünün farklı özelliklere sahip tüm bölgelerinde algılanabilir olmalıdır. ii) Damga çok rahatsız edici olmamalıdır ki orijinal görüntünün ayrıntıları mükemmel şekilde tanınabilsin. iii) Damga gömme, orijinal görüntüyü engellememeli veya önemli ölçüde parlaklaştırmamalıdır ve damgalanmış alan İGS tarafından yeterince algılanabilmelidir. iv) Gömülü damga, yaygın saldırılara karşı sağlam olmalıdır.

Görünür damgalama örneği Şekil 1.7'de verilmiştir.



Şekil 1.7. Görünür damgalama örneği [51]: a) Sayısal damga b) Orijinal görüntü c) Damgalanmış görüntü

Görünmez damgalama sistemlerinde damga, görüntü üzerinde yapılan modifikasyonlar algısal olarak fark edilmeyecek ve yalnızca sahibi veya yetkili kullanıcı tarafından uygun bir kod çözme mekanizması ile kurtarılabilecek şekilde gömülür. Görünmez damgalama, orijinal içeriğin görsel kalitesini ciddi şekilde bozmamalıdır. Görünmez damgalama kendi içinde kırılgan (fragile), yarı kırılgan (semi-fragile) ve dayanıklı (robust) damgalama olmak üzere sınıflandırılabilir.

Kırılgan tekniklerde, damgalanmış görüntü değiştirilirse ve/veya saldırıya uğrarsa damga çıkarılamaz. Bu nedenle kimlik doğrulama, dış müdahale algılama ve yerini belirleme gibi uygulamalar için yararlıdır. Bir saldırı girişiminin kolayca tespit edilebilmesi amacıyla değişikliklere karşı düşük dayanıklılık (yüksek hassasiyet) sağlar. Kırılgan damgalamanın en önemli özellikleri algılanamaz olması, kırılganlığı ve yüksek veri yükleme kapasitesi sağlamasıdır [53].

Yarı kırılgan teknikler, kasıtlı ve kasıtsız müdahaleleri ayırt edebilme yeteneğine sahiptir [53]. Yarı kırılgan damgalama kimlik doğrulama ve dış müdahale algılamanın özel durumları için uygulanabilir [10]. Örneğin, geometrik bozulmalar kasıtlı saldırılar olarak vurgulanırken kayıplı görüntü sıkıştırma meşru değişiklikler olarak değerlendirilebilir.

Dayanıklı damgalama teknikleri, yalnızca sıkıştırma, gürültü ekleme, filtreleme gibi genel işlemlerde değil, aynı zamanda döndürme, ölçekleme, dönüştürme, kırpma ve benzeri geometrik saldırılarda da hayatta kalabilen damgalama algoritmasıdır. Genellikle telif hakkı koruma, parmak izi, kopya kontrolü ve yayın izleme için kullanılır. Burada teknik zorluk, birbiriyle çelişen gereksinimler olan algılanamazlığı ve dayanıklılığı sağlamaktır [4]. İdeal olarak, etkili, dayanıklı bir damgalama şemasında damga, yalnızca orijinal içerik yok edilirse ortadan kaldırılabilir. Orijinal içeriğin değerini değiştirmek için gereken dayanıklılık ve bozulma derecesi, uygulamaya bağlı olarak çeşitlilik gösterebilir.

1.6. Biyometrik Damgalama

Geleneksel sayısal damgalama yöntemlerinde, damga, sözde rasgele sayı dizisinden, ikili görüntülerden veya kaotik bir diziden oluşur. Bu durumda, damganın sahipliğini doğrulamak daha zor olacaktır. Böyle damgalar, gerçek sahiplikten yararlanmak veya belirsizlik durumu yaratan kimlik doğrulama sonuçlarını yok etmek için kolayca tahrif edilebilir veya taklit edilebilirler. Sahiplik talebinde bulunmak için damganın daha güvenli bir şekilde tanımlanması gerekir. Bir damganın fiziksel veya mantıksal sahipliği sorununu çözmek için biyometrik tabanlı güvenlik şemalarının kullanılması potansiyel bir çözümdür. Benzersiz ve kullanıcıya özgü biyometrik özellikler, yetkili ve yetkisiz kullanıcılar arasında ayrım yapma yeteneğine sahiptir [54-57]. Bu nedenle, damga olarak iris, parmak izi, yüz, avuç içi izi, imza vb. gibi kullanıcıya özgü özelliklerin kullanılması, içeriğin gerçek sahibi olduğunu iddia eden bir kişinin, gerçek sahip olup olmadığını belirlemek için kesinlikle kritik olacaktır. Hak sahibi olduğunu iddia eden kişi için gömülen biyometrik damga,

damgalanmış görüntüden çıkarılır ve veri tabanında tutulan diğer örneklerle karşılaştırılır. Bir eşleşme bulunursa, o zaman sahiplik kanıtlanmış olur.

İris tanıma, en güvenilir ve doğru biyometrik teknolojilerden biridir [58, 59]. [59]'da ifade edildiğine göre, ses tanıma, yüz tanıma ve el geometrisinin aksine, iris tanıma, kişinin kimlik doğrulaması hususunda daha yüksek düzeyde güvenlik sağlar. İris tanıma ile parmak izi karşılaştırıldığında, her ikisi de diğer biyometrik teknolojilere göre daha yüksek basitliğe, doğruluğa ve güvenilirliğe sahiptir. Parmak izi tarayıcıları iris tarayıcılara göre nispeten daha ucuzdur ve oldukça yaygındır. Ancak irisi oluşturan desenlerin kopyalanması parmak izi sahteciliğine kıyasla daha zordur. [59]'da belirtildiğine göre iki irisin tamamen aynı olacağına dair istatistiksel olasılık 1072'de 1 olarak öngörülmektedir. Ayrıca iris desenleri durağandır ve hasar görmedikçe değişmeden kalır. İkizlerin bile tamamen bağımsız iris modelleri vardır. Bu avantajlar, otantik bir kişiyi sahtekârdan ayırt etme hususunda iris tanımayı cazip hâle getirmiştir.

Mevcut biyometrik damgalama algoritmaları iki küme halinde kategorize edilmiştir. İlk sette, biyometrik modellerin bütünlüğünü korumak için biyometrik veriler başka bir biyometrik görüntüye gizlenir [36, 60, 61]. İkinci sette biyometrik veriler, fikri mülkiyet haklarını ve telif hakkını korumak için doğal görüntülere yerleştirilir. Literatürde konuşma sinyali [62, 63], parmak izi [64-66], yüz [67, 68], iris [69-73] ve imza [74] gibi çeşitli biyometrik verilerin mülkiyet haklarını korumak amacıyla damga olarak kullanıldığı çalışmalar mevcuttur. Bir sonraki bölümde hem bu çalışmaların hem de geleneksel damgalamaya yönelik sistemlerin yer aldığı literatür özeti sunulmaktadır.

1.7. Literatür Çalışması

Telif hakkı korumaya yönelik çoğu sayısal damgalama uygulamalarında, damganın gömme gücünü belirleyen ölçekleme faktörünün genellikle orijinal içerik ya da damga bilgisinden bağımsız olacak şekilde sabit bir değere atandığı görülmektedir. Oysaki ölçekleme faktörü telif hakkı koruma uygulamalarının temel iki özelliği olan algılanamazlık ve dayanıklılık üzerinde önemli bir etkiye sahiptir ve damgalamada orijinal içeriğin her bir bölümünün yapısını dikkate almayan tek ölçekleme faktörünün kullanılması birbiriyle çelişen bu özellikler üzerinde genellikle iyi sonuçlar üretmez. Dolayısıyla ölçekleme faktörünün söz konusu özellikleri dengede tutmak amacıyla güçlü bir algoritma tarafından optimize edilmesi gerekmektedir. O sebeple tez kapsamında öncelikle biyometrik

damgalama için temel teşkil eden ve gömülen bilginin içeriğinden (yani kullanıcıya özgü ayırt edici bir özelliği temsil etmesi ya da geleneksel bir damga olması) bağımsız olarak optimal ölçekleme faktörlerinin saptanmasına yönelik gerçekleştirilen geleneksel damgalamaya odaklanılmıştır. Bu nedenle literatürdeki çalışmalar geleneksel damgalama ve biyometrik damgalama teknikleri olmak üzere aşağıda iki başlık altında incelenmiştir.

1.7.1. Geleneksel Damgalamaya Yönelik Çalışmalar

Damga olarak sözde rasgele sayı dizisi, ikili görüntü veya gri seviye görüntünün kullanıldığı dönüşüm alanında damgalamaya dayalı pek çok çalışma literatürde yer almaktadır. Bunlardan bazılarında tek dönüşüm alanı kullanılmış olmasına rağmen, farklı tekniklerin bir arada (hibrit) yer aldığı damgalama şemaları daha yaygındır. Son zamanlarda birbiriyle çelişen damgalama gereksinimlerini (dayanıklılık ve algılanamazlık) optimize etmek amacıyla, damgalama sürecinde doğadan esinlenmiş optimizasyon algoritmalarından yararlanılmıştır. Bu nedenle bu sınıftaki görüntü damgalama şemalarını, optimizasyon algoritması kullanmayan ve optimize edilmiş çalışmalar olmak üzere iki alt başlıkta incelemek mümkündür.

1.7.1.1. Optimizasyon Algoritması Kullanmayan Görüntü Damgalama Şemaları

Doğadan esinlenmiş algoritmalar, damgalamada genellikle gömme parametrelerini ya da pozisyonlarını belirlemede kullanılır. Optimizasyon algoritmalarının kullanılmadığı damgalama sistemlerinde ise bu faktörler çoğunlukla orijinal görüntüden bağımsız olarak seçilir.

Tek bir dönüşüm alanı tekniğinin kullanıldığı bir görüntü damgalama şeması, [75]'te önerilen AKD tabanlı yaklaşımdır. Burada, damga olarak 8×8 boyutlu ikili görüntü kullanılmıştır. İlk olarak damgalama algoritması, Toral Otomorfizm sistemi tarafından damga olarak kullanılan ikili görüntüyü karıştırır. Ardından, taşıyıcı görüntü olarak kullanılan 256×256 boyutlu gri seviye bir görüntünün blokları üzerinde AKD gerçekleştirilir. JPEG nicemleme tablosu yardımıyla AKD katsayıları nicemlenir. Ardından, katsayıların hala sıfıra eşit olmayan bazı istatistiksel özellikleri damganın gömülmesi için kullanılır. Önerilen sistemin TSGO değeri 35.662 dB bulunmuştur. Gömülme süreci göz

önüne alındığında, bu damgalama algoritmasının özellikle JPEG sıkıştırmaya karşı büyük bir dayanıklılığa sahip olması şaşırtıcı değildir.

AKD tabanlı bir başka çalışmada [76], renkli damga görüntüsü renkli taşıyıcı görüntüye gömülmüştür. İlk olarak, orijinal görüntü 8×8 boyutlu örtüşmeyen bloklara bölünür ve bu bloklar tek seviyeli AKD ile dönüştürülür. İkinci aşamada, düşük frekans bandındaki sol üst 4×4 katsayı iki seviyeli AKD tarafından tekrar dönüştürülür ve dönüştürülen bileşenler zigzag taramayla sıralanır. Son olarak, İGS'ye göre, sayısal damgalar sırasıyla bu blokların DC katsayısına ve ilk yedi AC katsayısına yerleştirilir. Bu çalışmada ortalama TSGO 44.1250 dB bulunurken, atak yokken NK 0.9971 olarak elde edilmiştir.

[77]'de, telif hakkı koruması için dalgacık katsayıları arasındaki mesafenin nicelleştirilmesine dayanan dayanıklı kör damgalama algoritması önerilmiştir. Dalgacık katsayıları bloklara bölünerek her bloktaki birinci, ikinci ve üçüncü maksimum katsayılar belirlenir. Daha sonra, birinci ve ikinci maksimum katsayılar ikili damga bitlerine bağlı olarak nicelendirilir. Blok tabanlı damgalama kullanılarak, orijinal görüntü veya damga kullanmadan damga çıkarılabilir. Bu çalışmada 512×512 boyutlu gri seviye görüntüye 32×16 boyutlu ikili damga gizlenmiştir. Gri seviye damgalanmış "Lena" görüntüsünün TSGO değeri 51.80 dB olarak bulunmuştur. Ancak ataklar karşısındaki dayanıklılığın çok yüksek olduğu söylenememektedir.

Bir başka çalışmada [78], orijinal görüntü önce 8×8 boyutlu bloklara bölünür ve her bloğa Hadamard dönüşümü uygulanarak damga gömülür. Önerilen yöntemde damgayı yerleştirme adımında, verimli gömme noktasını bulmak için enine arama algoritması kullanılır. Deneyler sonucu hesaplanan TSGO değeri 39.21 dB iken, önerilen sistemin, JPEG sıkıştırma, kırpma, keskinleştirme, filtreleme ve gürültü ekleme saldırılarına karşı önemli ölçüde direnç gösterdiği tespit edilmiştir.

Schur Ayrıştırmaya dayalı bir çalışmada [42], 32×32 boyutlu renkli görüntü damga olarak kullanılmış ve 512×512 boyutlu renkli görüntüye gömülmüştür. Bu çalışmada Schur ayrıştırma ile elde edilen 4×4 üniter matris U'nun, ikinci satır birinci sütun elemanı ile üçüncü satır birinci sütun elemanı arasındaki güçlü korelasyona bağlı olarak damga gömülür. Renkli "Lena" görüntüsü için TSGO değeri 39.4358 dB olarak bulunmuştur. Çalışma bazı saldırılar karşısında dayanıklı iken özellikle ortanca filtrelemeye karşı kötü bir performans sergilemiştir.

[79]'da yazarlar, ADD ve QR Ayrıştırmaya dayalı bir yöntem önermişlerdir. İlk olarak, 512×512 boyutlu renkli taşıyıcı görüntünün her bileşeni, bir seviyeli ADD ile dönüştürülür ve daha sonra, LL bant örtüşmeyen 4×4 pikselli bloklara bölünür. Ardından, seçilen her bir piksel bloğu QR Ayrıştırma ile ayrıştırılır ve matris R'deki ilk satır elemanlarının niceliği, damga bilgisinin gömülmesi için belirlenir. Burada kullanılan damga 32×32 boyutlu renkli bir görüntüdür. Çıkarma prosedüründe, damga, orijinal görüntüye veya orijinal damga bilgisine gerek olmadan damgalanmış görüntüden çıkarılabilir. Renkli "Lena" görüntüsü için elde edilen TSGO değeri 41.3784 dB bulunmuştur. Ayrıca, yöntemin yaygın görüntü işleme ataklarına karşı dayanıklılığının yüksek olduğu gözlenmiştir.

[80]'de yarı kör damgalama sistemi önerilmiştir. Orijinal görüntü zigzag tarama ile sıralanır ve ardından sıralanmış görüntüye AKD ve TDA uygulanır. Damga elde edilen tekil değerleri değiştirerek gömülür. 512×512 boyutlu gri seviye "Lena" görüntüsü için TSGO değeri 31.4550 dB bulunmuştur. Önerilen yöntem, Gauss bulanıklığı, keskinleştirme filtresi, JPEG sıkıştırma, histogram eşitleme gibi saldırılara karşı dayanıklı olsa da, döndürme, yeniden ölçekleme, kırpma gibi geometrik ataklara ve gürültü ataklarına karşı onun performansı düşüktür.

Telif hakkı koruma amacıyla yapılan bir başka çalışmada damgalama süreci TDA-ADD-AKD ve Kalman filtreleme yardımıyla gerçekleştirilmiştir [81]. İlk olarak TDA, hem orijinal görüntüye hem de damga görüntüsüne de uygulanır. Damga görüntüsünün TDA ile elde edilen köşegen bileşeninin, orijinal görüntünün köşegen bileşeni ile değiştirilmesiyle bir çıktı görüntüsü elde edilir. ADD, TDA tabanlı görüntüye uygulanır. ADD ile elde edilen, görüntünün dört alt bandı arasından LH bandı seçilir. AKD, ADD tabanlı görüntüye uygulanır. Böylece damgalanmış görüntü olarak adlandırılan bir görüntü elde edilir. Elde edilen damgalanmış görüntü üzerinde Kalman filtreleme gerçekleştirilir. "Lena" görüntüsü için Kalman Filtreleme tekniği ile geliştirilmiş TDA-ADD-AKD tabanlı yöntemin TSGO değeri 30.26 dB olarak bulunmuştur.

[82]'de AKD-TDA tabanlı bir damgalama yaklaşımı önerilmiştir. Görüntü önce 8×8 boyutlu bloklara bölünür ve ardından uygun bloklar İGS'ye bağlı olarak seçilir. Seçilen bloklara önce AKD ardından TDA uygulanır. Elde edilen U bileşeninin ilk sütun vektörü üzerindeki 3. ve 4. katsayı arasındaki ilişkiye bağlı olarak damga gömülür. 512×512 boyutlu gri seviye taşıyıcı görüntüye 32×32 boyutlu ikili damganın gömüldüğü çalışmada ortalama TSGO oranı 48.58 dB bulunmuştur.

[83]'teki yazarlar, renkli görüntüler için kör olmayan RGB, ADD ve TDA tabanlı bir damgalama yaklaşımı sunmuşlardır. RGB ile orijinal görüntü üç kanala dönüştürülür. Mavi kanal daha dayanıklı olduğundan, bu kanal ADD için seçilmiştir. Son olarak, damga, TDA ayrıştırma yoluyla tüm ADD alt bantlarına yerleştirilir. Bu çalışmanın avantajı, damganın tüm alt bantlara gömülü olmasından dolayı kapasitenin yüksek olmasıdır.

[84]'te ADD ve Kesirli Fourier Dönüşümünü (KFD) birleştirmeye dayanan bir görüntü damgalama tekniği sunulmaktadır. Önerilen teknikte, orijinal görüntü iki seviye ADD ile ayrıştırılır ve ardından orta frekans alt bantları KFD yardımıyla dönüştürülür. Damga, KFD katsayıları değiştirilerek gizlenir. Seçilen KFD katsayılarını damga pikselleriyle modifiye etmek için iki sözde rasgele gürültü dizisi kullanılır ve damga çıkarmada, gömme işleminde kullanılan aynı iki rasgele gürültü dizisine ve damga boyutuna ihtiyaç duyulur. Korelasyon faktörü, çıkarılan pikselin bir mi yoksa sıfır mı olduğunu belirlemek için kullanılır. Yöntemde 512×512 boyutlu gri seviye taşıyıcı görüntüye 20×50 boyutlu ikili damga gizlenmiştir. Deneysel sonuçlar, gömülen ve çıkarılan damga arasındaki korelasyon katsayısı 1 iken, TSGO değerinin 26.88 dB olduğunu göstermiştir.

[85]'te spektrum tabanlı dayanıklı bir görüntü damgalama yöntemi önerilmektedir. Damganın gömülmesi için orijinal görüntü örtüşmeyen bloklara bölünür ve her bloğa Sonlu Ridgelet Dönüşümü uygulanır. Dönüşüm katsayılarını içeren matriste her bir sütun Ridgelet uzayındaki yönlerden birini temsil eder. Damga bitlerini gömmek için, her bir sütundaki varyans hesaplanır. En büyük varyans değerine sahip sütun, Ridgelet uzayında damganın gömüleceği en iyi yön olarak düşünülür. Seçilen sütuna damga bitleri bir ölçekleme faktörü yardımıyla gömülür. Çıkarma adımında, damga, bozulmuş ve damgalanmış görüntüden kör olarak tespit edilir. Orijinal görüntü olarak 510×510 boyutlu gri seviye görüntünün kullanıldığı çalışmada 30×30 boyutlu ikili görüntü damga olarak seçilmiştir. Elde edilen TSGO değeri "Lena" görüntüsü için 48.87 dB'dir ve çeşitli saldırılar karşısında dayanıklılık performansı yüksektir.

1.7.1.2. Optimize Edilmiş Görüntü Damgalama Şemaları

Dayanıklı bir damgalama şemasının tasarlanmasındaki temel sorun, damgalanmış görüntünün algılanamazlığının sağlanması ile birlikte, şemanın geleneksel saldırılara direnme yeteneğinin nasıl arttırılacağıdır. Bunun başlıca nedeni, şiddetli saldırıların damgayı kapsayan örten görüntünün alanlarını bozmasıdır. Böylece, çıkarılan damganın kalitesi düşer

[86]. İyi bir dayanıklılık ve kabul edilebilir algılanamazlık kazanma yöntemleri, etkinliklerini kanıtlamış olmalarına rağmen, bazı geometrik ve sinyal işleme saldırılarına karşı koyamazlar. Bu nedenle dayanıklılık ve algılanamazlık arasındaki dengeyi sağlamak için doğadan esinlenmiş optimizasyon algoritmalarından yararlanılır. Doğadan esinlenmiş algoritmalarla geliştirilen damgalama şemalarını kullanan birçok çalışma literatürde mevcuttur. Bu çalışmalarda kullanılan doğadan esinlenmiş algoritmalar Karınca Kolonisi Optimizasyonu (KKO) [87, 88], Yapay Arı Kolonisi (YAK) [89-91], Guguk Kuşu Arama (GKA) [92], Diferansiyel Evrim (DE) [93-95], Ateş Böceği Algoritması (ABA) [96-100], Genetik Algoritma (GA) [101-103], Parçacık Sürüsü Optimizasyonu (PSO) [104, 105] vb. olarak sıralanabilir. Bir damgalama sistemindeki bu optimizasyon algoritmaları genellikle optimal gömme parametrelerini veya yerleştirme pozisyonlarını belirlemek için kullanılır. Tablo 1.1'de söz konusu optimizasyon algoritmalarının kullanıldığı görüntü damgalama şemalarının bir özeti yer almaktadır. Tabloda yer alan çalışmaların detayları aşağıda ayrıntılı olarak ele alınmıştır.

Optimal gömme parametrelerini tespit etmek için kullanılan çalışmalardan birinde [87], yazarlar Kaldıran Dalgacık Dönüşümü (KDD) ve TDA alanında kör olmayan damgalama gerçekleştirmişlerdir. KDD ile görüntü alt bantlarına ayrıldıktan sonra seçilen alt bandın TDA sonucu elde edilen tekil değerlerine damga gömülür. Burada, KKO'dan gömme adımındaki çoklu ölçekleme faktörlerini belirlemede yararlanılır. 256×256 boyutlu gri seviye taşıyıcı görüntüye 32×32 boyutlu ikili damganın gizlendiği çalışmada damgalanmış "Lena" görüntüsü için TSGO değeri 47.718 dB olarak bulunmuştur. Çalışma bazı ataklara karşı dirençli olsa da özellikle ortanca filtreleme ve döndürmeye karşı dayanıksızdır. Ayrıca çalışmada çoklu ölçekleme faktörünün kullanılmasının, tek ölçekleme faktörü kullanılmasına kıyasla ataklarda daha başarılı olduğu gözlenmiştir.

Tablo 1.1. Doğadan esinlenmiş algoritmalara dayalı görüntü damgalama

Kaynak Çalışma	Optimizasyon Algoritması	Dönüşüm Alanı	Damga Çıkarma Modu	Orijinal Görüntü Boyutu	Damga Boyutu	Gözlem
[87]	KKO	KDD-TDA	Kör Olmayan	256×256 (gri seviye)	32×32 (ikili)	TSGO= 47.718 dB
[88]	KKO	ADD-TDA	Kör Olmayan	256×256 (gri seviye)	32×32 (ikili)	TSGO= 50.942 dB
[89]	YAK	YDDADD-TDA	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 44.0207 dB, Kırpma ve Tuz & Biber gürültüsüne karşı dayanıksızdır.
[90]	YAK	TDD-TDA	Kör Olmayan	512×512 (gri seviye)	256×256	TSGO= 45.1242 dB
[91]	YAK	ADD-TDA	Kör Olmayan	512×512 (gri seviye)	64×64 (gri seviye)	TSGO= 31 dB
[92]	GKA	ADD	Kör Olmayan	256×256 (gri seviye)	128×128, 64×64	TSGO= 38.0358 dB (128×128), 37.9200 dB (64×64)
[93]	DE	TDA, ADD-TDA	Kör Olmayan	256×256 (gri seviye)	32×32 (ikili)	Damgalanmış görüntü ve orijinal görüntü arasındaki korelasyon 0.9995 (TDA), 0.9990 (ADD-TDA)
[94]	DE	ADD-TDA	Kör Olmayan	512×512 (gri seviye)	64×64 (gri seviye)	TSGO= 35.2357 dB

Tablo 1.1'in devamı

Kaynak Çalışma	Optimizasyon Algoritması	Dönüşüm Alanı	Damga Çıkarma Modu	Orijinal Görüntü Boyutu	Damga Boyutu	Gözlem
[95]	DE	AKD-TDA	Kör Olmayan	512×512 (gri seviye)	64×64 (gri seviye)	TSGO= 32.4527 dB
[96]	ABA	ADD-TDA	Kör Olmayan	256×256 (gri seviye)	32×32 (ikili)	TSGO= 55.7296 dB
[99]	ABA	ADD-TDA	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 52.1906 dB, Kırpma ve gürültü ataklarına karşı dayanıksızdır.
[98]	ABA	KDD-RA	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 38.8895 dB
[97]	ABA	KDD	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 37.9815 dB
[100]	ABA	Hadamard Dönüşümü	Kör	512×512 (gri seviye)	64×64 (ikili)	TSGO= 47.9843 dB, Ortalama filtre, ortanca filtre, gürültü atakları ve kırpmaya karşı dayanıklılığı azdır.
[106]	ABA	ADD-QR Ayrıştırma	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO=45.9035 dB, Ortalama NK=0.9560.

Tablo 1.1'in devamı

Kaynak Çalışma	Optimizasyon Algoritması	Dönüşüm Alanı	Damga Çıkarma Modu	Orijinal Görüntü Boyutu	Damga Boyutu	Gözlem
[107]	ABA	KDD	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO=36 dB üzerinde, Gürültü ataklarında referans çalışmadan daha üstün, Pürüzsüz görüntülerde dayanıklılığı atırmak için entropi kavramından yararlanılmıştır.
[101]	GA	TDA	Kör Olmayan	256×256 (gri seviye)	32×32 (ikili)	Damgalanmış görüntü ve orijinal görüntü arasındaki korelasyon 0.9997.
[102]	GA	TDA	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 44.97 dB, Keskinleştirme filtresi, histogram eşitleme ve tahrif dışındaki ataklara karşı dayanıklılığı düşüktür.

Tablo 1.1'in devamı

Kaynak Çalışma	Optimizasyon Algoritması	Dönüşüm Alanı	Damga Çıkarma Modu	Orijinal Görüntü Boyutu	Damga Boyutu	Gözlem
[103]	GA	ADD-AKD	Kör	512×512 (gri seviye)	32×32 (ikili)	TSGO= 41.5213 dB, Dönme, ortanca filtre, ortalama filtre, gürültü ve satır ve sütun kopyalamaya karşı dayanıklılığı düşüktür.
[104]	PSO	AKD-TDA, ADD-TDA	Kör Olmayan	512×512 (gri seviye)	256×256 (gri seviye)	TSGO= 32.17 dB (AKD-TDA), 33.93 dB (ADD-TDA)
[105]	PSO	TDA	Kör Olmayan	512×512 (gri seviye)	128×128 (gri seviye)	Orijinal görüntü ve damgalanmış görüntü arasındaki çapraz korelasyon 0.9915'dir.

[88]'de yazarlar ADD-TDA tabanlı bir yöntem sunmuşlardır. ADD ile alt bantlarına ayrılan görüntünün LH, HL ve HH bantlarından biri damganın gömüleceği alt bant olarak seçilir. Seçilen bu alt banda ters ADD uygulanır ve ardından TDA ile ayrıştırılır. Damga görüntüsü de şifrelendikten sonra TDA ile ayrıştırılır. Damgadan elde edilen U ve V matrisinin tek yönlü özet (hash) fonksiyonları hesaplanır. Şifrelenmiş damganın U ve V matrisi ile bunların özet değerleri yanlış pozitif problemini azaltmak için gizli anahtarlar olarak saklanır. Orijinal görüntünün alt bandından elde edilen tekil değerlere şifrelenmiş damganın tekil değerleri bir ölçekleme faktörü yardımıyla gömülür. Burada kullanılan çoklu ölçekleme faktörü KKO yardımıyla belirlenir. Damgalanmış tekil değer matrisi ters dönüşümler vasıtasıyla damgalanmış görüntüyü oluşturmak için kullanılır. Kör olmayan bu damgalama sisteminde 256×256 boyutlu gri seviye taşıyıcı görüntüye 32×32 boyutlu ikili damga gömülmüştür. Damgalanmış "Lena" görüntüsünün TSGO değeri 50.942 dB bulunmuştur. Sistemde tek ölçekleme faktöründense ACO ile belirlenmiş çoklu ölçekleme faktörünün, test sonuçlarını olumlu etkilediği gözlenmiştir.

[89]'da YAK'ın optimizasyon algoritması olarak kullanıldığı dalgacık tabanlı yaklaşım önerilmiştir. Burada ADD'nin 90° ve katlarında dönme ve görüntü çevirmeye karşı değişmez olduğu versiyonu Yeniden Dağıtılmış Değişmez ADD (YDDADD) dönüşüm alanı olarak kullanılmıştır. YDDADD ile elde edilen LL bant örtüşmeyen 4×4 boyutlu bloklara ayrılır. Damganın gömüleceği uygun bloklar İGS karakteristiğine bağlı olarak seçilir. Her bir bloğa TDA uygulandıktan sonra elde edilen U bileşeninin ilk sütun 2. ve 3. satır katsayıları arasındaki ilişkiye bağlı olarak damga gömülür. Bu çalışmada kör damgalama kullanıldığı için damganın kendisi ve orijinal görüntüye damga çıkarma sürecinde ihtiyaç duyulmaz. Burada damga gömme parametrelerini belirleme aşamasında YAK kullanılmıştır. 512×512 boyutlu gri seviye taşıyıcı görüntüye 32×32 boyutlu ikili damganın gizlendiği çalışmada damgalanmış "Lena" görüntüsü için TSGO değeri 44.0207 dB olarak bulunmuştur. Çalışma kırpma ve tuz ve biber gürültüsü atağına nispeten dirençsiz olsa da diğer test edilen ataklarda daha başarılıdır.

Tamsayı Dalgacık Dönüşümü (TDD) ve TDA tabanlı bir çalışmada [90], orijinal görüntü 1-seviye TDD ile alt bantlarına ayrılır. LL, LH ve HL bantlar TDA ile ayrıştırıldığında elde edilen tekil değerlere damga gömülür. U ve V bileşenlerine bağlı olarak elde edilen sayısal imza ise HH banda gömülür. Bu çalışmada, gömme adımında kullanılan ölçekleme faktörü YAK ile optimize edilmiştir. 512×512 boyutlu gri seviye taşıyıcı görüntüye 256×256 boyutlu damganın gömüldüğü yöntemde kör olmayan bir damgalama

şeması sunulduğu için dayanıklılığı yüksektir. Dolayısıyla algılanamazlıktan çok fazla ödün verilmemiştir. TSGO değeri 45.1242 dB bulunmuştur.

Görüntüye bağlı olarak seçilmesi gereken ölçekleme faktörünün YAK ile optimize edildiği bir başka çalışmada [91], 3-seviye ADD ile elde edilen LL_3, LH_3 ve HL_3 bantlar damga gömme alanı olarak seçilir. Damga bilgisine TDA uygulandığında elde edilen U bileşeni ölçekleme faktörü ile çarpılarak LH_3 ve HL_3 bantlarına eklenir. Ardından, LL_3 bandın TDA sonucu oluşturulan tekil değerlerine damganın tekil değerleri ölçekleme faktörü ile çarpıldıktan sonra ilave edilir. Burada önerilen yöntem kör olmayan yöntemdir ve 512×512 boyutlu gri seviye taşıyıcı görüntüye 64×64 boyutlu gri seviye görüntü gizlenmiştir. Damgalanmış "Lena" görüntüsüne ait TSGO değeri 31 dB'dir. Bu çalışmada dayanıklılık sınırlı sayıda görüntü işleme manipülasyonlarına ve kırpma ve ölçeklemeye karşı test edilmiştir.

Optimal ölçekleme faktörünün GKA ile tespit edilmeye çalışıldığı bir çalışmada [92], taşıyıcı görüntü ADD ile alt bantlarına ayrılmış ve LL ve HH bantlar damgalama alanı olarak seçilmiştir. LL ve HH bantlara damga eklenirken iki farklı ölçekleme faktöründen yararlanılmıştır. Burada taşıyıcı görüntü olarak 256×256 boyutlu gri seviye görüntü tercih edilirken, 1-seviye ADD uygulanırsa 128×128 boyutlu damga, 2-seviye ADD uygulanırsa 64×64 boyutlu damga kullanılmıştır. Kör olmayan bu damgalama yönteminde TSGO değeri 1-seviye ADD için 38.0358 dB, 2-seviye ADD için 37.9200 dB bulunmuştur. Çalışma atak yokken gömülen damgayı başarılı bir şekilde çıkarmış olsa da, ataklar karşısında direnci düşük bulunmuştur.

TDA ve ADD-TDA tabanında iki farklı kör olmayan yaklaşımın önerildiği bir çalışmada, ilk yöntemde orijinal görüntünün tekil değerleri çoklu ölçekleme faktörüyle birlikte değiştirilerek damga gömülmüştür [93]. İkinci yöntemde ise orijinal görüntü ADD ile dört banda ayrıştırıldıktan sonra her alt banda TDA uygulanır ve aynı damga çoklu ölçekleme faktörü yardımıyla tekil değerlere gömülür. Burada kullanılan çoklu ölçekleme faktörleri DE ile optimize edilir. Çalışmada orijinal görüntü olarak 256×256 boyutlu gri seviye görüntü kullanılırken, damga olarak 32×32 boyutlu ikili logo tercih edilmiştir. Damgalanmış görüntü ve orijinal görüntü arasında elde edilen korelasyon değeri TDA tabanlı yaklaşım için 0.9995, ADD-TDA tabanlı yaklaşım için 0.9990 olarak bulunmuştur.

[94]'te yazarlar ADD ve TDA'ya dayalı bir yöntem önermişledir. Orijinal görüntü önce 3-seviye ADD ile alt bantlarına ayrıştırılır. Elde edilen LL_3 ve HH_3 bantlarına TDA uygulanır. Damga tekil değerlere bir ölçeklendirme faktörü ile çarpılarak eklenir. Bu

ölçekleme faktörü, algılanamazlık ve dayanıklılığı dengelemek için DE ile optimize edilir. Modifiye edilmiş LL bant Arnold Dönüşümü ile karıştırılıp, ikili görüntü elde etmek için ona Otsu eşikleme metodu uygulanır. Gri seviye damgaya da, ikili damga elde etmek için Otsu eşikleme metodu uygulanır. Bu iki ikili görüntü bit temelinde ex-or işlemine tabi tutulup gizli anahtar üretilir. Bu gizli anahtar orijinal görüntüye gömülmeyip, çıkarma aşaması için kullanılır. Taşıyıcı görüntü olarak 512×512 boyutlu gri seviye görüntü kullanılan bu çalışmada, 64×64 boyutlu gri seviye ve ikili görüntü damga olarak kullanılmıştır. Önerilen kör olmayan damgalama şemasının TSGO değeri 35.2357 dB'dir ve test edilen görüntü işleme ve geometrik ataklara karşı dayanıklıdır.

DE tekniğini ölçekleme faktörünü optimize etmek için kullanan bir başka çalışma [95], AKD ve TDA tabanında bir yaklaşım önermiştir. Orijinal görüntü 8×8 boyutlu bloklara ayrıldıktan sonra her bloğa AKD uygulanır ve DC değerleri bir matriste (A) toplanır. Ardından A matrisine TDA uygulanır. Arnold Dönüşümü ile karıştırılan damga görüntüsü, A matrisinin tekil değerlerine DE yardımıyla elde edilen ölçekleme faktörüyle çarpılarak gizlenir. Damganın gömüldüğü diyagonal matrise TDA uygulanır. Elde edilen yeni diyagonal matris A matrisinin tekil vektörleriyle çarpılarak damgalanmış A matrisi elde edilir. Modifiye edilmiş DC değerler yerine konarak ters AKD ile damgalanmış görüntü oluşturulur. Bu çalışmada kör olmayan bir yöntem önerilmiştir. 512×512 boyutlu gri seviye iki farklı görüntü taşıyıcı görüntü olarak, 64×64 boyutlu gri seviye görüntü ise damga olarak kullanılmıştır. Damgalanmış "Airplane" ve "Baboon" görüntüleri için sırasıyla TSGO değeri 36.3848 dB ve 32.4527 dB olarak bulunmuştur.

Sayısal damgalama tekniklerinde yaygın olarak kullanılan doğadan esinlenmiş optimizasyon algoritmalarından biri de ABA'dır. ABA'ya dayalı kör olmayan bir çalışmada "Haar" dalgacığı kullanan ADD-TDA tabanlı bir yaklaşım önerilmiştir [96]. Orijinal görüntüye 3-seviye ADD uygulandıktan sonra elde edilen LL_3 banda TDA uygulanır. Elde edilen tekil değerlere TDA uygulanmış ikili damganın tekil değerleri ölçekleme faktörü ile çarpılarak gömülür. Güncellenen bu diyagonal matris, LL_3 bandının tekil vektörleriyle çarpılarak modifiye edilmiş alt bant elde edilir. Modifiye edilmiş alt bant diğer alt bantlarla birlikte 3-seviye ters ADD işlemine tabi tutularak damgalanmış görüntü elde edilir. ABA burada ölçekleme faktörünü belirlemek için kullanılmıştır. Çalışmada 256×256 boyutlu gri seviye taşıyıcı görüntü ve 32×32 boyutlu ikili damga kullanılmıştır. Çoklu ölçekleme faktörü kullanıldığı durumda elde edilen TSGO değeri "Lena" görüntüsü için 55.7296

dB'dir. Deneysel sonuçlar çalışmanın özellikle kırpma atağına karşı dayanıksız olduğunu göstermiştir.

[99]'da ADD-TDA alanında kör damgalama yöntemi önerilmiştir. Burada öncelikle 512×512'lik orijinal görüntü 8×8 boyutlu örtüşmeyen bloklara ayrılır ve 32×32 boyutlu damganın gömüleceği bloklar İGS yardımıyla seçilir. Seçilen blokların (x, y) koordinatları A ve B matrislerinde saklanır. Damga elemanları bir gizli anahtar yardımıyla MD5'e dayalı bir algoritma ile karıştırılır. Karıştırılan damganın her bitini bir bloğa gömmek için öncelikle bloklara ADD uygulanır. Elde edilen LL bant TDA ile ayrıştırılır. U matrisinin birinci sütun 2. ve 3. elemanları daha dayanıklı damga elde etmek için kullanılır. Damganın gömülmesi aşamasında U matrisinin katsayılarının güncellenmesinde yararlanılan eşik değerleri optimize etmek için Karşıtlık ve Boyut Tabanlı Değiştirilmiş ABA'dan yararlanılır. Deneysel sonuçlara göre damgalanmış gri seviye "Lena" görüntüsü için TSGO değeri 52.1906 dB bulunmuştur ve atak yokken damga başarılı bir şekilde çıkarılmıştır. Ancak özellikle kırpma ve gürültü atağına karşı çalışmanın dayanıklılığı düşüktür.

ABA tabanlı bir başka çalışma [98]'de önerilmiştir. Bu çalışmada öncelikle damga Fibonacci-Q Dönüşümü yardımıyla karıştırılır. Ardından, 512×512 boyutlu orijinal görüntü KDD yardımıyla alt bantlarına ayrıştırılır ve düşük frekanslı alt bant 3×3 boyutlu örtüşmeyen bloklara bölünür. Bloklar standart sapma değerlerine bağlı olarak artan sırada sıralandıktan sonra damga boyutu kadar (32×32) blok gömme sürecinde kullanılır ve bu blokların indeksleri damga çıkarma aşamasında kullanılmak üzere bir vektörde saklanır. Gömme adımında yer almayan bloklar Regresyon Ağacı (RA) oluşturmak amacıyla iki matrisi elde etmede kullanılır. Bu matrislerden biri Amaç Vektörü'dür ki; bu her bloğun merkezi katsayısını içeren bir sütun vektörüdür. Diğeri ise Giriş Matrisi adı verilen her bir satırında bir bloğa ait diğer katsayıları içeren matristir. Bu iki matris RA oluşturma parametresi olarak kullanılır. Oluşturulan RA ve bloğun merkezi katsayısına bağlı olarak, bloğa ilgili damga biti çoklu ölçekleme faktörü yardımıyla gömülür. Çoklu ölçekleme faktörü dayanıklılık ve algılanamazlık arasında iyi bir ödünleşim elde etmek amacıyla ABA ile optimize edilir. Damga çıkarma adımında orijinal görüntüye ihtiyaç duyulmadığından bu yöntem kördür. Gri seviye damgalanmış "Lena" görüntüsü için TSGO 38.8895 dB bulunmuştur. Bu yöntemde çok sayıda atak test edilmiştir. Çalışma gürültü ataklarına karşı nispeten daha zayıf olsa da asıl başarısız olduğu atak dönmeye karşı performansta öne çıkmaktadır.

Tez kapsamında önerilen ABA tabanlı bir çalışmada [106], ADD ve QR Ayrıştırma damgalama alanı olarak seçilmiştir. 32×32 boyutunda ikili damgayı 512×512 boyutunda gri seviye taşıyıcı görüntüye gömmek için önce orijinal görüntü 6×6 boyutlu bloklara ayrılır. Standart sapması daha düşük olan damga boyutu kadar bloğun her birine "db2" filtre yardımıyla ADD uygulanır. Elde edilen LL banda QR ayrıştırma uygulanır. Damga [-1, 1] aralığındaki iki dizi ve ölçekleme faktörü yardımıyla R matrisinin ilk satırına gömülür. Burada kullanılan ölçekleme faktörünü optimize etmek amacıyla ABA'dan yararlanılmıştır. Damga çıkarma adımında gömme adımında kullanılan iki dizi ve seçilen blokların indeksi kullanıldığından yöntem kördür. Damgalanmış "Lena" görüntüsüne ait TSGO değeri 45.9035 dB bulunmuştur. Farklı ataklar karşısında yöntemin dayanıklılığı test edildiğinde ortalama NK 0.9560 olarak tespit edilmiştir.

ABA'nın damganın gömüleceği blokları seçmek için kullanıldığı çalışmalar da literatürde mevcuttur. Bunlardan biri, KDD'ye dayalı bir yöntemdir [97]. Öncelikle, 512×512 boyutlu orijinal görüntü KDD yardımıyla alt bantlarına ayrıştırılır ve LL bant 3×3 boyutlu örtüşmeyen bloklara bölünür. Her bir bloğun standart sapma değeri hesaplanır ve bloklar bu değere bağlı olarak azalan sırada sıralanırlar. İlk blokların bazı yüzdesi algılanamazlık ve dayanıklılığı dengelemek amacıyla göz ardı edilir. ABA burada göz ardı etme faktörünü belirlemek amacıyla kullanılır. ABA'nın uygulanması sonucu damganın gömüleceği bloklar bir vektörde tutulur ki; damga çıkarma adımında kullanılsın. Damga gömülmeden önce Arnold Dönüşümü ile karıştırılır. Damga gömmek için, damga biti 1 ise seçilen bloğun maksimum değeri bloğun merkezi katsayısına atanır. Eğer bit 0 ise, merkezi katsayı bloğun mininum değerine eşitlenir. Damga çıkarma merkezi katsayının minimum ve maksimum değere uzaklığına bağlı olarak yapıldığından yöntem kördür. 32×32 boyutlu ikili damganın gömüldüğü bu çalışmada damgalanmış gri seviye "Lena" görüntüsüne ait TSGO değeri 37.9815 dB olarak bulunmuştur. Çalışmanın farklı geometrik ataklar ve görüntü işleme atakları karşısında dayanıklılığı test edildiğinde, dönmeye karşı oldukça başarısız ancak diğer saldırılara karşı oldukça dirençli olduğu görülmüştür.

Damganın gömüleceği blokların ABA ile optimize edildiği bir diğer çalışmada [100], öncelikle orijinal görüntü 8×8 boyutlu örtüşmeyen bloklara ayrılır. Blokların entropisi hesaplanır. Burada her bloğa 4 bit gömülecektir. Düşük entropili bloklardan istenen blok sayısının iki katı kadarı seçilir. Ayrı Ayrık ABA kullanılarak en uygun bloklar seçilir ve bunların koordinatları iki ayrı vektörde tutulur. Seçili bloğa Hadamard Dönüşümü uygulanır. Dönüşüm sonrası elde edilen katsayılardan dördü komşularının değerlerinin ortalamasına ve

sabit bir eşik değere bağlı olarak damga bitini gömmek için modifiye edilir. Çıkarma adımında orijinal görüntü gerektirmeyen bu çalışma kördür. Çalışmada kullanılan gri seviye orijinal görüntünün boyutu 512×512 iken, ikili damga boyutu 64×64'tür. Damgalanmış "Lena" görüntüsü için TSGO değeri 47.9843 dB olarak hesaplanmıştır. Yöntem ortalama filtre, ortanca filtre, gürültü atakları ve kırpmaya karşı çok yüksek dayanıklılığa sahip değildir.

Tez kapsamında önerilen diğer çalışmada damganın gömüleceği bloklar ABA'ya bağlı olarak seçilmiştir [107]. [97]'deki yazarlar tarafından sunulan KDD-ABA alanındaki blok tabanlı yöntemi gökyüzü, deniz gibi piksel parlaklıklarının birbirine yakın olduğu tek düze görüntülerde de etkili hale getirebilmek için burada entropi kavramından yararlanılmıştır. Entropi, karmaşıklığın bir ölçüsü olarak tanımlanır. Pürüzsüz bölgelerde entropi düşüktür. Bu bölgelerdeki bloğun değerleri birbirine çok yakın olduğundan, bloğa gömülü olan bit çıkarma işleminde tespit edilemeyebilir. Bu nedenle damganın gömüleceği bloğun yer aldığı bölgenin entropisine bakılarak farklı şekillerde gömme yapılır. Çalışmada öncelikle KDD ile ayrıştırılan orijinal görüntünün LL bandı 4 bölgeye (2×2) bölünür. Her bölgenin entropisi hesaplanır. Ardından LL bant 3×3 boyutlu bloklara bölünür ve algılanamazlık ve dayanıklılık açısından en optimum bloklar ABA tarafından seçilir. Damganın gömüleceği 3×3 boyutlu blok, karmaşıklık düzeyinin düşük olduğu bölgede yer alıyorsa, bloğun bulunduğu 6×6'lık alanın en büyük ve en küçük değeri hesaplanır. Eğer bloğun yer aldığı bölgenin karmaşıklık düzeyi belirli bir eşik değerin üstünde ise söz konusu 3×3'lük bloğun en büyük ve en küçük değeri hesaplanır. Seçilen bloğun merkez pikseline damga biti 1 ise en büyük değer, 0 ise en küçük değer atanır. Damga çıkarmanın kör olarak yapıldığı bu çalışmada, çeşitli tek düze görüntüler için elde edilen TSGO değeri 36 dB'nin üzerinde bulunmuştur. Önerilen yöntem [97] ile kıyaslandığında özellikle gürültü ataklarında daha başarılı bulunmuştur.

[101]'de damga gömme aşamasındaki çoklu ölçekleme faktörünün GA ile optimize edildiği bir yaklaşım sunulmuştur. Orijinal görüntü TDA ile ayrıştırıldığında elde edilen tekil değerlere damga biti bir ölçekleme faktörü ile çarpılarak eklenir. Orijinal görüntü olarak 256×256 boyutlu gri seviye görüntünün, damga olarak ise 32×32 boyutlu ikili görüntünün tercih edildiği bu kör olmayan damgalama şemasında, damgalanmış görüntü ve orijinal görüntü arasında elde edilen korelasyon değeri 0.9997 olarak bulunmuştur.

[102]'de yazarlar bir önceki çalışmada olduğu gibi TDA ile GA'yı bir arada kullanmışlardır. Orijinal görüntü 8×8 boyutlu örtüşmeyen bloklara ayrıldıktan sonra her

blok TDA ile ayrıştırılır. Diyagonal matrisin 0 olmayan değerlerinin sayısı bloğun karmaşıklığını belirlemek için hesaplanır. Daha büyük karmaşıklığa sahip bloklar damgayı gömmek üzere seçilir. Her seçilen blokta U matrisinin birinci sütununun 4. ve 5. katsayısı arasındaki ilişkiye bağlı olarak damga gömülür. Bu kör yöntemde GA damganın gömme gücünün optimizasyonunda kullanılır. Çalışmada 512×512 boyutlu gri seviye görüntüye, 32×32 boyutlu ikili görüntü gizlenmiştir. Deneysel sonuçlara göre TSGO değeri 44.97 dB bulunmuştur. Ancak Keskinleştirme filtresi, histogram eşitleme ve tahrif dışındaki ataklara karşı dayanıklılığı düşüktür.

Bir başka GA tabanlı çalışmada, sayısal görüntünün telif hakkını korumak için ADD-AKD tabanlı yaklaşım önerilmiştir [103]. Orijinal görüntü önce 2 seviye ADD ile ayrıştırılır. Ardından HL_2 bant 4×4 boyutlu bloklara bölünür ve her bloğa AKD uygulanır. "pattern_0" adında sözde rasgele bir dizi oluşturulur ve bu dizinin her bitini ters çevirerek "pattern_1" dizisi elde edilir. Bu dizilerin uzunluğu AKD'nin orta frekans bandındaki elemanların sayısına eşittir. 1 değerli biti gömmek için AKD'nin orta frekans katsayılarına "pattern_1" dizisinin bir ölçekleme faktörü ile çarpılıp eklenmesiyle, 0 değerli biti gömmek için ise AKD'nin orta frekans katsayılarına "pattern_0" dizisinin bir ölçekleme faktörü ile çarpılıp eklenmesiyle damga gömülmüş olur. Damga çıkarma adımında ise orta frekans katsayılarının bu dizilerle olan korelasyonuna bağlı olarak damganın 1 mi yoksa 0 mı olduğu belirlenir. Dolayısıyla bu yöntem kördür. GA optimum gömme parametrelerini bulmak için bu çalışmada kullanılmıştır. 512×512 boyutlu gri seviye görüntüye, 32×32 boyutlu ikili damganın gömüldüğü bu çalışmada, damgalanmış "Lena" görüntüsünün TSGO değeri 41.5213 dB bulunmuştur. Çalışma özellikle dönme, ortanca filtre, ortalama filtre, gürültü ve satır ve sütun kopyalamaya karşı çok dirençli değildir.

[104]'te yazarlar ölçekleme faktörünün PSO ile optimize edildiği iki farklı yaklaşım önermişlerdir. Birinci yöntemde (AKD-TDA tabanlı) damganın TDA sonucu elde edilen temel bileşenleri (sol tekil vektör ve tekil değerler çarpımı) AKD ile dönüştürülmüş orijinal görüntünün tekil değerlerine bir ölçekleme faktörü yardımıyla gömülür ve damga kör olmayan bir yöntemle çıkarılır. İkinci yöntemde (ADD-TDA tabanlı) ise ADD ile ayrıştırılan orijinal görüntünün her bir alt bandına TDA uygulanır. Damganın temel bileşenleri her bir alt banttaki tekil değerlere bir ölçekleme faktörü yardımıyla gömülür. 512×512 boyutlu gri seviye görüntüye 256×256 boyutlu gri seviye görüntünün gömüldüğü bu çalışmada birinci yöntem için TSGO 32.17 dB, ikinci yöntem için TSGO 33.93 dB bulunmuştur. Birinci yöntemin JPEG sıkıştırma ve ölçekleme dışındaki ataklarda çok başarılı olmadığı

gözlenmiştir. İkinci yöntem kullanılarak gömülen ve çıkarılan damga arasındaki korelasyon katsayısı birinci yönteme göre biraz daha yüksek bulunmuştur.

Bir başka PSO tabanlı yaklaşımda [105], 512×512 boyutlu gri seviye orijinal görüntü ve 128×128 boyutlu gri seviye damga görüntüsü kullanılmıştır. Orijinal görüntü TDA ile ayrıştırıldıktan sonra damga bir ölçekleme faktörü (PSO ile optimize edilmiş) ile çarpılarak orijinal görüntünün tekil değerlerine gömülür. Kör olmayan çıkarma yönteminin kullanıldığı bu çalışmada orijinal görüntü ve damgalanmış görüntü arasındaki çapraz korelasyon katsayısı "Lena" görüntüsü için 0.9915 bulunmuştur. Çalışmada 6 farklı atak için dayanıklılık test edilmiş ve gömülen ve çıkarılan damga arasındaki çapraz korelasyon katsayısı 0.9'un üzerinde bulunmuştur.

Geleneksel damgalamaya yönelik çalışmalar incelendiğinde damgalama şemalarının performansının biraz daha iyileştirilmesi adına tek dönüşüm tekniği yerine birden fazla dönüşüm tekniğinin ele alındığı hibrit yaklaşımlar daha ön plana çıkmaktadır. Özellikle AKD, ADD ve benzeri temel dönüşüm teknikleri ile birlikte matris dönüşümlerinden TDA'nın yer aldığı birçok yöntemin önerilmesi, damgalama algoritmalarının işlevselliğinin, TDA kullanılarak geliştirilebileceğinin kanıtı niteliğindedir. Ancak TDA tabanlı bazı damgalama şemalarının kusurları mevcuttur. Şöyle ki literatürde yer alan bazı yöntemler sadece damganın tekil değerlerini orijinal görüntüye gömerlerken tekil vektörlerini damga çıkarma aşamasında gizli anahtarlar olarak kullanırlar. Yani damganın tekil değerlerini gömmek için orijinal görüntünün tekil değerlerini modifiye ederler. Tekil değerler görüntünün yapısıyla ilgili önemli bilgi içermediğinden, sadece görüntünün parlaklığını temsil ettiğinden dolayı bu yerleştirme stratejisi yanlış pozitif problemine yol açmaktadır. Yani hiç gömülmeyen bir damga damgalanmış içerikten çıkarılabilir. O nedenle görüntünün yapısı ve geometrik özelliklerini taşıyan tekil vektörler damgalama alanı seçilerek bu problem elimine edilmeye çalışılır. Çalışmalarda ayrıca sadeliği, kolay uygulanabilmesi ve esnekliği ve farklı uygulamalarda diğerlerinden daha iyi performans sergilemesi sebebiyle ABA ve ondan türetilmiş algoritmaların sıkça başvurulan bir optimizasyon tekniği olması dikkat çekmektedir.

1.7.2. Biyometrik Damgalamaya Yönelik Çalışmalar

Geleneksel damgalama sistemlerinde sayısal damganın sahipliği konusu dikkate alınmamıştır. Dolayısıyla anlaşmazlık durumunda, sayısal damganın aidiyetini belirlemek

zor olabilir. İkili görüntü, kaotik dizi ya da sözde rasgele sayı dizisi, sahiplik kanıtlama için talep edilemez. Sayısal damga, yalnızca fiziksel veya mantıksal olarak sahiplenilebildiği zaman bu amaçla kullanılabilir. Örneğin, tüm bireyler için benzersiz olan biyometrik özelliklerin damga olarak kullanıldığı biyometrik damgalama sistemleri, sayısal damganın mülkiyeti sorununun üstesinden gelmek için potansiyel bir çözüm olabilir. Sayısal içeriğin telif hakkını koruma amacıyla önerilen biyometrik damgalama yöntemlerini, damga olarak tek biyometrik özelliğinin kullanıldığı şemalar (unimodal) ve çoklu biyometrik özelliklerin kullanıldığı şemalar (multimodal) olmak üzere ayırmak mümkündür. Tek biyometrik özelliğe dayalı biyometrik sistemlerin sahtekârlık sorunlarıyla karşı karşıya kalma ihtimalinin yüksek olduğu düşünülerek, hak talebinde bulunan sahip için gerçek ve sahtekâr girişimleri arasında ayrım yapma kararının, dikkate alınan birden çok biyometrik özelliğin birleşik ölçümüne dayandığı çoklu biyometrik sistemler tercih edilir. Tek biyometrik özelliğin ve birden çok biyometrik özelliğin kullanıldığı damgalama yöntemleri aşağıda alt başlıklar halinde incelenmiştir.

1.7.2.1. Tek Modelli Biyometrik Damgalama Şemaları

Bu bölümde farklı biyometrik özelliklerin telif hakkı koruma uygulamalarında kullanıldığı tek modelli damgalama sistemlerine değinilmiştir.

[63]'te konuşma sinyalinin damga olarak kullanıldığı ADD ve Hızlı Ayrık Curvelet Dönüşümüne dayalı bir çalışma önerilmiştir. Konuşma sinyali öncelikle matris forma dönüştürülür ve önce AKD, ardından elde edilen dönüşüm katsayılarına TDA uygulanır. Elde edilen tekil değer matrisi damga olarak kullanılır. Orijinal görüntünün dalgacık katsayılarına Ayrık Curvelet Dönüşümü uygulanır. Bu hibrit dönüşümün yüksek frekanslı katsayıları damga matrisinin katsayılarını gömmek üzere seçilir. Damganın çıkarma aşamasında orijinal görüntünün katsayıları kullanıldığı için bu kör olmayan bir damgalama yöntemidir. Burada kullanılan gri seviye orijinal görüntü boyutu 192×192'dir. Konuşma sinyali de 36864 örnekten oluşur ve bu sinyal de 192×192 boyutlu matris formuna dönüştürülür. Damgalanmış gri seviye "Lena" görüntüsü için elde edilen TSGO değeri 28.65 dB'dir. Atak olmadığı durumda BHO değeri 0.0036 olarak bulunmuştur.

[64]'te parmak izi görüntülerinin damga olarak doğal görüntülere gömüldüğü bir sistem önerilmiştir. Parmak izi ayrıntı noktalarının koordinat ve açı bilgileri 8×8 boyutlu AKD blokların orta frekans bandına gömülür. Damgalanmış renkli görüntülerin TSGO

değeri 25 dB üzerinde bulunmuştur. Çalışma sadece bazı sinyal işleme atakları karşısında test edilmiş ve NK değeri 0.91'in üzerinde hesaplanmıştır. Kimlik doğrulama bu çalışmada test edilmemiştir.

[65]'te parmak izinin AKD-TDA alanında damgalandığı bir görüntü damgalama şeması sunulmuştur. Öncelikle orijinal görüntünün AKD'si hesaplanır. AKD katsayıları daha sonra zigzag dizisi kullanılarak dört çeyreğe bölünür. Dört çeyreğin hepsi TDA ile ayrıştırılır ve damga yalnızca elde edilen tekil değerlere gömülür. Kör olmayan bu damgalama sisteminde damgalanmış görüntünün TSGO değeri 75.4852 dB olarak hesaplanmıştır.

ADD-TDA tabanlı parmak izi damgalamaya yönelik bir çalışma [66]'daki yazarlar tarafından önerilmiştir. Orijinal görüntü kaldıran tabanlı ADD ile alt bantlarına ayrılır. Ardından her bir alt bant TDA ile ayrıştırılır. Parmak izi şablonunun Ampirik Mod Ayrışımı tabanlı ikili kodu tekil değer matrisine gömülür. FVC 2004 veri tabanında 10 kişinin parmak izine ait 7 adet görüntünün yer aldığı, toplam 70 görüntüden oluşan bir veri tabanı üzerinden testlerin gerçekleştirildiği bu çalışmada, bazı basit filtreleme atakları karşısında gömülen parmak izi özniteliklerinin başarılı şekilde çıkarıldığı gözlenmiştir.

Yüz görüntüsünün biyometrik damga olarak kullanıldığı bir çalışmada dalgacık tabanlı dört kör damgalama yöntemi önerilmiş ve karşılaştırılmıştır [67]. İki damgalama yöntemi, ADD'ye, kalan iki damgalama yöntemi ise Artımsal Ayrık Dalgacık Dönüşümüne (AADD) dayanmaktadır. Her dönüşümdeki damgalama yöntemlerinden birinde, çıkarılan damganın güvenilirliğini geliştirmek amacıyla ağırlıklı ikili kodlamadan faydalanılmıştır. Burada yararlanılan taşıyıcı gri seviye görüntü 512×512 piksel boyutunda ve damga olarak kullanılan gri seviye görüntü ise 64×64 piksel boyutundadır. Yöntemler arasında damgalanmış görüntü ve orijinal görüntü arasındaki en düşük TSGO değeri 41.53 dB, en yüksek TSGO değeri 52.37 dB olarak bulunmuştur. Atak yokken çıkarılan damganın NK değeri en düşük 0.6589 iken, en yüksek 1 olarak hesaplanmıştır.

Yüz öz niteliklerinin damga olarak kullanıldığı bir çalışmada, beş farklı senaryo kullanılarak damga gömülmüştür [68]. Bunlardan ilki uzaysal alanda, ikincisi Fourier Mellin Dönüşümüne dayalı, üçüncüsü AKD alanında, dördüncü ve beşinci ise ADD'ye dayalı yöntemlerdir. Bu algoritmaların performansı, çıkarılan yüz özellik vektörleri üzerinde eğitilmiş ve test edilmiş sinir ağları kullanılarak elde edilen tanımlama doğruluğuna göre değerlendirilmiştir. Tanımlama doğruluğu açısından AKD tabanlı yöntemin performansı diğerlerine oranla daha üstün bulunmuştur.

[74]'te imza verisinin damgalandığı kör olmayan bir çalışmadan bahsedilmiştir. Renkli taşıyıcı görüntü öncelikle YCbCr renk uzayına çevrilir, ardından Y kanalı ADD ile alt bantlarına ayrılır. Biyometrik görüntü de ADD ile alt bantlarına ayrıştırılır. Biyometrik görüntünün her bir alt bandının dalgacık katsayıları, orijinal görüntünün Y bileşeninin karşılık gelen alt bandına çarpımsal damga denklemi kullanılarak eklenir. Ters dönüşümlerle damgalanmış görüntü elde edilir. 512×512 piksel boyutunda renkli taşıyıcı görüntüye 512×512 piksel boyutunda ikili imza görüntüsünün gömüldüğü çalışmada damgalanmış "Lena" görüntüsüne ait TSGO değeri 51.95 dB olarak bulunmuştur. Çeşitli ataklar karşısında gömülen ve çıkarılan imza görüntüsü arasındaki YBİ değerinin 0.89-0.91 aralığında olduğu gözlenmiştir.

Fikri mülkiyet haklarını ve telif hakkını korumak için doğal görüntülere iris görüntüsünün biyometrik deseninin gömüldüğü bir çalışmada AKD katsayıları damga gömmek için tercih edilmiştir [69]. Göz görüntüsünden iris şablonun elde etmek için öncelikle tüm görüntüden iris bölgesinin ayrılması gerekir. Bu amaçla, görüntüye göz bebeği ve iris sınırlarını ayırt etmek için Hough Dönüşümü (HD) uygulanır. HD önce iris ve sklera adı verilen göz akı sınırını belirlemek için, ardından göz bebeği ve iris sınırını ayırt etmek için uygulanır. Her bir yuvarlak şekil için çap, x koordinatı ve y koordinatı olmak üzere toplamda 6 parametre kaydedilir. Önce doğrusal HD kullanılarak üst ve alt göz kapağına bir çizgi geçirilerek göz kapakları izole edilir. Daha sonra, göz bebeğine en yakın olan iris kenarındaki ilk çizgi ile kesişen ikinci bir yatay çizgi çizilir. Kirpikler, göz görüntüsünün geri kalanıyla karşılaştırıldığında oldukça koyu olduğu için kirpiklerin izole edilmesi amacıyla bir eşikleme tekniği kullanılır. Daugmann'ın lastik levha (rubber sheet) modeline dayanan bir yöntem iris bölgelerinin normalizasyonu için kullanılır. Göz bebeğinin merkezi, referans nokta olarak kabul edilir ve radyal vektörler iris bölgesinden geçirilir. Her radyal çizgi boyunca bir dizi veri noktası seçilir ve bu, radyal çözünürlük olarak tanımlanır. İris bölgesi etrafında dolaşan radyal çizgilerin sayısı açısal çözünürlük olarak tanımlanır. Her bir radyal çizgi boyunca sabit sayıda nokta seçilir, böylece yarıçapın belirli bir açıda ne kadar dar veya geniş olduğuna bakılmaksızın sabit sayıda radyal veri noktası alınır. Özellik kodlaması, normalleştirilmiş iris deseninin 1-boyutlu Log-Gabor dalgacıklarıyla evriştirilmesiyle gerçekleştirilir. Log Gabor filtresi kullanılarak oluşturulan şablon, tek boyutlu bir vektöre dönüştürülür. Bu tek boyutlu vektör, görüntü damgalamak için sayısal damga olarak kullanılır. Elde edilen damgayı görüntüye gömmek için 8×8 AKD bloğunun orta frekans bandının iki katsayısı kullanılır. Bu iki katsayının rasgele seçilmesi yerine JPEG

nicemleme tablosuna bağlı olarak seçilmesi sinyal işleme saldırılarına ekstra dayanıklılık sağlamaktadır. 1024×1024 boyutlu taşıyıcı görüntünün kullanıldığı şemada, ikili damga boyutu 240 radyal yön boyunca 20 nokta seçilen polar iris görüntüsünün 2 katı uzunluğundadır. Elde edilen TSGO değeri gri seviye "Lena" görüntüsü için 79.8832 dB'dir. Çalışmanın dayanıklılığı sadece görüntü işleme ataklarına karşı test edilmiştir. Kurtarılan damga, kimlik doğrulama amacıyla veri tabanındaki örneklerle NK yardımıyla kıyaslanır. Grafiklere bakıldığında, veri tabanındaki numunelerden birinin NK değerinin diğerlerinin aksine son derece yüksek olması örneklerden biriyle açıkça eşleştirilmesi anlamına gelir.

[70]'te yazarlar göz görüntüsünden elde edilen iris özniteliklerini ses sinyaline gömmek için TDA alanında titreşim modülasyon nicemlemesi kullanmışlardır. İris özniteliklerini çıkarmak için [69]'da kullanılan yöntem uygulanmıştır. Örnek başına 16 bitte 44.1 KHz'te örneklenen ses dosyalarında deneyler yapılmıştır. Classic2 ses dosyasının Sinyal Gürültü Oranı (SGO) 25.1 dB olarak bulunmuştur. Yöntemin özellikle Gauss gürültüsüne karşı dayanıksız olduğu görülmüştür.

İris özniteliklerinin gri seviye görüntülere gömüldüğü bir çalışmada [71], ADD-TDA tabanlı kör olmayan bir yöntem önerilmiştir. İris verilerini damga olarak kullanmak için Bath Üniversitesinden elde edilen göz görüntüleri kullanılmıştır. Veri tabanında hem sol hem de sağ göz için ayrı ayrı 20 görüntü mevcuttur. Böylelikle 20 farklı kişiye ait sadece sol göz görüntülerinin alındığı 20×20 görüntüden oluşan (yani 400 görüntü) bir veri setinden yararlanılır. Bu 400 görüntü önce minimum sınırlı izotetik dikdörtgen (MSİD) formatında irisin normalleştirilmesi ve çıkarılması sürecine tabi tutulur. MSİD formatındaki görüntüler, her biri 120 × 200 piksel boyutunda normalize edilmiş dikdörtgen iris şablonları elde etmek için işlenir. Normalize edilmiş 120×200 boyutlu iris görüntülerine, 1×200 boyutlu piksel seti elde etmek için sütun bazında, bir boyutlu AKD uygulanır ve ardından her bir sütunun DC değeri korunur. Bu 200 DC değeri, ikili yani 200×8 bit formatına dönüştürülür ve bu bit dizisine Döngüsel Artıklık Denetimi (DAD) tabanlı hata kontrol kodlaması eklenir. İkili damga elde edildikten sonra, görüntü ADD ile alt bantlarına ayrıştırılır ve her bir alt banda TDA uygulanır. İristen elde edilen ikili damga öz değer matrislerine gömülür. Damgalanmış görüntünün TSGO değeri 53 dB ve üzeri bulunmuştur. Çalışmada ataklara karşı dayanıklılık sonuçları verilmemiştir. Ancak 11 farklı tipte atak için toplam 77 farklı durumun doğru algılama, yanlış reddetme ve yanlış kabul sayıları verilmiştir. Yaklaşık olarak yanlış reddetme oranı toplam durumun %9.75'ini, yanlış kabul oranı %0.3'ünü, doğru kabul oranı ise %89.85'ini oluşturmaktadır.

[72]'de Bath Üniversitesi'nden alınan veri tabanı kullanılarak damgalama yapılmıştır. Göz görüntülerinden kirpik, göz akı, göz kapağı gibi faktörleri elimine etmek için MSİD formatı uygulanır ve 120 × 200 piksel boyutunda normalize edilmiş dikdörtgen iris şablonları elde edilir. İris şablonunun her bir sütununa bir boyutlu AKD uygulanır ve elde edilen 200 DC değer 8 bit formatında ikili değere dönüştürülür. 1600 bitlik bu ikili dizi 4 parçaya bölünüp, her bir parça Bose, Chaudhuri, and Hocquenghem (BCH) hata kontol kodlamaya tabi tutulur. Elde edilen ikili damgayı standart gri seviye test görüntüsüne gömmek için görüntü önce dört eşit parçaya bölünür. Her bir parçaya ayrı ayrı AKD uygulanır. AKD ile dönüştürülmüş alt görüntülere TDA uygulanır. Damga tekil değer matrisine gömülür. Ters dönüşümler yardımıyla damgalanmış görüntü elde edilir. Damga kör olmayan yöntemle çıkarılır. Çalışmada algılanamazlık ve dayanıklılık sonuçları rapor edilmemiştir. 400 görüntü üzerinde 10 farklı atak grubundan oluşan toplamda 70 farklı durum karşısında kimlik doğrulama performansı ölçülmüştür. Elde edilen bulgulara göre yanlış reddetme oranı toplam durumun yaklaşık %8.66'sını, yanlış kabul oranı yaklaşık %0.52'sini, doğru kabul oranı ise yaklaşık %90.82'sini oluşturmaktadır.

[73]'te ICE-Right iris veri tabanı kullanılmıştır. Göz görüntüsü üzerinde $N \times M$ konumlarından bir ızgara oluşturulur ve Karmaşık Gabor Dalgacıkları, bu ızgaranın bir iç çarpımı tarafından yapılır. Sonuç olarak, karmaşık iç çapımlar elde edilir ve ardından 2 bit olarak nicelendirilir. Ayrıca bunlar, 2 bitlik hücrelerin $N \times M$ dizisinin bir kodunda toplanır. Elde edilen 256 baytlık (2048 bit) iris kodu damga olarak kullanılır. Damga yerleştirme işleminde ilk dört bayttan damgalama pozisyonunu belirlemede yararlanılır. Geri kalan bitleri uzaysal alanda EAB tekniğine göre gömmek için XOR fonksiyonundan faydalanılır. Damga çıkarma aşamasında, orijinal içerik yerine damgalanmış içerik kullanılarak XOR işlemi tekrarlanır. Sahte giriş görüntüsü veya sahte iris kodu girilmesi durumunda, sistem orijinal ile aynı olmayan, tanımlanamayan bir görüntü üretir. Çalışmanın sonuçları yalnızca tuz ve biber gürültüsü, Gauss filtreleme ve kırpmaya karşı test edilmiştir.

Parmak izi, parmak damarı, avuç içi damarı, yüz, retina gibi farklı biyometrik modeller arasında iris, en güvenilirlerinden biridir. İris özniteliklerinin önemli ölçüde benzersiz olması neticesinde yanlış kabul oranı ve yanlış reddetme oranı dikkate değer ölçüde daha düşüktür. Bunun yanı sıra kopyalanmasının zor olması ve durağan olması gibi özellikleri de göz önünde bulundurulunca tez kapsamında iris verisine odaklanılmış ve yalnızca iris verisinin orijinal görüntülere gömüldüğü tek modelli dayanıklı sistemler tasarlanmıştır.

1.7.2.2. Çok Modelli Biyometrik Damgalama Şemaları

Bu bölümde, iki veya daha fazla biyometrik özelliğin bir arada yer aldığı çalışmalara değinilmiştir. Tez çalışmasında damga olarak iris verisi tercih edildiği için irisle birlikte farklı biyometrik verilerin damga olarak kullanıldığı literatür çalışmalarına yer verilmiştir.

[108]'de parmak izi ve iris görüntüleri farklı birleştirme teknikleriyle birleştirilip, gri seviye görüntülere çeşitli gömme yöntemleri kullanılarak gömülmüştür ve bunların kıyaslaması yapılmıştır. Birleştirme yöntemi olarak, Temel Bileşenler Analizi (TBA), ADD, LP ve Yoğunluk-Renk-Doyum dönüşümü test edilmiştir. Birleşim için ADD yönteminin daha iyi olduğu karşılaştırmalar sonucu tespit edilmiştir. UBIRIS veri tabanından elde edilen 150×200 piksellik göz görüntüsünden 64×512 boyutlu dikdörtgensel iris görüntüsü elde edilir. Parmak izi için giriş olarak 200×200 piksel boyutundaki görüntüler alınır. Elde edilen çıktı görüntüsünün iskeletleştirilmiş versiyonu 200×200 piksel boyutundadır. Her iki görüntü de 512×512 piksel olarak yeniden boyutlandırılır. ADD yardımıyla birleştirilmiş çıktı görüntüleri de 512×512 piksel boyutundadır. Burada AKD, TDA ve Bakteriyel Besin Arama Optimizasyonu (BBAO) yöntemleriyle damgalama gerçekleştirilir. AKD ve TDA yöntemiyle elde edilen TSGO değeri 30 ve 40 dB arasında değişirken, BBAO yöntemi daha iyi (50 dB civarında) TSGO değerine sahiptir. Ataklar karşısında NK ve Normalleştirilmiş Mutlak Hata (NMH) açısından da BBAO'nun daha iyi sonuç verdiği (NK 0.94 üzeri, NMH yaklaşık 0.003) rapor edilmişse de bu atakların ne olduğuna ve özelliklerine değinilmemiştir.

[56]'da iris görüntüsü ve parmak izi görüntüsünden çıkarılan özelliklerin füzyonu ile oluşturulan sayısal desen, sayısal görüntü ve ses sinyalleri üzerine gizlenerek damgalama gerçekleştirilmiştir. CASIA veri tabanından elde edilen iris görüntülerinin şablonu değiştirilmiş Daugmann'ın lastik levha modeli yardımıyla çıkarılır ki; açısal çözünürlük ve radyal çözünürlük benzersiz tanımlama için yeterli bilgi sağlayabilsin. Parmak izi verilerini elde etmek için bu çalışmada Digital Persona U.are.U. 4500 parmak izi tarayıcı kullanılmıştır. Parmak izindeki ayrıntı noktaların açı ve koordinatları benzersiz tanımlama için şablon olarak kullanılır. Damga oluşturmada, bu iki biyometrik özelliğin stratejik olarak birleştirilmesi için kombinasyonel lojik işlemi kullanılır. Nihai ikili damga boyutu 9600 bit olarak tanımlanmıştır. Sayısal görüntünün damgalaması için, öncelikle görüntü 8×8 piksel boyutundaki örtüşmeyen görüntülere ayrılır. Her bloğa AKD uygulanarak görüntü dönüşüm alanına taşınır. Orta frekans bandından iki katsayı JPEG nicemleme tablosuna bağlı olarak

damga gömmek için seçilir. Gömülecek damga biti 1 ise ilk katsayının ikinciden büyük olması beklenirken, 0 gömmek için ilk katsayının ikinciden küçük olması beklenir. Eğer bu koşul sağlanmazsa, katsayılar yer değiştirilir. Renkli "Lena" görüntüsü için TSGO 91.56 dB olarak bulunmuştur. Çalışmanın dayanıklılığı sadece bazı görüntü işleme atakları için test edilmiştir. NK değeri 0.9'un üstünde hesaplanmış olsa da BHO değerlerinin oldukça kötü olduğu tespit edilmiştir.

İris ve parmak izinin damga olarak kullanıldığı bir başka çalışmada [109], AKD tekniği damga gömme alanı olarak seçilmiştir. İris görüntüleri CASIA veri tabanından, parmak izi görüntüleri ise FVC2004 veri tabanından alınmıştır. Parmak izi ayrıntı noktaları çıkarıldıktan sonra, her bir ayrıntı noktası ile ilişkili olan ve dönmeye karşı değişmeyen 15 özel özellik vektörü oluşturulmuştur. Bir parmak izi şablonu ortalama 25 ayrıntı noktadan meydana geldiği ve her bir vektör 4 bit akışı ile temsil edildiği için parmak izinden elde edilen damga boyutu yaklaşık 1500 bitten oluşur. Parmak izi eşleştirme Öklit Uzaklığına dayalı özel tanımlanmış bir benzerlik seviyesi ile yapılır. Göz görüntülerine gelince, irisin iç ve sınırlandırılmış dış sınırı arasındaki bölge Daugmann'ın lastik levha modeli ile sabit boyutlarda dikdörtgen şeride dönüştürülür. Damga olarak kullanılan iris çekirdek özelliğinin boyutu, 348 bittir. Giriş iris özelliği ile alınan iris özelliği arasındaki eşleştirme, standart Hamming Uzaklığı (HU) ile yapılır. Bu çalışmada damgayı gri seviye görüntüye gömmek için, öncelikle orijinal görüntü 8×8 piksel boyutundaki örtüşmeyen bloklara ayrılır ve her bloğa AKD uygulanır. Damganın gömüleceği bloklar Hessian matris yardımıyla seçilir. Damgayı düşük frekans bandındaki AC bloklara gömmek için 8 komşu AKD bloktaki DC değerlerden yararlanılır. Damga çıkarma adımının kör olarak gerçekleştiği bu şemada 512×512 boyutlu damgalanmış gri seviye "Cameraman" görüntüsü için TSGO değeri 38.2340 dB olarak bulunmuştur. Önerilen yöntemin dayanıklılığı BHO üzerinden ölçülmüştür. Yöntemin doğrulama performansı Yanlış Kabul Oranı (YKO) ve Yanlış Reddetme Oranına (YRO) bağlı hesaplanan Eşit Hata Oranı (EHO) ile test edilmiştir. Deneysel sonuçlara göre damgalanmış ancak herhangi bir saldırıya uğramamış bir görüntüden çıkarılan parmak izi öznitelikleri için EHO %6.40 iken, iris desenleri için bu değer %3.60 olarak bulunmuştur. Damgalama gerçekleşmeden iris ve parmak izinin modifiye yaklaşımla birleştirilmesiyle elde edilen çaprazlama noktasının ise %1.2 olduğu tespit edilmiştir.

İris ve parmak izinin bir arada kullanıldığı bir başka çalışmada [57], Bağımsız Bileşenler Analizi (BBA) damgalama alanı olarak tercih edilmiştir. Orijinal görüntü BBA tabanlarını oluşturmak için önce 4 gözlem görüntüsüne bölünür. Daha iyi bir dayanıklılık

elde etmek için en yüksek enerjili iki taban damga gömmek için seçilir. Parmak izi görüntüsü Arnold dönüşümü yardımıyla karıştırıldıktan sonra birinci tabana gömülürken, ikili haldeki iris şablonu ikinci tabana gömülür. Damgalanmış tabanlara ters BBA dönüşümü uygulanarak damgalanmış görüntü elde edilir. Parmak izi görüntüsünün çıkarılması için orijinal görüntü gerekliyken, iris şablonunu geri kazanmak için orijinal görüntüye ihtiyaç yoktur. Parmak izi görüntüsünü eşleştirmek için eşleştirme skoru kullanılan çalışmada, iris şablonunun kimlik doğrulaması HU'ya bağlı olarak yapılır. Bu iki biyometrik özelliğin kimlik doğrulamasını eş zamanlı yapmak için normalleştirilmiş skorların ağırlıklı toplamından yararlanılır. Çalışmada kullanılan parmak izi ve iris verileri SDUMLA-HMT veri tabanından elde edilmiştir. Damgalanmış ancak saldırıya uğramamış "Lena" görüntüsünden, parmak izi için EHO 6.52, iris için EHO 3.57, bu iki biyometrik özelliğin kimlik doğrulaması eş zamanlı yapıldığında ise EHO 0.50 olarak bulunmuştur.

AADD kullanılan bir biyometrik damgalama şemasında, iris ve yüz verilerinden damga oluşturmada yararlanılmıştır [110]. SDUMLA-HMT veri tabanının kullanıldığı bu çalışmada, gri seviye iris görüntüsü birinci damga ve ikili haldeki yüz öz nitelikleri ikinci damga olarak kullanılır. Damga gömme aşamasında ilk olarak, orijinal görüntüye L seviye AADD uygulanır. Bu ayrışma sonucu bir alt bant seçilir ve rasgele hale getirilir. Arnold'ın kedi haritası yardımıyla karıştırılan damgaya ve seçilen alt banda TDA uygulanır. Alt bandın tekil değerlerine, damganın tekil değerleri bir ölçekleme faktörü ile çarpılarak eklenir. Ters TDA ile modifiye edilmiş alt bant elde edilir. Rasgele hale getirme işlemi ve AADD işleminin sırasıyla tersi alınarak damgalanmış görüntü elde edilir. Ardından ikili haldeki yüz öz niteliklerinin gömülmesi için, hata yayma yöntemi kullanılarak damgalanmış görüntünün yarı tonlu sürümü elde edilir ve yarı tonlu görüntü ikili damga ile bit bazında EX-OR işlemine tabi tutulur. EX-OR işleminin sonucu, ikili damgayı kurtarmak için gizli anahtar olarak çıkarma aşamasında kullanılır. İrisin çıkarılması ise orijinal içeriğe bağlı olarak yapılır. İris ve yüz özniteliklerinin kimlik doğrulaması d1 uzaklık ölçütü ile gerçekleştirilir. Elde edilen bulgulara göre 512×512 boyutlu damgalanmış gri seviye "Lena" görüntüsü için TSGO değeri 36.85 dB'dir. Çalışmada farklı ataklar karşısında NK değeri ölçülerek dayanıklılık test edilmiştir. Kimlik doğrulama aşamasına gelince damgalanmış ve atak uygulanmamış görüntüden çıkarılan iris görüntüsü için EHO değeri 4.24, yüz öznitelikleri için EHO değeri 6.68 ve birleştirilmiş skor için EHO değeri 0.52 olarak bulunmuştur.

AADD ve TDA'nın damgalama alanı olarak kullanıldığı bir çalışmada [111] parmak izi, iris ve imza verileri renkli görüntülere gömülmüştür. Damgalama gerçekleşmeden önce

bu üç damga AKD ve normal dağılım matrisi yardımıyla sıkıştırılmış algılama ölçümlerine çevrilmiştir. Damgalanmış renkli görüntü elde etmek için her bir damganın sıkıştırılmış algılama ölçümlerinin tekil değeri, orijinal görüntünün R, G ve B kanallarından birinin düşük frekanslı dalgacık katsayılarının tekil değerlerine ölçekleme faktörü yardımıyla eklenir. Damga çıkarma adımında orijinal görüntüye ihtiyaç duyulan bu yöntemde elde edilen TSGO değeri 43.56 dB ve çeşitli sinyal işleme atakları, rotasyon ve kırpmaya karşı ortalama NK değeri ise 0.9979 bulunmuştur. Ancak çıkarılan damgaların hiç birinde kimlik doğrulama performansı test edilmemiştir.

Tablo 1.2'de iris biyometrik verilerinin doğal görüntülere gömüldüğü yukarıda bahsi geçen tek modelli ve çok modelli dayanıklı damgalama yöntemlerinin bir özeti yer almaktadır. Biyometrik damgalamaya yönelik çalışmalarda, genellikle dayanıklılık ve algılanamazlığın yanı sıra geleneksel damgalamadan farklı olarak biyometrik özelliklerin kimlik doğrulama performansları da dikkate alınmıştır. Tek biyometrik özelliğin doğrulama hassasiyetinin yeterli bulunmadığı durumlarda, bireysel ölçümlerin güçlerini artırmak ve zayıflıklarını azaltmak amacıyla birden fazla bağımsız biyometrik özellik çeşitli birleştirme teknikleriyle birleştirilmiştir (çok modelli biyometrik damgalama). Etkili bir birleştirme şeması kimlik doğrulama performansını artırmaya yardımcı olur. Ancak tek modelli biyometrik sistemlere kıyasla hesaplama ve depolama için daha fazla kaynak gerektirirler.

Tablo 1.2. İris tabanlı biyometrik damgalama yöntemleri

Kaynak Çalışma	Biyometrik Özellik	Dönüşüm Alanı	Veri Tabanı	Orijinal İçerik	Damga Boyutu	Damga Çıkarma	Gözlem
[69]	İris	AKD	Belirtilmemiş.	1024×1024 boyutlu görüntü	$2 \times 20 \times 240$	Kör	-TSGO = 79.8832 dB, -Sınırlı sayıda görüntü işleme atakları test edilmiştir.
[70]	İris	TDA	Belirtilmemiş.	Ses Sinyali, Örnek başına 16 bitte 44.1 KHz'de örneklenen ses dosyaları	$2 \times 20 \times 240$	Kör	-SGO = 25.1 dB, -Sınırlı sayıda atak test edilmiştir.
[71]	İris	ADD-TDA	Bath Üniversitesi	Belirtilmemiş.	1600 bit + DAD kodu	Kör Olmayan	-TSGO = 53 dB, -Dayanıklılık test edilmemiştir, -Yanlış reddetme oranı toplam durumun %9.75'ini, -Yanlış kabul oranı %0.3'ünü, -Doğru kabul oranı ise %89.85'ini oluşturmaktadır.
[72]	İris	AKD-TDA	Bath Üniversitesi	Belirtilmemiş.	4×511	Kör Olmayan	-Algılanamazlık belirtilmemiştir, -Dayanıklılık test edilmemiştir, -Yanlış reddetme oranı toplam durumun yaklaşık %8.66'sını, Yanlış kabul oranı yaklaşık %0.52'sini, -Doğru kabul oranı ise yaklaşık %90.82'sini oluşturmaktadır.

Tablo 1.2'nin devamı

Kaynak Çalışma	Biyometrik Özellik	Dönüşüm Alanı	Veri Tabanı	Orijinal İçerik	Damga Boyutu	Damga Çıkarma	Gözlem
[73]	İris	EAB (XOR)	ICE-Right (NIST)	1024×1024 boyutlu gri seviye görüntü, 512×512 boyutlu gri seviye ve renkli görüntü	2016 bit	Kör (Orijinal içerik yerine damgalanmış içerik kullanılarak çıkarılır.)	-Çalışmanın sonuçları yalnızca tuz ve biber gürültüsü, Gauss filtreleme ve kırpmaya karşı test edilmiştir.
[56]	Parmak izi + iris	AKD	Parmak izi Digital Persona U.are.U. 4500 parmak izi tarayıcı, İris CASIA.	1024×1024 boyutlu renkli ve gri seviye görüntü	9600 bit	Kör	-Renkli "Lena" görüntüsü için TSGO 91.56 dB, -Dayanıklılık sadece bazı görüntü işleme atakları için test edilmiştir, -NK değeri 0.9'un üstündedir, -BHO değerleri oldukça kötü bulunmuştur.
[57]	Parmak izi + iris	BBA	SDUMLA-HMT	512×512 boyutlu gri seviye görüntü	İris 20×240, parmak izi 256×256	Parmak izi kör olmayan, iris kör	-Parmak izini eşleştirmek için eşleştirme skoru, -İris şablonunu eşleştirmek için HU, -Parmak izi için EHO 6.52, -İris için EHO 3.57, -İki biyometrik özellik birlikte değerlendirildiğinde EHO 0.50.

Tablo 1.2'nin devamı

Kaynak Çalışma	Biyometrik Özellik	Dönüşüm Alanı	Veri Tabanı	Orijinal İçerik	Damga Boyutu	Damga Çıkarma	Gözlem
[108]	Parmak izi + iris	3 yöntem AKD, TDA, BBAO	İris UBIRIS, Parmak izi gerçek zamanlı	512×512 boyutlu gri seviye görüntü	İris ve Parmak izi 512×512	Kör Olmayan	-Parmak izi ve iris ADD ile birleştirilmiştir, -BBAO tabanlı yöntem daha iyi sonuç vermiştir (TSGO yaklaşık 50 dB, NK 0.94 üzeri, NMH yaklaşık 0.003).
[109]	Parmak izi + iris	AKD	Parmak izi FVC2004, İris CASIA	512×512 boyutlu gri seviye görüntü	Parmak izi yaklaşık 1500 bit, iris 348 bit	Kör	-TSGO 38.2340 dB, -Parmak izini eşleştirmek için Öklit uzaklığı, -İrisi eşleştirmek için HU, -Parmak izi için EHO (%) 6.40, -İris için EHO (%) 3.60.
[110]	Yüz + iris	AADD-TDA	SDUMLA-HMT	512×512 boyutlu gri seviye görüntü	İris 512×512, Yüz belirtilmemiş.	Kör Olmayan	-TSGO 36.85 dB, -İris ve parmak izi eşleştirme için d1 uzaklığı, -İris için EHO 4.24, -Yüz öznitelikleri için EHO 6.68, -İki biyometrik özellik birlikte değerlendirildiğinde EHO 0.52.
[111]	Parmak izi + iris + imza	AADD-TDA	Belirtilmemiş	176×176 ve 128×128 boyutlu renkli görüntü	128×128	Kör Olmayan	-TSGO 43.56 dB, -Ataklar karşısında ortalama NK0.9979 -Kimlik doğrulama hassasiyeti ele alınmamıştır.

1.8. Tezin Kapsamı

Sayısal teknolojilerin gelişmesiyle, görüntü, video, ses ve metin gibi sayısal içerikler erişim ve zaman kısıtlamaları olmadan internet üzerinden kolayca aktarılır. Bu durum, çoklu ortam verilerinin yasa dışı amaçlarla kolayca çoğaltılmasına veya değiştirilmesine izin verir. Sayısal damgalama, çoklu ortam verilerini yönetmek, yasadışı kopyalama ve manipülasyona karşı korumak ve bundan kaynaklanan telif hakkı sorunlarını ortadan kaldırmak için etkili bir çözüm sağlar. Bu tez çalışmasında, sayısal damgalamadan doğal görüntülerin telif hakkı ve fikri mülkiyet haklarının korunması amacıyla yararlanılmıştır. Doğal görüntülerde damgalama yaparken görsel kalitenin korunmasının yanı sıra, farklı ataklar karşısında dayanıklılığın üst düzeye çıkarılması amaçlanmıştır. Ayrıca biyometrik damgalama alanında algısal şeffaflıktan ve dayanıklılıktan ödün vermeden, tek bir biyometrik veriden yararlanarak içeriğin gerçek sahibini doğrulamada hata oranını minimize etmeye yönelik yeni yöntemler geliştirilmiştir.

Tezde yer alan çalışmaları iki ana başlık altında toplamak mümkündür. İlk kısımda, geleneksel damgalamaya yönelik sistem tanıtılmıştır. Burada ADD ile TDA'nın üstünlüklerinden yararlanan yeni bir gri seviye görüntü damgalama şeması önerilmiştir. İkili görüntünün damga olarak yer aldığı bu yöntemde, damga gömme adımında kullanılan ölçekleme faktörü ABA'nın değiştirilmiş sürümü olan Kendinden Uyarlanabilir Adımlı ABA (KUAABA) ile optimize edilmiştir.

Çalışmanın ikinci kısmında, ADD'nin dönme ve görüntü çevirme gibi geometrik ataklara karşı dayanıklılığını iyileştirmek için YDDADD'nin dönüşüm tekniği olarak tercih edildiği biyometrik damgalama sistemleri sunulmuştur. Bu bölümde, iris verisinden elde edilen kod renkli görüntülere gizlenmiştir. YDDADD alanında, TDA ve ona alternatif olabilecek etkili ayrıştırma tekniklerine (QR Ayrıştırma ve Schur Ayrıştırma) dayanan damgalama şemaları tasarlanmış ve performansları incelenmiştir. Ayrıca damgalama sürecinde sabit, ABA ile optimize edilmiş ve KUAABA ile optimize edilmiş eşik değerler, önerilen her sistem için ayrı ayrı kullanılarak algılanamazlık, dayanıklılık ve biyometrik verinin doğrulama performansı açısından en uygun yöntem belirlenmeye çalışılmıştır.

Tezin ikinci bölümünde, sonuçlardan bağımsız olarak geleneksel damgalamaya ve biyometrik damgalamaya yönelik yapılan çalışmalar detaylandırılmıştır. Tezin üçüncü bölümünde, tespit edilen en uygun sistem için deneyler sonucu elde edilen bulgular irdelenmiş ve bu bulguların yaygın kullanılan değerlendirme ölçütleri ile başarı oranları

gösterilmiştir. Ayrıca literatürde var olan damgalama çalışmalarıyla önerilen sistemlerin mukayesesi yapılmıştır. Son olarak tezin dördüncü ve beşinci bölümlerinde bu çalışmaların sonuçlarından, önerilerden ve gelecekteki çalışmalardan bahsedilmiştir.

2. YAPILAN ÇALIŞMALAR

Tez kapsamında sayısal görüntülerde telif hakkı korumaya yönelik dayanıklı damgalama çalışmaları üzerinde durulmuştur. Telif hakkı koruma uygulamalarının hem dayanıklılığının yüksek olması hem de algılanamazlık kriterini karşılaması gerekir. Ancak bu gereksinimler birbirleriyle çelişmektedir. Bu nedenle, damgayı gömmek için orijinal içerikte yapılması gereken değişikliklerin miktarının algılanamazlık ve dayanıklılık arasında iyi bir denge sağlanacak şekilde belirlenmesi çok önemlidir. Bu değişiklik miktarları genellikle gömme gücü adı verilen parametreler tarafından ayarlanır. Çoğu damgalama yönteminde, damganın gömme gücünü belirleyen ölçekleme faktörünün sabit alınması içeriğin her bir bölümünün yapısının dikkate alınmaması nedeniyle genellikle iyi algılanamazlık ve dayanıklılık sonuçları üretmez. Ölçekleme faktörlerinin yüksek değerleri, damgalamanın dayanıklılığını arttırırken damgalanmış içeriğin şeffaflığını azaltır. Öte yandan, ölçekleme faktörlerinin düşük değerleri, algılanamazlığı korur, ancak dayanıklılığı olumsuz etkiler. Görüldüğü üzere bu faktörleri seçmek zordur ve algılanamazlık ve dayanıklılık arasında iyi bir değiş tokuşa ulaşmak için optimal çoklu ölçekleme faktörlerini bulma hususunda verimli ve güçlü bir algoritma gereklidir. O nedenle tez kapsamında öncelikle blok tabanlı geleneksel damgalama yöntemi ile her görüntü ve bloğa özgü optimal ölçekleme faktörünü belirlemeye yönelik çalışma gerçekleştirilmiştir. Ardından damganın fiziksel veya mantıksal sahipliği sorununu çözmek için biyometrik tabanlı damgalamaya odaklanılmıştır. O nedenle yapılan çalışmaları geleneksel ve biyometrik damgalama çalışmaları olarak iki ana başlık altında incelemek mümkündür.

Bölüm 2.1'de, geleneksel damgalama alanında yapılan gri seviye görüntüler üzerindeki ADD-TDA-KUAABA tabanlı yöntemin [112] detayları verilmiştir. Burada FLD yardımıyla karıştırılan ikili görüntü orijinal görüntüye ADD-TDA alanında gömülmüştür. Damga gömme sürecinde her bloğa özgü seçilen ölçekleme faktörü algılanamazlık ve dayanıklılık arasındaki ödünleşimi belirlemek üzere KUAABA tarafından optimize edilmiştir. Bölüm 2.2'de ise renkli görüntüler üzerinde gerçekleştirilen YDDADD alanında biyometrik damgalamaya değinilmiştir. Geometrik ataklardaki üstünlüğünden dolayı tercih edilen YDDADD üç farklı ayrıştırma tekniği ile birlikte ele alınmıştır. Bu teknikler TDA, QR Ayrıştırma ve Schur Ayrıştırma'dır. Damga gömme sürecinde her teknik için kullanılan ölçekleme faktörleri hem sabit seçilerek, hem de ABA ve KUAABA ile ayrı ayrı optimize

edilerek performansları araştırılmıştır. Elde edilen sonuçlar dayanıklılık, algılanamazlık ve biyometrik verinin kimlik doğrulama hassasiyeti açısından değerlendirilerek en uygun yöntem belirlenmeye çalışılmıştır.

2.1. Geleneksel Damgalamaya Yönelik Çalışma

Sayısal görüntülerde telif hakkı korumaya yönelik damgalama tekniklerinde göz önünde bulundurulması gereken temel iki hususdan biri orijinal görüntü ve damgalanmış görüntü arasındaki farkı ifade eden algılanamazlık ve diğeri damgalanmış görüntüye saldırılar gerçekleştikten sonra bile damganın başarılı bir şekilde algılanmasına işaret eden dayanıklılıktır. Çoğu damgalama tekniğinde, damgayı gömmek için orijinal görüntülerde meydana gelecek değişim miktarı farklılık gösterir. Dolayısıyla, değişim miktarını damgalama yönteminin algılanamazlığı ve dayanıklılığı arasında iyi bir denge kuracak şekilde belirlemek çok önemlidir. Genellikle bu miktar ölçekleme faktörü ya da gömme gücü adı verilen parametrelerle ayarlanır. Birçok damgalama yönteminde içeriğin her bir bölümünün özelliklerini göz ardı eden tek ölçekleme faktörü kullanılır. Bu durum algılanamazlık ve dayanıklılık sonuçlarını olumsuz etkileyebilir. Algılanamazlık ve dayanıklılık arasında iyi bir denge kurmak amacıyla çoklu ölçekleme faktörlerini optimize etmede sezgisel yöntemlerden yararlanılabilir. Bu nedenle, gri seviye görüntülerin telif hakkının korunmasını amaçlayan bu çalışmada KUAABA ile optimize edilmiş ADD-TDA tabanlı damgalama yöntemi önerilmiştir. Yöntemin detayları alt başlıklar halinde incelenmiştir.

2.1.1. ADD-TDA-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntem

Görüntü damgalama şemalarının performansının, ADD, AKD ve AFD gibi diğer dönüşümlerle TDA kullanılarak geliştirilebileceği açıktır [89]. ADD'nin de, iyi uzaysal yerelleştirme sağlaması ve İGS'ye benzer çoklu çözünürlük özelliklerine sahip olmasından dolayı ADD-TDA alanı damgalama açısından ilgi çekici hale gelmiştir.

Bu çalışmada, dayanıklılığı geliştirmesi açısından ADD sonucu elde edilen düşük frekanslı alt bant (LL) tercih edilmiştir. LL bandın bloklarına TDA uygulandığında üç matris elde edilir. [113]'te yazarlar, TDA tabanlı damgalama algoritmalarını geliştirmek amacıyla

damgayı TDA'nın U bileşenine gömerken algılanamazlığı ve kapasiteyi artırmak adına katsayıları değiştirmek için bir kılavuz sunmuşlardır. Bu kılavuza göre, U matrisinin sütun vektöründeki katsayıları değiştirmek, satır vektöründeki katsayıları değiştirmekten daha az görünür bozulmaya neden olacaktır. [114]'te ise, orijinal görüntü bloğunun U matrisi ile bozulmuş görüntü bloğunun U matrisinin sadece ilk sütunundaki katsayıların sayısal sembollerinin değişmez olduğu, diğer sütunlar için ise sayısal sembollerin değiştiği rapor edilmektedir. Dolayısıyla, U bileşeninin yalnızca ilk sütununun değişmez büyüklük ilişkisini koruduğu düşünülmektedir. Bu durum, Şekil 2.1'de verilen örnek orijinal görüntü bloğu ve bozulmuş görüntü bloğuna ait U bileşeninin katsayılarında görülmektedir. Bu nedenle bu çalışmada U bileşeninin modifikasyonuna dayanan kör bir damgalama sistemi önerilmiştir. Çalışmada ayrıca güvenliği sağlamak amacıyla damga bilgisi gömülmeden önce Fibonacci-Lucas Dönüşümü (FLD) yardımıyla karıştırılır ve ikili damga anlamsız bir hale getirilir. Damga çıkarıldıktan sonra da tekrar ters FLD ve güvenlik anahtarı yardımıyla orijinal haline getirilmeye çalışılır. Bu çalışmada ayrıca dayanıklılık ve algılanamazlığı dengelemek amacıyla ABA'nın değiştirilmiş sürümü olan KUAABA tercih edilmiştir.

(a) Orijinal blok

158	156	158	159
157	156	156	156
157	158	156	153
155	154	153	154

(b) (a)'nın JPEG sıkıştırılmış versiyonu

155	155	155	154
155	155	154	154
155	154	154	154
154	154	154	154

(c) (a)'nın U bileşeni

-0.5056	0.6127	-0.4989	0.3466
-0.5008	0.0840	0.0122	-0.8614
-0.5000	-0.7818	-0.3076	0.2101
-0.4936	0.0792	0.8102	0.3061

(d) (b)'nin U bileşeni

-0.5012	0.6532	0.2678	-0.5004
-0.5004	-0.2708	0.6545	0.4980
-0.4996	-0.6536	-0.2729	-0.4988
-0.4988	0.2699	-0.6523	0.5028

Şekil 2.1. TDA ile dönüştürülmüş orijinal blok ve JPEG sıkıştırılmış bloğun U bileşeninin katsayıları arasındaki ilişki

2.1.1.1. Kullanılan Teorik Kavramlar

Bu bölümde güvenlik düzeyini artırmak için tercih edilen ve görüntü karıştırma yöntemlerinden biri olan FLD ayrıntılı olarak tanıtılmıştır. Ayrıca ABA'nın özellikleri ve uygulanma adımları verildikten sonra KUAABA'ya ait detaylar ele alınmıştır.

2.1.1.1.1. Fibonacci Lucas Dönüşümü (FLD)

Arnold'ın kedi haritası, Fibonacci-Q dönüşümü gibi görüntü karıştırma yöntemleri, son yıllarda sayısal damgalama ve steganografide güvenliği sağlamak için yaygın olarak kullanılmaktadır. Karıştırma yöntemleri anlamlı bir görüntüye uygulandığında, görüntünün piksellerini karıştırarak onu şifreler. Böylece görüntü tamamen anlamsız bir forma dönüşür. Çalışmada, [115] tarafından önerilen Fibonacci ve Lucas serilerine dayanan bir karıştırma yöntemi kullanılmıştır. FLD hem basit hem de güçlü 2×2 boyutlu kaotik bir haritadır. Lucas serisi, Fibonacci serisinin özel bir halidir. Fibonacci serisi ve Lucas serisi (2.1) ve (2.2)'de tanımlanmıştır.

$$F_n = \begin{cases} 0, & n = 1 \\ 1, & n = 2 \\ F_{n-1} + F_{n-2}, & değilse \end{cases} \tag{2.1}$$

$$L_n = \begin{cases} 2, & n = 1 \\ 1, & n = 2 \\ L_{n-1} + L_{n-2}, & değilse \end{cases} \tag{2.2}$$

Fibonacci ve Lucas serilerine bağlı olarak FLD (2.3)'teki gibi tanımlanır.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{n} \tag{2.3}$$

Denklemin ilk satırı Fibonacci serisini, ikinci satırı ise Lucas serisini içerir. Fibonacci serisi, çekirdek değeri (0 ve 1) değiştirilerek birkaç farklı kombinasyona dönüştürülebilir.

Örneğin $Fibo_{11}$ serisi, çekirdek değerlerinin 1 ve 1'e atandığı Fibonacci serisinin bir versiyonudur. Bu serilerin elemanları aşağıdaki gibidir:

$$\begin{aligned} Fibo_{11} &= 1,1,2,3,5,8,13,21,34,\ldots \\ Fibo_{31} &= 3,1,4,5,9,14,23,37,60,\ldots \\ Fibo_{32} &= 3,2,5,7,12,19,31,50,81,\ldots \end{aligned} \tag{2.4}$$

FLD, periyodiklik özelliğine sahiptir. Bu nedenle, belirli bir yinelemeden sonra orijinal görüntü elde edilir. Arnold'un kedi haritası ve Fibonacci-Q tek bir 2×2 harita kullanırken, FLD'nin bir dizi 2×2 haritası vardır. Bu nedenle diğer kaotik haritalara göre daha yüksek güvenlik sağlar. Görüntünün şifrelenmesi ve şifresinin çözülmesi, karıştırılacak yineleme sayısını belirleyen aynı güvenlik anahtarıyla yapılır.

2.1.1.1.2. Kendinden Uyarlanabilir Adımlı Ateş Böceği Algoritması (KUAABA)

ABA, Yang tarafından önerilen biyolojiden esinlenmiş meta-sezgisel bir algoritmadır [116]. Çok modelli ve lineer olmayan optimizasyon problemlerini çözmek için geliştirilmiştir. Ateş böceklerinin birbirleriyle iletişim kurmada veya doğal ışığı gösteren biyolüminesans süreciyle eşleri bulmadaki içgüdüsel davranış örüntüsünden esinlenmiştir [117-119]. Sadelik, kolay uygulama, esneklik, bu algoritmanın güçlü noktalarıdır [120]. Algoritmanın inşasında dikkate alınan bazı kurallar aşağıda verilmiştir [121]:

1. Ateş böcekleri üniseks olduklarından cinsiyetten bağımsız olarak birbirlerini etkilerler.
2. Çekicilik parlaklığa bağlıdır. Böylece, daha az parlaklığa sahip ateş böceği daha parlak olana doğru hareket eder (maksimum durumda). Işıksızlık durumunda ya da daha parlak ateş böceği bulunamaz ise rastgele hareket eder.
3. Ateş böceğinin ışık yoğunluğu, optimize edilmiş amaç fonksiyon değeri ile belirlenir.

Ateş böceği algoritmasında iki önemli husus vardır: parlaklık değişimi ve çekiciliğin formüle edilmesi. $d_{i,j}$ uzaklığındaki iki ateş böceği, i ve j, arasındaki çekicilik oranı, mesafeden kaynaklanan ışık yoğunluğunun azalmasıyla oluşur. Kaynaktan uzaklık arttıkça, ışık yoğunluğu azaldığından ve ışık ortam tarafından emildiğinden, ışık yoğunluğu I, d mesafesi ve ışık emme parametresi γ ile üstel ve monoton olarak değişmelidir [122]:

$$I(d) = I_0 e^{-\gamma d} \tag{2.5}$$

Burada, I_0 kaynaktaki ışık parlaklığıdır. Bir ateş böceğinin çekiciliği, β, ışık şiddeti ile orantılı olduğu için (2.6)'daki gibi hesaplanır:

$$\beta(d) = \beta_0 e^{-\gamma d^2} \tag{2.6}$$

Burada, β_0, d =0 iken söz konusu olan çekicilik oranıdır. x_i ve x_j konumundaki iki ateş böceği arasındaki uzaklığı hesaplamak için kartezyen uzaklığı şu şekilde kullanılır:

$$d_{i,j} = \left\| x_i - x_j \right\| = \sqrt{\sum_{k=1}^{dim} \left(x_{i,k} - x_{j,k} \right)^2} \tag{2.7}$$

Burada dim uzaysal koordinat boyutunu ifade eder. Amaç fonksiyonunu maksimize etme durumunda, ateş böceğinin hareketleri, daha düşük parlaklığa sahip olan ateş böceğinin daha parlak ateş böceğinden etkilenmesi sonucu belirlenir. Bu süreç en iyi sonuca varılıncaya kadar devam eder. Ateş böceğinin yer değişmesini belirleyen süreç şu şekilde formüle edilir:

$$x_i = x_i + \beta_0 e^{-\gamma d_{ij}^2} \left(x_j - x_i \right) + \alpha \varepsilon_i \tag{2.8}$$

Burada, birinci bileşen, ateş böceği i'nin mevcut konumu, ikinci bileşen daha çekici başka bir ateş böceğine çekilme ve son bileşen rastgele bir yürüyüştür [123]. Ateş böceği algoritmasının sözde kodu Şekil 2.2'de verilen algoritmada yer almaktadır.

Standart ABA'da, her ateş böceğinin α rastgele hale getirme parametresi [0, 1] aralığında homojen dağılımla üretilir. ABA'da genelde aynı adım ya da lineer adım kullanılır, adım sadece maksimum yinelemeye bağlıdır, farklı ateş böceklerine uyarlanamaz. α adımı her ateş böceği için aynı olduğundan veya yinelemeye bağlı olarak doğrusal olarak değiştiğinden, ateş böceklerinin deneyimleri ve mevcut konumları göz ardı edilir. Bu durum, ateş böceği algoritmasının yerel optimumda sıkışıp kalmasına neden olabilir. Bunun yanı sıra, adım büyük seçilirse ve en uygun çözüm ateş böceğine yakınsa, ateş böceği onu

atlayabilir. Dolayısıyla, α, algoritmanın yakınsaması ve araştırma alanının küresel keşfinde etkilidir. Bundan dolayı, her bir ateş böceğinin tarihsel bilgisini ve şu andaki durumunu dikkate alan, KUAABA önerilmiştir [124]. KUAABA her ateş böceğinin adımlarını yinelemeden yinelemeye geçmiş ve mevcut durumlara bağlı olarak değiştirir. [124]'e göre ateş böceği en iyi çözüme yakınsa küçük bir adım atmalıdır. Aksi takdirde adım değeri büyük olmalıdır. Tarihsel bilgiler, ateş böceğinin son iki yinelemesinin optimum değerine göre hesaplanır. Her ateş böceğinin α adımı (2.9) ve (2.10)'daki gibi belirlenir.

$$h_i(t) = \frac{1}{\sqrt{(f_{pi}(t-1) - f_{pi}(t-2))^2 + 1}} \tag{2.9}$$

$$\alpha_i(t+1) = 1 - \frac{1}{\sqrt{(f_{best}(t) - f_i(t))^2 + h_i(t)^2 + 1}} \tag{2.10}$$

Ateş böceği algoritmasının sözde kodu

```
Algoritmanın başlangıç parametreleri:
    Ateş böceklerinin sayısı n
    γ, β, α
Amaç fonksiyonunu tanımla f(x), x = (x_1, x_2, ··· , x_m)
Ateş böceklerinin ilk popülasyonunu rasgele oluştur x_i (i = 1, 2, ··· , n)
x_i deki her bir ateş böceği için f(x_i) tarafından belirlenen I_i ışık parlaklığını
 hesapla
while Sonlandırma koşulu do
    for i ← 1 to n do
        for j ← 1 to n do
            if I_j > I_i then
                i ateş böceğini j ye dogru m boyutta hareket ettir
            end
            d uzaklığına bağlı olarak çekiciliği e^(−γd^2) üzerinden değiştir
            Yeni çözümleri değerlendir ve ışık parlaklığını güncelle
        end
    end
    Ateşböceklerini sırala ve mevcut en iyi çözümü geri döndür
end
```

Şekil 2.2. Ateş böceği algoritması

$h_i(t)$, i. ateş böceğinin geçmiş iki yinelemesinin tarih bilgisini yansıtır. $f_{pi}(t-1)$ ve $f_{pi}(t-2)$, i. ateş böceğinin en iyi iki çözümünün uygunluk derecesidir. f_{best} popülasyonda o ana kadar bulunan en iyi çözümün uygunluk derecesidir. f_i, i. ateş böceğinin o anki uygunluk değeridir. Her bir ateş böceğinin bir sonraki adımı mevcut uygunluk değeri ile popülasyonun en iyi uygunluk değeri arasındaki farka göre belirlenir. Böylece ateş böceğinin adımı her yinelemeye göre veya aynı yinelemede değişebilir. Açıkçası, her ateş böceği adımı çeşitli problemler için farklıdır, çünkü farklı uygunluk fonksiyonları kullanılır. KUAABA'nın algoritma adımları aşağıda verilmiştir.

Adım 1: İlk ateş böceği popülasyonunu rastgele oluştur $x_i(i=1,2,...,n)$.

Adım 2: Her bir ateş böceği için $f(x_i)$'ye bağlı olarak I_i parlaklığını hesapla.

Adım 3: Her bir ateş böceği için (2.9) ve (2.10)'u kullanarak α adımını hesapla.

Adım 4: Ateş böceği i'yi (2.8)'i kullanarak daha parlak olana doğru hareket ettir.

Adım 5: Çözüm kümesini güncelle.

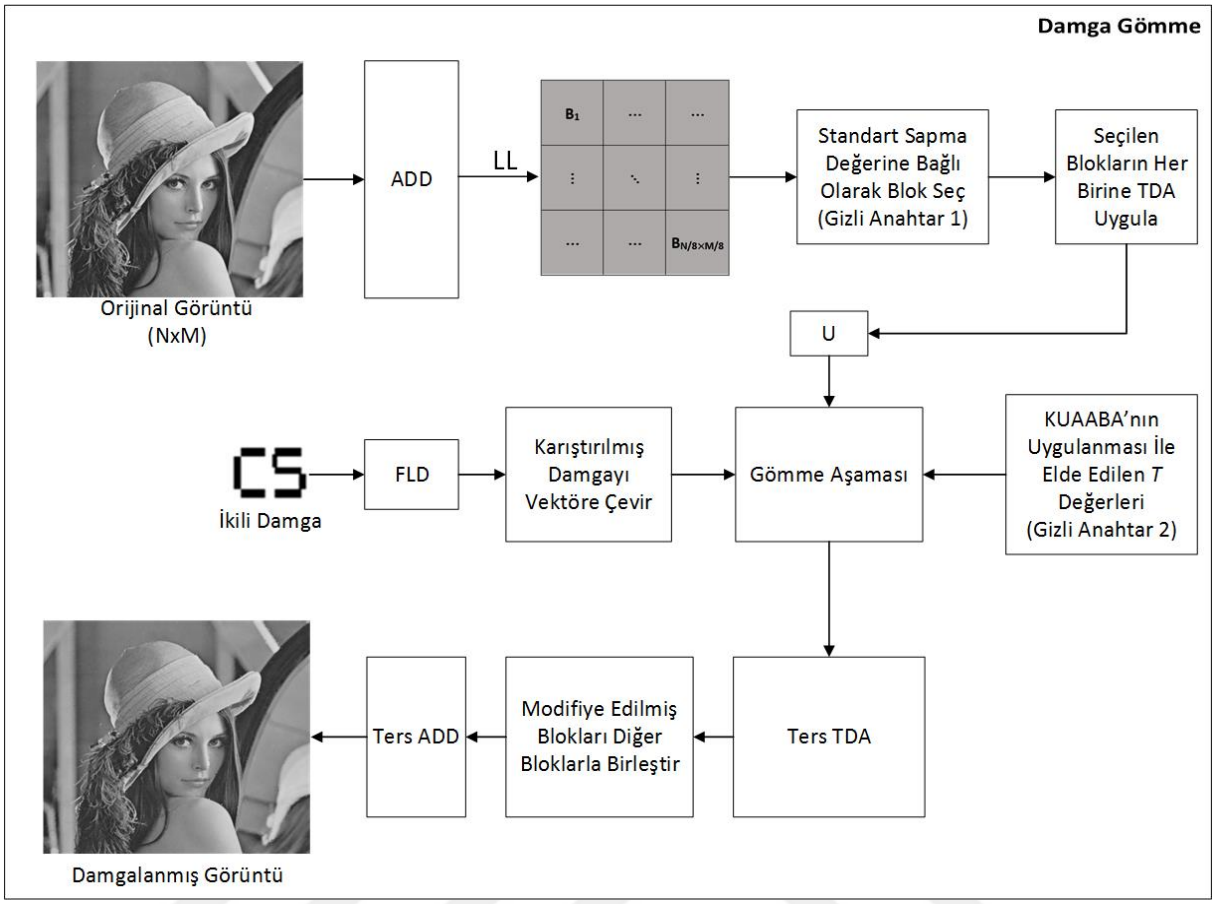
Adım 6: Sonlandırma kriteri sağlandıysa süreci sonlandır, yoksa adım 2'ye git.

2.1.1.2. Önerilen Yöntem

Bu çalışmada KUAABA ile optimize edilmiş ADD-TDA tabanlı yöntem önerilmiştir. Gri seviye görüntülerde ADD alanında TDA tekniği yardımıyla blok tabanlı kör ve dayanıklı damgalama gerçekleştirilmiştir. Damganın gömüleceği pozisyonlar, ADD'nin LL alt bandındaki blokların standart sapma değerlerine bağlı olarak seçilmiştir. KUAABA, birbirleriyle çelişen dayanıklılık ve algılanamazlığı dengelemek amacıyla gömme aşamasında kullanılan çoklu ölçeklendirme faktörlerinin belirlenmesinde kullanılmıştır.

2.1.1.2.1. Damga Gömme Süreci

$n \times n$ boyutlu ikili damgayı $M \times N$ boyutunda gri seviye orijinal görüntüye (I) gömmek için gerekli akış şeması Şekil 2.3'te verilmiştir.



Şekil 2.3. ADD-TDA-KUAABA tabanlı sistemin damga gömme süreci

Şekle göre öncelikle damga FLD ile anlamsız bir görüntü oluşturmak için karıştırılır. FLD'nin Fibonacci serisi için çekirdek değerinin 3 ve 2'ye ayarlandığı $Fibo_{32}$ tercih edilir. Karıştırılmış damga bitleri n^2 uzunluğunda tek boyutlu vektör şekline dönüştürülür. Gri seviye görüntü 1-seviye ADD ile ayrıştırılır. ADD sonucu $^{M}/_{2} \times {}^{N}/_{2}$ boyutuna sahip dört alt bant elde edilir. Görüntü enerjisinin çoğu LL bant olarak bilinen düşük frekanslı alt bantta yoğunlaştığından dolayı damganın buraya gizlenmesi, dayanıklılığı artırır. Bu nedenle damganın gömüleceği alan olarak LL bant tercih edilir. Blok tabanlı yaklaşımla damgalama gerçekleşeceği için LL bant bloklara bölünür. Burada dikkat edilmesi gereken husus her bloğa tek damga biti gömüleceği için blok sayısının en azından damga boyutuna eşit olmasıdır. Damga uzunluğundan daha fazla blok olması durumunda bloklar standart sapma değerlerine göre artan sırada sıralanır. İlk n^2 blok damga bitlerinin gizleneceği yerler olarak belirlenir. Blokların indeksleri damga çıkarma sürecinde kullanılmak üzere bir vektörde (*Gizli Anahtar 1*) saklanır. Seçilen bloklar TDA ile ayrıştırılır. TDA sonucu üç matris elde edilir: U, S ve V. U bileşeninin sütun vektöründeki katsayıların değiştirilmesinin daha az

görünür bozulmaya neden olması ve yalnızca ilk sütunun değişmez büyüklük ilişkisini koruduğunun düşünülmesinden dolayı damga biti U'nun birinci sütun ikinci katsayısına ($U_{2,1}$) gömülür. Eğer damga bitinin değeri 1 ise birinci sütun elemanlarının mutlak değerlerinin en büyüğü ($MaxU$) belirlenir. Birinci sütun ikinci katsayının değeri, işareti korunmak suretiyle değeri $MaxU + T(i)$'ye atanır. Eğer gömülecek bit 0 ise, U'nun ilk sütun elemanlarından mutlak değer olarak en küçüğü ($MinU$) tespit edilir. $U_{2,1}$'in büyüklüğü $MinU - T(i)$ olarak ayarlanır. Burada $T(i)$, i. blok için damganın gömme gücünü belirleyen ölçekleme faktörüdür. Her bloğa özgü ölçekleme faktörü KUAABA ile optimize edilmiştir. KUAABA'nın uygulanma süreci Bölüm 2.1.1.2.3'te verilmiştir. $U_{2,1}$'in damga bitine göre modifikasyonu Şekil 2.4'te gösterildiği gibidir:

U bileşeninin modifikasyonu

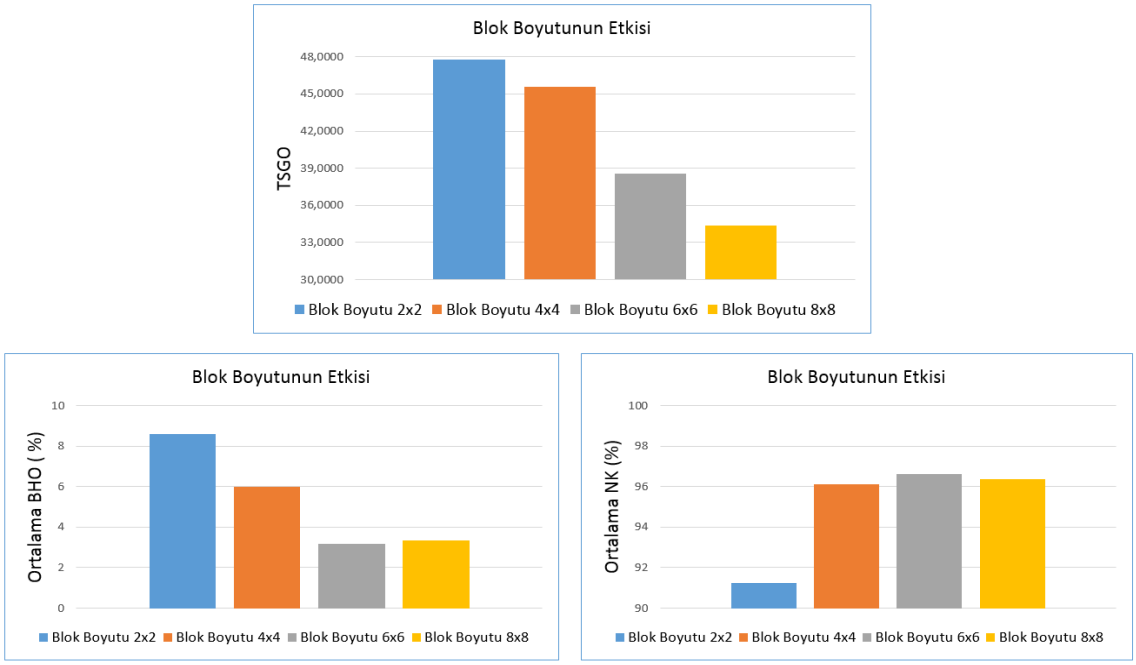
if $w_i = 1$ **then**
  $MaxU = max(|U(:,1)|)$
  $U_{2,1} = sign(U_{2,1}) \times (MaxU + T(i))$
else
  $MinU = min(|U(:,1)|)$
  $U_{2,1} = sign(U_{2,1}) \times (MinU - T(i))$
end

Şekil 2.4. Damga bitinin gömülmesi için U bileşeninin modifikasyonu

Şekildeki w_i, i. damga bitini, $|\cdot|$ mutlak değer fonksiyonunu, $U(:,1)$ U matrisinin birinci sütün elemanlarını, *sign*, işaret fonksiyonunu ifade etmektedir. Damga gömüldükten sonra S ve V matrisleri yardımıyla ters TDA uygulanır ve damgalanmış blok elde edilir. Seçilen bloklar damgalandıktan sonra, modifiye edilmiş LL bandı oluşturmak üzere diğer bloklarla birleştirilir. LL bant, damgalanma sürecinde kullanılmayan diğer alt bantlarla (LH, HL, HH) birlikte ters ADD işlemine tabi tutulur. Böylece damgalanmış görüntü üretilmiş olur.

Şekil 2.5'te farklı blok boyutları seçildiğinde önerilen sistemin elde ettiği dayanıklılık ve algılanamazlık sonuçları yer almaktadır. Bu grafikler dikkate alındığında, algılanamazlık açısından 2×2 ve 4×4 piksel boyutlu blokların TSGO değeri 45 dB'nin üzerindeyken, 6×6 ve 8×8 piksel boyutlu bloklar seçildiğinde bu değer 39 dB'nin altına düşmektedir. 2×2 boyutlu blok kullanılan şema, 4×4 boyutlu blok kullanana kıyasla algılanamazlığı

yaklaşık 2.2 dB daha iyileştirmiş olmasına rağmen, dayanıklılık performansını olumsuz etkilemiştir. 2×2 boyutlu blok için ortalama NK yaklaşık %91, ortalama BHO ise yaklaşık %9 olarak hesaplanmıştır. Oysa, 4×4 pikselden oluşan blok tercih edildiğinde ortalama NK ve BHO sırasıyla yaklaşık %96 ve %6 olarak bulunmuştur. Bu nedenle damganın gömüleceği blok boyutu 4×4 seçilmiştir.



Şekil 2.5. Blok boyutunun damgalama performansına etkisi

Yukarıda detayları verilen damgalama süreci aşağıda adımlar halinde verilmiştir:

Adım 1: İkili damga öncelikle bir anahtar kullanılarak FLD ile karıştırılır. FLD'nin Fibonacci serisi için $Fibo_{32}$ kullanılır. Ardından karıştırılmış ikili damga n^2 uzunluğunda satır vektörü formuna çevrilir.

Adım 2: Orijinal görüntüye 1-seviye ADD uygulanır. ADD uygulanınca, orijinal görüntü $M/2 \times N/2$ boyutunda 4 ayrı alt banda bölünür. Bunlar LL, LH, HL, HH bantlarıdır.

Adım 3: İkili damgayı gömmek için LL alt bandı kullanılır. LL bant 4×4 boyutlu örtüşmeyen bloklara bölünür. Önerilen yöntemde, damga bitlerinin her biri farklı bir bloğa gömülecektir. Bu nedenle, örtüşmeyen blokların sayısı, en azından damga bitlerinin sayısına eşit olmalıdır.

Adım 4: Örtüşmeyen bloklar, standart sapma değerlerine bağlı olarak artan sırada düzenlenir. İlk $n \times n$ blok, veriyi gömmek üzere seçilir. Çıkarma aşamasında, bu blokların konumu gereklidir, bu yüzden seçilen blokların indeksleri bir dizide tutulup (*Gizli Anahtar 1*) giriş parametresi olarak çıkarma işlevine geçirilir.

Adım 5: Damga bitlerini gömmek için öncelikle standart sapma değerine bağlı olarak belirlenen bloklara TDA uygulanır.

Adım 6: TDA sonucu üç matris (U, S ve V) elde edilir. [113]'e göre, U matrisinin sütun vektöründeki katsayıların modifikasyonu, satır vektöründeki katsayıların modifikasyonuna kıyasla daha az bozulmaya neden olacaktır. Ayrıca, U bileşeninin yalnızca ilk sütununun değişmez büyüklük ilişkisini koruduğu düşünüldüğünde, gömme aşamasında, U matrisinin ilk sütunundaki ikinci katsayı değiştirilir. Damga biti 1 ise, U'nun ilk sütun vektörünün mutlak değerlerinin maksimum değeri ($MaxU$) hesaplanır. Daha sonra, $|U_{2,1}|$'in değeri $MaxU + T(i)$ olarak değiştirilir. Damga biti 0 ise, U matrisinin ilk sütun vektörünün minimum mutlak değeri ($MinU$) hesaplanır. $MinU - T(i)$ değeri $|U_{2,1}|$'e atanır. $T(i)$, i. bloğunun ölçeklendirme faktörüdür (*Gizli Anahtar 2*) ve KUAABA tarafından belirlenir.

Adım 7: Damgalanmış U matrisi ve S ve V matrislerine ters TDA uygulanarak modifiye edilmiş blok elde edilir.

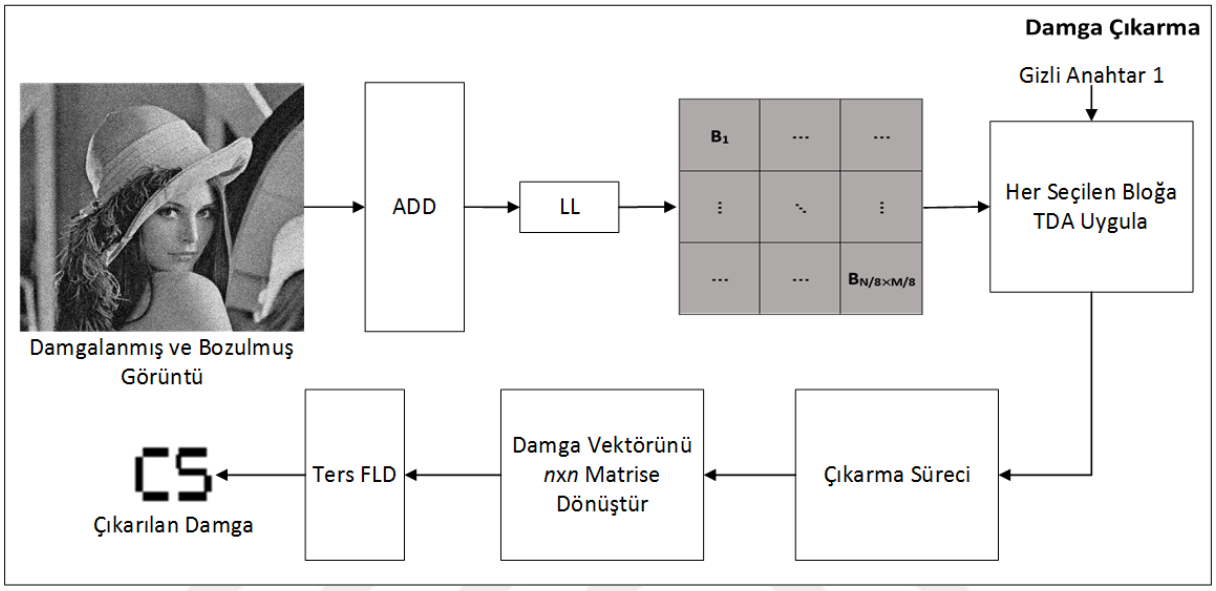
Adım 8: Adım 6 ve 7 tüm damga bitleri gömülünceye kadar sürdürülür.

Adım 9: Modifiye edilmiş bloklar diğer bloklarla birleştirilerek damgalanmış LL bant elde edilir. LL bant diğer alt bantlarla birlikte ters ADD işlemine tabi tutularak damgalanmış görüntü oluşturulur.

2.1.1.2.2. Damga Çıkarma Süreci

Önerilen yöntem kördür. Bu nedenle, ne orijinal içerik ne de gömülen sinyal damga çıkarma aşamasında gereklidir. Damga çıkarma sürecinin şematik diyagramı Şekil 2.6'da verilmiştir. Damgalanmış ve muhtemelen bozulmuş gri seviye görüntü (I^{wc}) öncelikle 1-seviye ADD dönüşümü ile ayrıştırılır. Düşük frekanslı alt bant damga gömme sürecinde kullanıldığı için, bitler yalnızca bu bant kullanılarak çıkarılır. LL bant (LL^{wc}) 4×4 pikselden oluşan örtüşmeyen bloklara ayrılır. *Gizli Anahtar 1*'de indeksleri saklı olan bloklardan damgayı çıkarmak için öncelikle her birine TDA uygulanır. TDA ile elde edilen U^{wc} bileşeninin ilk sütunundaki katsayıların mutlak değerce en büyük ($MaxU$) ve en küçük

($MinU$) olanı hesaplanır. $U_{2,1}^{wc}$'in büyüklüğü $MaxU$'ya daha yakınsa çıkarılan bit 1'e, değilse 0'a atanır. Tüm damgalanmış bloklardan bitler çıkarıldıktan sonra n^2 uzunluğundaki w^{ex} damga vektörü 2-boyutlu $n \times n$ formuna dönüştürülür. Son olarak $n \times n$ boyutlu matrise ters FLD işlemi uygulanarak ikili damga elde edilmiş olur.



Şekil 2.6. ADD-TDA-KUAABA tabanlı sistemin damga çıkarma süreci

Damganın çıkarılması sürecine ait adımlar şu şekilde verilebilir:

Adım 1: Damgalanmış ve ardından bozulmuş görüntüye (I^{wc}) 1 seviye ADD uygulanır.

Adım 2: İkili damgayı çıkarmak için düşük frekanslı alt bant (LL^{wc}) 4×4 boyutlu örtüşmeyen bloklara bölünür.

Adım 3: Damganın çıkarılacağı bloklar *Gizli anahtar 1* yardımıyla seçilir.

Adım 4: Bu blokların her biri TDA yardımıyla U, S ve V bileşenlerine ayrıştırılır.

Adım 5: Gömülen damga U^{wc} bileşeninden Şekil 2.7'de verilen kurallara bağlı olarak çıkarılır. Burada yer alan w_i^{ex}, i indeksli bloktan çıkarılan damga bitini simgeler.

Adım 6: Tüm bitler çıkarıldıktan sonra, damga vektörü 2-boyutlu forma dönüştürülür.

Adım 7: Ters FLD karıştırılmış damga bitlerine uygulanır.

$$
\begin{aligned}
&MaxU = max\left(\left|U^{wc}(:,1)\right|\right)\\
&MinU = min\left(\left|U^{wc}(:,1)\right|\right)\\
&DiffMax = \left|MaxU - \left|U_{2,1}^{wc}\right|\right|\\
&DiffMin = \left|MinU - \left|U_{2,1}^{wc}\right|\right|\\
&w_i^{ex} = \begin{cases} 1, & DiffMax \leq DiffMin \\ 0, & değilse \end{cases}
\end{aligned}
$$

Şekil 2.7. *U* bileşeninden damganın çıkarılması

2.1.1.2.3. KUAABA'nın Uygulanması

Bu çalışmada birbiriyle çelişen damgalama gereksinimleri algılanamazlık ve dayanıklılık arasında iyi bir ödünleşim elde etmek için ABA'nın değiştirilmiş bir sürümü olan KUAABA'dan yararlanılmıştır. Optimizasyon algoritması gömme sürecinde kullanılan ve ölçekleme faktörü olarak da bilinen çoklu eşik değerlerini seçmek için kullanılır.

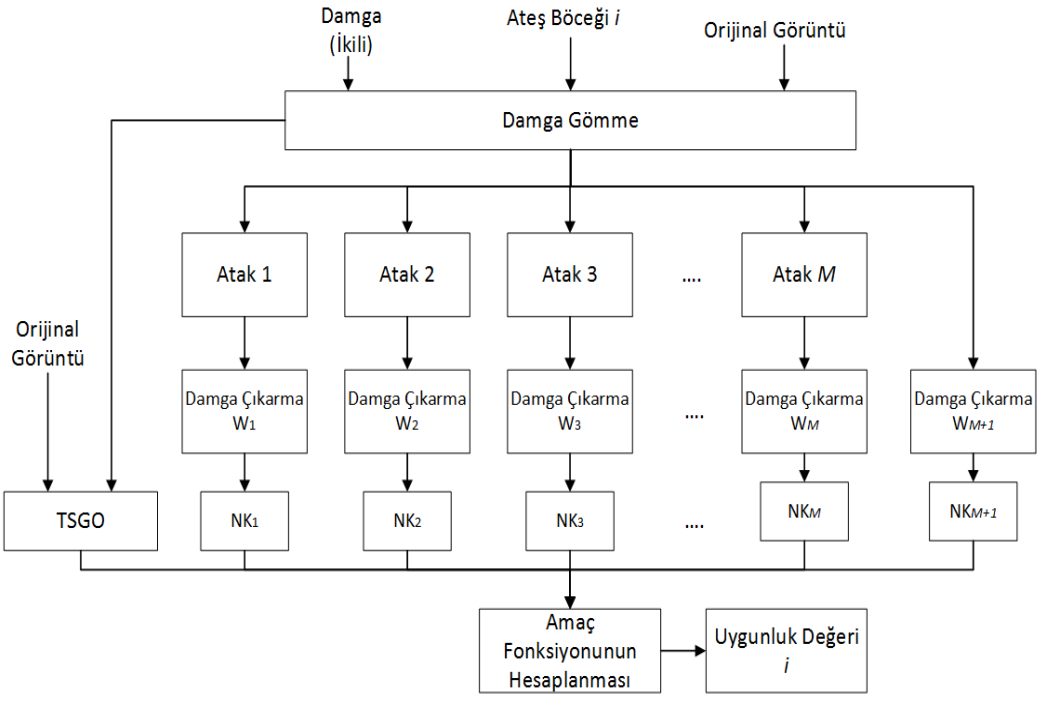
Gömme aşamasında U matrisinin ilk sütunundaki ikinci elemanın değerini ayarlamak için kullanılan ölçeklendirme faktörü, T, damgalamanın başarısı için önemlidir. Ölçekleme faktörü çok küçük seçilirse, algılanamazlık artar, ancak dayanıklılık azalır. Tam tersi ölçekleme faktörü çok yüksek ayarlanmışsa, dayanıklılık artsa bile damgalanmış görüntünün bozulma oranı da artacaktır. Bu nedenle, standart sapmaya bağlı olarak seçilen her blok için gereken ölçeklendirme faktörü optimize edilmelidir.

Her bir ateş böceği için uygunluk değerinin hesaplanması sürecine ait blok diyagram Şekil 2.8'de verilmiştir. Optimizasyon aşamasında öncelikle KUAABA için parametreler belirlenir. Popülasyon boyutu, p, 10'a ayarlanmıştır ve $\beta_0$ve γ sırasıyla 0.1 ve 1'e atanmıştır. Önerilen yöntemde çoklu ölçekleme faktörü belirleneceğinden her ateş böceğinin boyutu damga boyutuna $(n \times n)$ eşit olmalıdır. Başlangıçta $n \times n$ boyutlu p ateş böceği için rasgele değerler atanır. Her ateş böceğinde yer alan bu rasgele değerler ölçekleme faktörü olarak kullanılarak Bölüm 2.1.1.2.1'de verildiği şekilde damga gömülür. Damgalanmış görüntü ve orijinal görüntüye bağlı olarak TSGO hesaplanır. Damgalanmış görüntüden Bölüm 2.1.1.2.2'ye bağlı olarak damga çıkarılır ve orijinal damga ve çıkarılan damga arasındaki NK değeri hesaplanır. Damgalanmış görüntüye ayrı ayrı sekiz atak uygulanır: Görüntünün merkezinden 100×100 boyutlu bir bölgenin kırpılması, 70 kalite faktörü ile JPEG

sıkıştırma, ortalama filtre, Gauss filtresi, keskinleştirme filtresi, tuz & biber gürültüsü, Gauss gürültüsü, benek gürültüsü. Dolayısıyla sekiz adet damgalanmış ve bozulmuş görüntü elde edilir. Bu sekiz görüntü için damga çıkarma süreci işletilir ve her bir görüntüden çıkarılan damga ve orijinal damgaya bağlı olarak NK hesaplanır. Burada optimize edilmeye çalışılan amaç fonksiyonu (2.11)'de verilmiştir.

$$\mathrm{OF} = 0.01 \times \mathrm{TSGO} + \frac{1}{M+1}\sum_{i=1}^{M+1} NK_i \tag{2.11}$$

Bir adet sadece damgalanmış ve sekiz adet damgalanmış ve atak uygulanmış görüntüden elde edilen NK değerlerinin ortalaması ve TSGO değerine bağlı olarak amaç fonksiyonu hesaplanır. Elde edilen OF değeri ilgili ateş böceğinin parlaklığını ifade eder. Ateş böceklerinin adımı Bölüm 2.1.1.1.2'de verilen (2.9) ve (2.10)'a göre güncellenir ve ateş böcekleri daha parlak olana yani OF değeri daha yüksek olana doğru hareket ettirilir. Algoritma daha iyi çözümler bulduğu sürece bu süreç devam ettirilir. Yoksa en yüksek parlaklığa sahip olan, çözüm kümesi olarak belirlenir. Optimizasyon algoritmasının uygulanması aşağıdaki adımlarda verilmiştir:



Şekil 2.8.Ateş böceğinin uygunluk değerinin hesaplanması

Adım 1: $n \times n$ boyutunda p ateş böceği rastgele oluşturulur. Bir bloğa yalnızca bir bit gömüleceğinden, her ateş böceğinin boyutu damga boyutuna eşit olmalıdır.

Popülasyondaki her bir ateş böceği için 2-7 arasındaki adımlar gerçekleştirilir:

Adım 2: Damga, damga gömme sürecine bağlı olarak gömülür.

Adım 3: Damgalanmış görüntü ve orijinal görüntü arasında TSGO hesaplanır.

Adım 4: Damgalanmış görüntüye M saldırı uygulanır ve M bozulmuş ve damgalanmış görüntü elde edilir.

Adım 5: Bir adet damgalanmış görüntüden, M tane de bozulmuş ve damgalanmış görüntüden damga çıkarma sürecine bağlı olarak damga çıkarılır.

Adım 6: Orijinal damga ve çıkarılan damga arasında NK hesaplanır.

Adım 7: NK ve TSGO değerine bağlı olarak amaç fonksiyonu hesaplanır.

Adım 8: Her bir ateş böceğinin adımı (2.9) ve (2.10)'a bağlı olarak güncellenir. Ateş böcekleri daha parlak olana doğru hareket ettirilir.

Adım 9: Optimizasyon algoritması daha iyi çözümler bulduğu sürece, 2-8 arası adımlar sürdürülür.

Adım 10: Yinelemeler artık daha iyi sonuçlar vermediğinde algoritma sona erer.

Adım 11: Ateş böcekleri sıralandıktan sonra uygunluk değeri en yüksek olan en iyi çözüm olarak seçilir.

Özetlenecek olursa, geleneksel damgalamaya yönelik çalışmada gri seviye görüntülere ikili damgayı gömmek için öncelikle görüntü ADD ile alt bileşenlerine ayrılır. Düşük frekanslı alt bant (LL) görüntü enerjisinin çoğunu içerdiğinden damganın yerleştirileceği alan olarak tercih edilir. Blok tabanlı bir yöntem önerildiğinden LL bant 4×4 pikselden oluşan bloklara bölünür. Standart sapma değeri daha düşük olan damga boyutu kadar blok TDA ile ayrıştırılır. TDA sonucu elde edilen U bileşenine FLD ile karıştırılmış ve vektör forma çevrilmiş damga biti ölçekleme faktörü yardımıyla gömülür. Burada kullanılan ölçekleme faktörünün dayanıklılık ve algılanamazlık üzerinde etkisi vardır. Zira çok büyük ölçekleme faktörünün seçilmesi dayanıklılığı artırırken algılanamazlığı azaltır. Tam tersi, küçük ölçekleme faktörü ise algılanamazlık üzerine olumlu etki etse de dayanıklılık performansını azaltır. Bu nedenle bloğa özgü ölçekleme faktörü etkili bir optimizasyon algoritması olan KUAABA ile belirlenir. Damga çıkarma sürecinde U bileşenden damga orijinal görüntüye ihtiyaç duymadan kör olarak çıkarılır.

2.2. Biyometrik Damgalamaya Yönelik Çalışma

Sayısal damgalama teknolojilerinde damga tipi olarak rasgele ikili dizi, rasgele Gauss dizisi, ikili görüntü (logo) veya gri seviye görüntüler kullanılmaktadır. Bu tür damgalar somut mülkiyet için talep edilemezler. Öte yandan, bireylerin fizyolojik veya davranışsal özelliklerine göre otomatik olarak tanınmasına fırsat veren biyometrikler, tanımlama/doğrulama uygulamalarında yüksek düzeyde güvenlik ve kolaylık sağlar. Dolayısıyla biyometrik verilerin damgalama teknikleriyle birleştirilmesi damganın sahipliği konusunda potansiyel çözüm gibi görünmektedir. Kullanıcıya özgü niteliklerin sayısal damgalamada kullanılması, belirli bir kişinin içeriğe erişme yetkisinin olup olmadığını veya mevcut kullanıcının içeriğin yasal sahibi olup olmadığını belirlemek amacıyla önemlidir. Çalışmanın ikinci kısmında bahsi geçen sebeplerden ötürü iris kodunun damga olarak kullanıldığı biyometrik damgalama yöntemlerine odaklanılmıştır. Aşağıda iris verisinden elde edilen ikili kodun YDDADD alanında farklı tekniklerle renkli görüntülere gömüldüğü yaklaşımlar ele alınmıştır. Ayrıca bu yaklaşımlarda yer alan ölçekleme faktörlerinin, ABA ile optimize edildiği ve KUAABA ile optimize edildiği durumlar incelenmiştir. Optimizasyon algoritması kullanılmadan ölçekleme faktörünün sabit bir değere atandığı zaman elde edilen sonuçlar optimize edilen sonuçlar ile algılanamazlık, dayanıklılık ve kimlik doğrulama hassasiyeti üzerinden karşılaştırılmıştır.

2.2.1. YDDADD Alanında İris Tabanlı Biyometrik Damgalama

[58, 59]'da belirtildiğine göre iris tanıma, en güvenilir ve en doğru biyometrik teknolojilerden biridir. Bundan dolayı, otantik kişiyi bir sahtekârdan ayırt etmede iris tanımanın kullanılması ilgi çekicidir. Bu çalışmada kullanılan iris görüntüleri Bath Üniversitesi veri tabanına aittir. Çalışmanın amacı, orijinal görüntünün kimlik doğrulaması ve sahipliği için dayanıklı biyometrik damgalama sistemi önermektir. Bu nedenle, iris biyometrik verilerini kullanılabilir ve sağlam bir biçimde normalleştirmek için basit bir metodoloji kullanılmıştır [125, 126].

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 [127]. 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 arttırmanın yollarını belirlemek yararlı olacaktır. Bu çalışmada [127] 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.

Son birkaç yılda, araştırmacılar telif hakkı koruma uygulamaları için çeşitli TDA tabanlı teknikler önermişlerdir. Bu tekniklerin en yaygın saldırılara karşı dayanıklı olduğu kanıtlanmıştır. Ancak, TDA sayısal olarak zorlu bir işlemdir. Bu nedenle, bu çalışmada TDA'nın yanı sıra QR Ayrıştırma ve Schur Ayrıştırmanın performansı da değerlendirilmiştir. Çalışmada renkli görüntüler üzerinde damgalama yapmak için ise YCbCr renk uzayından yararlanılmıştır.

2.2.1.1. Kullanılan Teorik Kavramlar

Bu bölümde ADD'den türetilmiş 90° ve katlarında rotasyon ve satır/sütun bazında görüntü çevirme karşısında dayanıklı olan YDDADD'ye değinilmiştir. Söz konusu geometrik ataklar karşısında değişmezlik elde etmek amacıyla gerekli işlem adımları aşağıda verilen alt başlıkta incelenmiştir.

2.2.1.1.1. Yeniden Dağıtılmış Değişmez Ayrık Dalgacık Dönüşümü (YDDADD)

Bu çalışmada [127]'de önerilen ve damgalamanın geometrik bozulmalara dayanıklı alanda yapıldığı YDDADD'den yararlanılmıştır. 90° ve katları döndürme ve görüntü çevirmede dalgacık katsayılarında değişmezlik elde etmek için, bir I görüntüsü verildiğinde, normalleştirme prosedürü aşağıdaki gibi formüle edilir [127]:

i. Orijinal görüntü dört (2×2), eşit boyutlu alt görüntüye bölünür ve (2.12)'de belirtilen ortalama parlaklık matrisi elde edilir:

$$ortalama = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \quad a,b,c,d \geq 0 \tag{2.12}$$

ii. Normalizasyon matrisi *S* şu şekilde tanımlanır:

$$S \triangleq \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} = \begin{pmatrix} a+b+c+d & a+b-c-d \\ a-b+c-d & a-b-c+d \end{pmatrix} \tag{2.13}$$

Burada S_{11}, S_{12}, S_{21} ve S_{22}'nin hiçbirinin 0'a eşit olmadığı ve $|S_{21}| \neq |S_{12}|$ koşulunun sağlandığı varsayılır. Doğal görüntülerde bu iki şart zaten sağlanır. Normalizasyon matrisinin işaret matrisi şu şekilde elde edilir:

$$Sign = \begin{pmatrix} Sg_{11} & Sg_{12} \\ Sg_{21} & Sg_{22} \end{pmatrix}, \; Sg_{ij} \in \{-1,+1\} \tag{2.14}$$

iii. Görüntü yeniden dağıtılır ve yeniden dağıtılmış görüntü *NI* ile ifade edilir.

$$\begin{aligned} &NI(2i-1,2j-1) = I(i,j), && 1 \leq i \leq M/2, 1 \leq j \leq N/2 \\ &NI(2i-1,2j-N) = I(i,3N/2 - j + 1), && 1 \leq i \leq M/2, N/2 < j \leq N \\ &NI(2i-M,2j-1) = I(3M/2 - i + 1, j), && M/2 < i \leq M, 1 \leq j \leq N/2 \\ &NI(2i-M,2j-N) = I(3M/2 - i + 1, 3N/2 - j + 1), && M/2 < i \leq M, N/2 < j \leq N \end{aligned} \tag{2.15}$$

iv. Yeni görüntü *NI* 1 seviye Haar dalgacık dönüşümü ile alt bantlarına ayrıştırılır. Burada alt bantlar (2.16)'daki gibi *A* matrisleriyle eşleştirilir.

$$\begin{pmatrix} \mathbf{LL} & \mathbf{HL} \\ \mathbf{LH} & \mathbf{HH} \end{pmatrix} \triangleq \begin{pmatrix} \mathbf{A_{11}} & \mathbf{A_{12}} \\ \mathbf{A_{21}} & \mathbf{A_{22}} \end{pmatrix} \tag{2.16}$$

v. Alt bant, işaret matrisiyle çarpılır. Elde edilen yeni matris *B* ile ifade edilir.

$$B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} Sg_{11} \times A_{11} & Sg_{12} \times A_{12} \\ Sg_{21} \times A_{21} & Sg_{22} \times A_{22} \end{pmatrix} \quad (2.17)$$

vi. Eğer $|S_{21}| < |S_{12}|$ ise, B matrisi geometrik değişmez alandır. Değilse, B_{12} ve B_{21} yer değiştirir ve B'nin her bir alt bandının devriği alınır.

$$B = \begin{pmatrix} B_{11}{}^{T} & B_{21}{}^{T} \\ B_{12}{}^{T} & B_{22}{}^{T} \end{pmatrix} \quad (2.18)$$

Burada B_{ij}^{T}, B_{ij} matrisinin devrik matrisini ifade eder.

En son elde edilen B matrisi 90° ve katlarında rotasyona ve görüntü çevirmeye karşı değişmezdir. Yani orijinal görüntü satır veya sütun bazında çevrilirse ya da 90° katlarında dönmeye maruz kalırsa aynı dalgacık uzayı elde edilir. Sonuç olarak, kör ya da kör olmayan mevcut dalgacık tabanlı damgalama şemaları, geometrik çarpıklıklarla başa çıkmak için sağlamlıklarını artırmak üzere değişmez dalgacık alanı kullanılarak yeniden tasarlanabilir.

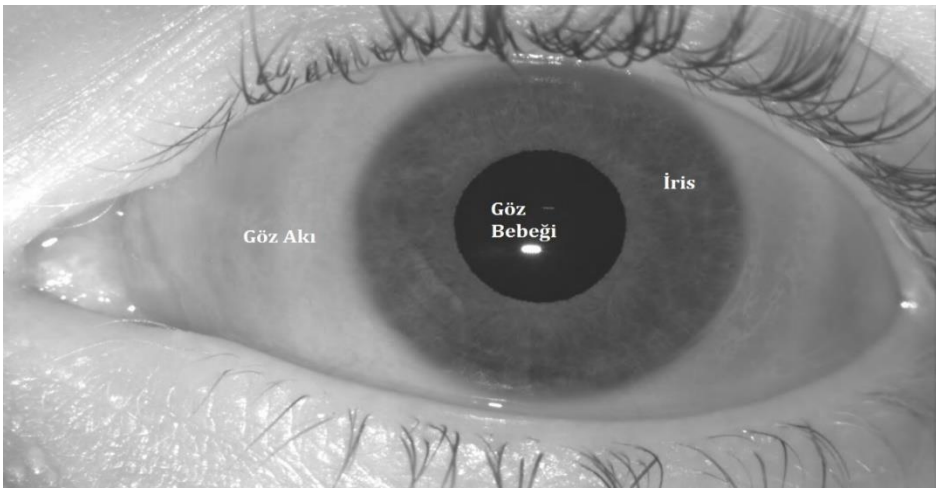
2.2.1.2. Önerilen Yöntem

Bu kısımda göz görüntüsünden elde edilen ikili iris kodunu renkli görüntülere YDDADD alanında gömmek ve damgalanmış görüntüden iris kodunu yeniden elde etmek için gerekli süreçler tanıtılmıştır. Öncelikle veri tabanından alınan görüntüden ikili iris kodunun nasıl elde edildiği tartışılmıştır. Ardından tercih edilen renk uzayı gerekçeleriyle birlikte ele alınmıştır. Son olarak damga gömme ve çıkarma adımlarına yer verilmiştir. Damgalama sürecinde YDDADD ile birlikte üç farklı ayrıştırma tekniği test edilmiştir. Her bir teknik için gerekli prosedürler ayrıntılı olarak incelenmiştir. Damga gömme sürecinde kullanılan çoklu ölçekleme faktörünün optimizasyonu ABA ve KUAABA ile gerçekleştirilmiştir. KUAABA'nın uygulanma süreci Bölüm 2.1.1.2.3'de anlatılmıştı. ABA'nın gerçeklenmesi ise Bölüm 2.2.1.2.5'te ele alınmıştır.

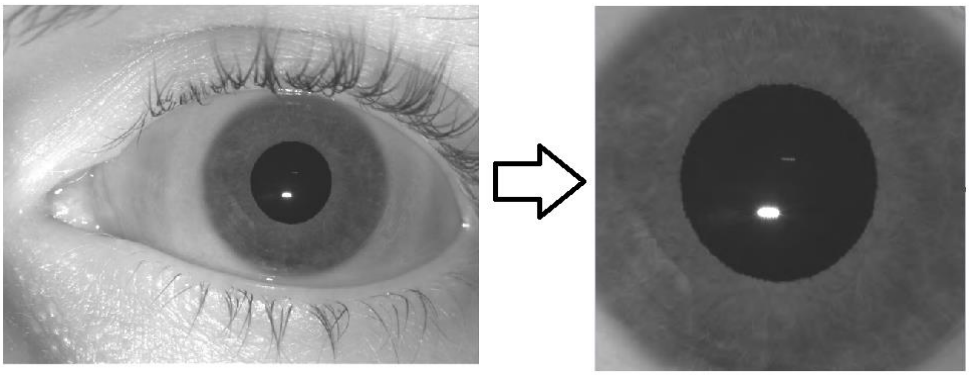
2.2.1.2.1. Damga Hazırlama

Bath Üniversitesi iris veri tabanından elde edilen göz görüntüleri bu çalışmada damga oluşturmak için kullanılmıştır. Şekil 2.9'da göz görüntüsünün önden görünüşü yer almaktadır. Burada, göz akı, göz bebeği, göz bebeğinin etrafındaki renkli kısım ve irisin açıkça tanımlandığı gözün ayrıntıları verilmektedir. İris kodunu elde etmeden önce, göz akı, göz bebeği, göz kapağı gibi olumsuz faktörlerin göz görüntüsünden çıkarılması için görüntü normalleştirilmelidir. Bu faktörleri ortadan kaldırmak için göz görüntüsüne MSİD formatı uygulanır.

İristen öznitelik çıkarmak için, ilk olarak, bir kızılötesi kamera tarafından çekilen iris veri tabanından 1280×960 boyutlu göz görüntüsünün gözbebeği sınırları tespit edilir. Burada veri tabanının iris yarıçapı değerleri 190-200 piksel arasında değişirken, göz bebeği yarıçapı 95-105 piksel arasındadır [59]. Göz bebeğinin yeri, bir grup koyu renkli pikselin yerinin aranmasıyla bulunur. Daire algılama işlemini daha verimli ve doğru yapmak için, algoritma iris/göz akı sınırlarını arar. Göz bebeği ve iris arasındaki yarıçap farkı 100'den fazla olmadığından, tespit edilen göz bebeğinin çevresinde 100 piksel alınır ve göz bebeği her zaman iris bölgesinde olduğundan, resim bilgilerinin geri kalanı kaldırılır. Bu işlemde üst ve alt göz kapağı çıkarılır. Bu işlem tamamlandıktan sonra, resim Şekil 2.10'da gösterildiği gibi azaltılmış bir biçimde saklanır.



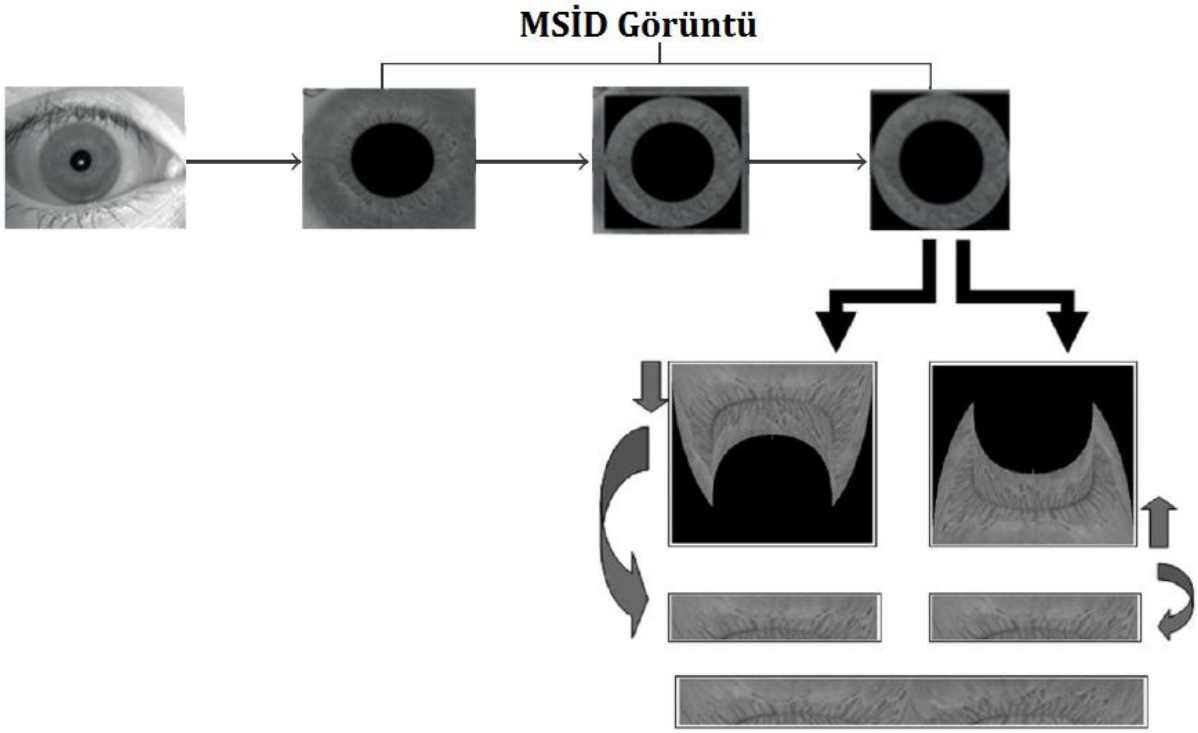
Şekil 2.9. Gözün önden görünüşü



Şekil 2.10. İris çıkarma süreci [59].

Normalizasyon aşamasında, iris bölgesi, karşılaştırmaları mümkün kılmak için sabit boyutlara sahip olacak şekilde dönüştürülür. Bunu yapmak için göz bebeğinin sınırından ayrı olarak 70 piksel uzaklıktan başka bir daire çizilir. Bu, veri tabanında yer alan her görüntü için irisin aynı sayıda pikselini dikkate almak amacıyla yapılır. İlgili bölge, göz bebeği ile dairesel sınır arasındaki bölgedir. Bunun dışındaki bölgeler kaldırılır. Burada, görüntünün üst kısmında sıfır olmayan görüntü piksellerinin en üste, sıfır görüntü piksellerinin dibe kaydırılması ile bir görüntü elde edilir. Görüntünün alt kısmı için de sıfır olmayan görüntü pikselleri en alta, sıfır olan görüntü pikselleri en üste kaydırılarak ikinci bölge elde edilir. Bundan sonra görüntünün üst kısmı için, üstten 90 piksel alınıp kalan kısmın çıkarılmasıyla bir alt görüntü elde edilir. Esas olarak irisin üst kısmı ve yandan bir kısmı oluşur. Benzer şekilde, görüntünün alt kısmı için, alttan 90 piksel alınıp bölümün geri kalanının çıkarılmasıyla ikinci alt görüntü elde edilir. Böylece irisin alt kısmı ve yandan bir kısmı oluşur. Son olarak, bu iki alt görüntü, normalize irisin elde edilmesi için Şekil 2.11'de gösterildiği gibi birleştirilir.

Elde edilen normalize iris iki kübik enterpolasyon kullanılarak kıyaslama için aynı boyuta getirilir. Bu çalışmada 120×200 boyutlu normalize iris kullanılır. Normalize edilmiş 120×200 boyutundaki iris görüntülere, sütun bazında, bir boyutlu AKD uygulanır ve her bir kolonun DC değeri tutulur. Ardından, bu 1 × 200 boyutlu DC değerleri gömülecek olan damganın yükünü hafifletmek için bir anahtar değere bölündükten sonra, 8 × 200 boyutlu ikili dizeye dönüştürülür ve damga elde edilmiş olur.



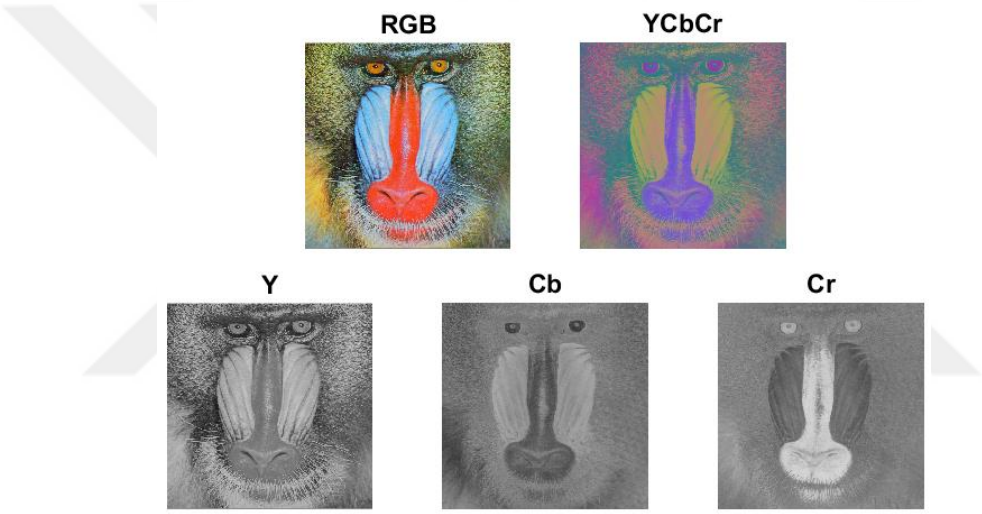
Şekil 2.11. İris görüntüsünün normalizasyon süreci [72].

2.2.1.2.2. Renk Uzayı Dönüşümü

Renk uzayı, renk bilgilerini üç veya dört farklı renk bileşeni olarak temsil eden matematiksel modeldir [128]. Renklerin nasıl temsil edildiğini açıklar ve her bir renk spektrumunun nasıl göründüğünü öğrenmek için renk uzayının bileşenlerini doğru bir şekilde belirler. Renkli görüntü damgalama şemalarında RGB, YUV, CIELab, YCbCr gibi farklı renk modelleri sıkça tercih edilir [129].

RGB televizyon ve bilgisayar monitörlerinde yaygın olarak kullanılan ve kırmızı, yeşil ve mavi kanallardan oluşan renk uzayıdır. Farklı renk uzayları, RGB'den doğrusal veya doğrusal olmayan dönüşümle elde edilebilir. Renkli görüntüleri temsil etmek için sıkça rastlanan modellerden bir diğeri ise YCbCr renk uzayıdır. YCbCr modeli rengi gri ölçekli kısım (luma veya Y bileşeni) ve iki krominans bileşeni (Cb ve Cr bileşenleri) ile tarif eder. Işık parlaklığı bu uzayda Y bileşeni ile temsil edilirken, Cb mavi ve luma bileşen farkını (B-Y), Cr de kırmızı ve luma bileşen farkını (R-Y) ifade etmektedir. RGB modelinde renk kanalları arasındaki korelasyon yüksektir. Dolayısıyla, damga RGB alanına gömülü ise, bu üç renk kanalı damganın enerjisini eşit olarak emdiğinden, damgalamanın sıkıştırma veya

filtreleme saldırılarına karşı dayanıklılığı azalacaktır [130]. [130]'da belirtildiğine göre RGB uzayının aksine, YCbCr modelinin renk kanalları daha az ilişkilidir ve oldukça bağımsızdır. Dolayısıyla, orijinal görüntünün bir bileşenindeki değişikliklerin diğer bileşenlerdeki değişiklikler üzerindeki etkisi minimumdur. Ayrıca [131]'de yazarlar RGB, YUV, YCbCr renk kanallarında damgalama tekniklerini incelemişler ve performanslarını analiz etmişlerdir. Bu çalışmaya göre, YCbCr renk uzayına yerleştirilen damganın RGB ve YUV renk uzayına kıyasla daha dayanıklı ve şeffaf olduğu kanıtlanmıştır. Bu nedenlerle çalışmada YCbCr modeli tercih edilmiştir. Şekil 2.12'de RGB uzayında ve YCbCr uzayında temsil edilen "Baboon" görüntüleri ve buna ait renk bileşenleri yer almaktadır.



Şekil 2.12. RGB ve YCbCr uzayında "Baboon" görüntüsü

YCbCr renk uzayı insan gözünün özelliklerini kullanır. İnsan gözü ışık parlaklığı değişikliklerine karşı daha duyarlı iken ton değişikliklerine karşı daha az duyarlıdır [128]. YCbCr renk uzayının üç kanalının enerji dağılımına bakıldığında, enerjinin çoğu Y kanalında yoğunlaşmaktadır. [132]'de ifade edildiğine göre İGS'nin renk duyarlılığı göz önüne alındığında ise, Cb kanalı en az duyarlıdır. Dolayısıyla damga bilgisinin Y bileşenine gizlenmesi damgalama şemasının saldırılara karşı daha dayanıklı olması anlamına gelirken, damgalamanın Cb kanalında gerçekleşmesi ise daha iyi şeffaflık performansı sağlayacaktır. Dayanıklılığı daha üst seviyede tutmak ve çıkarılan iris kodunun kimlik doğrulama hatalarını minimize etmek adına orijinal görüntünün Y kanalı, önerilen şemalarda damgalama alanı olarak seçilmiştir.

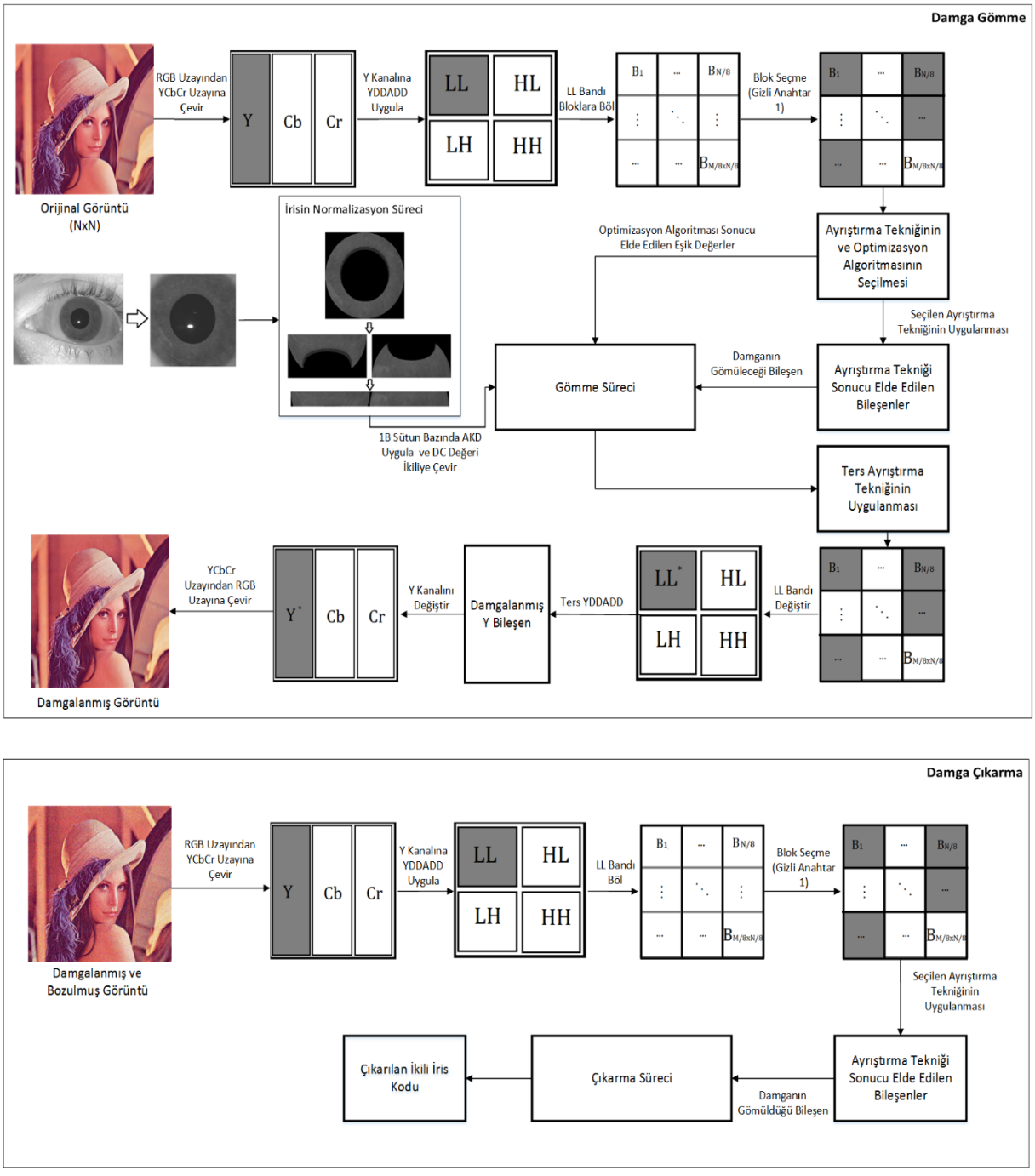
2.2.1.2.3. Damga Gömme Süreci

Şekil 2.13'te önerilen damgalama sürecinin şematik diyagramı gösterilmiştir. Göz görüntülerinden elde edilen iris kodunu renkli görüntülere gömmek için öncelikle RGB uzayındaki görüntüyü (I) YCbCr uzayına dönüştürmek gerekir. Bölüm 2.2.1.2.2'de ifade edildiğine göre YCbCr dönüşümü sonrası elde edilen Y kanalı (I_Y) görüntü enerjisinin çoğunu içerdiğinden, bu kanala "Haar" filtre yardımıyla YDDADD uygulanır. YDDADD sonucu elde edilen dört alt banttan düşük frekanslı alt bant (LL) damgayı gömmek üzere seçilir. LL bant her biri 4×4 pikselden oluşan örtüşmeyen bloklara bölünür ve bloklar standart sapma değerlerine göre artan sırada sıralanır. Standart sapma değeri daha düşük olan damga boyutu kadar blok seçilir ve indeksleri damga çıkarma sürecinde kullanılmak üzere bir vektörde saklanır ($Gizli\ Anahtar\ 1$). Bu aşamadan sonra kullanılacak ayrıştırma tekniğine göre damga gömme işlemi gerçekleştirilir. Aşağıda bu tekniklerin detayları verilmiştir.

TDA'nın uygulanması: YDDADD alanında damgalamada ayrıştırma tekniği olarak TDA seçildiğinde öncelikle seçilen blok ($blok_i$) TDA ile üç bileşene ayrılır (U_i, S_i ve V_i). Damgalamayı gerçekleştirmede U_i matrisinin ilk sütunu Bölüm 2.1.1'de bahsedilen özelliklerinden dolayı tercih edilir. Eğer gömülecek damga biti 1 ise ilk sütundaki katsayılardan mutlak değerce en büyük olanı ($MaxU$) belirlenir ve bu sütundaki ikinci elamanın ($U_{i_{2,1}}$) işareti aynı kalmakla birlikte değeri, $MaxU + T(i)$ olarak güncellenir. Gömülecek bit 0 olduğunda, U_i matrisinin ilk sütun katsayılarının mutlak değer olarak en küçüğü ($MinU$) tespit edilir. Birinci sütun ikinci elemanın işareti değiştirilmeden, büyüklüğüne $MinU - T(i)$ değeri atanır. Burada geçen $T(i)$, i. bloğun ölçekleme faktörüdür ve seçilen optimizasyon algoritmasına (ABA ya da KUAABA) bağlı olarak belirlenir. KUAABA'nın uygulanması için Bölüm 2.1.1.2.3'te verilen prosedür işletilecektir. ABA için ise Bölüm 2.2.1.2.5'te anlatılacak olan süreç gerçekleştirilecektir. Damgalanmış U matrisi (U_i^*), S_i ve V_i matrislerine ters TDA uygulanarak damgalanmış blok ($blok_i^*$) elde edilir. TDA kullanılarak damga gömme süreci için gereken adımlar şu şekildedir:

Adım i: Seçilen bloklara damga bitlerini gömmek için öncelikle bloğa TDA uygulanır.

$$[U_i, S_i, V_i] = TDA(blok_i) \tag{2.19}$$



Şekil 2.13. Optimize edilmiş YDDADD tabanlı biyometrik damgalama sisteminin damgalama süreci

Adım ii: TDA sonucu üç bileşen (U_i, S_i ve V_i) elde edilir. U_i matrisinin ilk sütunundaki ikinci katsayı damga gömmek için modifiye edilir. Damga biti 1 ise, U_i'nin ilk sütun vektörünün mutlak değerlerinin maksimum değeri ($MaxU$) hesaplanır. Daha sonra, $U_{i_{2,1}}$'in

değeri $sign(U_{i_{2,1}}) \times (MaxU + T(i))$ olarak değiştirilir. Damga biti 0 ise, U matrisinin ilk sütun vektörünün mutlak değerce minimumu ($MinU$) hesaplanır. $sign(U_{i_{2,1}}) \times \big(MinU - T(i)\big)$ değeri $U_{i_{2,1}}$'e atanır. Burada $T(i)$ i. bloğun ölçeklendirme faktörü, $sign$ işaret fonksiyonudur.

Adım iii: Modifiye edilmiş U matrisi (U_i^*), S_i ve V_i matrisleriyle birlikte ters TDA işlemine tabi tutularak modifiye edilmiş blok elde edilir. Burada, V_i^T, V_i'nin devrik matrisini ifade eder.

$$blok_i^* = U_i^* \times S_i \times V_i^T \tag{2.20}$$

QR Ayrıştırmanın uygulanması: QR Ayrıştırma sonucu Q ve R matrisleri elde edilir. R matrisinin bir özelliği, giriş matrisinin sütunları (bir görüntü durumunda olduğu gibi) yüksek olasılıkla ilişkilendirildiğinde, R matrisinin ilk satır elemanlarının mutlak değeri, diğer satırların mutlak değerinden daha büyüktür. Dolayısıyla, ilk satırdaki küçük değişiklikler orijinal görüntünün görsel kalitesinde daha az bozulmaya sebep olacaktır [49]. Örnek bir giriş matrisi için QR Ayrıştırma sonucu elde edilen R matrisi Şekil 2.14'te verilmiştir.

155	156	157	158
154	156	155	153
155	157	158	159
153	154	155	154

(a) Giriş Matrisi

-308.5045	-311.5060	-312.5076	-312.0182
0	-0.9953	0.0159	0.5493
0	0	-1.4051	-3.5052
0	0	0	-1.4371

(b) R Matrisi

Şekil 2.14. Örnek giriş matrisine ilişkin R matrisi

Damga gömme sürecinde öncelikle seçilen her bloğa ($blok_i$) QR Ayrıştırma uygulanır. R_i matrisinin ilk satırına damga gömmek için, [-1, 1] aralığında artan sırada rastgele bir dizi (D1) ve aynı aralıkta azalan sırada rastgele bir dizi (D0) oluşturulur. D1 ve D0, sırasıyla *Gizli Anahtar 2* ve *Gizli Anahtar 3* adlı iki vektörde tutulur ve damga çıkarma sürecinde de kullanılır. Damga biti 1 ise R_i matrisinin birinci satır elemanlarına ($R_i(1,:)$) $D1 \times T_i$ eklenir. Eğer gömülecek bit 0 ise aynı katsayılar $D0 \times T_i$ ile toplanır. Bloğa özgü

ölçekleme faktörü (T_i) seçilen optimizasyon algoritmasına göre belirlenir. Bu algoritmaların uygulanma prosedürleri Bölüm 2.1.1.2.3 ve Bölüm 2.2.1.2.5'te yer almaktadır. Damgalanmış blok ($blok_i^*$) Q_i ve damgalanmış R_i'nin (R_i^*) çarpımı ile elde edilir. R matrisine damga gömmek için gereken adımlar aşağıdaki gibidir:

Adım i: YDDADD sonucu LL banttan seçilen her bir bloğa ($blok_i$) QR Ayrıştırma uygulanır. Elde edilen R_i matrisi damga gömmek için kullanılır.

$$[Q_i, R_i] = QR(blok_i) \tag{2.21}$$

Adım ii: 1 değerli biti gömmek için [-1, 1] aralığında artan sırada rastgele bir dizi (D1) oluşturulur. 0 değerli biti gömmek için [1, -1] aralığında azalan sırada rastgele bir dizi (D0) oluşturulur. D1 ve D0, sırasıyla *Gizli Anahtar 2* ve *Gizli Anahtar 3* adlı iki vektörde tutulur.

Adım iii: Aşağıdaki denklemler damgayı yerleştirmek için kullanılır. Burada T_i damganın gömme kuvvetini kontrol eden eşik değeri ifade eder.

$$R_i^* = R_i \tag{2.22}$$

$$R_i^*(1,:) = \begin{cases} R_i^*(1,:) + D0 \times T_i, & if\ w_i == 0 \\ R_i^*(1,:) + D1 \times T_i, & if\ w_i == 1 \end{cases} \tag{2.23}$$

Adım iv: Damgalanmış blok ($blok_i^*$) aşağıdaki gibi hesaplanır:

$$blok_i^* = Q_i R_i^* \tag{2.24}$$

Schur Ayrıştırmanın uygulanması: [42]'de rapor edildiğine göre, Schur Ayrıştırmadan sonra görüntü bloğunun üniter matrisi U'nun tüm ilk sütun elemanları aynı işarete sahiptir ve değerleri çok yakındır. Bu nedenle damganın Schur Ayrıştırma sonucu elde edilen U bileşeninin ilk sütun vektörüne gömülmesi daha uygun olacaktır. Öncelikle seçilen blok ($blok_i$) Schur Ayrıştırma ile U_i ve V_i bileşenlerine ayrıştırılır. U_i'nin birinci sütun ikinci katsayısına ($U_{i_{2,1}}$) damga gömmek için, birinci sütun elemanlarının mutlak değerlerinin en büyük ve en küçük olanı ($MaxU$ ve $MinU$) belirlenir. Eğer gömülecek bit 1 ise $U_{i_{2,1}}$'in değeri $MaxU + T_i$ olarak, 0 ise $MinU - T_i$ olarak değiştirilir. $U_{i_{2,1}}$'in işaretinin korunması için bu

katsayıya atanan değer işaret fonksiyonuyla ($sign(U_{i_{2,1}})$) çarpılır. Güncellenmiş U_i matrisi (U_i^*), V_i ile birlikte ters Schur ayrıştırmaya tabi tutularak damgalanmış blok ($blok_i^*$) elde edilir. Diğer iki ayrıştırma tekniğinde olduğu gibi burada bahsi geçen çoklu ölçekleme faktörlerinin optimizasyonu (T) ABA (Bölüm 2.2.1.2.5) ve KUAABA (Bölüm 2.1.1.2.3) için ayrı ayrı test edilmiştir.

YDDADD'nin LL bandındaki seçilmiş bloklara Schur Ayrıştırma ile damga gömülmesi durumunda gereken adımlar aşağıdaki gibidir:

Adım i: Standart sapmaya göre belirlenen her bir bloğa Schur Ayrıştırma uygulanır. Elde edilen U_i matrisi damga gömmek için kullanılır.

$$[U_i, V_i] = Schur(blok_i) \tag{2.25}$$

Adım ii: Ortaya çıkan U_i bileşeninin ilk sütununun katsayıları aynı işarete sahiptir. Ayrıca değerleri birbirine çok yakındır. Bu nedenle, U_i bileşeninin ilk sütun vektörü damga gömmek üzere değiştirilir. 1 değerli bit gömülecekse, ilk sütun vektörünün mutlak değerlerinin maksimumu ($MaxU$) belirlenir. Ardından U_i bileşeninin ilk sütun vektörünün ikinci katsayısı $U_{i_{2,1}}$'in mutlak değeri ($\left|U_{i_{2,1}}\right|$), $MaxU + T_i$ olarak güncellenir. 0 değerli bit gömülecekse, U_i bileşeninin ilk sütun vektörünün mutlak değerlerinin minimumu ($MinU$) belirlenir. U_i bileşeninin ilk sütun vektörünün ikinci katsayısı $U_{i_{2,1}}$'in mutlak değeri ($\left|U_{i_{2,1}}\right|$), $MinU - T_i$ olarak ayarlanır. Burada T_i damganın gömme gücünü ifade eder.

$$MaxU = \max\left(\left|U_i(:,1)\right|\right) \tag{2.26}$$

$$MinU = \min\left(\left|U_i(:,1)\right|\right) \tag{2.27}$$

$$U_i^* = U_i \tag{2.28}$$

$$U_{i_{2,1}}^* = \begin{cases} sign(U_{i_{2,1}}) \times (MaxU + T_i), & if\ w_i == 1 \\ sign(U_{i_{2,1}}) \times (MinU - T_i), & if\ w_i == 0 \end{cases} \tag{2.29}$$

Adım iii: Damgalanmış blok ($blok_i^*$) ters Schur Ayrıştırma ile elde edilir.

$$blok_i^* = U_i^* \times V_i \times U_i^{*T} \tag{2.30}$$

Tercih edilen ayrıştırma tekniğine bağlı olarak seçilen bloklar yukarıda verildiği şekilde damgalanır. Damgalanan bloklar diğerleriyle birleştirilip damgalanmış LL bant (LL^*) oluşturulur ve LH, HL ve HH bant ile ters YDDADD'ye tabi tutulur. Damgalanmış Y bileşen (I_Y^*), Cb bileşeni ve Cr bileşeni ile birlikte RGB uzayına çevrilerek damgalanmış görüntü (I^w) elde edilir.

Yukarıda, $N \times N$ boyutundaki renkli orijinal görüntüye (I), 8×200 bitten oluşan ikili iris kodunu gömmek için gerekli süreç detaylıca anlatılmıştır. Aşağıda bu sürece ait akış adımlar halinde verilmiştir.

Adım 1: RGB uzayındaki renkli görüntü ilk olarak YCbCr uzayına dönüştürülür.

$$[I_Y, I_{Cb}, I_{Cr}] = RGB\_YCbCr(I) \tag{2.31}$$

Adım 2: Y kanalına (I_Y) "Haar" filtre kullanılarak YDDADD uygulanır.

$$[LL, LH, HL, HH] = YDDADD(I_Y) \tag{2.32}$$

Adım 3: LL bant 4×4 boyutlu örtüşmeyen bloklara ayrılır.

Adım 4: Her bloğa bir bit gizlendiğinde, damga boyutundan daha fazla blok elde edilirse, damganın gömüleceği uygun blokları belirlemek için tüm bloklar standart sapma değerlerine bağlı olarak artan sırada sıralanır. Sıralanan bloklardan ilk 1600 tanesi, gömme konumu olarak seçilir ve damga çıkarma aşamasında kullanmak için bir vektörde tutulur (*Gizli Anahtar 1*).

Adım 5: Belirlenen bloklara seçilen ayrıştırma tekniği uygulanır. Ayrıştırma sonucu elde edilen ilgili alt bileşene damga gömülür. Burada damganın gömme kuvvetini kontrol eden her bloğa özgü eşik değer, tercih edilen optimizasyon algoritması tarafından belirlenir.

Adım 6: Damgalanmış blok, damgalanmış bileşen ve diğer alt bileşenlere uygulanan ayrıştırma tekniğinin tersi ile oluşturulur.

Adım 7: Tüm damga bitleri gömüldükten sonra, ortaya çıkan değiştirilmiş bloklar diğer bloklarla birleştirilir ve damgalanmış LL bant (LL^*) elde edilir. Ardından, damgalanmış Y bileşenini (I_Y^*) elde etmek için ters YDDADD uygulanır.

$$I_Y^* = YDDADD^{-1}(LL^*, LH, HL, HH) \tag{2.33}$$

Adım 8: Damgalanmış Y bileşeni diğer iki renk bileşeniyle birlikte, damgalanmış renkli görüntü (I^w) elde etmek için RGB renk uzayına dönüştürülür.

$$I^w = YCbCr\_RGB(I_Y^*, I_{Cb}, I_{Cr}) \tag{2.34}$$

2.2.1.2.4. Damga Çıkarma Süreci

YDDADD alanında her üç ayrıştırma tekniği için tasarlanan sistemler damga çıkarma açısından kördür. Damga çıkarma adımında yalnızca ilgili gizli anahtarlar kullanılır. Ne orijinal görüntü ne de damga bilgisi damga çıkarma adımında gereklidir. Damgalanmış ve muhtemelen saldırıya uğramış bir görüntüden (I^{wc}) iris kodunu çıkarmak için öncelikle görüntü YCbCr uzayına dönüştürülür. Y kanalı (I_Y^{wc}) "Haar" filtre kullanılarak YDDADD ile alt bantlarına ayrıştırılır. LL bant (LL^{wc}) örtüşmeyen 4×4 piksel boyutlu bloklara ayrılır. *Gizli Anahtar 1* yardımıyla damganın gömüldüğü bloklar seçilir. Seçilen ayrıştırma tekniğine özgü damga çıkarma süreci aşağıda anlatılmaktadır.

TDA ile damga çıkarma: *Gizli Anahtar 1* ile seçilen bloğa ($blok_i^{wc}$) TDA uygulandığında elde edilen U bileşeni **(U_i^{wc})** damga çıkarmak üzere seçilir. Öncelikle U_i^{wc}'nin birinci sütun bileşenlerinin mutlak değerler açısından maksimum ($MaxU$) ve minimum ($MinU$) olanı bulunur. Bu sütundaki ikinci katsayının mutlak değeri ($\left|U_{i_{2,1}}^{wc}\right|$) $MaxU$'ya daha yakınsa çıkarılan bit 1, $MinU$'ya daha yakınsa çıkarılan bit 0'dır. TDA için gerekli çıkarma adımları aşağıda verilmiştir:

Adım i: Seçilen blokların her biri TDA ile U_i, S_i ve V_i bileşenlerine ayrıştırılır.

$$[U_i^{wc}, S_i^{wc}, V_i^{wc}] = SVD(blok_i^{wc}) \tag{2.35}$$

Adım ii: Gömülen damga U_i^{wc} bileşeninden Şekil 2.15'te verilen denklemlere bağlı olarak çıkarılır. Burada w_i^{ex}, çıkarılan i indeksli damga bitini ifade eder.

$$
\begin{aligned}
&MaxU = max\left(|U_i^{wc}(:,1)|\right)\\
&MinU = min\left(|U_i^{wc}(:,1)|\right)\\
&DiffMax = \left|MaxU - \left|U_{i2,1}^{wc}\right|\right|\\
&DiffMin = \left|MinU - \left|U_{i2,1}^{wc}\right|\right|\\
&w_i^{ex} = \begin{cases} 1, & DiffMax \leq DiffMin \\ 0, & değilse \end{cases}
\end{aligned}
$$

Şekil 2.15. YDDADD-TDA alanına gömülen damganın U bileşeninden çıkarılması

QR Ayrıştırma ile damga çıkarma: LL bandın ilgili bloğundan ($blok_i^{wc}$) gömülen damgayı çıkarmak için ilk olarak bu blok QR Ayrıştırma ile bileşenlerine (Q_i^{wc}, R_i^{wc}) ayrıştırılır. R_i^{wc}'nin birinci satır elemanları ile $Gizli\ Anahtar\ 2$'de tutulan $D1$ arasındaki korelasyon ($corr1$) ve $Gizli\ Anahtar\ 3$'te tutulan $D0$ arasındaki korelasyon ($corr0$) hesaplanır. Elde edilen korelasyon katsayılarından $corr1$ daha büyükse çıkarılan bit 1, değilse çıkarılan bit 0'dır. QR Ayrıştırma için uygulanan damga çıkarma adımları şu şekildedir:

Adım i: Seçilen bloklardan damga bitini geri kazanmak için her birine QR Ayrıştırma uygulanır.

$$[Q_i^{wc}, R_i^{wc}] = QR(blok_i^{wc}) \tag{2.36}$$

Adım ii: Elde edilen R_i^{wc} matrisine gömülü olan damgayı çıkarmak için aşağıdaki eşitliklerden yararlanılır.

$$corr0 = corr(R_i^{wc}(1,:), D0) \tag{2.37}$$

$$corr1 = corr(R_i^{wc}(1,:), D1) \tag{2.38}$$

$$w_i^{ex} = \begin{cases} 0, & corr0 > corr1 \\ 1, & corr1 \geq corr0 \end{cases} \quad (2.39)$$

Burada, $corr$ korelasyonu ifade etmektedir.

Schur Ayrıştırma ile damga çıkarma: Gömülen bitleri çıkarmak için damgalanmış her bir bloğa Schur Ayrıştırma uygulanır. U bileşeninin (U_i^{wc}) birinci sütun vektörünün mutlak değeri en büyük olan ve en küçük olan katsayıları sırasıyla $MaxU$ ve $MinU$ değişkenlerine atanır. Aynı bileşenin birinci sütun ikinci satırda yer alan elemanının mutlak değeri ($absU21$) hesaplanır. $absU21$ $MaxU$'ya daha yakınsa çıkarılan bit 1, $MinU$'ya daha yakınsa çıkarılan bit 0'dır. Schur Ayrıştırma için gerekli çıkarma adımları aşağıda verilmiştir.

Adım i: Her bir seçilen bloktan damga bitini çıkarmak için ilgili bloğa Schur Ayrıştırma uygulanır.

$$[U_i^{wc}, V_i^{wc}] = Schur(blok_i^{wc}) \quad (2.40)$$

Adım ii: Elde edilen U_i^{wc} matrisinin birinci sütun vektörüne gömülü olan damgayı çıkarmak için Şekil 2.16'da verilen ifadeden yararlanılır. Burada w_i^{ex}, i indeksli çıkartılmış damga bitini temsil eder.

$$\begin{aligned} absU21 &= \left|U_{i\,2,1}^{wc}\right| \\ MaxU &= max\left(\left|U_i^{wc}(:,1)\right|\right) \\ MinU &= min\left(\left|U_i^{wc}(:,1)\right|\right) \\ DiffMax &= |MaxU - absU21| \\ DiffMin &= |MinU - absU21| \\ w_i^{ex} &= \begin{cases} 1, & DiffMax \leq DiffMin \\ 0, & değilse \end{cases} \end{aligned}$$

Şekil 2.16. YDDADD-Schur Ayrıştırma alanına gömülen damganın U bileşeninden çıkarılması

Gömülen ikili iris kodunu damgalanmış ve muhtemelen saldırıya uğramış görüntüden bu üç ayrıştırma tekniği ile çıkarmak için yukarıda detayları verilen süreç, aşağıdaki adımlar yardımıyla özetlenebilir:

Adım :1 RGB uzayındaki renkli damgalanmış ve muhtemelen bozulmuş görüntü (I^{wc}) ilk olarak YCbCr uzayına dönüştürülür.

$$[I_Y{}^{wc}, I_{Cb}{}^{wc}, I_{Cr}{}^{wc}] = RGB\_YCbCr(I^{wc}) \tag{2.41}$$

Adım 2: Elde edilen Y kanalına (I_Y^{wc}) "Haar" filtre yardımıyla YDDADD uygulanır.

$$[LL^{wc}, LH^{wc}, HL^{wc}, HH^{wc}] = YDDADD(I_Y{}^{wc}) \tag{2.42}$$

Adım 3: LL bant (LL^{wc}) 4×4 boyutlu örtüşmeyen bloklara ayrılır.

Adım 4: Damga bitlerinin gömülü olduğu bloklar, *Gizli Anahtar 1* kullanılarak seçilir.

Adım 5: Standart sapma değerlerine göre belirlenen bloklardan gömülen biti çıkarmak için bloğa ilgili ayrıştırma tekniği uygulanır.

Adım 6: Seçilen ayrıştırma tekniğine özgü damga çıkarma prosedürü yardımıyla damgalanmış bileşenden damga çıkarılır.

2.2.1.2.5. ABA'nın Uygulanması

Bu çalışmada birbiriyle çelişen damgalama gereksinimleri algılanamazlık ve dayanıklılık arasında iyi bir ödünleşim elde etmek için ABA ve ABA'nın değiştirilmiş bir sürümü olan KUAABA'dan yararlanılmıştır. Her iki optimizasyon algoritması gömme sürecinde kullanılan ve ölçekleme faktörü olarak da bilinen çoklu eşik değerlerini seçmek için kullanılır. KUAABA'nın uygulanma süreci Bölüm 2.1.1.2.3'te verildiği gibidir.

ABA'nın uygulanması için popülasyon boyutu, p, 10'a, α, $\beta_0$ve γ sırasıyla 0.1, 0.1, 1'e ayarlanmıştır. Her blok için farklı ölçekleme faktörü kullanılacağından ateş böceklerinin boyutu damga boyutuna eşit seçilmelidir. İlk iterasyon için ateş böceklerine rasgele değerler atanır. Her bir ateş böceği için, bu rasgele değerler ölçekleme faktörü olarak kullanılarak damga gömme süreci gerçekleştirilir. Damgalanmış görüntü ve orijinal görüntüye bağlı olarak TSGO hesaplanır. Bölüm 2.1.1.2.3'te verilen ataklar damgalanmış görüntüye

uygulanarak sekiz adet bozulmuş ve damgalanmış görüntü oluşturulur. Hem atak olmadığı durumda hem de bu ataklar söz konusu olduğunda oluşturulan görüntülerden damga çıkarılır ve gömülen damga ile arasındaki NK hesaplanır. TSGO ve ortalama NK'ya bağlı olarak amaç fonksiyonu (2.11) yardımıyla bulunur. Bu fonksiyondan elde edilen uygunluk değeri ateş böceğinin parlaklığı olarak ifade edilir. Her bir ateş böceği (2.8)'e bağlı olarak daha parlak olana doğru hareket ettirilir. Güncellenen konumlarla ateş böcekleri için bir sonraki iterasyon başlar. Bu süreç algoritma daha iyi çözümler bulduğu sürece devam ettirilir. Optimizasyon aşaması bittiğinde ise sıralanan ateş böcekleri arasından parlaklığı en yüksek olan çözüm kümesi olarak belirlenir. ABA optimizasyonu için gerekli prosedür aşağıda verildiği şekildedir:

Adım 1: Damga boyutu kadar p ateş böceği rastgele oluşturulur. Bir bloğa tek bit gömüleceğinden, her ateş böceğinin boyutu damga boyutuna eşit olmalıdır.

Popülasyondaki her ateş böceği için 2-7 arasındaki adımlar gerçekleştirilir:

Adım 2: Damga, damga gömme sürecine bağlı olarak gömülür.

Adım 3: Damgalanmış görüntü ve orijinal görüntü arasında TSGO hesaplanır.

Adım 4: Damgalanmış görüntüye M saldırı uygulanır ve M bozulmuş ve damgalanmış görüntü elde edilir.

Adım 5: Bir adet damgalanmış görüntüden, M tane de bozulmuş ve damgalanmış görüntüden damga çıkarma sürecine bağlı olarak damga çıkarılır.

Adım 6: Orijinal damga ve çıkarılan damga arasındaki NK değeri belirlenir.

Adım 7: Ortalama NK ve TSGO'ya bağlı olarak amaç fonksiyonu hesaplanır.

Adım 8: Ateş böcekleri daha parlak olana, yani uygunluk değeri daha yüksek olana, doğru hareket ettirilir.

Adım 9: Optimizasyon algoritması daha iyi çözümler bulduğu sürece, 2-8 arası adımlar sürdürülür.

Adım 10: Yinelemeler artık daha iyi sonuçlar vermediğinde algoritma sona erer. Ateş böcekleri sıralandıktan sonra uygunluk değeri en yüksek olan en iyi çözüm olarak seçilir.

2.2.1.3. Kimlik Doğrulama Süreci

YDDADD alanında iris tabanlı biyometrik damgalama şemalarının her birinde damgalanmış görüntüden iris kodunun kurtarılması yoluyla sayısal görüntünün gerçek sahiplerinin kimlik doğrulamasını gerçekleştirilir. Bu amaçla çıkarılan iris kodu, kullanıcılar

tarafından sağlanan diğer iris kodları ile karşılaştırılır. Yöntemlerde kullanılan benzerlik ölçüsü, HU ölçütüdür. HU'nun ölçüm metriği olarak seçilmesinin nedeni, iris kodunun ikili olması ve HU'nun iki ikili dizinin farklı olduğu bit konumlarının sayısını basitçe yakalayabilmesidir. Çıkarılan iris kodu ile kullanıcılar tarafından sağlanan diğer örnekler arasındaki benzerlik skoru, önceden tanımlanmış eşik değerine göre kontrol edilir. HU belirlenen eşik değerinin altındaysa giriş iris kodu gerçek olarak ilan edilir, aksi takdirde sahtekâr olarak sınıflandırılır.

2.2.1.4. Uygun Yöntemin Belirlenmesi

Bu çalışmada YDDADD alanında detayları önceki bölümlerde verilen üç ayrıştırma tekniği incelenmiştir. Bunun yanı sıra gömme adımında, sabit ölçekleme faktörü (optimizasyon algoritması uygulanmadan), ABA ile optimize edilmiş çoklu ölçekleme faktörü ve KUAABA ile optimize edilmiş çoklu ölçekleme faktörü kullanılarak yöntemlerin algılanamazlık (TSGO), dayanıklılık (ortalama NK (%), ortalama BHO (%)) ve kimlik doğrulama performansları (ortalama EHO (%)) test edilmiştir. Elde edilen test sonuçları Tablo 2.1'de yer almaktadır.

Tablo 2.1. YDDADD alanında kullanılan yöntemlerin performanslarının karşılaştırılması

	Sabit Ölçekleme Faktörü			**ABA**			**KUAABA**		
	TDA	**Schur**	**QR**	**TDA**	**Schur**	**QR**	**TDA**	**Schur**	**QR**
TSGO	35.0304	37.0304	38.1205	35.1704	37.3665	38.6705	35.7705	37.9401	**40.5822**
Ort. NK(%)	98.01	97.52	97.72	98.83	98.59	98.90	**99.10**	98.82	98.20
Ort. BHO (%)	1.92	2.18	1.98	1.65	1.73	**0.91**	1.23	1.71	1.56
Ort. EHO (%)	0.10	0.11	0.10	0.10	0.10	0.08	0.09	0.09	**0.07**

Tablo incelendiğinde, TSGO açısından hem optimizasyon algoritmaları kullanıldığında hem de sabit ölçekleme faktörü kullanıldığında QR Ayrıştırma daha iyi performans sergilemiştir. Dayanıklılık dikkate alındığında, ABA ve KUAABA ile optimize edilmiş çoklu ölçekleme faktörleri ile hesaplanan ortalama NK değerleri için sonuçlar birbirine çok yakın bulunmuştur. Ortalama NK %98.2 ile %99.10 arasında değişmektedir.

Benzer şekilde ortalama BHO için de ABA ve KUAABA kullanıldığında sabit ölçekleme faktörüne göre daha iyi sonuçlar elde edilse de bu değerler dar bir aralığa yığılmıştır. Kimlik doğrulama performansı incelendiğinde KUAABA'dan elde edilen hata oranı nispeten daha düşüktür.

Tablodaki verilere göre; dayanıklılık ve kimlik doğrulama hassasiyeti açısından sonuçlar birbirine daha yakın bulunmuştur. Asıl fark yaratan unsur ise algılanamazlıkta saklıdır. KUAABA tarafından optimize edilmiş QR Ayrıştırma TSGO'yu 40 dB'nin üzerine çıkardığı halde, ortalama NK ve BHO değerleri diğerleriyle yakın bulunduğu ve ortalama EHO değeri ise en düşük olan yöntem olduğu için en uygun yöntem olarak seçilmiştir.

3. BULGULAR

Bu kısımda Bölüm 2'de tanıtılan geleneksel tabanlı ve biyometrik tabanlı damgalama yöntemlerine ait araştırma bulguları detaylandırılmıştır. Ayrıca bu çalışmalardan elde edilen deneysel sonuçlar, literatürde yer alan damgalama şemalarıyla kıyaslanarak, önerilen sistemlerin avantaj ve dezavantajları irdelenmiştir. Tablo 3.1 dayanıklılığı test etmek amacıyla, tez kapsamında damgalanmış görüntülere uygulanan saldırıların kısaltmasını ve bunlara ait açıklamaları göstermektedir.

Tablo 3.1. Damgalanmış görüntülere uygulanan atakların tanımı

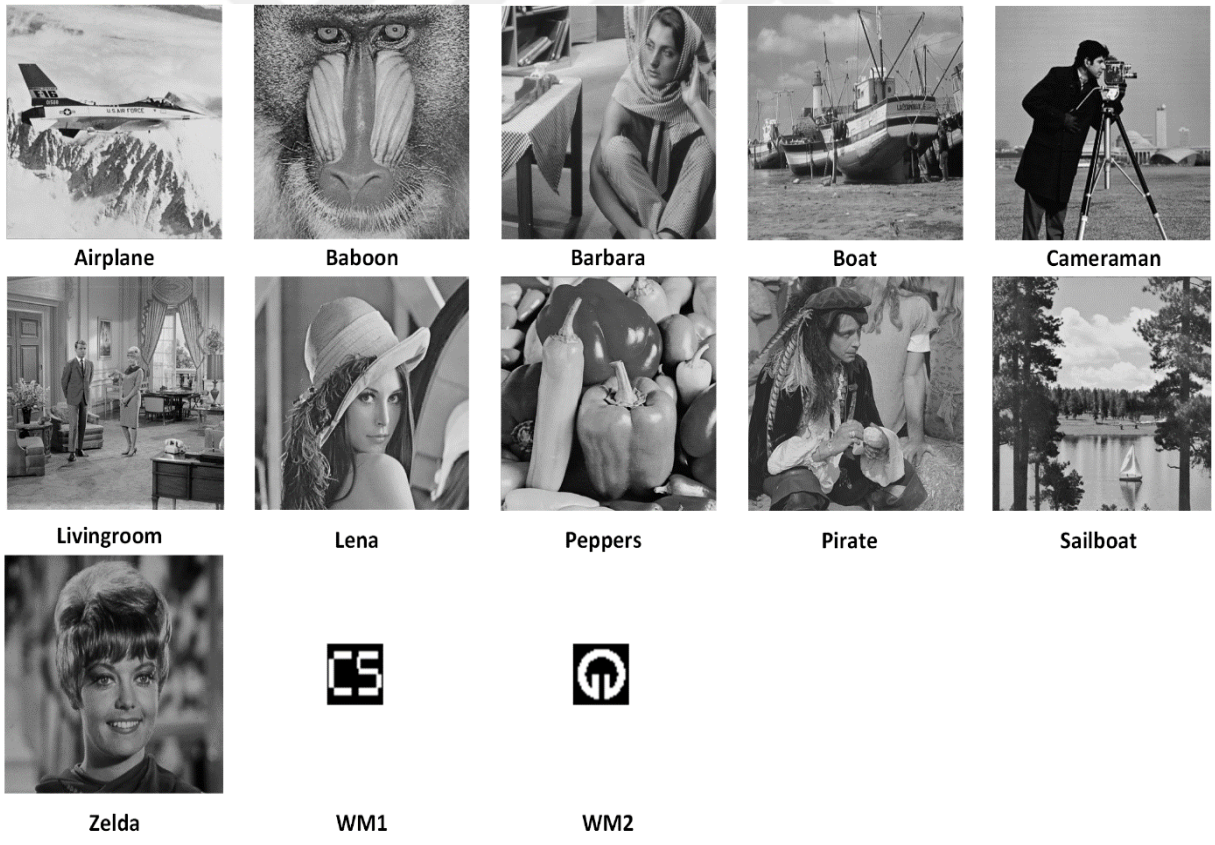
Atak	**Tanımı**	**Atak**	**Tanımı**
NA	Herhangi bir atak uygulanmadı	MDF nxn	Ortanca filtresi (Pencere boyutu nxn)
SPN d	Tuz & biber gürültüsü (yoğunluk d)	SF	Keskinleştirme filtresi
PN	Poisson gürültüsü	WF	Wiener filtre (Maske boyutu 3x3)
SN v	Benek gürültüsü (varyans v)	HE	Histogram eşitleme
GN v	Gaussian gürültüsü (Ortalama 0 ve varyans v)	RS 512-n-512	Yeniden ölçekleme 512-n-512
CR-T	Görüntünün üst-sol kısmından 100x100 boyutlu bir karenin kırpılması	GC	Gama düzeltme (Gama değeri 0.2)
CR-C	Görüntünün merkezinden 100x100 boyutlu bir karenin kırpılması	RT n	n derece rotasyon
CR-B	Görüntünün alt-sağ kısmından 100x100 boyutlu bir karenin kırpılması	FC	Sütun bazında çevirme
COM Q	JPEG sıkıştırma (Kalite faktörü Q)	FR	Satır bazında çevirme
GF nxn	Gaussian filtre (Maske boyutu nxn)	DL	Görüntüden rasgele 20 satır ve 20 sütun silme
MF	Ortalama filtresi (Maske boyutu 3x3)	WC bpp	Dalgacık sıkıştırma (bpp=piksel başına bit)

3.1. Geleneksel Damgalamaya Yönelik Çalışmanın Değerlendirilmesi

Bu bölümde gri seviye görüntülere ikili damganın gömüldüğü ADD-TDA-KUAABA tabanlı çalışmanın araştırma bulguları ele alınmıştır.

3.1.1. ADD-TDA-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntemin Değerlendirilmesi

ADD-TDA-KUAABA tabanlı sistemde standart gri seviye test görüntülerinin telif haklarının ve fikri mülkiyet haklarının korunması için dayanıklı damgalama şeması önerilmiştir. Önerilen sistemde, tüm deneyler için 512×512 gri seviye test görüntüsüne 32×32 boyutlu ikili damga (logo) yerleştirilmiştir. Bazı veri tabanlarından toplanan "Airplane", "Baboon", "Barbara", "Boat", "Cameraman", "Couple", "Lena", "Peppers", "Pirate", "Sailboat" ve "Zelda" imgeleri orijinal görüntü olarak kullanılmıştır. Damga Görüntüsü 1 (WM1) [97]'den alınmıştır. Damga Görüntüsü 2 (WM2) ise Karadeniz Teknik Üniversitesi ambleminden alınmıştır. Test görüntüleri, WM1 ve WM2 Şekil 3.1'de verilmiştir. Şekil 3.2'de ise damgalanmış ve saldırıya uğramış "Lena" görüntüleri verilmiştir.



Şekil 3.1. Deneylerde kullanılan test görüntüleri ve ikili damgalar

Önerilen sistemin üstünlüğünü kanıtlamak için önceki literatür çalışmaları ile karşılaştırma yapılmıştır. Tablo 3.2'de çalışmalarda kullanılan gri seviye orijinal görüntü ve ikili damga boyutunun kıyaslaması mevcuttur. [97-99] çalışmalarında yer alan orijinal görüntü 512×512, ikili damga ise 32×32 piksel boyutundadır. [85]'te önerilen yöntemde test edilen orijinal görüntü ve damga boyutu ise bu çalışmada kullanılanlara yakındır.

Şekil 3.2. Damgalanmış ve atak uygulanmış "Lena" görüntüleri: (a) SPN d=0.05, (b) PN, (c) SN v=0.009, (d) GN v=0.009, (e) CR-T, (f) CR-C, (g) CR-B, (h) COM Q=50, (i) GF 3x3 (j) MF , (k) MDF 3x3, (l) SF, (m) WF, (n) HE, (o) RS 512-256-512, (p) GC

Tablo 3.2. Kullanılan orijinal görüntü ve damga boyutunun referans çalışmalarla kıyaslanması

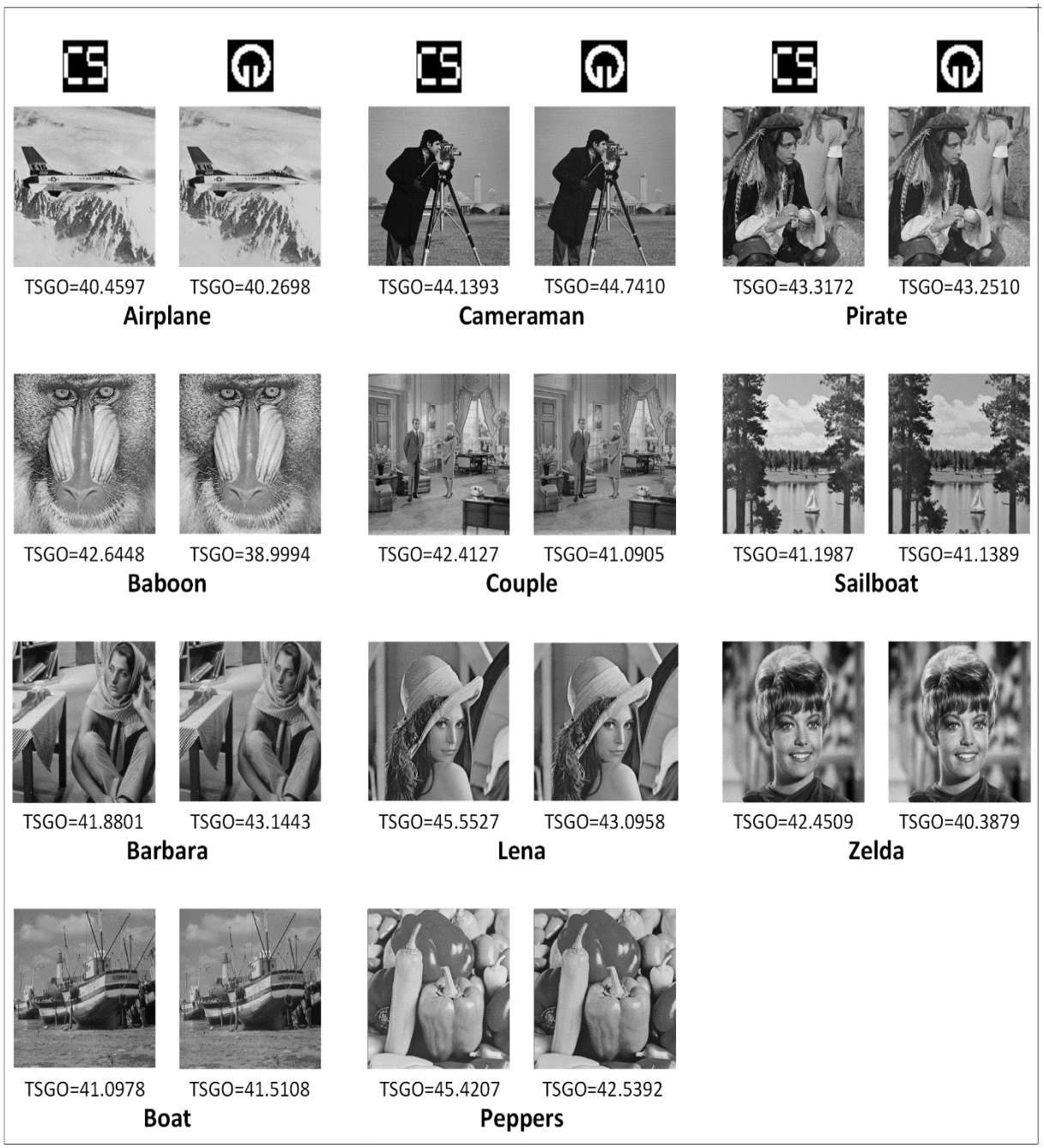
	[85]	[97]	[98]	[99]	ADD – TDA – KUAABA
Orijinal Görüntü Boyutu	510×510	512×512	512×512	512×512	512×512
Damga Boyutu	30×30	32×32	32×32	32×32	32×32

3.1.1.1. ADD-TDA-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntemin Algılanamazlık Performansı

Bu çalışmada damgalanmış görüntülerin görsel kalitesi TSGO metriği yardımıyla değerlendirilir. Şekil 3.3, WM1 ve WM2 ikili damgaları bahsi geçen test görüntülerine ayrı ayrı gömüldüğünde elde edilen TSGO değerlerini içermektedir. Tablo 3.3'te ise elde edilen TSGO değerlerinin referans çalışmalardakilerle karşılaştırması yapılmıştır. Bu tabloya göre, on bir standart test görüntüsü için önerilen yöntem tarafından hesaplanan ortalama TSGO değeri 42.7795 dB olarak bulunmuştur.

Tablo 3.3. Damgalanmış görüntülerin TSGO (dB) değerlerinin karşılaştırılması

Orijinal Görüntü	[85]	[97]	[98]	[99]	ADD – TDA – KUAABA
Airplane	46.31	37.7658	--	--	40.4597
Baboon	48.51	33.2136	38.4569	53.3506	42.6448
Barbara	51.08	36.2540	38.8425	--	41.8801
Boat	48.01	37.7568	38.8059	53.0877	41.0978
Cameraman	--	38.3383	--	--	44.1393
Couple	--	--	--	51.0125	42.4127
Lena	48.87	37.9815	38.8895	52.1906	45.5527
Peppers	48.49	37.1583	38.9708	51.9802	45.4207
Pirate	--	37.9239	--	54.1380	43.3172
Sailboat	--	35.5835	--	--	41.1987
Zelda	--	--	--	--	42.4509



Şekil 3.3. Damgalanmış test görüntüleri ve TSGO değerleri

40 dB'nin üzerinde bulunan ortalama TSGO, önerilen yöntemin iyi bir görsel kaliteye sahip olduğunu ve gömülen damganın insan algısal sistemi tarafından görünmez olduğunu göstermektedir. Mevcut çalışmanın TSGO değerinin [97, 98]'de rapor edilen TSGO değerine göre tüm test görüntülerinde daha yüksek olduğu gözlenmiştir. Ancak bu şemanın algısal performansı diğer iki çalışmadan ([85, 99]) nispeten daha düşüktür. Çalışmalarda rapor edilmeyen sonuçlar "--" ile gösterilmiştir.

3.1.1.2. ADD-TDA-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntemin Dayanıklılık Performansı

Bu çalışmada saldırılara karşı dayanıklılık NK ve BHO değerlerine bağlı olarak ölçülür. Tablo 3.4'te, damgalanmış (atak içermeyen) ve bozulmuş (atak içeren) görüntüler için gömülen damga ile çıkartılmış damga arasındaki NK (%) değerleri rapor edilir. Tablo 3.5 ise BHO (%) değerlerini içerir. Damgalanmış görüntüye hiçbir saldırı uygulanmadığında, NK %100 ve BHO %0 olarak bulunmuştur.

Gürültü atakları: Tüm taşıyıcı görüntüler için önerilen yöntemin NK değeri, gürültülü saldırılar arasında Poisson gürültüsüne (PN) ve benek gürültüsüne (SN 0.001) karşı %100'e eşittir. Aynı saldırılar için BHO %0'dır. 0.005 ve 0.009 varyanslı benek gürültüsü için ortalama NK sırasıyla %98.21 ve %94.87'dir. Bunlar için ortalama BHO %1.66 ve %4.82 olarak bulunmuştur. $d = 0.01$ yoğunluktaki tuz & biber gürültüsü için (SPN 0.01), yöntemin NK ve BHO değerlerinin ortalaması sırasıyla %93.04 ve %6.42'dir. Yoğunluk arttıkça tuz & biber gürültüsüne karşı dayanıklılık nispeten azalır. Önerilen şemanın 0.001 varyanslı Gauss gürültüsüne (GN 0.001) karşı ortalama NK değeri %96.14 iken, ortalama BHO değeri %3.63'tür. Varyans 0.005 ve 0.009 olduğunda, ortalama NK %80'in üzerindedir. Bu sonuçlar, yöntemin gürültü ataklarına, özellikle benek gürültüsü ve Poisson gürültüsüne karşı dayanıklı olduğunu kanıtlamaktadır.

Kırpma: 100×100 boyutlu bir karesel alan görüntünün merkezinden (CR-C), sol üst köşesinden (CR-T) veya sağ alt köşesinden (CR-B) ayrı ayrı kırpıldığında, yöntem damgayı başarılı bir şekilde çıkarır. Bu üç kırpma atağı için ortalama NK %96'nın üzerindedir. Ortalama BHO ise yaklaşık %2'dir. Damga ardışık bloklara yerleştirilmediğinden, yöntem kırpma saldırısından minimum düzeyde etkilenir.

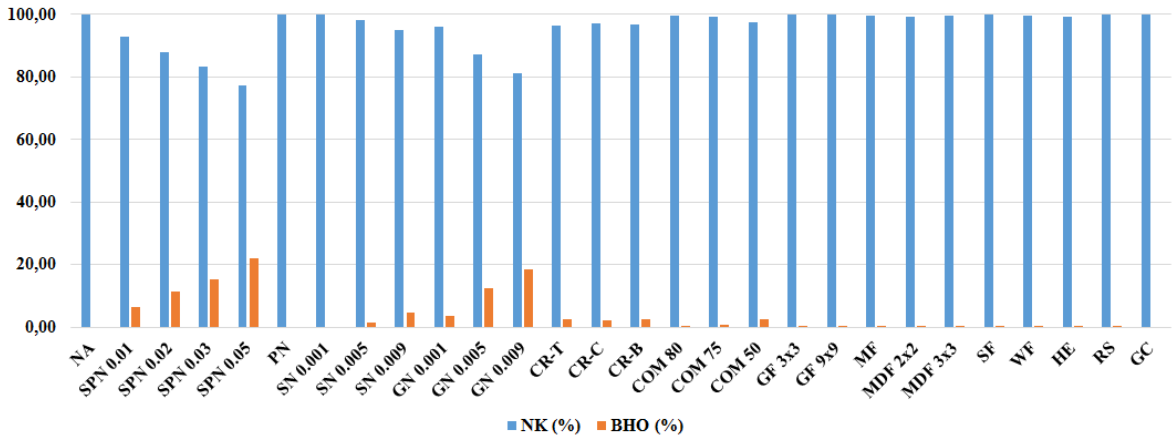
JPEG sıkıştırma: 80, 75 ve 50 kalite faktörü ile JPEG sıkıştırma (COM) için dayanıklılık ölçüldüğünde NK değerlerinin %100'e çok yakın olduğu görülmektedir. NK değerleriyle tutarlı olarak BHO değeri de çok düşüktür. Ortalama BHO Q=80 iken %0.5, Q=75 iken %0.73 ve Q=50 iken %2.49 olarak bulunmuştur. Bu sonuçlar, önerilen şemanın JPEG sıkıştırma saldırısına karşı dayanıklı olduğunun göstergesidir.

Filtreleme: Bu çalışmada, çeşitli filtreleme ataklarına karşı dayanıklılık ele alınmıştır. Bunlar arasında yöntemin Gauss filtre (GF) saldırısına karşı performans çok iyidir. Şöyle ki ortalama NK ve ortalama BHO sırasıyla %99.98 ve %0.02 olarak bulunmuştur. Yine elde

edilen sonuçlara göre ortalama NK ve BHO değerleri ortanca filtre (MDF) saldırısı için sırasıyla %99.78 ve %0.21'dir. Ortalama filtre (MF) atağına karşı ortalama NK %99.67 olarak bulunmuştur. Aynı filtreleme saldırısına karşı ortalama BHO %0.21'dir. Önerilen yöntem, keskinleştirme filtresine (SF) karşı da dayanıklıdır. Ortalama NK ve BHO %100 ve %0.01 olarak hesaplanmıştır. Wiener filtrede (WF) NK ve BHO %99.79 ve %0.18 olarak bulunmuştur. Bu sonuçlara göre damga, filtreleme saldırılarında neredeyse hatasız olarak çıkarılmaktadır.

Diğer ataklar: Histogram eşitleme (HE) ve yeniden ölçekleme (RS) için, ortalama NK çok yüksektir ve bu ataklar için ortalama BHO değerleri %0'a çok yakındır. Gama düzeltmeye (GC) karşı dayanıklılık test edildiğinde, NK %100 olarak bulunur. Aynı atak için ortalama BHO'nun %0 olduğu gözlenmektedir.

Şekil 3.4 damgalanmış on bir test görüntüsüne yukarıda bahsi geçen ataklar uygulandığında elde edilen ortalama NK (%) ve BHO (%) değerlerini göstermektedir. Görüldüğü üzere atak yokken (NA) gömülen ikili damga hatasız çıkarılmıştır. Poisson gürültüsü (PN), benek gürültüsü (SN), kırpma (CR-T, CR-C, CR-B), JPEG sıkıştırma (COM), filtreleme atakları (GF, MF, MDF, SF, WF), histogram eşitleme (HE), yeniden ölçekleme (RS), gama düzeltme (GC) söz konusu olduğunda da NK oldukça yüksek ve BHO ise %0 ya da %0'a yakın bulunmuştur. Yöntemin dayanıklılığının tuz & biber gürültüsü (SPN) ve Gauss gürültüsüne (GN) karşı nispeten daha düşük olduğu tespit edilmiştir. Ayrıca bu sonuçlardan NK ve BHO değerleri arasında tutarlılık olduğu da görülmektedir.



Şekil 3.4. 11 test görüntüsüne ait ortalama NK/BHO grafiği

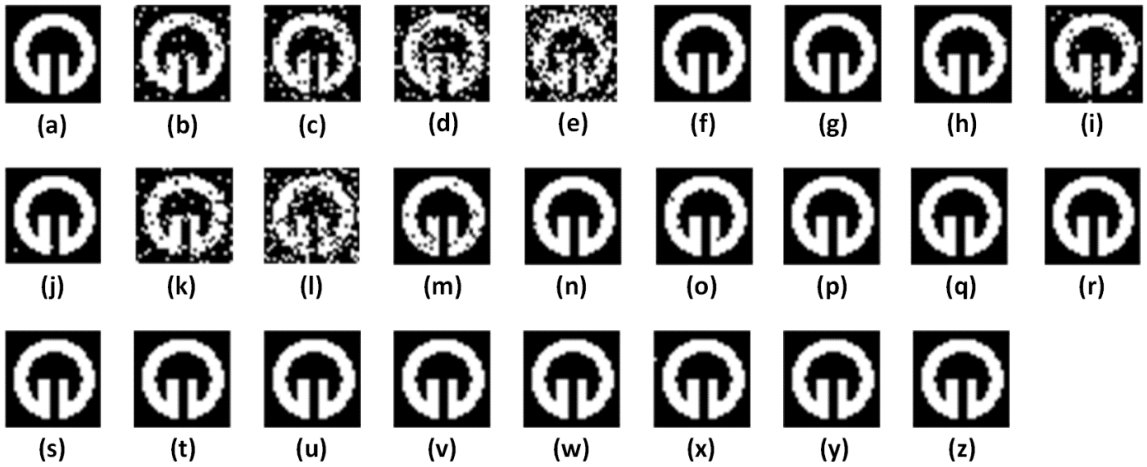
Tablo 3.4. Ataklar karşısında 11 test görüntüsüne ait NK (%) değerleri

Atak	Airplane	Baboon	Barbara	Boat	Cameraman	Couple	Lena	Peppers	Pirate	Sailboat	Zelda
NA	100	100	100	100	100	100	100	100	100	100	100
SPN 0.01	96.38	94.1	92.36	93.3	89.41	94.24	94.5	90.62	90.21	94.77	93.57
SPN 0.02	94.5	90.88	88.34	88.34	81.64	88.74	89.14	84.58	83.51	90.21	86.19
SPN 0.03	93.16	85.52	84.85	85.66	74.53	83.91	83.51	81.23	78.82	85.12	82.17
SPN 0.05	84.05	84.05	77.75	77.61	69.44	79.36	72.92	71.31	72.79	82.84	76.27
PN	100	100	100	100	100	100	100	100	100	100	100
SN 0.001	100	100	100	100	100	100	100	100	100	100	100
SN 0.005	97.45	95.84	99.87	99.73	99.06	99.2	97.72	93.43	99.87	98.53	99.6
SN 0.009	91.55	89.95	99.33	99.06	96.65	96.25	89.68	89.68	99.2	95.44	96.78
GN 0.001	100	99.73	94.91	97.72	88.34	98.66	98.53	90.62	94.24	98.26	96.51
GN 0.005	97.05	87.4	84.18	91.96	79.22	90.62	84.45	76.27	86.33	93.3	88.07
GN 0.009	91.29	83.24	78.55	87	73.99	80.56	77.35	71.05	80.83	87	83.11
CR-T	99.33	100	94.1	90.35	95.84	96.65	94.91	97.72	97.05	99.87	95.71
CR-C	99.33	89.54	93.3	99.46	97.05	97.72	100	99.33	95.44	96.78	98.93
CR-B	96.25	92.76	96.25	99.73	100	94.91	99.1	97.05	100	92.23	95.04
COM 80	100	100	99.87	100	96.11	100	100	98.93	100	100	99.73
COM 75	100	100	99.73	100	95.44	100	100	97.59	100	100	99.2
COM 50	99.87	100	95.44	99.2	88.61	99.73	99.33	93.97	98.66	99.46	98.12
GF 3x3	100	100	100	100	100	99.87	100	99.87	100	100	100
GF 9x9	100	100	100	100	100	99.87	100	99.87	100	100	100
MF	100	99.6	99.87	99.6	99.87	99.6	100	98.66	99.33	100	99.87
MDF 2x2	100	99.33	99.46	99.2	100	99.73	100	96.92	99.06	99.87	99.73
MDF 3x3	100	99.87	100	100	99.87	99.73	100	98.12	100	100	99.87
SF	100	100	100	100	100	100	100	100	100	100	100
WF	100	99.6	99.87	99.87	99.87	99.73	100	98.93	100	100	99.87
HE	100	100	99.6	97.05	100	99.87	99.73	97.72	100	100	98.79
RS 512-256-512	100	99.73	99.73	100	99.87	99.87	100	99.06	99.73	100	100
GC	100	100	100	100	100	100	100	100	100	100	100

Tablo 3.5. Ataklar karşısında 11 test görüntüsüne ait BHO (%) değerleri

Atak	Airplane	Baboon	Barbara	Boat	Cameraman	Couple	Lena	Peppers	Pirate	Sailboat	Zelda
NA	0	0	0	0	0	0	0	0	0	0	0
SPN 0.01	3.42	5.86	6.84	6.05	9.18	6.05	6.05	8.89	8.5	4.1	5.66
SPN 0.02	6.15	9.08	10.55	10.45	16.5	11.04	11.33	14.16	14.26	9.18	12.6
SPN 0.03	7.32	15.04	14.84	12.4	22.66	14.65	16.02	19.14	18.65	12.99	16.41
SPN 0.05	14.84	16.6	21.58	20.51	28.42	20.31	26.66	28.42	24.41	16.8	22.46
PN	0	0	0	0	0	0	0	0	0	0	0
SN 0.001	0	0	0	0	0	0	0	0	0	0	0
SN 0.005	2.25	3.61	0.1	0.2	0.98	0.68	2.44	6.05	0.1	1.37	0.49
SN 0.009	7.91	9.38	0.49	0.78	3.13	3.61	10.25	10.06	0.68	3.61	3.13
GN 0.001	0	0.49	5.47	1.86	10.84	1.17	1.56	9.08	4.59	1.66	3.22
GN 0.005	2.54	12.3	16.5	8.2	19.82	9.57	15.43	23.14	13.18	6.54	11.62
GN 0.009	8.69	16.99	20.61	12.6	24.51	19.43	22.46	29.98	19.24	12.6	16.6
CR-T	0.49	0	4.39	7.03	3.03	2.44	3.81	1.66	2.15	0.1	3.13
CR-C	0.49	7.62	5.08	0.39	2.25	1.66	0.1	0.49	3.42	2.44	0.88
CR-B	2.73	5.27	2.73	0.2	0	3.71	0.68	2.15	0	5.66	3.81
COM 80	0	0	0.1	0.1	3.61	0	0	1.46	0	0	0.2
COM 75	0	0	0.2	0.1	4.59	0	0	2.44	0.1	0	0.59
COM 50	0.1	0	4.2	0.59	11.62	0.29	0.59	6.74	0.98	0.49	1.76
GF 3x3	0	0	0	0	0	0.1	0	0.1	0	0	0
GF 9x9	0	0	0	0	0	0.1	0	0.1	0	0	0
MF	0.1	0.29	0.1	0.29	0.1	0.29	0.49	1.27	0.49	0	0.1
MDF 2x2	0.1	0.78	0.39	0.59	0	0.39	0	3.13	0.78	0.1	0.2
MDF 3x3	0	0.2	0.1	0	0.1	0.2	0	1.56	0	0.1	0.1
SF	0	0	0	0	0	0.1	0	0	0	0	0
WF	0	0.29	0.1	0.1	0.1	0.2	0	1.07	0	0	0.1
HE	0	0	0.49	2.15	0	0.2	0.2	1.66	0	0.1	0.88
RS 512-256-512	0.1	0.2	0.2	0	0.2	0.1	0	1.27	0.2	0	0.1
GC	0	0	0	0	0	0	0	0	0	0	0

Tablo 3.6'da "Lena" görüntüsünün NK değerleri, referans çalışmalar ile karşılaştırılmıştır. Atak yokken (NA) tüm çalışmalar NK'yi %100 olarak bulmuşlardır. Tuz & biber gürültüsü (SPN) için önerilen yöntem [97, 98]'le benzer sonuçlara sahipken, [99]'da önerilen yöntemden daha üstün bulunmuştur. Poisson gürültüsü (PN) için [97, 98] ve önerilen yöntemin NK değerleri aynı çıkmıştır. Çalışmanın performansının benek gürültüsü (SN) ve Gauss gürültüsüne (GN) karşı [97]'de verilen sonuçlara göre daha kötü, [98]'de önerilen yöntemden ise daha üstün olduğu görülmektedir. Merkezi kırpma atağında (CR-C) bu çalışmanın NK değeri [97-99]'a kıyasla daha yüksek bulunmuştur. JPEG sıkıştırmaya (COM) karşı [85, 97] ile benzer performans sergileyen yöntemin, [98, 99]'da verilen algoritmalardan daha dayanıklı olduğu gözlenmiştir. Filtreleme ataklarının tümünde (GF, MF, MDF, SF, WF), yeniden ölçekleme (RS) ve gama düzeltmede (GC) ADD-TDA-KUAABA tabanlı çalışma NK değerini %100 bulmuştur. Dolayısıyla diğer çalışmalardakinden daha yüksek veya onlara eşit performans sergilemektedir. Son olarak histogram eşitlemeye (HE) karşı önerilen çalışmanın NK değeri [97-99]'la yakın bulunmuştur. Damgalanmış ve bozulmuş "Lena" görüntüsünden çıkarılan damgalar Şekil 3.5'teki gibi verilmiştir.



Şekil 3.5. Damgalanmış ve bozulmuş "Lena" görüntüsünden çıkarılan damgalar: (a) NA (b) SPN d=0.01, (c) SPN d=0.02, (d) SPN d=0.03, (e) SPN d=0.05, (f) PN, (g) SN v=0.001, (h) SN v=0.005, (i) SN v=0.009, (j) GN v=0.001, (k) GN v=0.005, (l) GN v=0.009, (m) CR-T, (n) CR-C, (o) CR-B, (p) COM Q=80, (q) COM Q=75, (r) COM Q=50, (s) GF 3x3, (t) MF, (u) MDF 3x3, (v) SF, (w) WF (x) HE, (y) RS 512-256-512, (z) GC

Tablo 3.6. “Lena” görüntüsüne ait NK (%) değerlerinin karşılaştırılması

Atak	[85]	[97]	[98]	[99]	ADD – TDA – KUAABA
NA	**100**	**100**	**100**	**100**	**100**
SPN 0.01	--	**96.09**	93.17	88.30	94.50
SPN 0.02	--	87.76	**90.16**	--	89.14
SPN 0.03	--	**84.54**	83.74	--	83.51
PN	--	**100**	**100**	--	**100**
SN 0.001	--	**100**	99.55	--	**100**
SN 0.005	--	**99.75**	96.62	--	97.72
SN 0.009	--	**98.25**	89.82	--	89.68
GN 0.001	--	**100**	98.42	--	98.53
GN 0.005	--	**91.95**	81.99	--	84.45
GN 0.009	--	**80.97**	68.87	--	77.35
CR-T	--	**98.50**	94.33	--	94.91
CR-C	--	96.25	99.55	89.50	**100**
CR-B	--	98.25	99.09	--	**99.10**
COM 80	**100**	**100**	**100**	--	**100**
COM 75	**100**	**100**	99.77	97.52	**100**
COM 50	**100**	**100**	98.18	--	99.33
GF 3x3	98.60	**100**	**100**	--	**100**
GF 9x9	--	--	--	99.98	**100**
MF	--	97.27	99.32	--	**100**
MDF 3x3	98.20	90.13	99.09	97.25	**100**
SF	--	**100**	**100**	**100**	**100**
WF	--	**100**	**100**	--	**100**
HE	--	**100**	**100**	99.89	99.73
RS 512-256-512	--	**100**	**100**	99.90	**100**
GC	--	--	--	**100**	**100**

Standart test görüntülerine ek olarak, Pasadena-Houses-2000 veri setinin 30 görüntüsü de orijinal görüntü olarak kullanılmış ve performanslar ölçülmüştür. Bunun için öncelikle tüm ev görüntüleri 512×512 boyutlu gri tonlama moduna dönüştürülmüştür. Sadece damgalanmış görüntülerin TSGO değerleri değil, aynı zamanda saldırıya uğrayan her görüntüden çıkarılan damgaların gömülen damga ile arasındaki ortalama NK değerleri ve ortalama BHO değerleri de hesaplanmıştır. Tablo 3.7 söz konusu sonuçları içermektedir. Elde edilen bulgulara göre damgalanmış ev görüntüleri ile orijinal görüntüler arasındaki TSGO değerleri 40 dB’nin üzerindedir. Dolayısıyla algılanamazlık açısından [97, 98]’e kıyasla daha üstündür. Ayrıca, ortalama NK değerleri de her iki çalışmadakilerden daha yüksektir. BHO açısından karşılaştırıldığında, önerilen yöntemin [98]’den tamamen, [97]’den ise çoğu durumda daha başarılı olduğu görülmektedir.

Tablo 3.7.Ev görüntülerine ait TSGO, NK (%) ve BHO (%) değerlerinin karşılaştırılması

Orijinal Görüntü	TSGO (dB)			NK (%)			BHO (%)		
	[97]	[98]	ADD-TDA-KUA ABA	[97]	[98]	ADD-TDA-KUA ABA	[97]	[98]	ADD-TDA-KUA ABA
	38.2561	38.1872	**43.8782**	90.71	85.81	**94.53**	**4.7**	7.14	4.92
	39.3486	38.1323	**49.4043**	89.22	86.8	**91.11**	**5.37**	6.66	7.95
	38.1799	38.0094	**46.4247**	90.1	85.12	**92.44**	**4.96**	7.29	6.88
	37.2022	38.0651	**44.7083**	90.85	83.92	**92.99**	**4.7**	7.92	6.18
	33.9351	37.7955	**40.0783**	92.3	74.2	**96.85**	4.03	12.37	**2.96**
	35.9447	37.9878	**44.5368**	91.63	84.05	**93.82**	**4.29**	7.84	5.69
	37.9812	38.0788	**46.4974**	90.53	85.97	**93.37**	**4.89**	6.91	6.22
	37.1024	38.0823	**43.1923**	89.17	84.04	**94.04**	5.45	7.73	**5.39**
	34.4320	38.1023	**42.6572**	90.95	85.91	**95.1**	4.71	7.07	**4.34**
	36.9445	38.1412	**40.2821**	91.36	83.21	**96.04**	4.55	8.33	**3.5**
	32.9763	37.9499	**40.0733**	92.39	81.63	**95.27**	**4.06**	8.96	4.3
	33.1625	38.1617	**41.6755**	92.46	84.5	**96.62**	3.93	7.74	**3.13**
	33.9325	37.9947	**40.0015**	91.82	81.57	**96.91**	4.28	9.26	**2.77**
	37.2329	38.0846	**40.5406**	91.17	78.77	**96.72**	4.49	10	**3.11**
	37.2124	38.3340	**40.6509**	91.12	82.57	**97.21**	4.68	8.38	**2.65**

Tablo 3.7'nin devamı

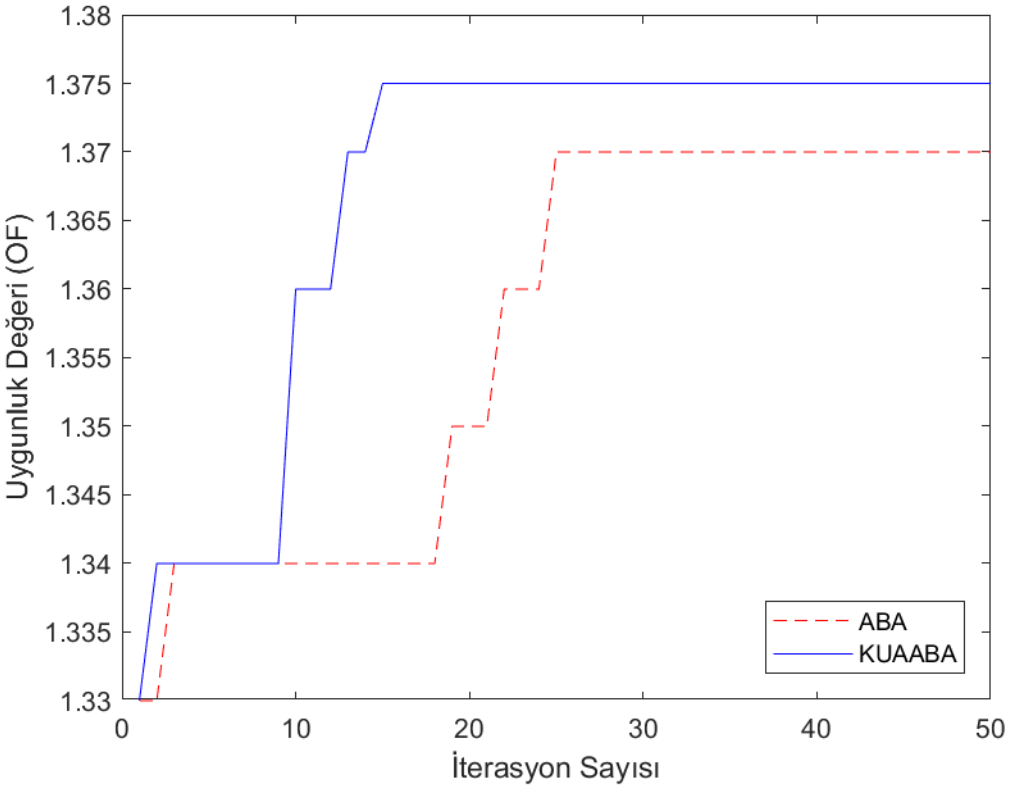
Orijinal Görüntü	TSGO (dB)			NK (%)			BHO (%)		
	[97]	[98]	ADD-TDA-KUA ABA	[97]	[98]	ADD-TDA-KUA ABA	[97]	[98]	ADD-TDA-KUA ABA
	35.1527	38.1204	**41.0026**	92.03	75.2	**96.98**	4.02	11.36	**2.99**
	35.6091	38.2407	**40.6039**	91.11	82.18	**97.57**	4.61	8.53	**2.45**
	33.8661	38.2792	**41.3683**	92.05	75.95	**96.26**	4.01	10.95	**3.52**
	32.8616	38.0968	**41.2550**	92.24	78.55	**95.38**	**3.81**	10.19	4.14
	37.4727	38.1008	**41.9300**	90.29	86.12	**96.64**	4.96	6.95	**3.22**
	35.6887	38.2225	**40.9958**	91.81	81.67	**96.31**	4.25	8.71	**3.41**
	36.5983	38.1525	**40.3198**	91.26	81.09	**96.56**	4.65	8.92	**3.13**
	36.6024	38.0825	**41.7738**	90.8	79.28	**95.36**	4.83	9.83	**4.21**
	34.0981	38.3493	**40.9779**	92.14	75.56	**96.92**	3.6	11.27	**3.03**
	33.2033	38.1281	**41.1654**	92.75	84.21	**96.96**	3.85	7.69	**2.9**
	29.3282	37.9210	**40.7469**	93.03	77.62	**96.3**	3.64	10.8	**3.37**
	35.7498	38.1293	**42.0664**	91.7	84.25	**96.1**	4.14	7.74	**3.75**
	36.5906	38.0960	**42.4703**	90.84	83.65	**94.95**	**4.54**	7.94	4.77
	37.2811	38.0930	**42.8490**	90.21	84.91	**96.56**	4.97	7.4	**3.31**
	36.6035	38.3473	**42.0160**	90.83	75.99	**95.14**	4.65	11.22	**4.51**
Ortalama	35.6850	38.1155	**42.2047**	91.30	81.81	**95.57**	4.45	8.77	**4.09**

3.1.1.3. ADD-TDA-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntemin Sonuçları

ADD-TDA-KUAABA tabanlı yöntem hem standart on bir test görüntüsü üzerinde hem de ev görüntüleri üzerinde algılanamazlık ve dayanıklılık açısından test edilmiştir. On bir görüntü için ortalama TSGO değeri 42.7795 dB bulunmuştur. Bu görüntülerden elde edilen ortalama NK ve BHO değerleri incelendiğinde atak olmadığı durumda (NA) ve benek gürültüsü (SN), kırpma (CR), JPEG sıkıştırma (COM), filtreleme (GF, MF, MDF, SF, WF), yeniden ölçekleme (RS), gama düzeltme (GC) ataklarına karşı yöntemin dayanıklılığı çok yüksek bulunmuştur. Gauss gürültüsü (GN) ve tuz & biber gürültüsüne (SPN) karşı ise nispeten daha düşük performans göstermiştir. Tüm ataklar için ortalama NK %95.83, BHO ise %3.91 olarak hesaplanmıştır. Pasadena-Houses-2000 veri setinden alınan 30 görüntü için önerilen çalışma 42.2047 dB ortalama TSGO, %95.57 ortalama NK ve %4.09 ortalama BHO değerlerine sahiptir.

Çalışmanın performansı hem standart test görüntüleri için hem ev görüntüleri için referans çalışmalarla kıyaslandığında hem TSGO değeri [97, 98]'den daha yüksek bulunmuştur, hem de ataklar karşısındaki dayanıklılığı bu çalışmalardan kötü değildir. [85]'le karşılaştırıldığında ise önerilen yöntemin TSGO değeri biraz daha düşük olsa da test edilen filtreleme ataklarında daha üstün performans sergilemiştir. [99]'da yazarlar 50 dB üzerinde TSGO hesaplamışlardır. Ancak bu yöntem dayanıklılık açısından gürültü atakları gibi bozulmanın daha fazla olduğu durumları değerlendirmemiştir. Test ettiği ataklar karşısında da önerilen çalışma bu yöntemin önüne geçmiştir.

Şekil 3.6'da, ADD-TDA alanındaki standart ABA'nın ve KUAABA'nın yakınsama performansları verilmiştir. KUAABA, her bir ateş böceğinin adımlarını geçmiş bilgilerine ve mevcut durumuna göre güncellediğinden, algoritmanın yakınsaması üzerinde etkilidir. Şekle göre, KUAABA'nın yakınsama hızı ABA'dan daha yüksek bulunmuştur. Ayrıca KUAABA tabanlı yöntem, hemen hemen tüm yinelemelerde ABA tabanlı yöntemi geride bırakmaktadır.



Şekil 3.6. ABA ve KUAABA'nın performansının karşılaştırılması

3.2. Biyometrik Damgalamaya Yönelik Çalışmanın Değerlendirilmesi

Araştırma bulgularının ikinci kısmında renkli görüntülerde iris biyometrisini kullanan damgalama şemasının deneysel sonuçları detaylandırılmıştır.

3.2.1. Renkli Görüntülerde YDDADD-QR Ayrıştırma-Kendinden Uyarlanabilir Adımlı ABA Tabanlı Yöntemin Değerlendirilmesi

Bu bölümde, YDDADD-QR Ayrıştırma alanında damgayı renkli görüntülere gömen, KUAABA ile optimize edilmiş sistemin bulguları irdelenmiştir. Deneyler sırasında, Bath Üniversitesi veri tabanından toplanan göz görüntülerinden elde edilen ve 8×200 bitten oluşan ikili iris kodu 512×512 boyutlu renkli görüntüye gizlenmiştir. Yöntemin performansı, algılanamazlık, dayanıklılık ve kimlik doğrulama açısından değerlendirilmiştir.

3.2.1.1. Önerilen Biyometrik Damgalama Yönteminin Algılanamazlık Performansı

Renkli görüntüler üzerinde gerçekleştirilen YDDADD-QR-KUAABA tabanlı damgalama algoritmasının damga çıkarma süreci kördür. Kör olmayan damgalama sistemleri damganın algılanma sürecinde orijinal görüntüye ihtiyaç duyduğundan kör sistemlere kıyasla daha dayanıklıdır. Kör damgalamaya dayalı bir yöntemde ise yüksek dayanıklılık elde etmek için algılanamazlıktan bir miktar ödün verilmesi kaçınılmazdır. Önerilen damgalama algoritması kör olmasına rağmen, görsel niteliği oldukça iyidir. 512×512 boyutlu orijinal görüntüye 1600 bitten oluşan iris kodu gömüldüğünde elde edilen TSGO değeri 40.5822 dB olarak bulunmuştur.

Tablo 3.8. Önerilen yöntemin referans çalışmalarla algılanamazlık açısından kıyaslanması

	[97]	[98]	[133]	[134]	YDDADD-QR-KUAABA
Damga Çıkarma Modu	Kör	Kör	Kör	Kör	Kör
Damga Tipi	İkili	İkili	İkili	İkili	Biyometrik
Damga Boyutu	1024 bit ($\mathbf{32 \times 32}$)	1024 bit ($\mathbf{32 \times 32}$)	1024 bit ($\mathbf{32 \times 32}$)	1024 bit ($\mathbf{32 \times 32}$)	**1600 bit**
Damganın Gömüldüğü Ortam	Gri seviye görüntü	Gri seviye görüntü	Gri seviye görüntü	Gri seviye görüntü	YCbCr uzayı (Y kanalı)
Orijinal Görüntü Boyutu	$\mathbf{512 \times 512}$	$\mathbf{512 \times 512}$	$\mathbf{512 \times 512}$	$\mathbf{512 \times 512}$	$\mathbf{512 \times 512}$
TSGO (dB)	37.9815	38.8895	40.07	40.22	**40.5822**

Yöntemin algılanamazlık performansı dayanıklı ve kör görüntü damgalama yöntemleriyle ([97, 98, 133, 134]) kıyaslanmıştır. [97] ve [98]'de yazarlar gri seviye görüntülerde KDD'ye dayalı damgalama şeması sunmuşlardır. [133]'te ADD alanında AKD ve TDA'nın kombinasyonuna bağlı bir algoritma önerilmiştir. [134]'te ise Durağan Dalgacık Dönüşümü ve Hızlandırılmış Dayanıklı Öznitelik yaklaşımının bir arada kullanıldığı damgalama yöntemi geliştirilmiştir. Tablo 3.8, biyometrik damgalama yönteminin damgalanmış görüntü ve orijinal görüntü arasında hesaplanan TSGO değeri, damga boyutu, orijinal görüntü boyutu gibi açılardan yukarıda bahsi geçen literatür çalışmalarıyla

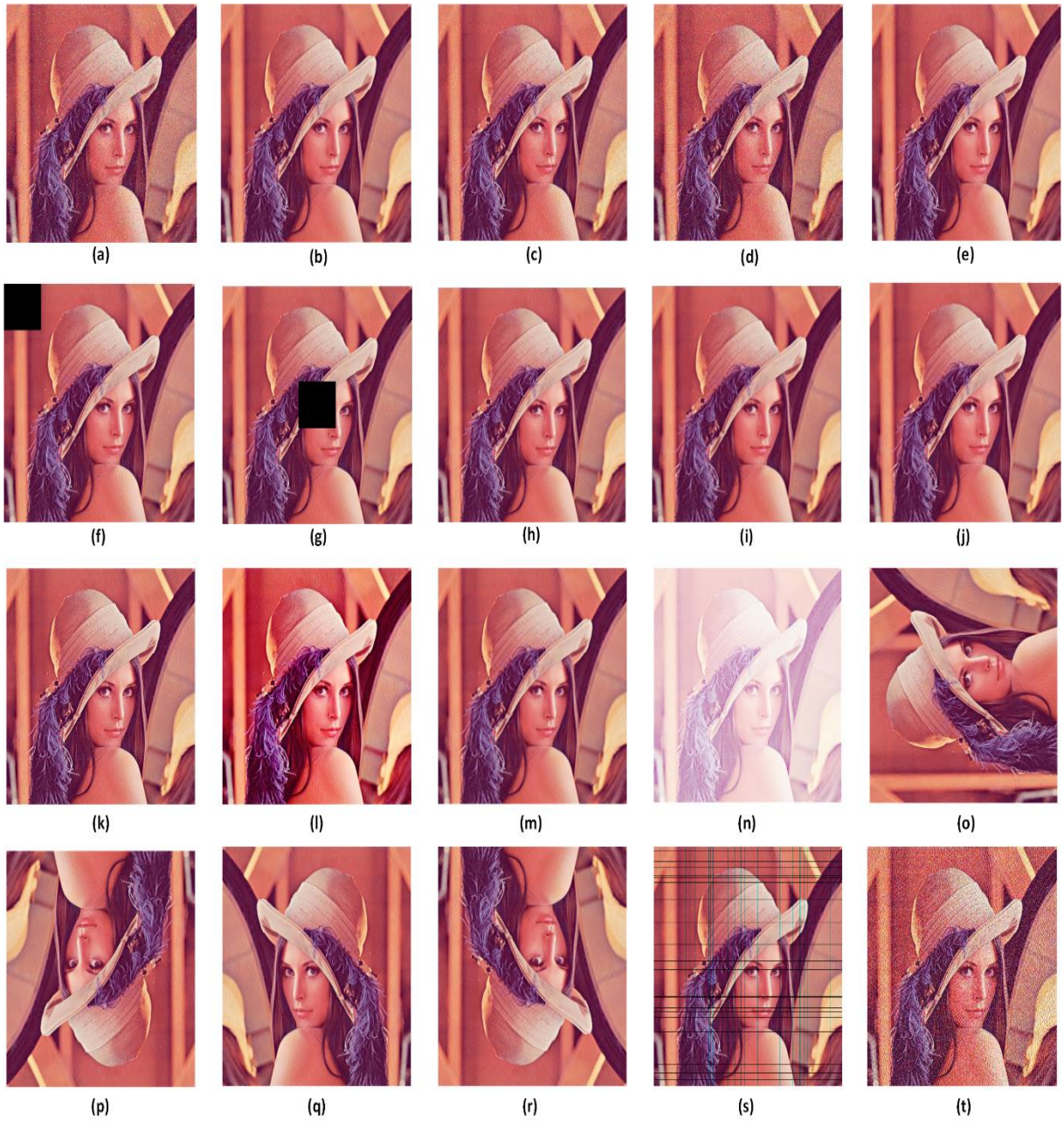
kıyaslamasını içerir. Tabloya göre [97], [98], [133] ve [134]'te sunulan gri seviye görüntü damgalama yöntemlerinin sırasıyla 37.9815 dB, 38.8895 dB, 40.07 dB ve 40.22 dB TSGO değerlerine sahip olduğu gözlenmektedir. Bu verilere göre TSGO değerleri karşılaştırıldığında, söz konusu sistemde damga boyutu daha fazla olmasına rağmen algılanamazlık performansının referans çalışmalardakinden daha iyi olduğu anlaşılmaktadır.

3.2.1.2. Önerilen Biyometrik Damgalama Yönteminin Dayanıklılık Performansı

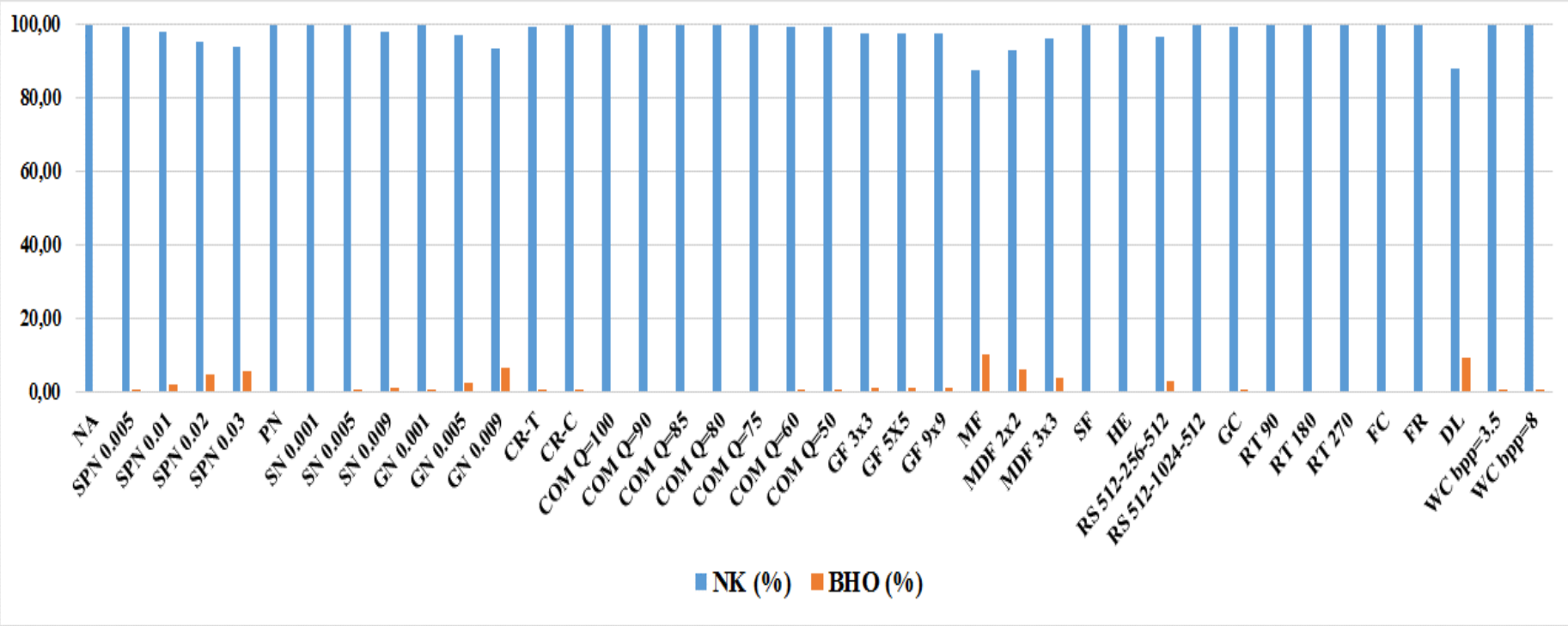
Bu bölümde, önerilen yöntemin geometrik saldırılara ve yaygın sinyal işleme saldırılarına karşı dayanıklılığı tartışılmıştır. Dayanıklılık NK ve BHO üzerinden değerlendirilmiştir. Şekil 3.7'de damgalanmış ve atak uygulanmış renkli "Lena" görüntüleri verilmiştir. Şekil 3.8 ise ataklar karşısında önerilen yöntem tarafından elde edilen NK (%) ve BHO (%) değerlerini göstermektedir. Şekil incelendiğinde yöntemin NK değerlerinin oldukça yüksek ve bu değerlerle tutarlı olarak hata oranının oldukça düşük olduğu gözlenmektedir. Performansın diğerlerine kıyasla daha az olduğu iki durumun ortalama filtre atağına (MF) ve rasgele satır ve sütun silme atağına karşı olduğu görülmektedir. Ancak söz konusu ataklarda dahi yüzde doksana yakın bir başarı elde edilmiştir.

Sunulan yöntemlerde dayanıklılığı değerlendirmek için kullanılan saldırılar, [97, 98, 133, 134]'te verilen geleneksel damgalama şemalarındakilere benzerdir. Bu nedenle YDDADD-QR-KUAABA tabanlı sistemin dayanıklılık performansı bu çalışmalarla karşılaştırılmıştır. NK ve BHO değerlerinin kıyaslaması sırasıyla Tablo 3.9 ve 3.10'da verilmiştir. Aşağıda farklı atak grupları için çalışmanın performansı ayrı ayrı değerlendirilmiştir.

Atak yok: Tablo 3.9 ve 3.10'a göre, damgalanmış görüntü herhangi bir saldırıya maruz kalmadığında (NA), bu tezde sunulan yöntem gömülü iris kodunu hatasız çıkarır. Önerilen çalışmanın NK değeri %100 iken, BHO değeri %0 olarak bulunmuştur. Benzer şekilde, [97, 98, 133, 134]'te verilen yöntemler de NK'yi %100 ve BHO'yu %0 olarak bulmuştur.



Şekil 3.7. Damgalanmış ve atak uygulanmış renkli “Lena” görüntüleri: (a) SPN d=0.03, (b) PN, (c) SN v=0.009, (d) GN v=0.009, (e) COM Q=50, (f) CR-TL, (g) CR-C, (h) GF 9x9, (i) MF, (j) MDF 3x3, (k) SF, (l) HE, (m) RS 512-256-512, (n) GC, (o) RT 90, (p) RT 180, (q) FC, (r) FR, (s) DL, (t) WC bpp=8



Şekil 3.8. Ataklar karşısında önerilen yöntemin NK/BHO grafiği

Tablo 3.9. YDDADD-QR-KUAABA tabanlı yöntemin NK (%) değerlerinin mevcut literatür çalışmalarındakilerle karşılaştırılması

Ataklar	[97]	[98]	[133]	[134]	YDDADD-QR-KUAABA	Ataklar	[97]	[98]	[133]	[134]	YDDADD-QR-KUAABA
NA	**100**	**100**	**100**	**100**	**100**	CR-C	96.25	99.55	--	99.3	**100**
SPN 0.005	--	--	--	--	**99.51**	GF 3x3	**100**	**100**	--	**100**	97.40
SPN 0.01	96.09	93.17	88.17	**100**	98.15	GF 5x5	**100**	**100**	--	--	97.40
SPN 0.02	87.76	90.16	83.86	**98.2**	95.43	GF 9x9	--	--	--	--	97.40
SPN 0.03	84.54	83.74	--	89.4	**94.19**	MF	97.27	**99.32**	96.41	28.3	87.76
PN	**100**	**100**	--	**100**	**100**	MDF 2x2	--	--	--	--	**92.95**
SN 0.001	**100**	99.55	--	**100**	**100**	MDF 3x3	90.13	99.09	**99.67**	--	96.42
SN 0.005	99.75	96.62	--	99.8	**99.88**	SF	**100**	**100**	99.93	**100**	**100**
SN 0.009	98.25	89.82	--	96.1	**98.27**	HE	**100**	**100**	99.53	**100**	**100**
GN 0.001	**100**	98.42	--	99.1	99.75	RS 512-256-512	**100**	**100**	99.87	--	96.66
GN 0.005	91.95	81.99	84.70	85.2	**97.28**	RS 512-1024-512	**100**	**100**	**100**	--	**100**
GN 0.009	80.97	68.87	--	72.4	**93.70**	GC	--	--	--	--	**99.38**
COM Q=100	--	--	--	--	**100**	RT 90	10.84	11.87	--	**100**	**100**
COM Q=90	--	--	--	96.8	**100**	RT 180	10.15	12.00	--	**100**	**100**
COM Q=85	--	--	--	82.1	**100**	RT 270	--	--	--	98.9	**100**
COM Q=80	**100**	**100**	--	--	**100**	FC	--	--	--	--	**100**
COM Q=75	**100**	99.77	--	--	**100**	FR	--	--	--	--	**100**
COM Q=60	--	--	--	--	**99.51**	DL	--	--	--	--	**88.13**
COM Q=50	**100**	98.18	94.49	--	99.51	WC bpp=3.5	--	--	--	--	**100**
CR-T	98.50	94.33	--	**100**	99.51	WC bpp=8	--	--	--	--	**100**

Tablo 3.10. YDDADD-QR-KUAABA tabanlı yöntemin BHO (%) değerlerinin mevcut literatür çalışmalarındakilerle karşılaştırılması

Ataklar	[97]	[98]	[133]	[134]	YDDADD-QR-KUAABA	Ataklar	[97]	[98]	[133]	[134]	YDDADD-QR-KUAABA
NA	**0**	**0**	**0**	**0**	**0**	CR-C	1.46	**0.2**	--	0.3	0.75
SPN 0.005	--	--	--	--	**0.63**	GF 3x3	**0**	**0**	--	**0**	1.31
SPN 0.01	1.56	2.93	16.50	**0**	1.88	GF 5x5	**0**	**0**	--	--	1.31
SPN 0.02	4.98	4.3	22.17	**0.8**	4.81	GF 9x9	--	--	--	--	1.31
SPN 0.03	6.35	7.23	--	**4.6**	5.88	MF	1.07	**0.29**	5.18	39.9	10.00
PN	**0**	**0**	--	**0**	**0**	MDF 2x2	--	--	--	--	5.94
SN 0.001	**0**	0.2	--	**0**	**0**	MDF 3x3	3.91	**0.39**	0.49	--	3.63
SN 0.005	**0.1**	1.46	--	**0.1**	0.13	SF	**0**	**0**	0.10	**0**	**0**
SN 0.009	**0.68**	4.39	--	1.7	1.25	HE	**0**	**0**	0.68	**0**	**0**
GN 0.001	**0**	0.68	--	0.4	0.13	RS 512-256-512	**0**	**0**	0.20	--	3.06
GN 0.005	3.22	8.11	21.00	6.4	**2.56**	RS 512-1024-512	**0**	**0**	**0**	--	**0**
GN 0.009	7.91	14.55	--	12.2	**6.50**	GC	--	--	--	--	**0.56**
COM Q=100	--	--	--	--	**0**	RT 90	52.05	47.85	--	**0**	**0**
COM Q=90	--	--	--	1.4	**0**	RT 180	51.56	50	--	**0**	**0**
COM Q=85	--	--	--	7.5	**0**	RT 270	--	--	--	0.5	**0**
COM Q=80	**0**	**0**	--	--	**0**	FC	--	--	--	--	**0**
COM Q=75	**0**	0.1	--	--	**0**	FR	--	--	--	--	**0**
COM Q=60	--	--	--	--	**0.44**	DL	--	--	--	--	**9.19**
COM Q=50	**0**	0.78	7.91	--	0.50	WC bpp=3.5	--	--	--	--	**0.06**
CR-T	0.59	2.44	--	**0**	0.31	WC bpp=8	--	--	--	--	**0.13**

Gürültü atakları: Damgalanmış görüntüye farklı gürültüler uygulandığında, YDDADD-QR-KUAABA tabanlı yöntemin oldukça başarılı olduğu gözlenmiştir. Test edilen gürültü ataklarında ortalama NK %97.83 olarak bulunmuşken, BHO değerlerinin ortalamasının ise %2.16 olduğu tespit edilmiştir. [97, 98, 133] tarafından önerilen sistemlerle karşılaştırıldığında, çalışmanın performansının daha yüksek olduğu görülmektedir. Önerilen sistem özellikle tuz & biber gürültüsüne (SPN) ve Gauss gürültüsüne (GN) karşı bu çalışmalardan daha dayanıklıdır. Örneğin, [97]'deki yazarlar NK'yi GN 0.009 için %80.97 olarak bulurken, [98]'de önerilen yöntemde bu değer %68.87'dir. Oysa bu çalışmada GN 0.009 atağına karşı NK %93.70 olarak hesaplanmıştır. Yine [133]'te GN 0.005 için NK ve BHO sırasıyla %84.70 ve %21.00 olarak bulunmuştur. Aynı saldırı için önerilen yöntemde NK'nın %97.28, BHO'nun ise %2.56 olduğu görülmektedir. Tuz & biber gürültüsüne karşı farklı yoğunluk değerlerinde bu çalışma %94'ün üstünde NK değeri elde etmiştir. $d = 0.01$ yoğunluktaki tuz & biber gürültüsü (SPN 0.01) için önerilen yöntemde ve [97, 98, 133]'te verilen NK sonuçları sırasıyla %98.15, %96.09, %93.17 ve %88.17 bulunmuştur. Dolayısıyla bu atak için özellikle [133]'e kıyasla yöntemin çok daha üstün olduğu görülmektedir. YDDADD-QR-KUAABA tabanlı çalışmanın dayanıklılığı [134]'te önerilen damgalama algoritmasınınkiyle kıyaslandığında, $d = 0.01$ ve $d = 0.02$ yoğunluklu tuz & biber gürültüsü için referans çalışma biraz daha yüksek NK değerine sahiptir. Ancak $d = 0.03$ olduğunda bu tezde sunulan yöntemden elde edilen NK %94.19 iken, [134]'teki yazarlar bu değeri %89.4 olarak bulmuşlardır. Her iki çalışma Gauss gürültüsüne karşı karşılaştırıldığında önerilen yöntemin daha üstün olduğu görülmektedir. Örneğin varyans 0.009 olduğunda (GN 0.009) [134]'te ele alınan çalışmanın NK (%72.4) ve BHO (%12.2) değerinin bu çalışmadan daha kötü olduğu gözlenmektedir. Poisson gürültüsüne (PN) karşı tüm yöntemler aynı performansa sahiptir. Benek gürültüsü (SN) için ise çalışma [97] ve [134] ile yakın sonuçlar bulurken, [98]'den oldukça iyi performans sergilemiştir. SN 0.009 için önerilen yönteme, [97], [98] ve [134]'e ait NK değerleri sırasıyla %98.27, %98.25, %89.82 ve %96.1 olarak bulunmuştur. Tüm gürültü saldırıları dikkate alındığında YDDADD-QR-KUAABA tabanlı çalışmanın NK değerleri %90'ın üzerinde, BHO ise %6.50'nin altında çıkmıştır.

JPEG sıkıştırma: Önerilen şemada, damgalanmış görüntülere farklı kalite faktörlerine (Q) sahip JPEG sıkıştırma (COM) saldırıları uygulanmaktadır. Q 100, 90, 85, 80 ve 75 olduğunda NK %100 ve BHO %0'dır. Test edilen tüm kalite faktörleri için ise ortalama NK ve ortalama BHO sırasıyla %99. 86 ve %0.13 olarak bulunmuştur. Tablo 3.9 ve 3.10'a göre, [97] tarafından önerilen çalışmanın YDDADD-QR-KUAABA tabanlı yönteme göre biraz daha iyi sağlamlığa sahip olduğu görülmektedir. [97]'deki yazarlar, 50 kalite faktörü ile JPEG sıkıştırma için NK'yi

%100 olarak gösterirken, bu değer YDDADD-QR-KUAABA'ya dayalı algoritma tarafından %99.51 olarak hesaplanmıştır. [98], [133] ve [134] ile kıyaslandığında ise bu çalışmanın JPEG sıkıştırma atağına karşı hem NK hem BHO değerlerinin daha üstün olduğu gözlenmiştir. Örneğin Q=50 iken, [98] ve [133]'te yazarlar NK'yi sırasıyla %98.18 ve %94.49, BHO'yu ise %0.78 ve %7.91 olarak bulmuşlardır. Oysa önerilen yöntemde bu değerler %99.51 ve %0.50 olarak ölçülmüştür. Yine Q=90 ve Q=85 olduğunda bu çalışma gömülen damgayı hatasız çıkarırken, [134]'teki yazarlar NK'nin %96.8 (Q=90) ve %82.1 (Q=85) ve BHO'nun %1.4 (Q=90) ve %7.5 (Q=85) olduğunu göstermişlerdir.

Kırpma: Önerilen yöntemde damganın gömüleceği yerler blokların standart sapma değerlerine bağlı olarak seçildiğinden, kırpma saldırılarına karşı oldukça dirençlidir. Damgalanmış görüntünün sol üstünden 100×100 boyutunda bir kare kırpıldığında (CR-T), YDDADD-QR-KUAABA tabanlı yöntemin NK ve BHO değerleri sırasıyla %99.51 ve %0.31 olarak bulunmuştur. Damgalanmış görüntünün ortasından aynı boyuttaki bir kare kırpılırsa (CR-C), sistem %0.75'lik BHO ile iris kodunu çıkarır. Yöntemin kırpma saldırılarına karşı [97, 98] tarafından önerilen yöntemlerden üstün olduğu Tablo 3.9 ve 3.10'dan görülebilir. Örneğin CR-T için NK değeri [97]'deki yazarlar tarafından %98.50, [98]'dekiler tarafından ise %94.33 olarak hesaplanmıştır. [134] ile kıyaslandığında ise NK ve BHO sonuçları oldukça yakın bulunmuştur.

Filtreleme: Gauss filtresi (GF), ortalama filtresi (MF), ortanca filtresi (MDF) ve keskinleştirme filtresine (SF) karşı çalışmanın dayanıklılığı test edildiğinde, ortalama NK ve BHO değerleri %95.62 ve %3.36 olarak bulunmuştur. Yöntem ortalama filtresi dışında diğer filtreleme ataklarına karşı %90'ın üzerinde NK değerine sahiptir. [97, 98, 134]'te ele alınan yöntemler Gauss filtresine karşı önerilen şemadan daha üstün performansa sahiptir. Ortanca filtresi için ise önerilen yöntem [97]'yi NK ve BHO açısından geride bıraksa da, [98] ve [133]'te sunulan sistemlerden daha dayanıklı değildir. Ortalama filtresi söz konusu olduğunda önerilen yöntem NK ve BHO değerlerini sırasıyla %87.76 ve %10.00 olarak hesaplamıştır. Bu sonuçların [97], [98] ve [133]'te yer alan verilerden biraz daha kötü olduğu görülmektedir. Ancak çalışma [134] ile karşılaştırıldığında daha üstün bulunmuştur. Nitekim [134]'te NK ve BHO değerleri sırasıyla %28.3 ve %39.9 olarak ölçülmüştür. Keskinleştirme filtresinde YDDADD-QR-KUAABA tabanlı çalışma ve [97, 98, 134]'te verilen çalışmalar damgalanmış görüntüden damgayı hatasız çıkarabilmiştir. Ancak [133]'te önerilen yöntem bunların bir miktar gerisinde kalmıştır.

Histogram eşitleme: Bu atağa (HE) karşı önerilen yöntem gömülü iris kodunu hatasız bir şekilde kurtarır. NK ve BHO değerleri sırasıyla %100 ve %0 olarak bulunmuştur. [97, 98, 134]'te sunulan yöntemler de aynı performansa sahiptir. [133]'te ise yazarlar NK'yi %99.53, BHO'yu ise %0.98 olarak hesaplamışlardır.

Yeniden ölçekleme: 512-1024-512 yeniden ölçeklemede (RS), YDDADD-QR-KUAABA tabanlı yöntem için NK %100 iken BHO %0'dır. 512-256-512 yeniden ölçeklemede ise, NK ve BHO değerleri sırasıyla %96.66 ve %3.06 olarak bulunmuştur. [97, 98, 133]'teki yazarlar, 512-1024-512 yeniden ölçekleme saldırısına karşı bu çalışmayla aynı sonuçlar bulmuş olsalar da, 512-256-512 yeniden ölçeklemede nispeten daha başarılılardır. [97] ve [98]'de önerilen çalışmalar NK ve BHO'yu sırasıyla %100 ve %0 olarak hesaplarken, [133]'teki yazarlar bu değerlerin %99.87 ve %0.20 olduğunu rapor etmişlerdir.

Gama düzeltme: Gama düzeltme (GC) atağı için, yöntem NK değerini %99.38, BHO değerini ise %0.56 olarak bulmuştur. Bu verilere göre söz konusu atağa karşı dayanıklılığın çok yüksek olduğunu ifade etmek gerekir.

Dönme ve görüntü çevirme: YDDADD'nin yapısı gereği önerilen sistem 90°, 180°, 270° rotasyon (RT) ve yatay ve dikey çevirmeye (FC ve FR) karşı değişmez bir alan sunmaktadır. Bu sebeple söz konusu saldırılara karşı NK değerleri %100 ve BHO değerleri %0'dır. Ancak [97, 98]'de 90° rotasyona karşı NK sırasıyla %10.84 ve %11.87, BHO ise %52.05 ve %47.85 olarak bulunmuştur. Dolayısıyla [97] ve [98]'de önerilen çalışmaların bu atağa karşı dirençsiz olduğu söylenebilir. [134]'te yazarlar 90° ve 180° rotasyona karşı önerilen yöntemle aynı performansa sahipken, 270°'lik dönme söz konusu olduğunda bu çalışmadan biraz daha dayanıksız bulunmuştur. [133]'te ise rotasyona karşı herhangi bir bulguya yer verilmemiştir. Ayrıca, dört referans çalışma da görüntü çevirmeye karşı dayanıklılığı test etmemişlerdir.

Rasgele satır ve sütun silme: Araştırılan diğer saldırıların aksine, damgalanmış görüntüden rasgele yirmi satır ve yirmi sütun silindiğinde (DL) yöntemin başarısı nispeten zayıf görünmektedir. Bu atak için NK %88.13, BHO ise %9.19 olarak bulunmuştur. Geleneksel damgalamaya dayanan referans çalışmalar, bu saldırıya karşı performanslarını rapor etmediğinden karşılaştırma yapılamamıştır.

Dalgacık sıkıştırma: bpp 3.5 ve 8 için çalışmanın dalgacık sıkıştırma (WC) atağına karşı oldukça dirençli olduğu tespit edilmiştir. Her iki durumda da NK değeri %100, BHO değeri ise yaklaşık %0'dır.

Özetle, önerilen sistemin farklı saldırılar karşısında oldukça başarılı bir performans sergilediği gözlenmektedir. Tüm ataklara karşı ortalama NK ve ortalama BHO değerleri

hesaplandığında, sırasıyla %98.20 ve %1.56 olarak bulunmuştur. Bu veriler, yöntemin yüksek düzeyde dayanıklılığa sahip olduğunun kanıtıdır. Önerilen çalışma referans çalışmalardan daha yüksek veri yükleme kapasitesine sahip olduğu halde gürültü atakları (SPN, SN, GN, PN), kırpma (CR) ve özellikle rotasyona (RT) karşı [97], [98] ve [133]'teki çalışmalardan, gürültü atakları, JPEG sıkıştırma (COM) ve ortalama filtresine (MF) karşı [134]'teki çalışmadan daha üstündür. JPEG sıkıştırma açısından [97]'de ele alınan yaklaşım nispeten daha dayanıklı olsa da, önerilen yöntem bu atağa karşı [98, 133]'te sunulan çalışmalardan daha iyi performansa sahiptir. Kırpma söz konusu olduğunda YDDADD-QR-KUAABA tabanlı çalışmanın dayanıklılığı [134]'tekine benzer bulunmuştur. Keskinleştirme filtresi (SF), histogram eşitleme (HE) ve yeniden ölçekleme (RS) atakları açısından sonuçların çok yakın olduğu görülmüştür. [97]'de tanıtılan yöntem Gauss filtresi (GF) ve ortalama filtresine (MF) göre, [98]'deki Gauss filtresi, ortalama filtresi ve ortanca filtresine (MDF) göre, [133]'teki ortalama filtresi ve ortanca filtresine göre, [134]'teki ise Gauss filtresine göre önerilen çalışmadan daha iyi performansa sahiptir. Geleneksel damgalama şemalarından farklı olarak bu çalışmanın yatay çevirme (FC), dikey çevirme (FR), rastgele satır ve sütunların silinmesi (DL) ve dalgacık sıkıştırmaya (WC) karşı dayanıklılığı da araştırılmış ve sonuçlar oldukça başarılı bulunmuştur.

İris biyometrisinin damga olarak kullanıldığı bu çalışma ile Bölüm 2.1'de verilen ADD-TDA-KUAABA tabanlı geleneksel damgalama şemasının performansı kıyaslanacak olursa 32×32 boyutunda (1024 bit) ikili damgayı orijinal görüntüye gömen ADD-TDA-KUAABA tabanlı yöntemin ortalama TSGO değeri 42.7795 dB olarak bulunmuştur. YDDADD-QR-KUAABA tabanlı çalışmadaki veri ekleme kapasitesi daha yüksek olduğundan (1600 bit) algılanamazlık performansının bir miktar düşük olması kaçınılmazdır. Buna karşılık dayanıklılık test edildiğinde YDDADD-QR-KUAABA tabanlı yöntemin daha başarılı olduğu söylenebilir. Tablo 3.11'de on bir test görüntüsü için geleneksel damgalama şemasının ortalama dayanıklılık sonuçları söz konusu biyometrik damgalama şemasınınkilerle birlikte ele alınmıştır. Buna göre YDDADD-QR-KUAABA tabanlı yöntem gürültü ataklarına karşı ADD-TDA-KUAABA tabanlı yöntemden daha üstün bulunmuştur. Şöyle ki damgalanmış görüntüye $d = 0.03$ yoğunluğa sahip tuz & biber gürültüsü (SPN 0.03) uygulandığında NK ve BHO değerleri ADD-TDA-KUAABA tabanlı çalışma tarafından %83.50 ve %15.47, YDDADD-QR-KUAABA tabanlı çalışma tarafından ise %94.19 ve %5.88 olarak tespit edilmiştir. Benzer şekilde benek gürültüsü (SN 0.009) için YDDADD-QR-KUAABA tabanlı biyometrik damgalama tekniği gömülen damgayı %1.25 hata oranı ile çıkarmışken, ADD-TDA-KUAABA tabanlı yöntemde bu oranın %4.82 olduğu gözlenmektedir. Gauss gürültüsü (GN 0.005 ve GN

0.009) için de YDDADD-QR-KUAABA tabanlı çalışmanın dayanıklılığı %10'dan daha fazla iyileştirdiği Tablo 3.11'den görülmektedir.

JPEG sıkıştırma (COM) atağına karşı yöntemler ele alındığında da önerilen biyometrik tabanlı yöntemin performansı daha üstün bulunmuştur. Örneğin, Q 50 kalite faktörüne sahip JPEG sıkıştırmaya karşı ADD-TDA-KUAABA tabanlı yöntem NK ve BHO değerlerini sırasıyla %97.49 ve %2.49 olarak hesaplamıştır. Oysaki bu değerlerin YDDADD-QR-KUAABA tabanlı yöntem için %99.51 ve %0.50 olduğu tablodan görülmektedir.

Kırpma ataklarına (CR-T ve CR-C) karşı YDDADD-QR-KUAABA tabanlı yöntem geleneksel damgalama çalışmasını geride bırakmıştır. ADD-TDA-KUAABA'ya dayalı damgalama şeması söz konusu ataklar için NK değerini yaklaşık %96, BHO değerini ise yaklaşık %2 olarak bulmuşken, YDDADD-QR-KUAABA'ya dayalı şema gömülen damgayı yaklaşık %0 hata ile çıkarabilmiştir.

Filtreleme atakları uygulandığında biyometrik damgalama şemasının dayanıklılığının biraz daha düşük olduğu gözlenmektedir. Gauss filtresi (GF), ortanca filtre (MDF), keskinleştirme filtresi (SF) söz konusu olduğunda ADD-TDA-KUAABA tabanlı çalışma damgalanmış görüntüden ikili damgayı neredeyse hatasız olarak elde edebilmektedir. Ortalama filtre (MF) uygulandığında ise çalışmanın performansı diğer filtreleme ataklarına kıyasla biraz daha düşük bulunmuştur. Söz konusu atak için çıkarılan ve gömülen damga arasındaki NK ve BHO değerleri sırasıyla %96.67 ve %0.32 bulunmuştur. Buna karşın YDDADD-QR-KUAABA tabanlı damgalama çalışması NK'yı Gauss filtresi için %97.40, ortalama filtresi için %87.76, ortanca filtre (MDF 2x2 ve MDF 3x3) için ortalama %94.7 olarak hesaplamıştır. Filtreleme atakları içinden yalnızca keskinleştirme filtresine karşı iki yöntemin dayanıklılığı oldukça yakın bulunmuştur.

Önerilen her iki çalışma da histogram eşitleme (HE) ve gama düzeltme (GC) saldırıları karşısında benzer performans sergilemişlerdir. Yeniden ölçeklemeye (RS 512-256-512) karşı da geleneksel tabanlı damgalama algoritması daha başarılı bulunmuştur.

Tez kapsamında sunulan geleneksel ve biyometrik tabanlı çalışmaların performansı özetlenecek olursa, biyometrik tabanlı çalışma daha fazla veri gömdüğü halde gürültü, JPEG sıkıştırma, kırpma atakları karşısında daha üst seviyede dayanıklılık elde etmiştir. Ayrıca satır ve sütun bazında görüntü çevirme ve 90° ve katlarında rotasyon gibi geometrik ataklarda da ikili iris kodunu hatasız çıkarabilmiştir. Geleneksel damgalama şemasının ise filtreleme ve

Tablo 3.11. YDDADD-QR-KUAABA tabanlı yöntemin dayanıklılık performansının önerilen geleneksel damgalama yöntemiyle (ADD-TDA-KUAABA) karşılaştırılması

Ataklar	NK (%)		BHO (%)		Ataklar	NK (%)		BHO (%)	
	ADD-TDA-KUAABA	YDDADD-QR-KUAABA	ADD-TDA-KUAABA	YDDADD-QR-KUAABA		ADD-TDA-KUAABA	YDDADD-QR-KUAABA	ADD-TDA-KUAABA	YDDADD-QR-KUAABA
NA	**100**	**100**	**0**	**0**	COM Q=50	97.49	**99.51**	2.49	**0.50**
SPN 0.01	93.04	**98.15**	6.42	**1.88**	CR-T	96.50	**99.51**	2.57	**0.31**
SPN 0.02	87.83	**95.43**	11.39	**4.81**	CR-C	96.99	**100**	2.26	**0.75**
SPN 0.03	83.50	**94.19**	15.47	**5.88**	GF 3x3	**99.98**	97.40	**0.02**	1.31
PN	**100**	**100**	**0**	**0**	GF 5x5	**99.98**	97.40	**0.02**	1.31
SN 0.001	**100**	**100**	**0**	**0**	GF 9x9	**99.98**	97.40	**0.02**	1.31
SN 0.005	98.21	**99.88**	1.66	**0.13**	MF	**99.67**	87.76	**0.32**	10.00
SN 0.009	94.87	**98.27**	4.82	**1.25**	MDF 2x2	**99.39**	92.95	**0.59**	5.94
GN 0.001	96.14	**99.75**	3.63	**0.13**	MDF 3x3	**99.78**	96.42	**0.21**	3.63
GN 0.005	87.17	**97.28**	12.62	**2.56**	SF	**100**	**100**	0.01	**0**
GN 0.009	81.27	**93.70**	18.52	**6.50**	HE	99.34	**100**	0.52	**0**
COM Q=80	99.51	**100**	0.50	**0**	RS 512-256-512	**99.82**	96.66	**0.21**	3.06
COM Q=75	99.27	**100**	0.73	**0**	GC	**100**	99.38	**0**	**0.56**

yeniden ölçekleme ataklarına karşı YDDADD-QR-KUAABA tabanlı çalışmadan dirençli olduğu tespit edilmiştir.

3.2.1.3. Kimlik Doğrulama

Biyometrik damgalamada dikkate alınması gereken bir husus, biyometrik şablonların tanıma performansından ödün verilmemesi için oldukça sağlam bir damgalama şeması tasarlamaktır. Sunulan yöntemde, damgalanmış görüntüden çıkarılan iris kodu ile diğer örnekler arasında HU kullanılarak elde edilen benzerlik ölçüsüne bağlı olarak sahiplik doğrulama yapılır. Bu benzerlik skoru, doğrulama hatalarını detaylandırmak için 0.01 aralıklarla 0 ila 0.2 arasındaki eşik değerlerle karşılaştırılır. Böylece iki irisin aynı göze ait olup olmadığını değerlendirmede referans olarak kullanılacak eşik değer tahmin edilir.

Önerilen şemada, veri tabanından alınan 40 farklı kişinin iris görüntüleri kullanılmıştır. Her göz için 10 farklı görüntü kullanıldığından, toplam 400 (40×10) görüntü test edilmiştir. Kimlik doğrulama performansını değerlendirmek için, bir gözün her bir iris kodu, aynı gözün diğer tüm iris kodlarıyla eşleştirilir (sınıf içi eşleştirme). Bu eşleşme YRO'yu ölçerken, farklı gözlerin iris kodları arasındaki sınıflar arası eşleşme YKO'yu ölçer. Eşleşen çift, iris veri tabanındaki aynı irisin 10 kodundan birine aitse, eşleşme gerçek olarak kabul edilir, aksi takdirde sahtekâr olarak etiketlenir.

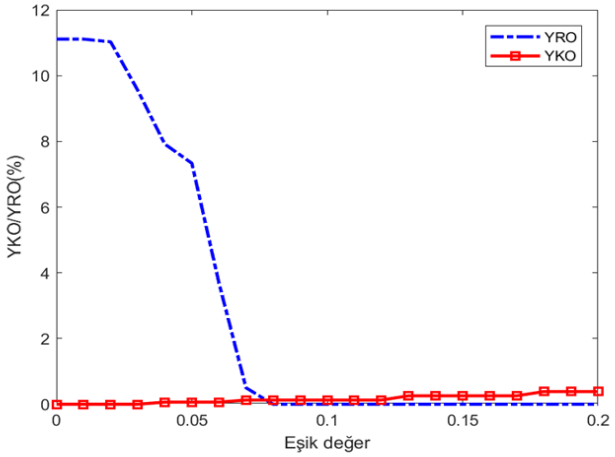
YRO, yetkili kullanıcıların sistem tarafından reddedilme olasılığı anlamına gelirken, YKO, yetkisiz kişilerin sisteme erişme yeteneğini ifade eder. Gerçek Kabul Oranı (GKO) ise, yetkili kullanıcıların sistem tarafından kabul edilme olasılığını ölçer. Bu nedenle, GKO $1 - YRO$'ya eşittir [109]. Bir biyometrik sistemin duyarlılığı arttıkça YKO düşer ancak YRO artar. EHO, YKO ve YRO için eşik değerleri önceden belirlemek amacıyla kullanılan biyometrik güvenlik sistemi algoritmasıdır. Oranların eşit olduğu ortak değer EHO olarak adlandırılır. EHO ne kadar düşük olursa biyometrik sistemin doğruluğu da o kadar yüksek olur. Şekil 3.9'da, $d = 0.03$ yoğunluktaki tuz & biber gürültüsüne (SPN 0.03), $v = 0.009$ varyanslı Gauss gürültüsüne (GN 0.009) ve $Q = 50$ kalite faktörü ile JPEG sıkıştırmaya (OM Q=50) karşı yöntem tarafından elde edilen YRO (%) ve YKO (%) değerleri verilmiştir. Bu şekle göre YRO ve YKO'nun eşit olduğu eşik değerlere karşı düşen noktaların 0'a çok yakın olduğu görülmektedir.

Tablo 3.12, 0-0.2 arasındaki eşik değerler kullanıldığında 40 damgalanmış görüntü (saldırı içeren ve içermeyen) için hesaplanan EHO değerlerini göstermektedir. Daha düşük

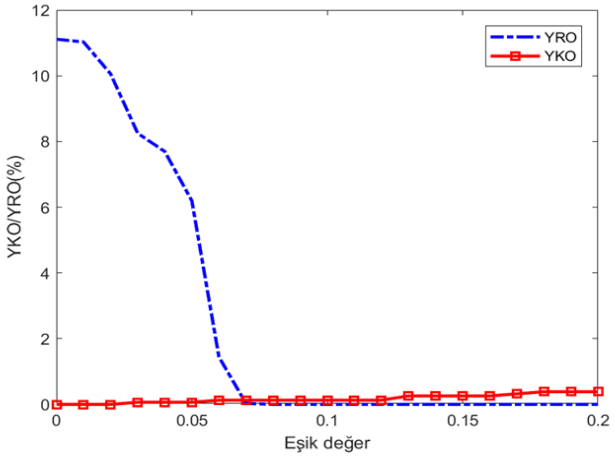
EHO'ya sahip bir sistem daha güvenilirdir ve 40 farklı durum göz önüne alındığında EHO değerlerinin ortalaması %0.07 olarak ölçülmüştür. Önerilen yöntemin yalnızca rasgele 20 satır ve 20 sütun silme atağında (DL) EHO değeri %0.1'in üzerine (%0.17) çıkmıştır. Bu durum dayanıklılık sonuçları ile tutarlı bulunmuştur. Nitekim, söz konusu atak için NK değerinin %90'ın altına düştüğü daha önceki bölümlerde ifade edilmişti. Bunun dışındaki ataklarda EHO'nun %0.1'in altında bulunduğu bu tablodan gözlenmektedir. Elde edilen sonuçlar kimlik doğrulama açısından önerilen çalışmanın doğruluk performansının oldukça yüksek olduğunu göstermektedir.

Tablo 3.12. YDDADD-QR-KUAABA tabanlı yöntemin ataklar karşısında EHO (%) değerleri

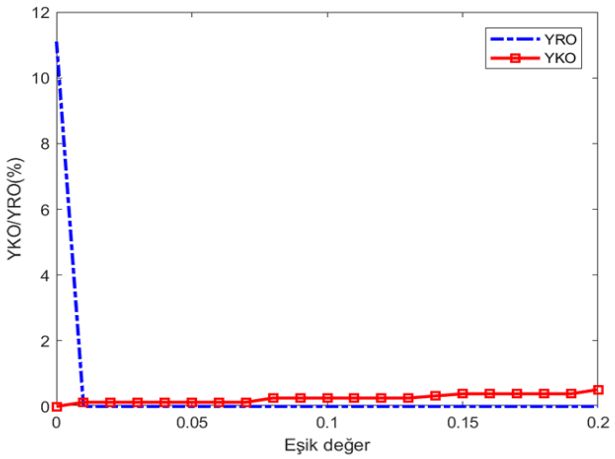
Ataklar		Ataklar		Ataklar	
NA	0.06	COM Q=85	0.06	SF	0.06
SPN 0.005	0.06	COM Q=80	0.06	HE	0.06
SPN 0.01	0.06	COM Q=75	0.06	RS 512-256-512	0.09
SPN 0.02	0.09	COM Q=60	0.06	RS 512-1024-512	0.06
SPN 0.03	0.06	COM Q=50	0.06	GC	0.06
PN	0.06	CR-T	0.06	RT 90	0.06
SN 0.001	0.06	CR-C	0.06	RT 180	0.06
SN 0.005	0.06	GF 3x3	0.09	RT 270	0.06
SN 0.009	0.06	GF 5x5	0.09	FC	0.06
GN 0.001	0.06	GF 9x9	0.09	FR	0.06
GN 0.005	0.06	MF	0.06	DL	0.17
GN 0.009	0.08	MDF 2x2	0.06	WC bpp=3.5	0.06
COM Q=100	0.06	MDF 3x3	0.08	WC bpp=8	0.06
COM Q=90	0.06				



(a)



(b)



(c)

Şekil 3.9. YDDADD-QR-KUAABA tabanlı yönteme ait YKO (%) ve YRO (%): (a) SPN d=0.03, (b) GN v=0.009, (c) COM Q=50

Tablo 3.13 önerilen şemanın, Bath Üniversitesi veri tabanı kullanan iris tabanlı damgalama şemaları ile kıyaslamasını içermektedir. Tabloda yer alan veriler YDDADD-QR-KUAABA tabanlı yöntemin eşik değeri 0.09 alınarak elde edilmiştir. Karşılaştırma, JPEG sıkıştırma (COM), Gauss filtresi (GS), keskinleştirme filtresi (SF) ve dalgacık sıkıştırma (WC) saldırılarına karşı kabul edilen "gerçek" sayılarına bağlı olarak yapılır. Bu tabloya göre, YDDADD-QR-KUAABA tabanlı sistem, tüm yetkili kullanıcıların sisteme erişmesine izin verirken, [71, 72]'de verilen yöntemler bazı yetkili kullanıcıları sahtekâr olarak etiketlemişlerdir. Bu çalışmada sunulan sistemin [71, 72]'deki iris tabanlı damgalama yöntemlerine göre bir başka avantajı ise, geometrik saldırılara ve gürültü eklemeye karşı üstün performansa sahip olmasıdır. Nitekim [71, 72]'deki yazarlar bu ataklara karşı performansı değerlendirmemişlerdir.

Tablo 3.13. YDDADD-QR-KUAABA tabanlı yöntemin gerçek kabul sayılarının literatürdeki çalışmalarla karşılaştırılması

	Gerçek Kabullerin Sayısı		
Ataklar	YDDADD-QR-KUAABA	[71]	[72]
COM (Q=100, 90, 85, 80, 75, 60, 50)	**2800**	2766	2724
Filtreleme (GF 3x3, GF 5x5, SF)	**1200**	1193	1189
WC (bpp=3.5, 8)	**800**	784	--

Tablo 3.14, çeşitli biyometrik tabanlı sayısal damgalama çalışmalarının özetini içermektedir. İlgili çalışmalar, önerdikleri yaklaşımların etkinliğini kanıtlamak için farklı biyometrik özellikler kullanmışlardır. Dolayısıyla önerilen yöntem ile literatür çalışmaları arasında geçerli bir karşılaştırma yapılamamıştır. Tabloda yer alan NK ve BHO sonuçları çıkarılan iris verisi için ilgili yöntemde test edilen ataklar karşısında hesaplanan değerlerin ortalamasını yansıtmaktadır. EHO ise atak olmadığı durumda sistem tarafından hesaplanan hata oranını ifade etmektedir. Tabloya bakıldığında tek modelli, yani yalnızca iris verisinin kullanıldığı YDDADD-QR-KUAABA tabanlı çalışmanın hem algılanamazlık, hem dayanıklılık hem de kimlik doğrulama hassasiyeti açısından gereksinimleri karşıladığı görülmektedir.

Tablo 3.14. Farklı biyometrik tabanlı damgalama yöntemlerinin özeti

	Biyometrik Özellik	**Kullanılan Yöntem**	**Sonuçlar**
[57]	İris, Parmak İzi	BBA (İris = Kör Parmak izi = Kör olmayan)	TSGO = -- Ortalama NK = -- Ortalama BHO = -- EHO = 3.57 (iris) EHO = 6.52 (parmak izi) EHO= 0.50 (iris + parmak izi)
[71]	İris	ADD, TDA (Kör olmayan)	TSGO = 53 dB Ortalama NK = -- Ortalama BHO = -- Ortalama EHO = -- GKO = %89.85
[72]	İris	AKD, TDA (Kör olmayan)	TSGO = -- Ortalama NK = -- Ortalama BHO = -- Ortalama EHO = -- GKO = %90.82
[109]	İris, Parmak İzi	AKD (Kör)	TSGO = 38.2340 dB Ortalama BHO = %0.03 EHO = %3.60 (iris) EHO = %6.40 (parmak izi) EHO = %1.20 (iris + parmak izi)
[110]	İris, Yüz	AADD, TDA (Kör olmayan)	TSGO = 36.85 dB Ortalama NK = %87.93 EHO = 4.24 (iris) EHO = 6.68 (yüz) EHO = 0.52 (iris + yüz)
[111]	İris, Parmak İzi, İmza	AADD, TDA (Kör olmayan)	TSGO = 43.56 dB Ortalama NK = %99.79 Ortalama BHO = -- EHO = --
[135]	İris, Parmak İzi	Slantlet Dönüşümü, TDA (Kör olmayan)	TSGO = 52.09 dB Ortalama NK = %98.33 Ortalama NMH = %6.85 EHO = --
YDDADD-QR-KUAABA	İris	YDDADD, QR Ayrıştırma (Kör)	TSGO=40.5822 dB Ortalama NK = %98.20 Ortalama BHO = %1.56 EHO = %0.06

3.2.1.4. Önerilen Biyometrik Damgalama Yönteminin Sonuçları

Tezin ikinci aşamasında renkli görüntülerin telif hakkının korunması için iris kodunun damga olarak kullanıldığı YDDADD-QR-KUAABA tabanlı dayanıklı ve kör yaklaşım ele alınmıştır. Yöntemin sonuçları üç ayrı kapsamda incelenmiştir: Algılanamazlık, dayanıklılık ve kimlik doğrulama. Algılanamazlık performansı literatürde yaygın olarak kullanılan TSGO metriğine bağlı olarak değerlendirilmiştir. Önerilen yöntemin TSGO değeri 40.5822 dB olarak bulunmuştur. Dolayısıyla damganın varlığı damgalanmış görüntülerde hissedilmemektedir. Ayrıca mevcut referans çalışmalarla kıyaslandığında burada daha fazla veri gömüldüğü halde TSGO değerinin daha yüksek olduğu görülmektedir.

Yöntemin dayanıklılığı hem yaygın sinyal işleme ataklarına hem de geometrik ataklara karşı test edilmiştir. Bir tane sadece damgalanmış ve otuz dokuz tane damgalandıktan sonra atak uygulanmış görüntüden çıkarılan iris kodu ile gömülen iris kodu arasında NK ve BHO değerleri hesaplanarak ölçümler gerçekleştirilmiştir. Ataklar karşısında elde edilen ortalama NK %98.20, ortalama BHO ise %1.56 olarak bulunmuştur. Bu durum yöntemin üst seviyede dayanıklılığa sahip olduğunun göstergesidir. Çalışmanın en dikkat çekici noktası YDDADD'nin yapısından dolayı satır veya sütün bazında görüntü çevirme ve 90° ve katlarında rotasyon karşısındaki performansıdır. Söz konusu ataklar için önerilen yöntem gömülen damgayı hatasız olarak çıkarabilmektedir. Bunun yanı sıra, gürültü atakları, JPEG sıkıştırma, kırpma, filtreleme atakları, yeniden ölçekleme, histogram eşitleme, gama düzeltme ve dalgacık sıkıştırmaya karşı da dayanıklılığının oldukça yüksek olduğu tespit edilmiştir. Önerilen yöntemin veri ekleme kapasitesinin daha fazla olduğu göz önünde bulundurularak referans çalışmalarla kıyaslandığında özellikle gürültü ataklarına, kırpmaya ve rotasyona karşı yöntemin daha başarılı olduğu, ortalama filtresine karşı ise bunların bazılarının ([97, 98, 133]) biraz gerisinde kaldığı gözlenmiştir.

Yöntem Bölüm 2.1'de tanıtılan ADD-TDA-KUAABA tabanlı geleneksel damgalama çalışmasıyla kıyaslandığında daha fazla miktarda bit gömdüğü halde gürültü, JPEG sıkıştırma, kırpma ve geometrik ataklarda yüksek başarı elde etmiştir. Yalnızca filtreleme atakları ve yeniden ölçekleme atağında ADD-TDA-KUAABA tabanlı yöntem YDDADD-QR-KUAABA tabanlı yöntemin önüne geçmiştir.

Son olarak çıkarılan iris kodunun kimlik doğrulama hassasiyeti test edilmiştir. YRO ve YKO'ya bağlı olarak yöntemin EHO değeri ortalama %0.07 olarak hesaplanmıştır. EHO'nun

0’ya yakın olması hata oranının düşük olduğunu göstermektedir. Dolayısıyla önerilen çalışma sahiplik doğrulama açısından oldukça iyi performansa sahiptir. Aynı veri tabanını kullanan damgalama şemalarıyla gerçek kabul sayıları karşılaştırıldığında ise yöntemin diğerlerinin aksine tüm yetkili kullanıcıları tespit edebildiği gözlenmektedir.

4. SONUÇLAR

Sayısal teknolojinin gelişmesiyle, video, ses, metin ve görüntü gibi sayısal medya içerikleri, erişim ve zaman kısıtlamaları olmaksızın internet üzerinden kolayca aktarılabilir. Bu durum, çoklu ortam verilerinin yasa dışı amaçlarla kolayca çoğaltılmasına veya değiştirilmesine izin verir. Sayısal damgalama, çoklu ortam verilerini yönetmek ve yasadışı kopyalama ve değişime karşı korumak ve bundan kaynaklanan telif hakkı sorunlarını ortadan kaldırmak için etkili bir çözüm sağlar.

Literatürde sayısal damgalamanın uygulandığı çeşitli uygulama alanları mevcuttur. Bu çalışmada sayısal görüntülerin telif hakkı ve fikri mülkiyet haklarının korunması için dayanıklı damgalama şemaları önerilmiştir.

Görüntü damgalama, uzaysal alanda veya dönüşüm alanında uygulanabilir. Uzaysal alan yöntemleri, orijinal görüntünün piksel değerlerini doğrudan değiştirerek damgayı ekler. Genel olarak, uzaysal alanda damgalama düşük karmaşıklık ve kolay uygulama avantajlarına sahiptir, ancak saldırılara açık olma eğilimindedir. Uzaysal alana kıyasla, damganın dönüştürülmüş görüntünün katsayılarını değiştirerek gizlendiği dönüşüm alanı yöntemlerinin genellikle saldırılara karşı daha dayanıklı olduğu kabul edilir. Bunlar arasında ADD tabanlı görüntü damgalama tekniklerinin çoklu çözünürlük gösterimi, mükemmel zaman frekans analizi gibi avantajları tercih edilen dayanıklılık ve algılanamazlık özelliklerini elde etmek açısından ön plana çıkmaktadır.

Telif hakkı korumaya yönelik dayanıklı görüntü damgalama algoritmalarının temel amacı, düşük kaliteli bozulma ve yüksek dayanıklılık ile damgalanmış görüntü üretmektir. Ancak algılanamazlık ve dayanıklılık birbiriyle çeliştiği için sayısal damgalama yöntemleri söz konusu iki kavramı otomatik olarak dengeleyemezler. Bunlar arasında uygun bir ödünleşim elde etmek zor olduğundan bu, optimizasyon problemi olarak görülebilir. O nedenle gerçeklemesi kolay, basit ve esnek oluşu sebebiyle ABA ve ABA'nın türevi olan KUAABA bahsi geçen kavramları dengelemek amacıyla kullanılır.

Geleneksel sayısal damgalama yöntemlerinde, damga, sözde rastgele sayı dizisinden, ikili görüntülerden veya kaotik diziden oluşur. Bu durumda, damganın sahipliğini doğrulamak daha

zor olacaktır. O sebeple, sahiplik talebinde bulunmak için damganın daha güvenli bir şekilde tanımlanması gerekir. Damganın fiziksel veya mantıksal sahipliği sorununu çözmek için biyometrik tabanlı güvenlik şemalarının kullanılması potansiyel bir çözümdür. Benzersiz ve kişiye özgü biyometrik veriler, yetkili ve yetkisiz kullanıcılar arasında ayrım yapma yeteneğine sahiptir. Dolayısıyla, iris, parmak izi, yüz, avuç içi izi, imza vb. bireysel özelliklerin damga olarak kullanılması, içerik üzerinde hak iddia eden kişinin gerçek sahip olup olmadığını belirlemek için kesinlikle kritik olacaktır.

İris tanıma, en güvenilir ve doğru biyometrik teknolojilerden biridir Yüz tanıma, ses tanıma ve el geometrisinin aksine, iris tanıma, kimlik doğrulamaya daha yüksek düzeyde güvenlik sağlar. Yine iris tanıma ile parmak izi karşılaştırıldığında, her ikisi de diğer biyometrik teknolojilere göre daha yüksek basitliğe, doğruluğa ve güvenilirliğe sahiptir. Ancak parmak izinden farklı olarak iris desenlerinin kopyalanmasının daha zor olması iris tanımayı ön plana çıkarmaktadır. Bu nedenlerle tez çalışmasında iris tabanlı damgalamaya ağırlık verilmiştir.

Tez süresince sayısal görüntülerin telif hakkını koruma amacıyla sunulan dayanıklı yöntemlerden elde edilen sonuçları aşağıda verildiği gibi özetlemek mümkündür.

Görüntü damgalama şemalarının performansının, diğer dönüşümlerle birlikte TDA kullanılarak geliştirilebileceği literatürde yer alan çalışmalarca kanıtlanmıştır. ADD'nin de, iyi uzaysal yerelleştirme sağlaması, üstün İGS modellemesi ve çoklu çözünürlük özelliklerine sahip olmasından dolayı çalışmanın birinci kısmında bu iki dönüşüm yöntemi bir arada kullanılmıştır. İlk olarak, orijinal görüntü tek seviyeli ADD ile ayrıştırılır ve dayanıklılığı artırması sebebiyle elde edilen düşük frekanslı alt bant örtüşmeyen bloklara bölünür. Damganın gömüleceği bloklar standart sapma değerlerine göre seçilir. Seçilen her blok TDA tarafından dönüştürülür ve dönüştürülmüş blokların U bileşeninin birinci sütununun ikinci katsayısı damga gömmek için bir ölçeklendirme faktörüne bağlı olarak modifiye edilir. Ölçeklendirme faktörü, dayanıklılık ve görsel kalite açısından damgalama başarısında çok etkilidir. Her blok farklı desenler sergilediğinden, çeşitli orijinal görüntü ve bloklar için uygun ölçeklendirme faktörleri bulmak zordur. Bu nedenle KUAABA, çoklu ölçeklendirme faktörlerini optimize etmek için kullanılır. Burada, damgalamanın güvenlik gereksinimi FLD tarafından karşılanmaktadır. Önerilen sistem, on bir gri seviye test görüntüsü ve otuz ev görüntüsü üzerinde çalıştırılır ve performansı önceki benzer çalışmalarla karşılaştırılır. Deneysel sonuçlara göre, yöntem dayanıklılığı ve görsel şeffaflığı geliştirmektedir. NK ve BHO değerleri diğer yöntemlerle karşılaştırıldığında, saldırıların çoğunda dayanıklılığın diğer şemalara göre

daha yüksek olduğu görülmektedir. Özellikle önerilen sistem filtreleme, kırpma, sıkıştırma gibi saldırılara karşı diğer çalışmalardan daha dirençli bulunmuştur.

Tezin ikinci kısmında, renkli görüntülere biyometrik desenlerden oluşturulan ikili damganın gömülmesine odaklanılmıştır. Literatür çalışmalarında sayısal damgalamada ADD ve TDA yöntemlerinin bir arada kullanıldığı birçok yayın mevcuttur. Oysa QR Ayrıştırma da TDA kadar iyi bir performansa sahiptir. Ayrıca telif hakkı koruma amacıyla yapılan biyometrik damgalama şemalarında bilindiği kadarı ile QR Ayrıştırmaya yönelik bir çalışma yoktur. QR Ayrıştırmanın yanı sıra TDA'ya alternatif olarak damgalama şemalarında kullanılan bir diğer yöntem ise Schur Ayrıştırmadır. Schur Ayrıştırma TDA'ya göre daha az hesaplama gerektirmesi ve TDA'nın üstünlüklerine sahip olması sebebiyle avantajlı bir tekniktir. Ayrıca literatürde Schur Ayrıştırma ile ilişkilendirilmiş daha az sayıda çalışma mevcuttur. Bunun yanı sıra bu bölümde geleneksel dalgacık dönüşümünden farklı olarak 90° katlarında rotasyon ve görüntü çevirmeye karşı dayanıklı bir teknik olan YDDADD temel dönüşüm alanı olarak tercih edilmiştir. Dolayısıyla bu bölümde YDDADD alanında TDA, QR Ayrıştırma ve Schur Ayrıştırma teknikleri (YDDADD-TDA, YDDADD-QR Ayrıştırma, YDDADD-Schur Ayrıştırma) ayrı ayrı incelenmiştir. Ayrıca çalışmada gömme adımında kullanılan ölçekleme faktörü, hem sabit seçilerek, hem de ABA ve KUAABA ile dayanıklılık ve algılanamazlığı dengelemek amacıyla optimize edilerek elde edilen sonuçlar karşılaştırılmıştır. Böylece en uygun dönüşüm alanı tekniği ve en uygun optimizasyon algoritması belirlenmeye çalışılmıştır.

Her üç yöntemde de Bath Üniversitesinden elde edilen iris şablonunun AKD yardımıyla ikili koda dönüştürülmesi ile oluşturulan dizi damga olarak kullanılmaktadır. Söz konusu yöntemlerde, renkli taşıyıcı görüntü için YCbCr modelinin renk kanalları daha az ilişkili olduğundan, bu renk uzayı tercih edilmekte ve damga, dayanıklılığı artırmak adına görüntünün enerjisinin çoğunu içeren Y kanalına gömülmektedir. Damganın gömülmesi aşamasında öncelikle görüntünün Y kanalı "Haar" filtre yardımıyla YDDADD ile ayrıştırılır. Düşük frekanslı alt bant bloklara bölünür ve standart sapma değeri daha düşük olan bloklar damga gömme pozisyonu olarak belirlenir. Eğer matris ayrıştırma tekniği olarak TDA seçilirse U bileşeninin sütun vektöründeki katsayıları değiştirmenin, satır vektöründeki katsayıları değiştirmekten daha az görünür bozulmaya neden olması ve yalnızca ilk sütununun değişmez büyüklük ilişkisini koruması sebebiyle bu bileşenin ikinci satır birinci sütun katsayısı modifiye edilir. Eğer bloğa QR Ayrıştırma uygulanacaksa R matrisi damganın gömüleceği alan olarak tercih edilir. QR ile ayrıştırılacak giriş matrisinin sütunları ilişkili olduğunda, R matrisinin ilk satır elemanlarının mutlak değeri, diğer satırların mutlak değerinden çok daha büyük olacaktır.

Dolayısıyla, ilk satıra damga bitleri gömüldüğünde orijinal görüntünün görsel kalitesinde daha az bozulma meydana gelecektir. Bu nedenle damga R matrisinin ilk satırına gizlenir. Eğer YDDADD alanında Schur Ayrıştırma tekniği ile damgalama gerçekleşecekse Schur Ayrıştırmadan sonra elde edilen üniter matrisin (U) tüm ilk sütun elemanlarının aynı işarete sahip olması ve değerlerinin birbirine çok yakın olmasından dolayı bu matris damgayı gömmek üzere tercih edilir. Damga bitleri seçilen ayrıştırma tekniğinin özelliklerine bağlı olarak gömüldükten ve damgalanmış bloğa ters ayrıştırma uygulandıktan sonra ters YDDADD yardımıyla damgalanmış Y bileşen elde edilir. Cb ve Cr kanalları ile birlikte bu bileşen RGB uzayına çevrilerek damgalanmış renkli görüntü oluşturulur. Her üç yöntemde de kör damgalama gerçekleştiğinden damga çıkarma sürecinde orijinal görüntüye ihtiyaç duyulmaz.

Dayanıklılık, algılanamazlık ve kimlik doğrulama açısından çalışmalar kıyaslandığında, KUAABA ile optimize edilmiş YDDADD-QR Ayrıştırmaya dayalı yöntem hem algılanamazlığı daha üst seviyeye çıkardığı hem de daha az sahiplik doğrulama hatasına sahip olduğu için ön plana çıkmaktadır. O nedenle bu yöntemin deneysel sonuçları ayrıntılı olarak irdelenmiştir.

YDDADD-QR-KUAABA tabanlı çalışmanın algılanamazlığı test edildiğinde TSGO değeri 40 dB'nin üzerinde bulunmuştur. Dolayısıyla damgalanmış görüntünün görsel kalitesinin iyi olduğu ve gömülen damganın varlığının damgalanmış görüntülerde kesinlikle hissedilmediği söylenebilir. Dayanıklılık incelendiğinde ise hem NK değerinin hem de BHO değerinin oldukça üstün olduğu görülmektedir. Kırk farklı durum için ortalama NK %98.20, ortalama BHO ise %1.56 bulunmuştur. Yöntem atak olmadığı durumda ve gürültü atakları, JPEG sıkıştırma, kırpma, Gauss filtresi, ortanca filtresi, keskinleştirme filtresi, histogram eşitleme, yeniden ölçekleme, gama düzeltme, rotasyon, görüntü çevirme ve dalgacık sıkıştırma atakları söz konusu olduğunda gömülen iris kodunu ya hatasız olarak ya da yüksek oranda doğrulukla çıkarabilmektedir. Ancak ortalama filtresine ve görüntüden rasgele yirmi satır ve yirmi sütun silme atağına karşı diğer ataklardan biraz daha düşük bir performansa sahiptir.

Önerilen biyometrik tabanlı damgalama algoritmasının performansı geleneksel damgalama şemalarıyla algılanamazlık ve dayanıklılık açısından karşılaştırılmıştır. Dalgacık dönüşümüne dayalı dört kör görüntü damgalama algoritması ([97, 98, 133, 134]) daha az veri yükleme kapasitesine sahip olduğu halde, YDDADD-QR-KUAABA tabanlı çalışmanın görsel kalitesinin ve dayanıklılığının daha üstün olduğu bulunmuştur. Ataklar karşısında elde edilen NK ve BHO değerleri incelendiğinde JPEG sıkıştırma, keskinleştirme filtresi, histogram eşitleme ve yeniden ölçekleme atakları açısından sonuçların [97], [98] ve [133]'te elde

edilenlerle yakın olduğu gözlense de gürültü atakları, kırpma ve rotasyona karşı önerilen yöntem bahsi geçen literatür çalışmalarından oldukça başarılı bulunmuştur. [134] ile karşılaştırıldığında ise kırpma, keskinleştirme filtresi, histogram eşitleme ve rotasyon açısından elde edilen NK ve BHO değerleri yakın olsa da, gürültü atakları, JPEG sıkıştırma ve ortalama filtresi söz konusu olduğunda önerilen çalışma daha dirençli bulunmuştur. Yine bu yöntemlerde test edilmeyen satır veya sütun bazında görüntü çevirmeye, dalgacık sıkıştırmaya ve damgalanmış görüntüden rasgele yirmi satır ve yirmi sütun silinmesi durumuna karşı da YDDADD-QR-KUAABA tabanlı sistemin dayanıklılığının yüksek olduğu gözlenmiştir.

Tez kapsamında önerilen geleneksel damgalama ve biyometrik damgalama çalışmalarının dayanıklılık performansı birlikte değerlendirildiğinde YDDADD-QR-KUAABA tabanlı damgalama şeması daha yüksek veri yükleme kapasitesine sahip olmasına rağmen gürültü, JPEG sıkıştırma, kırpma gibi ataklarda ve geometrik bozulmalarda daha dirençli bulunmuştur. ADD-TDA-KUAABA tabanlı çalışma ise yalnızca filtreleme ve yeniden ölçekleme atağına karşı biyometrik damgalama yöntemini geride bırakmıştır.

İris biyometrisini kullanan çalışmanın kimlik doğrulama performansı YRO ve YKO yardımıyla hesaplanan EHO'ya bağlı olarak değerlendirilmiştir. Elde edilen bulgular irdelendiğinde tüm ataklar için ortalama EHO değerleri %0.07 bulunmuştur. EHO sıfıra yaklaştıkça doğrulama hassasiyetinin arttığı göz önüne alındığında yöntemin oldukça başarılı olduğu gözlenebilir. Bu çalışmayla aynı veri tabanını kullanan [71, 72]'de verilen kör olmayan damgalama sistemleriyle gerçek kabul sayıları açısından kıyaslama yapıldığında, YDDADD-QR-KUAABA tabanlı yöntem tüm yetkili kullanıcıların sisteme erişimine izin verirken, bahsi geçen referans çalışmalar bazı yetkili kullanıcıları sahtekâr olarak etiketlemektedir. Dolayısıyla önerilen biyometrik damgalama şemasının kimlik doğrulama performansı daha üstün bulunmuştur.

5. ÖNERİLER

Günümüzde internet teknolojilerinin ve bilgisayar ağlarının gelişimi görüntü, video, ses vb. çoklu ortam verilerini kolayca erişilebilir ve kopyalanabilir hale getirmiştir. Kopyalanan sayısal içeriklerin kalitesi, orijinal içeriklerle aynı olduğundan telif haklarını korumak önemli bir zorluk haline gelmiştir. Sayısal damgalama, bu tür sorunların üstesinden gelmek için ortaya çıkmış bir tekniktir.

Tez kapsamında ilk olarak gri seviye görüntüye ikili logonun gömüldüğü optimize edilmiş kör damgalama yöntemi önerilmiştir. Bu yöntem çeşitli gürültü ekleme, JPEG sıkıştırma, filtreleme, kırpma, yeniden ölçekleme gibi ataklar karşısında test edilmiş ve başarılı bulunmuştur. İkinci aşamada ise damganın ikili görüntülerden seçilmesinden kaynaklanabilecek aidiyet problemlerini çözmek için iris verisinden elde edilen ikili kod damga olarak tercih edilmiştir. Bu kısımda taşıyıcı içerik olarak gri seviye görüntü yerine renkli görüntülerden yararlanılmıştır. Ayrıca bir önceki çalışmadan farklı olarak 90° ve katlarında rotasyon ve görüntü çevirme gibi geometrik ataklar karşısında da dayanıklı yöntemler sunulmuştur. 90° ve katları dışındaki rotasyon atağında ya da görüntünün ötelenmesi durumunda orijinal görüntünün bir kısmı kaybolacaktır. Çalışma blok tabanlı olduğu için bu tarz ataklarda dayanıklılık performansı düşecektir. Bu nedenle dairesel alanda tanımlanan dönüşüm tekniklerinden yararlanılabilir. Bu tekniklerin yer aldığı bazı çalışmalar ([136-138]) damga boyutunun çok yüksek olmadığı durumlarda iyi görsel kalite elde edilebileceğini göstermiştir. Gömülecek bit sayısı arttığında ise aynı oranda algılanamazlık elde edebilmek için dayanıklılıktan feragat etmek gerekecektir. Ancak, önerilen biyometrik tabanlı telif hakkı koruma uygulamalarında dayanıklılığın yüksek seviyede tutulması şarttır. Bunu bahsi geçen tekniklerle sağlamak görüntüdeki bozulma oranını önemli ölçüde artıracaktır. Bu hususlar göz önüne alındığında, biyometrik tabanlı kör damgalama şeması tasarlamak için ilgili biyometrik özelliği daha az sayıda veri ile temsil edebilecek öznitelik çıkarma yöntemleri araştırılabilir. Böylece gömülecek veri miktarı azaldığından TSGO değeri artacaktır.

Daha önce kör damgalama yöntemlerinin kör olmayan yöntemlere kıyasla dayanıklılıklarının daha düşük olduğundan bahsedilmişti. Orijinal görüntünün damga çıkarma adımında kullanılmadığı kör sistemler tasarlandığında yüksek dayanıklılık elde etmek için algılanamazlıktan bir miktar ödün verilmesi kaçınılmazdır. Gelecek çalışmalarda damgalanmış görüntülerde meydana gelecek görsel bozulmayı azaltmak amacıyla, kullanılan matris

ayrıştırma tekniklerinde damganın gömüldüğü bileşende meydana gelecek değişimin diğer bileşenlerde yer alan verilerle telafi edilip edilemeyeceği araştırılabilir. Böylece dayanıklılık korunarak, daha yüksek TSGO değeri elde edilebilir.

Bu tez çalışmasında renkli görüntülerde damgalama gerçekleştirilirken YCbCr uzayı tercih edilmişti. Damga dayanıklılığı artırmak adına enerjinin çoğunu içeren Y kanalına gizlenmişti. Ancak Cb kanalının İGS açısından en az duyarlı olmasından dolayı bu kanalda damgalama görsel kaliteyi iyileştirebilir. Gelecek çalışmalarda her bir kanalın avantajını birleştirmek için tek kanal yerine iki veya üç kanaldan yararlanılabilir.

6. KAYNAKLAR

1. Cox, I. J. ve Miller, M. L. Review of watermarking and the importance of perceptual modeling, Human Vision and Electronic Imaging II, 1997, International Society for Optics and Photonics, 92-99.

2. Al-maweri, N. a. A. S., Ali, R., Adnan, W. A. W., Ramli, A. R. ve Ahmad, S. M. S., State-of-the-Art in Techniques of Text Digital Watermarking: Challenges and Limitations, J. Comput. Sci., 12,2 (2016) 62-80.

3. Kamaruddin, N. S., Kamsin, A., Por, L. Y. ve Rahman, H., A review of text watermarking: theory, methods, and applications, IEEE Access, 6,(2018) 8011-8028.

4. Podilchuk, C. I. ve Delp, E. J., Digital watermarking: algorithms and applications, IEEE signal processing Magazine, 18,4 (2001) 33-46.

5. Asikuzzaman, M. ve Pickering, M. R., An overview of digital video watermarking, IEEE Transactions on Circuits and Systems for Video Technology, 28,9 (2017) 2131-2153.

6. Jayamalar, T. ve Radha, V., Survey on digital video watermarking techniques and attacks on watermarks, International Journal of Engineering Science and Technology, 2,12 (2010) 6963-6967.

7. Milosav, P., Banjac, Z., Milosavljević, M., Tomislav, U. ve Abdelrahman Mohamed Mostafa, M. Overview and Classification of Digital Watermarking Algorithms, Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research, 2019, Singidunum University, 537-545.

8. Ahmed, K. A., Digital watermarking of still images, Doktora Tezi, The University of Manchester Faculty of Engineering and Physical Sciences, United Kingdom, 2013.

9. Barni, M., Bartolini, F., Cappellini, V. ve Piva, A., A DCT-domain system for robust image watermarking, Signal processing, 66,3 (1998) 357-372.

10. Woo, C.-S., Digital image watermarking methods for copyright protection and authentication, Doktora Tezi, Queensland University of Technology, 2007.

11. Tao, H., Chongmin, L., Zain, J. M. ve Abdalla, A. N., Robust image watermarking theories and techniques: A review, Journal of applied research and technology, 12,1 (2014) 122-138.

12. Shukla, D. ve Sharma, M., Watermarking schemes for copy protection: A survey, International Journal of Computer Science and Engineering Survey, 3,1 (2012) 65.

13. Cox, I. J., Miller, M. L., Linnartz, J. ve Kalker, T., A review of watermarking principles and practices, Digital signal processing for multimedia systems, (1999) 461-482.

14. Cox, I. J., Miller, M. L. ve Bloom, J. A. Watermarking applications and their properties, Proceedings International Conference on Information Technology: Coding and Computing (Cat. No. PR00540), 2000, IEEE, 6-10.

15. Liu, J. ve He, X. A review study on digital watermarking, 2005 International Conference on Information and Communication Technologies, 2005, IEEE, 337-341.

16. Chen, T.-S., Chang, C.-C. ve Hwang, M.-S., A virtual image cryptosystem based upon vector quantization, IEEE transactions on Image Processing, 7,10 (1998) 1485-1488.

17. Kuo, T.-Y., Su, P.-C. ve Tsai, C.-M., Improved visual information fidelity based on sensitivity characteristics of digital images, Journal of Visual Communication and Image Representation, 40,(2016) 76-84.

18. Kumar, P. A. ve Sankaran, P. Visual information fidelity in evaluating retinex enhancement algorithms, 2014 International Conference on Communication and Signal Processing, 2014, IEEE, 167-171.

19. Sikander, B., Ishtiaq, M., Jaffar, M. A., Tariq, M. ve Mirza, A. M. Adaptive digital watermarking of images using Genetic Algorithm, 2010 International Conference on Information Science and Applications, 2010, IEEE, 1-8.

20. Cox, I., Miller, M., Bloom, J., Fridrich, J. ve Kalker, T., Digital watermarking and steganography, Morgan kaufmann, 2007.

21. Begum, M. ve Uddin, M. S., Digital Image Watermarking Techniques: A Review, Information, 11,2 (2020) 110.

22. Balci, S. E., Robust Watermarking of Images, Yüksek Lisans Tezi, The Middle East Technical University, Department of Electrical and Electronics Engineering, Ankara, 2003.

23. Kumar, S., Singh, B. K. ve Yadav, M., A Recent Survey on Multimedia and Database Watermarking, Multimedia Tools and Applications, (2020) 1-49.

24. Qasim, A. F., Reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images, Doktora Tezi, University of Salford, UK, 2019.

25. Chitra, K. ve Venkatesan, V. P. Spatial domain watermarking technique: An introspective study, Proceedings of the International Conference on Informatics and Analytics, 2016, 1-6.

26. Zeki, A. M. ve Manaf, A. A., A novel digital watermarking technique based on ISB (Intermediate Significant Bit), World Academy of Science, Engineering and Technology, 50,(2009) 989-996.

27. Mohammed, G. N., Yasin, A. ve Zeki, A. M. Robust image watermarking based on dual intermediate significant bit (DISB), 2014 6th International Conference on Computer Science and Information Technology (CSIT), 2014, IEEE, 18-22.

28. He-Jing, W., A DCT Domain Image Watermarking Method Based on Matlab, International Journal of Advanced Network Monitoring and Controls, 2,2 (2017) 38-45.

29. Ahmed, N., Natarajan, T. ve Rao, K. R., Discrete cosine transform, IEEE transactions on Computers, 100,1 (1974) 90-93.

30. Hamidi, M., El Haziti, M., Cherifi, H. ve El Hassouni, M., Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform, Multimedia Tools and Applications, 77,20 (2018) 27181-27214.

31. Cai, Y.-m., Guo, W.-q. ve Ding, H.-y., An Audio Blind Watermarking Scheme Based on DWT-SVD, Journal of Software, 8,7 (2013) 1801-1808.

32. Debnath, L. ve Shah, F. A., Wavelet transforms and their applications, Springer, 2002.

33. Villanueva-Luna, A. E., Flores-Gil, A., Jaramillo-Nuñez, A., Ortiz-Lima, C. M., Sanchez-Lucero, D., Aguilar-Soto, J. G. ve May-Alarcon, M., De-noising audio signals using MATLAB wavelets toolbox, INTECH Open Access Publisher, 2011.

34. Vetrivelan, P. ve Kandaswamy, A., Contourlet Based Digital Image Watermarking, CiiT International Journal of Digital Image Processing, 3,10 (2011) 644-650.

35. Nguyen, S. C., Ha, K. H. ve Nguyen, H. M. A new image watermarking scheme using contourlet transforms, 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 2016, IEEE, 1-6.

36. Kumar, N. K. ve Sheeba, V. Blind biometric watermarking based on contourlet transform, 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), 2012, IEEE, 1-6.

37. Loukhaoukha, K. ve Chouinard, J.-Y. Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification, 2009 11th Canadian Workshop on Information Theory, 2009, IEEE, 177-182.

38. Makbol, N. M. ve Khoo, B. E., Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, AEU-International Journal of Electronics and Communications, 67,2 (2013) 102-112.

39. Makbol, N. M. ve Khoo, B. E., A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition, Digital Signal Processing, 33,(2014) 134-147.

40. Yanovsky, I., QR Decomposition with Gram-Schmidt, University of California, Los Angeles, 2012.

41. Naderahmadian, Y. ve Hosseini-Khayat, S. Fast watermarking based on QR decomposition in wavelet domain, 2010 Sixth international conference on intelligent information hiding and multimedia signal processing, 2010, IEEE, 127-130.

42. Su, Q., Niu, Y., Liu, X. ve Zhu, Y., Embedding color watermarks in color images based on Schur decomposition, Optics Communications, 285,7 (2012) 1792-1802.

43. Karajeh, H., Khatib, T., Rajab, L. ve Maqableh, M., A robust digital audio watermarking scheme based on DWT and Schur decomposition, Multimedia Tools and Applications, 78,13 (2019) 18395-18418.

44. Su, Q. ve Chen, B., An improved color image watermarking scheme based on Schur decomposition, Multimedia Tools and Applications, 76,22 (2017) 24221-24249.

45. Mohammad, A. A., A new digital image watermarking scheme based on Schur decomposition, Multimedia Tools and Applications, 59,3 (2012) 851-883.

46. Singh, N., Jain, M. ve Sharma, S., A Survey of Digital Watermarking Techniques, International Journal of Modern Communication Technologies and Research, 1,6 (2013) 265852.

47. Liu, L., A survey of digital watermarking technologies, Department of Electrical and Computer Engineering, State University of New York at Stony Brook, NY, (2005) 11794-2350.

48. Zaiane, O., Nascimento, M. ve Oliveira, S., Digital Watermarking: Status, Limitations and Prospects, (2002).

49. Naderahmadian, Y. ve Hosseini-Khayat, S., Fast and robust watermarking in still images based on QR decomposition, Multimedia tools and applications, 72,3 (2014) 2597-2618.

50. Singh, P. ve Chadha, R. S., A Survey Of Digital Watermarking Techniques, Applications and Attacks, International Journal of Engineering and Innovative Technology (IJEIT), 2,9 (2013) 165-175.

51. Santoyo-Garcia, H., Fragoso-Navarro, E., Reyes-Reyes, R., Cruz-Ramos, C. ve Nakano-Miyatake, M., Visible watermarking technique based on human visual system for single sensor digital cameras, Security and Communication Networks, 2017,(2017).

52. Perez-Daniel, K. R., Garcia-Ugalde, F. ve Sanchez, V., Watermarking of HDR Images in the Spatial Domain With HVS-Imperceptibility, IEEE Access, 8,(2020) 156801-156817.

53. Thanki, R. ve Borra, S., Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing, Multimedia Tools and Applications, 78,10 (2019) 13905-13924.

54. Dutta, M. K., Gupta, P. ve Pathak, V. K. Biometric based unique key generation for authentic audio watermarking, International Conference on Pattern Recognition and Machine Intelligence, 2009, Springer, 458-463.

55. Dutta, M. K., Gupta, P. ve Pathak, V. K., Audio watermarking using pseudorandom sequences based on biometric templates, JCP, 5,3 (2010) 372-379.

56. Dutta, M. K., Singh, A. ve Burget, R., Digital ownership tags based on biometric features of iris and fingerprint for content protection and ownership of digital images and audio signals, Multimedia Tools and Applications, 75,23 (2016) 16287-16313.

57. Wójtowicz, W. ve Ogiela, M. R., Digital images authentication scheme based on bimodal biometric watermarking in an independent domain, Journal of Visual Communication and Image Representation, 38,(2016) 1-10.

58. Sarode, N. S. ve Patil, A., Review of iris recognition: an evolving biometrics identification technology, International Journal of Innovative Science and Modern Engineering, 2,10 (2014) 34-40.

59. Majumder, S., Singh, A. D. ve Mishra, M. A GUI based Iris authentication system for secured access, Int. Conf. Systemics, Cybernetics, Informatics (ICSCI-2009) under Pentagram Research, Hyderabad held, 2009, 7-10.

60. Bansal, R., Sehgal, P. ve Bedi, P., Securing fingerprint images using PSO-based wavelet domain watermarking, Information Security Journal: A Global Perspective, 21,2 (2012) 88-101.

61. Vatsa, M., Singh, R. ve Noore, A., Feature based RDWT watermarking for multimodal biometric system, Image and Vision Computing, 27,3 (2009) 293-304.

62. Revathi, A., Sasikaladevi, N. ve Jeyalakshmi, C., Digital speech watermarking to enhance the security using speech as a biometric for person authentication, International Journal of Speech Technology, 21,4 (2018) 1021-1031.

63. Thanki, R. M. ve Kothari, A. M., Hybrid domain watermarking technique for copyright protection of images using speech watermarks, Journal of Ambient Intelligence and Humanized Computing, 11,5 (2020) 1835-1857.

64. Dutta, M. K., Singh, A., Soni, K. M., Burget, R. ve Riha, K. Watermark generation from fingerprint features for digital right management control, 2013 36th International Conference on Telecommunications and Signal Processing (TSP), 2013, IEEE, 717-721.

65. Rao, N. N., Thrimurthy, P. ve Babu, B. R. An efficient copyright protection scheme for digital images using biometrics and watermarking, 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009, IEEE, 69-74.

66. Shaw, A. K., Majumder, S., Sarkar, S. ve Sarkar, S. K., A novel EMD based watermarking of fingerprint biometric using GEP, Procedia Technology, 10,(2013) 172-183.

67. Agarwal, H., Raman, B. ve Venkat, I., Blind reliable invisible watermarking method in wavelet domain for face image watermark, Multimedia Tools and Applications, 74,17 (2015) 6897-6935.

68. Wójtowicz, W. ve Ogiela, M. R., Biometric watermarks based on face recognition methods for authentication of digital images, Security and Communication Networks, 8,9 (2015) 1672-1687.

69. Dutta, M. K., Singh, A. ve Zia, T. A. An efficient and secure digital image watermarking using features from iris image, 2013 International Conference on Control Communication and Computing (ICCC), 2013, IEEE, 451-456.

70. Dutta, M. K., Singh, A., Burget, R., Atassi, H., Choudhary, A. ve Soni, K. M. Generation of biometric based unique digital watermark from iris image, 2013 36th International Conference on Telecommunications and Signal Processing (TSP), 2013, IEEE, 685-689.

71. Majumder, S., Devi, K. J. ve Sarkar, S. K., Singular value decomposition and wavelet-based iris biometric watermarking, IET biometrics, 2,1 (2013) 21-27.

72. Lu, J., Qu, T. ve Karimi, H. R., Novel iris biometric watermarking based on singular value decomposition and discrete cosine transform, Mathematical Problems in Engineering, 2014,(2014).

73. Umar, M. M., Mehmood, A., Song, H. ve Choo, K.-K. R., I-Marks: An iris code embedding system for ownership identification of multimedia content, Computers & Electrical Engineering, 63,(2017) 209-219.

74. Thanki, R., Dwivedi, V. V. ve Borisagar, K., Robust watermarking technique using different wavelet decomposition levels for signature image protection, Journal of Information and Communication Technology, 16,1 (2017) 157-174.

75. Zhou, Z., Chen, S. ve Wang, G. A robust digital image watermarking algorithm based on DCT domain for copyright protection, International Symposium on Smart Graphics, 2015, Springer, 132-142.

76. Su, Q., Wang, G., Jia, S., Zhang, X., Liu, Q. ve Liu, X., Embedding color image watermark in color image based on two-level DCT, Signal, Image and Video Processing, 9,5 (2015) 991-1007.

77. Sahraee, M. ve Ghofrani, S., A robust blind watermarking method using quantization of distance between wavelet coefficients, Signal, Image and Video Processing, 7,4 (2013) 799-807.

78. Sharmin, S., Khaliluzzaman, M., Mahiuddin, M. ve Kafi, A., Blind Digital Image Watermarking for Copyright Protection Based on Hadamard Transform, in *Emerging Technologies in Data Mining and Information Security*. 2019, Springer. p. 215-225.

79. Jia, S., Zhou, Q. ve Zhou, H., A novel color image watermarking scheme based on DWT and QR decomposition, Journal of Applied Science and Engineering, 20,2 (2017) 193-200.

80. Rahman, M. M., Ahammed, M. S., Ahmed, M. R. ve Izhar, M. N., A semi blind watermarking technique for copyright protection of image based on DCT and SVD domain, Global Journal of Research In Engineering, (2017).

81. Kaur, S. ve Sidhu, R. K., Robust digital image watermarking for copyright protection with SVD–DWT–DCT and Kalman filtering, International Journal Emerging Technologies in Engineering Research, 4,1 (2016) 59-63.

82. Lai, C.-C., An improved SVD-based watermarking scheme using human visual characteristics, Optics Communications, 284,4 (2011) 938-944.

83. Dharwadkar, N. V., Amberker, B. ve Gorai, A. Non-blind watermarking scheme for color images in RGB space using DWT-SVD, 2011 International Conference on Communications and Signal Processing, 2011, IEEE, 489-493.

84. Elshazly, E. H., Faragallah, O. S., Abbas, A. M., Ashour, M. A., El-Rabaie, E.-S. M., Kazemian, H., Alshebeili, S. A., Abd El-Samie, F. E. ve El-sayed, H. S., Robust and secure fractional wavelet image watermarking, Signal, Image and Video Processing, 9,1 (2015) 89-98.

85. Sadreazami, H. ve Amini, M., A robust spread spectrum based image watermarking in ridgelet domain, AEU-International Journal of Electronics and Communications, 66,5 (2012) 364-371.

86. Liu, Y., Wang, Y. ve Zhu, X., Novel robust multiple watermarking against regional attacks of digital images, Multimedia Tools and Applications, 74,13 (2015) 4765-4787.

87. Loukhaoukha, K., Chouinard, J.-Y. ve Taieb, M. H., Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization, Journal of Information Hiding and Multimedia Signal Processing, 2,4 (2011) 303-319.

88. Loukhaoukha, K., Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain, Journal of Optimization, 2013,(2013).

89. Ali, M., Ahn, C. W., Pant, M. ve Siarry, P., An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony, Information Sciences, 301,(2015) 44-60.

90. Ansari, I. A., Pant, M. ve Ahn, C. W., Robust and false positive free watermarking in IWT domain using SVD and ABC, Engineering Applications of Artificial Intelligence, 49,(2016) 114-125.

91. Chen, Y., Yu, W. ve Feng, J., A reliable svd-dwt based watermarking scheme with artificial bee colony algorithm, International Journal of Digital Content Technology and its Applications, 6,22 (2012) 430.

92. Ali, M. ve Ahn, C. W., An optimal image watermarking approach through cuckoo search algorithm in wavelet domain, International Journal of System Assurance Engineering and Management, 9,3 (2018) 602-611.

93. Aslantas, V., SVD and DWT-SVD domain robust watermarking using differential evolution algorithm, in *Advances in Electrical Engineering and Computational Science*. 2009, Springer. p. 147-159.

94. Ali, M., Ahn, C. W. ve Siarry, P., Differential evolution algorithm for the selection of optimal scaling factors in image watermarking, Engineering Applications of Artificial Intelligence, 31,(2014) 15-26.

95. Ali, M., Ahn, C. W. ve Pant, M., A robust image watermarking technique using SVD and differential evolution in DCT domain, Optik, 125,1 (2014) 428-434.

96. Mishra, A., Agarwal, C., Sharma, A. ve Bedi, P., Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm, Expert Systems with Applications, 41,17 (2014) 7858-7867.

97. Kazemivash, B. ve Moghaddam, M. E., A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm, Multimedia Tools and Applications, 76,20 (2017) 20499-20524.

98. Kazemivash, B. ve Moghaddam, M. E., A predictive model-based image watermarking scheme using Regression Tree and Firefly algorithm, Soft Computing, 22,12 (2018) 4083-4098.

99. Moeinaddini, E. ve Afsari, F., Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm, Multimedia Tools and Applications, 77,19 (2018) 26083-26105.

100. Moeinaddini, E., Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm, Soft Computing, 23,19 (2019) 9685-9699.

101. Aslantas, V., A singular-value decomposition-based image watermarking using genetic algorithm, AEU-International Journal of Electronics and Communications, 62,5 (2008) 386-394.

102. Lai, C.-C., Yeh, C.-H., Ko, C.-H. ve Chiang, C.-Y. Image watermarking scheme using genetic algorithm, 2012 Sixth International Conference on Genetic and Evolutionary Computing, 2012, IEEE, 476-479.

103. Mingzhi, C., Yan, L., Yajian, Z. ve Min, L., A combined dwt and dct watermarking scheme optimized using genetic algorithm, Journal of multimedia, 8,3 (2013) 299-305.

104. Run, R.-S., Horng, S.-J., Lai, J.-L., Kao, T.-W. ve Chen, R.-J., An improved SVD-based watermarking technique for copyright protection, Expert Systems with applications, 39,1 (2012) 673-689.

105. Ansari, I. A. ve Pant, M. SVD watermarking: particle swarm optimization of scaling factors to increase the quality of watermark, Proceedings of Fourth International Conference on Soft Computing for Problem Solving, 2015, Springer, 209-218.

106. Altay, Ş. Y. ve Ulutaş, G. DWT-QR based blind image watermarking method using firefly algorithm, 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, IEEE, 1-4.

107. Altay, Ş. Y. ve Ulutaş, G. A Lwt-Firefly Algorithm Based Approach for Smooth Images Watermarking, 2019 4th International Conference on Computer Science and Engineering (UBMK), 2019, IEEE, 1-6.

108. Nair, S. A. H. ve Aruna, P., Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems, Alexandria Engineering Journal, 54,4 (2015) 1161-1174.

109. Paunwala, M. ve Patnaik, S., Biometric template protection with DCT-based watermarking, Machine vision and applications, 25,1 (2014) 263-275.

110. Singh, P., Raman, B. ve Roy, P. P., A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform, Multimedia Tools and Applications, 76,3 (2017) 3871-3897.

111. Thanki, R., Dwivedi, V., Borisagar, K. ve Borra, S., A watermarking algorithm for multiple watermarks protection using SVD and compressive sensing, Informatica, 41,4 (2017).

112. Altay, Ş. Y. ve Ulutaş, G., Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain, Multimedia Tools and Applications, (2021) 1-28.

113. Chung, K.-L., Yang, W.-N., Huang, Y.-H., Wu, S.-T. ve Hsu, Y.-C., On SVD-based watermarking algorithm, Applied Mathematics and Computation, 188,1 (2007) 54-57.

114. Fan, M.-Q., Wang, H.-X. ve Li, S.-K., Restudy on SVD-based watermarking scheme, Applied Mathematics and Computation, 203,2 (2008) 926-930.

115. Mishra, M., Mishra, P., Adhikary, M. ve Kumar, S., Image encryption using Fibonacci-Lucas transformation, International Journal on Cryptography and Information Security (IJCIS), 2,3 (2012) 131-141.

116. Yang, X.-S., Nature-inspired metaheuristic algorithms, Luniver press, 2010.

117. Kaur, R. ve Rattan, M., Optimization of the return loss of differentially fed microstrip patch antenna using ANN and firefly algorithm, Wireless Personal Communications, 80,4 (2015) 1547-1556.

118. Rahebi, J. ve Hardalaç, F., A new approach to optic disc detection in human retinal images using the firefly algorithm, Medical & biological engineering & computing, 54,2-3 (2016) 453-461.

119. Ijyas, V. T. ve Sameer, S., Firefly algorithm for joint estimation of frequency offsets and channel in OFDMA uplink, Wireless personal communications, 79,1 (2014) 565-580.

120. Ali, E., Speed control of DC series motor supplied by photovoltaic system via firefly algorithm, Neural Computing and Applications, 26,6 (2015) 1321-1332.

121. Yang, X.-S., Firefly algorithm, stochastic test functions and design optimisation, International journal of bio-inspired computation, 2,2 (2010) 78-84.

122. Zhang, L., Liu, L., Yang, X.-S. ve Dai, Y., A novel hybrid firefly algorithm for global optimization, PloS one, 11,9 (2016) e0163230.

123. Fister, I., Fister Jr, I., Yang, X.-S. ve Brest, J., A comprehensive review of firefly algorithms, Swarm and Evolutionary Computation, 13,(2013) 34-46.

124. Yu, S., Yang, S. ve Su, S., Self-adaptive step firefly algorithm, Journal of Applied Mathematics, 2013,(2013).

125. Monro, D. M. ve Zhang, Z. An effective human iris code with low complexity, IEEE International Conference on Image Processing 2005, 2005, IEEE, III-277.

126. Rakshit, S. ve Monro, D. M. Effects of sampling and compression on human iris verification, 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, 2006, IEEE, II-II.

127. Li, L., Xu, H.-H., Chang, C.-C. ve Ma, Y.-Y., A novel image watermarking in redistributed invariant wavelet domain, Journal of Systems and Software, 84,6 (2011) 923-929.

128. Ganesan, P., Rajini, V., Sathish, B., Kalist, V. ve Basha, S. K., Satellite image segmentation based on YCbCr color space, Indian Journal of Science and Technology, 8,1 (2015) 35.

129. Dharwadkar, N. V., Kulkarni, G. K., Melligeri, T. ve Amberker, B., The image watermarking scheme using edge information in YCbCr color space, International Proceedings of Computer Science and Information Technology, 56,(2012) 127.

130. Roy, A., Maiti, A. K. ve Ghosh, K., An HVS inspired robust non-blind watermarking scheme in YCbCr color space, International Journal of Image and Graphics, 18,03 (2018) 1850015.

131. Koju, R. ve Joshi, S. R., Comparative analysis of color image watermarking technique in rgb, yuv, and ycbcr color channels, Nepal Journal of Science and Technology, 15,2 (2014) 133-140.

132. Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W. ve Xiong, N. N., A robust watermarking scheme in YCbCr color space based on channel coding, IEEE Access, 7,(2019) 25026-25036.

133. Kang, X.-b., Zhao, F., Lin, G.-f. ve Chen, Y.-j., 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, 77,11 (2018) 13197-13224.

134. Pourhadi, A. ve Mahdavi-Nasab, H., A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain, Multimedia Tools and Applications, 79,(2020) 21653-21677.

135. Tarif, E. B., Wibowo, S., Wasimi, S. ve Tareef, A., A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system, Multimedia Tools and Applications, 77,2 (2018) 2485-2503.

136. Singh, C. ve Ranade, S. K., A high capacity image adaptive watermarking scheme with radial harmonic Fourier moments, Digital signal processing, 23,5 (2013) 1470-1482.

137. Hosny, K. M. ve Darwish, M. M., Invariant image watermarking using accurate polar harmonic transforms, Computers & Electrical Engineering, 62,(2017) 429-447.

138. Xu, H., Kang, X., Chen, Y. ve Wang, Y., Rotation and scale invariant image watermarking based on polar harmonic transforms, Optik, 183,(2019) 401-414.

ÖZGEÇMİŞ

İlk, orta ve lise öğrenimini Erzurum'da tamamladı. Karadeniz Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde lisans programına başladı ve 2010 yılında bu bölümden mezun oldu. Atatürk Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans öğrenimine başladı. Aynı yıl Atatürk Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak göreve başladı. Atatürk Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans öğrenimini tamamladı. Yabancı dil olarak iyi seviyede İngilizce bilmektedir.

SCI/SCI-E indekslerine giren dergilerde yayınlanan makaleler

1. Yücel Altay, Ş. ve Ulutaş, G., Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain, Multimedia Tools and Applications, (2021), https://doi.org/10.1007/s11042-020-10251-7.

SCI/SCI-E indekslerine giren dergilerde incelemede olan makaleler

1. Yücel Altay, Ş. ve Ulutaş, G., Biometric watermarking schemes based on QR decomposition and Schur decompositon in RIDWT domain, Ambient Intelligence and Humanized Computing.

Diğer dergilerde yayınlanan makaleler

1. Yücel Altay, Ş. ve Ulutaş, G., Sayısal görüntülerin telif hakkının korunması için iris tabanlı biyometrik damgalama yaklaşımı, Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi, 23,68, (2021) 531-546.

Uluslararası konferanslar kapsamında yapılan yayınlar

1. Yücel Altay, Ş. ve Ulutaş, G., A lwt-firefly algorithm based approach for smooth images watermarking, 2019 4th International Conference on Computer Science and Engineering (UBMK), 2019, IEEE, 1-6.
2. Yücel Altay, Ş. ve Ulutaş, G., Dwt-QR based blind image watermarking method using firefly algorithm, 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, IEEE, 1-4.