KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

SAYISAL GÖRÜNTÜLERDE KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

DOKTORA TEZİ

Gül TAHAOĞLU

KASIM 2021
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

SAYISAL GÖRÜNTÜLERDE KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

Gül TAHAOĞLU
ORCID : - - -

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

Tezin Enstitüye Verildiği Tarih : 13 / 10 /2021
Tezin Savunma Tarihi : 03 / 11 /2021

Tez Danışmanı : Doç. Dr. Güzin ULUTAŞ
ORCID : - - -

Trabzon 2021

ÖNSÖZ

Artan teknolojik gelişmelerle birlikte sayısal görüntülerin oluşturulması, iletilmesi ve kullanım alanlarında artış görülmüştür. Bununla birlikte sayısal görüntüler üzerinde değişiklik yapılmasına imkân sağlayan görüntü düzenleme yazılımlarının kullanımı kolaylaşmış ve daha sık kullanılır hale gelmiştir. Tıp, gazetecilik, hukuk gibi önemli alanlarda başvurulabilen sayısal görüntülerin, üzerinde herhangi bir değişiklik yapılıp yapılmadığının kontrolü (doğrulanması) önemli bir ihtiyaç haline gelmiştir. Bu tez çalışmasında yeni yaklaşımlar ile sayısal görüntülerde sıklıkla karşılaşılan kopyala-yapıştır sahteciliği tespitine ilişkin pasif görüntü doğrulama sistemi tasarlanmıştır.

Lisansüstü eğitimim boyunca danışmanlığımı üstlenen, her türlü destek ve katkılarıyla akademik bakış açımın gelişmesi konusunda emeğini esirgemeden beni yönlendiren, doktora sürecinin keyifli ilerlemesine imkân sağlayan çok değerli danışman hocam Sayın Doç. Dr. Güzin ULUTAŞ' a sonsuz teşekkürlerimi bir borç bilirim. Önerileriyle çalışmama katkıda bulunan tez izleme komitesi üyeleri hocalarım Prof. Dr. Vasıf NABİYEV' e ve Prof. Dr. Erhan COŞKUN' a teşekkürlerimi sunarım. Tez çalışması sırasında gerçekleştirilen 119E045 numaralı 1001 projesi ile maddi olarak beni destekleyen Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)'a teşekkürlerimi sunarım. Proje ekibinde yer alan diğer hocalarım ve arkadaşlarıma da şükranlarımı sunarım.

Doktora eğitimimde varlığı ile güç aldığım sevgili oğlum Kerem Batur'a, aileme ve dostlarıma teşekkürlerimi sunarım.

Bu tezin bundan sonraki çalışmalara katkı sağlaması temennisiyle.

Gül TAHAOĞLU

Trabzon, 2021

TEZ ETİK BEYANNAMESİ

Doktora Tezi olarak sunduğum “Sayısal Görüntülerde Kopyala-Yapıştır Sahteciliği Tespiti” başlıklı bu çalışmayı baştan sona kadar danışmanım Doç. Dr. Güzin ULUTAŞ’ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuvarlarda yaptığımı, 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. 13/10/2021

Gül TAHAOĞLU

İÇİNDEKİLER

Sayfa No

Doktora Tezi

ÖZET

SAYISAL GÖRÜNTÜLERDE KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

Gül TAHAOĞLU

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Güzin ULUTAŞ
2021, 156 Sayfa

Sayısal görüntüler üzerinde en sık karşılaşılan sahtecilik türlerinden biri kopyala-yapıştır sahteciliğidir. Tez çalışmasında kopyala-yapıştır sahteciliği tespiti yöntemlerindeki problemler irdelenmiş ve bu problemlerin üstesinden gelecek şekilde sahtecilik uygulanan görüntüleri tespit edebilecek yeni yöntemler önerilmiştir. Yapılan çalışmaların ilkinde görüntü L*a*b* renk uzayından değerlendirilmiş ve her bir renk kanalından çıkarılan anahtar noktaları aracılığıyla taslak sahte bölgeler belirlenmiştir. Sahte bölgenin kesin sınırlarının çizilmesinde, girdi görüntüsünden bağımsızlığı sağlayan dinamik lokalizasyon aşaması önerilmiştir. Önerilen ikinci yöntemde görüntünün dönme bağımsız özelliğini koruyan doku görüntüsü elde edilmiştir. Doku görüntüsünün bütününden elde edilen anahtar noktalarını birbiri ile eşleştirilerek şüpheli taslak bölgeler oluşturulmuştur. Taslak bölgelerde yer alan sahtecilik sınırların belirlenmesinde Ciratefi tabanlı bir yaklaşım sunulmuştur. Tez kapsamında önerilen yaklaşımlarla farklı atak tiplerine karsı (döndürme, ölçekleme, JPEG sıkıştırma, gürültü ekleme) dayanıklılık sağlanmıştır. Böylece uzman bir sistemden beklenir şekilde doğruluk oranları ile sahte görüntüler tespit edilmiştir. Önerilen kopyala-yapıştır sahteciliği tespit yöntemlerinden elde edilen sonuçların literatürdeki benzer çalışmalarla benzer çalışmalarla kıyaslaması gerçekleştirilerek üstünlükleri ortaya konmuştur.

Anahtar Kelimeler: Kopyala-Yapıştır Sahteciliği Tespiti, Pasif Yöntemler, Görüntü Sahteciliği, Sahtecilik Sınırlarının Belirlenmesi

Ph. D. Thesis

SUMMARY

COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES

Gül TAHAOĞLU

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Assoc. Prof. Güzin ULUTAŞ
2021, 156 Pages

One of the most common types of forgery on digital images is copy-move forgery. In the thesis study, the problems in copy-move forgery detection methods are examined and new methods are proposed to detect forged images to overcome these problems. In the first of the studies, the image was evaluated from the L*a*b* color space and the forged regions were determined roughly by the keypoints extracted from each color channel. A dynamic localization step is proposed, which provides independence from the input image, in delineating the precise boundaries of the forged region. In the second proposed method, a texture image that preserves the rotation-invariant feature of the image is obtained. Suspicious regions were created by matching the keypoints obtained from the whole texture image with each other. A Ciratefi-based approach is presented in determining the forgery limits in the roughly forged regions. With the approaches proposed in the thesis, robustness against different attack types (rotation, scaling, JPEG compression, noise addition) is provided. Thus, forged images were detected with the accuracy rates expected from an expert system. The results obtained from the proposed copy-paste fraud detection methods were compared with similar studies in the literature and their advantages were demonstrated.

Key Words: Copy-move Forgery Detection, Passive Methods, Image Forgery, Determining Tampering Regions

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

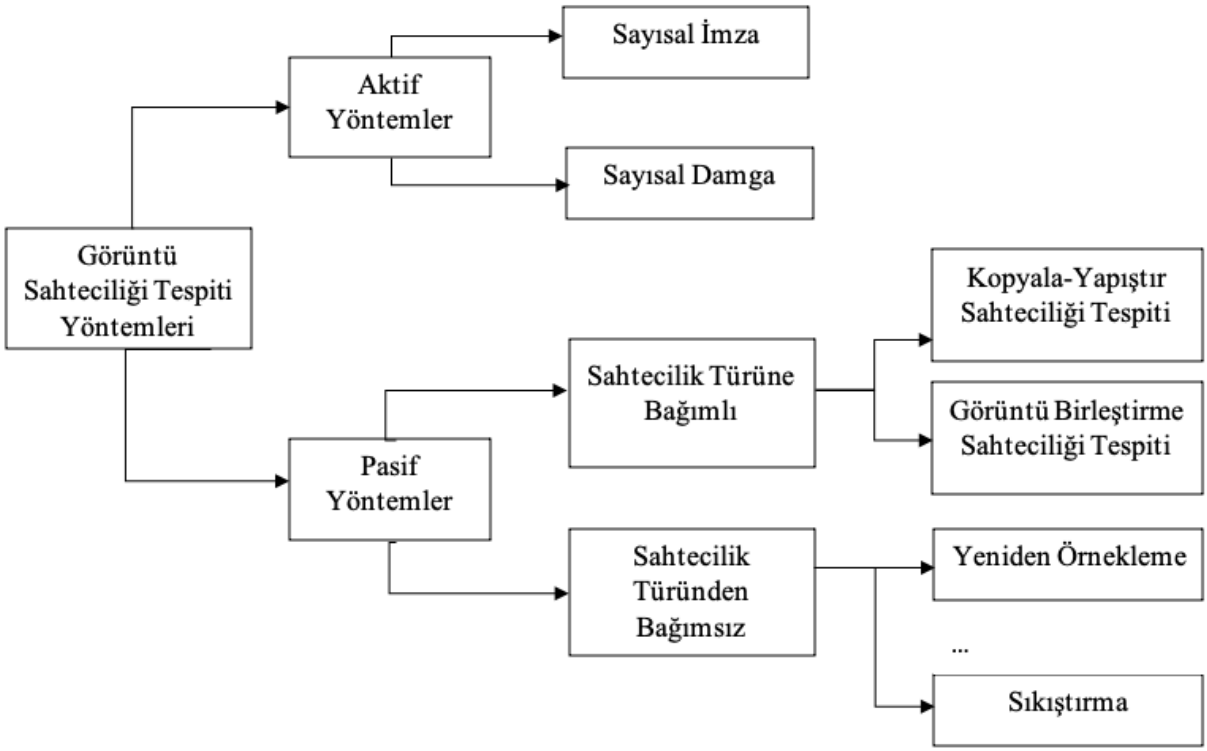
ADD	Ayrık Dalgacık Dönüşümü
AFD	Ayrık Fourier Dönüşümü
AKD	Ayrık Kosinüs Dönüşümü (DCT)
AWGN	Additive White Gaussian Noise
BBE	Bağlı Bileşen Etiketleme
BBF	Best Bin First
BRISK	Binary Robust Invariant Scalable Keypoints
CDF	Kümülatif Dağılım Fonksiyonu
DPO	Doğru Pozitif Oranı
DoG	Difference of Gausssian
g2NN	generalized 2 Nearest Neighbour
HSV	Hue Saturation Value
LBP	Local Binary Pattern
LBPROT	Rotation-invariant LBP
ORB	Oriented Fast and Robust BRIEF
RANSAC	Random Sample Consensus
RGB	Red Gren Blue
SIFT	Scale Invariant Feature Transform
SLIC	Simple Linear Iterative Clustering
SURF	Speeded Up Robust Feature
TBA	Temel Bileşenler Analizi
YPO	Yanlış Pozitif Ora

1. GENEL BİLGİLER

1.1. Giriş

Son yıllarda sayısal ortamların kullanımının giderek yaygınlaşması ve bu ortamların düzenlenmesinde faydalanılan yazılımların (Photoshop, GIMP) sayısındaki artış, doğrulama problemini beraberinde getirmiştir. Sayısal görüntülerin, günümüzde birçok alanda kullanımı mevcuttur. Özellikle adli olayların değerlendirilmesinde sayısal görüntülerin kullanımında artış yaşanmaktadır. Adli bir olayda, suçun aydınlatılmasında ve failinin tespitinde kullanılan en önemli mekanizma delillendirmedir [1]. Delil teşkil edecek sayısal görüntünün mahkeme esnasında kanıt olarak değerlendirilebilmesi için, görüntünün oluşturulduğu andan itibaren değiştirilip değiştirilmediğinin kontrolü oldukça önem arz etmektedir.

Sayısal görüntü doğrulama amacıyla literatürde birçok yöntem önerilmiştir. Şekil 1.1'de de görüleceği üzere temelde bu yöntemler aktif ve pasif doğrulama yöntemleri olmak üzere iki ana kategoride değerlendirilmektedir [2]. Aktif yöntemler kendi içerisinde sayısal damgalama ve sayısal imzalama olmak üzere iki alt kategoriye ayrılmaktadır. Telif hakkı koruma, kimlik tespiti, kopya engelleme, yayın denetleme ve verinin gerçekliğini kanıtlama gibi birçok alanda kullanılabilen sayısal damgalama, özel oluşturulmuş damga bilgisinin görüntü içine gizlenmesi temeline dayanmaktadır. Çıkarılan damga bilgisinin kontrolünün yapılmasıyla görüntünün bir değişime uğrayıp uğramadığı hakkında bilgi edinilmektedir [3, 4]. Damga bilgisinin görüntü oluşturulurken görüntünün içerisine yerleştirilmesi işleminin özel donanımlı kameralar veya sonradan yetkili yazılımlarca yapılmasına ihtiyaç duyulması, sayısal damgalama yöntemlerinin dezavantajı olarak ortaya çıkmaktadır. Aktif yöntemlerin bir diğer kategorisi de sayısal imzalardır ve sayısal damgalamaya benzer şekilde, özel oluşturulmuş bir verinin iletimini gerektirmesi ve özel yazılımlara ihtiyaç duyması sebebi ile benzer dezavantaj içermektedir. Aktif yöntemlerde var olan bu dezavantajlardan dolayı pasif doğrulama yöntemleri önerilmiştir.



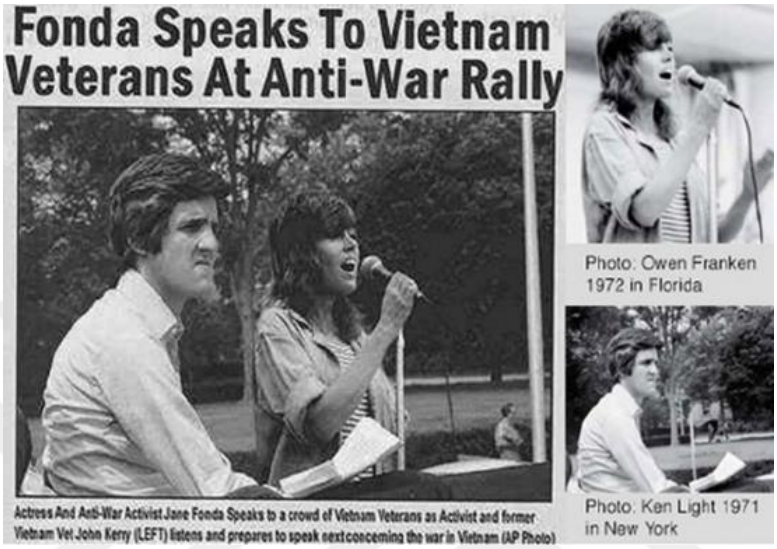
Şekil 1.1. Görüntü sahteciliği tespiti yöntemleri

1.2. Pasif Görüntü Doğrulama Yöntemleri

Pasif görüntü doğrulama yöntemlerinde, görüntünün doğruluğunun ortaya konmasında görüntüden çıkarılan istatistiksel özellikler kullanılmakta ve görüntü harici ekstra veri gereksinime ihtiyaç duyulmamaktadır [5]. Bu yöntemler, sahtecilik türünden bağımsız ve sahtecilik türüne bağımlı olarak iki gruba ayrılmaktadır. Sahtecilik türünden bağımsız yöntemler, görüntüde değişiklik yapıldıktan sonra uygulanan JPEG sıkıştırma, görüntü yeniden boyutlandırma gibi işlemlere ait izleri kullanarak doğrulama işlemini gerçekleştirmektedir. Sahtecilik tipine bağlı yöntemler ise görüntü birleştirme sahteciliği ve kopyala-yapıştır sahteciliği olarak iki sınıfta değerlendirilmektedir.

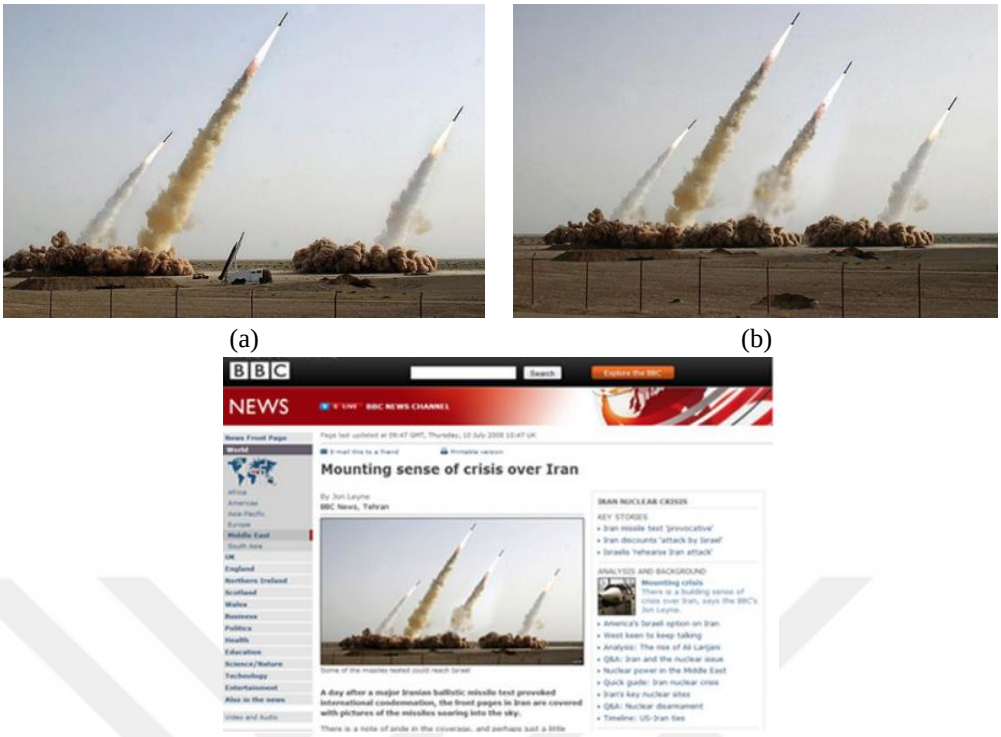
Görüntü birleştirme sahteciliği en az iki görüntüden alınan bölgelerin birleştirilmesi ile tek bir görüntü oluşturulması işlemidir. Farklı görüntülerden alınan bölgelerin öznitelikleri eklendiği orijinal görüntüye göre değişiklik göstererek belli tutarsızlıklara (kenar, gürültü, aydınlatma vs.) neden olacaktır. Bu tutarsızlıklar sahte görüntü tespitinde kullanılmaktadır. Şekil 1.2’ de bir haber gazetesinde yer alan görüntü birleştirme sahteciliği uygulanmış görüntü yer almaktadır [6]. Görüntü birleştirme sahteciliği tespit yöntemleri

bölge tabanlı ve sınır tabanlı tespit yöntemleri olarak ikiye ayrılmaktadır. Sınır tabanlı yöntemler birleştirme sınırlarındaki değişimleri algılamaktadırlar [7,8]. Bölge tabanlı yöntemler ise, sahteciliği tespit edebilmek için orijinal ve birleştirilmiş görüntülerden oluşturulan üretici modelde tutarlılık kontrolü yapmaktadırlar [9-12].



Şekil 1.2. Görüntü birleştirme sahteciliği örneği [6]

Kopyala-yapıştır sahteciliği, sayısal görüntüde bir bölgenin kopyalanması ve yine aynı görüntüye yapıştırılması ile gerçekleştirilen popüler bir sahtecilik türüdür. Bu sahtecilik yöntemi görüntü düzenleme yazılımlarının kullanılması ile insan gözünün fark edebileceği sahtecilik izleri bırakılmadan kolay bir şekilde gerçekleştirilebilmektedir. Kopyala-yapıştır sahteciliğindeki amaç genellikle bir objenin/bölgenin gizlenmesi veya çoğaltılmasıdır. Şekil 1.3' te bu sahteciliğe ilişkin bir örnek verilmiştir [13]. Şekil 1.3(a)'da orijinal görüntü yer alırken, mavi tabelanın kopyalanıp yapıştırılması ile Şekil 1.3(b)'deki sahte görüntü oluşturulmuştur.



Şekil 1.3. Kopyala-yapıştır sahteciliği örneği (a) Orijinal görüntü (b) Sahte görüntü (c) Sahte görüntünün yer aldığı basın yayını

Kopyala-yapıştır sahteciliği uygulanmış görüntünün yapısal analizi gerçekleştirildiğinde, kopyalanıp yapıştırılan bölgeler arasında yüksek oranda benzerlik gözlemlenmektedir. Bu benzerlik izlerini gidermek ve sahteciliğin tespitini zorlaştırmak amacı ile sahte görüntünün oluşturulmasında uygulanabilecek dönme, ölçekleme, gürültü ekleme, JPEG sıkıştırma, bulanıklaştırma ataklarının olabileceği, literatürde yer almaktadır. Ayrıca düşük kontrasta sahip bölgelerin (düz bölge/dokusuz bölge) ayırt ediciliğinin düşük olması sebebi ile sahtecilik gerçekleştirilirken kopyalanıp yapıştırılacak bölgenin bu tür bir bölgeden seçilmesi durumu, sahteciliğin tespitini zor hale getirmektedir. Önerilen sahtecilik tespiti yöntemlerinin bahsedilen ataklara karşı dayanıklılığı tartışılmakta ve değerlendirilmektedir. Literatürde kopyala-yapıştır sahteciliğinin tespiti için önerilen yöntemler, başlıca blok tabanlı yöntemler ve anahtar noktası tabanlı yöntemler olarak sınıflandırılmaktadır. Ayrıca bu iki yöntemdeki temel işlem adımlarının hibrit bir şekilde kullanılmasını öneren hibrit yaklaşımlar da bulunmaktadır. Anahtar noktası tabanlı yöntemler, ilk önerildiği zamanlarda sadece görüntünün sahte olup olmadığını ortaya koyan, ikili (binary) karar veren sistemlerdi. Daha sonra sahte bölgenin piksel bazlı işaretlemesini sağlayan çalışmalar önerildi. Tez kapsamında, kopyala-yapıştır sahteciliği uygulanmış

görüntülerde, görüntülerin sahte ve orijinal olarak sınıflandırılmasının ardından görüntünün sahte olması durumunda, sahte bölgelerin işaretlenmesi üzerinde çalışılmıştır. Bu alanda gerçeklenmesi amaçlanan hedefler aşağıdaki şekilde özetlenebilir.

1. Görüntü doğrulama performansının iyileştirilmesi
2. Sahte bölgelerin, bölge özelliğinden (dokulu/dokusuz) bağımsız bir şekilde tespit edilebilmesi
3. Önerilen yöntemin sahte görüntüler üzerinde uygulanabilecek farklı atak tiplerine karşı dayanıklılık göstermesi
4. Sahte bölge işaretleme performansının iyileştirilmesi

Yapılan çalışmalarda verilen hedefler doğrultusunda yüksek performans ile görüntü doğrulama ve sahte bölge işaretlemesi için literatüre katkı sağlayacak yeni yaklaşımlar önerilmiştir.

1.3. Tezin Kapsamı

Tez kapsamında pasif görüntü doğrulama yöntemleri tarafından değerlendirilen kopyala-yapıştır sahteciliği uygulanmış görüntülerin doğrulamasını gerçekleştiren ve görüntüdeki sahte bölgeleri tespit eden bir sistemin tasarımı gerçekleştirilmiştir.

Kopyala-yapıştır sahteciliği alanında literatürde yapılan çalışmaların kısaca tanımlamaları ve literatür taraması, genel bilgiler bölümünün bir sonraki alt başlığında verilecektir.

Yapılan çalışmalar kısmında sonuçlardan bağımsız olarak kopyala-yapıştır sahteciliği tespiti için önerilen çalışmalara ilişkin detaylar sunulacaktır. Tezde yer alan çalışmalar iki ana başlık altında toplanmıştır. İlk kısımda L*a*b renk uzayından faydalanarak anahtar noktası tabanlı şüpheli bölgelerin çıkarılması ve dinamik bir lokalizasyon yaklaşımı ile sahtecilik tespiti şeması önerilmiştir. Önerilen yöntemde RGB renk uzayında tanımlı girdi görüntüsünün L*a*b* renk uzayına dönüştürülmesi ve bu kanallardaki temsillerinden SIFT anahtar noktalarının çıkarılması gerçekleştirilmiştir. Her bir kanaldan çıkarılan anahtar noktaları kendi içerisinde eşleştirilmiş ve sahtecilik durumunu işaret eden yeterli eşleşmenin varlığının kontrolü ile girdi görüntüsünün doğrulanması gerçekleştirilmiştir. Eşleşen anahtar noktaların konumlarından faydalanarak şüpheli bölgeler belirlenmiş, ardından önerilen yeni bir lokalizasyon yaklaşımı ile sahte bölgelerin piksel bazında işaretlemesi gerçekleştirilmiştir.

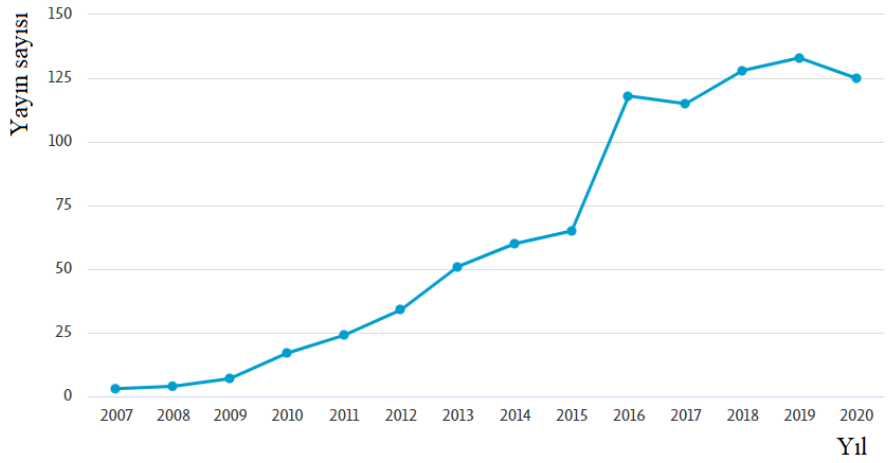
Yapılan çalışmalar bölümünün ikinci kısmında ise LBPROT ve SIFT yöntemine dayalı şüpheli bölge çıkarımı ve Ciratefi tabanlı lokalizasyon yaklaşımı ile sahtecilik tespiti yöntemi önerilmiştir. LBPROT operatörünün kullanımı ile girdi görüntüsünün dönme bağımsız doku görüntüsünün elde edilmesinin ardından SIFT anahtar noktaları çıkarılmıştır. Bir önceki yönteme benzer şekilde anahtar noktalarının eşleştirilmesi ile yeterli sayıda eşleşmenin kontrolü sonrası görüntünün doğrulanması gerçekleştirilmiştir. Görüntünün sahte olması söz konusu ise doğru eşleşen anahtar noktalarından faydalanara şüpheli bölgelere ilişkin ipuçları elde edilmiştir. Sahte bölgelerin piksel bazında işaretlenmesi için Ciratefi tabanlı yeni bir lokalizasyon aşaması önerilmiştir.

Tezin üçüncü bölümünde yapılan çalışmalara ilişkin elde edilen görsel sonuçların yanında bu alanda yaygın kullanılan performans değerlendirme metrikleri ile istatistiksel bulgular sunulmuştur. Literatürde yer alan popüler kopyala-yapıştır sahteciliği tespiti yöntemleri ile elde edilen sonuçlar karşılaştırılmış, yöntemlerin başarımları değerlendirilmiştir.

Son olarak tezin dördüncü ve beşinci bölümlerinde tez çalışmasının sonuçlarından, önerilerden ve gelecekteki çalışmalardan bahsedilmiştir.

1.4. Kopyala-Yapıştır Sahteciliği Tespiti Yöntemleri

Pasif görüntü doğrulama yöntemlerinin tespit etmeye çalıştığı en popüler görüntü sahteciliği yöntemi, kopyala-yapıştır sahteciliğidir [14]. Sayısal görüntüye ait istatistiksel özellikleri kullanarak kopyala-yapıştır sahteciliğinin tespit edilebilmesi için literatürde çeşitli yöntemler önerilmiştir. Şekil 1.4’ te Scopus veri tabanından elde edilen ‘copy-move forgery (kopyala-yapıştır sahteciliği)’ anahtar kelimesi ile elde edilen yıllara göre yapılan yayın sayılarına ait bir grafik yer almaktadır [15]. Bu alanda yapılan çalışmaların son yıllara doğru hız kazanmasına rağmen yine de önerilen yöntemlerde eksiklerin olması, konunun önemini ve araştırma potansiyelinin yüksekliğini göstermektedir.



Şekil 1.4. Kopyala-yapıştır sahteciliği alanında yapılmış yıllara göre yayın sayısı (www.scopus.com)

Kopyala-yapıştır sahteciliği hem nesne/bölge gizleme hem de nesne/bölge çoğaltma amacı ile gerçekleştirilmektedir. Dolayısı ile önerilen yöntemin girdi görüntüsündeki sahteciliği oluşturulma amacından bağımsız bir şekilde gerçekleştirebilmesi önem arz etmektedir. Şekil 1.5' te bu iki sahtecilik amacına ilişkin gerçekleştirilen sahte görüntü örnekleri verilmiştir.

Şekil 1.5. Nesne/bölge gizleme ve nesne/bölge çoğaltma sahteciliği örnekleri

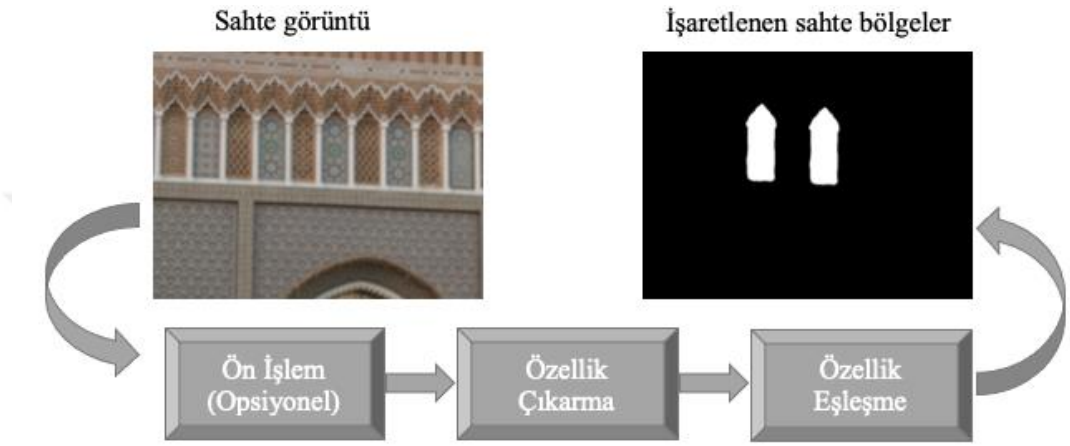
Gizlenen ya da tekrarlanan bölgelerin içeriğinin yine aynı görüntü içerisinden alınması, bölge çiftlerine ait renk paleti ve dinamik aralığı, görüntünün geri kalanı ile uyumlu kılar. Dolayısı ile bu sahtecilik türünün insan gözü ile fark edilmesi oldukça zordur. Bununla birlikte, çoğu sahtecilik işleminin ardından, gerçekleştirilen eylemi gizlemek amacıyla görüntü üzerine çeşitli operasyonlar uygulanabilir. Bu operasyonlar Tablo 1.1'de görüldüğü gibi genellikle geometrik dönüşüm atakları ve son işlem atakları olarak gruplandırılmaktadır. Geometrik dönüşüm atakları kopyalanan bölgenin yapıştırılmadan önce ölçeklenmesi, döndürülmesi, ötelenmesi veya bunlardan birden fazlasının aynı anda uygulanması şeklinde olabilir. Son işlem ataklarında ise kopyala-yapıştır işlemi sonrası oluşabilecek sahtecilik izlerinin (kenar keskinliği gibi) gizlenmesi amacı ile gerçekleştirilebilen ataklar olarak değerlendirilmektedir. Bu ataklar kopyala-yapıştır işlemi gerçekleştirildikten sonra çoğunlukla görüntünün bütününe uygulanmaktadır. Gürültü ekleme, JPEG sıkıştırma, bulanıklaştırma gibi görüntü değişim işlemleri bu ataklar arasında değerlendirilmektedir [16].

Tablo 1.1. Kopyala-yapıştır sahteciliğinde uygulanan atakların sınıflandırılması

Atak türü	**Atak işlemi**	**Açıklama**
Geometrik dönüşüm atakları	Dönme, ölçekleme, dönme ve ölçekleme, öteleme	Ön işlem atakları olarak da değerlendirilir, kopyalanan bölgeye yapıştırılmadan önce geometrik dönüşüm uygulanarak gerçekleştirilir
Son işlem atakları	Gürültü ekleme, JPEG sıkıştırma, bulanıklaştırma	Son işlem atakları olarak da değerlendirilir, sahte görüntü oluşturulduktan sonra uygulanır.

Şekil 1.6'da literatürde kopyala-yapıştır sahteciliği tespiti amaçlı önerilen yöntemlerin genel adımlarını içeren akış diyagramı vermiştir. Sahtecilik tespit yöntemleri genellikle girdi görüntüsünün renk uzayı değişimini içeren ön işlem adımından sonra özellik çıkarma ve eşleşme aşamaları gerçekleştirilerek sahte bölgelerin tespit edilmesi gerçekleştirilir. Bu temel aşamaları içeren kopyala-yapıştır sahteciliği tespiti yöntemleri öncelerde blok tabanlı ve anahtar noktası tabanlı olmak üzere iki sınıfta incelenirken, daha sonra bölüt tabanlı yöntemler de önerildi. Blok tabanlı çalışmalar özellik çıkarma aşamasından önce görüntüyü blok adı verilen sabit büyüklükte örtüşen veya örtüşmeyen karesel veya dairesel alt bloklara ayırmaktadır. Anahtar nokta tabanlı yöntemler ise görüntünün alt bloklara ayrılmadan,

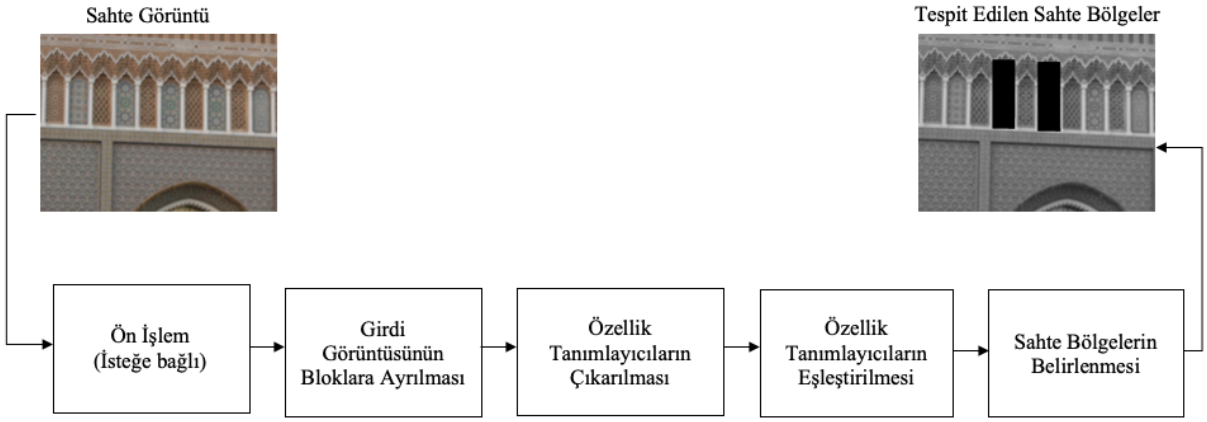
bütününden elde edilen anahtar noktalara ait özelliklerden faydalanarak sahtecilik tespitini gerçekleştirmektedir. Bölütleme tabanlı yöntemlerde, çoğunlukla görüntünün belli bir özelliğe göre tutarlı bölütlere ayrılmasından sonra, blok tabanlı ve/veya anahtar noktası tabanlı yöntemlerin avantajlarından faydalanılarak sahtecilik tespiti gerçekleştirilmektedir. Blok tabanlı, anahtar noktası tabanlı ve bölüt tabanlı çalışmalar alt bölümlerde detaylandırılacaktır.



Şekil 1.6. Kopyala-yapıştır sahteciliği tespit algoritmalarının genel akış diyagramı

1.4.1. Blok Tabanlı Yöntemler

Blok tabanlı yöntemlerde girdi olarak alınan test görüntü çoğunlukla ön işlem adımından geçtikten sonra aynı boyutlu karesel veya dairesel bloklara ayrılmaktadır. Ayrılan bu bloklara ait özellik vektörleri, çeşitli özellik çıkarma yöntemleri kullanılarak elde edilmektedir. Ardından sahte blokları temsil etmek üzere kullanılan özellik vektörlerinin en benzer olanlarının eşleştirilmesi gerçekleştirilir. Görüntüde orijinal olduğu halde benzer özellik gösteren bölgelerin varlığı, bu blokların sahte olarak işaretlenmesine sebep olacaktır. Bunun önüne geçebilmek için genellikle son aşamada blok konumlarından faydalanarak, işaretlenen blokların konumlarında tutarlılık/yoğunluk beklenmektedir. Son aşamada çoğunlukla kayma vektörü (shift vector) olarak da adlandırılan ve benzer blokları birbirine bağladığı düşünülen bu vektörlerin tutarlılığı analiz edilerek, sahte bölgelerin işaretlemesi gerçekleştirilir. Şekil 1.7’ de blok tabanlı yöntemlerin temel adımları verilmiştir.



Şekil 1.7. Blok tabanlı kopyala-yapıştır sahteciliği tespiti yöntemlerinin temel adımları

Kopyala-yapıştır sahteciliği tespitinde literatürde yaygın olarak kullanılan bu çalışma yapısının ana adımlara ilişkin detaylar aşağıdaki gibi tanımlanabilir:

Adım 1: MxNx3 boyutundaki renkli sahte görüntü ilk olarak gri seviyeye dönüştürülür (Renk bilgisini kullanan algoritmalar haricinde)

Adım 2: Görüntü bxb boyutlu bloklara bölünür. Böylece $N_b = (M - b + 1)x(N - b + 1)$ adet blok elde edilmiş olur.

Adım 3: K her bir bloğa ait özellik vektörünün boyutunu temsil etmek üzere, her bloğa ait 1xK boyutlu f_i özellik vektörleri elde edilir. Daha sonradan kullanmak üzere sol üst koordinat bilgisi; (x_i, y_i) olacak şekilde f_i vektöründe tutulur. Böylece f_i vektörünün boyutu $1x(K + 2)$ olur.

Adım 4: Bütün bloklara ait özellik vektörlerinin tutulduğu $N_b x(K + 2)$ boyutlu F özellik matrisi oluşturulur.

Adım 5: F özellik matrisinin satırları leksikografik olarak sıralanır. Böylece benzer vektörler birbirine yakınlaşır. Belirli bir eşik değerine göre en yakın komşuların arasından eşleşecek vektörler seçilir.

Adım 6: Eşleşen vektör çiftleri $i \neq j$ olmak üzere f_i ve f_j olsun. Eşleşen iki vektörün temsil ettiği bloklar arasındaki mutlak vektörel uzaklık s_i ile gösterilen kayma matrisinde (shift vector) tutulur. Eşitlik (1.1)' de kayma matrisinin ilgili satırına değer ataması verilmiştir. f_i^{K+1}, i ile gösterilen vektörün (K+1). elemanıdır.

$$s_i(dx, dy) = \left(f_i^{K+1} - f_j^{K+1}, f_i^{K+2} - f_j^{K+2}\right) \quad (1.1)$$

Adım 7: Aynı kayma vektörünü oluşturan her eşleşen blok çifti için bir C sayacı oluşturulur. Eşitlik (1.2)'de verilmiştir.

$$C(dx, dy) = C(dx, dy) + 1 \quad (1.2)$$

Adım 8: Kopyalanıp yapıştırılan bölgeler için bloklar her zaman aynı değişim vektöründe bulundukları için belirli bir eşik değeri altında olan sayaç değerine sahip eşleşme vektörünü oluşturan blok çiftlerinin elenmesi işlemi gerçekleştirilir. Eşik değerini sağlayan blokların ise eşleşme işlemi gerçekleştirilerek vektörlerin temsil ettiği BxB'lik blokların boyanması gerçekleştirilir.

Adım 9: Son işlem adımında yanlış doğru olarak tespit edilen bölgeler morfolojik işlemler ile minimize edilir.

1.4.1.1. Ön İşlem

Blok tabanlı yöntemlerin büyük bir çoğunluğunda ön işlem adımı olarak renk uzayları arasında dönüşüm yapılmaktadır. Bu sınıfta yer alan özellik tanımlayıcı elde etme yöntemlerinin çoğu gri seviye görüntüler üzerinde çalıştığı için ilk aşama olarak görüntünün gri seviyeye çevrilmesi aşaması gerçekleştiren çalışmalar çoğunluktadır. Bazı yöntemlerde ise RGB renk uzayının YCbCr renk uzayına dönüşümü sonrası sahtecilik tespiti gerçekleştirilmektedir. Yöntemlerden [17-20]'de sadece Y(parlaklık) kanalı kullanılırken, başka bir yöntem olan [21]'de ise diğer renk kanallarını da kullanılmıştır. Bunun yanında RGB renk uzayı ile Y kanalını [22-23] ve RGB ile gri seviye değerlerini kullanan çalışma da mevcuttur [24].

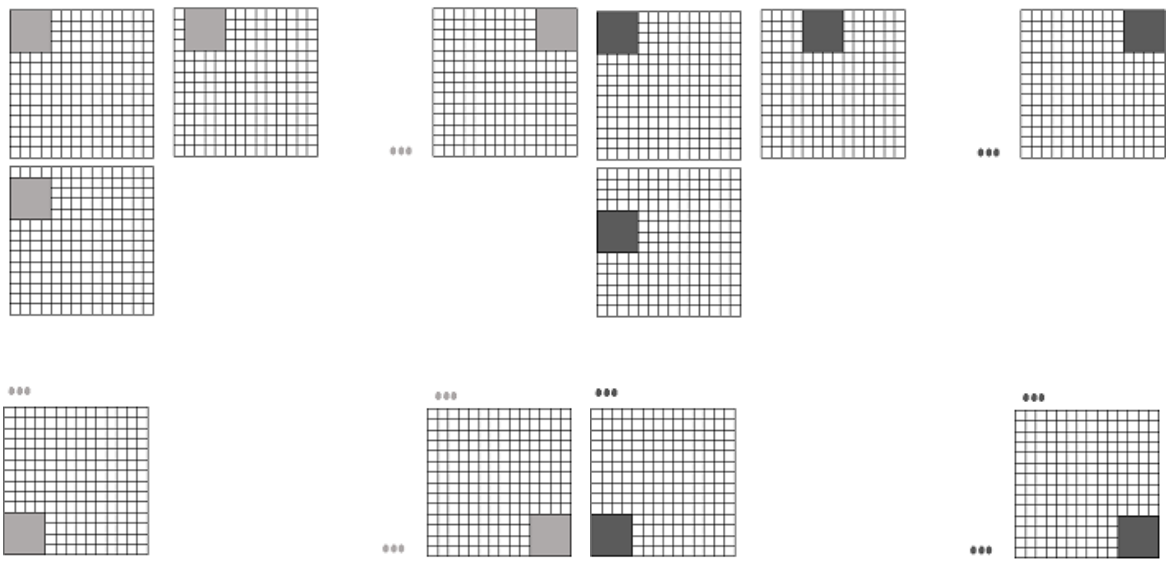
Ön işlem aşamasında renk uzayı dönüşümünün yanında, yöntemlerin daha hızlı çalışması amacı ile boyut azaltma ön işlem aşamasının gerçekleştirildiği çalışmalar da vardır. [25]' de Ayrık Dalgacık Dönüşümü (Discrete Dalgacık Transform-DWT, ADD) yöntemi kullanılarak boyut azaltma işlemi gerçekleştirilmiştir. Yine çalışma zamanının azaltılması amacı ile girdi görüntüsünün yeniden boyutlandırılması işlemini gerçekleştiren çalışmalar mevcuttur [17, 20].

Ön işlem aşamasında hedeflenen amaçlardan bir diğeri de görüntüye uygulanabilecek atakların etkilerinin azaltılması amacı ile görüntünün filtreden geçirilmesini öneren yöntemler mevcuttur. [27, 30]' de yer alan çalışmalarda bahsedilen amaçla alçak geçiren

filtre kullanılmıştır. [93]'de yer alan yöntemde ise sahtecilik tespitinin çalışma zamanının düşürülmesi amacı ile girdi görüntüsünün Gaussian piramidinden geçirilmesi işlemi gerçekleştirilmiştir. [91]' de yer alan yöntemde ise hem sahtecilik tespitinin çalışma zamanının düşürülmesi, hem de yöntemin JPEG sıkıştırma, gürültü ekleme ataklarına karşı daha dayanıklı hale getirilmesi için ön işlem aşaması olarak görüntünün Gaussian piramidinden geçirilmesi önerilmiştir.

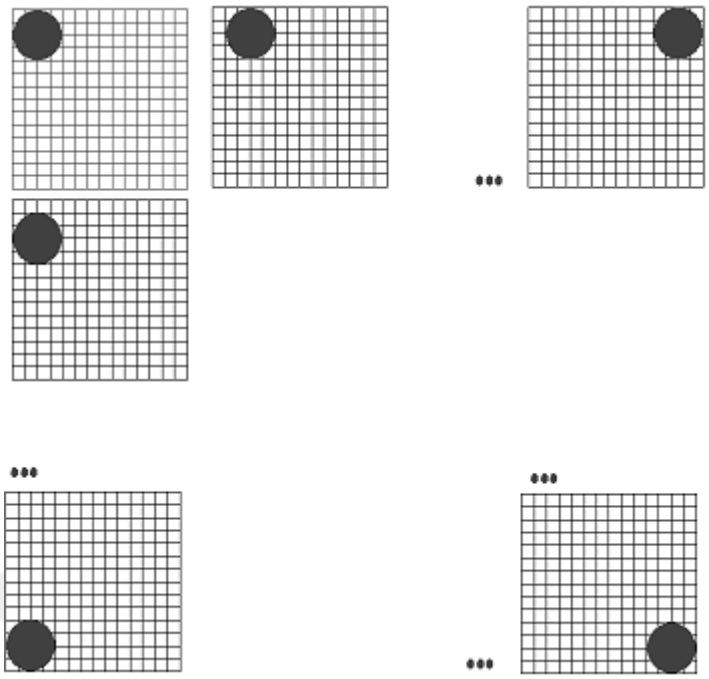
1.4.1.2. Görüntünün Bloklara Ayrılması

Bu sınıfta yer alan çalışmalarda ön işlem aşamasından sonra görüntünün tamamının alt bloklara ayrıştırılması aşaması gerçekleştirilir. Literatürde önerilen yöntemlerde bloklar birbiri ile örtüşen veya örtüşmeyen şekilde belirlenmektedir. Bunun yanında bloklar karesel veya dairesel olarak ayrıştırılmaktadır. Karesel bloklara ayırma en yaygın ayrıştırma şeklidir. Literatürde bu yaklaşım ile sahtecilik tespiti yapan birçok çalışma bulunmaktadır [29-49]. Şekil 1.8'de **4x4** boyutunda karesel bloklara ayırmaya ilişkin temsili bir görsel verilmiştir. (a)'da örtüşen blok örnekleri, (b)' de ise örtüşmeyen blok örnekleri yer almaktadır. Literatürde yer alan bazı çalışmalarda ise görüntünün karesel bloklara ayrılması yerine dairesel bloklara ayrılması gerçekleştirilmiştir. [27-28,49-55]. Şekil 1.9'da örtüşen dairesel bloklara ayrıştırmaya ilişkin temsili bir görsel verilmiştir.



(a) (b)

Şekil 1.8. 4x4 büyüklüğünde karesel bloklara ayırma (a)örtüşen karesel bloklar (b)örtüşmeyen karesel bloklar



Şekil 1.9. Örtüşen dairesel bloklara ayrıştırma

1.4.1.3. Özellik Tanımlayıcıların Çıkarılması

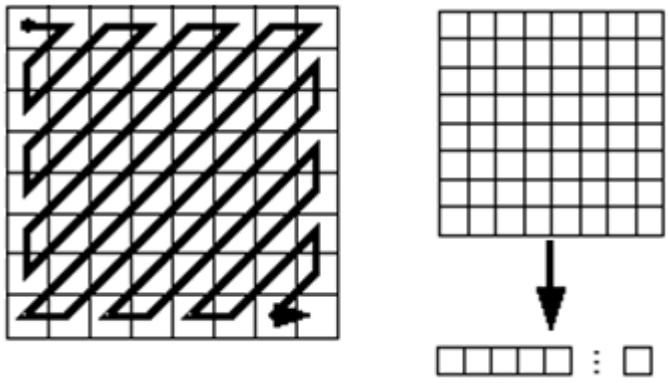
Kopyala-yapıştır sahteciliği tespitinde, sahte bölgelerin ortaya konmasında izlenen temel yaklaşım, en benzer bölgelerin bulunmasıdır. Bunun için blok tabanlı yöntemlerde bloklara ait özellik tanımlayıcılardan faydalanılarak bu amaç gerçekleştirilir. Bloklardan elde edilen özellik tanımlayıcıların ayırt ediciliğinin ve dayanıklılığının yüksek olması, yöntemin performansını olumlu yönde etkileyecektir. Literatürde özellik tanımlayıcıların elde edilmesinde kullanılan yaklaşımlar, Frekans tabanlı yöntemler, doku tabanlı yöntemler, moment tabanlı yöntemler, Log-polar dönüşüm tabanlı yöntemler, boyut azaltma tabanlı yöntemler şeklinde sınıflandırılabilir. Bu yöntemlere ilişkin detaylar aşağıda sunulmuştur.

Frekans tabanlı yöntemler: Frekans dönüşümü literatürde blok tabanlı kopyala-yapıştır sahteciliğinin tespiti yöntemlerinde en popüler özellik çıkarma tekniklerindendir. Performansı daha da iyileştirmek için Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform, DCT-AKD), Fourier Dönüşümü, Hızlı Walsh-Hadamard Dönüşümü (Fast Walsh-Hadamard Transform, FWHT), Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform, DWT-ADD), İkili Dalgacık Dönüşümü (Dyadic Wavelet Transform, DyWT) ve Wiener Filtre Dalgacık yöntemini temel alan çeşitli geliştirmeler önerilmiştir.

Literatürde kopyala-yapıştır sahteciliği tespiti için önerilen ilk çalışmada, Fridrich vd. özellik tanımlayıcıların çıkarılmasında Ayrık Kosinüs Dönüşümünden (Discrete Cosine Transform-AKD) faydalanılmıştır [31]. Bu yöntemde ilk olarak gri seviyeye dönüşümü gerçekleştirilen girdi görüntüsünün **BxB** boyutlu örtüşen karesel alt bloklara ayrılması gerçekleştirilir (Çalışmada $\mathbf{B = 16}$ olarak alınmıştır). Her bir bloğun AKD sonrası elde edilen katsayıların kuantalanmış hali blokları temsil eden özellik vektörünün elde edilmesinde kullanılmaktadır. Her bir bloktan elde edilen vektörler A özellik matrisinde depolanmıştır. Böylece **MxN** boyutlu bir görüntü için A matrisi $(\mathbf{M - B + 1})$ **x** $(\mathbf{N - B + 1})$ adet satır, **BxB** adet sütundan oluşmaktadır. Yöntemde her bir bloktan elde edilen katsayıların eşleşme aşamasının kolaylaştırılması için leksikografik olarak sıralanması gerçekleştirilmiştir. Hatalı işaretlemelerin önlenmesi amacı ile eşleşen blok çiftlerinin konumlarından faydalanarak kayma vektörleri oluşturulmuş ve eşleşme yoğunluğunun olduğu bölgeler haricindeki eşleşmeler hatalı eşleşme olarak kabul edilip dikkate alınmamıştır. Eşleşen blokların boyanması ile sahte bölgeler ifade edilmeye çalışılmıştır. Yöntemde AKD katsayılarının kullanılmasındaki amaç görüntünün JPEG sıkıştırma olması durumunda da değişmez özelliklerin elde edilmesini amaçlanmıştır, ancak bu atak türüne karşı yöntemin dayanıklılığına ilişkin detaylı deneyler yapılmamış, herhangi bir sonuç rapor edilmemiştir.

Popescu vd. tarafından önerilen yöntemde ise bir önceki çalışmada elde edilen özellik tanımlayıcı vektörlerinin boyutunun azaltılması için Temel Bileşenler Analizi (Principal Component Analysis, PCA-TBA) yöntemi kullanılmıştır [32]. Yapılan çalışmada yöntemin JPEG sıkıştırma ve gürültü ekleme atağı uygulanan dört adet sahte görüntü üzerinde görsel sonuç verilmiştir.

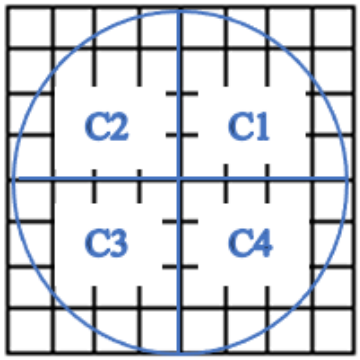
Huang vd. tarafından önerilen yöntemde ise örtüşen bloklardan AKD dönüşümü sonrası elde edilen kuantalanmış katsayılar zikzak tarama ile $\mathbf{1xB^2}$ boyutunda vektöre dönüştürülmüştür [33]. Şekil 1.10'da 8x8 boyutlu bir bloğun zikzak tarama ile 1x64 boyutlu vektöre dönüştürülmesi verilmiştir. Zikzak tarama ile alçak frekans bileşenleri vektörün ilk elemanlarını oluştururken, yüksek frekans bileşenleri vektörün son elemanlarında yer almaktadır. Önerilen bu yöntemde yüksek frekans bileşenlerinin olduğu vektörün son elemanları kırpılarak sadece vektörün ilk kısmını oluşturan alçak frekans bileşenleri depolanmıştır. Bu yaklaşım ile boyut azaltma gerçekleştirilerek daha hızlı sıralama ve eşleşme imkânı sağlanmıştır. Yöntemin sahte görüntüye JPEG sıkıştırma, bulanıklaştırma ve toplanır beyaz Gauss gürültüsü (additive white Gaussian noise, AWGN) ataklarının uygulanması durumunda performans analizi yapılmış, çalışma kapsamında hazırlanan örnek sahte görüntüler üzerinde Doğruluk (Accuracy) ve Yanlış Pozitif Oranı (False Positive Rate, FPR-YPO) metrikleri ile elde edilen sonuçlar rapor edilmiştir



Şekil 1.10. 8x8 boyutlu bir blok üzerinde zikzak tarama

Cao vd. tarafından önerilen yöntemde yine örtüşen blokların AKD ile katsayıları elde edilmiştir. Yöntemde karesel alt blokların özellik vektörlerinin oluşturulmasında zikzak tarama ile vektörlerin belirlenmesi yerine, bloğun dairesel temsilinden faydalanılmıştır. Yalnızca daire dışında kalan katsayıların değerlendirme dışı bırakılması, daire içinde kalan katsayıların C1, C2, C3 ve C4 olarak isimlendirilen bölgelere ayrılması gerçekleştirilmiş. Blokların bölgelere ayrılmasına ilişkin görsel Şekil 1.11'de verilmiştir. Her bir bölge için ilgili çembersel bölgelerde yer alan katsayılardan faydalanarak her bir blok için 1x4 boyutlu özellik vektörleri oluşturulmuştur. Böylece eşleşme aşamasının hesaplama zamanının

düşürülmesinde büyük oranda avantaj sağlanmıştır. Yöntemin gürültü ekleme ve bulanıklaştırma atakları altındaki performans analizleri rapor edilmiştir.



Şekil 1.11. [57]' de önerilen yöntemde özellik vektörlerinin oluşturulmasında belirlenen bölgeler

Shao vd. tarafından önerilen yöntemde [58], örtüşen dairesel bloklardan Ayrık Fourier Dönüşümü (Discrete Fourier Transform, DFT-AFD) ile özellik vektörlerinin elde edilmesi gerçekleştirilmiştir. Eşleşme aşamasında, AFD sonrası elde edilen katsayıların faz korelasyonlarının karşılaştırılması gerçekleştirilmiştir. Dairesel bloklardan faydalanılmasındaki amaç, dönme ataklarından bağımsızlığın elde edilmesidir. Yöntemin dönme, gürültü ekleme, JPEG sıkıştırma atakları altındaki testleri gerçekleştirilmiş bu ataklardaki performans sonuçları rapor edilmiştir. Yang vd. girdi görüntüsünün gri seviyeye dönüştürülmesinin ardından, görüntünün boyutunun azaltılması amacı ile Ayrık Dalgacık Dönüşümü (ADD) yaklaşımını kullanmışlardır [59]. Daha sonra, örtüşen bloklardan özellik vektörlerinin elde edilmesinde Hızlı Walsh-Hadamard Dönüşümü (Fast Walsh-Hadamard Transform, FWHT) kullanılmıştır. [60]'da önerilen yaklaşımda ise görüntünün bloklara ayrılmadan önce Ayrık Dalgacık Dönüşümü (ADD) gerçekleştirilmiştir. ADD sonrası alçak frekanslı alt bantlar (LL) kullanılarak görüntünün boyutunun azaltılması gerçekleşmiştir. Daha sonra alt bantlar örtüşmeyen bölgelere ayrılarak faz korelasyonu açısından değerlendirilmiştir. Muhammad vd. tarafından önerilen yöntemde İkili Dalgacık Dönüşümü (Dyadic Wavelet Transform, DyWT) yaklaşımından [61], Peng vd. tarafından önerilen yöntemde ise özellik vektörlerinin elde edilmesinde Wiener Filtre Dalgacık Dönüşümü yaklaşımından faydalanılmıştır [62]. Meena ve Tyaginin yaptığı çalışmada da blok tabanlı bir kopyala-yapıştır sahteciliği tespiti yöntemi önerilmiştir [80]. Örtüşen her bir alt bloktan Tetrolet dönüşüm kullanarak 4 adet alçak geçişli katsayı ve 12 adet yüksek geçişli katsayı

çıkarılır. Özellik vektörleri leksikografik olarak sıralanır ve Öklid uzaklığı tabanlı eşleşme yaklaşımı ile eşleştirilir. Yöntemin deneylerinde GRIP veriseti ve Comofod verisetinden bazı görüntüler seçilerek kullanılmıştır. Deneylerde atak durumlarındaki performans sonucu sadece bir görüntü üzerinden verilmiştir. Deneysel çalışmalar oldukça yetersiz tutulmuştur.

Doku tabanlı yöntemler: Doku, görüntüde çimen, bulut, ağaç, zemin gibi doğal görüntü bölgelerinde olabileceği gibi pürüzsüzlük (smoothness), süreklilik gibi doku içeriğini belirleyen görüntü özellikleri olarak ele alınmaktadır. Bu yüzden doku bilgisi, kopyala-yapıştır sahteciliği tespiti amacı ile, şüpheli görüntüde benzer bölgelerin araştırılmasında kullanan çalışmalar mevcuttur. Literatürde kopyala-yapıştır sahteciliği tespitinde renk bilgisinin de doku özelliklerinin karakterize edilmesi şeklinde yapılan çalışmalar yine bu kategoride değerlendirilmektedir [63]. Luo vd. tarafından önerilen yöntemde renkli girdi görüntüsünün örtüşen alt bloklara ayrılması sonrasında elde edilen bloklar için iki tür özellik çıkarılmıştır [64]. İlk olarak renkli görüntü bloklarının R, G ve B kanallarının ortalamaları özellik vektörünün bir bölümünü oluşturmuştur. İkinci tür özellikler, görüntünün YCbCr renk uzayında, Y kanalındaki temsilden elde edilmiştir. Bu kanalda temsil edilen görüntünün örtüşen alt bloklarından sırası ile dikey, yatay, sağa çapraz, sola çapraz şekilde ikiye ayrılması gerçekleştirilir. Oluşturulan her yarım parçanın parlaklık değerinin, tüm bloğun parlaklık değerine oranı ile elde edilen değerler ikinci tür özellik olarak depolanmaktadır. Yöntemin JPEG sıkıştırma, gürültü ekleme ve bulanıklaştırma atakları uygulanmış örnek sahte görüntülerde sahtecilik tespiti yapabildiği rapor edilmiştir. Bir diğer doku tabanlı yöntem Gharibi vd. tarafından önerilmiştir [66]. Önerilen bu yöntemde örtüşen alt blokların temsili için Gabor özelliklerden faydalanılmıştır. Her bloktan elde edilen Gabor özellikleri bir matriste depolandıktan sonra TBA ile özellik matrisinin boyut indirgenmesi gerçekleştirilmiştir. Hsu vd. tarafından önerilen yöntemde de yine Gabor özelliklerinden faydalanılmış, farklı ölçekleme faktörleri, rotasyon açıları ve frekansları kullanılmıştır [67]. Davarzani vd., Çoklu Çözünürlük Yerel İkili Örüntü (Multiresolution Local Binary Patterns, MLBP) yaklaşımını ile sahtecilik tespitine ilişkin çalışma gerçekleştirmişlerdir [68]. Örtüşen alt bloklardan Yerel İkili Örüntü (Local Binary Patterns, LBP) ile özellik vektörleri elde edilmiş, elde edilen özellik vektörleri leksikografik olarak sıralandıktan sonra k-d ağacı yaklaşımı ile eşleştirilmeleri gerçekleştirilmiştir. RANSAC (RANdom SAmple Consensus) algoritmasının kullanılması ile varsa hatalı eşleşmelerin giderilmesi gerçekleştirilmiştir. Önerilen yöntemin geometrik bozulma ve aydınlık değişimi durumlarında da sahtecilik tespiti yapabildiği rapor edilmiştir. Ustubioglu vd. tarafından

önerilen doku tabanlı yöntem ise Yerel Faz Nicemleme (Local Phase Quantization, LPQ) yaklaşımı ile örtüşen bloklardan doku özellikleri elde edilmiştir. Önerilen bu yöntemin özellikle bulanıklaştırma ataklarına karşı üstün performansı rapor edilmiştir [69].

Moment tabanlı yöntemler: Moment değişmezleri öteleme, döndürme ve ölçeklemeye göre değişmeyen özellikler olarak kullanılmaktadır. İkili bir görüntüde bir şekli sınıflandırma ve tanımlama için kullanılabilir. Kopyala-yapıştır sahteciliği tespitini gerçekleştirmek için de literatürde moment tabanlı yaklaşımlar önerilmiştir. Bunlardan ilki Mahdian vd. tarafından önerilen yöntemdir [34]. Yöntemde örtüşen alt bloklardan RGB renk kanalları için 24 bulanık değişmez moment hesaplanarak 72 boyutlu özellik vektörleri elde edilmiştir. Elde edilen özellik vektörlerinin en anlamlılarının kullanılarak boyut indirgenmesinin gerçekleştirilmesi için yine TBA yaklaşımından faydalanılmıştır. Önerilen yöntemde kullanılan bulanık değişmez momentler ile bulanıklaştırma ataklarına karşı dayanıklılığın yanında JPEG sıkıştırma ve gürültü ekleme ataklarına karşı dayanıklılık sağlandığı belirtilmiştir. İmamoğlu vd. tarafından önerilen yöntemde ise Krawtchouk momentleri kullanılarak alt bloklardan özellik vektörleri elde edilmiştir [71]. Yöntemin bulanıklaştırma ve gürültü ekleme atakları durumunda sahtecilik tespiti gerçekleştirebildiği raporlanmıştır. Dönme bağımsızlık özelliği ile öne çıkan Zernike momentlerden faydalanan sahtecilik tespiti yöntemi Ryu vd. tarafından önerilmiştir [72]. Yöntemde eşleşme aşamasında önceki standart yöntemlere benzer olarak özellik vektörlerinin leksikografik olarak sıralanması sonucu komşu vektörler arası Öklid uzaklık kontrolü gerçekleştirilmiştir. Aynı yazarlar bu çalışmanın genişletilmesi ile yine alt blokları Zernike momentler ile temsil etmiş, eşleşme aşamasında Locality Sensitive Hashing (LSH) yaklaşımı kullanılmıştır [73]. Chen vd. örtüşen alt blokların temsilinde 7 değişmez Hu momentleri yaklaşımından faydalanarak sahtecilik tespiti gerçekleştirmiştir [74]. Yöntemde, elde edilen 7 boyutlu özellik vektörlerinin eşleşmesinde genişleyen blok (expanding block, EB) yaklaşımından faydalanılmıştır. Bu yaklaşıma göre her bir özellik vektörünün ortalama ve varyans değerleri elde edilir ve elde edilen bu değerlere göre kendi içlerinde sıralanır. Sıralama sonrası komşu blokların ortalama ve varyans değerleri ve Öklid uzaklığı bakımından benzerliği söz konusu ise iki bloğun benzer bloklar olduğu ortaya konur. Zhong ve Pun arkadaşları tarafından önerilen yöntemde, görüntü alt bloklarından Normalized Moment Transformation ile özellik vektörleri elde edilmektedir [81]. Bu özellik vektörleri hash bilgisine göre hash tablosuna yerleştirilir. Yazarlar, birden fazla hash özelliklerini birleştirerek yeni iki geçişli bir hashleme yöntemi kullanmışlardır. Algoritma, en yakın iki eşleşen pikseli en yüksek

doğruluk ile araştırmayı amaçlar. Bunun için ilk aşamada, normalize edilmiş PCT ile HSV uzayından 2 boyutlu Hue, 2 boyutlu Saturation ve 1 boyutlu Gri özellikler elde edilir. İkinci aşamada, her pikselin 15 boyutlu özellik vektörü ileri ve geri hashleme ile iki aşamalı hash özelliği elde edilir. Böylece ileri(forward) hash tablosu ve geri(backward) hash tablosu oluşturulur. Bu hash tablolarından arama işleminde ise öncelikle ileri hash tablosundan arama gerçekleştirilir. Bulunan en iyi eşleşmelerin geri hash tablosundan aranması gerçekleştirilir.

Log polar dönüşüm tabanlı yöntemler: Log polar dönüşümü dönme, ölçekleme ve öteleme durumlarında dahi değişmez özelliklerin elde edilmesi tekniğidir. Bu teknik, kartezyen düzlemindeki noktaların (x, y), log-polar (x, h) noktalarına izdüşümünün gerçekleştirilmesi ile çalışır. Kopyala-yapıştır sahteciliği tespitinde log-polar dönüşümünün kullanıldığı ilk yöntem Fourier Mellin Dönüşümü (Fourier Mellin Transform, FMD) yaklaşımını kullanan çalışma olmuştur [36]. Yöntemde her bir alt bloğa Fourier dönüşümü uygulanmaktadır. FMD sonrası çıkarılan Fourier katsayılarının genlikleri log-polar koordinatlara haritalanmakta ve yarıçap boyunca log-polar değerleri blok özellik vektörünü oluşturmaktadır. Elde edilen özellik vektörlerinin eşleşmesinde ise Bloom filtrelerinden yararlanılmaktadır. Bu filtrelerin kullanımı sayesinde işlemsel karmaşıklığı azaltmıştır. Yöntemin ölçekleme, JPEG sıkıştırma, 10 dereceden daha az açılar için de dönme ataklarına karşı dayanıklılığı sınırlı sayıda görüntü üzerinde başarılı olduğu rapor edilmiştir. Bir başka çalışmada 10 dereceden daha fazla açılarla gerçekleştirilen dönme atakları karşı dayanıklılığını sağlamak amacı ile FMD ve vektör eritme filtresinin (vector erosion filter) kombine bir şekilde kullanılmıştır [75]. Deneysel analizlerin sonucuna göre, yöntemin 90 dereceye kadar dönme ataklarına ve küçük oranla gerçekleştirilen ölçekleme ataklarına karşı dayanıklı olduğu söylenmektedir. Ancak gürültü ekleme, bulanıklaştırma ve yüksek oranda ölçekleme atakları durumunda yöntem başarısız kalmaktadır. Log polar dönüşümdeki gelişmeler ışığında önerilen Polar Harmonik Dönüşüm (Polar Harmonic Transform, PHT) yaklaşımı Li vd. tarafından kullanılarak blok özellik vektörlerinin elde edilmesi gerçekleştirilmiştir [76]. Önerilen bu yöntemde görüntü karesel bloklar yerine dairesel alt bloklara ayrılmış, daha sonra özellik tanımlayıcıların elde edilmesi gerçekleştirilmiştir. [18]'de önerilen yöntemde ise [36]' da verilen yöntemden farklı olarak özellik vektörlerinin elde edilmesinde Log-Polar Fourier Dönüşümü (Log-Polar Fuorier Transform- LPFD) kullanılmıştır. Dairesel alt blokların log-polar dönüşümü sonrası iki boyutlu Fourier dönüşümü gerçekleştirilmiştir. Yöntemin dönme, ölçekleme ataklarına karşı dayanıklı

olduğu ancak gürültü ekleme, JPEG sıkıştırma gibi son işlem ataklarına karşı dayanıksız olduğu görülmüştür. [38]' de önerilen yöntemde, özellik vektörleri Log Polar Fraktal Fourier yaklaşımından faydalanarak elde edilmiştir. Log polar dönüşümü tabanlı yöntemlerde genel olarak dönme ve ölçekleme ataklarına karşı dayanıklılık sağlansa da çoğunlukla bulanıklaştırma, gürültü ekleme gibi görüntü bozma ataklarının olduğu durumda sahtecilik tespitinde başarısız kalmaktadır. Bu grupta yer alan yöntemlerin diğer dezavantajı ise bu algoritmalarda kullanılan eşik değerlerindeki sayının fazlalığıdır. Eşik değerlerinin girdi görüntüsünden bağımsız en uygun değere ayarlanması için öncesinde birçok testin gerçekleştirilmesi gerekliliği söz konusudur.

Boyut azaltma tabanlı yöntemler: Görüntü alt bloklarından elde edilen özellik vektörlerinin boyutunun azaltılması amacı ile önerilen yöntemler bu grupta yer almaktadır. Bu amaçla geliştirilen ilk yöntem Popescu ve Farid tarafından önerilmiş, TBA yaklaşımı kullanılarak özellik vektörü boyut azaltılması amaçlanmıştır [32]. Yönteme göre özellik matrisinin kovaryans matrisi hesaplanması sonrası kovaryans matrisinin öz vektörleri aracılığı ile yeni bir taban elde edilir. Her bloğun bu temel özvektörler üzerine projeksiyonu gerçekleştirilerek özellik vektörlerinin boyutu küçültülür. Sunulan yaklaşım ile zamansal açıdan avantaj sağlanmasının yanında gürültü ve kayıplı JPEG sıkıştırmaya da dayanıklılık sağlanabilmiştir. Ting ve Rang-Ding tarafından önerilen yöntemde ise boyut azaltmak amacı ile Tekil Değer Ayrışımı (Singular Value Decomposition, SVD, TDA) yaklaşımını kullanmışlardır [78]. Önerilen yöntem ile kısmi dönme ve gürültü ekleme ataklarına karşı dayanıklılık sağlansa da TDA ile boyut indirgenmesi sonucu bazı bilgilerin kaybolmuştur. Bu yüzden JPEG sıkıştırma ataklarına karşı dayanıklılık elde edilememiştir. Bir diğer çalışmada boyut azaltma aşamasının gerçekleştirilebilmesi için Lokal Doğrusal Gömüleme (Locally Linear Embedding, LLE, LDG) yaklaşımı kullanılmıştır [79]. Bu yaklaşım doğrusal olmayan veri kümesi arasındaki topolojik ilişkiyi bulur ve göreceli konumları değiştirmeden yüksek boyutlu verileri düşük boyutlu verilerle eşler. Priyanka vd. tarafından önerilen yöntemde, DCT ile frekans domenine dönüştürülerek temsil edilen bloklardan çıkarılan özellik vektörlerinin boyutları SVD ile kısaltılmıştır [82]. Görüntüyü sahte/orijinal olarak sınıflandırmak için SVM sınıflandırıcı kullanılmıştır. Görüntü sahte olarak belirlendi ise, özellik vektörleri üzerinde k-ortalamalar (k-means) kümeleme yaklaşımı kullanılmıştır. Uzaklık eşiğine göre benzer bloklar işaretlenmiştir. Yöntemin performans analizinde FAU isimli veri seti kullanılarak sonuçlar rapor edilmiştir. Geometrik dönüşüm ataklarına karşı dayanıklılık vurgulanmış olsa da sadece düşük oranlarda dönme ve ölçekleme atağı altında

testler yapılmıştır. Bir diğer boyut azaltma yaklaşımı kullanan yöntemde, örtüşen alt bloklardan Polar Complex Exponential Transform (PCET) ile geometrik dönüşümlere dayanıklı özellik vektörleri elde edilmiş ve sonrasında SVD yaklaşımı ile özellik vektörünün boyutu azaltılmıştır [83]. Daha sonra blokların histogramı ve Particle Swarm Optimization (PSO) algoritması kullanılarak optimum benzerlik eşiğini bulmak için kullanılmıştır. Belirlenen eşik değeri kullanarak blok eşleştirilmesi yapılmıştır. Deneylerde Comofod ve CASIA verisetinde yer alan sahte görüntüler kullanılmış olup piksel bazında bir değerlendirme yapılmamış, sadece görüntü bazında sahtecilik tespiti gerçekleştirilmiştir. Bu yaklaşımlardan TBA'nın çalışma zamanı açısından avantajı daha ön planda iken, LDG yaklaşımının yapıştırılan bölgedeki izlerin ayırt edilmesinde daha başarılı olduğu görülmektedir. TBA yaklaşımının kullanılması ile de genel sahtecilik tespiti performansının daha yüksek olduğu görülmektedir.

1.4.1.4. Özellik Tanımlayıcıların Eşleştirilmesi

Özellik çıkarımı aşaması tamamlandıktan sonraki adımda birbirine en benzer özelliğe sahip blokların araştırılması işlemi gerçekleştirilmektedir. Böylelikle aday kopyala-yapıştır çiftlerinin bulunması gerçekleştirilmektedir. Benzerlik araştırmasında en basit yöntem her bir özellik vektörünün geri kalan tüm vektörlerle karşılaştırılmasıdır. Fakat bu yöntemin hesaplama zamanı oldukça yüksek olmaktadır. Eşleşme aşamasında doğrusal arama mantığına dayanan yöntemlerin neden olduğu problemin üstesinden gelebilmek için öncelikle benzer blokların bir araya getirilmesi ve sonrasında her bloğun kendisinden sonra gelen belli sayıdaki bloklar ile kıyaslanması yatmaktadır. Bu tekniklerin en sık kullanılanı, özellik vektörlerinin hepsinin öncelikle bir matriste depolanması sonrası benzer vektörleri birbirine yakınlaştırmak için leksikografik (sözlük sıralaması) sıralamadır [84-85]. Leksikografik sıralama ile özellik vektörlerinin söz dizimsel olarak satır sıralaması gerçekleştirilmektedir. Ayrıca radix sıralama [86, 87], k-d ağacı [68, 34], sıfır sayısına göre sıralama [17], blooms filtrelerinin sayımı [36], tüm özellikler vektörlerinden maksimum varyansa sahip vektör bileşenlerine göre sıralama [88], blok sınıflama [89], hash değerlerinin kıyaslanması [90] teknikleri kullanılmaktadır. Benzer özelliklerin komşu duruma getirilmesinden sonra benzer özelliklerin kıyaslanmasında kullanılan benzerlik kriterleri bazıları şu şekildedir; Öklid uzaklığı [91-93], Hamming uzaklığı [17], mantıksal uzaklık

[94], Hausdorff uzaklığı [95], korelasyon katsayıları [96], faz korelasyonu [97, 98], normalize edilmiş kross spektrum [38, 74].

1.4.1.5. Sahte Bölgenin Belirlenmesi

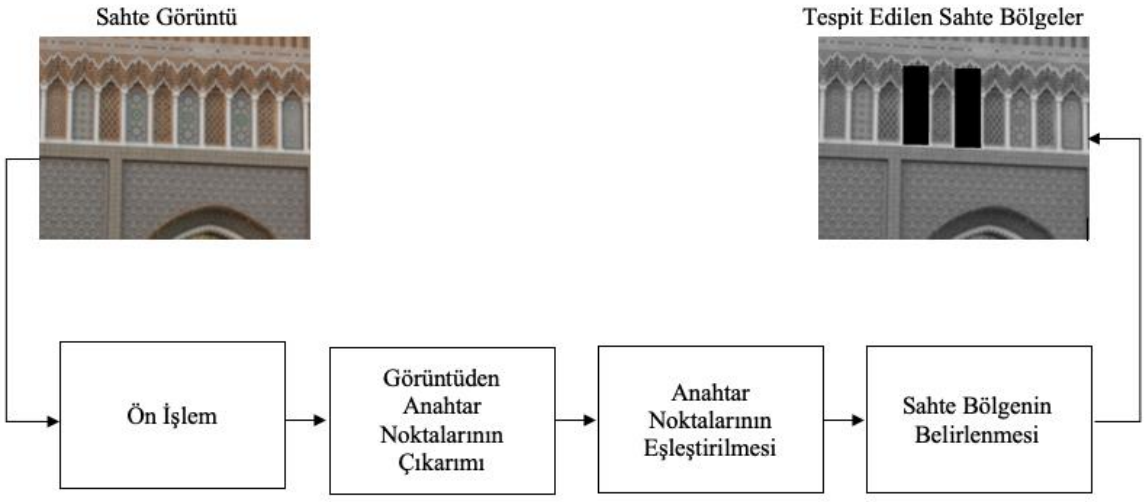
Blok tabanlı yöntemlerde, önceki bölümlerde belirtilen aşamaların tamamlanması sonrası sahte olarak belirlenen blokların işaretlenmiş olması, sahte bölgelerin net bir şekilde belirlenmesinde çoğunlukla yeterli olmayacaktır. Bazı girdi görüntülerinde, görüntünün doğası gereği benzer özellikleri barındıran orijinal bölgelerin varlığı söz konusu olabilir. Bu benzer özelliklerin varlığı da yöntemin yanlış işaretleme yapmasına sebebiyet verebilir. Bu tür durumların önüne geçebilmek için, literatürde sahte olarak işaretlenen blokların birbirine yakın konumlarda yoğunlaşması fikrinden yola çıkarak bazı yaklaşımlardan faydalanılmıştır. Bunlardan bazıları, Shift Vektörü, Uzaklık Kriteri ve Alan Kriteri, Aynı Afine Dönüşümü Seçimi gibi yaklaşımlardır. Shift Vektörü yaklaşımında, eşleşen özellik vektörlerinin ait olduğu blokların koordinatları $(\mathbf{x}, \mathbf{y})$ arasındaki mutlak farka bakılır. Aradaki fark literatürde kayma vektörü (shift vektör) olarak isimlendirilen vektörde tutulur. Bütün eşleşen blok çiftlerinden kayma vektörü değerleri hesaplanmakta, aynı vektör değerinin en fazla olduğu Shift Vektör değerine göre, bu vektör değerine sahip olmayan eşleşmelerin hatalı eşleşme olarak kabul edilip elenmesi işlemi gerçekleştirilmektedir. Bu yaklaşımı kullanan çalışmaların çoğunda bölgenin yapıştırılmadan önce dönme, ölçekleme gibi ön işlem ataklarının dikkate alınmadığı görülmektedir. [99, 100]. Daha sonra geliştirilen yöntemlerde ise bu atakların olabileceği de dikkate alınarak $\pm\boldsymbol{\partial}$ bir eşik kabulü ile hatalı işaretlemelerin giderilmesi gerçekleştirilmiştir. [102].

Bir diğer yaklaşımda ise görüntü içerisindeki komşu blokların benzer özelliklere sahip olabileceği durum dikkate alınarak Uzaklık Kriteri yaklaşımına göre hatalı işaretlenmiş blokların elenmesi amaçlanmıştır. Bunun için blokların birbirine uzaklıkları hesaplanarak, birbirine çok yakın blokların elenmesi gerçekleştirilir. Literatürdeki yöntemlerden bu amaç için, Öklid uzaklığı [32, 71, 98], maksimum normalize uzaklık [102, 103], en yakın komşu uzaklığının en yakın ikinci komşu uzaklığına oranı [104] yaklaşımları kullanılmıştır.

Alan kriteri yaklaşımından faydalanan çalışmalarda ise sahte bölge olarak işaretlenen bölgenin boyutunun görüntünün boyutu da dikkate alınarak küçük olmamasına dikkat edilmektedir [24, 28, 76]. Küçük boyutta belirlenen sahte bölgelerin elenmesi gerçekleştirilir. [87] ve [105]'deki çalışmalarda ise aynı afine dönüşüme sahip olan eşleşmelerin doğru eşleşme olarak kabul edilip sahte bölgelerin belirlenmesi yaklaşımına gidilmiştir.

1.4.2. Anahtar Noktası Tabanlı Yöntemler

Kopyala-yapıştır sahteciliği tespiti için önerilen blok tabanlı yöntemlerin özellikle geometrik dönüşüm ataklarına karşı dayanıksız oluşu ve görüntünün bütününden elde edilen blokların özellik çıkarma ve eşleşme aşamasında çalışma zamanının fazla olması araştırmacıları anahtar noktası tabanlı yöntemlere yönlendirmiştir. Bu sınıfta yer alan çalışmalar görüntüyü temsil eden değişmez anahtar noktalarından faydalanarak görüntüye uygulanan sahtecilik izlerini araştırmaktadır. Anahtar noktası tabanlı yöntemlerde kullanılan temel işlem adımları Şekil 1.12'de verilmiştir.



Şekil 1.12. Anahtar noktası tabanlı kopyala-yapıştır sahteciliği tespiti yöntemlerinin temel adımları

İlk aşama olarak çoğunlukla görüntünün renk uzayı değişimi veya aynı renk uzayında farklı seviyeye dönüştürülmesi ve/veya görüntünün doku bilgisinin elde edilmesi gibi ön işlem aşaması uygulanmaktadır. Ardından görüntünün bütününden anahtar noktaları ve bu noktalara ait özellik tanımlayıcı vektörler çıkartılmaktadır. Sahtecilik izlerinin bulunması

için özellik tanımlayıcı vektörlerden, birbirine en benzer olanların bulunabilmesi için anahtar noktalarının eşleştirilmesi aşaması gerçekleştirilmektedir. Anahtar noktalarının eşleştirilmesi ile sahte bölgede yer alan anahtar noktaları eşleştirilmiş olur. Sahte bölgelerin sınırlarının tam olarak belirlenmesi işlemi (lokalizasyon) aşamasını barındıran bazı çalışmalar da mevcuttur. Bu adımı gerçekleştirmeyen sadece görüntünün sahte olup olmadığını ortaya koyan çalışmalar da mevcuttur. Sahte bölgenin belirlenmesi aşamasında piksel tabanlı sahtecilik tespiti gerçekleştirilmektedir.

Anahtar noktası tabanlı yöntemlerde temel olarak kullanılan adımlar aşağıdaki gibi tanımlanabilir;

Adım 1: Girdi görüntüsüne ön işlem aşamasının uygulanması.

Adım 2: Görüntünün bütününden anahtar noktalarının ve bunlara ait özellik tanımlayıcıların elde edilmesi. (1xK boyutlu f_i özellik vektörünün elde edilmesi.)

Adım 3: Daha sonradan kullanılmak üzere anahtar noktalarına ait koordinat bilgisinin (x_i, y_i) de f_i vektörüne eklenmesi. (Böylece f_i vektörünün boyutu $1x(K+2)$) olur.

Adım 4: Bütün anahtar noktalarına ait tanımlayıcı bilgiler tutulduğu $Nx\,(K+2)$ boyutlu F özellik matrisi oluşturulur.

Adım 5: Özellik vektörlerinin mutlak uzaklık değerinin hesaplanmasıyla birlikte birbirine en yakın anahtar noktaların eşleştirilmesi gerçekleştirilir. Bu adımda ayrıca çoğunlukla oluşabilecek hatalı işaretlemelerin elenmesi işlemi gerçekleştirilmektedir.

Adım 6: Yeterli sayıda anahtar noktasının bulunması halinde görüntünün sahte/orijinal olduğu ortaya konmaktadır.

Adım 7: Sahte bölgenin sınırlarının işaretlenmesi aşamasında eşleşen anahtar noktalarından faydalanarak sahte piksellerin işaretlenmesi gerçekleştirilir.

Alt bölümlerde anahtar noktası tabanlı yöntemlerde kullanılan temel adımlara ilişkin literatürde yer alan çalışmalar verilerek detaylandırılacaktır.

1.4.2.1. Ön İşlem

Literatürde anahtar noktası tabanlı yöntemlerin ilki Huang ve arkadaşları tarafından 2008 yılında önerilmiştir [106]. Yöntemde girdi görüntüsünün ilk olarak RGB (Red, Green, Blue, Kırmızı Yeşil, Mavi) renk uzayında gri seviyeye dönüştürülmesi gerçekleştirilmiştir. Daha sonra geliştirilen yöntemlerin yine birçoğunda girdi görüntüsünün RGB renk uzayında gri seviyeli temsili kullanılmıştır [106-139]. Bu çalışmalarda girdi görüntüsünün gri

seviyeye dönüştürülmesinden sonra görüntünün bütününden anahtar noktalarının çıkarılması gerçekleştirilmiştir. Renk bilgisine ihtiyaç duyan çalışmalarda bu ön işlem aşaması gerçekleştirilmemiştir.

[140, 141]'de önerilen yöntemlerde ise ön işlem aşaması olarak görüntünün RGB renk uzayından HSV (Hue Saturation Value) renk uzayına dönüştürülmesi gerçekleştirilmiştir. İki yöntemde de daha sonraki aşamalarda oluşabilecek yanlış pozitif değerlendirmelerinin önüne geçmek amacı ile bahsedilen ön işlem gerçekleştirilmiştir.

1.4.2.2. Anahtar Noktalarının Çıkarılması

Huang ve arkadaşları tarafından önerilen yöntemde, anahtar noktalarının elde edilmesinde Ölçek Bağımsız Özellik Dönüşümü (Scale Invariant Feature Transform, SIFT) algoritmasının kullanılması önerilmiştir [106]. Ön işlem aşamasının ardından görüntünün bütününden SIFT anahtar noktaları çıkarılmıştır. Kullanılan SIFT algoritması ile anahtar noktalarına ait özellik tanımlayıcı vektörlerin elde edilmesi de gerçekleştirilmiştir. Elde edilen anahtar noktalarının, özellik vektörleri aracılığı ile eşleştirilmesi sağlanarak yöntem akışı devam etmektedir. [107-121]'de yer alan çalışmalarda da SIFT algoritmasından faydalanılmıştır. Anahtar noktası tabanlı kopyala-yapıştır sahteciliği tespiti yöntemlerinde en sık başvurulan anahtar noktası çıkarma algoritması SIFT algoritmasıdır. SIFT algoritmasının kullanıldığı yöntemlerde, algoritma doğrudan kullanılmış herhangi bir değişiklik yapılmamıştır. Bu algoritmaya dair detaylar alt bölümlerin ilkinde yer almaktadır.

Araştırmacılar daha sonra Hızlandırılmış Dayanıklı Özellikler (Speeded Up Robust Feature, SURF) algoritmasından faydalanarak elde edilen anahtar noktaları ile kopyala-yapıştır sahteciliği yöntemleri önermişlerdir [122-128]. Bu yöntemlerde SURF algoritmasının SIFT algoritmasına göre daha hızlı olması tercih sebebi olmuştur. Kopyala-yapıştır sahteciliği tespiti için önerilen yöntemlerde SIFT algoritmasından sonra en sık başvurulan anahtar noktası çıkarma yöntemi SURF olmuştur. Algoritmaya ait detaylar alt bölümlerin ikincisinde yer almaktadır.

Literatürde SIFT ve SURF algoritmasının haricinde Oriented Fast and Robust BRIEF (ORB) algoritmasının kullanılması ile sahtecilik tespiti yöntemleri öneren yöntemler mevcuttur [129,130]. [129]'da yazarlar ORB algoritmasına ölçek bağımsız özellik kazandırmak için, algoritmayı Gauss ölçek uzayında uygulamışlardır. Çalışmada ayrıca nesne kapama sahteciliği ele alınarak önerilen yöntemin başarısı vurgulanmıştır.

Anahtar noktası çıkarma yöntemlerinden Accelerated- KAZE (Hızlandırılmış KAZE, A-KAZE), BRISK (Binary Robust Invariant Scalable Keypoints) algoritmaları ile anahtar noktalarının elde edildiği sahtecilik tespiti yöntemleri de mevcuttur [131,132].

Literatürde ayrıca sık kullanılan anahtar noktası çıkarma algoritmalarının hibrit bir şekilde kullanılması ile sahtecilik tespiti yapan yöntemler de mevcuttur. [133, 134]'de SIFT ve SURF anahtar noktaları, [135]'de KAZE ve SIFT anahtar noktaları, [136]'da SURF ve A-KAZE anahtar noktaları, [138]' de AKAZE ve SIFT anahtar noktaları kullanılarak kopyala-yapıştır sahteciliği yöntemleri önerilmiştir. [138]'da önerilen yöntemde ise kopyala-yapıştır sahteciliği tespitine uygun, düşük kontrasta sahip bölgelerden de anahtar noktaları elde edebilmek amacı ile tekrarlamalı bir yöntem önerilmiştir.

1.4.2.2.1. Ölçekten Bağımsız Özellik Dönüşümü (Scale Invariant Feature Transform SIFT)

Ölçekten Bağımsız Öznitelik Dönüşümü (Scale Invariant Feature Transform, SIFT) algoritması, bir görüntüde ayırt edici yerel özellikleri çıkarmak için Lowe tarafından önerilmiştir [141]. SIFT ile ölçekleme, öteleme ve dönmeden bağımsız öznitelikler elde edilmesi sağlanmaktadır. Yöntem temelde dört adımdan oluşmaktadır, bunlar; ölçeksel uzaydaki ekstremum (uç değer) noktaların belirlenmesi, anahtar noktaların belirlenmesi, yön atama işlemi ve özellik tanımlayıcılarının belirlenmesi.

- Ölçeksel uzaydaki ekstrem (uç değer) noktaların tespiti: İlk adımda ölçeksel uzayda değişim göstermeyen noktaların belirlenmesi gerçekleştirilir. Bunun için yöntemde öncelikle ölçeksel uzay oluşturulmaktadır. SIFT algoritmasında Gauss ölçek uzayından faydalanılmıştır. Görüntünün farklı çekirdek değerine sahip Gauss süzgecinden geçirilmesi ve ardından birbirinden çıkartılması ile Gauss uzay farkı (Difference of Gausssian- DoG) elde edilmektedir. Buradaki amaç, görüntüdeki kenar bölgelerinin ve diğer ayrıntıların ortaya çıkarılmasıdır. Ayrıca yüksek frekans ayrıntılarını da yok eder.

Bir $I(x, y)$ girdi görüntüsünün Gauss filtresi $G(x, y, \sigma)$ ile konvolüsyon işlemi Eşiklik (1.3)'de verilmiştir.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{1.3}$$

Yöntemde Gauss ölçek uzayının oluşturulmasında farklı standart sapmalara sahip Gauss filtreleri kullanılmıştır. (1.4)'de farklı standart sapma değerine göre Gauss filtresi hesabı verilmiştir.

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{1.4}$$

Gauss filtresinin hesaplanmasında birinci ve ikinci ölçek için sırasıyla σ^1 ve σ^2 arasındaki oran k kadardır. (Yöntemde k=$\sqrt{2}$ olarak alınmıştır [142].) Bu durumda Gauss çekirdeği ölçek uzayı standart sapma değeri Eşitlik (1.5)'teki gibi hesaplanmaktadır.

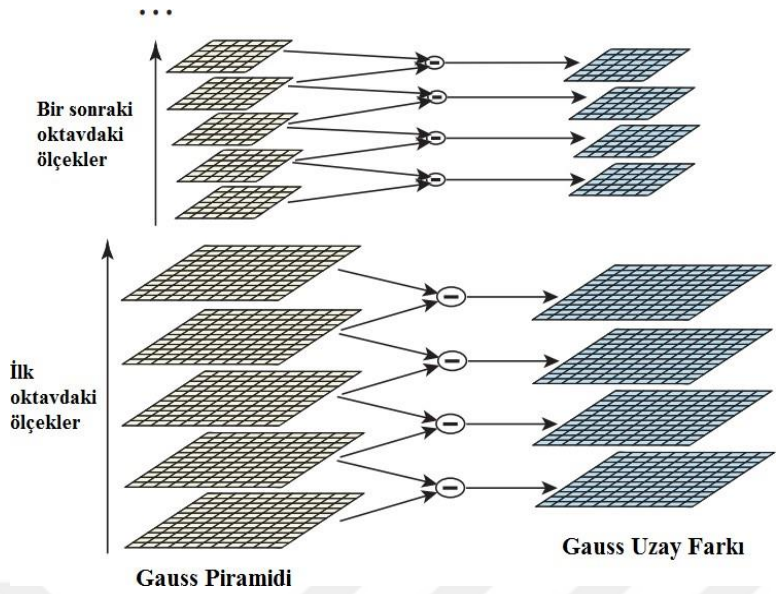
$$\sigma_n = k^{n-1}\sigma = \sqrt{2}^{n-1}\sigma \tag{1.5}$$

Ölçek uzayı, çarpım faktörü $k = 2^{1/s}$ olacak şekilde (x, y, σ) parametrelerinden dolayı üç boyutlu bir karşılaştırmaya ihtiyaç duyulduğu için her biri s+3 adet yumuşatılmış görüntü içeren oktav adı verilen serilere ayrılır. İkinci oktav, ilk oktavın σ_n kadar alt örneklenmiş ve boyutu yarı oranına indirgenmiş görüntü ile başlar. Sonraki her oktav için bu işlem bir önceki oktav kullanılarak oktav sayısı kadar benzer şekilde tekrarlanır.

Görüntünün Gauss ölçek uzayının oluşturulmasından sonraki adımda ise her oktav için Gauss uzay farkı (Difference of Gaussian, DoG) hesaplanır. DoG uzayı, farklı standart sapmalara sahip Gauss filtreleri ile konvolüsyonu gerçekleştirilmiş görüntülerin farkları alınarak elde edilmektedir, Eşitlik (1.6). İki ölçek uzay arasındaki farkların bulunmasına ilişkin genel yapı Şekil 1.13'te gösterilmiştir.

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned} \tag{1.6}$$

Gauss uzay farkı (DoG) oluşturulduktan sonra, ekstremum noktaların belirlenmesi gerçekleştirilir. Bunun için DoG görüntülerinde yer alan bütün pikseller kendi ölçeğindeki 8 komşusu ile, alt ve üst ölçeklerinde yer alan 9 piksel olmak üzere toplam 26 piksel ile karşılaştırılır. Eğer o anki piksel karşılaştırma yapılan pikseller arasında yerel maksimum veya yerel minimum olma özelliğine sahip ise ekstremum nokta olarak belirlenir ve aday anahtar noktası olma özelliğini gösterir.



Şekil 1.13. İki ölçek uzay arasındaki farkların (DoG)bulunması [141].

• Anahtar noktaların belirlenmesi: İkinci ana adımda aday anahtar noktaları arasından eleme işlemi yapılarak anahtar noktaları kesinleştirilir. Bu aşama, DoG operatörünün yoğun kenar olma özelliğine sahip olan bölgelerden etkilenmesi ve gürültü eklenme durumlarına karşı hassas olmasından dolayı düşük çözünürlüğe sahip ve kenarlarda yer alan anahtar noktaların minimize edilmesi gerekliliği temeline dayanır. Bunun için sırası ile iki yaklaşım kullanılmaktadır. İlkinde düşük çözünürlüğe sahip özellik noktalarının minimize edilmesi için DoG uzayında $D\,(x, y, \sigma)$ fonksiyonunun ikinci dereceden Taylor serisi kullanılmaktadır. Bu yaklaşım eşleşme ve durağanlık anlamında büyük bir gelişme sağlamaktadır. Eşitlik (1.7) ile özellik noktalarının yeni konumları belirlenmekte ve $D(\dot{x})$ elde edilmektedir.

$$\dot{x} = \frac{d^2D^{-2}}{dx^2}\frac{dD}{dx}, D(\dot{x}) = D + \frac{1}{2}\frac{dD^{\top}}{dx}\dot{x} \tag{1.7}$$

Her aday anahtar noktası için bu fonksiyon hesaplanarak $|D(\dot{x})|$ değerinin yazarlar tarafından 0.5 olarak belirlenen eşik değerinden küçük olması durumunda bu aday noktasının elenmesi gerçekleştirilir.

Aday anahtar noktalarının elenmesinde kullanılan ikinci yaklaşımda ise kenar bölgelerinde yer alan aday anahtar noktalarının elenmesi için Eşitlik (1.8)'de verilen Hessian matrisi kullanılmaktadır.

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \tag{1.8}$$

Eşitlik (1.9)'da verilen Hessian matrisinin öz değerleri ile elde edilen oranın belirlenen eşik değerinden büyük olması durumunda aday anahtar noktasının elenmesi gerçekleştirilir.

$$Tr(H) = D_{xx} + D_{yy} = \lambda_1 + \lambda_2, Det(H) = D_{xx}D_{yy} - \left(D_{xy}^2\right) = \lambda_1\lambda_2 \tag{1.9}$$

Burada λ_1 ve λ_2 öz değerlerdir. Eşitlik (1.10) yardımı ile $\lambda_1 = r\lambda_2$ olarak belirlenmiştir. Eğer $r > 10$ ise bu aday anahtar noktasının elenmesi gerçekleştirilir.

$$\frac{Tr(H)^2}{Det(H)} = \frac{(\lambda_1+\lambda_2)^2}{\lambda_1\lambda_2} = \frac{(r\lambda_2+\lambda_2)^2}{r{\lambda_2}^2} = \frac{(r+1)^2}{r}, \quad \frac{Tr(H)^2}{Det(H)} < \frac{(r+1)^2}{r} \tag{1.10}$$

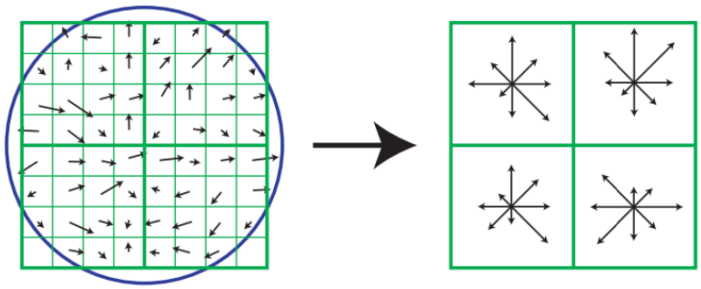
İki aşamalı eleme işleminin tamamlanması ile anahtar noktaları kesinleşmiş olur. Daha sonraki aşamada her bir anahtar noktasına yön atamasının yapılması gerçekleştirilmektedir.

- Anahtar noktalarına yön ataması: Belirlenen anahtar noktaların gradyan büyüklüğü $m(x, y)$ ve yönelimi $\theta(x, y)$, $L(x, y)$ görüntüsünün etrafındaki piksellerden faydalanarak Eşitlik (1.11)'deki gibi hesaplanmaktadır.

$$\begin{aligned} m(x,y) &= \sqrt{(L(x+1,y) - L(x-1,y)^2 + ((L(x,y+1) - L(x,y-1))^2} \\ \theta(x,y) &= tan^{-1}\frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)} \end{aligned} \tag{1.11}$$

Anahtar noktasının yöneliminin bulunması için öncelikle yön histogramı oluşturulur. Yön histogramı, her biri diğerinden 10 derece açı farkına sahip olacak şekilde 360 derecelik yön aralığını kapsayan 36 adet binden oluşur. Yön histogramı anahtar noktasının ölçeği olan σ'nın 1,5 katı kadar genişlikteki Gauss aralıklı dairesel penceresindeki özellik noktalarının gradyan büyüklük değeri olan $m(x, y)$ eklenmesi ile elde edilir. Örneğin pencere içerisindeki pikselin yönelimine en yakın binin değerine o pikselin gradyan büyüklüğü eklenir. Bu işlem pencere içerisindeki tüm pikseller için uygulanır. Oluşturulan histogramdaki en yüksek tepe noktasına sahip bin yönelim açı değerini vermektedir. Ayrıca aynı noktada farklı yönelime sahip anahtar noktaların (tüm anahtar noktaların %15'ini geçmemektedir) oluşturulması kararsızlığına sebep olabilme izlenimi verse de anahtar noktasının benzersizliğini sağlayarak dengeyi sağlamaktadır.

• Özellik tanımlayıcıların belirlenmesi: Bu adımda, belirlenen anahtar noktalarına ait ayırt edici özellik vektörlerinin oluşturulması sağlanmaktadır. Öncelikle anahtar noktası etrafında, bulunduğu ölçek ile orantılı mesafedeki komşu piksellerin gradyan büyüklükleri ve yönelim açıları belirlenir. Anahtar noktası etrafında 16x16 boyutlu bir blok alınmakta ve birbirleri arasında 45 derece açı farkı olacak şekilde 8 yönelime sahip yönelim histogramı içeren 4x4'lük örnekleme alanı oluşturulmaktadır. Her okun yönelimi histogramın yönelim bilgisini; büyüklüğü ise bir hesaplanan gradyan büyüklüğünü ifade eder. Böylece her biri 8 yönelimden oluşan 4x4 histogram alanına sahip bir anahtar noktası 4x4x8=124 boyutlu bir özellik tanımlayıcı vektör ile temsil edilmektedir. Şekil 1.14'te görüntü gradyanı ve anahtar nokta tanımlayıcılar verilmiştir. Şekilde 8x8 örnek kümesinden hesaplanan 2x2 boyutlu özellik tanımlayıcı dizisi gösterilmiştir. Özellik tanımlayıcı vektör, şekilde görülen okların uzunluğuna karşılık gelen yön histogramları değerlerini içeren bir vektör biçimindedir.



Şekil 1.14. Görüntü gradyanı ve anahtar nokta tanımlayıcılar [142]

1.4.2.2.2. Hızlandırılmış Dayanıklı Özellikler (Speeded Up Robust Feature, SURF)

SURF algoritması bir görüntüden dönme, ölçekleme ve ötelemeden etkilenmeyen yerel özellik noktaların çıkarılması için Bay tarafından önerilen algoritmadır [142]. Bu algoritma SIFT algoritmasına benzer adımları içerse de yöntemin daha hızlı çalışabilmesi amacı ile bazı iyileştirmeleri barındırmaktadır. İyileştirmelerin en önemlisi görüntünün konvolüsyon hesabı yapılırken tümlev görüntülerin kullanılması ve 2 boyutlu Haar dalgacıklarından faydalanılmasıdır. Böylece SURF algoritmasının SIFT'e göre yaklaşık dört kat daha düşük hesaplama karmaşıklığına sahip olması sağlanmıştır. Yönteme ait anahtar

noktalarının ve özellik tanımlayıcı vektörlerin elde edilmesi aşamalarına ilişkin detaylar aşağıdaki gibidir.

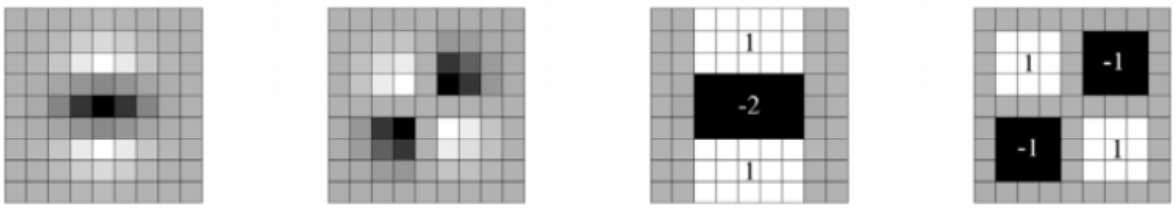
- Anahtar Noktalarının Belirlenmesi: Anahtar noktalarının elde edilmesinin ilk aşamasının temelinde Hessian matrisinin görüntüdeki farklı görüntü bölgesi (blob) ortaya çıkarma özelliğinden faydalanmak vardır. Hessian matris determinantı ölçüt olarak kullanılarak bölgeler arasındaki değişimler hakkında bilgi edinilmektedir. Bir I görüntüsünde, σ ölçeğindeki bir $x = (x, y)$ noktasının Hessian matrisi Eşitlik (1.12)'deki gibi elde edilmektedir.

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{xy}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix} \tag{1.12}$$

Burada $L_{xx}(x, \sigma)$, I görüntüsündeki (x, y) noktasının ikinci derece Gauss türevin konvolüsyon sonucudur, Eşitlik (1.13)'te verilmiştir. $L_{xy}(x, \sigma)$ ve $L_{yy}(x, \sigma)$'de (x, y) noktasının sırası ile xy ve y yönündeki ikinci derece türevlerinin konvolüsyonları olmak üzere benzer şekilde elde edilmektedir.

$$L_{xx}(x, \sigma) = I(x) * \frac{d^2}{dx^2} g(\sigma) \tag{1.13}$$

SURF algoritmasında Hessian matrisi için kullanılan Gauss fitresi uygulamak yerine kutu filtreleri kullanılmaktadır. Şekil 1.15'te $9x9$ boyutunda $\sigma = 1.2$ değeri ile Gauss filtresi kullanılarak elde edilen ölçek uzayın en alt seviyesindeki (en düşük ölçeği yani en yüksek uzaysak çözünürlüğü temsil eder) y ve xy yönündeki ikinci dereceden Gauss türevi ve bu türevlerin kutu filtreleri örnekleri bulunmaktadır. Burada renkli alanlar sıfırı, beyazlar pozitifi, siyahlar ise negatifi temsil etmektedir.



Şekil 1.15. Soldan sağa doğru: y yönünde ikinci derece Gauss türevi, xy yönünde ikinci derece Gauss türeci, bu türevlerin kutu filtreleri [142]

Hessian matrisinin determinantının hesaplama verimliliğini artırmak için bölgelere uygulanan ağırlıklar basit tutulur ve ayrıca Eşitlik (1.4)'deki gibi ağırlıkların daha da dengelenmesi gerekir. Buradaki denge değeri olan 0.9 değeri, Gauss çekirdekleri arasındaki enerji dönüşümü ile hesaplanır.

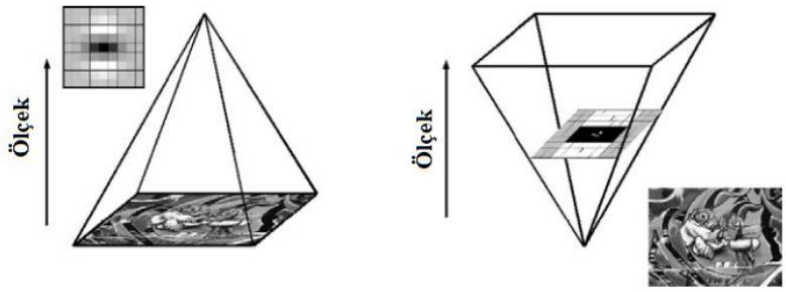
$$\det\left(\mathcal{H}_{\text{yaklaşık}}\right) = \mathrm{D_{xx}D_{yy}} - \left(0.9\mathrm{D_{xy}}\right)^2 \tag{1.14}$$

Yöntemde (x, y) noktasının kutu filtreler ile konvolüsyon işlemi yerine tümlev görüntüler kullanılarak işlem zamanının düşürülmesi hedeflenmiştir. Tümlev görüntüler, görüntünün her pikseli için Eşitlik (1.15)'deki değer hesaplanarak yeni bir görüntü elde edilmektedir. Bu da x ve y etrafındaki pikseller arasında kalan dikdörtgensel bölgede yer alan piksel değerlerinin toplamı ile elde edilmektedir.

$$\mathrm{I\Sigma(x,y)} = \sum_{\mathrm{i=0}}^{\mathrm{ist}} \Sigma_{\mathrm{j=0}}^{\sqrt{\leq \mathrm{y}}} \mathrm{I(i,j)} \tag{1.15}$$

Ölçek uzayı oluşturulurken kutu süzgeçleri ve tümlev görüntülerin kullanımından dolayı SIFT algoritmasında olduğu gibi bir önceki filtrelenmiş katmandaki görüntüye aynı filtre uygulanamamaktadır. Dolayısıyla yöntemde farklı boyutlarda ve ölçeklerde kutu süzgeçleri tümlev görüntülere uygulanarak ölçek-uzay yapısı oluşturulmaktadır. Ölçek uzayının oluşturulması işlemine 9x9'luk filtre ile başlanmakta ve daha sonra filtre boyutu sırasıyla 15x15, 21x21 ve 27x27 olacak şekilde uygulanmaktadır. Bu yüzden ölçek uzayı tekrarlamalı bir şekilde boyutu azalan görüntülerden ziyade artan ölçekli görüntülerden oluşmaktadır. SURF algoritmasında oluşturulan piramitsel ölçek uzayı Şekil 1.16'da sol taraftaki gibidir.

Yöntemde oluşturulan ölçek-uzayda Hessian matrisinin determinantlarının sonuçlarına göre anahtar noktaları belirlenmektedir. Biri pikselin olduğu ölçek olmak üzere alt ve üst komşu ölçekler arasından $3x3$ boyutlu alan içinde toplamda $3x3x3 = 27$ piksel arasından en yüksek gradyan değerine sahip piksel anahtar noktası olarak belirlenmektedir.



Şekil 1.16. Yöntemde kullanılan piramitsel ölçek uzay [143]

- Özellik Tanımlayıcıların Belirlenmesi: Anahtar noktalarını temsil etmek üzere özellik tanımlayıcıların atanması işleminde ilk olarak ilgili anahtar noktası etrafında çembersel bir alan belirlenir. Bu alana parlaklığa karşı duyarsız olması ve tümlev görüntü ile hızlı bir şekilde hesaplanabilmesi sebebi ile Haar dalgacık filtreleri uygulanır.

Anahtar noktalara dönme bağımsızlık sağlamak için özellik tanımlayıcıların belirlenmesinden önce oryantasyon tanımlanması yapılmaktadır. Bu amaçla ilk olarak anahtar noktasının tespit edildiği ölçek s ile temsil edilirse, anahtar noktası etrafında $6s$ yarıçaplı bir çember belirlenir. Belirlenen çember içinde Şekil 1.17'de gösterilen, kenar uzunluğu $4s$ olan x ve y yönündeki Haar-dalgacık yanıtları hesaplanır. Böylece x ve y yönündeki türevler olan dx ve dy elde edilmiş olur. Geometrik deformasyonlara ve lokalizasyon hatalarına karşı sağlamlığı artırmak için, dx ve dy yanıtları anahtar noktası merkez olacak şekilde Gauss ağırlıklandırılması yapılır ($\sigma = 3.3s$). Daha sonra her alt alan için elde edilen dx ve dy değerleri toplanır ve bu toplamlar tanımlayıcı vektörün ilk kısmını oluştururlar. Ayrıca tanımlayıcının kutupsal yoğunluk değişimleri hakkında bilgi de tutması için bu yanıtların mutlak değerlerinin ($|dx|$ ve $|dy|$) toplamları da elde edilir. Böylece her alt bölge dört boyutlu tanımlayıcı vektöre sahip olmuş olur. $v = (\sum dx, \sum dy, \sum |dx|, \sum |dy|)$. Her 4x4 boyutlu alt vektör için dört boyutlu vektör çıkartılır. Dolayısıyla $4x(4x4) = 64$ boyutlu tanımlayıcı vektör oluşturulmuş olur.

Şekil 1.17. Yöntemde kullanılan Haar dalgacık türleri (sol: y yönünde, sağ: x yönünde) [143]

1.4.2.3. Anahtar Noktalarının Eşleştirilmesi

Anahtar noktası tabanlı yöntemlerin ilki olan Huang vd.nin önerdiği yöntemde, ön işlem aşaması ve anahtar noktalarının elde edilmesinin ardından uygulanan eşleşme aşamasında Best Bin First (BBF) yaklaşımı kullanılarak birbirine en benzer anahtar noktalarının eşleştirilmesi gerçekleştirilmiştir [106]. Elde edilen bütün anahtar noktaları öncelikle eşit sayıda rastgele iki gruba ayrılmış, bu iki grupta yer alan anahtar noktaları kendilerine ait özellik tanımlayıcıların BBF yaklaşımının kullanılması ile eşleştirilmesi gerçekleştirilmiştir. Eşleşme aşamasında kullanılan ω eşik değerinin 0.1 ile 0.9 arasında değişimine göre elde edilen toplam eşleşme sayısı ve bunlar arasındaki hatalı eşleşmeler rapor edilerek çalışma tamamlanmıştır. Sahte bölgelerin piksel tabanlı işaretlenmesi gerçekleştirilmemiştir. Deneysel çalışmalarda yazarlar tarafından oluşturulan dört adet sahte görüntü sırası ile dönme, JPEG sıkıştırma ve gürültü ekleme atakları uygulanarak elde edilen eşleşme sonucu sunulmuştur. [107]'de önerilen yöntemde yine girdi görüntüsünden elde edilen SIFT anahtar noktaları BBF yaklaşımı ile eşleştirilmiştir.

[108]'de önerilen yöntemde görüntünün bütününden elde edilen SIFT anahtar noktaları yazarların genelleştirilmiş 2NN testi (Generalized 2 Nearest Neighbour, g2NN en yakın iki komşu) olarak temsil ettiği yaklaşım ile eşleştirilmiştir. Daha sonra eşleşen anahtar noktalarının Hiyerarşik Kümeleme (Hierarchical Clustering) yaklaşımı ile kümelendirilmesinin ardından Random SAmple Consensus (RANSAC) algoritması ile eşleşmeler arası geometrik dönüşüm tahmininde bulunulmuştur. Eşleşmeler arasındaki geometrik dönüşüm Eşitlik (1.16)'daki ifade edilmektedir. Burada H 3x3 boyutlu afin homografi matrisini temsil etmektedir. RANSAC ile elde edilen homografi matrisine uyum sağlamayan eşleşmeler hatalı eşleşme (outliers) olarak belirlenerek eşleşme matrisinden

çıkarılmıştır. Aynı yazarlar [110]'da önerdikleri yöntemde yine g2NN yaklaşımını kullanmışlardır.

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \tag{1.16}$$

[109]'da önerilen yöntemde SIFT anahtar noktalarının eşleştirilmesinde k-d ağacı yaklaşımından faydalanılmıştır. Yazarlar önerdikleri yaklaşımın daha az hatalı eşleşme ile sonuçlanması sebebi ile seçildiğinden bahsetmişlerdir. [111]'deki yaklaşımda ise SIFT anahtar noktaları Gaussian Mixture Model (GMM) yaklaşımı ile eşleştirilmiştir. Sunulan yaklaşım ile kopyalanan bölgenin birden fazla bölgeye yapıştırılması durumunda da etkin performans gösterebilmesi nedeni ile seçildiği raporlanmıştır. Bu çalışmada da yazarların yine hatalı eşleştirmelerin elenmesi için RANSAC yaklaşımından faydalandıkları yer almaktadır. Deneysel sonuçlar bölümünde Comofod verisetinden [143] ve yazarların GIMP yazılımı ile oluşturdukları sahte görüntüler üzerinde elde edilen görsel sonuçlardan faydalanılmıştır. [112]'de önerilen yöntemde elde edilen anahtar noktaları Best-Bin-First (BBF) algoritması kullanarak eşleştirilmiştir. [113]'de ise 2NN yaklaşımı ile anahtar noktaları eşleştirilmiştir. Yöntemde hatalı işaretlemelerin giderilmesi için Optimized Random Sampling Algorithm (ORSA) algoritmasından faydalanılmıştır. [114]'deki yöntemde de yine [108]'de önerilen g2NN yaklaşımı kullanarak anahtar noktaların eşleşmesi gerçekleştirilmiştir. [115]'de SIFT anahtar noktalarına ait özellik tanımlayıcılar yöntemde kullanılan teknik ile ikili forma dönüştürülmüştür. Daha sonra elde edilen ikili özellik vektörlerinden hash değerleri elde edilmiştir. Yöntemde aynı hash değere sahip özellik vektörlerinin arasından Hamming uzaklığı belirlenen eşik değerine göre kontrol edilerek eşleşme işlemi gerçekleştirilmiştir. [118]'de FUZZY C-means kümeleme yaklaşımı ile SIFT anahtar noktalarına ait özellik tanımlayıcıların kümelenmesi gerçekleştirilmiş, aynı kümede yer alan anahtar noktalarının yöntemde belirlenen uzaklık eşiğinden küçük olması durumunda eşleştirilmesi gerçekleştirilmiştir. [119]'daki yöntemde de g2NN yaklaşımı kullanılarak SIFT anahtar noktalarının eşleşmesi gerçekleştirilmiştir.

Chen ve arkadaşlarının [121]'de önerdikleri yöntem, SIFT anahtar noktalarının kümelenmesi ve daha sonra eşleştirilmesi temeline dayalı olup, çalışma zamanının düşürülmesi amaçlanmıştır. Kümeleme işlemi iki aşamada gerçekleştirilmiş ve bu aşamaların tamamlanması ile bütün anahtar noktaları altı kümeye ayrılmıştır. Anahtar

noktaları öncelikle anahtar noktalarını tanımlamada hesaplanan ölçek değerine göre sınıflandırılmıştır. Ölçek değerine göre üç küme oluşturulmuştur. Bir anahtar noktasının ölçek değeri σ_i olarak gösterildiğinde, $S_1 = \{0 \leq \sigma_i < 3\}, S_2 = \{2{,}5 \leq \sigma_i < 4\}, S_2 = \{3 \leq \sigma_i < 3{,}5\}$ durumlarına göre kümelenmesi gerçekleştirilir. Daha sonra her bir kümede yer alan anahtar noktaları, üç renk kanalı (RGB) için parlaklık bilgisine göre kümelenir. $R_1(0-127), R_2(128-255), G_1(0-127), G_1(128-255), B_1(0-127), B_2(128-255)$. Renge göre kümeleme işlemi tüm kombinasyonları sağlayacak şekilde değerlendirildiğinde sekiz kombinasyon elde edilmiş olur. Böylece, yönteme göre anahtar noktaları ile toplamda 3x8=24 küme oluşturulabilmektedir. Her bir kümede yer alan anahtar noktalarının kendi içerisinde Rg2NN(Revised g2NN) eşleşme yöntemi ile eşleştirilmesi ve hatalı eşleşmelerin olasılığı J-Linkage yaklaşımının kullanılması ile azaltılması önerilmiştir. Bu aşamada çıkarılan afin dönüşüm matrisinin elde edilmesi sonrasında görüntünün afin dönüşümü yapılarak girdi görüntüsü ile dönüşüm sonrası elde edilen görüntüde kopyalanan ve yapıştırılan bölgelerin üst üste çakışması amaçlanmıştır.

[144]'de önerilen yöntemde Fast Approximated LoG (FALoG) filtresi ve FRIF (Fast Robust Invariant Feature) algoritması kullanılarak anahtar noktaları ve özellik vektörleri elde edilmiştir. Anahtar noktalarının eşleşmesinde yine R2NN yaklaşımı kullanılmıştır. Hatalı eşleşmelerin giderilmesi için görüntü öncelikle SLIC algoritması ile segmentlere ayrılmıştır. Bir segmentte eşleşen anahtar sayısının 3'ten az olduğu durum, hatalı eşleşme olarak değerlendirilmiş ve bu durumda olan eşleşmeler eşleşme matrisinden çıkarılmıştır.

[145]'de Park ve Choeh (2017) tarafından önerilen yöntemde ise çoklu kopyala-yapıştır ataklarını da tespit edebilmek için SIFT anahtar noktaları adaptif g2NN(ag2NN) algoritması kullanılarak eşleştirilmiştir. Daha sonra geometrik dönüşüm tahmini Maximum Likelihood yöntemi kullanılarak eşleşen noktalar sayesinde gerçekleştirilmiştir. Elde edilen dönüşüm matrisine uygun olmayan eşleşmeler hatalı eşleşme olarak kabul edilip eşleşme matrisinden çıkarılmıştır.

1.4.2.4 Sahte Bölgelerin Belirlenmesi

Anahtar noktası tabanlı yöntemler başlangıçta sahte bölgelerde yer alan anahtar noktaları eşleşmelerinin rapor edilmesi ve yeterli eşleşmenin varlığı halinde görüntünün sahte olup olmadığını raporlayacak düzeyde olup sahte bölgelerin sınırlarını belirleyecek bir aşamayı kapsamamaktaydı. Sahte bölgelerin sınırlarının piksel tabanlı işaretlendiği ilk çalışma [110]'da yer alan Amerini ve arkadaşlarının 2013'te önerilmiştir. Anahtar nokta eşleşmesinin ardından var olan eşleşmeler arasındaki geometrik ilişki RANSAC yaklaşımı kullanılarak elde edilmiştir. Önerilen yaklaşım ile elde edilen **3x3** boyutlu H homografi matrisi bu ilişkiyi temsil etmektedir. Yöntemde matrise uyum sağlamayan eşleşmeler hatalı eşleşme olarak kabul edilip eşleşme matrisinden çıkarılmıştır. Sahte bölgelerin belirlenmesi aşamasında girdi görüntüsü homografi matris ile transform edilmiş, kopyalanan ve yapıştırılan bölgelerin nerede ise üst üste örtüşmesi sağlanmıştır. Daha sonra transform edilen görüntü ile gri seviyeli girdi görüntüsü arasında blok bazında zero mean normalized cross-correlation (ZNCC) yaklaşımı kullanılarak lokalizasyon işlemi gerçekleştirilmiştir.

[113]'de anahtar noktalarının eşleşmesinin ardından Optimized Random Sampling Algorithm (ORSA) yaklaşımı kullanılarak eşleşmeler arasındaki geometrik ilişki belirlenmiş, bu ilişkiye uymayan eşleşmelerin elenmesi gerçekleştirilmiştir. Daha sonra sahte bölgelerin belirlenmesi için Simple Linear Iterative Clustering (SLIC) algoritması ile görüntünün bölütlere ayrılması gerçekleştirilmiştir. Yöntem anahtar nokta eşleşmesinin olduğu bölütte yer alan pikselleri sahte piksel olarak belirleyip matematiksel morfolojik işlemler sonrası piksel bazlı lokalizasyon aşamasını tamamlamıştır.

[121]'de sahte bölgelerin sınırlarının belirlenmesi aşamasında, benzer komşuların araştırmasına dayanan bölge büyütme (region growing) tekniğine benzer bir lokalizasyon tekniği önerilmiştir. Bu aşamada, alt blokların PCT ve PSNR bilgilerinden faydalanılmıştır.

[144]'deki yöntemde anahtar nokta eşleşmesi aracılığı ile elde edilen afin dönüşüm matris ile transform edilmiş hali ile orijinal hali birebir karşılaştırılmıştır. Karşılaştırma için Normalized Production Correlation (NNPROD) kullanılmıştır. Yöntemin deneysel analizinde GRIP ve FAU verisetlerinden faydalanılmış, dönme, ölçekleme, bulanıklaştırma ve JPEG sıkıştırma ataklarına karşı yapılan testler rapor edilmiştir. Dönme atağı sonuçlarında yalnızca 2-10 derece dönme atağı uygulanan görüntüler kullanılmış olup daha büyük derece ile gerçekleştirilen ataklar ele alınmamıştır.

1.4.3. Bölüt Tabanlı Yöntemler

Literatürde blok tabanlı ve anahtar noktası tabanlı yöntemlerde iyileştirme üzerine çalışmalar devam ederken araştırmacılar görüntünün bölütlenmesine dayalı yaklaşımların sahtecilik tespitinde kullanılması amacı ile çalışmalarda bulunmuşlardır. Bu bölümde bu çalışmalardan bahsedilecektir.

Literatürdeki bölüt tabanlı sahtecilik tespiti yöntemlerinin ilki Li ve arkadaşları tarafından 2015 yılında önerilmiştir [146]. Yapılan çalışmada görüntü anahtar noktaları çıkarılmadan önce anlamsal olarak birbirinden bağımsız bölütlere ayrılır. Görüntünün bölütlenmesi için SLIC algoritmasından faydalanılmıştır. Bölütler arası yapılan eşleme ile kopyalanıp yapıştırılan bölgelerin tespit edilmesi amaçlanmıştır. Yöntemde eşleşme işlemi iki aşamadan oluşmaktadır. İlk aşamada anahtar noktaları ve bunlara ait özellik vektörleri çıkarılır ve eşleştirilir. Yöntem gürültü ekleme, JPEG sıkıştırma, 2-10 derecedeki dönme ve ölçekleme ataklarına karşı dayanıklı iken bulanıklaştırma atağına karşı dayanıksızdır.

Pun ve arkadaşları bir diğer bölüt tabanlı kopyala-yapıştır sahteciliği tespiti yöntemini önermişlerdir [147]. Görüntünün yine SLIC algoritması ile bölütlenmesi gerçekleştirilmektedir. İlk bölütleme işleminde bölüt boyutu sabit belirlenmiştir. Başlangıç bölütlerinden Ayrık Dalgacık Dönüşümü (ADD) aracılığı ile alçak frekans ve yüksek frekans enerjileri hesaplanıp enerji seviyelerine göre ilgili bölüt yeniden bölütlenmek üzere yeni bölüt boyutu belirlenmesi gerçekleştirilmiştir. Böylece adaptif bir şekilde belirlenen bölüt boyutlarına göre görüntü bölütlenmesi tamamlanmıştır. Ardından görüntünün her bir bölütünü temsil edecek şekilde SIFT algoritmasından faydalanarak, her bir bölütte yer alan anahtar noktasına ait özellik tanımlayıcılar bölüt özelliğini temsil edecek şekilde ayarlanmıştır. Bölüt özelliklerinin korelasyon katsayısı temelli eşleştirilmesi gerçekleştirilerek şüpheli sahte bölütler belirlenmiştir. Şüpheli sahte bölütlerin yerel renk bilgisine göre de bölge genişletmesi ve morfolojik işlem aşamalarının tamamlanması ile de sahte bölgelerin son hali ortaya konmuştur. Yöntemin dönme, ölçekleme ve JPEG sıkıştırma ataklarına karşı araştırmaları yapılarak dayanıklılık durumu ortaya konmuştur.

Bir diğer çalışmada, görüntünün bölütlenmesi mantığı hatalı eşleşmelerin giderilmesi amacı ile kullanılmıştır [138]. Yöntemde anahtar noktalarının eşleşmesinin tamamlanmasının ardından görüntü SLIC algoritması ile bölütlenerek anahtar noktası eşleşmesinin eşleşen bölüt çiftinde en az üç tane olup olmadığı değerlendirilmiştir.

[148]'de önerilen yöntemde ise anahtar noktalarının çıkarılmasından önce görüntünün SLIC algoritması ile örtüşmeyen bölütlere ayrılması gerçekleştirilmiştir. SIFT algoritması ile elde edilen anahtar noktalarının eşleşmesi ile eşleşen anahtar noktalarının yer aldığı bölütlerin eşleştirilmesi gerçekleştirilmiştir. Eşleşen iki bölüt arasında bir transformasyon matrisi tahmini yapılmaktadır. Bu matrisin tahmininin gerçekleştirilememesi durumunda blok tabanlı yöntemlerin mantığından faydalanarak benzer adımlar tekrarlanmıştır. Yapılan çalışmanın dönme, ölçekleme, JPEG sıkıştırma ve gürültü ekleme ataklarına dayanıklılığı deneysel sonuçlarda rapor edilmiştir. Ancak dönme atağı durumunda yalnızca 2, 4, 6, 8 ve 10 derece dönme atağı uygulanmış görüntüler kullanılmış olup, daha yüksek dereceli dönme durumlarındaki performans sonuçları verilmemiş ve bu atak durumundaki dayanıklılığı ile ilgili analizler yetersiz kalmıştır.

[149]'da yer alan yöntem Wang ve arkadaşları tarafından önerilmiş olup, görüntü Minimum Barrier Superpixel (MBS) yöntemi ile örtüşmeyen düzensiz bölütlere ayrılır. Her bir bölüt entropi bilgisine göre, dokusuz bölüt ve dokulu bölüt olarak sınıflandırılmaktadır. Dokulu ve dokusuz bölütlerin birleştirilmesi ile dokulu bölge ve dokusuz bölge olmak üzere görüntü iki sınıfa ayrılmıştır. Daha sonraki aşamalarda bu bölgelerden SURF (Speeded-up robust features) anahtar noktalarını çıkarılmıştır. Dokusuz bölgelerden daha fazla anahtar nokta elde edebilmek için anahtar noktası çıkarma yönteminde kullanılan kontrast eşik değeri daha düşük tutulmuş, özellik tanımlayıcı vektörler PCET (Polar Complex Exponential Transform) kullanılarak elde edilmiştir. Benzer anahtar noktalarının bulunması için geliştirilmiş g2NN yaklaşımından faydalanılmıştır. RANSAC ile olası hatalı eşleşmelerin giderilmesi amaçlanmıştır. Anahtar noktalarının etrafında bir dikdörtgensel bölge alınarak bu bölgenin içinde kalan sahtecilik sınırlarının belirlenmesi, yöntemin ikinci ana aşamasında gerçekleştirilmiştir. Belirlenen dikdörtgensel bölgeler, örtüşen karesel bloklara ayrılır ve her bir blok yine PCET ile elde edilen özellik vektörü ile temsil edilir. Benzer blokların bulunması için özellik vektörleri yine g2NN yaklaşımı ile eşleştirilmiştir. Matematiksel morfolojik işlemler ile sahtecilik sınırının daha düzgün belirlenmesi gerçekleştir. Yapılan çalışmaların değerlendirilmesinde GRIP ve FAU verisetleri kullanılmıştır ancak verisetinde yer alan görüntülerin bütünü değerlendirilmemiş, seçili bazı görüntüler üzerinden sonuç rapor edilmiştir.

[150]'de yer alan yöntem sahtecilik tespiti için ilk olarak girdi görüntüsünün SLIC ve k-means kümeleme yaklaşımı ile bölütlere ayrılmasını gerçekleştirmişlerdir. Bunun için öncelikle bütün görüntü SLIC bölütleme yöntemi ile düzensiz bölütlere ayrılmış, daha sonra

bütün görüntüden SIFT anahtar noktaları çıkarılmıştır. Her bir bölüt için B_i, o bölütte yer alan piksellerin ortalaması M_i, standart sapması S_i, o bölütteki anahtar nokta sayısının bütün görüntüden çıkarılan anahtar nokta sayısına oranı R_i değerleri hesaplanır. Bu üç değerin (M_i, S_i, R_i) ve K-means kümeleme yaklaşımının kullanılması ile görüntü dokulu ve dokusuz olmak üzere ikiye ayrılır. Dokulu bölgeler için SIFT ile anahtar noktaları kullanılırken, dokusuz bölgelerden dense Harris noktaları çıkarılır. Bu aşamada kontrast eşik değeri ($t_{th} = 10^{-5}$) oldukça düşük seçilmiştir. Anahtar noktalarının tanımlanması için 36 boyutlu sektör mask yaklaşımı kullanılmıştır. Ayrıca RGB renk kanallarının ortalamaları ve standart sapmaları da özellik vektörlerine dâhil edilerek, her bir anahtar noktası 42 boyutlu bir özellik tanımlayıcı vektör ile temsil edilmiştir. Özellik vektörlerinin eşleşmesinde g2NN yaklaşımı kullanılmış ve varsa hatalı eşleşmeler RANSAC ile giderilmiştir. Yapılan çalışmada, hatalı bölgelerin sınırlarının belirlenmesi gerçekleştirilmemiştir. Yalnızca görüntünün sahte olup olmağı ortaya konulmuş yani piksel bazlı bir değerlendirme yapılmamıştır.

1.4.4. Hibrit Yöntemler

Literatürdeki anahtar noktası tabanlı ve blok tabanlı yöntemlerin avantaj ve dezavantajlarının göz önünde bulundurularak bu iki yöntemi hibrit bir şekilde kullanan yöntemler bulunmaktadır. Bu yöntemlerden bazılarına bu bölümde yer verilecektir.

[149]'da yer alan yöntem bir önceki bölümde bölüt tabanlı yöntem olarak değerlendirilmiş olsa da görüntüden hem anahtar nokta özellikleri hem de blok özelliklerinin faydalanması sebebi ile bu kategoridede değerlendirilebilir. Yöntemde görüntünün bölütlenmesinin ardından her bir bölütün entropi bilgisine göre dokulu veya dokusuz olarak sınıflandırılması gerçekleştirilmiştir. Dokulu bölütler anahtar noktası tabanlı teknik ile araştırılırken, dokusuz bölütlerde yer alabilecek sahteciliğin tespiti için blok tabanlı tekniklerden faydalanılmıştır.

Bir diğer hibrit yaklaşım olan [151]'de, Sun ve arkadaşları temelde üç aşamadan oluşan bir sahtecilik tespit yöntemi önermişlerdir. İlk aşamada görüntü örtüşmeyen bloklara ayrılmaktadır ve görüntünün bütününden SIFT anahtar noktaları elde edilir. Bir bloktan elde edilen anahtar nokta sayısı önceden belirlenen eşik değerine göre karşılaştırılarak ilgili blok dokulu veya dokusuz olarak sınıflandırılmaktadır. SIFT algoritması ile dokulu bölgelerde yer alan anahtar noktalarına ait özellik tanımlayıcı vektörler elde edilirken, Zernike momentleri kullanılarak dokusuz bölgelere ait özellik vektörleri oluşturulur. Daha sonra dokulu ve dokusuz bölgelerden elde edilen özellik vektörleri kendi aralarında eşleştirilir.

Önerilen yöntemin dönme, ölçekleme ve JPEG sıkıştırma atakları durumundaki performans sonuçları verilirken gürültü ekleme ve bulanıklaştırma atakları gibi diğer ataklara karşı dayanıklılığı hakkında analizler yapılmamıştır.

Meena ve Tyagi'nin önerdikleri yöntemde, görüntü öncelikle düz bölge ve dokulu bölge olmak üzere ikiye ayrılır [152]. Bunun için görüntünün bütününe standart sapma filtresi kullanılmıştır. Her bir piksele, 9x9'luk filtre uygulanarak homojenlik eşiği (uniformity thresold U=2) uygunluğu kontrol edilmiştir. Homojenlik şartını sağlayan pikseller yani standart sapması düşük olan pikseller düz bölgeye, diğer pikseller dokulu bölgeye dâhil edilmiştir. Sahtecilik tespitinde dokulu ve dokusuz bölgeler için iki farklı yaklaşım uygulanmıştır. Dokulu bölgelerden SIFT anahtar noktaları çıkarılmış, g2NN yaklaşımı ile benzer anahtar noktaların eşleştirilmesi amaçlanmıştır. Varsa hatalı eşleşmelerin giderilmesi için öncelikle RANSAC algoritması ile afine transformasyon (dönüşüm) matrisi çıkarılmış, bu matrise uyum sağlamayan eşleşmeler hatalı eşleşme olarak değerlendirilmiştir. Yöntemin anlatımında eşleşen noktalar etrafında sahte bölgelerin sınırlarının belirlenmesinde fazla detay verilmemiş olup, anahtar noktalarının etrafında yer alan piksellerin sahte pikseller olarak ele alındığı belirtilmiştir. Dokusuz bölgelerin sahtecilik tespiti için önerilen yaklaşımda ilk olarak görüntü örtüşen karesel bloklara ayrılmıştır. FMT (Fourier Mellin Transform) ile görüntü bloklarından özellik vektörleri elde edilmiş olup referans alınan PatchMatch tabanlı eşleşme yöntemi uygulanmıştır. Varsa hatalı eşleşmelerin giderilmesi Dense Linear Fitting Error yaklaşımı ile giderilmiştir. Önerilen yöntemin performans değerlendirmesinde GRIP ve FAU dataseti kullanıldığı belirtilmiştir. GRIP veri setinin yalnızca plain (ataksız) görüntüleri kullanılmıştır. Ayrıca sonuç değerlendirmesi yalnızca görüntü bazında yapılmış olup, piksel bazında bir değerlendirme yapılmamıştır.

Bir diğer hibrit yaklaşımda ise ilk olarak görüntünün bütününden SIFT anahtar noktaları çıkarılmaktadır [153]. Yazarlar, SIFT anahtar noktalarına ait özellik tanımlayıcıları LBP histogramlarından çıkarılan bilgi ile desteklemişlerdir. Bunun için öncelikle, her anahtar noktasının etrafından 16x16 boyutlu pencere değerlendirilerek 256 boyutlu LBP kodu çıkarılmıştır. Bu histogram bilgisi, düzenli, düzensiz ve ardışık paternlerin gruplanması ile 10 boyuta düşürülmüştür. 128 boyutlu SIFT anahtar nokta tanımlayıcılara ek olarak çıkarılan 10 boyutlu özellik vektörleri değerlendirilmeye alınmak üzere, her bir anahtar nokta tanımlayıcısı için 138 boyutlu özellik vektörü elde edilmiştir. Bu özellik vektörlerinin eşleşmesinde yine g2NN yaklaşımı kullanılmakta ve varsa hatalı eşleştirmelerin giderilmesi

RANSAC ile sağlanmaktadır. Sahte bölgelerin sınırlarının belirlenmesi için afine transformasyon sonucu örtüşen iki görüntünün korelasyon haritası çıkarılmaktadır. Bu çalışmada düz bölgelerle yapılan sahteciliklerin tespiti için herhangi bir iyileştirme yapılmamış olup, kullanılan MIC-F220, COVERAGE, CMH verisetleri bu tarz zorlu görüntüleri barındırmamaktadır.

2. YAPILAN ÇALIŞMALAR

Tez kapsamında sayısal görüntülerde kopyala-yapıştır sahteciliği tespitine ilişkin ataklara karşı dayanıklı sahtecilik tespiti yöntemleri üzerinde durulmuştur. Yöntemlerin hem sahte veya orijinal görüntünün doğru bir şekilde etiketlenmesindeki hem de sahte görüntüdeki sahte bölgelerin işaretlenmesindeki başarısının yüksek olması gerekmektedir. Yapılan çalışmalarda kopyalanan ve yapıştırılan bölgenin düşük kontrasta sahip olma durumu göz önünde bulundurularak, bu özelliğe sahip sahte görüntülerin de tespit edilebilmesi dikkate alınmıştır. Ayrıca sahtecilik tespit yöntemlerinin girdi görüntüsüne uygulanabilecek dönme, ölçekleme gibi ön işlem ataklarına ve JPEG sıkıştırma, gürültü ekleme gibi son işlem ataklarına karşı dayanıklılığı önem arz etmektedir. Bu durumlar göz önüne alınarak tez kapsamında anahtar noktası tabanlı iki özgün kopyala-yapıştır sahteciliği tespiti yöntemi önerilmiştir.

Bölüm 2.1'de, yapılan çalışmaların ilki olan L*a*b ve RGB renk uzaylarında faydalanarak anahtar noktası tabanlı şüpheli bölgelerin çıkarılması ve dinamik bir lokalizasyon yaklaşımı ile sahtecilik tespiti yönteminin [162] detayları verilmiştir. Yöntemde düz bölgelerle yapılan sahteciliklerin tespit edilebilmesi için girdi görüntüsünün L*a*b* renk uzaylarındaki temsilinden faydalanılır. Görüntünün L*a*b* renk uzayına dönüştürülmesi sonrası, L* kanalında ve a* ve b* renk kanalındaki temsillerinin normalize edilmesi sonrası elde edilen görüntülerin histogram eşitlemesi gerçekleştirilerek görüntüdeki ayrıntıların öne çıkarılması amaçlanmaktadır. Ardından üç görüntünün bütününden SIFT anahtar noktalarının çıkarılması ve eşleştirilmesi sonrası şüpheli bölge tespiti gerçekleştirilmiştir. Lokalizasyon aşamasında ise şüpheli bölgelerin alt bloklarından AKD sonrası elde edilen özellik vektörleri yardımı ile benzer blokların ortaya konması amaçlanmaktadır. Lokalizasyon aşamasının girdi görüntüsünden bağımsızlık kazanabilmesi için, benzer blokların eşleştirilmesinde kullanılacak parametrenin dinamik bir şekilde bulunması sağlanmıştır.

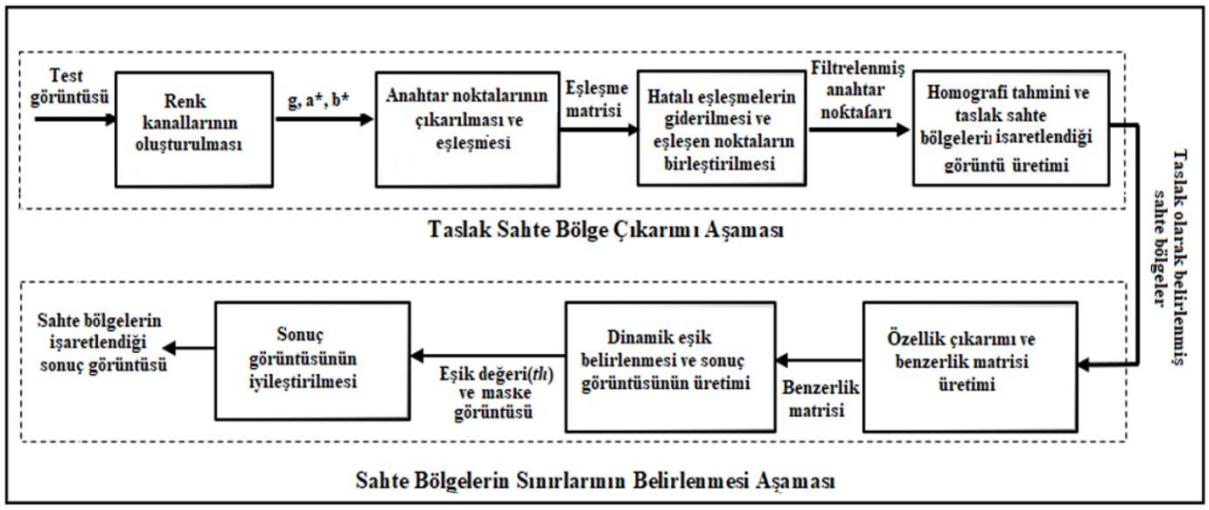
Bölüm 2.2'de ise ikinci yapılan çalışma olan LBPROT ve SIFT yöntemine dayalı şüpheli bölge çıkarımı ve Ciratefi tabanlı lokalizasyon yaklaşımı ile sahtecilik tespiti yöntemine [163] ilişkin detaylar vermiştir. Yöntemde öncelikle düz bölgelerle yapılan bir sahtecilikleri tespit edebilmek için görüntünün doku görüntüsü LBPROT ile elde edilmiştir. Doku görüntüsünden SIFT anahtar noktaları çıkarılmış ve bunların eşleştirilmesi sağlanmıştır. Yeterli sayıda eşleşmenin bulunması halinde görüntü sahte olarak belirmiş ve eşleşen anahtar noktalarının konumlarından faydalanarak sahte bölgelerin sınırlarının belirlenmesi için Ciratefi tabanlı yeni bir lokalizasyon yaklaşımı önerilmiştir.

2.1. L*a*b* Renk Uzayından Faydalanarak Anahtar Noktası Tabanlı Şüpheli Bölgelerin Çıkarılması ve Dinamik Bir Lokalizasyon Yaklaşımı ile Sahtecilik Tespiti

Tez kapsamında önerilen yöntemlerin ilkinde, literatürdeki yöntemlerin eksikliklerinin üstesinden gelmek amacı ile iki ana aşamadan oluşan özgün bir yöntem önerilmiştir Şekil 2.1'de bu aşamalar arası girdi ve çıktı verileri genel olarak verilmiştir. Taslak sahte bölge çıkarımı ve sahte bölge sınırlarının belirlenmesi aşamaları önerilen yöntemin temel iki aşamasıdır. Sisteme girdi olarak alınan renkli görüntünün ilk olarak Taslak sahte bölge çıkarımı aşamasına yönlendirilmesi ile önerilen yöntem icra edilmeye başlar. Bu aşamada öncelikle görüntünün RGB renk uzayından L*a*b* renk uzayına dönüştürülmesi sonrası görüntünün L*, a* ve b* renk kanallarının elde edilmesi gerçekleştirilir. Görüntünün farklı renk kanallarında değerlendirilmesi ile düşük kontrasta sahip bölgelerden de anahtar noktalarının elde edilebilmesi amaçlanmıştır. Yine bu adımda üç kanalda temsil edilen görüntüler, kontrast sınırlı adaptif histogram eşitleme yaklaşımı ile iyileştirilir. Daha sonra iyileştirilmiş görüntülerin her birinden, SIFT anahtar noktaları çıkarılarak, anahtar noktalara ait özellik tanımlayıcı vektörlerin yardımı ile kendi içlerinde eşleştirilmesi gerçekleştirilir. Üç görüntüden elde edilen eşleşme matrisleri olası hatalı eşleştirmelerden arındırıldıktan sonra birleştirilerek taslak sahte bölge çıkarımı aşamasının son adımı olan RANSAC ile homografi tahmini ve sahte bölgelerin yer aldığı taslak görüntü oluşturulur. Sahte bölgelerin sınırlarının belirlenmesi aşamasında ilk olarak, bu aşamaya yönlendirilen taslak sahte bölgelerden faydalanarak sahtecilik sınırlarının net bir şekilde belirlenmesi için bu bölgelerdeki alt blokların AKD tabanlı özellik vektörlerinden faydalanılır. Elde edilen özelliklerin eşleştirilmesi sırasında kullanılarak benzerlik eşiğinin dinamik bir şekilde belirlenmesi için öncelikle benzerlik matrisi oluşturulur ve dinamik belirleme ve sonuç

görüntüsünün üretimi aşamasına iletilir. Bu aşamada belirlenen eşik değerine uygun olarak eşleşen özellik vektörlerine sahip bloklar sahte blok olarak etiketlenir. Sonuç görüntüsünün iyileştirilmesi amacı ile temelde Bağlı Bileşen Etiketleme yaklaşımından faydalanan son işlem aşamasının icrası ile önerilen yöntem sahte bölgelerin işaretlendiği sonuç görüntüsünün üretimini tamamlamış olur.

Bu bölümün alt aşamalarında ilk olarak, yukarıda kısaca bahsedilen yöntemde kullanılan teorik kavramlar sunulacak, daha sonraki alt bölümde ise önerilen yöntemde yer alan aşamaların detaylı anlatımı yapılacaktır.



Şekil 2.1. Önerilen yöntemin blok diyagramı

2.1.1. Kullanılan Teorik Kavramlar

Bu bölümde ilk olarak girdi görüntüsüne ilişkin yeterli sayıda anahtar noktası elde edebilmek amacı ile faydalanılan L*a*b* renk uzayından, ardından görüntünün iyileştirmesi amacı ile kullanılan Kontrast Sınırlı Adaptif Histogram Eşitleme algoritmasından bahsedilmiştir. Daha sonra, anahtar noktalarının eşleştirilmesi sonrası varsa hatalı eşleşmelerin giderilmesi ve eşleşmeler arasındaki matematiksel modelin belirlenmesinde kullanılan RANSAC yaklaşımına yer verilecektir. Son olarak sahte bölgelerinin sınırlarının belirlenmesinde şüpheli bölgelerde yer alan alt blokların özelliklerinin elde edilmesinde faydalanılan AKD'den bahsedilecektir.

2.1.1.1. L*a*b* Renk Uzayı

Sayısal görüntülerin temsilinde kullanılan en önemli konulardan birisi de renk bilgisidir. Renkleri tanımlamak için kullanılan matematiksel modeller renk uzayı olarak adlandırılmaktadır. Renk uzayları bütün renkleri temsil edecek şekilde oluşturulmuştur. Renkmetri biliminin temeli olarak kabul edilen Grassmann'ın birinci kuralına göre bir rengin belirlenebilmesi için birbirinden bağımsız üç değişkene ihtiyaç duyulduğundan renk uzayları üç boyutlu olarak tasarlanmıştır. Bu üç değişken kullanılarak renklerin renk uzaylarındaki yerleri belirlenmektedir. Renk uzayları, farklı standartlara göre oluşturulur ve doğrusal/doğrusal olmayan yöntemlerle birbiri arasında dönüşümleri gerçekleştirilebilmektedir [160]. Günümüzde kullanılan 5 temel renk uzayı vardır. Farklı renk görüntüleme ve işleme cihazları farklı renk uzayları kullanır. Çoğu bilgisayar grafikleri sistemleri RGB renk uzayını kullanmaktadır. Grafik dosya sistemi RGB görüntülerini her bir değişkeni 8-bitlik olmak üzere, 24 bitlik görüntüler halinde saklar. RGB renk uzayının kullanımı bilgisayar grafikleri sistemlerinin tasarımını kolaylaştırmaktadır, ancak bazı uygulamalar için ideal olmayabilir.

L*a*b* renk uzayı CIELab olarak da literatürde yer almakta olup, renkler arasındaki fark edilebilir benzerlikleri olabildiğince ayırt edebilme ve rengin insan tarafından algılanışı üzerine kuruludur [161]. Bu uzayı da yine üç bileşenden oluşmaktadır; parlaklık (L*, lightness), tonlama (a*) ve doygunluk (b*). Bu bileşenlerden a* kırmızı/yeşil, b* sarı/mavi değerini gösterir. RGB renk uzayından L*a*b renk uzayına geçiş yapmak için doğrusal

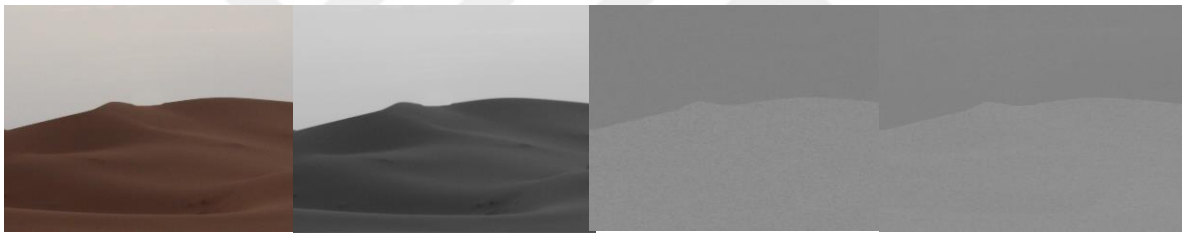
olmayan dönüşümler kullanılmaktadır. Bu dönüşümde ilk olarak RGB renk uzayından XYZ renk uzayına dönüşüm gerçekleştirilmektedir. Şekil 2.2'de örnek bir görüntünün L*a*b* renk uzayındaki her bir kanalı verilmiştir.

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.412453 & 0.357580 & 0.180423 \\ 0.212671 & 0.715160 & 0.072169 \\ 0.019334 & 0.119193 & 0.950227 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix},$$

$$f(t) = \begin{cases} \sqrt[3]{t} & \text{Eğer } t > \delta^3 \\ \frac{t}{3\delta^2} + \frac{4}{29} & \text{diğer durumlarda} \end{cases}, \quad L^\star = 116\, f\left(\frac{Y}{Y_n}\right) - 16,$$

$$a^\star = 500\left(f\left(\frac{X}{X_n}\right) - f\left(\frac{Y}{Y_n}\right)\right), \quad b^\star = 200\left(f\left(\frac{Y}{Y_n}\right) - f\left(\frac{Z}{Z_n}\right)\right) \tag{2.1}$$

Burada X_n, Y_n, Z_n değerleri CIE D65 standartlarına göre belirlenmiş olup, $X_n = 95.0489, Y_n = 100, Z_n = 108.8840$ şeklindedir [161].



(a) (b) (c) (d)

Şekil 2.2. Örnek görüntünün L*a*b* uzayındaki kanalları (a)Örnek sahte görüntü (b) L* kanalı (c) a* kanalı (d) b*kanalı

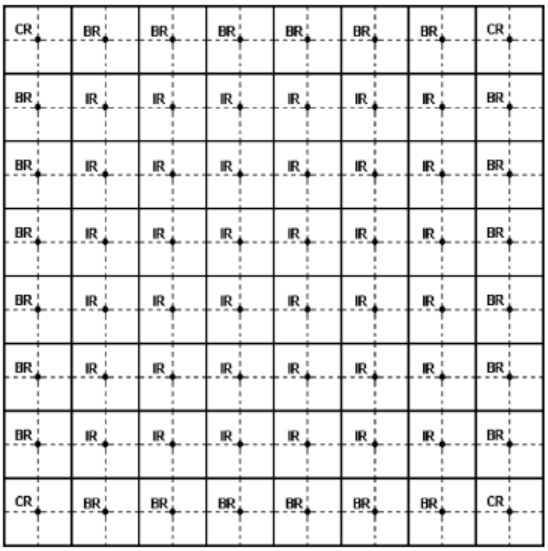
2.1.1.2. Kontrast Sınırlı Adaptif Histogram Eşitleme Algoritması

Sayısal görüntülerin iyileştirilmesinde kullanılan yöntemlerden biri olan histogram eşitleme ile tüm görüntünün yoğunluk dağılımı normalize edilerek düzgün bir yoğunluk dağılımına sahip görüntünün oluşturulması sağlanır. Klasik histogram eşitlemede tüm görüntünün yoğunluk bilgisi kullanılması durumu bazı görüntülerde ortalama yoğunluk orta seviyeye getirilmiş olduğundan solmuş bir ektiye sebep olabilir. Böyle bir durumda, tez çalışmasında amaçlanan, ayırt ediciliği yüksek anahtar noktaların elde edilmesi açısından negatif etki oluşturabilmektedir. Ayrıca görüntünün küçük bir bölgesinde kalabalık bir yoğunluğun varlığı durumu histogram eşitleme sonrası birçok gürültü pikselinin ortaya

çıkmasına neden olabilir. Bu problemlerin çözümü olarak yerel histogram eşitleme yöntemleri önerilmiştir [154].

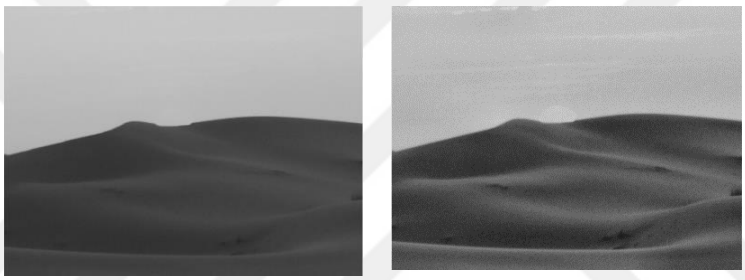
Adaptif histogram eşitleme yöntemi görüntüyü yerel bölgelere ayırarak histogram eşitleme işlemini gerçekleştirmektedir. Yöntemin temelinde görüntünün dikdörtgensel bölgelere bölünerek her bölgeye standart histogram eşitleme işleminin uygulanması yatar. Bölgelerin boyutları ve sayısı görüntüye göre değişebilmektedir. Alt bölgelere histogram eşitleme işlemi uygulandıktan sonra alt bölgelerin bi-lineer interpolasyon yöntemi ile birleştirilmesi gerçekleştirilir [155].

Adaptif histogram eşitlemenin dezavantajı olarak da gürültü probleminin ortaya çıkması literatürde yer almaktadır. Bu durumun engellenebilmesi için homojen bölgelerde kontrast iyileştirmenin sınırlandırılması çözüm olarak sunulmuştur [156]. Kontrast sınırlı adaptif histogram eşitleme yönteminde de yine görüntünün çoğunlukla eşit boyutlu eş örtüşmeyen bölgelere ayrılması ilk olarak gerçekleştirilir. Şekil 2.3'te 512x512 boyutlu bit görüntünün 64 eşit kare bölgelere ayrılmış halleri ve bölgelere atanan üç farklı etiketin olduğu görülmektedir. Şekildeki ilk bölgenin etiketi olan CR (corner regions) etiketinin, görüntüde toplamda dört köşede yer alan bölgelere atandığı görülmektedir. Şekilde 24 bölge için de BR (boarder regions) etiketinin atandığı görülmektedir. Görüntünün kenarlarında yer alan bölgeler için (köşeler hariç) bu etiket kullanılmaktadır. Diğer içte kalan 36 bölge için de IR (inner regions) etiketi kullanılmıştır [156].



Şekil 2.3. 512x512'lik bir görüntünün 64 eşit kare bölgeye ayrılmış hali ve etiketlenmesi [157]

Kontrast sınırlı adaptif histogram eşitleme yönteminde ilk olarak her alt bölgenin histogramı hesaplanmaktadır. Ardından istenen kontrast genişlik sınırına göre histogramların kırpılmasında kullanılarak kırpma sınır değeri elde edilmektedir. Hesaplanan histogramlar bu kırpma sınır değerini aşmayacak şekilde yeniden dağıtılmaktadır. Son olarak, gri tonlamalı haritalama için elde edilen kontrast sınırlı histogramların kümülatif dağılım fonksiyonları, CDF belirlenir. Kontrast sınırlı adaptif histogram eşitleme tekniğinde pikseller, en yakın dört bölgenin eşlemelerinden elde edilen sonuçların doğrusal olarak birleştirilmesiyle eşlenir. IR grubundaki bölgeler için bu yaklaşımın formülasyonu basittir. Ancak, CR ve BR gruplarındaki bölgeler için bu formülasyon bazı özel değerlendirmeleri gerektirir [157]. Şekil 2.4'te örnek bir gri seviyeli görüntünün kontrast sınırlı adaptif histogram eşitleme ile iyileştirilmiş hali verilmiştir.



(a) (b)

Şekil 2.4. Gri seviyeli bir görüntünün kontrast sınırlı adaptif histogram eşitleme sonrası durumu (a)gri seviyeli görüntü (b) kontrast sınırlı adaptif histogram eşitleme sonrası hali

2.1.1.3. RANSAC Algoritması

Fischler and Bolles tarafından 1981 yılında önerilen, bir dizi veriden elde edilebilecek matematiksel bir modelin parametrelerini tahmin etmek için önerilen yinelemeli (iteratif) bir yöntemdir [159]. Matematiksel modelinin çıkarıldığı veride, aykırı verilerin de bulunabileceği ve bunların elde edilecek matematiksel modeli etkilemeyeceği durumlarda kullanılmaktadır. Bu nedenle bir aykırı değer tespit yöntemi olarak da yorumlanabilir [160]. Yöntem ayrıca bir aykırı veri içermeyen bir veri kümesini en uygun şekilde açıklayan ve bunlara uygun bir modelin parametrelerini tahmin edebilmektedir. Veri kümesini girdi parametresi olarak alan ve bu veri kümesine uygun modeli ve modele uygun olmayan aykırı verileri çıkışa ileten RANSAC algoritmasının temel adımları aşağıdaki gibidir;

Adım 1: Minimum sayıda veriyi rastgele seç.

Adım 2: Seçilen verilere uygun model oluştur.

Adım 3: Tüm verilerden modele uygun olanları tespit et.

Adım 4: Modele uygun verilerin sayısını kontrol et. Eğer sayı yeterli ise devam et, sayı yeterli değil ise Adım 1'e git.

Adım 5: Modeli ve modele uygun olmayan verileri 'aykırı veri(outlier)' olarak çıkışa ilet.

Yöntemde bu beş adımın tamamlanması ile hem veri kümesine özel modelin çıkarılması hem de aykırı verilerin elenmesi sağlanabilmektedir.

2.1.1.4. Ayrık Kosinüs Dönüşümü

Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform, DCT, AKD), farklı frekanslarda salınan kosinüs fonksiyonlarının toplamı cinsinden sonlu bir veri noktaları dizisini ifade eder. İlk olarak 1974'te Nasir Ahmed tarafından önerilen bu yöntem, sinyal işleme ve veri sıkıştırmada yaygın olarak kullanılan bir dönüştürme tekniğidir [158].

Bir sinyalin frekans uzayında gösterimi, sinyalin içerdiği değişimleri ifade etmektedir. Sayısal görüntü işlemede görüntünün ayırt edici içeriklerin anlamlı hale gelmesinden dolayı AKD görüntü işleme uygulamalarında sıkça başvurulan yöntemlerden biridir. AKD'nin, sayısal görüntü, video ve ses dahil olmak üzere çoğu sayısal ortamda kullanılmasının yanında, telekomünikasyon cihazları, ağ bant genişliği kullanımını azaltma ve kısmi diferansiyel denklemlerin sayısal çözümü için spektral yöntemler gibi bilim ve mühendislikteki diğer birçok uygulama için de önemlidir.

AKD sayısal bir sinyale kosinüs fonksiyonu uygulayarak sinyalin frekans uzayına dönüştürülmesini sağlar. Bu dönüşümün yalnızca kosinüs fonksiyonlarını kullanması sebebi ile yalnız gerçek aritmetik hesaplama yapılmaktadır. MxN boyutundaki giriş resmi I için AKD katsayılarının hesabı Eşitlik 2.2'de verilmiştir.

$$C(u,v) = \alpha_u \alpha_v \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m,n) \cos\frac{\pi(2m+1)u}{2M} \cos\frac{\pi(2n+1)v}{2N}, 0 \le v \le N-1$$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, u = 0 \\ \sqrt{\frac{2}{M}}, 0 < u \le M-1 \end{cases}, \qquad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, v = 0 \\ \sqrt{\frac{2}{N}}, 0 < v \le N-1 \end{cases} \tag{2.2}$$

MxN boyutunda bir görüntüye bu dönüşüm uygulanması sonucu yine MxN boyutunda AKD katsayıları elde edilmektedir. Elde edilen AKD katsayıları alçak frekans bileşenleri,

orta bant bileşenleri ve yüksek frekans bileşenleri olarak sınıflandırılmaktadır. Alçak frekans bileşenlerinden yüksek frekans bileşenlerine doğru katsayıların içerdiği bilgi içeriği azalmaktadır. Alçak frekans bileşenlerinin çeşitli saldırılara karşı duyarlılığı, yüksek frekans bileşenlerine göre daha azdır. Şekil 2.5'te $8x8$ boyutlu bir bloğun AKD bileşenleri verilmiştir.

Şekil 2.5. AKD katsayılarının gruplanması

2.1.1.5. Bağlı Bileşen Etiketle Algoritması

Bağlı bileşen etiketleme (BBE), sayısal bir görüntünün tamamının tarayarak görüntüdeki piksellerini, piksel bağlantılarına göre gruplayan bağlı bileşenlerin alt kümelerinin belirli bir sezgisel yönteme dayalı olarak benzersiz bir şekilde etiketlendiği grafik teorisinin algoritmik bir uygulamasıdır. Yöntem çoğunlukla ikili görüntüler üzerinde uygulanmaktadır. Yöntemin tamamlanması sonrasında birbiri ile komşu olan yani bağlantısı olan piksellerin aynı grupta yer alması sağlanır. Her bir grubun numaralandırılarak etiketlendirilmesi gerçekleştirilir. Yöntem bağlantılı komşuların kontrolü açısından 4-komşuluk ve 8-komşuluk olarak ikiye ayrılmaktadır. 8-komşuluk yönteminde piksellerin çapraz konumundaki pikseller de komşu piksel olarak değerlendirilmektedir. Etiketleme algoritmasının temel adımları aşağıdaki gibidir:

Adım 1: İkili görüntüdeki piksellerin baştan sona kadar taranması.

Adım 2: İkili görüntüde o anki piksel değeri 1 ise komşuları kontrol et.

a. Eğer komşular etiketli değil ise piksele yeni etiket ata.

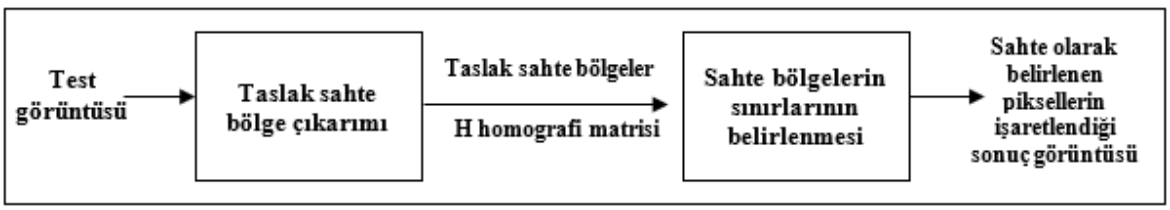
b. Eğer komşularından sadece biri önceden etiketlenmiş veya tüm komşularının etiketi aynı ise o anki piksele komşusunun etiketini ata.

c. Eğer iki komşu piksel farklı etikete sahip ise ilgili piksele üst komşusunun etiketini ata. Sol komşusu ile aynı etiket değerine sahip piksellerin hepsi ile kendi etiketini değiştir.

Adım 3: Görüntüde yer alan piksellerin hepsi taranmadı ise 2. Adıma git. Tamamlama bitti ise işlemi bitir.

2.1.2. Önerilen Yöntem

Yapılan çalışmada blok tabanlı ve anahtar noktası tabanlı yöntemlerin avantajlarını göz önünde bulundurarak daha yüksek performansa sahip bir yöntem önerilmiştir. Bu doğrultuda önerilen yöntem Şekil 2.6'da da gösterildiği gibi temelde iki ana aşamadan oluşmaktadır; taslak sahte bölge çıkarımı ve sahte bölgelerin sınırlarının belirlenmesi. Yöntemde, sisteme girdi olarak alınan test görüntüsünün, öncelikle taslak sahte bölge çıkarımı aşamasına yönlendirilmesi sağlanmıştır. Bu aşamanın tamamlanması ile elde edilen taslak sahte bölgelerin ve bölgeler arası geometrik ilişkiden elde edilen homografi matrisi H'nin ikinci ana aşamaya iletilmesi gerçekleştirilmektedir. Sahte bölgelerin sınırlarının belirlenmesi aşamasında ise benzer özellik vektörlerini ortaya koymak için dinamik bir eşik değeri belirlenir ve belirlenen eşiğe göre sahte bölgelerin işaretlemesi gerçekleştirilir. Daha sonra elde edilen binary görüntü üzerinde morfolojik işlemler uygulanarak piksel bazlı işaretlemenin daha yüksek doğrulukla yapılması sağlanmaktadır. Bu adımın icrası ile sahte olarak belirlenen piksellerin işaretlendiği sonuç görüntüsü elde edilerek yöntem tamamlanmaktadır. İki temel adımda gerçekleştirilen işlem adımlarının detayları iki alt başlık halinde sunulacaktır.

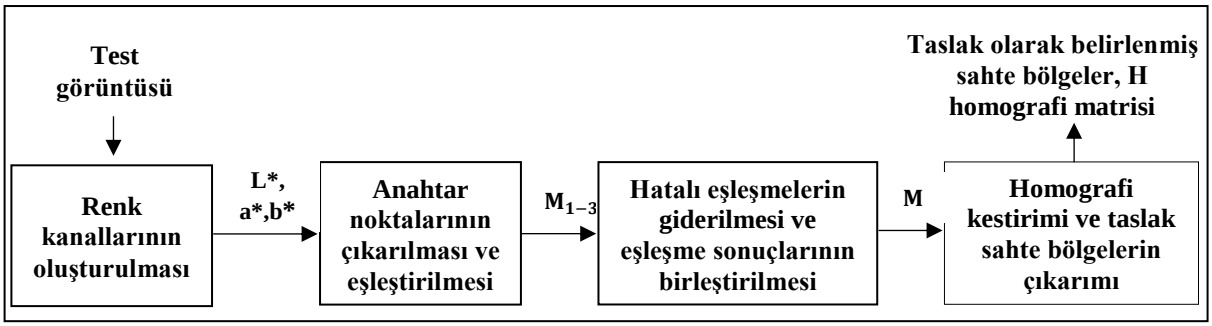


Şekil 2.6. Önerilen yöntemin alt adımları

2.1.2.1. Taslak Sahte Bölge Çıkarımı Aşaması

Taslak sahte bölgelerin çıkarılması aşamasında, görüntüden elde edilen anahtar noktalarından faydalanarak görüntünün sahte veya orijinal olma durumunun ortaya konması ve sahte görüntü olması durumunda da taslak sahte bölgelerin oluşturulması işlemi gerçekleştirilmektedir.

Önerilen yöntemin bu aşamasında, taslak olarak belirlenen sahte bölgeleri gösteren görüntüyü oluşturmak için dört adım kullanılır. Şekil 2.7'de önerilen adımları içeren blok diyagram yer almaktadır. İlk adımda görüntünün L*a*b* renk uzayında yer alan her bir kanaldaki temsili elde edilir. Bu adımda ayrıca bu renk kanalları üzerinde histogram eşitleme işlemi gerçekleştirilerek görüntülerin ayırt edici özelliğinin artırılması hedeflenmiştir. İkinci adımda ise ilk adımdan gelen üç görüntüden (L*, a*, b*) SIFT anahtar noktalarının çıkarılması ve bunların kendi içlerinde en benzerlerinin eşleştirilmesi gerçekleştirilmektedir. Her bir görüntüden elde edilen eşleşmeler M_1, M_2, M_3 isimli matrislerde depolanarak bir sonraki aşamaya iletilir. Üçüncü adım da eşleşme matrislerinde yer alan olası hatalı eşleştirmelerin elenmesi işlemi gerçekleştirilir ve eleme işleminden sonra $M = [M_1 \cup M_2 \cup M_3]$ olacak şekilde birleştirilerek dördüncü aşamaya aktarılır. Dördüncü ve son aşamada, homografi kestirimi ve eşleşmelerin etrafında belirlenecek taslak sahte bölgelerin çıkarılması ile yöntemin bu bölümü tamamlanmaktadır. Taslak olarak belirlenen sahte bölgelerin yer aldığı görüntü ve H homografi matrisi bu bölümün çıktısı olmaktadır. İşlem adımlarının detayları aşağıda sunulmuştur.

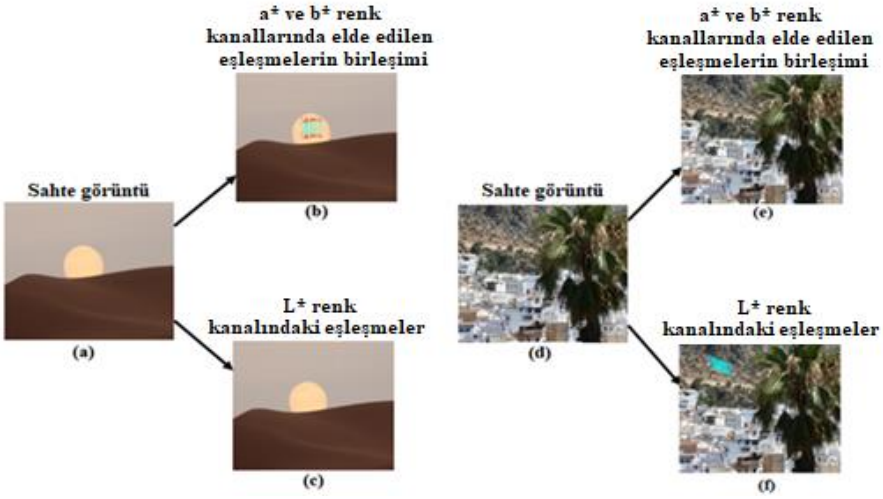


Şekil 2.7. Taslak Sahte Bölge Çıkarımı Aşamasının blok diyagramı

Literatürdeki birçok anahtar noktası tabanlı yöntem, önemli noktaları çıkarmak için test görüntüsünün gri seviye kanalını kullanır. Sahte görüntünün düşük kontrasta sahip bir bölgenin kopyalanıp yapıştırılması ile oluşturulması durumunda RGB renk uzayında anahtar

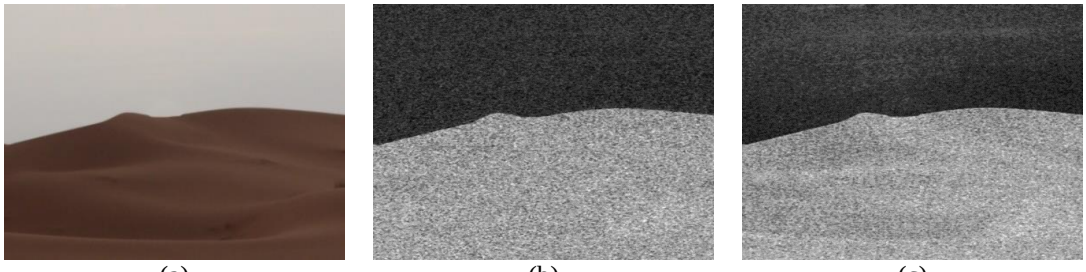
noktası çıkarmaya dayalı yöntemler bu bölgelerden yeterli sayıda anahtar noktası elde edemez ve dolayısıyla sahteciliklerin tespiti mümkün olmaz. Bazı çalışmalar, bu sınıfta yer alan yöntemlerde anahtar noktası çıkarma aşamasında kullanılan kontrast eşiğinin azaltılması durumunda daha fazla ana nokta elde edilebileceğini rapor etmişlerdir [28, 36]. Ancak, çıkarılan anahtar noktaların sayısı, yaklaşık 10 kat artmasına rağmen, doğru eşleşme sayısının yüzde yirmi azaldığını da belirtmişlerdir.

Yapılan tez çalışmasında renk uzaylarının sahte görüntüler üzerindeki etkisi üzerine yaptığımız araştırmalarda bazı ipuçları ile karşılaşılmıştır. Yapılan araştırmalarımız neticesinde düşük kontrasta sahip görüntülerde anahtar noktası çıkarma aşamasından önce Bölüm 2.1.1.1.'de sunulan L*a*b* renk uzayı kullanıldığında, gri seviyeye kıyasla [0 255] değerlerine normalize edilmiş a* ve b* renk kanallarında daha iyi performans verdiği tespit edilmiştir. Bununla birlikte L* kanalının [0 100] değerleri arasında kullanımı durumunda JPEG sıkıştırma ve gürültü ekleme atakları uygulanmış olsa bile daha etkili anahtar noktası elde edilebildiği görülmüştür. Bu konuda yapılan çalışmaya ilişkin örnek bir görsel Şekil 2.8'de sunulmuştur. Şekil 2.8(a)'da dokusuz bir bölge ile yapılan sahte bir görüntü yer alırken, (b)'de dokulu bölge ile yapılmış bir sahtecilik yer almaktadır. Ancak (b) görüntüsünde yer alan sahte görüntü JPEG sıkıştırma atağına maruz kalmıştır. Sahtecilik tespiti zor olan bu iki durumda renk uzaylarının etkileri araştırılmıştır. Bunun için test görüntülerinin hem L* kanalı hem de a* ve b* kanalında anahtar nokta çıkarma ve eşleşme aşamaları uygulanarak sonuçları değerlendirilmiştir. (b) ve (e) görüntülerinde görüntünün L*a*b* renk uzayına dönüştürülmesi sonrası a* kanalından elde edilen SIFT anahtar noktaları yer almaktadır. (c) ve (d)'de ise görüntülerin L* kanalından elde edilen SIFT anahtar nokta eşleşme sonucu sunulmuştur. Şekilde de görüldüğü gibi a veya b* renk kanalları düz bölgelerle yapılan sahteciliklerin tespit edilmesinde avantaj sağlarken, L* kanalı da son işlem ataklarına karşı avantaj sağlamıştır.



Şekil 2.8. Farklı renk kanallarında anahtar noktası eşleşme sonucu örneği. (a) Düz bölgelerin kopyalanıp yapıştırılması ile oluşturulan sahte görüntü (b)a* ve b* kanallarındaki eşleşmelerin birleşiminin sonucu (c) L* renk kanalındaki eşleşme sonucu (d) JPEG sıkıştırma atağı uygulanmış sahte görüntü (e)a* ve b* kanallarındaki eşleşmelerin birleşiminin sonucu (f) L* renk kanalındaki eşleşme sonucu

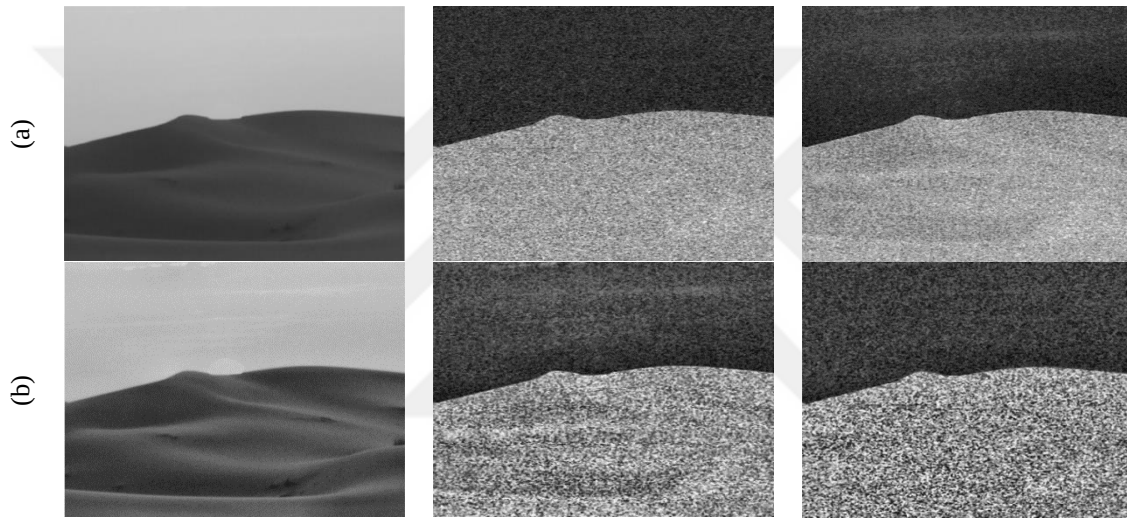
Önerilen sistemde, test görüntüsü olarak alınan görüntüye uygulanan atak durumundan veya kopyalanıp yapıştırılan bölge hakkında bir bilginin varlığı söz konusu değildir. Sistemin girdi görüntüsünden bağımsız, görüntüde var olabilecek bu iki zorluğa karşı da dayanıklı olması amaçlanmıştır. Bu doğrultuda görüntünün L*a*b* renk uzayındaki üç renk kanalı kullanılmıştır. Görüntünün L*a*b* renk uzayında a* ve b* renk kanallarının [0 255] değerlerine normalizasyonu gerçekleştirilerek görüntüye ait detayların ortaya çıkarılması sağlanmıştır. Şekil 2.9'da düz bölgelerin oldukça yoğun olduğu sahte bir görüntünün normalize edilmiş a* ve b* kanallarındaki temsilleri yer almaktadır.



(a) (b) (c)

Şekil 2.9. Elde edilen renk kanalları (a) örnek sahte görüntü (b) Normalize edilmiş a* renk kanalı (c) Normalize edilmiş b* renk kanalı

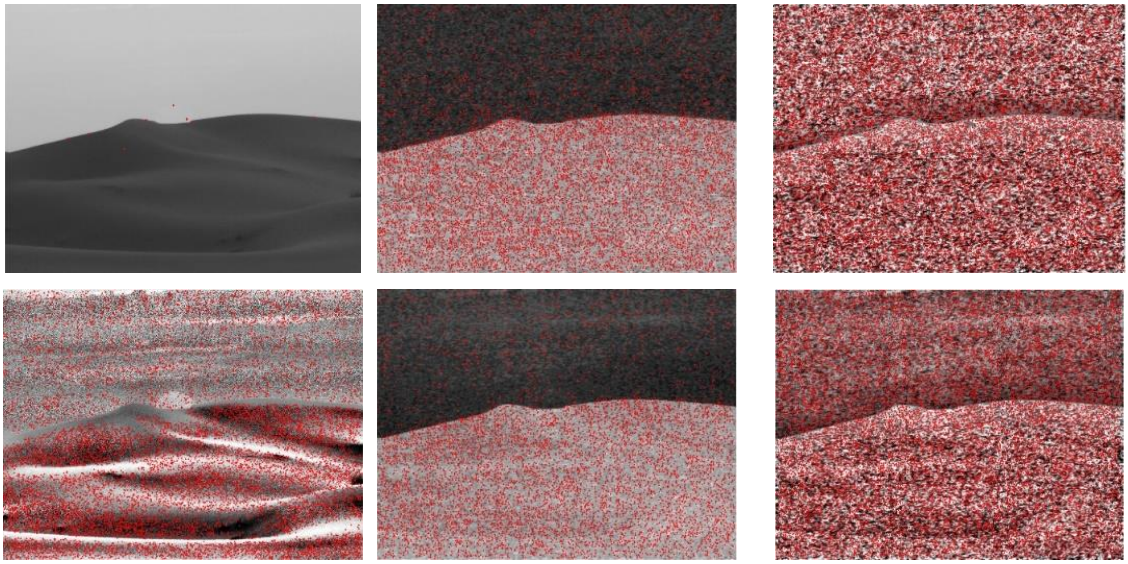
Önerilen yöntemde elde edilen renk kanaları üzerinde anahtar noktası elde etme ve eşleştirme performansını artırmak amacı ile Bölüm 2.1.1.2'de sunulan Kontrast Sınırlı Adaptif Histogram Eşitleme Algoritması kullanılmıştır. Önerilen yöntemde üç renk kanalından (L*, a*, b*) elde edilen görüntülerin iyileştirilmesi için uygulanan histogram eşitleme algoritmasında kesme limiti (clip limit) olarak adlandırılan parametre değeri γ deneysel çalışmalar ışığında, L* kanalı için γ=0.05, a* ve b* kanalları için γ=0.06 olarak belirlenmiştir. Şekil 2.10'da Şekil 2.9(a)'da verilen örnek sahte görüntüden elde edilen renk kanallarının histogram eşitleme öncesi ve sonrası halleri verilmiştir.



Şekil 2.10. Renk kanallarının kontrast sınırlı adaptif histogram eşitleme öncesi ve sonrası durumları (a)Histogram eşitleme öncesi (b)Histogram eşitleme sonrası

- **Anahtar Noktalarının Çıkarılması ve Eşleştirilmesi**

Bu aşamada ilk olarak yöntem, yukarıdaki aşamada elde edilen renk kanalları üzerinde Bölüm 1.4.2.2.1'de sunulan SIFT anahtar noktalarını çıkarmaktadır [142]. Şekil 2.11'de, Şekil 2.10'da yer alan görüntülerin histogram eşitleme öncesi ve sonrası hallerinden elde SIFT anahtar noktaları gösterilmiştir. Şekilde de görüldüğü gibi histogram eşitleme uygulanan görüntüde düşük kontrasta sahip bölgelerden de anahtar noktası elde edilebilmiştir.



Şekil 2.11. Histogram eşitleme öncesi ve sonrası görüntünün renk kanallarındaki temsillerinde elde edilen anahtar noktaları

Test görüntüsünün üç kanalının her birinden SIFT anahtar noktalarının elde edilmesinden sonra, her bir kanaldan elde edilen anahtar noktalarının kendi arasında eşleşmesi gerçekleştirilmektedir. Elde edilen anahtar noktaları genelleştirilmiş 2NN (g2NN) eşleşme yöntemi ile eşleştirilmiştir [108]. Yöntem öncelikle her bir özellik tanımlayıcı vektörün diğer vektörler ile Öklid uzaklık mesafesini hesaplar ve bunların sıralanması ile $D = \{d_1, d_2, \dots d_{n-1}\}$ elde edilir. Yöntem Eşitlik (2.3)'de verilen testin iteratif bir şekilde yapılması sonucu eşleşen anahtar noktaları belirlenir. (Yapılan deneyler sonucu $T = 0.6$ olarak ayarlanmıştır.)

$$d_1/d_2 < T \tag{2.3}$$

İterasyon son anahtar noktasının arama işlemi tamamlanıncaya kadar devam eder. Her bir görüntü kanalının kendi içinde eşleşmesi tamamlandıktan sonra, eşleşen anahtar noktaları M_i, M eşleşme matrisinde depolanır. Böylece bu aşamadan sonra üç adet matris elde edilmiş olur. (M_1, M_2, M_3).

- **Hatalı Eşleşmelerin Giderilmesi ve Eşleşme Sonuçlarının Birleştirilmesi**

Bir önceki adımda elde edilen (M_1, M_2, M_3) matrisleri için hatalı eşleşmelerin giderilmesi gerçekleştirilir. M_i matrisinde eşleşen ilk iki anahtar noktaları (x_1, y_1) ve

(x_2, y_2) olsun. Yöntemde iki noktanın Öklid mesafesi hesaplanmaktadır ve önceden belirlenmiş bir eşiğe göre $\|(x_1, y_1) - (x_2, y_2)\| < m$ olma durumu kontrol edilmektedir. Böylece birbirine çok yakın eşleşmelerin elimine edilmesi işlemi gerçekleştirilmiş olunur. Daha sonra her bir eşleşme kullanarak shift vektör değerleri hesaplanır $(s_1, s_2) = (|(x_1 - x_2)|, |(y_1 - y_2)|)$. Shift vektörlere ait sayılar $C(s_1, s_2)$ değişkeni ile tutulur. Dönme ataklarının olabileceği göz önünde tutularak $[s_1 - t_s, s_1 + t_s]$ ve $[s_2 - t_s, s_2 + t_s]$ aralıkların değişimi kabul edilir. $C(s_1, s_2) > n$ olması durumu sağlayan eşleşmeler doğru eşleşme olarak kabul edilir, şartı sağlamayan eşleşmelerin elenmesi işlemi gerçekleştirilir.

Hatalı eşleşmelerin giderilmesinin ardından üç kanaldan elde edilen eşleşme matrislerinin birleştirilmesi gerçekleştirilir, $M = [M_1 \cup M_2 \cup M_3]$. Yöntemde bir görüntüde en az 5 adet eşleşen anahtar noktasının bulunması durumunda görüntü "sahte" olarak etiketlenmesi gerçekleştirilir. Bundan sonraki aşamalarda sahte görüntüde piksel bazlı işaretleme için önerilen adımlar verilmiştir.

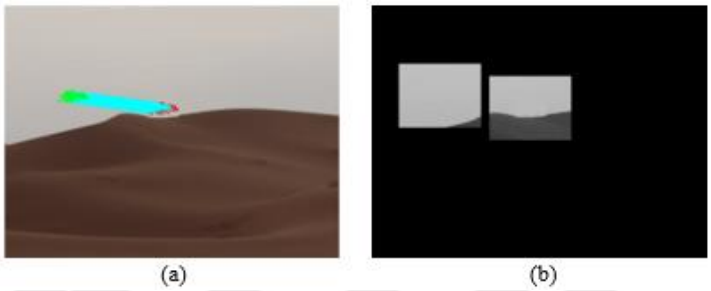
- **Homografi Kestirimi ve Taslak Sahte Bölgelerin Çıkarılması**

Bu aşamada eşleşen anahtar noktalarına ait konum bilgilerinin yer aldığı M eşleşme matrisi kullanılarak Bölüm 2.1.1.3'te sunulan RANSAC algoritması ile eşleşen anahtar noktaları arasında transformasyon matrisi (H) kestirimi yapılmaktadır. Transformasyon matrisi eşleşen anahtar noktaları arasındaki geometrik ilişkiyi barındırmaktadır. Buradaki amaç kopyalanan bölgenin, elde edilen matris ile transform edilmesi sonucu bölgelerin örtüşmesini sağlamaktır. Bir sonraki bölümde sunulacak olan Sahte bölgelerin sınırlarının belirlenmesi aşamasında kullanılmak üzere elde edilen H matrisinin bu aşamaya iletilmesi gerçekleştirilmiştir.

Yöntemin bu aşamasında ayrıca bir önceki adımda elde edilen eşleşme matrisi M yardımı ile şüpheli kaynak ve hedef bölgeler taslak olarak belirlenecektir. Bu belirleme için eşleşme matrisinde yer alan hedef ve kaynak anahtar noktalarının konumları etrafında bir sınır çizilecektir. $\text{Source}_{\text{region}}$ ve $\text{Dest}_{\text{region}}$ olarak isimlendirilen bu bölgeler Eşitlik (2.4)'deki gibi elde edilecektir.

$$\begin{aligned} \text{Source}_{\text{region}} &= I\left(\left(\min_{x_s} - r\right) : \left(\max_{x_s} + r\right), \left(\min_{y_s} - r\right) : \left(\max_{y_s} + r\right)\right) \\ \text{Dest}_{\text{region}} &= I\left(\left(\min_{x_d} - r\right) : \left(\max_{x_d} + r\right), \left(\min_{y_d} - r\right) : \left(\max_{y_d} + r\right)\right) \end{aligned} \tag{2.4}$$

Burada $\min_{x_s}, \max_{x_s}, \min_{y_s}$ ve $\max_{y_s}$ ifadeleri kaynak bölgede yer alan anahtar noktalarına ait minimum ve maksimum noktaları temsil ederken $\min_{x_d}, \max_{x_d}, \min_{y_d}, \max_{y_d}$ ifadeleri de benzer şekilde hedef bölgede yer alan anahtar noktalarını temsil etmektedir. Bu piksel konumlarının r parametresi ile genişletilmiş bölgesi arasında yer alan bölge şüpheli bölge olarak değerlendirilir. Yalnızca şüpheli bölgelere ait piksel değerlerinin yer aldığı görüntü "Taslak görüntü (R)" olarak isimlendirilmiştir. Şekil 2.12'de eşleşen anahtar noktaları etrafındaki bölgeleri gösteren Taslak görüntü verilmiştir.

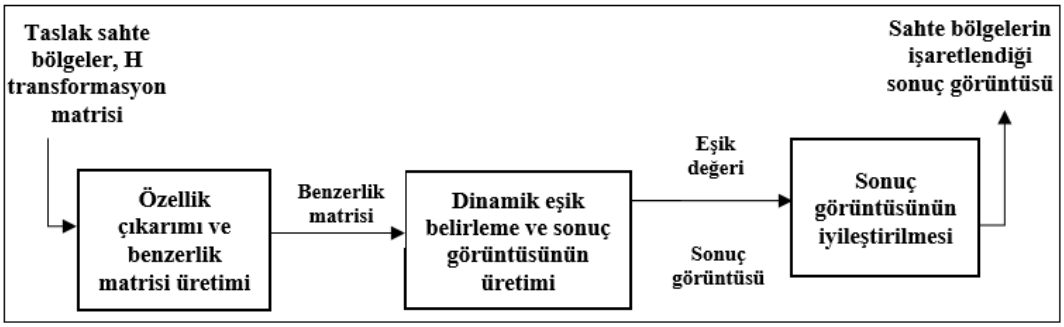


Şekil 2.12. (a) Eşleşen anahtar noktalarının birleşimi (b) Taslak sahte bölgeleri içeren taslak görüntü, (R)

2.1.2.2. Sahte Bölgelerin Sınırlarının Belirlenmesi Aşaması

Önerilen yöntemin bu adımında, önceki aşamadan bu aşamaya aktarılan taslak sahte bölgelerde yer alan sahte bölgelerin sınırlarının netleştirilmesi hedeflenmiştir. Şekil 2.13'te bu adımların, girdi ve çıktı verileri ile yer aldığı blok diyagram verilmiştir. Sahte bölgelerin sınırlarının belirlenmesinde bu bölgelerin alt bloklar halinde değerlendirilmesi ve birbirine en benzer bloklarının belirlenmesi bu aşamanın motivasyonu olmuştur. Girdi görüntüsüne uygulanabilecek geometrik dönüşüm ataklarının varlığı söz konusu olabileceğinden bu aşamaya aktarılan H transformasyon matrisinden faydalanarak R görüntüsünün transform edilmesi gerçekleştirilecektir. Transformasyon sonrası taslak hedef ve taslak kaynak bölgede yer alan alt blokların karşılıklı olarak değerlendirilmesi gerçekleştirilecektir. Bu değerlendirmede kullanılacak benzerlik parametresinin dinamik olarak belirlenmesi bu aşamanın önemli bir detayını oluşturmaktadır. Eşik değerine göre alt bloklardan elde edilen özellik vektörleri karşılaştırılıp benzerlik şartını sağlayan blokların sahte olarak etiketlenmesi ile sonuç görüntüsü üretimi gerçekleştirilecektir. Olası hatalı eşleştirmelerin

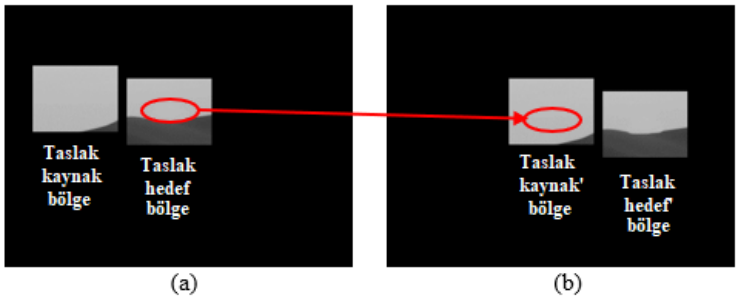
giderilmesi için son adım olan sonuç görüntüsünün iyileştirilmesi adımı icra edilerek önerilen yöntemin son çıktısı olan sahte bölgelerin işaretlendiği sonuç görüntüsü üretimi tamamlanmış olacaktır. Alt bölümlerde bu aşamaya ait detaylara yer verilecektir.



Şekil 2.13. Sahte Bölgelerin Sınırlarının Belirlenmesi Aşamasının blok diyagramı

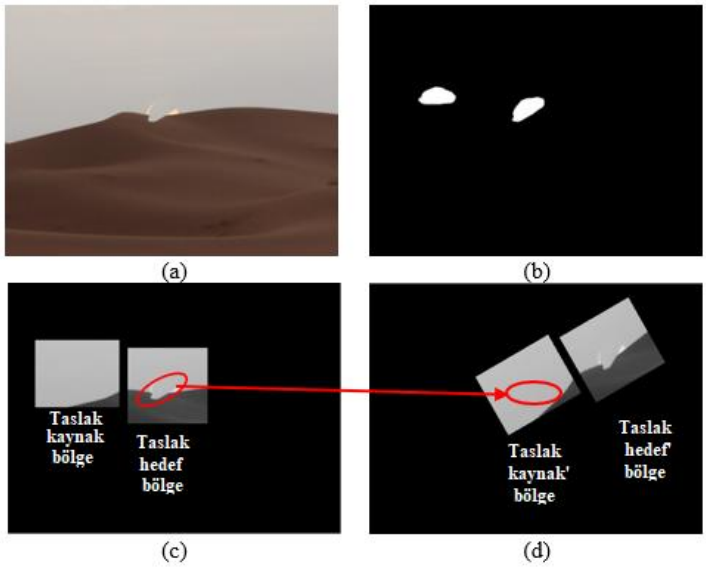
- **Özellik çıkarımı ve benzerlik matrisi üretimi**

Sahte bölgelerin sınırlarının belirlenmesinde ilk olarak bu aşamaya gelen taslak sahte bölgelerin alt bloklarına ait özellik vektörlerinin elde edilmesi amaçlanmıştır. Girdi görüntüsünde geometrik dönüşüm atakları olabileceği durumu söz konusu olabilmektedir. Bu durum göz önüne alınarak, öncelikle taslak sahte bölgelerin geometrik dönüşümden bağımsızlığının sağlanması için R görüntüsünün H matrisi ile transformasyonu gerçekleştirilmektedir. Transformasyon sonucu elde edilen görüntü yöntemde R′ olarak adlandırılmıştır. Böylece R görüntüsünde yer alan taslak kaynak bölgesinin, R′ görüntüsünde yer alan taslak hedef bölgesi ile nerede ise örtüşmesi gerçekleştirilmiştir. Şekil 2.15'te, R görüntüsünün H matrisi ile transformasyonu sonucu olan R′ görüntüsü yer almaktadır. R görüntüsünde birinci bölgede kırmızı ok ile gösterilen konumda yer alan sahte bölgenin, R′ görüntüsünde ikinci bölgede yer aldığı görülmektedir.



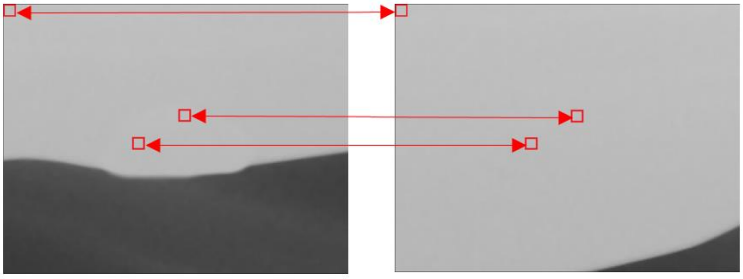
Şekil 2.14. (a) Taslak görüntü, R (b) Taslak görüntünün transform edilmiş hali, R' görüntüsü

Sahte görüntüde dönme atağı veya ölçekleme atağı olması durumunda da yine sahte bölgelerin örtüşmesi aynı işlem adımı ile sağlanmıştır. Şekil 2.15'te dönme atağı uygulanarak elde edilmiş sahte görüntüye ait bir örnek yer almaktadır.



Şekil 2.15. Örnek bir dönme atağı ile yapılmış sahte görüntünün transformasyon sonucu (a) Sahte görüntü (b) Sahtecilik maskesi (c) Taslak görüntü R (d) taslak görüntünün transformasyon sonucu R'

Görüntünün transformasyonu sonrasında R görüntüsünde birinci bölge (taslak kaynak), R′ görüntüsünde ikinci bölge (taslak hedef) $15x15$'lik örtüşen alt bloklara ayrılmaktadır. Şekil 2.16'da Şekil 2.14'te yer alan taslak sahte bölgelerdeki birbirine karşılık gelen bloklar görülmektedir. Bu bölgelerde yer alan karşılıklı blokların benzerliğinin kontrolünün yapılması için bloklardan AKD sonrası özellik vektörlerinin çıkarılması gerçekleştirilecektir. Geometrik dönüşüm ataklarından bağımsız hale getirilen taslak sahte bölgelerin JPEG sıkıştırma ataklarına karşı dayanıklı hale gelmesi için yöntemde AKD tabanlı özelliklerden faydalanılmıştır.



Şekil 2.16. Birbirine karşılık gelen alt blok örnekleri

Özellik vektörlerinin elde edilmesi için öncelikle blokların AKD ile frekans domenine transform edilmesi gerçekleştirilir. AKD bileşenlerinin zigzag taramasının ardından elde edilen ilk 16 bileşen özellik vektörlerini temsil etmek için kullanılır. Özellik vektörlerinde yer alan değerlerin en yakın tamsayıya yuvalanması durumu o anki bloğun karakteristiğine göre karar verilmektedir. R görüntüsünde, o anki blok B ile gösterilirse, bloğa ait özellik vektörü $F_R^{x,y}$ Eşitlik (2.5)'teki gibi elde edilir.

$$F_R^{x,y} = \begin{cases} \text{zigzag (DCT(B))} & \text{if } B_{max} - B_{min} \leq \partial \\ \text{zigzag (DCT(B))} & \text{if } B_{max} - B_{min} > \partial \end{cases} \quad (2.5)$$

Burada B_{max} ve B_{min} bloğa ait maksimum ve minimum yoğunluk değerleridir. Dolayısıyla düşük kontrast karakteristiğine sahip olan bir bloğa ait özellik vektörleri elde edilirken AKD bileşenleri yuvarlanmaz. Bunun sebebi düşük kontrasta sahip bir bloktan ayırt edici özelliklerin az olması sebebi ile frekans bileşenlerinde ekstra bir bilgi kaybına sebep olmamaktır. R'görüntüsünde yer alan B' alt bloklarından da benzer şekilde özellik vektörleri elde edilir.

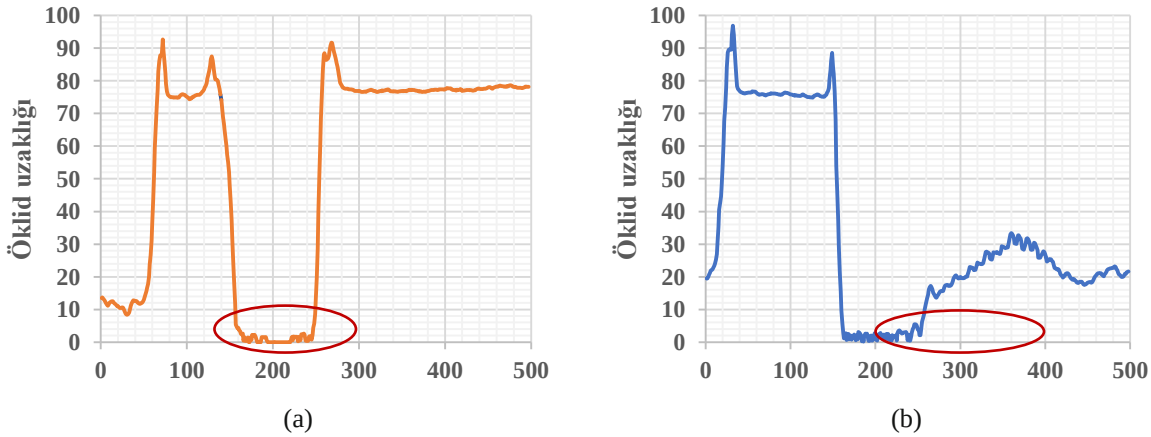
Karşılık gelen blokların sahte veya orijinal olma durumlarının özellik vektörlerine göre belirlenmesinde kullanılacak eşik değerinin belirlenmesi için S benzerlik matrisi oluşturulmaktadır. R görüntüsünde ele alınan bölgede, sol üst köşe noktası (x, y) noktasında yer alan bir bloğun benzerlik matrisindeki değeri R' görüntüsünde ele alınan bölgedeki $(x + w, y + w)$, $w \in \{-1,1\}$ ile başlayan karşılık düşen blok ve bunların 4 örtüşen komşusu ile arasındaki Öklid uzaklığı durumuna göre belirlenir. Buradaki amaç H matrisi ile elde edilen R' görüntüsünde olası kayma durumlarının da göz önüne alınmasıdır. İlgili blok ile karşılık düşen dört blok arasındaki Öklid uzaklıklarının en küçük değeri benzerlik matrisinde depolanmaktadır. $S^{x,y}$ benzerlik matrisinin elde edilişi Eşitlik (2.6)'da formüle edilmiştir.

$$S^{x,y} = \left(\min_{w \in \{-1,1\}} \left\| \left(F_R^{x,y}, F_{R'}^{x+w,y+w} \right) \right\| \right) \quad (2.6)$$

- **Dinamik Eşik Değerinin Belirlenmesi ve Sonuç Görüntüsünün Üretimi**

Bu aşamada benzerlik matrisi S kullanılarak, görüntüye özgü dinamik bir eşik değeri belirlenir ve bu eşik değerine göre eşleşme işlemi gerçekleştirilir. Bu doğrultuda eşleşen anahtar noktalarından rastgele seçilerek bu anahtar noktasının yer aldığı görüntü satırında yer alan bloklar değerlendirilir. Bu satır boyunca yer alan alt bloklara ait benzerlik matrisinde minimum değerler sürekliliğini sağlayan bloklar sahte blok olarak değerlendirilir. Yöntemde, bu sürekliliğin sağlandığı uzaklık değerlerinin ortalaması alınarak eğik değeri belirlenmiş olur.

Şekil 2.17'de benzerlik matrisinde yer alan bir satırdaki Öklid uzaklıklarının grafiksel gösterimi örneği verilmiştir. (a)'daki herhangi bir atak uygulanmamış sahte görüntüye ait bir satırı göstermekte iken (b)'de son işlem atağına maruz kalmış bir görüntüden elde edilen satırdaki uzaklık değerleri verilmiştir. Görüntüde atak olması durumunda da yöntemde dikkate alınan durumun varlığının söz konusu olduğu yapılan testlerde görülmüş olup bunun bir örneği de Şekil 2.17(b)'de sunulmuştur. Belirli bir süre minimum durumunu koruması hali sahteciliğin var olduğunu ifade etmektedir. Bu şartı sağlayan Öklid uzaklıklarının ortalama değeri, sahtecilik tespitinde kullanılacak eşik değeri olarak belirlenir. Algoritma 1'de bu aşamalara ait Matlab kodu verilmiştir.



Şekil 2.17. Dikkate alınan bloklar arasındaki Öklid mesafesi (a) Son işlemden geçirilmemiş sahte bir görüntü için S'den bir satır (b) Son işlemden geçirilmiş görüntüden sonra S'den aynı satır

Belirlenen eşik değeri th'a göre Msk olarak isimlendirilen ikili görüntüde (x, y) ile başlayan bloğa ait piksel değeri Eşitlik (2.7)'deki gibi belirlenerek elde edilir.

$$\forall x, y: (S^{xy} \leq th) \Rightarrow Msk^{x.y} = 255, x = 0 \dots b - 1, y = 0 \dots b - 1 \quad (2.7)$$

Şekil 2.18'de, Şekil 2.13'te verilen sahte görüntünün sahte blok işaretlemesi sonucu elde edilen sonuç görüntüsü yer almaktadır. Örnekteki görüntüde düşük kontrasta sahip birbirine oldukça benzer bölgelerin varlığı sebebi ile doğru işaretlemelerin yanında orijinal olduğu halde sahte olarak işaretlenen bloklar da yer almaktadır. Bir sonraki aşamada bu görüntünün iyileştirilmesi gerçekleştirilecektir.

Algoritma 1. Dinamik eşik belirleme
Girdi: Benzerlik Matrisi S, Eşleşme Matrisi M
Çıktı: Eşik değeri (th)

```
Function th= DinamikEsikBelirleme(S, M)
     [n, m] = size(S);
     th_avg = 0; th_min = 10;
     [U] = size(M,1);
     r = M(floor(rand * U),2);
     line = S(r, :);
     global_min = min(line);
     for j = 1 to m
         k = 0;
         if abs(line(j)-global_min)<=th_min
             index= j; k = j+1;
             while (abs(line(k)-line(k-1))<=th_min) && (k<=m)
                  k = k + 1;
             end
         end if
         if  k>0 break; end if
     end
     th= mean(line(index, k-1));
     return th;
end
```

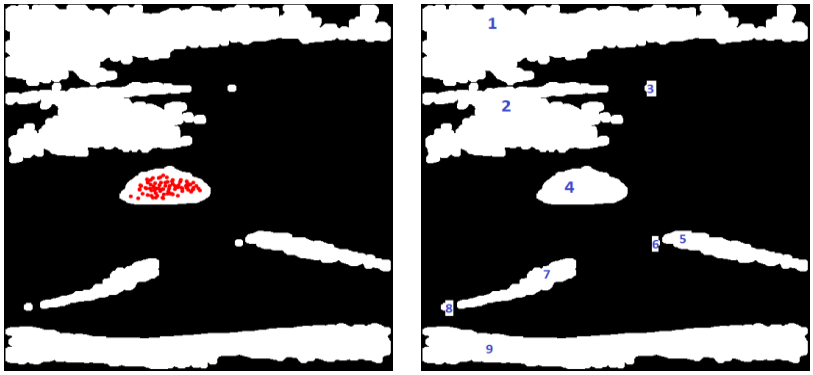
Şekil 2.18. Elde edilen binary görüntü

- **Bağlı Bileşen Etiketleme ve Sonuç Maskesi Üretimi**

Önerilen yöntemde bu aşamada sonuç görüntüsünün hatalı işaretlemelerden alındırılması amaçlanmıştır. Öncelikle taslak sahte bölgenin doku bilgisine göre Msk görüntüsüne morfolojik işlem uygular. Taslak sahte bölgenin kontrast bilgisine göre morfolojik açma veya kapama işlemi uygulanır. Bu işlemlerin uygulanma şartları aşağıdaki gibidir.

- Eğer değerlendirmeye alınan bölge düşük kontrasta sahip ise $(B_{düz} > B_{karmaşık})$, morfolojik açma (opening) işlemi uygulanır
- Eğer değerlendirmeye alınan bölge yüksek kontrasta sahip ise $(B_{düz} < B_{karmaşık})$, morfolojik kapama (closing) işlemi uygulanır

Morfolojik işlemden sonra Bölüm 2.1.1.5'te sunulan bağlı bileşen etiketleme algoritması kullanılarak ikili görüntünün etiketlenmesi gerçekleştirilir. Hatalı işaretlemelerin giderilmesinde bağlı bileşenlerde yer alan eşleşen anahtar noktaları dikkate alınmıştır. Yöntemde anahtar noktaların yer aldığı bağlı bileşen doğru işaretlemenin olduğu bölge olarak kabul edilirken, diğer bileşenler hatalı işaretlenmiş bölge olarak sonuç görüntüsünden çıkarılır. Daha önceki şekillerde de yer alan örnek sahte görüntü üzerindeki etkisi Şekil 2.19'da sunulmuştur. Şekil 2.19(a)'da morfolojik işlemler sonucu elde edilen görüntünün bilgi içeren bölgesinin yakınlaştırılmış hali gösterilmiştir. Aynı zamanda bu görüntüde eşleşen anahtar noktaları da yer almaktadır. (b)'de ise bağlı bileşen etiketlemesi algoritmasının sonucu yer almaktadır. Örnekte de görüldüğü gibi 9 bileşen bulunmaktadır, ancak eşleşen anahtar noktaları 4. bileşende yer almıştır. Bu durum göz önünde bulundurularak anahtar noktalarını kapsayan bileşenin sahte bölge diğerlerinin ise hatalı bölge olarak etiketlendirilmesi önerilmektedir.



(a) (b)

Şekil 2.19. (a) Bir önceki aşamada elde edilen doğru eşleşen anahtar noktaları (b) bağlı bileşenlerin etiketleri

Önerilen adımların uygulanması ile hatalı eşleşmeler giderilerek doğru bölgenin çıkarılması sağlanır. Görüntünün transformasyonu sonrası taslak hedef ve taslak kaynak bölgeleri üst üste örtüştürülerek tek bölge üzerinde işlem adımları uygulanmıştır. Dolayısı ile bu aşamaların sonucunda hedef bölgesi üzerinde sahte bölgenin sınırları belirlenmiş oldu. Hem kopyalanan hem yapıştırılan bölgelerin gösterildiği final sonuç maskesi ise doğru bölgenin gösterildiği görüntünün homografi matrisi H ile ters transformasyonu sonucu elde edilerek yöntem tamamlanmış olur. Şekil 2.20 (a)'da anlatımda kullanılan örnek sahte görüntünün hatalı işaretlemelerden arındırılması sonucu sahte bölgenin işaretlenmesi gösterilmiştir. (b)'de ise (a)'daki görüntünün ters transformasyon ile elde edilen sonuç maskesi görülmektedir. Önerilen yöntemde sunulan aşamaların tamamlaması ile sahte olarak belirlenen görüntüde yer alan sahte bölgelerin sınırlarının netliği kazanmıştır.

(a) (b)

Şekil 2.20. (a) Hatalı bileşenlerin elenmesinden sonra elde edilen sonuç (b) Ters transformasyon sonucu elde edilen sonuç maskesi

Bu bölümde tez kapsamında önerilen "L*a*b Renk Uzayından Faydalanarak Anahtar Noktası Tabanlı Şüpheli Bölgelerin Çıkarılması ve Dinamik Bir Lokalizasyon Yaklaşımı ile

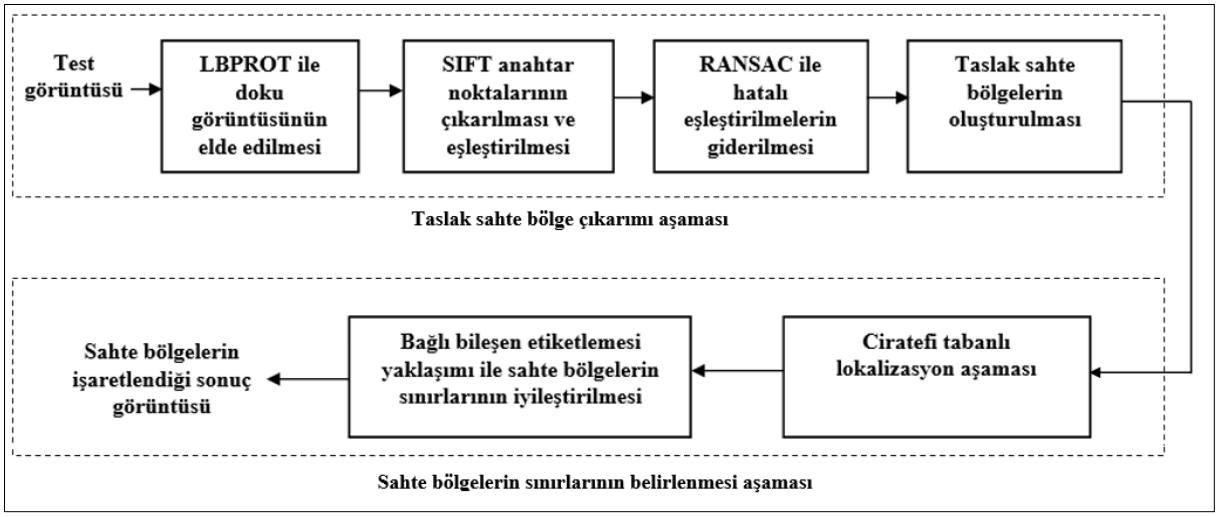
Sahtecilik Tespiti" yöntemine ilişkin detaylara yer verilmiştir. Sistemin girdisi olarak alınan RGB renk uzayında temsil edilen test görüntüsünün L*a*b* renk uzayına dönüştürülmesi, özellikle düşük kontrasta sahip bölgelere ait detayların elde edilmesi amacı ile gerçekleştirildi. Böylece literatürde anahtar noktası tabanlı yöntemlerde karşılaşılan, düşük kontrasta sahip bölgelerle yapılan sahteciliklerin tespit edilememesi problemi özgün bir yaklaşımla giderilmiştir. Sahtecilik ipuçlarının elde edilmesi için üç kanalda temsil edilen görüntülerden SIFT anahtar noktaları elde edilerek ve bunların kendi içlerinde eşleştirilmesi sağlandı. Geometrik dönüşüm bağımsız özelliğe sahip anahtar noktalarından faydalanmak, bu ataklara karşı dayanıklılık hedefinin gerçekleştirilmesine vesile olmuştur. İyileştirilmiş üç kanaldan da anahtar nokta eşleşmelerinin elde edilmesi, doğru eşleşen anahtar nokta sayısını arttırmış, bu da bu eşleşmelerden elde edilen transformasyon matrisi tahmininin daha etkin olmasını sağlamıştır. Yeterli sayıda eşleşmenin var oluşu ile görüntünün sahte veya orijinal olma durumu ortaya konmuş, sahte olarak etiketlenen görüntülerde eşleşmeler etrafında taslak sahte bölgeler oluşturulmuştur. Taslak sahte bölgelerin yer aldığı görüntü, anahtar nokta eşleşmelerinden elde edilen transformasyon matrisine göre transform edilerek, taslak sahte ve taslak hedef bölgelerin örtüşmesi sağlanmıştır. Transformasyon matrisinin etkin bir şekilde belirlenmesi sayesinde bu bölgelerin örtüştürülmesindeki başarımı artırmıştır. Böylece yöntemin piksel bazlı sahtecilik tespitindeki başarısı olumlu yönde etkilendiği görüldü. Örtüşen bölgelerde yer alan örtüşen alt blokların AKD özelliklerinden faydalanıldı. Böylece AKD tabanlı özelliklerin kullanılması ile son işlem ataklarına karşı dayanıklılık amacına ulaşıldı. Taslak kaynak ve taslak hedef bölgede karşılık düşen blokların AKD tabanlı özelliklerin karşılaştırmasında kullanılan eşik değerleri dinamik olarak elde edilmişti. Böylece yöntemin lokalizasyon aşamasındaki performansı girdi görüntüsünden bağımsızlık kazanmış, yüksek performans ile sahte piksellerin etiketlenebilmesi sağlandı.

2.2. LBPROT ve SIFT Yöntemine Dayalı Şüpheli Bölge Çıkarımı ve Ciratefi Tabanlı Lokalizasyon Yaklaşımı ile Sahtecilik Tespiti

Tez kapsamında önerilen yöntemlerin ikincisinde, hem bir önceki çalışmada karşılaşılan zorluklara alternatif yaklaşımlar önerilmiş, hem de literatürdeki eksikliklerin göz önüne alınması ile yüksek performans ile sahtecilik tespiti amaçlanmıştır. Önerilen yöntem temelde yine iki aşamadan oluşmaktadır; Taslak sahte bölge çıkarımı ve sahte bölge

sınırlarının belirlenmesi. Şekil 2.21'de bu aşamaların yer aldığı yönteme ilişkin genel blok diyagram verilmiştir.

Sisteme girdi olarak alınan renkli görüntünün ilk olarak Taslak sahte bölge çıkarımı aşamasına yönlendirilmesi ile önerilen yöntem icra edilmeye başlar. Düşük kontrasta sahip bölgelerden de ayırt ediciliği yüksek anahtar noktalarının elde edilebilmesi için girdi görüntüsünün doku görüntüsü çıkarılmıştır. Bunun için dönme ölçekleme gibi ataklara karşı da dayanıklılığı sağlayan LBPROT operatöründen faydalanılmıştır. İkinci aşamada ise doku görüntüsünden SIFT anahtar noktalarının elde edilmesi ve bunların özellik tanımlayıcı vektörleri aracılığı ile eşleştirilmesi gerçekleştirilmiştir. RANSAC ile eşleşen anahtar noktaları arasındaki matematiksel ilişki belirlenmiş ve bu ilişkiyi temsil eden modele uymayan eşleşmelerin elenmesi gerçekleştirilmiştir. Hatalı eşleşmelerden arınan eşleşme matrisinde yer alan anahtar noktalarının konum bilgilerinden faydalanarak taslak sahte bölgelerin sınırları belirlenmiştir. Böylece yöntemin ilk ana aşaması olan Taslak sahte bölge çıkarımı aşaması tamamlanmıştır. İkinci ana aşamada, bu taslak olarak belirlenen sahte bölgelerin sınırları, eşleşen anahtar noktaları ve taslak sahte bölgelerden faydalanarak kesinleştirilmiştir. Bu doğrultuda öncelikle önerilen Ciratefi tabanlı lokalizasyon aşaması icra edilmiş ve olarak hatalı işaretlemeler Bağlı Bileşen Etiketlemesi yaklaşımı ile giderilmiştir.



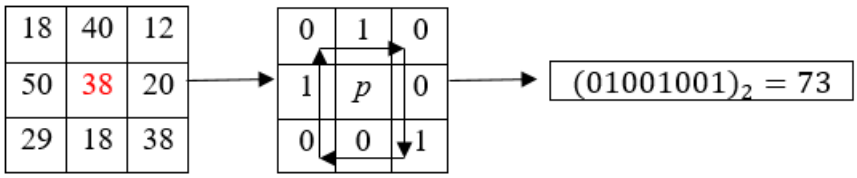
Şekil 2.21. Önerilen yöntemin genel akış diyagramı

2.2.1. Kullanılan Teorik Kavramlar

Bu bölümde önerilen yöntemde kullanılan teorik kavramlardan bahsedilecektir. Bu doğrultuda ilk olarak girdi görüntüsünden doku bilgilerinin çıkarılması amacı ile kullanılan LBPROT operatörü sunulacaktır. Daha sonra sahte bölgelerin sınırlarının belirlenmesi amacı ile gerçekleştirilen aşamada kullanılan Ciratefi algoritmasının detaylarından bahsedilecektir.

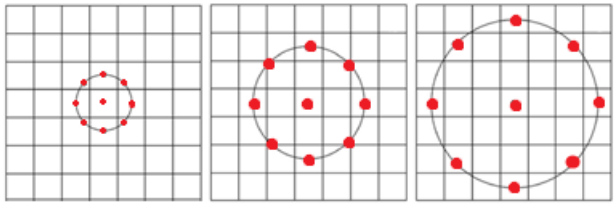
2.2.1.1. LBPROT Operatörü

LBPROT, temel Local Binary Pattern (Yerel İkili Örüntü, LBP) [165] operatörünün rotasyondan bağımsız şekli olup, önerilen çalışmada görüntüden doku bilgisi çıkarım amacıyla kullanılmıştır. LBP ilk olarak 1994'te Ojala ve arkadaşları tarafından önerilmiştir [165]. Şekil 2.22'de temel hesaplama mantığı verilen yöntemde, her bir bloktaki merkez piksel ile komşu pikselleri arasındaki ikili fark hesaplanarak ilgili piksel temsil edilmektedir. Genel LBP operatöründe örneklenen nokta sayısı ve komşuluk boyutunda herhangi bir sınırlama yoktur. Aynı yazarlar tarafından 2002 yılında sunulan çalışmada ise dönme bağımsızlığı barındıran, LBP'nin genelleştirilmiş hali önerilmiştir [166].



Şekil 2.22. LBP Operatörü

I gri seviye görüntü olmak üzere x. satır ve y. sütundaki bir piksel $i_c = I(x, y)$ olsun. (x, y) noktasının çembersel komşuluğunu, r yarıçapında P adet komşu pikseller oluşturacaktır. Şekil 2.23'te farklı r yarıçapındaki 8 komşu noktalı çembersel komşuluklar görülmektedir. Şekilde çember üzerinde yer alan kırmızı noktalar P adet komşu piksel noktalarını göstermektedir.



(a) (b) (c)

Şekil 2.23. 8 komşuluklu R yarıçaplı çembersel komşuluklar (a) LBP (8,1) (b) LBP (8,2) (c) LBP (8,3)

i_p, P noktalarının gri seviye değerini göstermek üzere örneklenen (x, y) noktası Eşitlik (2.8)'deki gibi hesaplanmaktadır. Önerilen yöntemde (x, y) noktasının 8 çembersel komşuluğu ve r yarıçapı kullanılmıştır.

$$\begin{aligned} i_p &= I(x_p, y_p), \quad p = 0, \dots P-1 \\ x_p &= x + r\cos(2\pi p/P) \\ y_p &= y - r\sin(2\pi p/P) \end{aligned} \tag{2.8}$$

$s(t)$ birim basamak fonksiyonunu göstermek üzere $t \geq 0$ olma durumunda fonksiyon bir aksi durumda sıfır sonucunu geri döndürecektir. Birim basamak fonksiyonu kullanılarak 8 komşuluklu r yarıçaplı noktanın LBP değeri Eşitlik (2.9)'da verildiği gibi hesaplanmaktadır.

$$LBP(x_p, y_p) = \sum_{p=0}^{7} s(i_p - i_c)2^p \tag{2.9}$$

Eğer görüntüdeki bir bölge herhangi bir bölgeye yapıştırılmadan önce döndürüldüyse, bölgenin LBP örüntüsü de merkezi etrafında dönecektir. Önerilen yöntemde LBPROT operatörü kullanılarak yöntemin rotasyon ataklarına dayanıklı olması sağlanmıştır. LBPROT operatörü Eşitlik (2.10)'da tanımlanmıştır. $ROR(x, i)$ gösterimi x bit dizisinin i adımlarla sağa döndürülmüş dairesel bit dizisini ifade etmektedir.

$$LBP^{ri}_{x_p, y_p} = \min_i ROR(LBP(x_p, y_p), i) \tag{2.10}$$

LBPROT operatörü, dairesel bit dizisi işlemleri sonuçları arasından en küçük LBP koda sahip olanını seçmektedir. En küçük LBP kodu, $LBP^{ri}_{x_v y_0}$, 3x3'lük bloğun merkez pikselini etiketlemek için kullanılır.

2.2.1.2. Ciratefi Algoritması

Ciratefi algoritması ilk olarak gri seviye görüntülerde dönme, ölçekleme gibi geometrik dönüşümlerin yanında, renk ve kontrast değişimlerine karşıda dayanıklı olacak şekilde, Q olarak isimlendirilebilecek bir şablon(template) görüntüsünün, büyük bir A görüntüsünde varlığının araştırılması temeline dayanır [167]. 2011 yılında Araújo vd. tarafından önerilmiştir. Algoritma ardışık olarak kullanılan 3 filtreden oluşmaktadır, bu filtreler Cifi (Circular Sampling Filter, Dairesel örnekleme filtresi), Rafi (Radial sampling filter, Radyal örnekleme) ve Tefi Template Matching, Şablon Eşleştirme Filtresi) olarak isimlendirilmiştir. Her filtreleme aşaması sonrasında, Q şablon görüntüsü ile eşleşemeyecek piksellerin elenmesi gerçekleştirilir. Cifi ve Rafi filtreleri ile ayrıca, ölçekleme oranı ve dönüş açısı hesabı yapmaktadır.

Ciratefi algoritması temelde ayrık bir dizi açı ve ölçek bilgisi kullanır. Ayrıca bu bilgiler kullanılarak yapılacak eşleşmelerde oluşabilecek sapmaların hatalı eşleşmelere sebep olmasını engellemek için A ve Q görüntülerinin ikisi de alçak geçiren filtre ile (Örneğin Gauss filtresi) bulanıklaştırılması gerçekleştirilir. Bu filtreleme ile açı ve ölçek kullanılmasının sebep olacağı hataların azalması sağlanır.

- **Korelasyon Katsayısı (Correlation coefficient)**

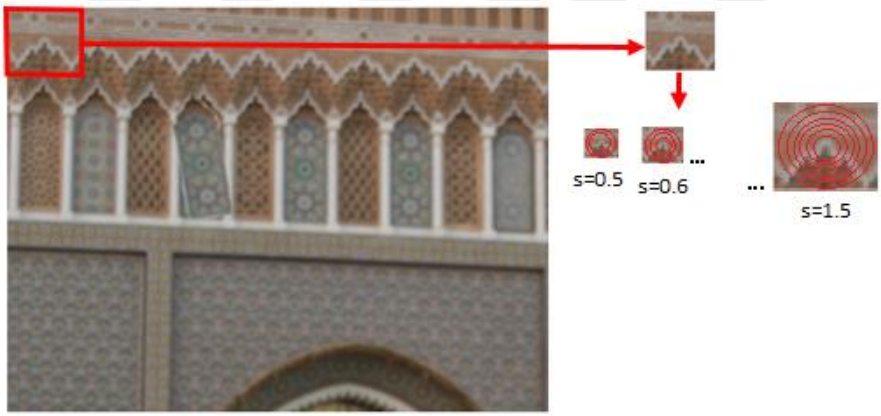
Orijinal Ciratefi algoritmasında, bir Q görüntüsünün A görüntüsünde aranması sırasında uygulanan her bir alt adımda, Q görüntüsünün A görüntüsünde yer alan bir (x, y) pikseli etrafındaki bölgeye ne kadar benzer olduğunu değerlendirmek için Korelasyon katsayısı kullanılmaktadır. v ve w sırasıyla Q ve A görüntüsündeki (x, y) etrafında yer alan görüntü bölgesinin gri seviye ortalama parlaklık değerlerini temsil ettiği varsayılırsa, korelasyon katsayısı Eşitlik (2.11)'deki gibi ifade edilebilir.

$$X(v, w) = \frac{\tilde{v}, \tilde{w}}{\|\tilde{v}\|.\|\tilde{w}\|} \tag{2.11}$$

Burada, $\tilde{v} = v - \bar{v}$'dir ve $\tilde{v}$ ifadesi v vektörünün ortalamasını ifade etmektedir. (Aynı durum $\tilde{w}$ ve $\bar{w}$ içinde geçerlidir.) Sıfıra bölme hatası alınmaması adına $\tilde{v}$ ve $\tilde{w}$ vektörlerinin boş olmayan vektörler olması gerekmektedir. Bu durumda Sıfırdan farklı olan bu iki vektör için, korelasyon katsayısı -1 ile +1 arasında değişmektedir. Korelasyon değeri 0'dan büyük olan bir eşik değeri t ile kontrol edilerek Q template görüntüsünün $A(x, y)$ görüntüsü ile eşleştiği ortaya konulmaktadır.

- **Birinci Filtre: Cifi Filtresi**

Ciratefi algoritmasında kullanılan ilk filtre Cifi (Circular Sampling Filter, Dairesel örnekleme filtresi) olarak isimlendirilmiştir. A görüntüsünde aranan Q template görüntüsünün, birinci derece aday piksellerin ve en iyi eşleşmenin sağlandığı ölçek değerinin bulunması için farklı yarıçapta dairesel örneklendirilmesi gerçekleştirilir. Şekil 2.24'te görüntüde yer alan bir alt blok herhangi bir bloğun farklı yarıçap değerleri ile örneklenmesi gösterilmiştir.



Şekil 2.24. Farklı yarıçap değerleri ile dairesel örnekleme

Bir B alt bloğu için görüntüsü için (x, y) pikselinden r kadar uzakta yer alan gri seviyeli piksellerin ortalamasını temsil eden dairesel örnekleme φ, Eşitlik (2.12)'de verildiği gibidir.

$$S_B^{\varphi}(x, y, r) = 1/2\pi r \int_0^{2\pi} A(x + t\cos\theta, y + r\sin\theta)d\theta \qquad (2.12)$$

B ile gösterilen blok, farklı oranlarda ölçeklemelere tabi tutularak $(s_0 = 0.5, s_2 = 0.6, \cdots, s_{i-1} = 1.5)$ n adet ölçeklendirilmiş alt görüntünün oluşturulmasında kullanılacaktır, $B_0 \cdots B_{i-1}$. Daha sonra yeniden ölçeklendirilmesi gerçekleştirilmiş her bir görüntü önceden belirlenen açı değerlerine göre $(r_0, r_1, \dots, r_j)$ j adet dairesel örneklendirilmeleri elde edilecektir. Buna göre sırası ile ölçek ve yarıçap özelliklerini göz önünde bulunduran i satır ve j sütundan oluşan ölçek ve rotasyon bağımsız 2 boyutlu özellik tablosu ifadesi Eşitlik (2.13)'deki gibidir.

$$C_Q = [a, b] = s_{Q_a}^{\varphi}(x_0, y_0, r_a), \quad 0 \le a < i, \quad 0 \le b < j \tag{2.13}$$

Burada, (x_0, y_0) Q template görüntüsünün merkez pikselidir. Büyük oranda küçültülmüş görüntüde bazı dairelerin elde edilememe durumları olabilmektedir. Bu daireler korelasyon hesabında kullanılmamaktadır ve C_Q(say, 1) tablosunda tutulmaktadır.

Bir A görüntüsündeki analizde, her bir (x, y) pikseli için l adet dairesel örneklemeyi barındırmak üzere Eşitlik (2,14)'de verilen 3 boyutlu görüntü oluşturulmaktadır.

$$C_A = [x, y, k] = S_A^{\varphi}([x, y, r]), \quad 0 \le k < l, \quad (x, y) \in \text{domain}(A) \tag{2.14}$$

Cifi filtresi her bir (x, y) pikseli için en iyi eşleşmeyi veren dairesel örneklemenin gerçekleştiği ölçeğin bulunmasında C_Q ve C_A matrislerini kullanmaktadır. Eşitlik (2.15)'de gösterildiği gibi template görüntüsünün, A görüntüsündeki maksimum korelasyon şartını sağlayan piksellerin seçimi sağlanır.

$$X_{A,Q}^{\varphi}(x, y) = \text{MAX}_{i=0}^{n-1}\left[X\left(C_Q[i], C_A[x, y]\right)\right] \tag{2.15}$$

Burada, $X\left(C_Q[i], C_A[x, y]\right)$ ifadesi $C_Q[i]$ ve $C_A[x, y]$ vektörleri arasındaki korelasyon katsayısıdır. Eğer $X_{A,Q}^{\varphi}(x, y) \ge t$ şartı sağlanırsa (x, y) pikseli "birinci derece aday piksel" olarak etiketlenmektedir.

(x, y) birinci derece aday pikseli için "en iyi ölçek oranı" korelasyon değerini maksimum veren ölçek oranıdır. Bu durum Eşitlik (2.16)'daki gibi formüle edilmiştir.

$$G_A{}^{\Omega}{}_{,Q}\,(x, y) = \text{ARGMAX}^{n-1}\,[X\,(C_Q\,[i], C_A[x, y])] \tag{2.16}$$

- **İkinci Filtre: Rafi Filtresi**

İkinci filtre Rafi (Radial sampling filter, Radyal örnekleme) filtresi A ve Q görüntülerinin radyal doğrularına iz düşümlerini kullanır. Şekil 2.25'te bir görüntüye ait radyal izdüşümü örneği verilmiştir. Bu filtre ile "birinci derece aday piksel"lerin belirli şartları sağlaması durumunda "ikinci derece aday piksel" olarak terfi edilmesi sağlanır. Koşulları sağlamayan aday piksellerin ise elenmesi gerçekleştirilir. Ayrıca "ikinci derece aday piksel"lerin elde edildiği açı değeri "en iyi eşleşme açısı" olarak tayin edilir. Bir B görüntüsü göz önüne alındığında, (x, y) noktasından λ uzunluğa ve α eğimine sahip, radyal çizgide bulunan piksellerinin gri seviye ortalaması olmak üzere radyal örnekleme şu şekilde tanımlanır:

$$S_B^{\emptyset}(x, y, \lambda, \alpha) = 1/\lambda \int_0^{\lambda} B(x + t\cos\alpha, y + t\sin\alpha)dt \quad (2.17)$$

Q template görüntüsü ve m adet açı değeri; $a_0, a_1, \ldots, a_{m-1}$ verildiğinde, Q görüntüsü r_{l-1}: en büyük örnekleme açısı değerini kullanarak, radyal örneklemesi gerçekleştirilir. Böylece m adet farklı özellik vektörüne sahip vektör elde edilmiş olur. Bu durum Eşitlik (2.18)'de formüle edilmiştir. Burada (x_0, y_0), Q görüntüsünün merkez pikselidir.

$$R_Q[j] = S_Q^{\emptyset}(x_0, y_0, r_{1-1}, a_j), 0 \leq j < m \quad (2.18)$$

Her bir "birinci derece aday piksel" (x, y) için, Formül (2.16) ile bulunan $G_A^{\Omega}{}_{,Q}$ (x, y) ölçek değeri olmak üzere, A görüntüsünün radyal örneklemesi Eşitlik (2.19)'daki gibi ifade edilmektedir.

$$R_A[x, y, j] = s_Q^{\emptyset}(x, y, s_i r_{1-1}, a_j), 0 \leq j < m \quad (2.19)$$

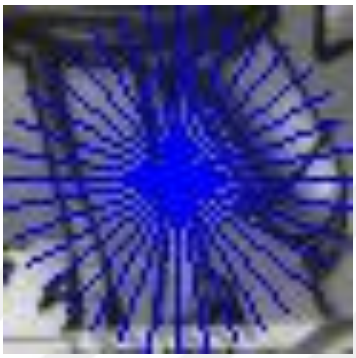
Burada, $s_i r_{l-1}$; ölçeklenmiş template görüntüsü Q_i'nin açı değeridir.

"Birinci derece aday piksel" lerin her biri (x, y) için, Rafi filtresi, Eşitlik (2.20)'de verilen radyal örnekleme korelasyonunu en iyi eşleşme açısında tespit etmek için $R_A[x, y]$ ve R_0 vektörünü kullanır.

$$X_{A,Q}^{\varphi}(x, y) = MAX_{j=0}^{m-1}[X(R_A[x, y], cshift_j, R_Q)] \quad (2.20)$$

Burada, cshift_j dairesel kaydırma anlamına gelir. Birinci derece aday piksellerin ikinci derece aday piksel olarak terfi edilebilmesi için $X^{\varphi}_{A,Q}(x,y) > t_2$ koşulunun sağlanması gerekir. İkinci derece aday pikseller için en iyi dönme açısı korelasyon değerimi maksimize edebilen değerdir. Bu durum Eşitlik (2.21) ile verilmiştir.

$$G^{\emptyset}_{A,Q(x,y)} = \text{ARGMAX}_{j=0}^{m-1}\left[X\left(R_A[x,y],\ \text{cshift}_j, R_Q\right)\right] \quad (2.21)$$



Şekil 2.25. Bir görüntünün radyal izdüşümleri

- **Üçüncü Filtre: Tefi**

Tefi (Template Matching, Şablon Eşleştirme Filtresi) olarak adlandırılan üçüncü filtre, her ikinci sınıf aday pikselin komşusu ile Cifi ve Rafi tarafından belirlenen ölçek ve açı kullanılarak ölçeklendirilen ve döndürülen şablon arasındaki korelasyon katsayısını hesaplar.

Tefi önce Q template görüntüsünü tüm açılara ve ölçeklere göre yeniden boyutlandırıp döndürür ve bunları T_Q adlı bir tabloda saklar. (x,y) ikinci derece aday piksel olsun, olası ölçek; $G_A{}^{\Omega}{}_{,Q}$ (x, y) ve olası açı; $G_A{}^{\emptyset}{}_{,Q}$ (x, y). Tefi, A görüntüsünde yer alan (x, y) pikseli için, $T_Q[i,j]$' de yer alan görüntüler ile arasındaki korelasyon katsayısını hesaplar. Algoritmayı daha sağlam kılmak için Tefi, ölçekleri (i-1), (i), (i + 1) ve açıları (j-1), (j), (j + 1) olacak şekilde alır ve en büyük korelasyon katsayısını bulur.

Korelasyon katsayısı bir t_3 eşiğinden daha büyük değeri veren (x,y) pikseli için Q template görüntüsünün eşleşmesinin doğruluğu, ilgili açı ve ölçekte olduğu kabul edilir. Ayrıca Q template görüntüsünün A görüntüsünde olduğu kesin olarak bilinirse eşik değerine gerek kalmadan en yüksek korelasyona sahip piksel eşleşmenin olduğu merkez piksek olarak seçilir.

2.2.2. Önerilen Yöntem

Yapılan çalışmada düz bölgelerle yapılan sahtecilikleri dahi tespit edebilen, ön işlem ve son işlem ataklarına karşı dayanıklı özgün bir kopyala-yapıştır sahteciliği yöntemi önerilmiştir. Önerilen yöntem Şekil 2.26'da gösterildiği gibi temelde iki aşamadan oluşmaktadır. Bu aşamaların ilkinde öncelikle girdi görüntüne ait doku görüntüsü çıkarılmış, doku görüntüsünün bütününden anahtar noktaları elde edilmiştir. Sahte bölgede yer alan anahtar noktaları benzer özellik göstereceğinden anahtar noktalarının eşleşmesi gerçekleştirilmiştir. Eşleşen anahtar noktalarının konum bilgisinden faydalanılarak taslak sahte bölgelerin çıkarılması işlemi gerçekleştirilmiştir. İkinci ana aşamada ise, bu aşamaya yönlendirilen anahtar nokta eşleşmeleri ile taslak olarak belirlenen sahte bölgelerde, sahtecilik sınırlarının temelde Ciratefi tabanlı yeni bir lokalizasyon yaklaşımı ile kesinleştirilmesi sağlanacaktır. Bu adımın icrası ile sahte olarak belirlenen piksellerin işaretlendiği sonuç görüntüsü elde edilerek yöntem tamamlanmaktadır. İki temel adımda gerçekleştirilen işlem adımlarına ilişkin detaylar iki alt başlık halinde sunulacaktır.

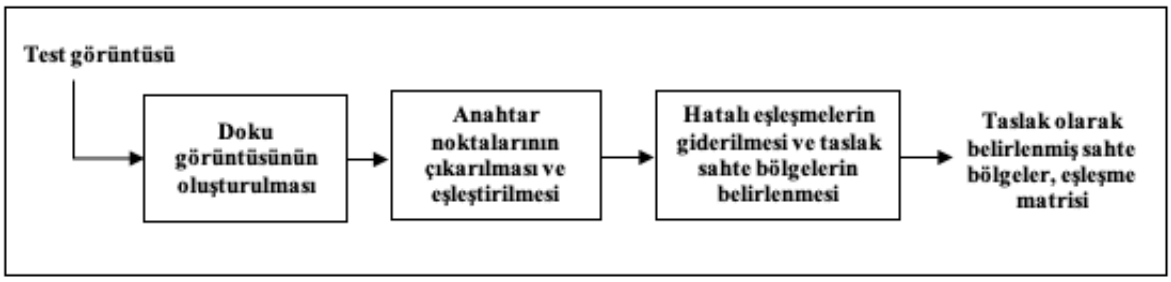
Şekil 2.26. Önerilen yöntemin alt adımları

2.2.2.1. Taslak Sahte Bölgelerin Çıkarımı

Taslak sahte bölgelerin çıkarımı aşamasında, anahtar noktası tabanlı bir yaklaşımla girdi görüntüsünün öncelikle sahte veya orijinal olma durumu belirlenmiş, daha sonra görüntünün sahte olması durumu söz konusu ise taslak sahte bölgelerin çıkarımı gerçekleştirilmiştir. Bu aşamaya ilişkin detaylar bu bölümün devamında verilmiştir.

Girdi görüntüsünün doğrulanması ve taslak sahte bölgelerin çıkarımı için gerçekleştirilen işlem adımları üç ana aşamada toplanmıştır. Şekil 2.27'de bu adımları içeren blok diyagram sunulmuştur. İlk adımda girdi görüntüsünün LBPROT operatörü yardımı ile doku görüntüsü elde edilmiştir. İkinci adımda elde edilen doku görüntüsünün bütününden SIFT anahtar noktaları ve bunlara ait özellik tanımlayıcılar elde edilmiştir. Ardından elde

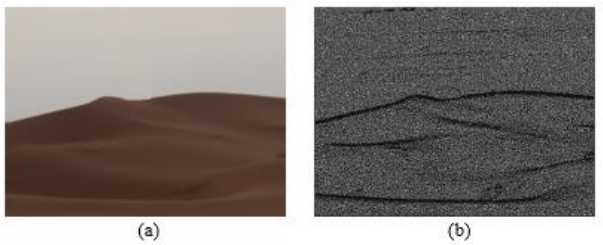
edilen anahtar noktaların eşleştirilmesi gerçekleştirilerek ikinci adım tamamlanmıştır. Üçüncü adımda ise olası hatalı eşleşmelerin giderilmesi için RANSAC algoritmasından faydalanılmıştır. Anahtar nokta eşleşmeleri, hatalı eşleşmelerden arındırıldıktan sonra yeterli sayıda eşleşmenin varlığı durumuna göre görüntünün sahte veya orijinal olma durumu ortaya konmuştur. Görüntünün sahte olması durumunda şüpheli sahte bölgeler taslak olarak belirlenerek yöntemin bu aşaması tamamlanmıştır.



Şekil 2.27. Taslak sahte bölge çıkarımı aşamasının blok diyagramı

- **Doku Görüntüsünün Oluşturulması**

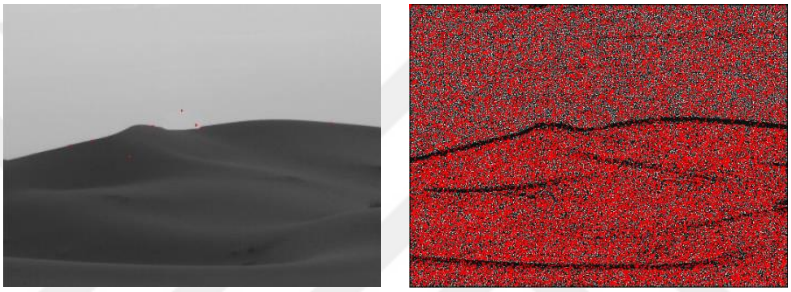
Önerilen yöntemde özellikle geometrik dönüşüm ataklarında yüksek dayanıklılık sağlayan anahtar noktası yaklaşımlar referans alınmıştır. Anahtar noktası tabanlı yöntemlerinde düşük kontrasta sahip bölgelerden anahtar nokta çıkarılamadığı için bu özelliğe sahip bölgelerle yapılan sahteciliklerin tespit edilememesi problemi önceki bölümlerde de bahsedilmişti. Önerilen yöntemde bu problemin üstesinden gelebilmek amacı ile girdi görüntüsünün öncelikle doku görüntüsünün çıkarılması gerçekleştirilmiştir. Doku bilgisinin çıkarımında LBPROT operatöründen faydalanılmıştır. Bölüm 2.2.1.1'de teorik detayları sunulan LBPRPOT operatörü komşu sayısı P=8 ve yarıçap değeri $r = 3$ olacak şekilde kullanılmıştır. Şekil 2.28'de örnek sahte görüntüden LBPROT uygulanarak elde edilen doku görüntüsü verilmiştir.



Şekil 2.28. (a)Kopyala-yapıştır sahteciliği uygulanmış görüntü (b) LBPROT operatörü kullanılarak elde edilen doku görüntüsü

- **Anahtar Noktası Çıkarma ve Eşleştirme**

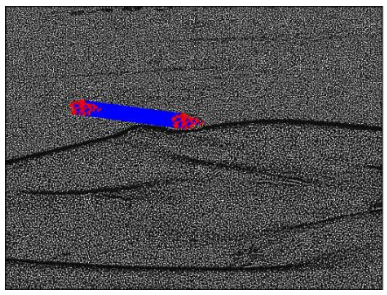
Bu aşamada ilk olarak, yukarıdaki aşamada elde edilen doku görüntüsünden Bölüm 1.4.2.2.1'de sunulan SIFT anahtar noktaları çıkarılmaktadır [142]. Şekil 2.29'da düz bölgelerin yoğun olduğu sahte bir görüntüden elde edilen SIFT anahtar noktaları gösterilmiştir. (a)'da görüntünün gri seviyeli halinden doku çıkarma aşaması olmadan elde edilen anahtar noktaları verilmiştir. (b)'de ise bir önceki aşamanın gerçekleştirilmesi sonrası elde edilen doku görüntüsü üzerinde çıkarılan anahtar noktaları gösterilmiştir. Şekildeki örnekte de görüldüğü gibi bir önceki aşamanın gerçekleştirilmesi ile bu aşamada görüntü üzerinden yeterli sayıda anahtar noktalarının elde edilebilmesi sağlanmıştır.



(a) (b)

Şekil 2.29. Sahte doku görüntüsünden elde edilen SIFT anahtar noktaları

SIFT anahtar noktalarının elde edilmesi aşaması tamamlandıktan sonra, elde edilen anahtar noktalarının özellik tanımlayıcı vektörler yardımı ile eşleştirilmesi gerçekleştirilmiştir. Bunun için yine bir önceki yöntemde kullanılan genelleştirilmiş 2NN (g2NN) yaklaşımı aynı parametre değerleri ile uygulanmıştır [108]. Şekil 2.30'da Şekil 2.29(b)'de gösterilen anahtar noktalarının eşleşmeleri sonucu sunulmuştur.



Şekil 2.30. Sahte doku görüntüsünden elde edilen SIFT anahtar noktalarının eşleşme sonucu

- **Hatalı Eşleşmelerin Giderilmesi ve Taslak Sahte Bölgelerin Belirlenmesi**

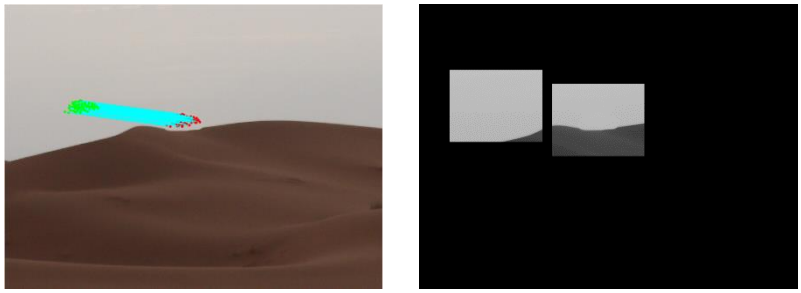
Önerilen yöntemde eşleşen anahtar noktalarındaki geometrik ilişkiyi barındıran matematiksel modelin belirlenmesinde RANSAC (Random Sample Consensus) algoritmasından faydalanılmıştır.

RANSAC (Random Sample Consensus) yüksek oranda yanlış eşleşmelere sahip veri setindeki hataları minimize etmek için Fischler tarafından önerilen tekrarlamalı bir yöntemdir [159]. Model parametrelerini tahmin etmek için gerekli olan minimum sayıda gözlem noktası (veri) içeren kümeyi kullanarak, tutarlı veri noktalarıyla bu kümeyi genişletip aday çözümler üretir. Bu yöntemde rastgele eşleşen belli sayıda anahtar noktaları seçilerek Eşitlik (2.11)'de eşleşen anahtar noktaları ve 3x3'lük H transformasyon matrisi arasındaki ilişki verilmiştir.

$$\begin{bmatrix} x_i' \\ y_i' \\ 1 \end{bmatrix} = H \begin{bmatrix} x_i \\ y_i \\ 1 \end{bmatrix} \tag{2.11}$$

Eşleşen anahtar noktaları, RANSAC yaklaşımı ile tahmini yapılan H transformasyon matrisine göre transform edilir. Daha sonra, her bir anahtar noktasının yeni konumları ile eşleşmesinin gerçekleştirildiği anahtar noktası arasındaki Öklid uzaklığı kontrol edilmektedir. Bu uzaklığın önceden belirlenen γ eşik değerinden küçük olması durumunda bu eşleşme doğru eşleşme (inlier) olarak kabul edilir. Bu eşikten büyük uzaklığa sahip eşleşmeler de yanlış/aykırı eşleşme olarak kabul edilmektedir. Yöntemde en fazla doğru eşleşme bulunana kadar, önceden belirlenmiş iterasyon sayısına göre, $N_{iterasyon}$, en uygun transformasyon kestirimi gerçekleştirilir. Yapılan çalışmada gerçekleştirilen deneyler ışığında γ= 0.05 ve $N_{iterasyon}$=1000 olarak alınmıştır. Belirlenen parametrelerin kullanımı ile yöntemin tamamlanması sonucu aykırı eşleşmeler M eşleşme matrisinden çıkarılmıştır.

M matrisinde yer alan doğru eşleşmelerin konumlarından faydalanarak şüpheli kaynak ve hedef bölgeler kabaca belirlenecektir. Bu aşamada bir önceki yöntemde önerilmiş olan kaynak hedef belirleme yaklaşımı kullanılmıştır. Şekil 2.31'de eşleşen anahtar noktaları etrafındaki bölgeleri gösteren şüpheli kaynak ve hedef bölgeleri belirlenmiştir.

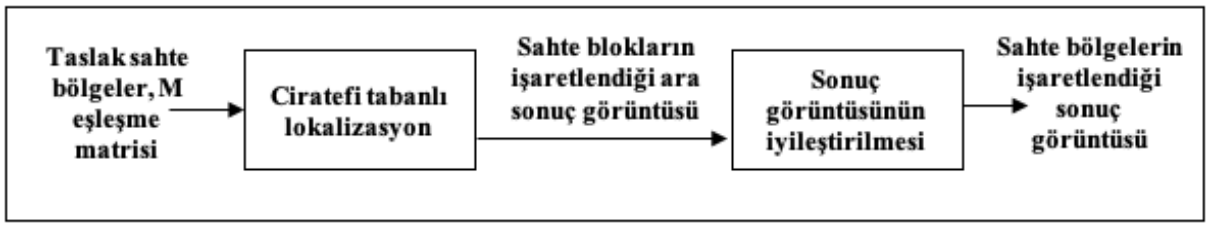


(a) (b)

Şekil 2.31. (a) Eşleşen anahtar noktaları(b) Şüpheli kaynak ve hedef bölgeleri

2.2.2.2. Sahtecilik Sınırlarının Belirlenmesi

Önerilen yöntemin bu adımında, taslak sahte bölgelerde yer alan sahte bölgelerin sınırlarının, M eşleşme matrisinde yer alan anahtar noktaları aracılığı ile netleştirilmesi hedeflenmiştir. Şekil 2.32'de önerilen işlem adımlarının girdi ve çıktı verileri ile yer aldığı blok diyagram verilmiştir. Sahte bölgelerin sınırlarının belirlenmesinde taslak sahte bölgelerden bir bölgede yer alan anahtar noktaları merkez kabul edilerek alt görüntü blokları oluşturulacaktır. Anahtar noktasının merkez olduğu alt blokların örtüşen komşularının ikinci bölgede benzerlerinin olup olmadığı kontrol edilecektir. Benzerliğin kontrolünde dönme ve ölçekleme bağımsızlığı sağlayan Ciratefi tabanlı bir yaklaşımın kullanılması önerilmiştir. Komşu blokların önerilen yaklaşım ile kontrol edilmesi sonrası sahte blok veya orijinal blok olarak etiketlemesi gerçekleştirilecektir. Sahte blok olarak etiketlenen blokların da yine 8 yönlü komşulukları aday sahte blok olarak değerlendirilmeleri gerçekleştirilecektir. Aday sahte blok kalmayıncaya kadar lokalizasyon aşaması icra edilecektir. Bu yaklaşımın tamamlanması sonrası sahte blokların işaretlenerek ikili (binary) bir maske görüntüsünün oluşturulması gerçekleştirilmiştir. Oluşturulan maske görüntüsünde varsa hatalı işaretlemelerin giderilmesi için önceki yöntemde önerilen yaklaşımlardan olan bağlı bileşen etiketlemesine dayalı iyileştirme aşamasından faydalanılacaktır. Böylece önerilen yöntemin son çıktısı olan sahte bölgelerin işaretlendiği sonuç görüntüsü üretimi ile yöntem tamamlanmış olacaktır. Alt bölümlerde bu aşamaya ait detaylara yer verilecektir.



Şekil 2.32.Sahte bölgelerin sınırlarının belirlenmesi aşamasının blok diyagramı

- **Ciratefi Tabanlı Lokalizasyon Yaklaşımı**

Yapılan çalışmada M eşleşme matrisinde yer alan anahtar noktaları ve taslak sahte bölgelerin kullanımı ile temelde Ciratefi algoritmasına dayanan bir yaklaşım ile sahte blokların işaretlenmesi gerçekleştirilecektir. Bu doğrultuda bu iki taslak sahte bölgeden rastgele seçilmek üzere bir bölge 'taslak kaynak bölge' diğer bölge ise 'taslak hedef bölge' olarak belirlenecektir. Yöntemde, taslak kaynak bölgede yer alan anahtar noktalar merkez kabul edilerek, bu noktalar etrafında belirlenen 17x17 boyutlu karesel bloklar 'sahte blok' olarak kabul edilir. Sahte blokların komşuluğunda yer alan blokların, taslak hedef bölgede benzerlerinin bulunmasına dayanan bir arama yaklaşımı ile sahte bölgelerin genişletilmesi hedeflenmiştir.

Genişletme işleminde şu yaklaşım önerilmiştir; İlk olarak taslak kaynak ve taslak hedef bölgede yer alan anahtar noktalar arasındaki dönme veya ölçekleme bilgisi Ciratefi yaklaşımı ile elde edilir. Sahte olarak atanan blokların sekiz yönlü örtüşen komşuları aday sahte blok olarak belirlenir. Her bir aday sahte bloğun taslak hedef bölgede en benzerlerinin aranması Ciratefi yaklaşımına göre gerçekleştirilmektedir. Bulunan eşleşmeler arasındaki ölçme ve dönme bilgisinin ilk adımda bulunan bilgiler ile tutarlılığı kontrol edilir. Önerilen yaklaşıma göre bir aday bloğun, hedef bölgede benzerinin bulunması durumunda, bu aday bloğun ve bulunan benzer bloğun sahte blok olarak etiketlenmesi gerçekleştirilmektedir. Taslak kaynak bölgede sahte olarak belirlenen her blok için bir örtüşen sekiz yönlü komşu blokların sahte veya orijinal olma durumunun kontrolü aday sahte blok kalmayıncaya kadar önerilen arama işlemi iteratif bir şekilde devam eder. İterasyonun tamamlanması sonrası sahte olarak belirlenen blokların işaretlenmesi gerçekleştirilir. Yukarıda bahsedilen yaklaşımda önerilen işlem adımları şu şekildedir;

Adım 1: Taslak kaynak ve taslak hedef bölgenin belirlenmesi.

Adım 2: Taslak kaynak bölgede yer alan anahtar noktaları merkez olacak şekilde 17x17 boyutlu blok ‘sahte blok’ olarak etiketlenir.

Adım 3: Taslak kaynak ve taslak hedef bölgede yer alan anahtar noktalar arasındaki dönme veya ölçekleme bilgisi Ciratefi yaklaşımı ile elde edilir.

Adım 4: Aday sahte blokların merkezi konumunu depolayacak şekilde bir yığın veri yapısı oluşturulur.

Adım 5: Her bir sahte bloğun örtüşen 8 yönlü komşusunda yer alan bloklar ‘aday sahte blok’ olarak belirlenir. Aday sahte blokların merkez konum bilgisi yığına itilir.

Adım 6: Yığın boş değil ise devam et. Yığın boş ise sahte blokların işaretlendiği sonuç görüntüsünü oluştur.

Adım 7: Aday sahte bloğun Ciratefi ile taslak hedef bölgesindeki karşılığının dönme ve ölçekleme bilgisi Adım 3’te bulunan bilgiler ile kontrol edilir. Tutarlılık var ise aday sahte blok ‘sahte blok’ olarak etiketlenir. Adım 5’ e gidilir.

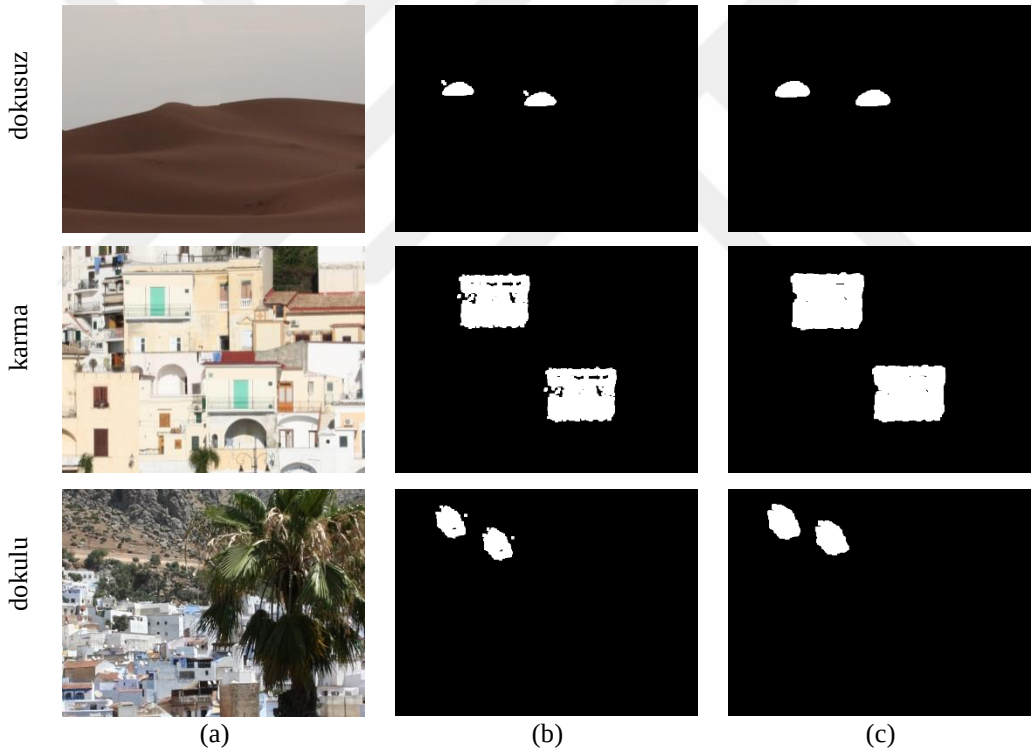
Önerilen işlem adımları içeren Ciratefi tabanlı lokalizasyon aşamasına ilişkin Matlab kodu Algoritma 2’de verilmiştir.

Algoritma 2. Ciratefi tabanlı lokalizasyon
Girdi: Eşleşme Matrisi (M[xi,yi,xj,yj]), Taslak bölgeler R1,R2
Çıktı: Sahte Blok Matrisi (SB)

```
Function M= BlokEslesle(M, R1,R2)
    Adaylar=[]; //aday blokların merkezleri depolanacak yığın veri
                  yapısı
    Adaylar=[{M(xi-1, yi-1) (xj-1, yj-1)};… ;{M(xi+1, yi+1) (xj+1,
                  yj+1)}]
             //Eşleşme matrisinde bulunan noktaların 8 komşuluğundaki
             //piksellerin aday sahte blok olarak değerlendirilmek
             //üzere matrise eklenmesi
    [aci,olcek,x_,y_]=Ciratefi[(xi,yi)];// anahtar nokta
                                        eşleşmelerinden
                                        //faydalanarak eşleşmeler
                                        arası //açı ve ölçek
                                        bilgisinin elde //edilmesi
    While Adaylar =∅
          indeks=size(Adaylar,1);
          x= Adaylar (indeks,1); y= Adaylar (indeks,2);
          blok1= R1(x:8+x:8+ y:8+y:8);
          [aci1,olcek1,x1,y1]=Ciratefi[(xi,yi)];
          if aci1=aci &&olcak1=olcek;
              M [M; x y x1 y1];
              Adaylar(indeks,:)=[];
          Else
              Adaylar(indeks,:)=[];
          End
     End
End
```

- **Hatalı İşaretlemenin Giderilmesi**

Önerilen yöntemde bu aşamada sonuç görüntüsünün hatalı işaretlemelerden arındırılarak iyileştirilmesi amaçlanmıştır. Bunun için öncelikle Bölüm 2.1.1.5'te sunulan bağlı bileşen etiketleme algoritması kullanılarak ikili görüntünün etiketlenmesi gerçekleştirilir. Önerilen yaklaşımda bağlı bileşenlerde yer alan piksel sayısının kontrolü ile küçük boyutlu işaretlemelerin giderilmesi hedeflenmiştir. Her bir bileşende yer alan toplam piksel sayısı ∂ eşik değerine göre kontrol edilir. $\partial < 70$ olması durumunda bu bileşenin hatalı işaretleme olduğu kabul edilerek sonuç görüntüsünden çıkarılır. Son olarak morfolojik genişletme (dilation) kullanılarak sonuç görüntüsünün son hali elde edilir. Şekil 2.33'te dokusuz, dokulu ve karma (hem düz hem dokulu) bölgeler içeren sahte görüntüler üzerinde bu aşamadan önce ve sonra elde edilen görüntüler yer almaktadır.



Şekil 2.33. (a)Sahte görüntüler (b) Son işlem adımı öncesi işaretlenen sahte bölgeler (c)Son işlem adımı sonrası sahte bölgelerin gösterildiği sonuç görüntüsü

Yukarıda tez kapsamında önerilen "LBPROT ve SIFT Yöntemine Dayalı Şüpheli Bölge Çıkarımı ve Ciratefi Tabanlı Lokalizasyon Yaklaşımı ile Sahtecilik Tespiti" yöntemine ilişkin detaylar sunulmuştur. Anahtar noktası tabanlı yöntemlerde, düşük

kontrasta sahip bölgelerden anahtar noktalarının elde edilememesi durumunun üstesinden gelebilmek için, yöntemde girdi görüntüsünün LBPROT operatörü aracılığı ile doku görüntüsü elde edilmiştir. Doku görüntüsünün bütününden elde edilen SIFT anahtar noktalarının birbirine en benzerlerinin eşleştirilmesi sonrası, yeterli eşleşmenin varlığı ile görüntünün sahte olduğu ortaya konmuştur. Görüntünün sahte olması durumunda sahte bölgeler taslak olarak eşleşen anahtar noktaları etrafında belirlenmiştir. Sahtecilik sınırlarının belirlenmesi için Ciratefi tabanlı özgün bir yaklaşım önerilmiştir. Bu doğrultuda taslak kaynak bölgede yer alan anahtar noktalarının komşuluğundaki alt blokların en benzerlerinin taslak hedef bölgede Ciratefi yöntemi ile aranması sağlanmıştır. Ciratefi yaklaşımının dönme ve ölçekleme bağımsızlık sağlayan filtreleri kullanması sayesinde, yüksek parametrelerle gerçekleştirilen geometrik ataklarına karşı dayanıklılık hedefi gerçekleştirilmiştir. Yöntemin literatürde yer alan verisetleri üzerinde popüler çalışmalarla kıyaslanması üçüncü bölümde sunulacaktır.

3. BULGULAR VE İRDELEME

Bu bölümde doktora tezi kapsamında gerçekleştirilen çalışmalara ilişkin deneysel bulguların literatürde var olan referans çalışmalar ile sonuç kıyaslaması gerçekleştirilerek önerilen yöntemlerin avantaj ve dezavantajları irdelenecektir. Alt bölümlerde öncelikle kullanılan veri tabanları ile çalışmaların performans kıyaslaması için kullanılan ölçütler verilecek daha sonra da önerilen yöntemlerin diğer çalışmalarla kıyaslamalarına ilişkin detaylar sunulacaktır. Son bölümde ise tez kapsamında önerilen iki yöntemin verisetleri üzerinde karşılaştırmalı analizini içeren detaylar verilecektir.

3.1. Kullanılan Veri Setleri

Tez kapsamında önerilen yöntemlerin performans değerlendirmesinde literatürde yer alan popüler kopyala-yapıştır sahteciliği verisetlerinden olan GRIP [41], CMH [139] ve tez kapsamında oluşturulan veriseti kullanılmıştır. Bu verisetlerinde hem ataksız sahte görüntüler hem de bazı son işlem ve ön işlem ataklarına maruz bırakılarak oluşturulan sahte görüntüler ile her bir sahte görüntüye ait sahtecilik maskeleri yer almaktadır. Bu sahte görüntülerin oluşturulmasında kopyalanan bölgelerin dokulu yani yüksek kontrast bilgisine sahip bölge olma özelliği gösteren örneklerine ek olarak dokusuz yani düşük kontrast bilgisine sahip bölgelerle oluşturulduğu da görülmektedir. Ayrıca dokusuz ve dokulu bölgelerin bulunduğu karma bölge olarak adlandırabileceğimiz bölgelerle gerçekleştirilen sahte görüntüler bulunmaktadır. Şekil 3.1'de GRIP verisetinde yer alan örnek sahte görüntülere, Şekil 3.2'de ise CMH verisetinde yer alan örnek sahte görüntülere yer verilmiştir. Bu veri setlerinin seçilmesinin nedeni, veri setlerinde dokusuz bölgelerle oluşturulan sahte görüntülerin sayıca fazla olmasıdır. Literatürde özellikle dokusuz bölgelerle oluşturulan sahte görüntülerin tespitinde anahtar noktası tabanlı yöntemlerin performans düşüklüğü durumu göz önünde bulundurulmuş, önerilen yöntemlerin bu durumdaki görüntülerde gösterdikleri performanslar üzerine deneyler gerçekleştirilmiştir.

Şekil 3.1. GRIP verisetinde yer alan farklı doku bilgisine sahip (dokulu, düz ve karışık) örnek sahte görüntüler ve sahtecilik maskeleri

GRIP ve CMH'da yer alan sahte görüntülere ilişkin detaylar aşağıdaki şekilde verilmiştir.

GRIP verisetinde, ataksız görüntülere ek olarak bazı son işlem ve ön işlem ataklarına maruz kalarak oluşturulan sahte görüntüler yer almaktadır. Bu atakların türleri, atakları oluştururken kullanılan parametreler ve her bir atak türünden verisetinde kaç adet bulunduğuna dair bilgiler Tablo 3.1'de verilmiştir.

Tablo 3.1. GRIP verisetinde yer alan görüntülerin oluşturulmasında kullanılan parametreler ve atak bazında görüntü sayıları

Atak türü	**Parametreler**	**Görüntü sayısı**
Dönme	Dönme derecesi =2°, 4°, 6°, 8°, 10°, 20°, 30°,45°, 60°, 75°, 90°,105°, 180°	13x80= 1040
Ölçekleme	Ölçekleme oranı (%) = 50, 80, 93, 95, 97, 99, 101, 103, 105, 107, 109, 120, 200	13x80=1040
Gürültü ekleme	$\sigma = 0.02, 0.04, 0.06, 0.08, 0.1$	5x80=400
JPEG sıkıştırma	Kalite faktörü= 20, 30, 40, 50, 60, 70, 80, 100	8x80=640

CMH verisetinde toplamda 216 adet kopyala-yapıştır sahteciliği uygulanmış, boyutları 845x634 ile 1296x972 arasında değişen görüntüler bulunmaktadır. Verisetinde yer alan sahte görüntüler yazarlar tarafından dört grupta değerlendirilmiştir.

• CMH1 grubunda 23 adet ekstra atak uygulanmamış (ataksız) sahte görüntüler bulunmaktadır.

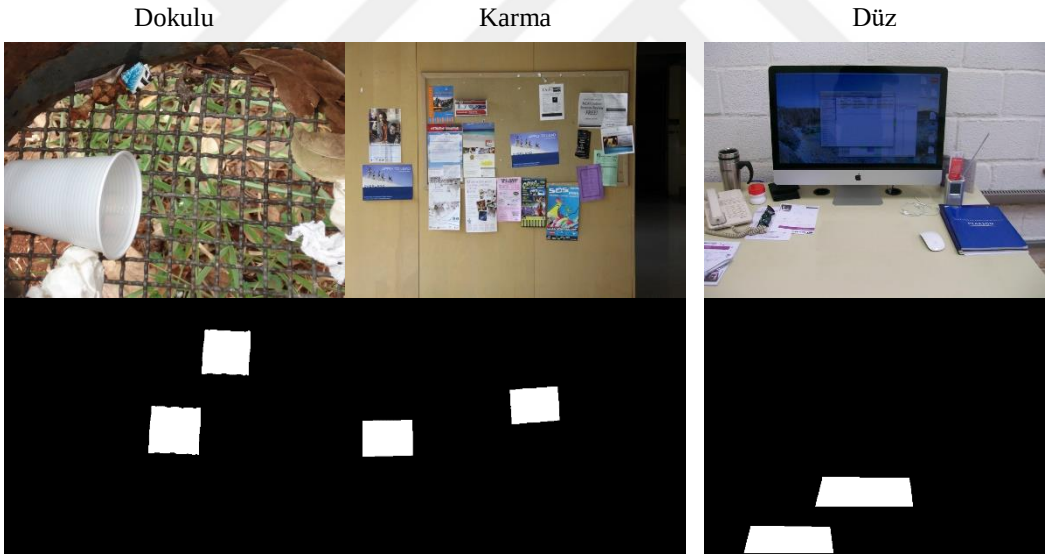
• CMH2 grubunda 25 adet dönme atağına maruz kalarak oluşturulmuş sahte görüntü yer almaktadır. ($-90°$ ile $180°$ arasında değişen açı değerleri);

• CMH3 grubunda yine 25 adet ölçekleme atağına maruz kalarak oluşturulmuş sahte görüntü yer almaktadır.

• CMH4 grubunda 35 adet farklı oranlarda hem dönme hem ölçekleme atağına maruz kalarak oluşturulan sahte görüntüler yer almaktadır.

• CMH ALL isimli grupta CMH1-4 grubundaki sahte görüntülerin hepsi yer almaktadır. Böylece bu grupta 108 adet sahte görüntü bulunmaktadır.

• CMH COMPRESSED isimli grupta CMH ALL grubundaki bütün sahte görüntülerin JPEG sıkıştırma uygulanarak depolanan halleri mevcuttur. JPEG sıkıştırma atağı uygulanırken kullanılan kalite faktörü 70, 80 ve 90 olacak şekilde rastgele belirlenmiştir.



Şekil 3.2. CMH verisetinde yer alan farklı doku bilgisine sahip (dokulu, düz ve karışık) örnek sahte görüntüler ve sahtecilik maskeleri

Önerilen yöntemlerin literatürdeki yöntemlerle karşılaştırmalarının yapılması için tez kapsamında Gerçekçi Kopyala-Yapıştır Sahteciliği Veri seti (Realistic Copy-Move Forgery Dataset) oluşturulmuştur. Veri setinde, farklı boyutlara sahip 80 adet orijinal görüntü ve görüntülerin, anlamlı bölgelerinin kopyalanıp, aynı görüntü içerisinde farklı bir bölgeye yapıştırılarak sahte halleri üretilmiştir. Sahte görüntülerin oluşturulmasında çevrimiçi ve

ücretsiz erişimli GIMP (GNU Image Manipulation Program) yazılımı kullanılmıştır. Ataksız görüntülere ek olarak, verisetinde yer alacak ataklı sahte görüntülerin üretimini gerçekleştirebilecek açık kaynak kodlu bir yazılım geliştirilmiştir. Geliştirilen yazılım ile sahte görüntüde yer alan hedef ve kaynak bölgesine ait konum bilgilerinin çıkarılması sağlanarak, kopyalanan bölgenin, ölçeklenerek veya döndürülerek yapıştırılması ile geometrik dönüşüm atakları uygulanabilmektedir. Ayrıca ilgili yazılım ile sahte görüntünün bulanıklaştırma veya JPEG sıkıştırma atağı uygulayabilme imkânı da sağlanmıştır.

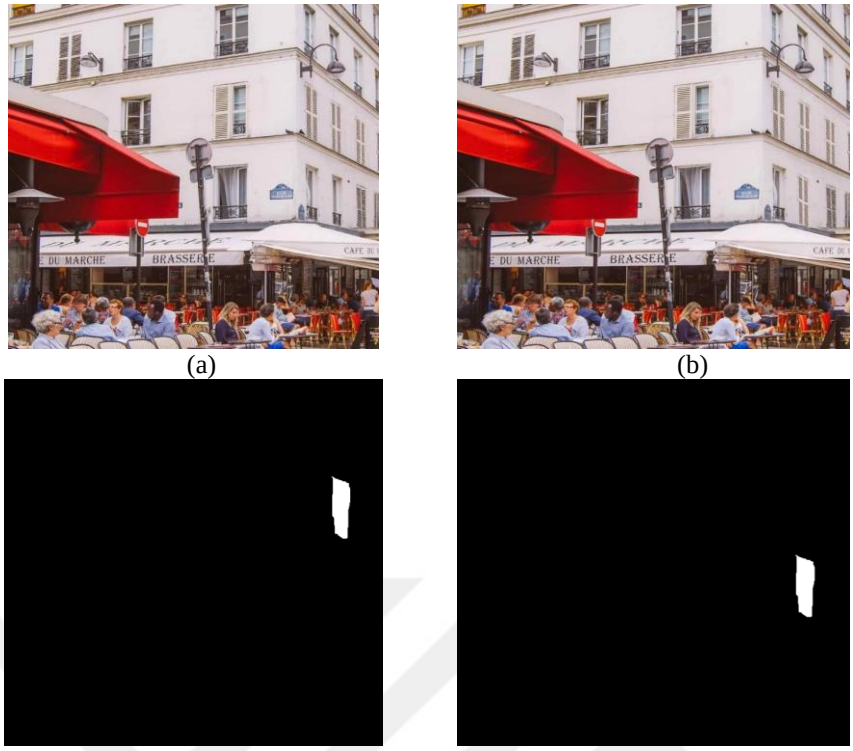
Veriseti oluşturulurken literatürde tespiti zor olan sahtecilik durumları da değerlendirmeye alınarak tespiti zor sahte görüntüler oluşturulmuştur. Bunlardan,

(i) görüntünün doğasında benzer örüntüleri içeren bölgelerin yer aldığı mimari görüntüler üzerinde yapılan sahteciliklere,

(ii) düşük kontrasta sahip bölgelerle yapılan sahteciliklere,

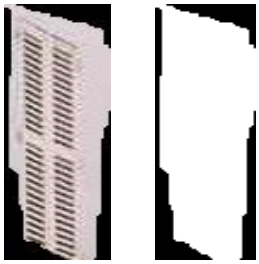
(iii) küçük boyutlu bölgelerin çoğaltılması ile gerçekleştirilen sahteciliklere yer verilmiştir.

Şekil 3.3'te verilen örnekte, (a)'da orijinal görüntü bulunmaktadır. Orijinal görüntüde, binanın ikinci katının sağ cephesinde yer alan ikinci panjurlu pencerenin yer aldığı bölge kopyalanmış, hemen alt katındaki pencereye yapıştırılmıştır. Böylece (b)'de yer alan sahte görüntü oluşturulmuştur. Şekil 3.3 (c) ve (d)' de sırası ile kopyalanan bölge (kaynak) ve yapıştırılan bölge (hedef) yer almaktadır.



Şekil 3.3. (a) Orijinal görüntü (b) Kopyala-yapıştır sahteciliği uygulanmış görüntü (c) Kopyalanan bölge (kaynak) (d)Yapıştırılan bölge(hedef)

Şekil 3. 3, oluşturulan veri tabanında yer alan ataksız bir kopyala-yapıştır sahteciliği örneğidir. Sahte görüntünün dönme ve ölçekleme atağı uygulanmış hallerini de elde edebilmek için geliştirilen yazılım iki aşamadan oluşmaktadır. Öncelikle oluşturulacak sahte görüntü için kopyalanan (kaynak) ve yapıştırılan bölgeye (hedef) ait konum bilgilerin çıkarılması gerçekleştirilmiştir. Böylece her bir görüntü için, her iki bölgenin en sol üst köşesinde yer alan pikselin konum bilgisi [*kaynak_x kaynak_y hedef_x hedef_y]* kaydedilmektedir. Ayrıca sahte bölge ve sahtecilik işlemine maskenin üretilmesi için, sahte bölgenin alfa kanalı da kaydedilmektedir. Şekil 3.4'te, Şekil 3.3'te yer alan örnekteki kopyalanan sahte bölge ve maskesi gösterilmiştir. Veri setinde yer alan 80 görüntü için, bahsedilen işlemin bir defa gerçekleştirilmesi yeterli olmuştur.



(a) (b)

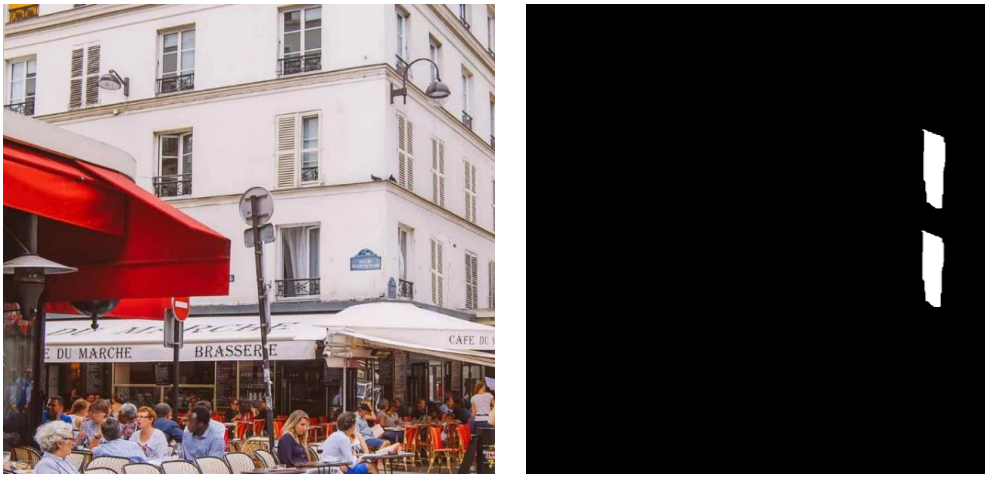
Şekil 3.4. (a)Sahte bölge (b) Sahte bölge maskesi (alfa kanalı)

İkinci aşamada, ilk aşamada elde edilen hedef ve kaynak bölgesinin konumları, alfa kanalı ve görüntünün orijinal hali kullanılarak ataklı sahte görüntüler ve bu görüntülere ait maskeler otomatik ve hızlı bir şekilde oluşturulmaktadır. İstenen atak türüne göre, sahte bölge ve maskesi, istenen derecede döndürülerek veya istenen oranda ölçeklenerek hedef bölgenin piksel değerlerinin güncellenmesi gerçekleştirilmektedir. Tablo 3.2'te oluşturulan verisetinde yer alan atak türleri ve kullanılan parametreler yer almaktadır.

Tablo 3.2. Oluşturulan veri setinde uygulanan atak durumlarına ilişkin parametreler

Atak çeşidi	**Parametreleri**	**Toplam görüntü sayısı**
Dönme	2°, 4°, 6°, 8°, 10°, 20°, 75°, 180°	8x80=640
Ölçekleme	%50, 80, 93, 97, 120, 200	6x80=480

Şekil 3.5'te ölçekleme oranı değerinin 0.97 olması istendiği durumdaki sahte görüntü ve sahtecilik maskesi sırası ile verilmiştir. Şekil 3.6'da ise bir dönme atağı örneği mevcut olup, dönme açısının 20 derece olması istendiği durumda elde edilen sahte görüntü ve sahtecilik maskesi sırası ile verilmiştir.



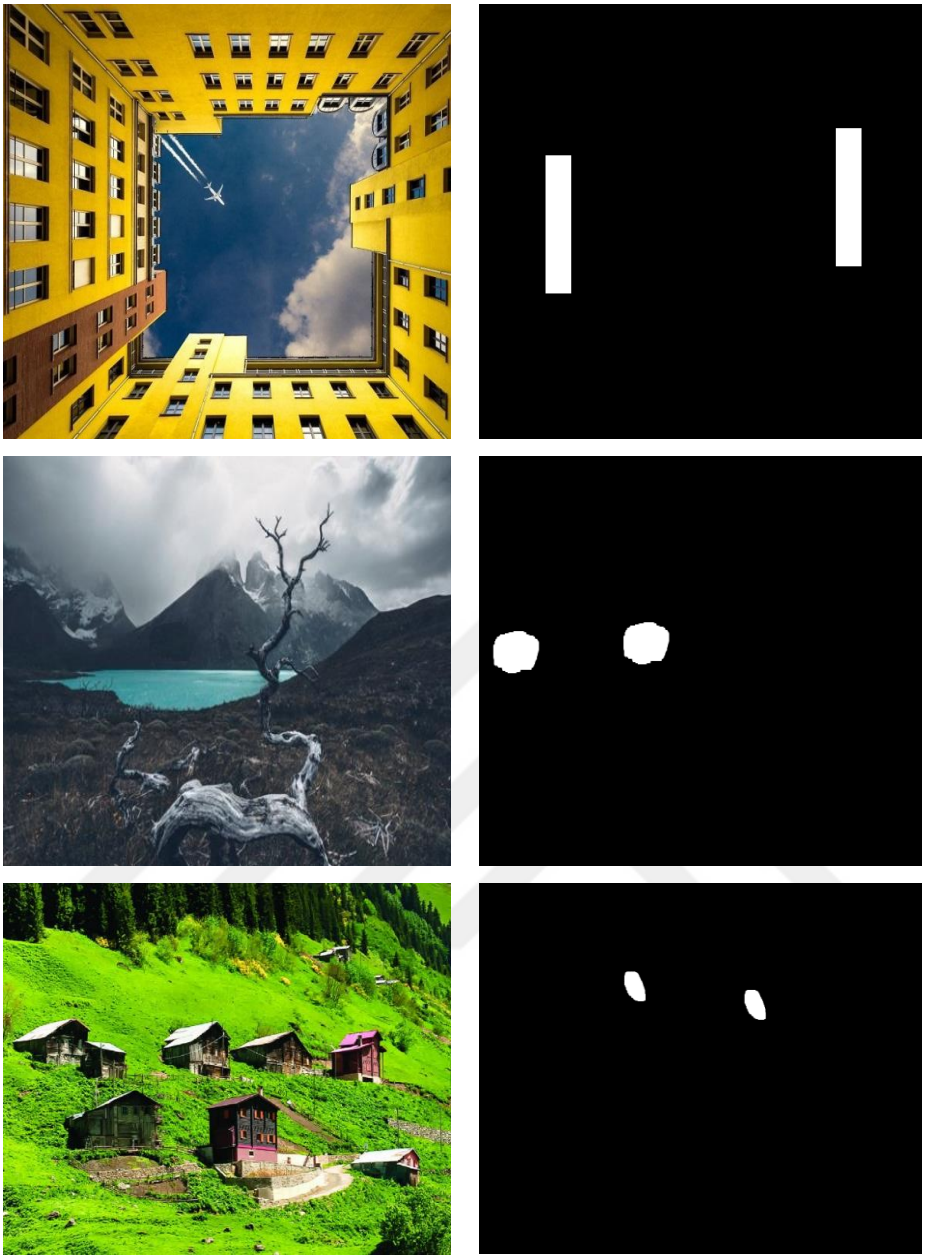
(a) (b)

Şekil 3.5. (a) 0,97 oranında ölçekleme atağı uygulanmış sahte görüntü (b)Sahtecilik maskesi

(a) (b)

Şekil 3.6. (a)20 derece dönme atağı uygulanmış sahte görüntü (b)Sahtecilik maskesi

Şekil 3.7'te, oluşturulan verisetinde, yukarıda bahsedilen durumlara örnek olan sahte görüntüler ve sahtecilik maskeleri sırası ile verilmiştir.



Şekil 3.7. Oluşturulan verisetinde tespiti zor olan sahte görüntüler ve sahtecilik maskeleri

3.2. Kullanılan Performans Değerlendirme Ölçütleri

Performans değerlendirmesinde hem görüntü seviyesinde hem de piksel seviyesinde başarı ölçülmüştür. Görüntü seviyesindeki değerlendirmede, bir görüntünün sahte olup olmadığının doğru bir şekilde yapılıp yapılamadığı ele alınır. Piksel seviyesindeki değerlendirmede ise görüntüdeki her bir pikselin sahte/orijinal etiketlenmesinin performansı değerlendirilir. Bu değerlendirmeler için Kesinlik (Precision), Recall (Duyarlılık) ve F-measure (F-ölçütü) metrikleri kullanılmıştır. Eşitlik (3.1)'de bu ölçütlerin hesaplanması verilmektedir.

$$\text{Kesinlik} = \frac{D_P}{D_P+Y_P}, \text{Duyarlılık} = \frac{D_P}{D_P+Y_N}, \quad \text{F} - \text{ölçütü} = 2x\frac{\text{Kesinlik.Duyarlılık}}{\text{Kesinlik} + \text{Duyarlılık}} \qquad (3.1)$$

Burada D_P, Y_P ve Y_N olarak gösterilen kısaltmaların anlamları Tablo 3.3'te verilmiştir. Hem piksel seviyesindeki hem de piksel seviyesindeki değerlendirmeler için kullanılan metriklerin hesaplanmasında kullanılan bu kısaltmaların anlamları tabloda ayrı ayrı yer almaktadır.

Tablo 3.3. Eşitlik (3.1)'deki kısaltmaların anlamları

Metrik	Piksel seviyesinde	Görüntü seviyesinde
D_P	Doğru bir şekilde tespit edilen sahte piksellerin sayısı	Doğru bir şekilde tespit edilen sahte görüntülerin sayısı
Y_P	Orijinal olduğu halde yanlışlıkla sahte olarak etiketlenen piksel sayısı	Orijinal olduğu halde yanlışlıkla sahte olarak etiketlenen görüntü sayısı
Y_N	Sahte olup tespiti yapılamayan piksel sayısı	Sahte olup tespiti yapılamayan görüntü sayısı

Literatürde bu veriseti kullanılarak verilen sonuçlarda DPO (TPR, Duyarlılık), YPO ve Doğruluk (Accuracy) metrikleri kullanılmıştır. Yapılan çalışmada da literatürden toplanan verilerin sonuç karşılaştırmasında kullanılabilmesi için yine aynı metrikler kullanılarak önerilen yöntemin performans sonuçları elde edilmiştir. Eşitlik (3.2)'de bu metriklerin nasıl elde edildiği verilmiştir. DPO ve Doğruluk metriği sonucunun 1'e; YPO

metriği sonucunun 0'a yaklaşması yüksek sahtecilik tespiti performansını temsil etmektedir. Buna göre performans değerlendirmesi yapılmıştır.

$$\text{DPO} = \frac{\text{D}_\text{P}}{\text{D}+\text{Y}_\text{N}}, \text{YPO} = \frac{\text{Y}_\text{P}}{\text{Y}_\text{P}+\text{D}_\text{N}}, \text{Doğruluk } = \frac{\text{DPO}+\text{DYO}}{2}, \text{DYO} = 1 - \text{YPO} \quad (3.2)$$

Burada, $\text{D}_\text{P}, \text{Y}_\text{N}, \text{Y}_\text{P}$ gösterimlerinin piksel seviyesindeki değerlendirme için ifade ettiği anlamlar Tablo 3.4'te verilmişti, D_N ifadesi ise orijinal olup orijinal olarak işaretlenen piksellerin sayısını temsil etmektedir.

3.3. L*a*b ve RGB Renk Uzaylarında Faydalanarak Anahtar Noktası Tabanlı Şüpheli Bölgelerin Çıkarılması ve Dinamik Bir Lokalizasyon Yaklaşımı ile Sahtecilik Tespitinin Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Bu bölümde tez kapsamında önerilen ilk yöntemin literatürde yer alan popüler çalışmalar ile karşılaştırmalı performans değerlendirmesi yapılmıştır. Deneyler 3.4-GHz Intel Core i7 CPU ve 16 GB RAM hafızaya sahip masaüstü bilgisayarda, Matlab R2018b platformunda gerçekleştirilmiştir. Performans analizlerine ilişkin detaylar veri setlerine göre iki alt bölümde verilmiştir.

3.3.1. GRIP Verisetinde Elde Edilen Deneysel Sonuçlar

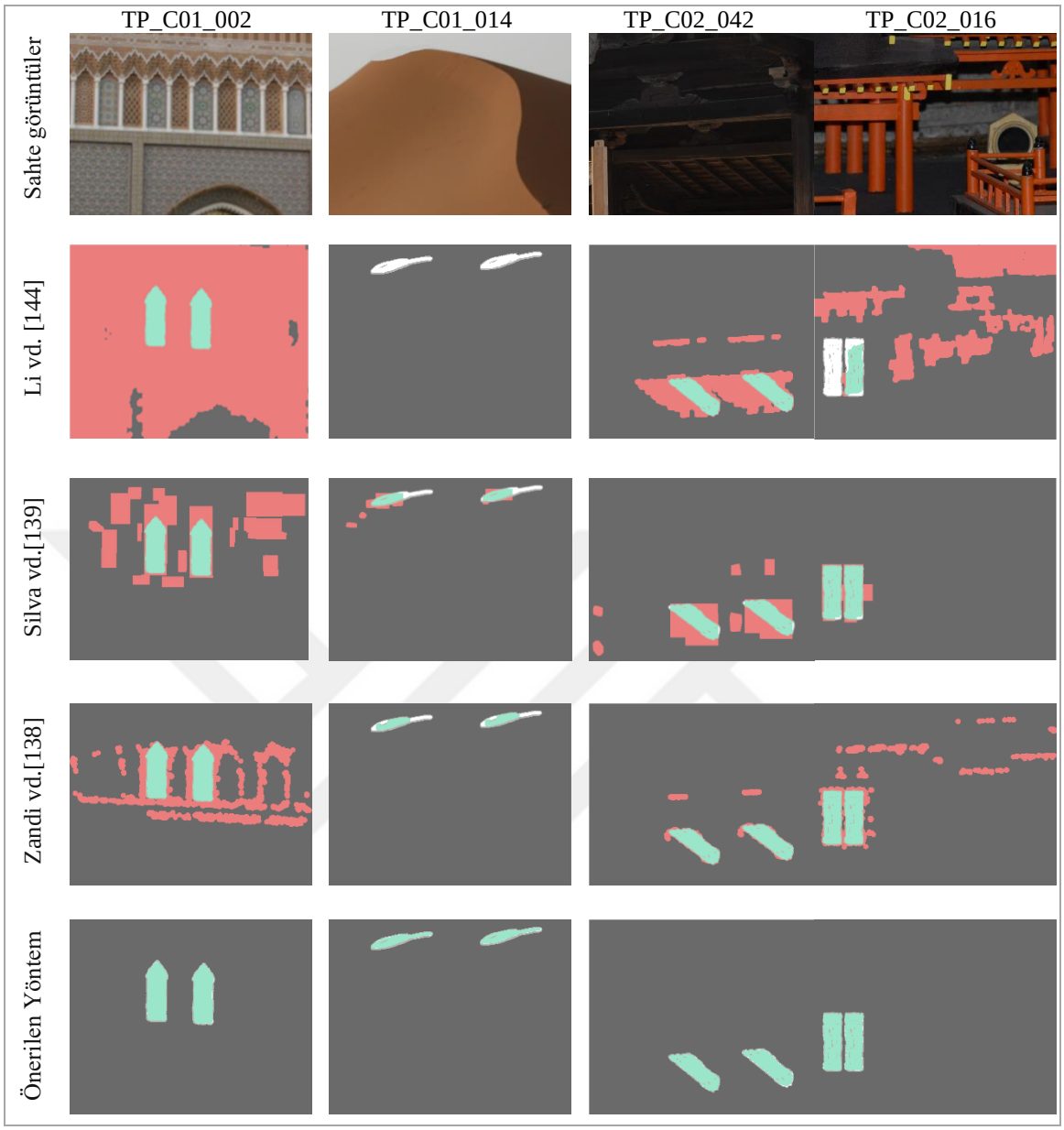
Önerilen yöntemin ilk değerlendirmesinde GRIP verisetinde yer alan görüntüler kullanıldı. Bu veriseti üzerinde literatürde yer alan popüler kopyala-yapıştır sahteciliği tespiti yöntemlerinin sonuçlarının karşılaştırması yapıldı, Referans çalışmalardan Bravo ve Nandi [23], Ryu vd. [40], Christlein vd. [89], Zandi vd. [138], Silva vd. [139], Li vd. [144], Pun vd. [147] tarafından önerilen yöntemlerle yapılan karşılaştırmalara yer verilmiştir.

İlk olarak önerilen yöntem ile referans çalışmalardan yazarların tarafımızca kod paylaşımında bulunmaları sebebi ile bazı referans çalışmalardan elde edinilen görsel sonuçlar sunulacaktır. Görsel sonuçlarda sunulmak üzere belirlenen örnek sahte görüntüler tespit edilebilmesi zor olan görüntülerden seçilmiştir. Görsel sonuçlarda;

- Yeşil pikseller sahte piksellerin sahte olarak etiketlendiği pikselleri,
- Kırmızı pikseller orijinal piksellerin sahte olarak etiketlendiği pikselleri,
- Beyaz pikseller sahte piksellerin, doğru olarak etiketlendiği pikselleri temsil etmektedir.

Şekil 3.8'de GRIP veri setinde sahtecilik tespiti zor olarak nitelendirilebilecek örnek sahte görüntülerden elde edilen görsel sonuçlar verilmiştir. Referans çalışmalardan Li vd. [144], Silva vd. [40] ve Zandi vd. [138] tarafından önerilen yöntemlerin ilgili yazarlar tarafından açık kaynak kodları paylaşılmıştır. Bu sayede bu yöntemlerin kullanılması ile her bir görüntüde ayrı ayrı görsel sonuçlar elde edilebilmiştir.

Sahte görüntülerden ilki olan, GRIP verisetinde TP_C01_002 olarak isimlendirilmiş görüntü, mimari örüntüleri içeren, birbirine benzer özellik barındıran görüntü bölgelerini içermektedir. Bu tarz bir görüntüde benzer görüntü bölgelerinin çok olması sebebi ile orijinal olduğu halde sahte olarak işaretlenebilecek piksellerin fazla olması olasıdır. Referans çalışmalardan Li vd. [144] tarafından önerilen yöntemde görüntünün neredeyse bütününün sahte olarak işaretlendiği, hatalı işaretlemelerin fazlaca olduğu görülmektedir. Silva vd. [139] ve Zandi vd. [138] tarafından önerilen yöntemlerde de yine orijinal olduğu halde sahte olarak işaretlenen piksellerin varlığı söz konusudur. TP_C01_014 olarak isimlendirilen ikinci sahte görüntü ise oldukça düşük kontrasta sahip düz bölgelerle oluşturulmuş bir sahte görüntüdür. Li vd. [144] bölüt tabanlı bir yöntem olmasına karşın temelde anahtar noktalarının eşleşmeleri üzerine kuruludur. Bu tarz görüntülerde anahtar noktası tabanlı yöntemlerin başarısız olduğu bilgisi literatürde yer almakla birlikte örnek sahte görüntüde de yöntemin başarısızlığı görülmüştür. Silva vd. [139] tarafından önerilen yöntem ile ilk görüntüdeki sonuca nispeten daha az olsa da hatalı işaretlemelerin varlığı görülmektedir. Zandi vd. [138] tarafından önerilen yöntemde anahtar noktası tabanlı yöntemlerin düz bölgelerle gerçekleştirilen sahteciliklerin üstesinden gelinmek için önerilen anahtar nokta çıkarma yaklaşımı bu sahte görüntüde görüntünün sahte olduğunu tespit etse de dar bölgelerdeki işaretlemede yetersiz kalmıştır. Önerilen yöntem ile sahte bölgelerin daha doğru işaretlendiği görülmektedir. TP_C02_016 isimli son görüntüde de yine orijinal olduğu halde birbirine benzer görüntü bölgelerini yoğun bir şekilde içermektedir. Bu yüzden referans yöntemlerde hatalı işaretlemelerde yoğunluk oluştuğu görülmüştür. Ancak görüntüdeki benzer bölgelerin varlığına rağmen önerilen yöntem ile hem sahte bölgenin daha doğru işaretlendiği hem de hatalı işaretlemelerin arındırıldığı bir sonuç görüntüsü üretilmiştir. Önerilen yöntem ile, ekstra atak uygulanmasa da tespiti zor olan bu dört sahte görüntü için de minimum sayıda hatalı işaretleme ile sahte bölgelerin doğru bir şekilde tespit edilebildiği görülmektedir.



Şekil 3.8. Ataksız görüntülerde elde edilen görsel sonuçlar

Önerilen yöntem ile referans yöntemlerin, sahte görüntünün ekstra bir atağa maruz kalmaması durumunda, gösterdiği performanslara ilişkin yapılan analizlerde veri setinde yer alan 80 adet ataksız görüntü kullanılarak hem görüntü seviyesinde hem de piksel seviyesinde bir değerlendirme yapılmıştır. Görüntü seviyesindeki analizler, yöntemlerin test görüntüsünü sahte/orijinal olarak etiketleme performansı üzerine gerçekleştirilirken, piksel seviyesindeki analizler test görüntüsünde yer alan piksellerin doğru bir şekilde etiketlenebilmesi üzerine gerçekleştirilmektedir. Tablo 3.4'te yöntemlerin GRIP verisetindeki 80 adet ataksız görüntünün ve bunlara ait sahtecilik maskesinin kullanılması

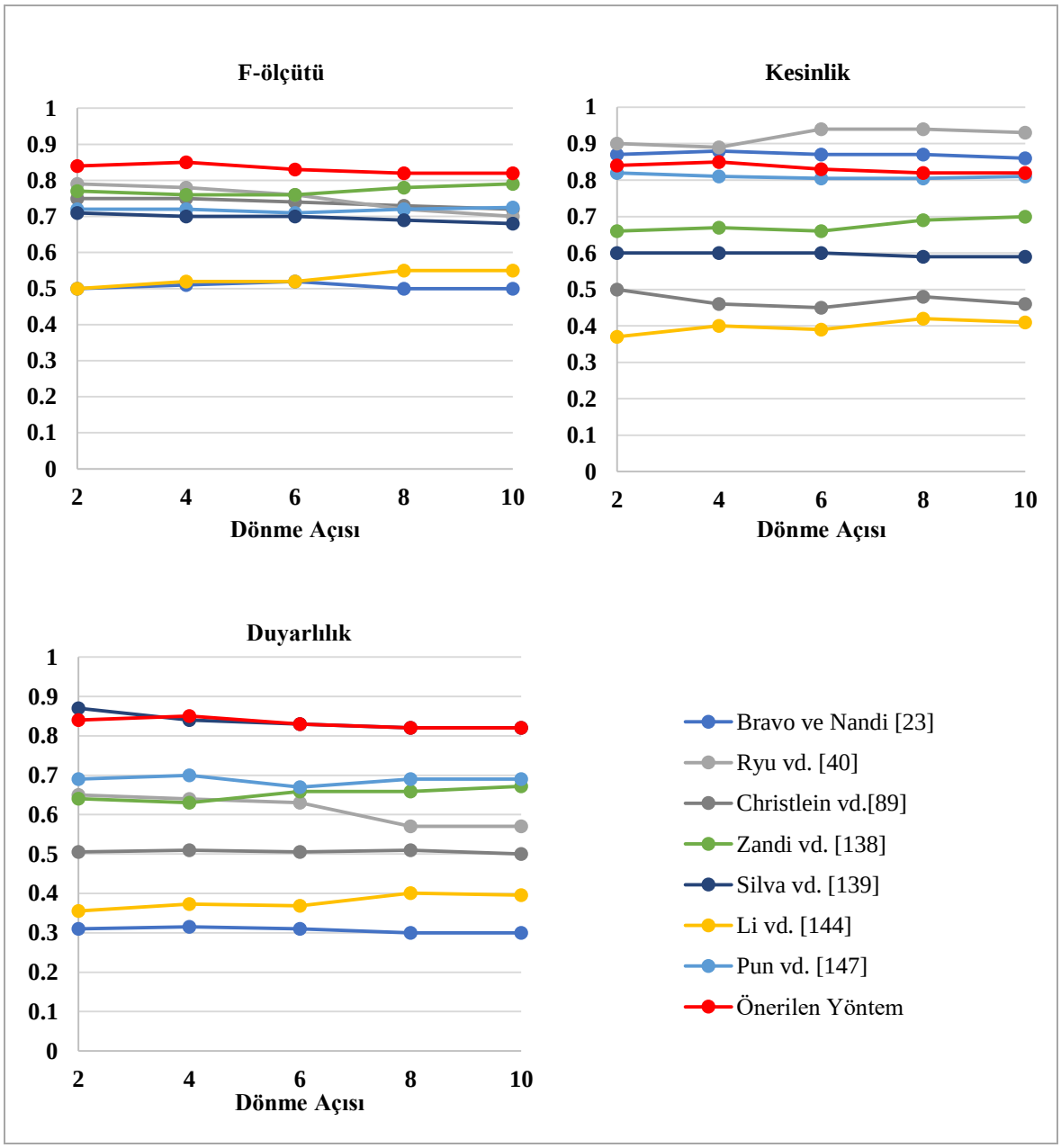
ile elde edilen ortalama F-ölçütü metrik sonuçları verilmiştir. Önerilen yöntem ile hem piksel seviyesinde hem de görüntü seviyesinde referans çalışmalara göre üstünlük elde edildiği görülmektedir.

Tablo 3.4. Ataksız kopyala-yapıştır sahteciliği durumunda, görüntü ve piksel seviyesindeki değerlendirmelere göre ortalama F-ölçütü değerleri

Yöntemler	**Görüntü seviyesi**	**Piksel seviyesi**
Bravo ve Nandi [23]	0,95	0,84
Ryu vd. [40]	0,94	0,89
Cozzolino vd. [42]	0,94	0,91
Silva vd. [139]	0,83	0,66
Amerini vd. [110]	0,67	0,44
Li vd. [144]	0,72	0,52
Pun vd. [147]	0,95	0,78
Zandi vd. [138]	0,86	0,85
Önerilen yöntem	0,97	0,94

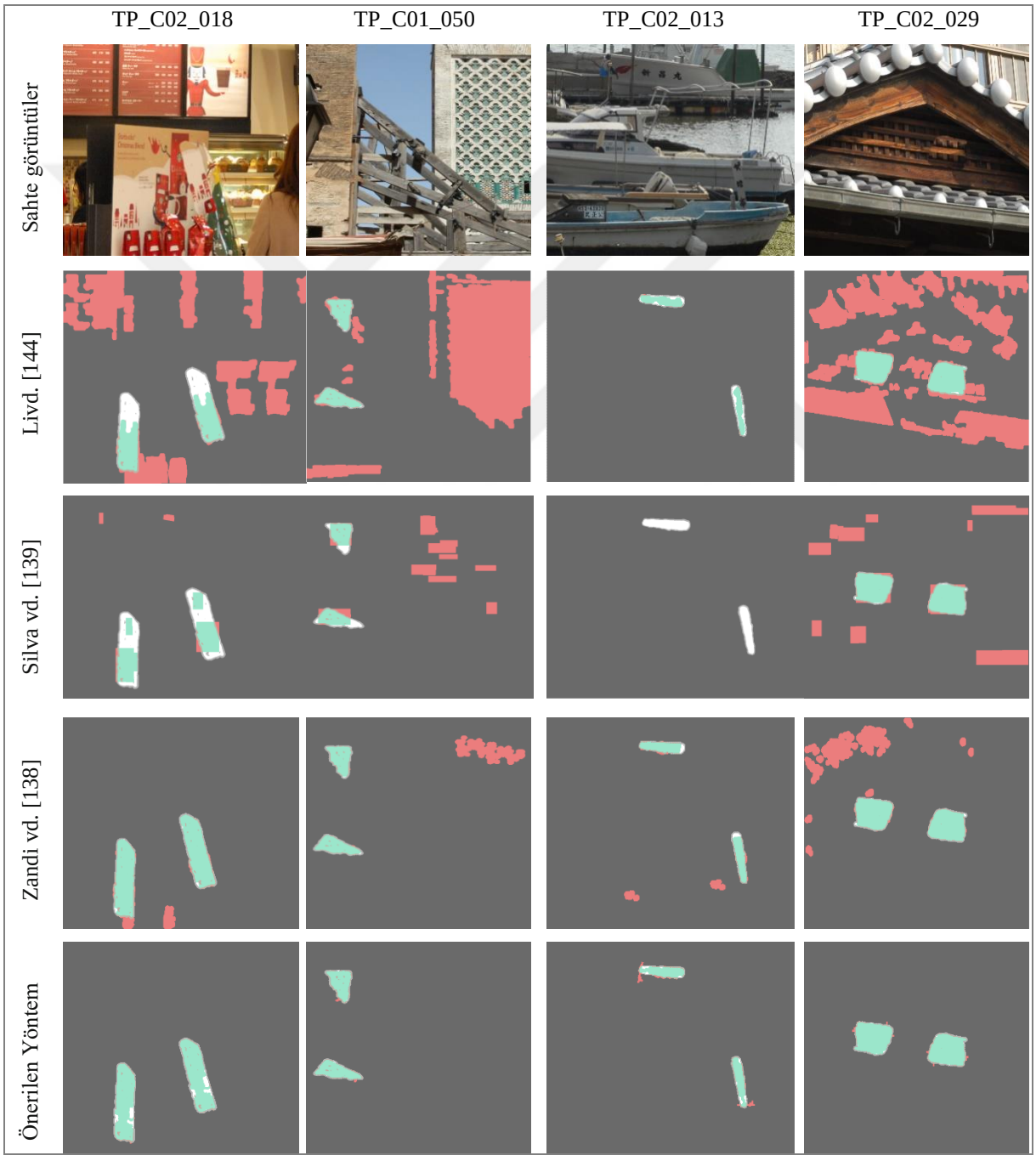
Gerçekleştirilen deneylerin ikinci aşamasında görüntüye dönme atağının uygulanması durumundaki performansları değerlendirildi. Bunun için öncelikle verisetinde yer alan 2°-10° arasında 2'şerli artan açı dereceleri ile dönme atağı uygulanmış sahte görüntüler kullanıldı. Her bir atak durumunun verisetindeki 80 görüntünün hepsine uygulanmış toplamda 400 görüntü kullanıldı. Bu deneye ilişkin elde edilen ortalama Duyarlılık, Kesinlik ve bunların harmonik ortalaması olan F-ölçütü metrikleri ile elde edilen sonuçlar grafiksel olarak Şekil 3.9'da sunulmuştur. Bravo ve Nandi [23] tarafından önerilen yöntem blok tabanlı bir yöntem olması sebebi ile dönme atağına karşı dayanıklılığa sahip değildir. Bu sebeple en düşük ortalama F-ölçütü sonucu bu yöntem ile elde edilmiştir. Li vd. [144] tarafından önerilen yöntem temelde anahtar noktalarından faydalandığı için dönme atağına karşı dayanıklı olsa da GRIP verisetindeki düz bölgelerle gerçekleştirilen sahte görüntülerdeki doğrulamada yeterli başarıyı sağlayamamıştır. Christlein vd. [89] tarafından yöntemde yine bir anahtar noktası tabanlı yöntemdir. Bir önceki yöntemde bahsedilen sebeple verisetinde yer alan görüntülerin ortalaması alındığı durumda düşük ortalama sonuca sahip olduğu söylenebilir. Bravo ve Nandi [23] ve Ryu vd. [40] tarafından önerilen

yöntemlerin de önerilen yöntemlere göre daha yüksek ortalama Kesinlik değeri, daha düşük ortalama Duyarlılık değerine sahip olmasının sebebi, bu yöntemlerin sahte bölgeleri işaretlemede başarılı olmasına karşın yüksek oranda hatalı işaretlemelere sahip olmasıdır. Dönme atağı durumunda, Kesinlik ve Duyarlılık metriklerinin harmonik ortalaması olan F-ölçütü metriği ile elde edilen ortalama sonuçlardan en yüksek sonucu üreten önerilen yöntem olmuştur.



Şekil 3.9. Dönme atağı durumunda elde edilen ortalama sonuçların grafiksel gösterimi

Şekil 3.10'da ise yukarıdan aşağıya doğru sırasıyla 20°, 60°, 105°, 180° derece ile daha büyük açılarla dönme atağı uygulanmış bazı örnek sahte görüntüler üzerinden elde edilen görsel sonuçlar sunulmuştur. Bu sahte görüntülerde benzer örüntü içeren görüntü bölgelerinin oldukça fazla olduğu görülmektedir. Önerilen yöntem ile büyük derece dönme atağı durumunda daha az hatalı işaretleme ve daha yüksek doğru işaretlemelerin gerçekleştirilebildiği, örnek görsel sonuçlarda görülmektedir.



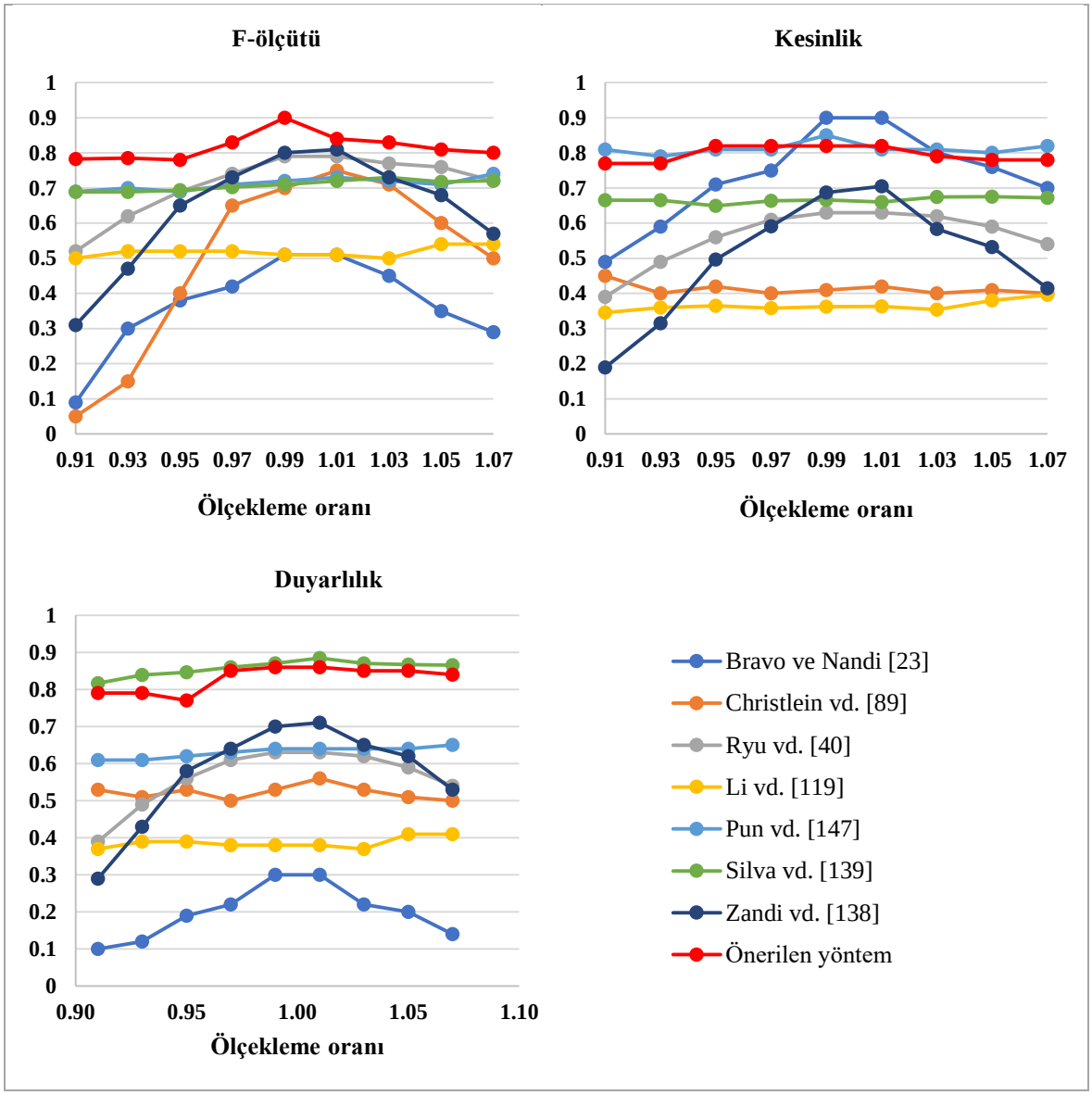
Şekil 3.10. Dönme atağına maruz kalmış sahte görüntülerden elde edilen görsel sonuçlar

Verisetinde yer alan her biri $30^{\circ}, 60^{\circ}, 90^{\circ}$ ve 180° derecelerle dönme atağı uygulanmış 80x4=320 adet sahte görüntü üzerinden F-ölçütü metriği kullanılarak elde edilen ortalama sonuçlar Tablo 3.5'te verilmiştir. Önerilen yöntemin dört açı durumunda da daha yüksek ortalama sonuca sahip olduğu görülmektedir.

Tablo 3.5. Büyük derece dönme atağı uygulanmış görüntüler üzerinde F-ölçütü metriği ile elde edilen ortalama sonuçlar

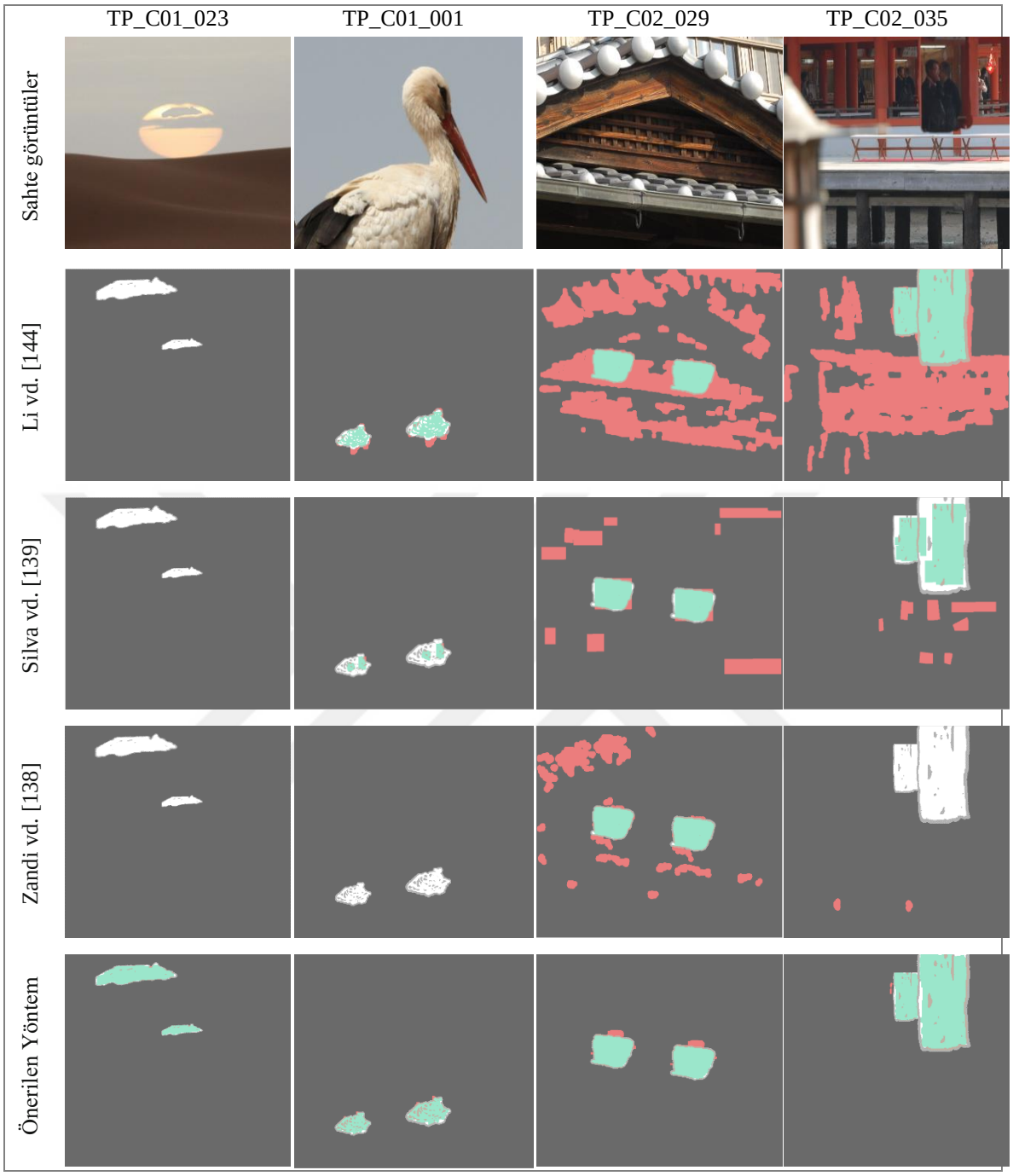
Yöntemler	**30°**	**60°**	**90°**	**180°**
Bravo ve Nandi [23]	0,48	0,48	0,59	0,59
Christlein vd. [89]	0,56	0,56	0,56	0,56
Li vd. [144]	0,55	0,55	0,55	0,55
Zandi vd. [138]	0,78	0,78	0,78	0,78
Önerilen yöntem	**0,85**	**0,83**	**0,80**	**0,87**

Bir sonraki deneysel analiz, GRIP veriseti üzerinde önerilen yöntemin referans yöntemlere göre ölçekleme atağındaki performansı üzerine yapıldı. Gerçekleştirilen deneyler sırasında %0.91-%1.07 oranları arasında %0.02 aralıklarla ölçeklendirilmiş toplam 800 adet sahte görüntü kullanıldı. Her bir ölçekleme durumunda elde edilen ortalama Kesinlik, Duyarlılık ve F-ölçütü sonuçlarının grafiksel gösterimi Şekil 3.11'de sunulmuştur. Bravo ve Nandi [23] tarafından önerilen yöntem blok tabanlı olması sebebi ile ölçekleme atağında da düşük performans sergilemiştir. Diğer yöntemlerden Zandi vd. [138] tarafından önerilen yöntemde ise ölçekleme oranı arttıkça yöntemin performansındaki düşüklük grafiklerden görülmektedir. Önerilen yöntemin bu atak türünde de performans üstünlüğü görülmektedir.



Şekil 3.11. Ölçekleme atağı durumunda elde edilen ortalama sonuçların grafiksel gösterimi

Şekil 3.12'de ise gerçekleştirilen ölçekleme atağı durumundaki analizlerin örnek görsel sonuçlarına yer verilmiştir. Görsel sonuçlarda yer alan görüntülerde sırası ile (%)0.5, 0.8, 1.03, ve 2 oranlarında ölçekleme atağı vardır. İlk görüntünün düz bölgelerle gerçekleştirilmiş bir görüntü olmasının yanı sıra literatüre göre büyük oranda ölçekleme atağı uygulanmış görüntü olduğu söylenebilir. Bu iki zorlu koşulu barındıran bu görüntü için referans yöntemlerin hiçbiri sahtecilik tespitinde bulunamamıştır. Önerilen yöntem ile sahte bölgenin işaretlemesi başarılı bir şekilde gerçekleştirilmiştir. 0.8 oranında ölçekleme atağı uygulanan ikinci görüntü için de anahtar noktası tabanlı olmasına karşın Zandi vd. [138] tarafından önerilen yöntemin başarısız olduğu görülmektedir.



Şekil 3.12. Ölçekleme atağına maruz kalmış sahte görüntülerden elde edilen görsel sonuçlar

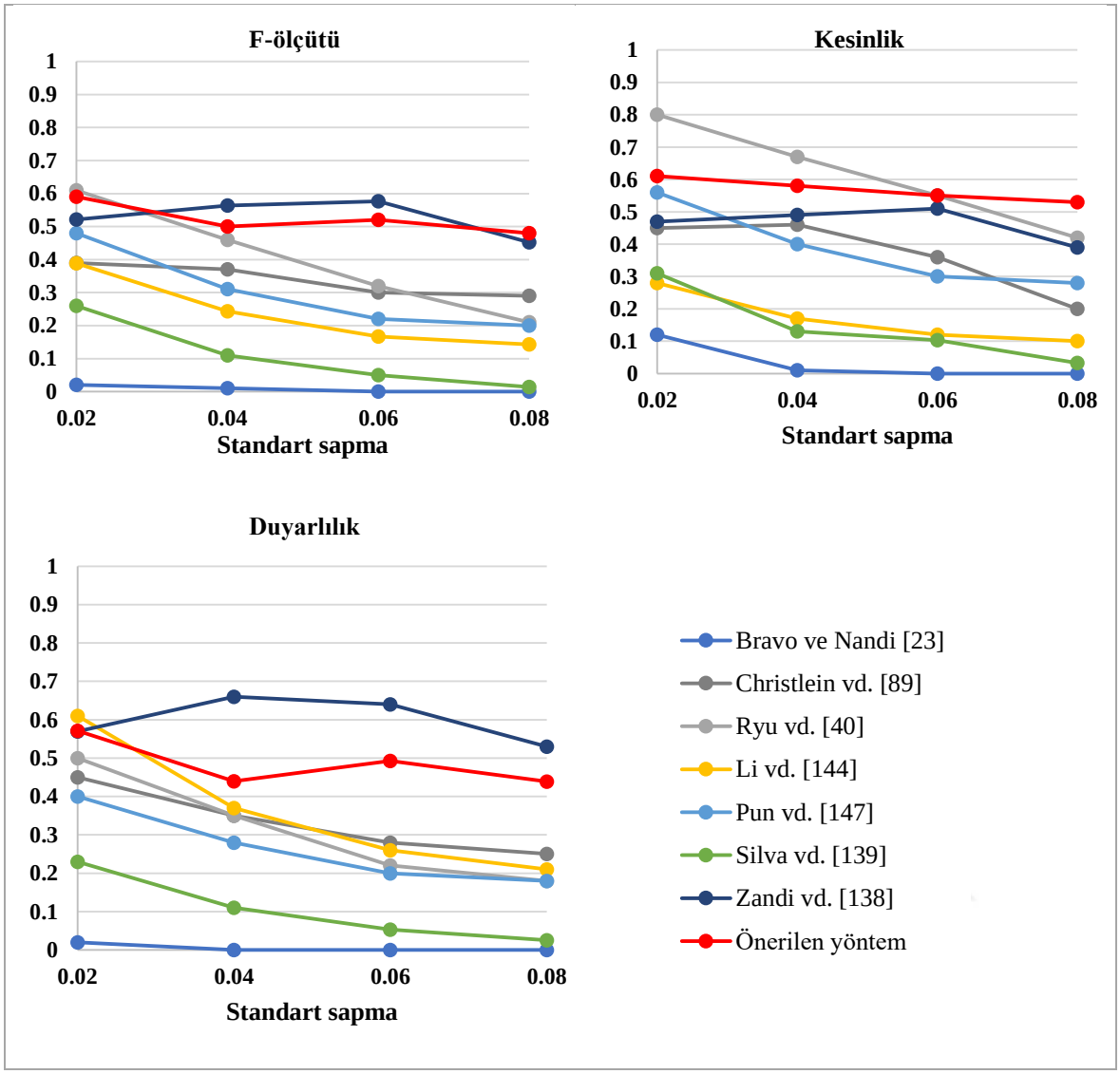
Büyük oranda ölçekleme atağı durumunda daha detaylı yapılan analizde hem görüntü seviyesinde hem de piksel seviyesinde performans değerlendirmesi gerçekleştirilmiştir. Verisetinde (%) 0.5,0.8, 1.2 ve 2 oranlarla gerçekleştirilen 4x80=400 adet sahte görüntü kullanılarak elde edilen deneylere ilişkin F-ölçütü metriği kullanılarak elde edilen ortalama sonuçlar Tablo 3.6'da verilmiştir. Bu dört durum için de önerilen yöntem ile en yüksek sonuçlar elde edilmiştir.

Tablo 3.6. Büyük oranda ölçekleme atağı uygulanmış görüntüler üzerinde F-ölçütü metriği ile elde edilen

Değerlendirme	**Görüntü seviyesi**				**Piksel seviyesi**			
Ölçekleme oranı (%)	**0,5**	**0,8**	**1,2**	**2**	**0,5**	**0,8**	**1,2**	**2**
Bravo ve Nandi [23]	0	0,35	0,10	0,05	0	0,05	0,05	0
Christlein vd. [89]	0,001	0,001	0	0	0	0	0	0
Li vd. [144]	0,51	0,72	0,74	0,71	0,25	0,48	0,56	0,57
Zandi vd. [138]	0,10	0,20	0,15	0,01	0,01	0,02	0,06	0,009
Önerilen yöntem1	**0,72**	**0,84**	**0,89**	**0,88**	**0,36**	**0,62**	**0,68**	**0,65**

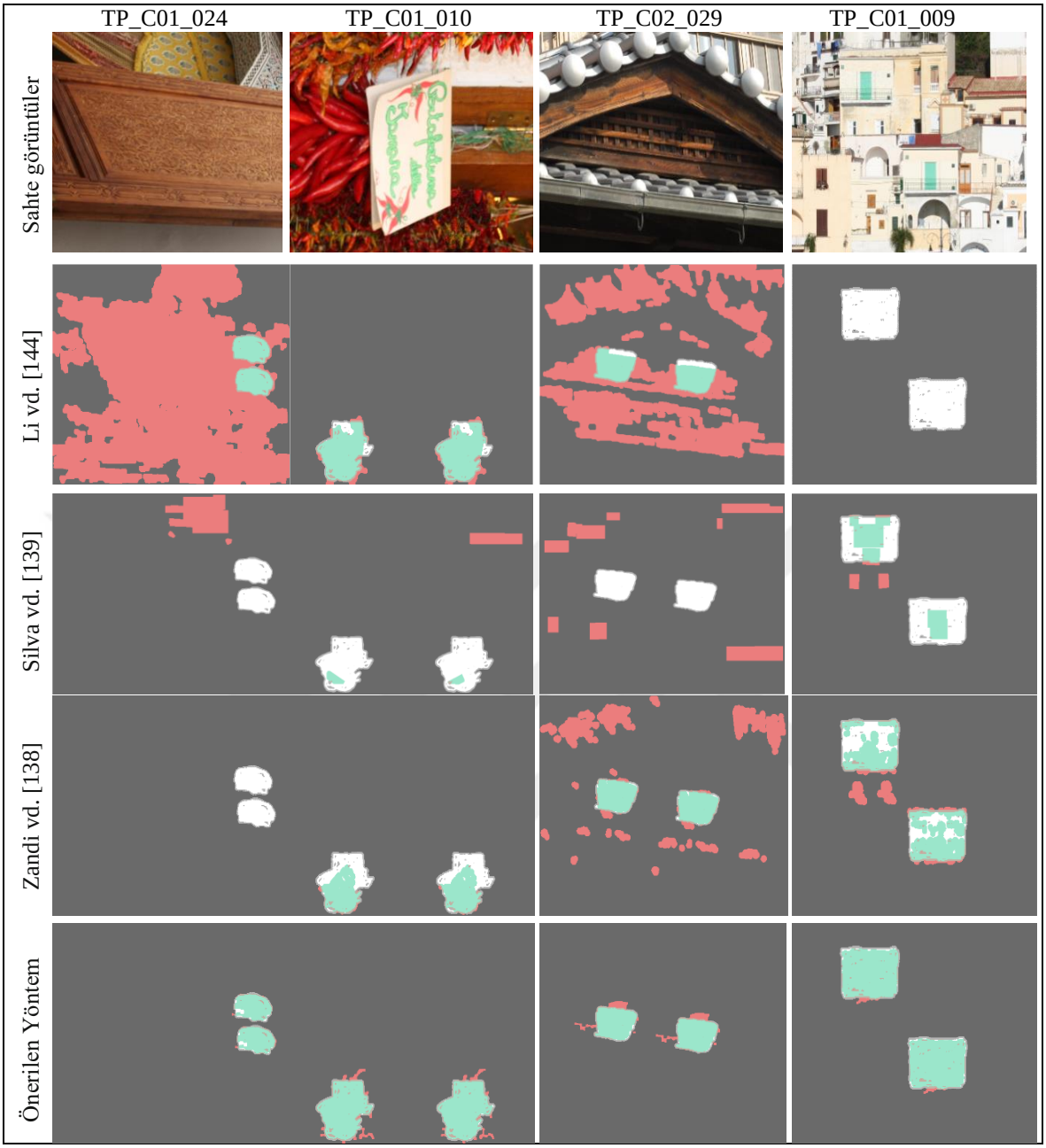
GRIP verisetinde gerçekleştirilen bir sonraki deneysel analizde, yöntemlerin gürültü ekleme atakları durumundaki dayanıklılığı incelenmiştir. Bunun için verisetinde yer alan standart sapma (σ) değerleri 0.02, 0.04, 0.06 ve 0.08 olan sahte görüntüler kullanılmıştır. F-ölçütü metriğine göre yapılan değerlendirmede önerilen yöntem ile Zandi vd. [138] tarafından önerilen yönteme ait sonuçların birbirine oldukça yakın olduğu görülmektedir.

Gürültü ekleme atağına maruz kalan örnek görüntülerden elde edilen sonuçlara Şekil 3.14'te yer verilmiştir. Şekilde yer alan sahte görüntüler sırası ile 0.08, 0.06, 0.04, 0.02 standart sapma değerleri ile gürültü ekleme atağına maruz kalmıştır. Zandi vd. [138] tarafından önerilen yöntem ile ortalama sonuçlarda önerilen yöntem ile oldukça yakın değerler elde edilse de ilk görüntü gibi benzer örüntü içeren görüntü bölgelerinin fazla olduğu görüntülerde bu yöntemin başarısız olduğu görülmektedir. Diğer üç görüntüde de görüldüğü gibi önerilen yöntem ile sahte bölgelerin işaretlemesinde oldukça tatmin edici görsel sonuçlar elde edilmiştir.

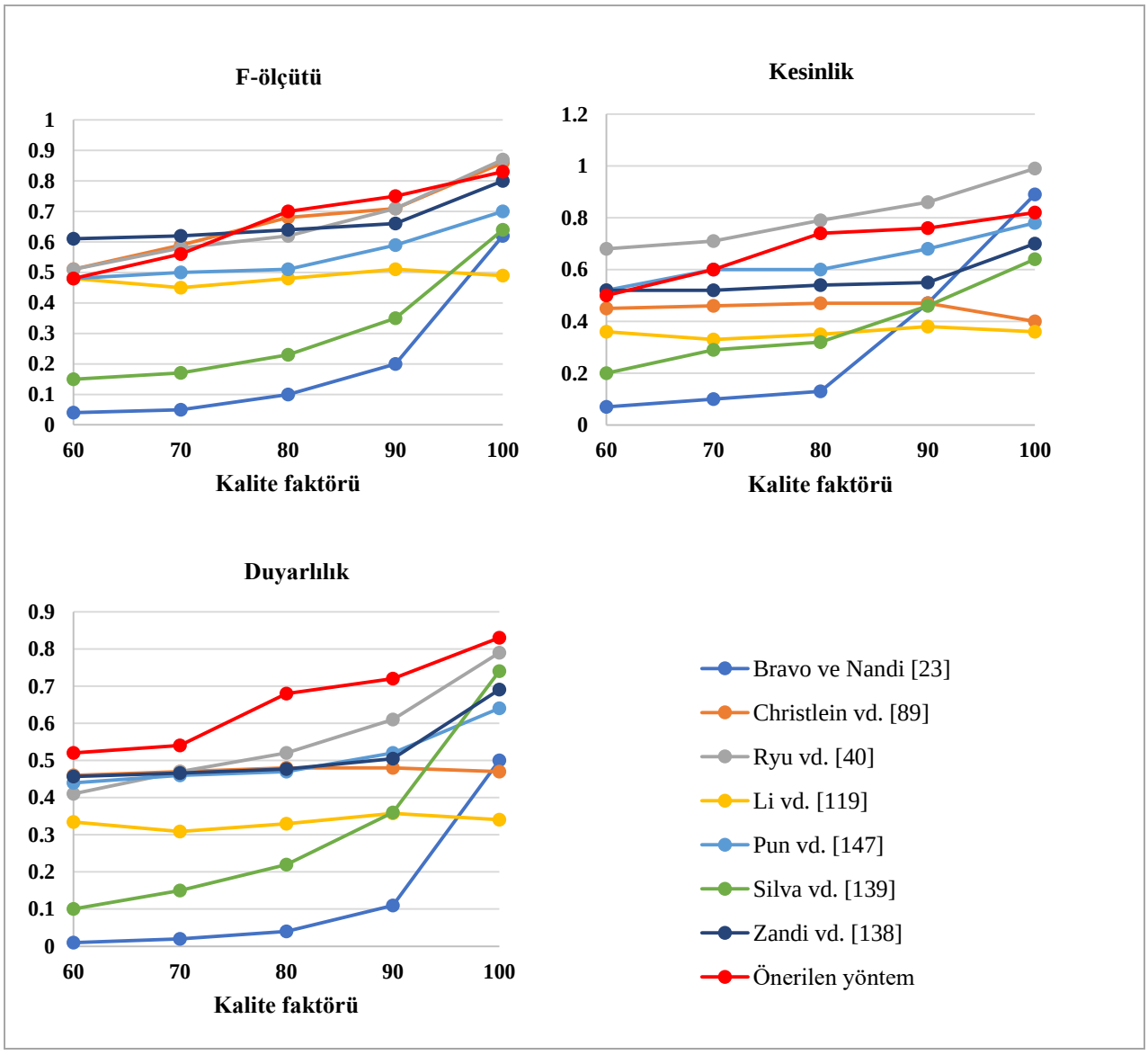


Şekil 3.13. Gürültü ekleme atağı durumunda elde edilen ortalama sonuçların grafiksel gösterimi

GRIP verisetindeki son analizde JPEG sıkıştırma atağına karşı yöntemlerin performans değerlendirmeleri yapılmıştır. Bunun için verisetinde yer alan kalite faktörleri 60,70,80,90 ve 100 olmak üzere kayıplı JPEG sıkıştırma atağına maruz kalmış 80x5=400 adet sahte görüntü kullanılmıştır. Her bir kalite faktörü değeri durumunda uygulanan atağı barındıran görüntülerden elde edilen ortalama F-ölçütü, Kesinlik ve Duyarlılık değerleri grafiksel olarak Şekil 3.14'te gösterilmiştir. Önerilen yöntemin anlatımında sunulduğu üzere anahtar noktalarının a* ve b* kanallarından elde edilmesi durumunda son işlem ataklarına karşı dayanıklılığının düşük olmasından ötürü kalite faktörü 70 ve 60 olması durumunda önerilen yöntemin proformasında düşüşe sebep olmuştur.

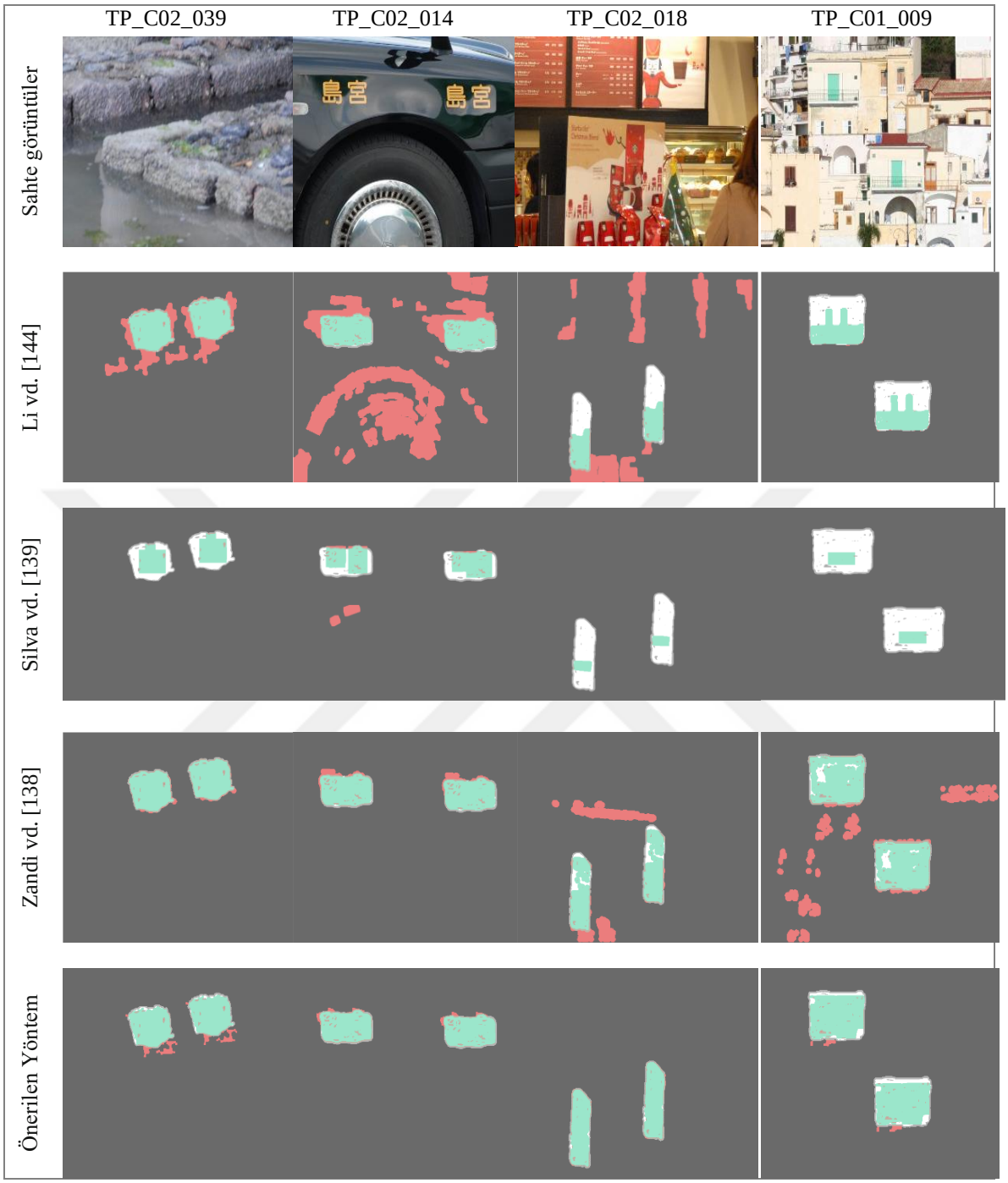


Şekil 3.14. Gürültü ekleme atağına maruz kalmış sahte görüntülerden elde edilen görsel sonuçlar



Şekil 3.15. JPEG sıkıştırma atağı durumunda elde edilen ortalama sonuçların grafiksel gösterimi

Şekil 3.16'da verilen görsel sonuçlar ise soldan sağa aşağı sırasıyla 90, 70, 50 ve 30 kalite faktörü ile JPEG sıkıştırma atağına maruz kalmış görüntüler üzerinden elde edilmiştir. Önerilen yöntem ile hatalı işaretlemelerin daha az görüldüğü sahte bölgelerde yer alan piksellerin belirlenmesinde daha yüksek oranla işaretleme yapıldığı görülmektedir.



Şekil 3.16. JPEG sıkıştırma atağına maruz kalmış sahte görüntülerden elde edilen görsel sonuçlar

3.3.2. CMH Verisetinde Elde Edilen Deneysel Sonuçlar

Bu bölümde literatürde popüler olarak kullanılan kopyala-yapıştır sahteciliği veri setlerinden diğeri olan CMH [139] veriseti üzerinde performans değerlendirmelerine ilişkin sonuçlar sunulacaktır. Bölüm 3.1'de sunulduğu üzere, bu verisetinde, dönme, ölçekleme, dönme ve ölçekleme atakları uygulanmış görüntüler ve bunların JPEG sıkıştırma atağı uygulanmış halleri bulunmaktadır. Bu verisetinde gerçekleştirilen testlere göre ilk olarak rastgele seçilen sahte görüntüler üzerinde önerilen yöntem ile Silva vd. [139] ve Zandi vd. [138] tarafından önerilen yöntemlerden elde edilen görsel sonuçlar sunulacaktır. Şekil 3.17'de örnek sahte görüntüler ve elde edilen görsel sonuçların bir önceki görsel sonuçlarda kullanılan renk kodları ile işaretlenmiş hallerine yer verilmiştir. Örnek sahte görüntüler üzerinde önerilen yöntem ile daha az hatalı işaretleme ve sahte bölgelerin daha doğru işaretlendiği görülmektedir.

Deneysel analizlerin devamında CMH verisetinde yer alan dört alt grupta (CMH1-4) yer alan bütün sahte görüntüler üzerinde gerçekleştirilen performans sonuçları ayrı ayrı sunulacaktır. Literatürde bu veriseti üzerinde gerçekleştirilen deneylerde DPO, YPO ve Doğruluk metrikleri kullanıldığı için yapılan tez çalışmasında da karşılaştırmalı adil bir değerlendirme gerçekleştirebilmek için bu metriklerin kullanımı sağlanmıştır [139,170]. Bu metriklerden DPO ve Doğruluk değerinin sonucunun 1'e yakınlaşması, YPO metriğinin ise 0'a yaklaşması daha yüksek performansı nitelendirmektedir.

İlk olarak CMH1 olarak isimlendirilen grup üzerindeki sonuçlar sunulmuştur. Bu grupta yer alan 23 adet ataksız sahte görüntüden elde edilen ortalama metrik sonuçları Tablo 3.7' de verilmiştir. En iyi durum olarak kabul edilen ataksız görüntüler üzerinde yapılan testlerde literatürdeki çalışmalar önerilen yöntem ile elde edilen sonuçlara oldukça yakın olsa da en yüksek performansın önerilen yöntem ile elde edilebildiği söylenebilir.

Şekil 3.17. CMH verisetinde yer alan örnek sahte görüntüler üzerinde elde edilen görsel sonuçlar

Tablo 3.7. CMH1 grubundaki görüntüler üzerinde ortalama sonuçlar (ataksız görüntüler)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,48	0,0020	0,74
Silva vd. [139]	0,94	0,0017	0,96
Zandi vd. [138]	0,85	0,0174	0,92
Li ve Zhou vd. [119]	0,83	0,0013	0,92
Huang ve Ciou [170]	0,96	0,0231	0,97
Önerilen yöntem	0,97	0,0100	0,98

CMH2 grubunda yer alan dönme atağı uygulanmış görüntülerin kullanımı ile de bu verisetindeki ikinci analiz gerçekleştirilmiştir. Bu analizde 25 adet dönme atağı uygulanmış sahte görüntü kullanılmış ve elde edilen ortalama metrik sonuçları Tablo 3.8'de verilmiştir. Tabloda yer alan referans yöntemlerin hepsi temelde anahtar noktalarından faydalansa da Huang ve Ciou [170] tarafından önerilen yöntem haricindeki yöntemlerden oldukça düşük sonuçlar elde edilmiştir. Önerilen yöntem ile [170]'den elde edilen sonuçlar da birbirine oldukça yakın olup, önerilen yöntemin ortalama 0,98 oranla DPO ve Doğruluk değerine sahip olması yöntemin bu atak durumunda dahi yüksek başarısını ortaya koymaktadır.

Tablo 3.8. CMH2 grubundaki görüntüler üzerinde ortalama sonuçlar (dönme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,47	0,0014	0,73
Silva vd. [139]	0,70	0,0066	0,84
Zandi vd. [138]	0,52	0,0007	0,76
Li ve Zhou vd. [119]	0,60	0,0005	0,80
Huang ve Ciou [170]	0,97	0,0117	0,97
Önerilen yöntem	0,97	0,006	0,98

Ölçekleme atağı uygulanmış sahte görüntüleri barındıran CMH3 grubundaki görüntülerden elde edilen ortalama sonuçlar ise Tablo 3.9'da sunulmuştur. Bu grupta yer alan 25 adet sahte görüntüden elde edilen ortalama DPO, YPO ve Doğruluk metriğine göre önerilen yöntem ile en yüksek başarım elde edilmiştir.

Tablo 3.9. CMH3 grubundaki görüntüler üzerinde ortalama sonuçlar (ölçekleme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,64	0,0124	0,82
Silva vd. [139]	0,48	0,0016	0,74
Zandi vd. [138]	0,21	0,0163	0,60
Li ve Zhou vd. [119]	0,36	0	0,68
Huang ve Ciou [170]	0,86	0,0218	0,92
Önerilen yöntem	0,92	0,02	0,95

CMH4 grubunda yer alan hem dönme hem ölçekleme atağına maruz bırakılan 35 adet sahte görüntünün kullanılması ile gerçekleştirilen deneylerin sonuçları ise Tablo 3.10'da

sunulmuştur. Önerilen yöntemin bu iki atağı birlikte barındıran sahte görüntülerde dahi referans yöntemlere göre üstünlüğü tablodan da görülmektedir.

Tablo 3.10. CMH4 grubundaki görüntüler üzerinde ortalama sonuçlar (hem dönme hem ölçekleme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,56	0,0024	0,78
Silva vd. [139]	0,64	0,0129	0,82
Zandi vd. [138]	0,57	0,0136	0,60
Li ve Zhou vd. [119]	0,44	0,0010	0,72
Huang ve Ciou [170]	0,87	0,02	0,92
Önerilen yöntem	0,90	0,03	0,93

Literatürde CMH verisetinde CMH1-CMH4 grubunda yer alan 108 görüntünün hepsinden elde edilen ortalama sonuçları rapor eden çalışmalar bulunmaktadır [47,54,140,170,172]. Performans karşılaştırmasında bu çalışmalara da yer verebilmek için, dört grupta elde edilen ortalama sonuçlar hesaplanmıştır. Elde edilen ortalama performans metrikleri Tablo 3.11'de verilmiştir. Literatürde CMHALL grubu olarak sonuçları bunulan [42, 47, 54, 108, 110, 119, 139, 139, 147, 169, 170, 171]'de önerilen yöntemler ile önerilen yöntemin sonuçlarının karşılaştırılması yapıldığında, önerilen yöntemin referans alınan on iki yöntemden daha üstün performansa sahip olduğu görülmektedir.

CMH veriseti üzerinde yapılan son değerlendirmede bu verisetinde yer alan 108 adet sahte görüntünün kalite faktörü 70,80 ve 90 olmak üzere rastgele kalite faktörü değerlerle kayıplı JPEG sıkıştırma atağına maruz kalmış halleri kullanılmıştır. Verisetinde CMHCompressed olarak isimlendirilen grubu oluşturan bu görüntüler kullanılarak elde edilen ortalama DPO, YPO ve Doğruluk metrikleri Tablo 3.12'de verilmiştir. JPEG sıkıştırma atağı durumunda da önerilen yöntemin referans yöntemlere göre yüksek performansa sahip olduğu söylenebilir.

Tablo 3.11. CMH ALL veri grubunda yer alan sahte görüntülerden elde edilen ortalama sonuçlar

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [108]	0,50	0,0019	0,75
Amerini vd. [110]	0,55	0,0023	0,77
Li vd. [144]	0,71	0,0263	0,84
Pun vd. [147]	0,70	0,0149	0,84
Silva vd. [139]	0,72	0,0122	0,85
Cozzolino vd. [42]	0,72	0,0023	0,85
Emam vd. [54]	0,64	0,0269	0,81
Zandi vd. [138]	0,46	0,0137	0,72
Jin vd. [169]	0,81	0,0400	0,88
Pun vd. [47]	0,81	0,0014	0,90
Li vd. [119]	0,56	0,0008	0,78
Vaishnavi ve Subashini [171]	0,80	0,0028	0,90
Huang ve Ciou [170]	0,91	0,020	0,94
Önerilen Yöntem	0,95	0,0022	0,96

Tablo 3.12. CMHCompressed veri grubunda yer alan sahte görüntülerden elde edilen ortalama sonuçlar

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [108]	0,35	0,0069	0,65
Amerini vd. [110]	0,48	0,0002	0,74
Li vd. [144]	0,54	0,0015	0,77
Pun vd. [147]	0,68	0,0369	0,82
Silva vd. [139]	0,68	0,0002	0,84
Cozzolino vd. [42]	0,49	0,0007	0,75
Emam vd. [54]	0,67	0,0205	0,82
Zandi vd. [138]	0,57	0,0398	0,76
Jin vd. [169]	0,45	0,0365	0,72
Pun vd. [147]	0,35	0,0139	0,67
Li vd. [119]	0,76	0,0098	0,87
Vaishnavi ve Subashini [171]	0,79	0,0052	0,89
Huang ve Ciou [170]	0,68	0,0122	0,83
Önerilen Yöntem	**0,89**	0,0062	**0,94**

Bu bölümde tez kapsamında önerilen L*a*b renk uzayından faydalanarak anahtar noktası tabanlı şüpheli bölgelerin çıkarılması ve dinamik bir lokalizasyon yaklaşımı ile sahtecilik tespiti yönteminin literatürdeki popüler verisetleri üzerinde performans değerlendirmesi tamamlanmış, referans yöntemlere göre karşılaştırmalı deneysel sonuçlar sunulmuştur.

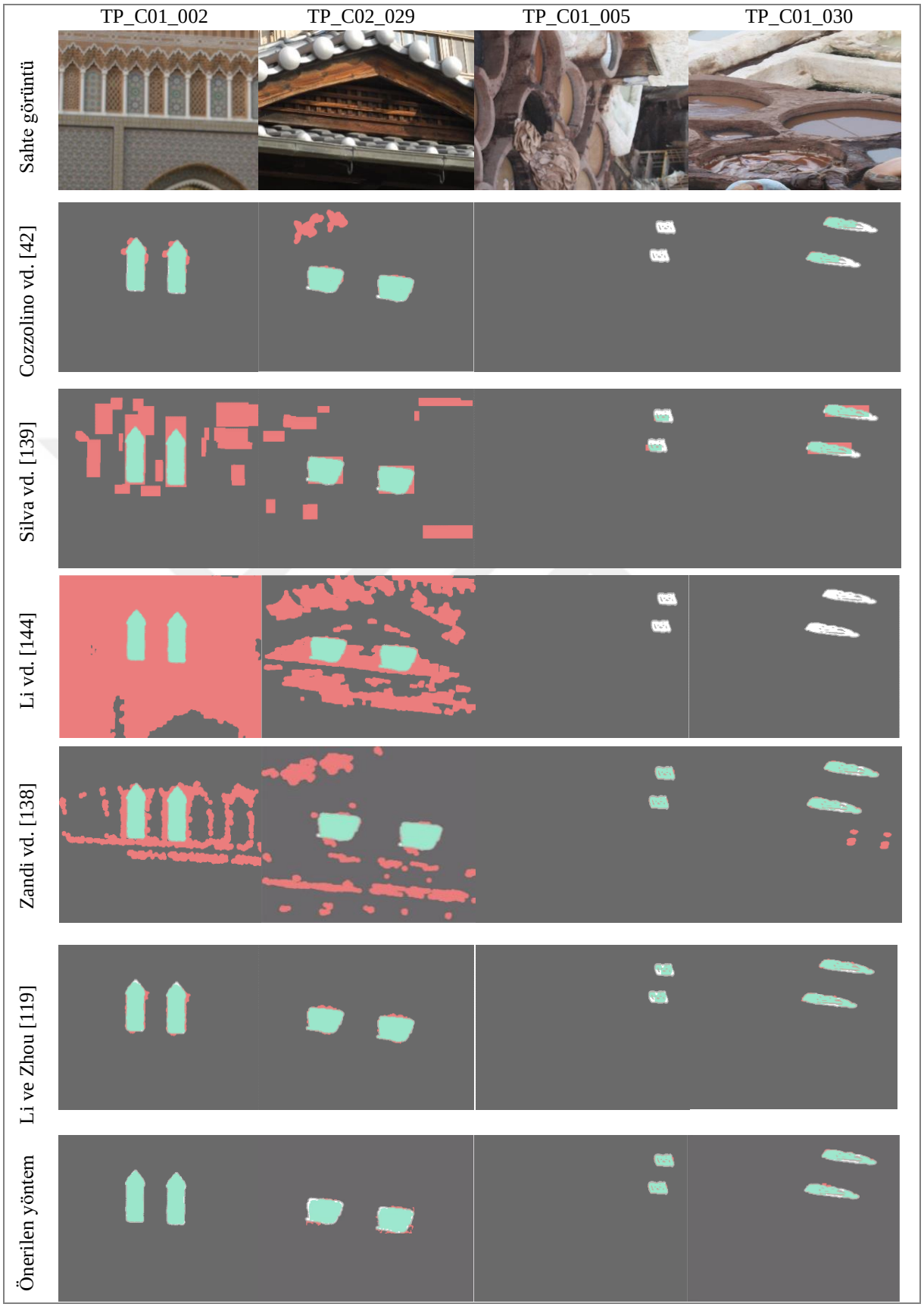
3.4. LBPROT ve SIFT Yöntemine Dayalı Şüpheli Bölge Çıkarımı ve Ciratefi Tabanlı Lokalizasyon Yaklaşımı ile Sahtecilik Tespitinin Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Bu bölümde tez kapsamında önerilen ikinci yöntemin performans değerlendirmelerine ilişkin deneysel sonuçlar sunulacaktır. İlk olarak GRIP verisetinden, ardından CMH verisetinden ve son olarak tez kapsamında tarafımızca üretilen verisetinden elde edilen deneysel sonuçlara ilişkin detaylar verilmiştir.

3.4.1. GRIP Verisetinde Elde Edilen Deneysel Sonuçlar

GRIP verisetinin kullanımı ile önerilen ikinci yöntemin ve literatürdeki popüler kopyala-yapıştır sahteciliği tespiti yöntemlerinin karşılaştırmalı analizi bu bölümde sunulacaktır. İlk olarak bu verisetinden seçilen tespiti zor sahte görüntüler üzerinde elde edilen görsel sonuçlar sunulacaktır. Ardından verisetinde yer alan bütün görüntülerin kullanımı ile elde edilen ortalama sonuçların karşılaştırmalı analizleri verilecektir.

Şekil 3.18'de sahte görüntüler ve bu görüntüler üzerinde elde edilen görsel sonuçlar sunulmuştur. İlk satırda GRIP verisetinde yer alan sahte görüntüler bulunmaktadır. Cozzolino vd. [42], Silva vd. [139], Li vd. [144], Zandi vd. [138] ve Li ve Zhou [119] tarafından önerilen yöntemler ve önerilen yöntemden elde edilen sonuçların renk kodları ile temsil edilen hallerine yer verilmiştir. İlk iki sahte görüntü benzer mimari görüntü bölgelerini bulunduran sahte görüntülerdir. Bu yüzden bu görüntülerde hatalı işaretlemenin azlığı yöntemlerin başarısını göstermektedir. Şekilde de görüldüğü gibi bu iki görüntüde de hatalı işaretlemeyi temsil eden kırmızı piksellerin varlığı oldukça az olup, sahte bölgelerin doğru bir şekilde işaretlendiği görülmektedir. Son iki sütunda ise düşük kontrasta sahip bölgelerle gerçekleştirilen sahte görüntüler bulunmaktadır. Bu iki görüntü için de önerilen yöntem ile oldukça başarılı işaretlemelerin olduğu görsel sonuçlar üretilmiştir.



Şekil 3.18. Referans çalışmalar ve önerilen yöntem ile elde edilen görsel sonuçlar

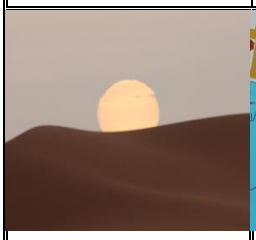
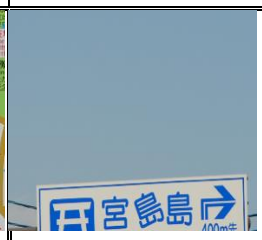
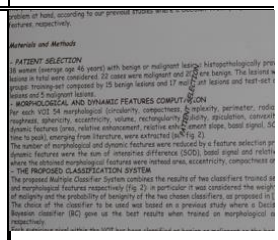
Tablo 3.13'te GRIP verisetindeki 80 adet ataksız görüntülerin ve 80 adet orijinal görüntünün kullanılması ile öncelikle görüntü seviyesinde yapılan değerlendirmeye ilişkin ortalama F-ölçütü sonucuna yer verilmiştir. Daha önceki bölümde de bahsedildiği gibi, görüntü seviyesinde yapılan değerlendirmede, girdi görüntüsünün sahte/orijinal olarak etiketlenmesi üzerine gerçekleştirilen performansa yer verilmektedir. Piksel seviyesinde yapılan değerlendirme sonuçları da bu tabloda yer almıştır. Referans yöntemlerden [40,42,110,138,139,144,147]'de önerilen çalışmaların sonuçları literatürden elde edilerek karşılaştırmalı değerlendirme için sonuçların yer aldığı tablo hazırlanmıştır. Önerilen yöntemin iki değerlendirme içinde en yüksek doğruluk oranına sahip olduğu görülmektedir.

Tablo 3.13. Ataksız kopyala-yapıştır sahteciliği durumunda, görüntü ve piksel seviyesindeki değerlendirmelere göre ortalama F-ölçütü değerleri

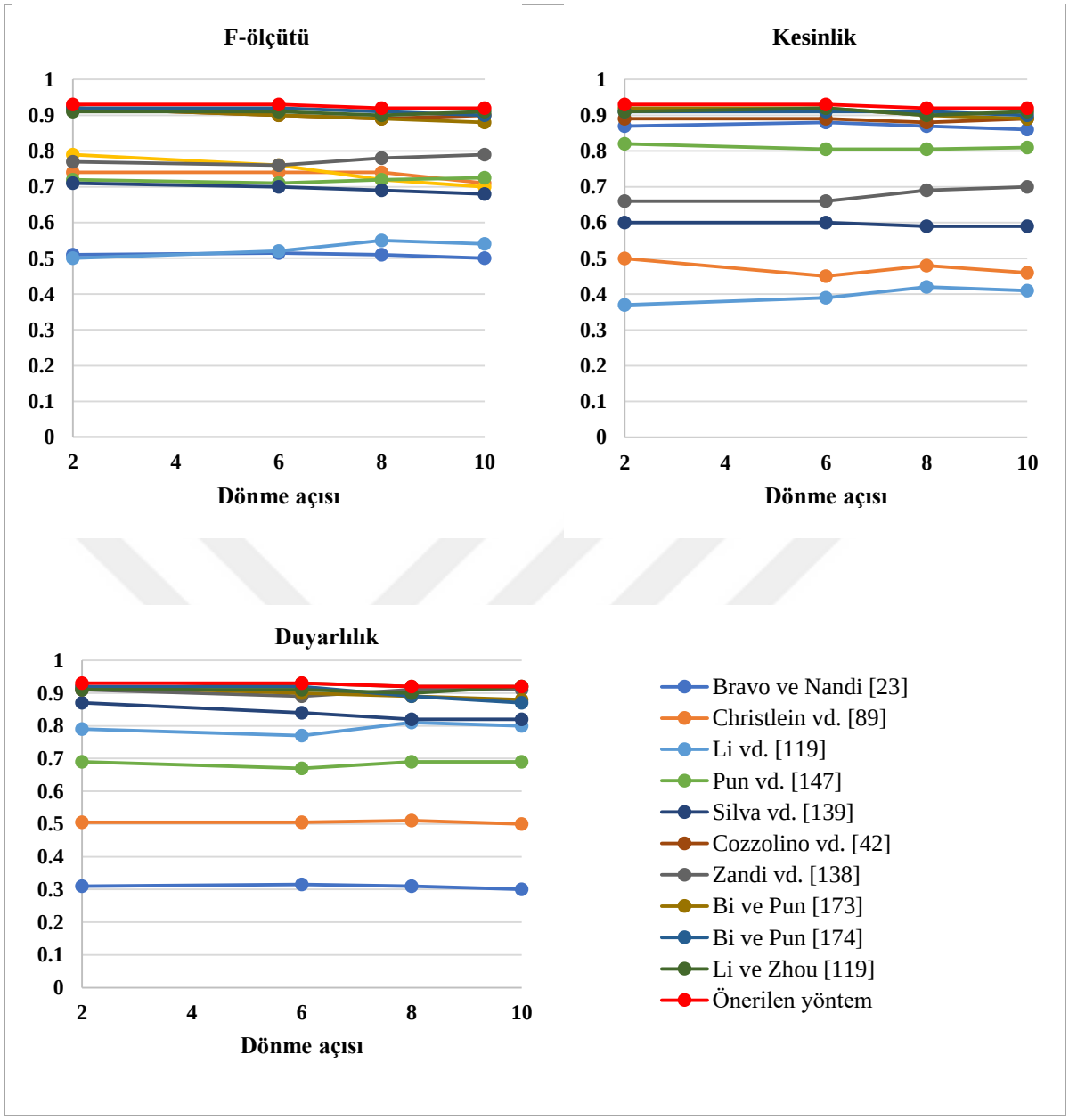
Yöntemler	Görüntü seviyesi	Piksel seviyesi
Ryu vd. [40]	0,94	0,89
Cozzolino vd. [42]	0,94	0,91
Silva vd. [139]	0,83	0,66
Amerini vd. [110]	0,67	0,44
Li vd. [144]	0,72	0,52
Pun vd. [147]	0,95	0,78
Zandi vd. [138]	0,86	0,85
Önerilen	0,96	0,92

İkinci deneyde yöntemlerin dönme atağı altındaki başarıları analiz edilmiştir. Tablo 3.14'de örnek sahte görüntüler, bu görüntüler üzerinde uygulanan atağın açı değeri ve sahtecilik maskesi verilmiştir. Referans çalışmalardan [42, 119, 138, 139, 144] ile örnek görüntüler tek tek test edilmiş elde edilen, Kesinlik(K), Duyarlılık (D) ve F-ölçütü(F) değerleri sırası ile verilmiştir. TP_C01_013 isimli ilk görüntü düz bölgelerle yapılan bir sahtecilik örneğidir. Li vd. [144] temelde anahtar noktalarına dayanan bir yöntem olup, düz bölgelerle yapılan sahtecilikleri tespit edemeyen bir yöntemdir. Dolayısı ile bu görüntününde sahte olduğu ortaya konamamıştır. Zandi vd. [138] tarafından önerilen yöntemde ise düz bölgelerle yapılan sahtecilikleri tespit edebilmek adına bir şema önerilse de dönme atağı olması durumunda sahtecilik tespiti yapılamamıştır. Önerilen yöntem ile en yüksek doğruluk oranı ile sahte bölgenin tespiti başarılı bir şekilde gerçekleştirilmiştir. Diğer sahte görüntüler dokulu bölgelerle yapılan sahtecilik örneklerindendir. Bu üç örnek için de önerilen yöntem yüksek başarım oranı ile sahtecilik tespitini gerçekleştirebilmiştir.

Tablo 3.14. Dönme atağına maruz kalmış örnek sahte görüntüler üzerinde elde edilen sonuçlar

Açı	**6°**			**8°**			**20°**			**75°**		
	TP_C01_013			TP_C01_050			TP_C02_017			TP_C02_015		
Sahte görüntü												
Maske												
	K	**D**	**F**	**K**	**D**	**F**	**K**	**D**	**F**	**K**	**D**	**F**
[42]	0,9	0,8	0,8	1	0,7	0,8	0	0	0	0	0	0
[139]	0,6	0,2	0,3	0,9	0,1	0,2	0,9	0,1	0,2	0	0	0
[144]	0	0	0	1	0,9	0,9	0,9	0,8	0,9	0,9	0,9	**0,9**
[138]	0	0	0	1	0,2	0,3	1	0,3	0,5	0,9	0,1	0,2
[119]	0,9	0,5	0,7	0,8	0,7	0,8	0,7	0,7	0,7	0,9	0,7	0,8
Ö	0,9	0,9	**0,9**	0,9	0,9	**0,9**	0,9	0,9	**0,9**	0,9	0,9	0,9

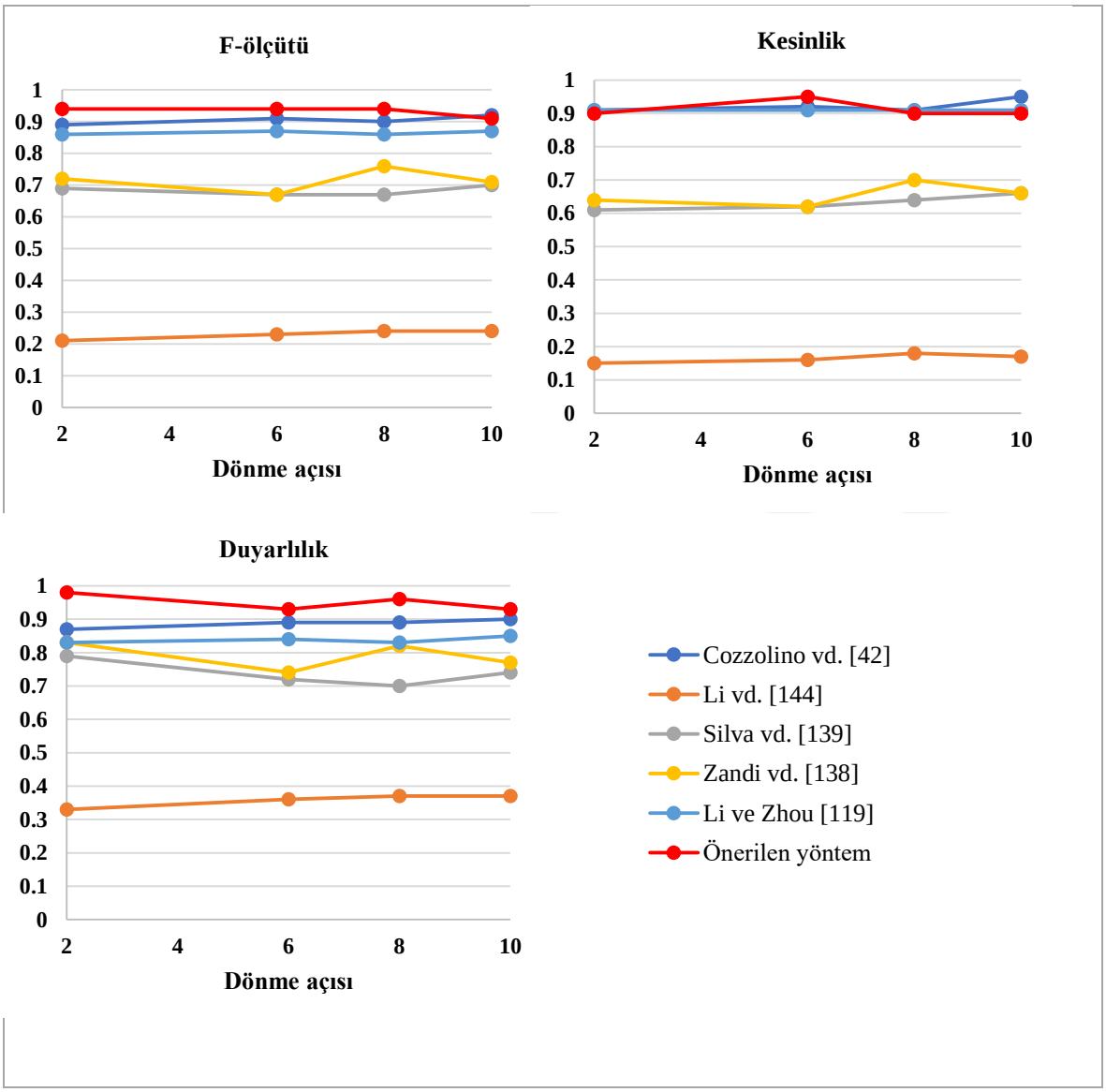
Yöntemlerin dönme atağı altındaki başarım analizini daha detaylı yapabilmek adına, performans değerlendirmesi küçük derecelerle ve büyük derecelerle yapılan ataklara karşı dayanıklılık olmak üzere iki aşamada gerçekleştirilmiştir. Bunun için ilk olarak GRIP verisetinde yer alan $2°, 6°, 8°, 10°$ ile dönme atağı uygulanmış 320 görüntü kullanıldı. Şekil 3.19'da derece bazında elde edilen ortalama Kesinlik, Duyarlılık ve F-ölçütü değerleri grafiksel olarak verilmiştir. [23], [89], [147], [173], [174]'de yer alan çalışmaların sonuçları literaturden toplanmıştır. [Veriseti büyük oranda düz bölgelerle yapılan sahte görüntüleri içerdiğinden anahtar noktası tabanlı yöntemler bu görüntülerin sahte olduğunun tespitini yapamamıştır [119, 173,174]'deki yöntemlerin sonuçları önerilen yöntemin sonuçlarına yakın olsa da önerilen yöntem en yüksek doğruluğa sahiptir.



Şekil 3.19. Dönme atağı altında sırası ile F-ölçütü, Kesinlik ve Duyarlılık metrikleri kullanılarak elde edilen ortalama sonuçlar

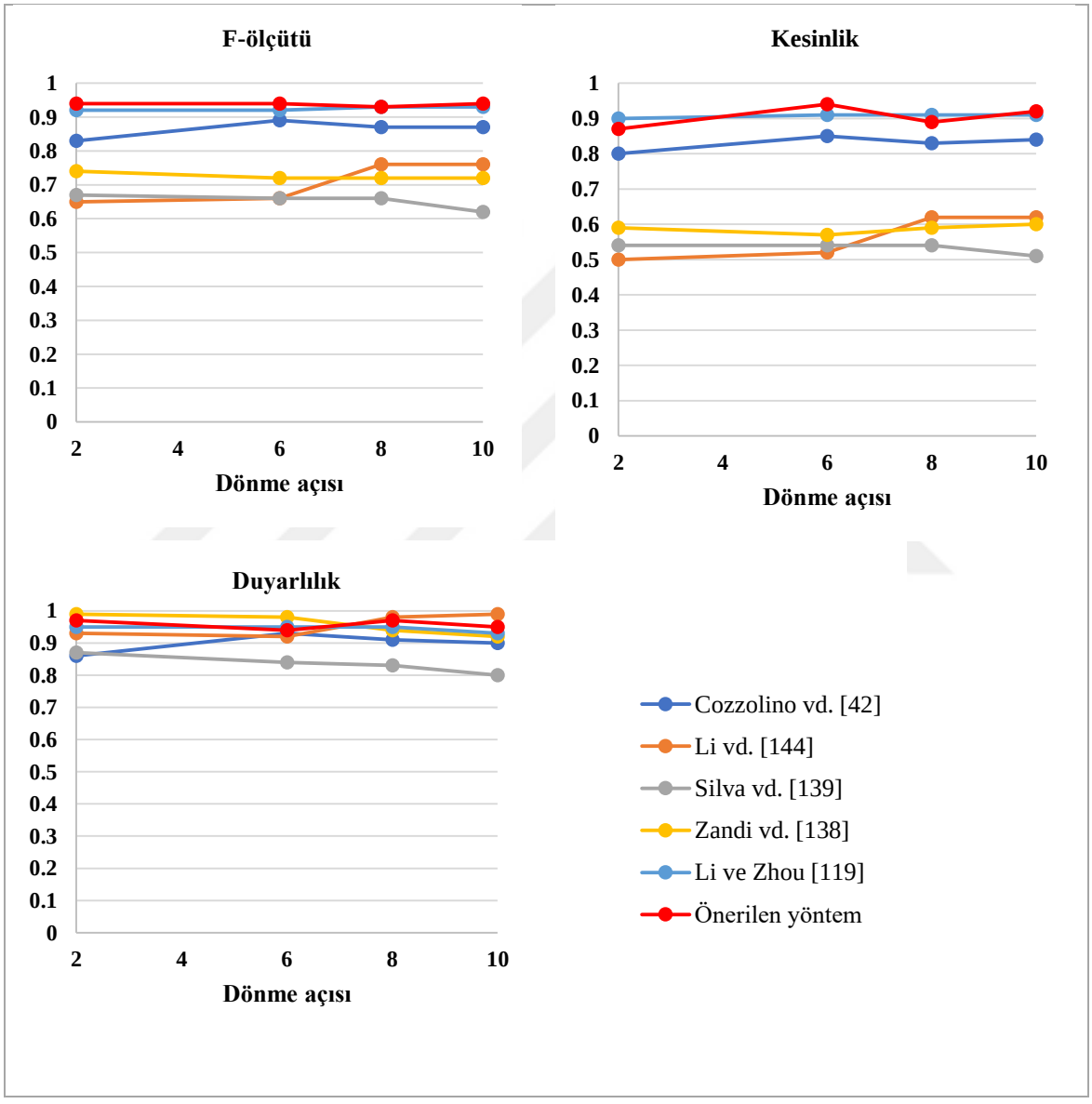
GRIP verisetinde yer alan görüntüler hem dokusuz bölgelerle yapılan sahteciliklerden hem de dokulu bölgelerle yapılan sahtecilikleri içeriğinden bu iki sahtecilik türünden elde edilen sonuçların ayrı ayrı değerlendirmesi de yapılmıştır. Bunun için sadece dokulu bölgelerle yapılan 20 görüntü ve sadece smooth bölgelerle yapılan 20 görüntü seçilmiştir. [42,119,138,139,144]'de yer alan yöntemler ve önerilen yöntemin, bu görüntüler üzerinde test edilerek elde edilen ortalama sonuçlar Şekil 3.20'de verilmiştir. [144]'deki yöntem,

anahtar noktası tabanlı bir yöntem olup, düz bölgelerden anahtar nokta çıkarmaya yönelik bir yenilik olmadığı için oldukça başarısız olmuştur. [42] ve [119]'daki yöntemler nispeten bu sorunu çözmeye çalışan yöntemler olduğu için biraz daha yüksek sonuçlar elde edilebilmiştir. Keza yöntem [139], kontrast eşiğini düşürerek düz bölgelerden de anahtar noktası elde etmiş olsa da lokalizasyon aşamasındaki sebebi ile iyi performans gösterememiştir.



Şekil 3.20. Yalnızca düz bölgelerle yapılan sahtecilikleri içeren görüntüler üzerinde dönme atağı altında elde edilen ortalama sonuçlar

Dönme atağı değerlendirmesinde diğer bir aşama olan, yanlızca dokulu bölgelerle yapılan sahteciliklerin tespitine ilişkin performans değerlendirmesi sonuçları Şekil 3.21'de verilmiştir. Bu analizde verisetinde yer alan sadece dokulu bölgelerle yapılan 20 adet sahte görüntünün 2, 6, 8 ve 10 derece dönme atağı uygulanmış halleri olmak üzere 80 adet görüntü kullanılmıştır.



Şekil 3.21. Yalnızca dokulu bölgelerle yapılan sahtecilikleri içeren görüntüler üzerinde dönme atağı altında elde edilen ortalama sonuçlar

Yöntemlerin ayrıca büyük derecelerle dönme atağı uygulanmış sahte görüntülerdeki performans değerlendirmeleri yapılmıştır. Bunun için verisetinde yer alan 20, 75 ve 180

derece dönme atağına maruz kalmış 80x3=320 adet görüntü kullanılmıştır. Elde edilen ortalama F-ölçütü, Kesinlik ve Duyarlılık değerleri Tablo 3.15'de verilmiştir. Önerilen yöntemin başarısı bu test aşamasında da ortaya konmuştur.

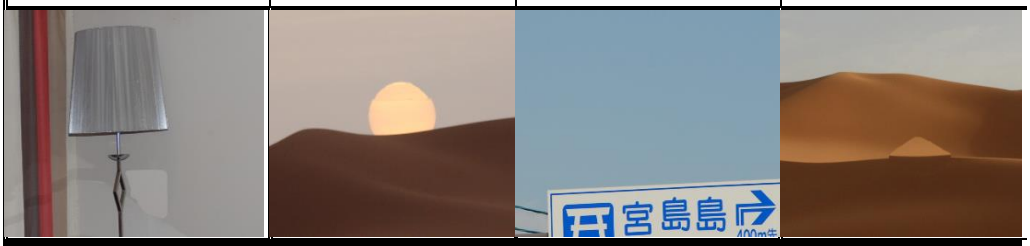
Yöntemlerin performans analizinin devamında, ölçekleme atağına karşı dayanıklılığın değerlendirmesi yapılmıştır. Tablo 3.16'da verilen örnek sahte görüntüler oluşturulurken, kopyalanan bölge sırası ile 0.08, 0.93, 0.97 ve 1.2 oranlarında ölçeklendirildikten sonra yapıştırılmıştır.

Tablo 3.15. Büyük açı değerleri ile gerçekleştirilen dönme atağına maruz kalmış görüntülerden elde edilen ortalama sonuçlar

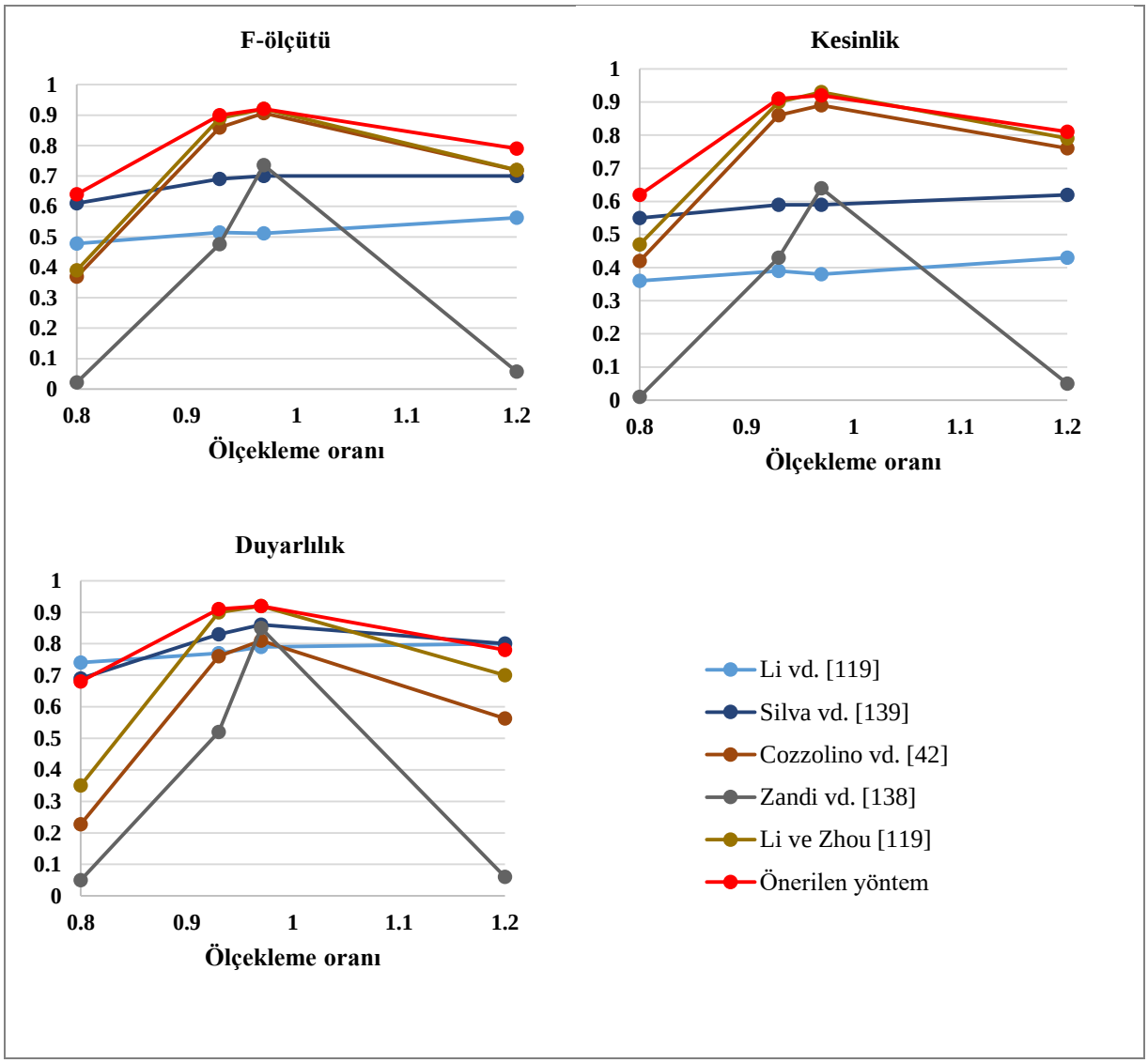
	F-ölçütü			**Kesinlik**			**Duyarlılık**		
Yöntemler	**20°**	**75°**	**180°**	**20°**	**75°**	**180°**	**20°**	**75°**	**180°**
Cozzolino vd. [42]	0,88	0,63	0,68	0,88	0,66	0,68	0,88	0,61	0,68
Silva vd. [139]	0,52	0,60	0,64	0,45	0,56	0,56	0,63	0,64	0,73
Li vd. [144]	0,55	0,53	0,60	0,43	0,42	0,29	0,76	0,70	0,47
Zandi vd. [138]	0,74	0,73	0,79	0,63	0,63	0,70	0,88	0,89	0,92
Li ve Zhou [119]	0,89	0,87	0,91	**0,90**	0,82	**0,92**	0,90	0,87	0,93
Önerilen yöntem	**0,91**	**0,90**	**0,92**	**0,90**	**0,89**	0,91	**0,93**	**0,92**	**0,94**

Şekil 3.22'de, verisetinde yer alan, ölçekleme oranı %0.08, %0.93, %0.97 ve %1.2 olmak üzere 320 görüntü üzerinde yöntemlerin analizleri yapılmıştır. Zandi vd. [138] tarafından önerilen yöntemin, yazarlar tarafından ölçekleme atağına karşı dayanıklı olduğu rapor edilse de 0.08 oranında ölçekleme olduğu durumda sahtecilik tespiti yapılamamış, 1.2 oranında ölçekleme atağında da çok az görüntüde sahtecilik tespiti gerçekleştirilebilmiştir. Cozzolino vd.[42] ve Li ve Zhou [119] tarafından önerilen yöntemler %0.93 ve %0.97 oranında ölçekleme atağı olduğu durumda F-ölçütü metriği ile elde edilen ortalama sonuçlara göre, önerilen yönteme oldukça yakın sonuçlar üretse de %0.8 ve %1.2 oranda ölçekleme atağı altında performansları oldukça düşmüştür. Ortalama sonuçlara göre, önerilen yöntemin, literatürde problem olarak değerlendirilen büyük oranlarla ölçekleme atağı uygulanmış sahteciliklerin tespitindeki başarısı ortaya konmuştur.

Tablo 3.16. Ölçekleme atağı altında elde edilen örnek sonuçlar

Oran	**0.08**			**0.93**			**0.97**			**1.2**		
	TP_C02_002			TP_C01_013			TP_C02_017			TP_C01_019		
Sahte görüntü												
Maske												
	K	**D**	**F**	**K**	**D**	**F**	**K**	**D**	**F**	**K**	**D**	**F**
[42]	0	0	0	0,5	1	0,7	0	0	0	0,1	1	0,2
[139]	0,8	0,3	0,5	0,8	0,3	0,4	0,8	0,5	0,6	0,8	0,5	0,6
[144]	0	0	0	0	0	0	0,9	0,9	**0,9**	0	0	0
[138]	0	0	0	0	0	0	1	0,1	0,2	0	0	0
[119]	0	0	0	0,9	0,4	0,6	0,8	0,7	0,8	0,9	0,6	0,7
Ö	0,8	0,7	**0,8**	0,9	0,8	**0,8**	0,9	0,9	0,9	0,7	0,7	**0,7**

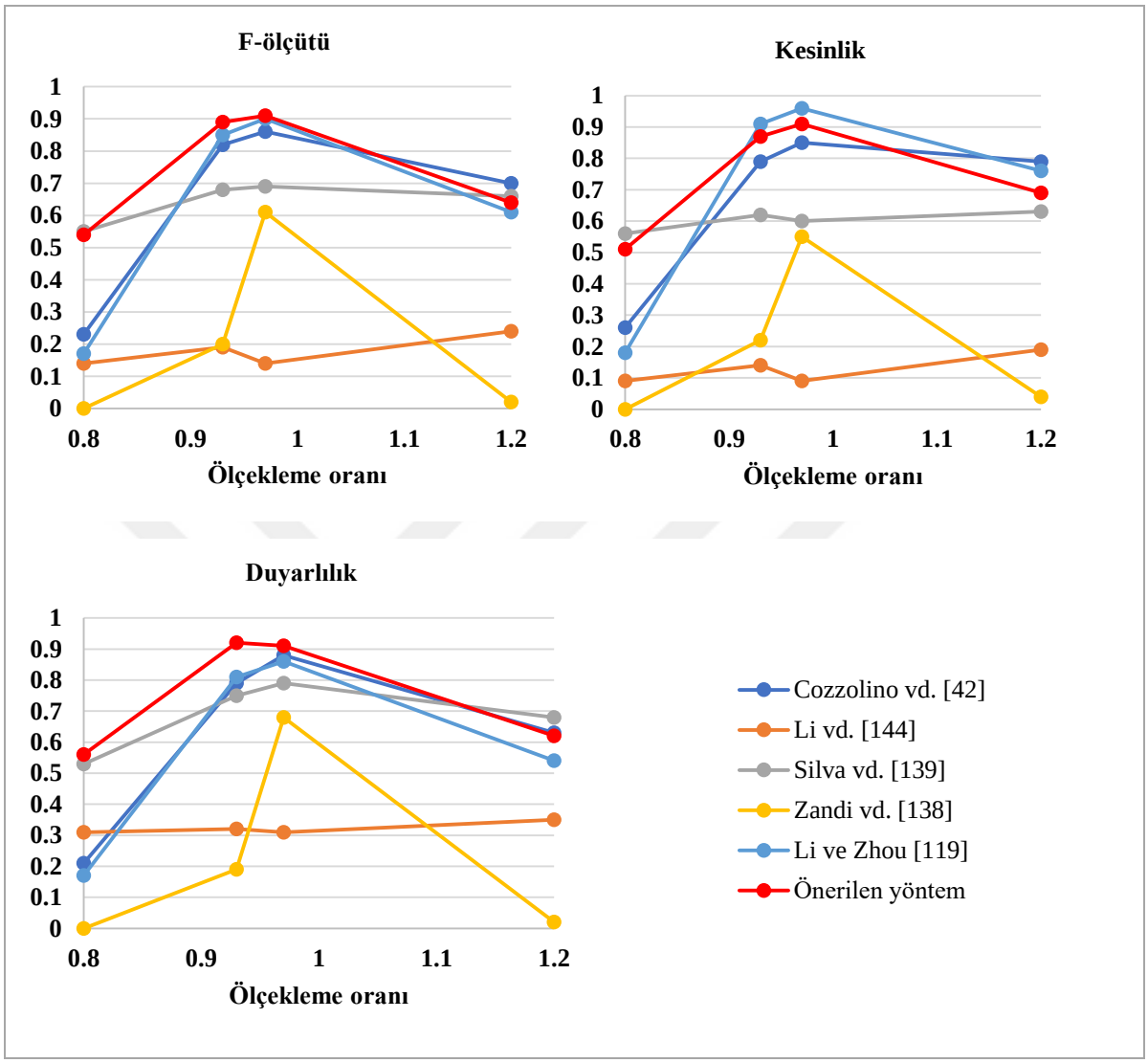
Ölçekleme atağına karşı dayanıklılığın görüntü türüne göre değerlendirilebilmesi için, veri setinden 20 adet düz bölgelerle yapılan sahte görüntü ve 20 adet dokulu bölgelerle yapılan sahte görüntü seçilmiştir. Yöntemlerin düz bölgelerle yapılan sahte görüntüler üzerindeki değerlendirmeleri sonucu elde edilen ortalama F-ölçütü, Kesinlik ve Duyarlılık değerleri grafiksel olarak verilmiştir. Li vd. [144] tarafından yöntem bütün oranlarda oldukça düşük sonuçlar vermiştir. Zandi vd. [138] tarafından önerilen yöntem ile 0.08 ve 1.2 oranında ölçekleme atağı durumunda olan görüntülerin hiç birinin tespitini gerçekleştirememiştir.



Şekil 3.22. Ölçekleme atağı altındaki ortalama sonuçlar

Şekil 3.24'te ise sadece dokulu bölgelerle yapılan sahte görüntülerin ölçekleme atağına karşı ortalama sonuçları grafiksel olarak verilmiştir. Li vd.[144] tarafından önerilen yöntem ile elde edilen sonuçların Duyarlılık değerleri yüksek, Kesinlik değeri düşük çıkmıştır. Bu durum, sahte piksellerin tespitinde sahtecilik bölgesinin doğru tespitinin yapıldığını ancak yüksek oranda orijinal olduğu halde sahte olarak işaretlenen piksel olduğunu göstermektedir. Grafiksel analizlere göre, önerilen yöntemin piksel seviyesinde ölçekleme atağına karşı yüksek performansı ortaya konmuştur. Yöntemlerin performansları, ölçekleme oranının 0.08 ve 1.2 olduğu durumlardaki görüntü seviyesinde de araştırılmıştır. Buna göre veri setindeki

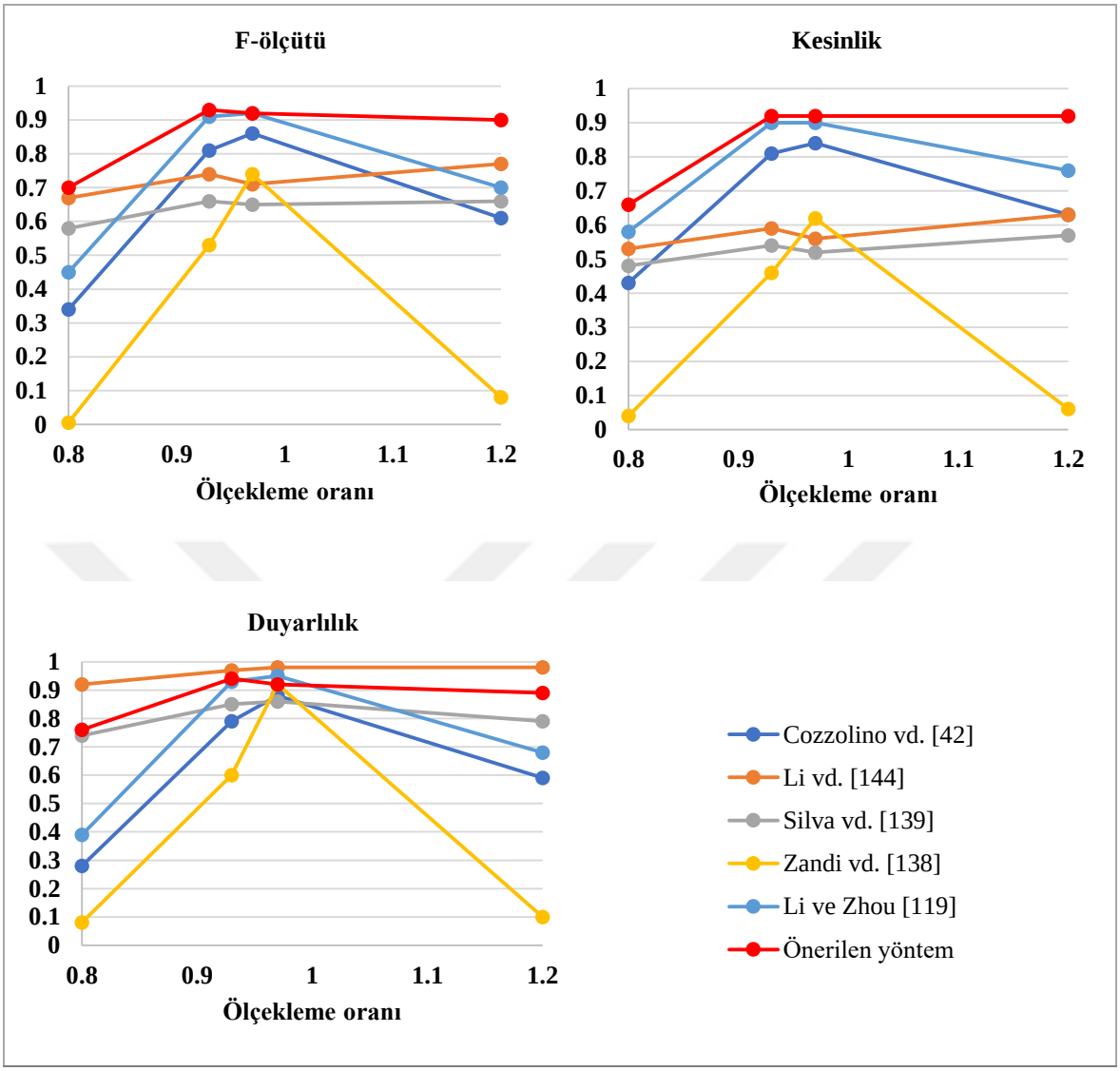
80’er olmak üzere 160 görüntü üzerinden elde edilen F-ölçütü sonuçları Tablo 3.17’de verilmiştir. Önerilen yöntemin bu analizde de başarılı olduğu ortaya konmuştur.



Şekil 3.23. Ölçekleme atağı uygulanmış düşük kontrasta sahip bölgelerle yapılan sahte görüntülerden elde edilen ortalama sonuçlar

Tablo 3.17. Görüntü seviyesinde değerlendirme için Büyük oranla yapılan ölçekleme atağı altında ortalama F-ölçütü değerleri

Test	**Görüntü seviyesi**	
Ölçekleme oranı	**0,8**	**1,2**
Christlein vd. [89]	0,20	0,11
Cozzolino vd.[42]	0,57	0,81
Silva vd. [139]	0,79	0,80
Li vd. [144]	0,72	0,74
Zandi vd. [138]	0,20	0,15
Li ve Zhou [119]	0,66	0,91
Önerilen yöntem	0,90	0,94



Şekil 3.24. Ölçekleme atağı uygulanmış dokulu bölgelerle yapılan sahteciliklerde dönme atağına karşı ortalama sonuçlar

3.4.2. CMH Verisetindeki Deneysel Sonuçlar

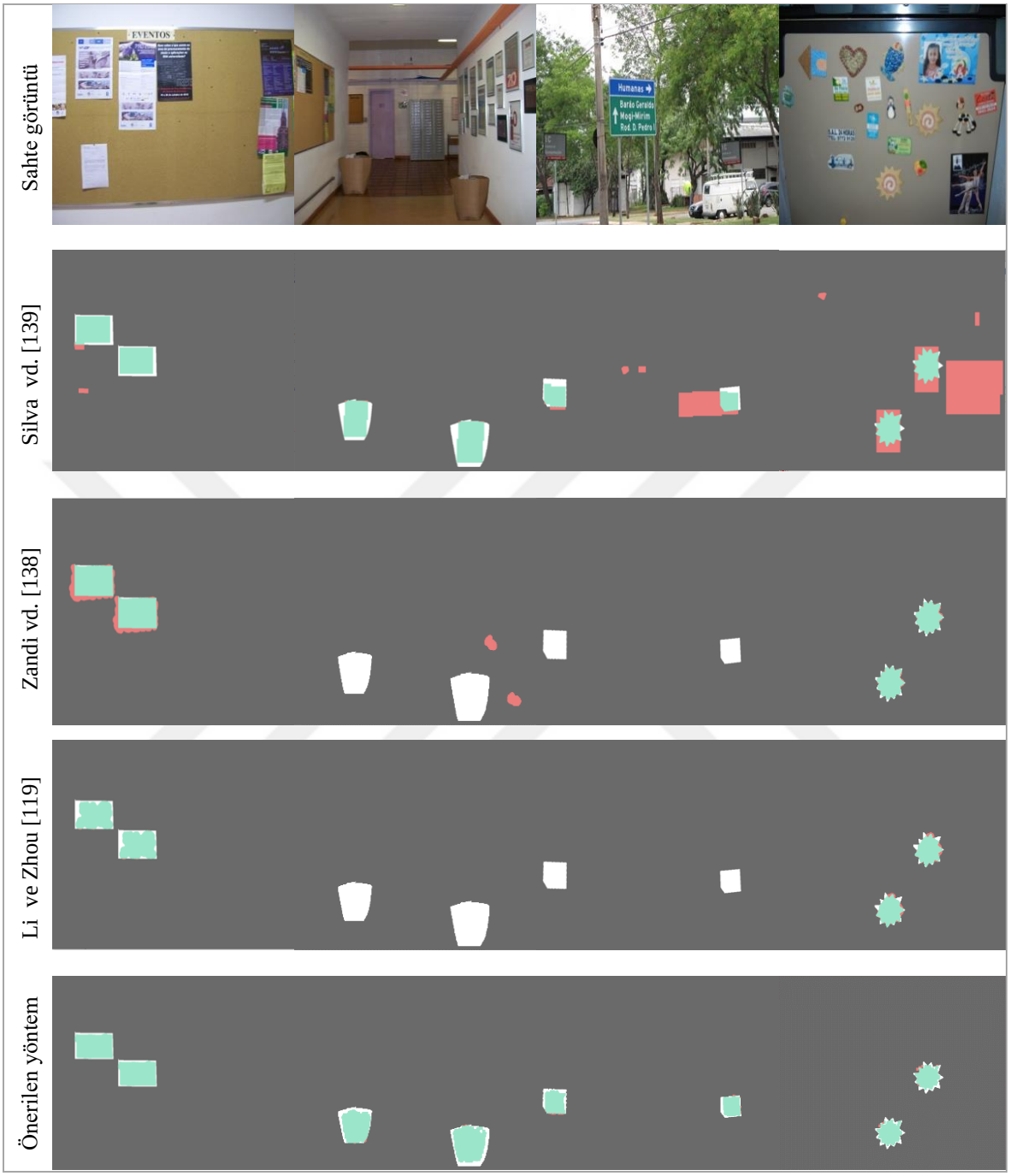
Bu bölümde tez kapsamında önerilen ikinci yöntemin CMH veriseti üzerindeki karşılaştırmalı performans analizine yer verilmiştir. Şekil 3.25'de önerilen yöntem ve referans çalışmalardan elde edilen görsel sonuçlar yer almaktadır. Silva vd. [139], Zandi vd. [138], Li ve Zhou [119] tarafından önerilen çalışmaların kaynak kodları tarafımızca

paylaşıldığı için karşılaştırmada bu yöntemler kullanılmıştır. Bu çalışmalardan elde edilen görsel sonuçlar her bir sahte görüntü için yukarıdan aşağı sırası ile verilmiştir. Son satırda önerilen yöntemden elde edilen görsel sonuçlar yer almaktadır. Görsel sonuçların oluşturulmasında kullanılan renk kodlarının anlamları bir önceki bölümde verilen görsel sonuçlar ile aynıdır. İlk ataksız sahte görüntü yer almaktadır. Silva vd. [139] ve Zandi vd. [138] tarafından önerilen yöntemlerden elde edilen görsel sonuçlarda az da olsa yanlış pozitif işaretlenen piksellerin varlığı görülmektedir. Li ve Zhou [119] tarafından önerilen yöntem ile de sahte piksellerin doğru pozitif olarak işaretlemesinin önerilen yöntem kadar olmadığı görülmektedir. İkinci sahte görüntü ise ölçekleme atağına maruz bırakılarak oluşturulmuş bir görüntüdür. Zandi vd. [138] ve Li ve Zhou [119] tarafından önerilen yöntemlerin bu sahteciliği tespit edemediği görülmektedir. Üçüncü sahte görüntü ise hem ölçekleme hem dönme atağına uygulanmış sahte görüntüdür. Silva vd. [139] tarafından önerilen yöntemde büyük miktarda yanlış pozitif işaretlemesinin olduğu ve yine Zandi vd. [138], Li ve Zhou [119]'daki yöntemlerin bu sahteciliği tespit edemediği görülmüştür. Son sahte görüntü ise JPEG sıkıştırma atağına maruz kalmış bir görüntüdür. Zandi vd. [138], Li ve Zhou [119] tarafından önerilen yöntemler bu sahteciliği tespit edemezken, Silva vd. [139] tarafından önerilen yöntem ile yüksek oranda yanlış pozitif işaretlenmiş pikseller görülmüştür.

CMH verisetindeki daha detaylı analizde her bir alt grupta yer alan sahte görüntülerden elde edilen sonuçlar grup bazlı değerlendirilmiştir. İlk olarak CMH1 de yer alan ataksız sahte görüntüler kullanılmıştır. DPO, YPO ve Doğruluk metriklerine göre elde edilen ortalama sonuçlar Tablo 3.18'de verilmiştir. Amerini vd. [110] tarafından önerilen yöntemin bu verisetindeki sonuçları literatürden elde edilmiştir. Amerini vd. [110] tarafından önerilen yöntem ile en düşük DPO ve Doğruluk oranı elde edilmiştir. Silva vd. [139] tarafından önerilen yöntem ile de önerilen yönteme en yakın DPO ve Doğruluk metriği değeri bulunmuş olsa da en yüksek performans sonuçları önerilen yöntem ile bulunmuştur.

Tablo 3.18. CMH1 grubundaki görüntüler üzerinde ortalama sonuçlar (ataksız sahte görüntüler)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,48	0,0020	0,74
Silva vd. [139]	0,94	0,0017	0,96
Zandi vd. [138]	0,85	0,0174	0,92
Li ve Zhou vd. [119]	0,83	0,0013	0,92
Önerilen yöntem	0,96	0,0023	0,98



Şekil 3.25. Önerilen yöntem ve referans yöntemlerden elde edilen görsel sonuçlar

Bir sonraki analizde CMH2 grubunda yer alan bütün sahte görüntüler kullanılarak yöntemlerin bu görüntüler üzerinde verdiği ortalama sonuçlar Tablo 3.19'da görülmektedir. Amerini vd. [110] tarafından önerilen yöntem, bu görüntüler üzerinde oldukça düşük

performans göstermiştir. Bu yöntem anahtar noktası tabanlı bir yöntem olmasına rağmen verisetindeki tespiti zor görüntüler sebebi ile düşük performansa sahiptir. Önerilen yöntemin dönme atağı durumunda da referans yöntemlere göre üstün başarısı görülmektedir.

Tablo 3.19. CMH2 grubundaki görüntüler üzerinde ortalama sonuçlar (dönme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,47	0,0014	0,73
Silva vd. [139]	0,70	0,0066	0,84
Zandi vd. [138]	0,52	0,0007	0,76
Li ve Zhou vd. [119]	0,60	0,0005	0,80
Önerilen yöntem	0,78	0,0160	0,88

CMH3 grubunda yer alan, ölçekleme atağı uygulanmış sahte görüntülerden elde edilen ortalama sonuçlar Tablo 3.20'de yer almaktadır. Zandi vd. [138] ve Li ve Zhou [119] tarafından önerilen yöntemler anahtar noktası tabanlı yöntem olmasına rağmen en düşük performans sonuçları bu yöntemlerden elde edilmiştir. Tablodan da görüldüğü gibi referans alınan yöntemlere göre en yüksek ortalama sonuç önerilen yöntem ile elde edildi.

Tablo 3.20. CMH3 grubundaki görüntüler üzerinde ortalama sonuçlar (ölçekleme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,64	0,0124	0,82
Silva vd. [139]	0,48	0,0016	0,74
Zandi vd. [138]	0,21	0,0163	0,60
Li ve Zhou vd. [119]	0,36	0	0,68
Önerilen yöntem	0,81	0,0079	0,90

CMH4 grubundaki hem ölçekleme hem dönme atağına maruz kalmış sahte görüntülerden elde edilen sonuçlar ise Tablo 3.21'de verilmiştir. İki atağın aynı anda uygulanması durumunda dahi önerilen yöntemin oldukça tatmin edici sonuçlar ürettiği görülmektedir. Tablo 3.22'de ise bu dört alt grupta yer alan görüntülerden elde edilen sonuçların ortalamaları verilmiştir. Literatürde bu verisetinin alt gruplarının birleştirilmesi ile sonuçlarının verildiği ekstra referans yöntemlerin sonuçları da tabloda yer almaktadır. Tablodan da görüldüğü gibi önerilen yöntem ile referans alınan 13 çalışmadan daha yüksek performans ile sahtecilik tespiti gerçekleştirilebilmiştir.

Tablo 3.21. CMH4 grubundaki görüntüler üzerinde ortalama sonuçlar (hem dönme hem ölçekleme atağı)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [110]	0,56	0,0024	0,78
Silva vd. [139]	0,64	0,0129	0,82
Zandi vd. [138]	0,57	0,0136	0,60
Li ve Zhou vd. [119]	0,44	0,0010	0,72
Önerilen yöntem	0,77	0,0144	0,88

Tablo 3.22. Bütün verisetindeki ortalama sonuçlar (CMHALL)

Yöntemler	**DPO**	**YPO**	**Doğruluk**
Amerini vd. [108]	0,50	0,0019	0,75
Amerini vd. [110]	0,55	0,0023	0,77
Li vd. [145]	0,71	0,0263	0,84
Pun vd. [146]	0,70	0,0149	0,84
Silva vd. [139]	0,72	0,0122	0,85
Cozzolino vd. [42]	0,72	0,0023	0,85
Emam vd. [54]	0,64	0,0269	0,81
Zandi vd. [138]	0,46	0,0137	0,72
Jin vd. [169]	0,81	0,0400	0,88
Pun vd. [147]	0,81	0,0014	0,90
Li ve Zhou [119]	0,56	0,0008	0,78
Vaishnavi ve Subashini [171]	0,80	0,0028	0,90
Huang ve Ciou [170]	0,91	0,0200	0,94
Önerilen Yöntem	0,93	0,0101	0,96

Tablo 3.23'te CMHAll grubunda yer alan görüntülerin JPEG sıkıştırma atağı sonrası hallerini barındıran CMHCompressed olarak isimlendirilen gruptan elde edilen ortalama sonuçlar verilmiştir. Literatürde bu verisetinin alt gruplarının birleştirilmesi ile sonuçlarının verildiği ek referans çalışmaların sonuçları da tabloda sunuldu. Tablodan da görüldüğü gibi önerilen yöntem ile referans alınan 13 çalışmadan daha yüksek performans ile sahtecilik tespiti gerçekleştirilebilmiştir.

Tablo 3.23. JPEG sıkıştırma atağı altındaki ortalama sonuçlar (CMHCompressed)

Yöntemler	DPO	YPO	Doğruluk
Amerini vd. [108]	0,35	0,0069	0,6473
Amerini vd. [110]	0,48	0,0002	0,7404
Li vd. [144]	0,54	0,0015	0,7689
Pun vd. [147]	0,68	0,0369	0,8217
Silva vd. [139]	0,68	**0,0002**	0,8380
Cozzolino vd. [42]	0,49	0,0007	0,7478
Emam vd. [54]	0,67	0,0205	0,8259
Zandi vd. [138]	0,57	0,0398	0,7641
Jin vd. [169]	0,45	0,0365	0,7097
Pun vd. [147]	0,35	0,0139	0,6694
Li ve Zhou [119]	0,76	0,0098	0,8735
Vaishnavi ve Subashini [171]	0,79	0,0052	0,89
Huang ve Ciou [170]	**0,68**	0,1220	**0,83**
Önerilen yöntem	**0,84**	0,0384	**0,90**

3.4.3. Tez Kapsamında Oluşturulan Veri Setinde Elde Edilen Deneysel Sonuçlar

Proje kapsamında hazırlanan verisetinde yer alan görüntüler üzerinde, önerilen yöntem ile Cozzolino vd. [42], Silva vd. [139], Zandi vd. [138], Li ve Zhou [119]'da önerilen çalışmaların performans değerlendirmesi bu bölümde yer alacaktır. Verisetinde her bir atak türünde 80'er adet görüntü bulunmaktadır ve değerlendirme sonuçları bu görüntülerden elde edilen ortalama sonuçlar şeklinde verilecektir.

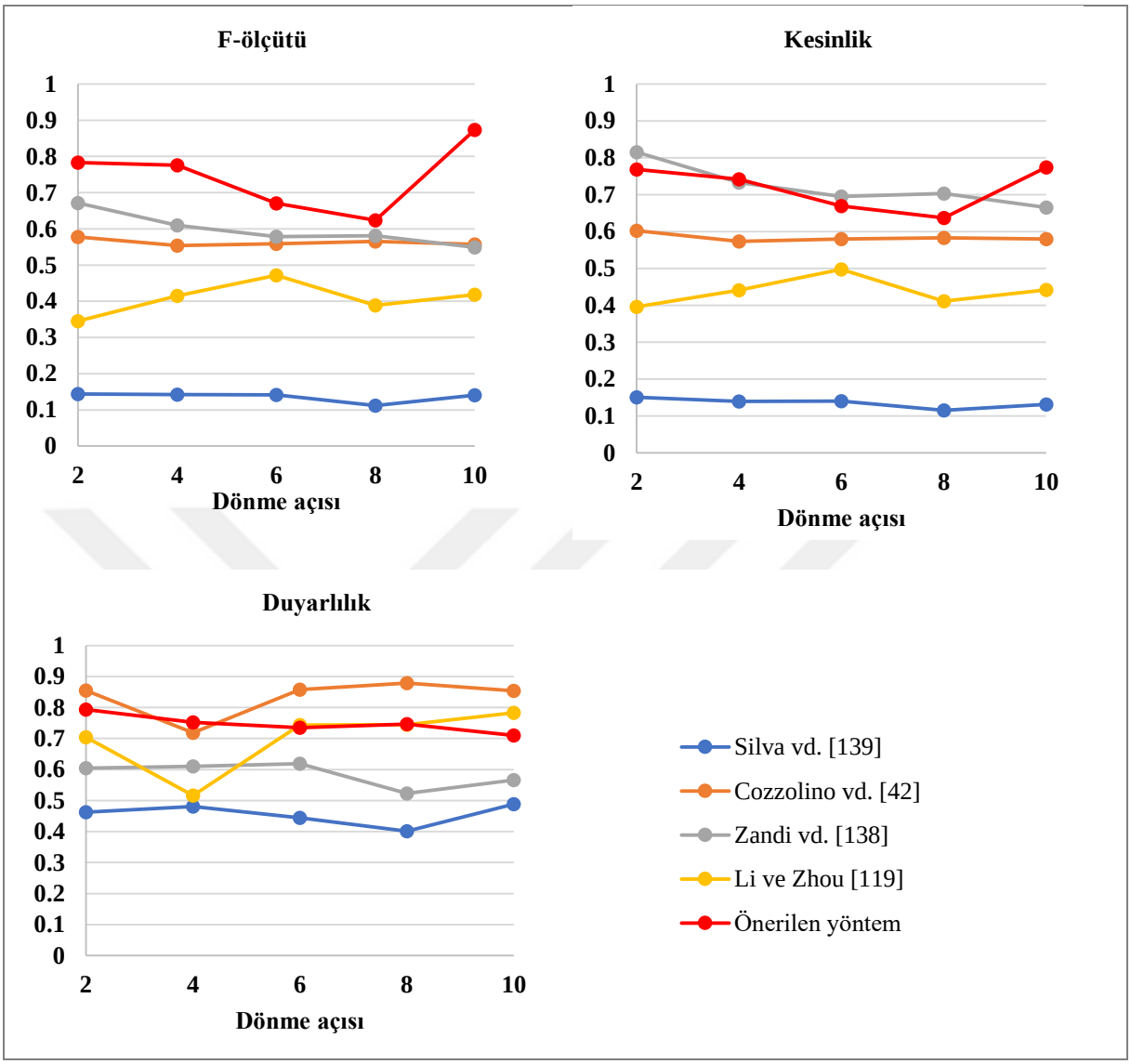
İlk olarak ataksız kopyala-yapıştır sahteciliği durumundaki performans değerlendirmesi yapılmıştır. Bu aşamada sahtecilik tespiti değerlendirmesi hem görüntü seviyesinde hem de piksel seviyesinde gerçekleştirilmiştir. Görüntü seviyesindeki değerlendirme, sahte bir görüntünün sahte olarak ortaya konabilme performansı hakkında bilgi verirken, piksel seviyesindeki değerlendirme sahte görüntüde kopyalanıp yapıştırılan bölgede yer alan sahte piksellerin tespiti performansını sunmaktadır. Tablo 3.24'te görüntü ve piksel seviyesinde F-ölçütü metriği kullanarak elde edilen ortalama sonuçlar verilmiştir. Önerilen yöntem ile iki değerlendirme durumunda da daha yüksek sonuç elde edildiği tablodan da görülmektedir.

Tablo 3.24. Ataksız kopyala-yapıştır sahteciliği durumunda, görüntü ve piksel seviyesindeki değerlendirmelere göre ortalama F-ölçütü değerleri

Yöntemler	**Görüntü seviyesi**	**Piksel seviyesi**
Cozzolino vd. [42]	0,74	0,60
Silva vd. [139]	0,35	0,20
Zandi vd. [138]	0,83	0,76
Li ve Zhou [119]	0,77	0,62
Önerilen yöntem	**0,97**	**0,86**

Yöntemlerin dönme atağı altındaki karşılaştırmalı performans değerlendirmesi, hazırlanan veriseti üzerinde yer alan görüntüler ile de gerçekleştirilmiştir. Bu değerlendirme piksel seviyesinde gerçekleştirilmiştir Bunun için ilk olarak $2^{\circ}, 4^{\circ}, 6^{\circ}, 8^{\circ}\ 10^{\circ}$ ile dönme atağı uygulanmış, 5x80=400 adet sahte görüntü kullanılmıştır. F-ölçütü, Kesinlik ve Duyarlılık metrikleri ile elde edilen ortalama sonuçlar ile oluşturulan grafikler Şekil 3.26'da verilmiştir. Zandi vd. [138] ile önerilen yönteme göre daha yüksek Kesinlik sonucu elde edilmiş ancak bu yöntemin hatalı işaretleme oranının yüksek olması sebebi ile Duyarlılık sonucu daha düşüktür. Önerilen yöntemin, Kesinlik ve Duyarlılık metriğinin harmonik ortalamasını temsil eden F-ölçütü metriği ile en yüksek performansa sahip olduğu görülmektedir.

Yöntemlerin daha büyük derecelerle dönme atağı uygulandığı durumdaki performans değerlendirmesi için verisetinde yer alan $20^{\circ}, 75^{\circ}, 180^{\circ}$ ile dönme atağı uygulanmış görüntüler kullanılmıştır. Bu görüntüler üzerinde elde edilen ortalama sonuçlar Tablo 3.25 ile verilmiştir. Büyük derece dönme atağı durumunda da Zandi vd. [138] tarafından önerilen yöntem ile en yüksek Kesinlik sonucu elde edilirken, Duyarlılık sonucu düşüktür. Bu yöntem ile sahte bölgelerin tespiti yüksek doğrulukla yapılmıştır. Ancak sahte olmayan piksellerin, sahte olarak etiketlenmesi durumu yüksek olduğu için Duyarlılık metriği ile daha düşük sonuç elde edilmiştir. Silva vd. [139] tarafından önerilen yöntem ile elde edilen sonuçlara göre Duyarlılık metriği ile elde edilen sonucun yüksek olması hatalı işaretleme oranı düşük olduğunu ifade etse de Kesinlik metriği ile elde edilen ortalama sonucun düşük olması doğru işaretleme oranın düşük olduğunu ifade eder. Önerilen yöntem ile büyük derece dönme atağı durumlarında da en yüksek ortalama F-ölçütü metriği sonucu elde edilerek yöntemin üstün başarısı ortaya konmuştur.

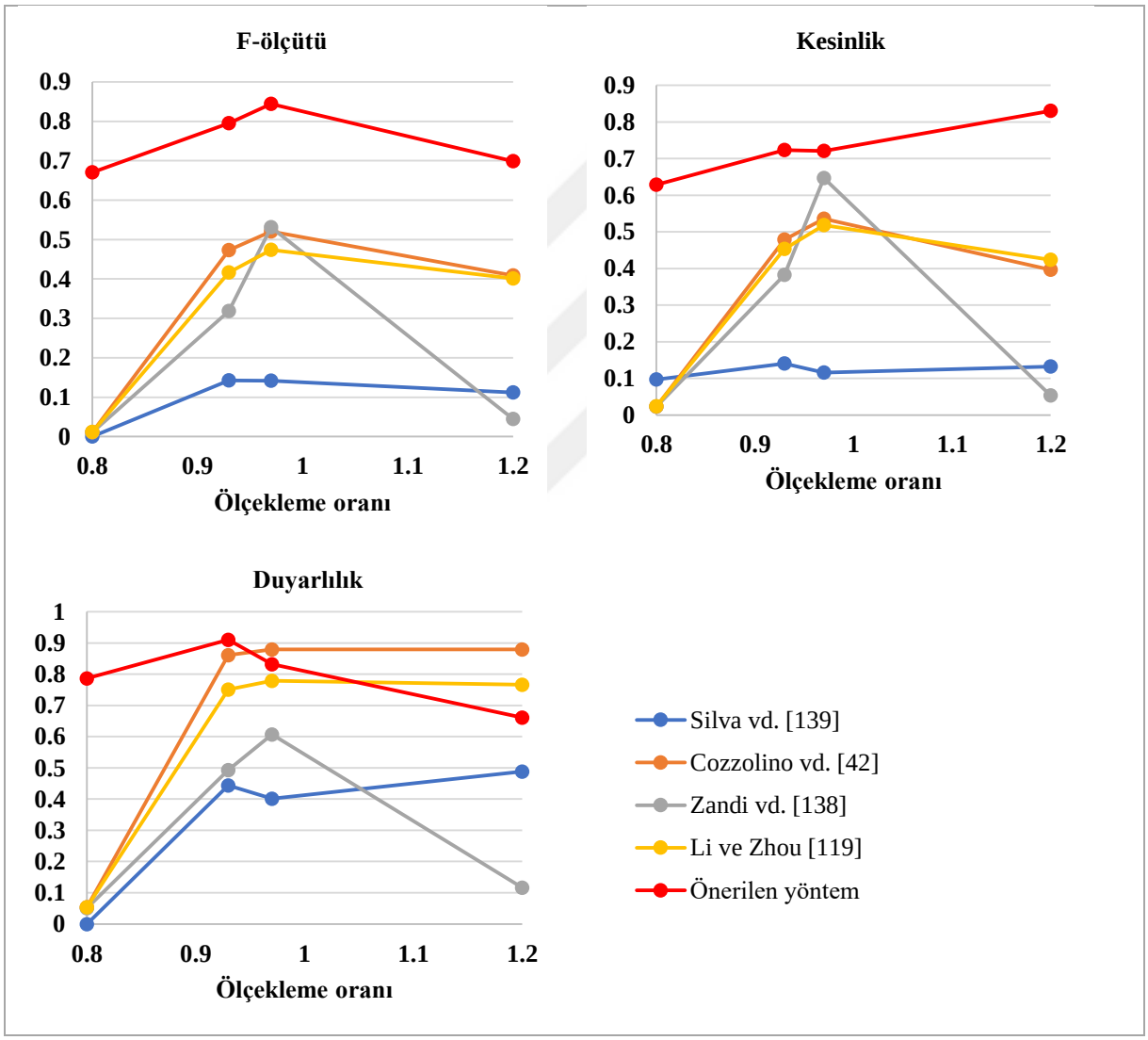


Şekil 3.26. Dönme atağı durumunda F-ölçütü, Kesinlik ve Duyarlılık metrikleri kullanılarak elde edilen ortalama sonuçların grafiksel gösterimi

Tablo 3.25. Büyük açı değerleri ile gerçekleştirilen dönme atağına maruz kalmış görüntülerden elde edilen ortalama sonuçlar

Yöntemler	F-ölçütü			Kesinlik			Duyarlılık		
	20°	75°	180°	20°	75°	180°	20°	75°	180°
Cozzolino vd. [42]	0,51	0,46	0,51	0,53	0,47	0,53	**0,86**	**0,89**	**0,89**
Silva vd. [139]	0,11	0,12	0,15	0,10	0,12	0,15	0,42	0,43	0,50
Zandi vd. [138]	0,60	0,60	0,76	**0,73**	**0,72**	**0,90**	0,66	0,68	0,73
Li ve Zhou [119]	0,43	0,43	0,50	0,47	0,47	0,56	0,76	0,79	0,77
Önerilen	**0,71**	**0,58**	**0,79**	0,67	0,56	0,73	0,78	0,62	0,87

Yapılan son testte hazırlanan verisetinde yer alan ölçekleme atağına maruz kalmış görüntüler kullanılarak performans değerlendirmesi yapılmıştır. Bunun için 0.8, 0.93, 0.97, 1.2 ve 2 oranında ölçekleme atağı uygulanmış 5x80=400 görüntü kullanılmıştır. Kesinlik, Duyarlılık ve F-ölçütü metriği kullanılarak elde edilen sonuçların ortalamaları Şekil 3.27'de yer alan grafiklerde sırası ile verilmiştir. Literatürde çözülemeyen sorun olarak ele alınan, büyük oranda ölçekleme durumlarındaki sahtecilik tespitinde önerilen yöntemin üstün başarısı açıkça görülmektedir.



Şekil 3.27. Ölçekleme atağı durumunda F-ölçütü, Kesinlik ve Duyarlılık metrikleri kullanılarak elde edilen ortalama sonuçların grafiksel gösterimi

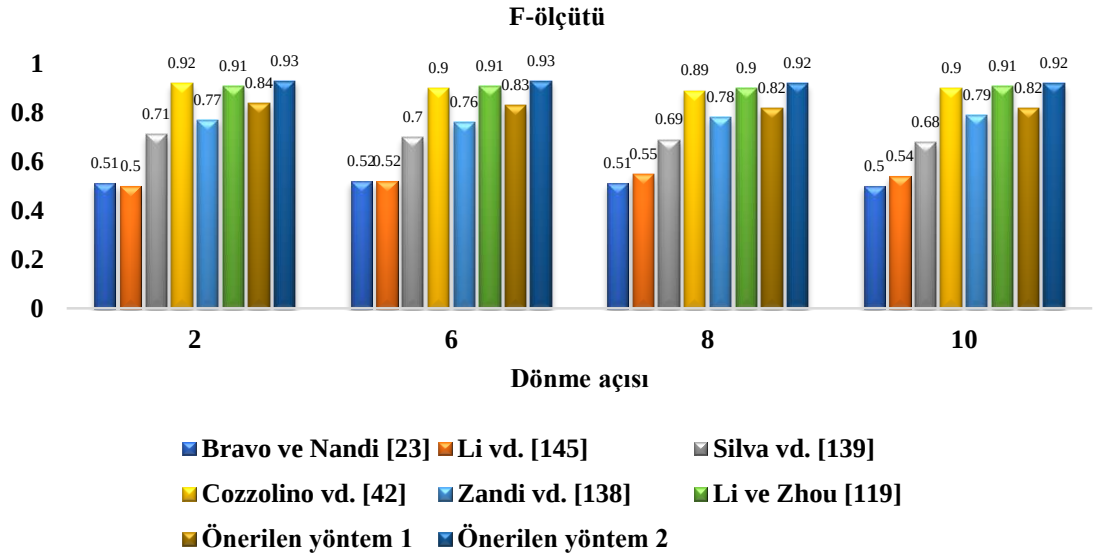
3.5. Tez Kapsamında Önerilen Yöntemlerin Karşılaştırmalı Analizi

Bu bölümde tez kapsamında önerilen iki özgün yöntemin birbirleri performans karşılaştırmaları yapılıp detaylı analizleri sunulacaktır. Karşılaştırmalarda literatürdeki çalışmaların da verisetleri üzerindeki ortalama sonuçlarına yer verilecektir. Bunun için ilk olarak GRIP verisetindeki 80 adet ataksız sahte görüntüler üzerinde performans değerlendirmesi yapılmıştır. Tablo 3.26'da yöntemlerin görüntü seviyesindeki ve piksel seviyesindeki analizlerine göre elde edilen ortalama F-ölçütü sonuçları verilmiştir. Önerilen iki yöntemin de referans yöntemlere göre düşük kontrasta sahip sahte bölgeleri içeren sahte görüntülerin oldukça fazla olduğu bu veri setinde üstün başarısı söylenebilir. Daha sonraki analizlerde görüntülerde atak olması durumundaki performans karşılaştırmasına yer verilecektir.

Tablo 3.26. GRIP Ataksız kopyala-yapıştır sahteciliği durumunda ortalama F-ölçütü değerleri

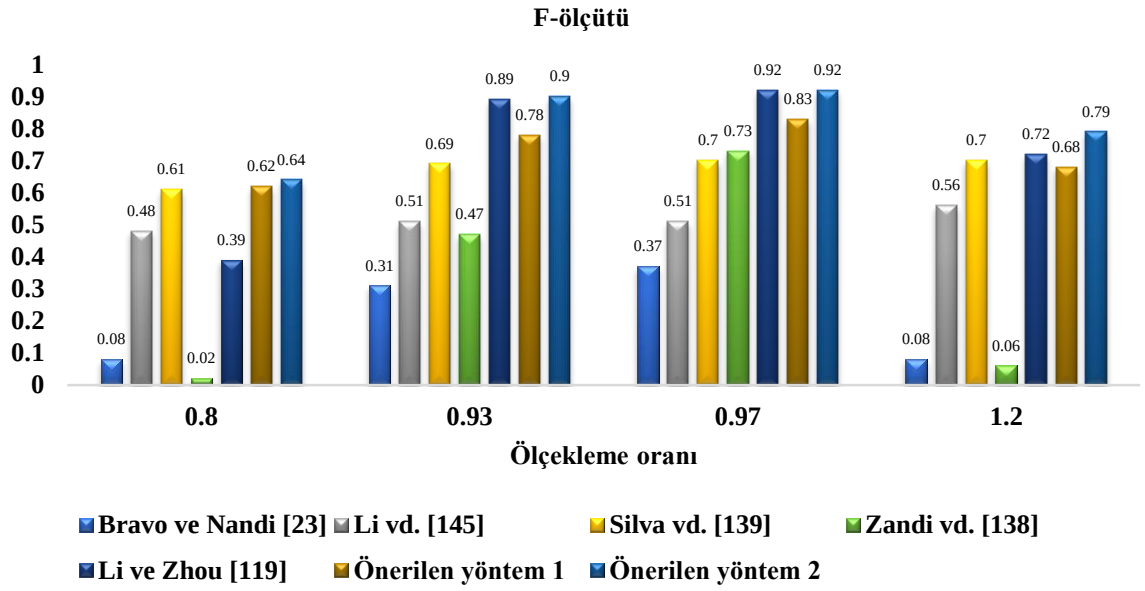
Yöntemler	Görüntü seviyesi	Piksel seviyesi
Ryu vd. [40]	0,94	0,89
Cozzolino vd. [42]	0,94	0,91
Silva vd. [139]	0,83	0,66
Amerini vd. [110]	0,67	0,44
Li vd. [144]	0,72	0,52
Pun vd. [147]	0,95	0,78
Zandi vd. [138]	0,86	0,85
Önerilen yöntem 1	0,97	0,94
Önerilen yöntem 2	0,96	0,92

GRIP verisetinde dönme atağı bulunan her birinden 80 adet olmak üzere sahte görüntülerden elde edilen ortalama F-ölçütü sonuçlarının bar grafiği gösterimi Şekil 3.28'de yer almaktadır. Buna göre ikinci önerilen yöntem ile daha yüksek F-ölçütü değerlerinin elde edildiği görülmektedir.



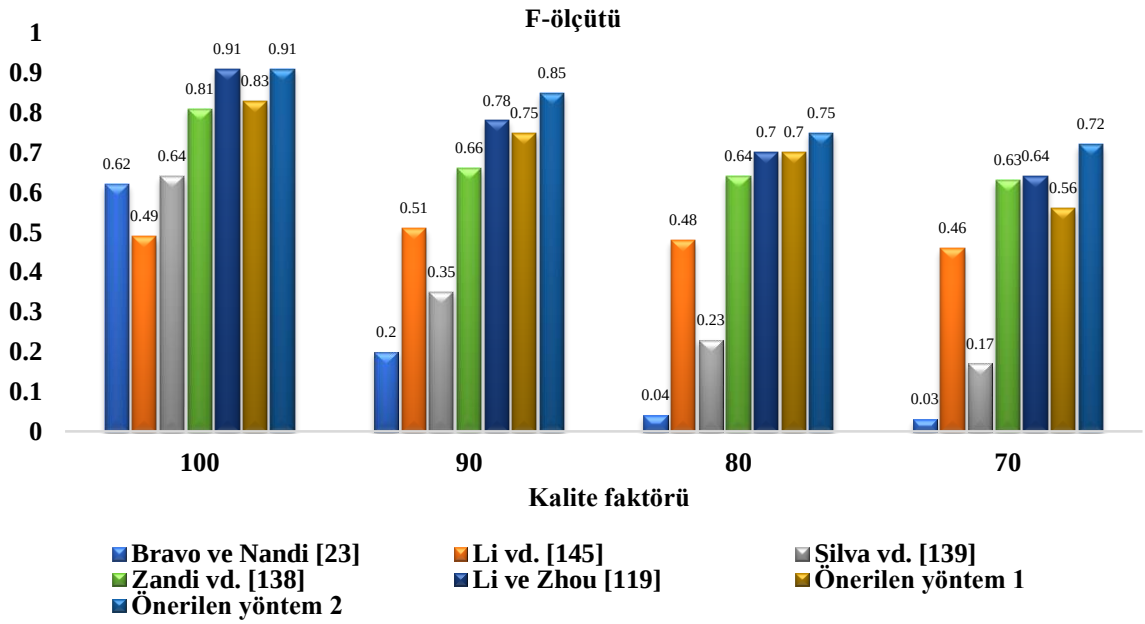
Şekil 3.28. Dönme atağı durumunda önerilen yöntemlerin karşılaştırmalı ortalama F-ölçütü sonuçlarının grafiksel gösterimi

Ölçekleme atağı altındaki performans karşılaştırmasında, GRIP verisetindeki görüntülerden elde edilen ortalama F-ölçütü sonuçları Şekil 3.29'da verilmiştir. Grafikten de görüldüğü gibi ikinci önerilen yöntem ile daha yüksek sonuçların elde edildiği söylenebilir.



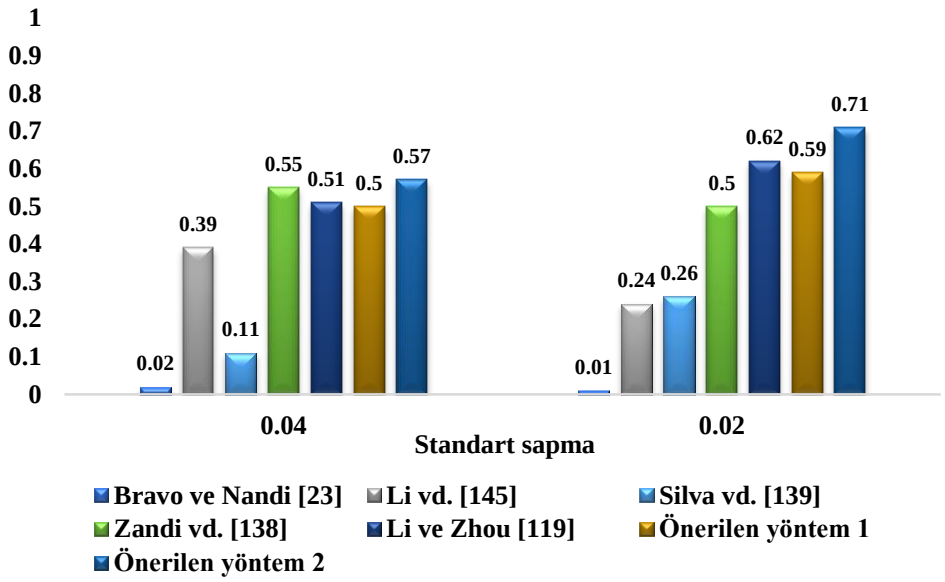
Şekil 3.29. Ölçekleme atağı durumunda önerilen yöntemlerin karşılaştırmalı ortalama F-ölçütü sonuçlarının grafiksel gösterimi

JPEG sıkıştırma atağı durumundaki karşılaştırmalı F-ölçütü sonuçlarının yer aldığı grafikler Şekil 3.30'da sunulmuştur. GRIP verisetindeki bu atak türüne maruz kalan görüntülerde ikinci önerilen yöntemin daha yüksek performansa sahip olduğu görülmektedir.



Şekil 3.30. JPEG sıkıştırma atağı durumunda önerilen yöntemlerin karşılaştırmalı ortalama F-ölçütü sonuçlarının grafiksel gösterimi

GRIP verisetindeki son karşılaştırmalı analizde gürültü ekleme atağı durumu ele alınmıştır. Verisetindeki standart sapma değeri 0.02 ve 0.04 için yapılan karşılaştırmada iki yöntem ile elde edilen ortalama F-ölçütü değerleri (%) Şekil 3.31'de verilmiştir. Standart sapma değeri $\sigma = 0.04$ olduğu durumda iki yöntemin sonuçları birbirine oldukça yakın olsa da iki değerlendirme için de ikinci önerilen yöntem ile daha başarılı sonuçlar elde edilmiştir.



Şekil 3.31. Gürültü ekleme atağı durumunda önerilen yöntemlerin karşılaştırmalı ortalama F-ölçütü sonuçlarının grafiksel gösterimi

Önerilen iki yöntemin karşılaştırmalı analizindeki ikinci kısımda CMH verisetindeki sonuçlar değerlendirilmiştir. CMH verisetindeki CMH1-CMH4 grubunda yer alan 108 görüntünün birleştirilmesi ile oluşturulan CMHAll grubunda elde edilen ortalama DPO, YPO ve Doğruluk metriklerinin sonuçları Tablo 3.27'de verilmiştir. DPO metriği ile elde edilen sonuçların birbirine oldukça yakın olmasına rağmen, ikinci yöntem ile daha yüksek YPO elde edilmesi sebebi ile Doğruluk metriği değeri daha düşük çıkmıştır. Bu verisetinde birinci yöntemin daha başarılı olduğu söylenebilir.

CMHAll grubundaki bütün sahte görüntülerin JPEG sıkıştırma atağına maruz bırakılması ile elde edilen CMHCompressed grubunda yer alan sahte görüntüler üzerinde yapılan karşılaştırmaya ilişkin sonuçlar Tablo 3.28'de verilmiştir. Bu gruptaki görüntüler üzerinde de birinci yöntem ile daha yüksek performans elde edildiği görülmektedir.

Önerilen yöntemlerin karşılaştırmasında son olarak, test görüntünün doğrulanması hususundaki çalışma zamanı karşılaştırmasına ilişkin bir değerlendirme gerçekleştirilmiştir. Bunun için GRIP verisetindeki 80 adet ataksız görüntüler kullanılarak çalışma zamanları hesaplanmıştır. Bir görüntü için ortalama çalışma zamanı süreleri Tablo 3.29'da sunulmuştur. Önerilen ikinci yöntemin, önerilen ilk yönteme göre daha kısa sürede görüntü doğrulaması gerçekleştirdiği görülmektedir. Referans yöntemlerde çalışma zamanı daha kısa olan yöntemler olsa da bu yöntemler performans açısından üstünlük gösterememiştir.

Tablo 3.27. Bütün verisetindeki ortalama sonuçlar (CMHALL)

Yöntemler	DPO	YPO	Doğruluk
Amerini vd. [108]	0,50	0,0019	0,75
Amerini vd. [110]	0,55	0,0023	0,77
Li vd. [145]	0,71	0,0263	0,84
Pun vd. [146]	0,70	0,0149	0,84
Silva vd. [139]	0,72	0,0122	0,85
Cozzolino vd. [42]	0,72	0,0023	0,85
Emam vd. [54]	0,64	0,0269	0,81
Zandi vd. [138]	0,46	0,0137	0,72
Jin vd. [169]	0,81	0,0400	0,88
Pun vd. [147]	0,81	0,0014	0,90
Li vd. [119]	0,56	0,0008	0,78
Vaishnavi ve Subashini [171]	0,80	0,0028	0,90
Huang ve Ciou [170]	0,91	0,0200	0,94
Önerilen yöntem1	0,95	0,0226	0,96
Önerilen Yöntem 2	0,93	0,0101	0,96

Tablo 3.28. JPEG sıkıştırma atağı uygulanmış bütün verisetindeki ortalama sonuçlar (CMH Compressed)

Yöntemler	DPO	YPO	Doğruluk
Amerini vd. [108]	0,35	0,0069	0,64
Amerini vd. [110]	0,48	0,0002	0,74
Li vd. [144]	0,54	0,0015	0,76
Pun vd. [147]	0,68	0,0369	0,82
Silva vd. [139]	0,68	**0,0002**	0,83
Cozzolino vd. [42]	0,49	0,0007	0,74
Emam vd. [54]	0,67	0,0205	0,82
Zandi vd. [138]	0,57	0,0398	0,76
Jin vd. [169]	0,45	0,0365	0,70
Pun vd. [147]	0,35	0,0139	0,66
Li vd. [119]	0,76	0,0098	0,87
Vaishnavi ve Subashini [171]	0,79	0,0052	0,89
Huang ve Ciou [170]	**0,68**	0,1220	**0,83**
Önerilen yöntem 1	0,89	0,0062	0,94
Önerilen yöntem 2	0,84	0,0384	0,90

Tablo 3.29. Bir görüntünün doğrulanması için ortalama çalışma zamanı

Yöntemler	Çalışma zamanı (sn)
Silva vd. [139]	9.4
Cozzolino vd. [140]	23.2
Zandi vd. [138]	116.7
Li ve Zhou [119]	19.2
Önerilen yöntem 1	114.58
Önerilen yöntem 2	99.78

Tez kapsamında önerilen iki yöntemin, iki veriseti üzerinde yapılan karşılaştırmasında, ikinci yöntemin GRIP veriseti üzerindeki bütün atak durumlarında daha başarılı olduğu görülmektedir. GRIP verisetinde düz bölgelerle gerçekleştirilen sahte görüntü sayısı CMH veri setine göre oldukça fazladır. İkinci yöntemin barındırdığı hem sahte bölge çıkarma aşaması hem de lokalizasyon aşaması GRIP veriseti üzerinde yöntemin daha etkin olmasını sağlamıştır. Çalışma zamanı açısından da ikinci yöntemin daha kısa sürede görüntü doğrulama işleminin gerçekleştirilmesi, bu yöntemin bu açıdan daha etkin olduğu söylenebilir.

Deneysel çalışmalardan elde edilen bulgularda da sunulduğu gibi tez kapsamında önerilen iki özgün yöntemin literatürdeki çalışmalara göre üstünlükleri sunulmuş, adli birimlerce kullanılabilir sistemler geliştirilmiştir.

Bu bölümde tez kapsamında önerilen ikinci yöntemin üç verisetinde de detaylı analizleri yapılarak literatürde yer alan popüler sahtecilik tespit yöntemleri ile karşılaştırmaları sunulmuştur.

4. SONUÇLAR

Teknolojideki hızlı gelişme sayesinde son zamanlarda, sayısal görüntülerin oluşturulması, iletilmesi ve depolanmasında büyük bir artış görülmektedir. Bununla birlikte, görüntü düzenleme araçlarının kolay kullanılabilirliği ve ücretsiz erişimli olması, görüntüler üzerinde uzmanlık gerektirmeden gerçekleştirilebilecek işlemleri mümkün hale getirmiştir. Yapılan işlemler görüntü kalitesini artırmak, netleştirmek gibi iyi niyetli olsa da kimi zaman da görüntünün içeriğinin değiştirilerek sahte hallerinin oluşturulması gibi kötü niyetli olmaktadır. Tıp, gazetecilik, hukuk gibi birçok önemli alanda başvurulan sayısal görüntülerin içeriklerinin değişime uğrayıp uğramadığının doğrulanması büyük önem arz etmektedir.

Son yıllarda sayısal görüntülerin doğrulanması ve değiştirilmediğinin ispatı için araştırmacılar tarafından çeşitli yöntemler geliştirilmektedir. Literatürde sayısal görüntü doğrulama yöntemleri aktif ve pasif yöntemler olmak üzere iki alt kategoride değerlendirilmektedir. Aktif doğrulama yöntemlerinden olan sayısal damga/imzada görüntüye gömülmüş özel bilginin kontrolü ile görüntü içeriğinin korunduğu doğrulanmaktadır. Genel amaçlı kullanılan görüntü oluşturma cihazları görüntüye damga/imza bilgisini yerleştirecek özellikte olmaması ve bu bilginin sonradan gömülmesinin de ek maliyet gerektirmesi durumları bu yöntemlerin dezavantajını oluşturmaktadır. Sayısal görüntülerin adli incelenmesinde en çok başvurulan pasif doğrulama yöntemleri ise görüntünün doğrulanmasında ek damga/imza bilgisine ihtiyaç duymamaktadır. Bu yöntemler görüntünün oluşturulmadan önce içeriğini koruma amaçlı bir önlem alınmaması durumunda dahi görüntü doğrulama işlemini gerçekleştirmektedirler. Bu amaçla görüntüden elde edilebilecek özellikler kullanılmakta, ek veri veya görüntünün özel donanımlı cihazlarla oluşturulma şartına ihtiyaç duymamaktadırlar. Bu avantajlarından dolayı pasif doğrulama yöntemleri, özellikle pratikte kullanılabilecek, pek çok durum için tek çözüm haline gelmiştir.

Literatürde pasif doğrulama yöntemlerinin kullanımı ile görüntü sahteciliklerinin tespitini yapabilen yöntemlerde doğrulama performansının yükseltilmesi, sahte görüntünün oluşturulmasında görüntü özelliğinden bağımsızlığın sağlanabilmesi, kullanılan eşik değerlerinin girdi görüntüsünden bağımsız bir şekilde dinamik olarak belirlenmesi, ön işlem ve son işlem ataklarına karşı dayanıklı olması, düz bölgelerle yapılan sahteciliklerin tespit edilebilmesi araştırmacıların iyileştirmeyi hedeflediği unsurlardır. Tez sürecinde tarafımızca da bu hedefler doğrultusunda önerilen sahtecilik tespit yöntemleri ve elde edilen sonuçlar aşağıdaki şekilde özetlenebilir:

1. Girdi görüntüsünün L*a*b* renk uzayındaki temsili ile literatürde ilk kez normalize edilmiş a* ve b* kanalının kullanımı ile görüntüye ait detayların belirgin hale gelmesi sayesinde daha fazla sayıda ve ayırt ediciliği yüksek SIFT anahtar noktaları elde edilebilmiştir. Elde edilen anahtar noktalarının eşleşmesi sonrası doğru eşleşmelerden faydalanarak şüpheli sahte bölgeler oluşturulmuştur. Şüpheli sahte bölgelerin lokalizasyon aşamasında DCT özelliklerden faydalanarak özgün bir dinamik eşik belirleme aşaması önerilmiştir. Yöntemin dönme, ölçekleme, JPEG sıkıştırma ve gürültü ekleme ataklarına karşı dayanıklılığı yapılan deneylerle gösterilmiştir. Literatürdeki popüler çalışmalardan [23, 40, 42, 54, 89, 108, 110, 119, 138, 139, 144, 147, 169, 170, 171] ile yapılan karşılaştırmalara göre önerilen yöntem ile daha yüksek doğruluk oranı ve daha düşük yanlış negatif değerlerinin elde edildiği deneysel çalışmalarla ispatlanmıştır.

2. Önerilen ikinci yöntemde, ilk olarak, düz bölgelerden de ayırt ediciliği yüksek SIFT anahtar noktalarının elde edilebilmesi için doku bilgisinin çıkarılması gerçekleştirilmiştir. Bunun için geometrik dönüşüm bağımsızlığı sağlayan LBPROT operatöründen faydalanıldı. Doku görüntüsünden elde edilen SIFT anahtar noktalarının eşleşmesi sonrası eşleşen anahtar noktalarının etrafında şüpheli sahte bölgeler belirlendi. Sahte bölgelerin sınırlarının netleştirilmesi aşamasında ise literatürde ilk tarafa Ciratefi tabanlı yaklaşımdan faydalanılmıştır. Önerilen lokalizasyon aşamasının iyileştirilmesi için son işlem aşamasının tamamlanması ile sahte bölgelerin işaretlenmesi tamamlanmıştır. Yöntemin dönme, ölçekleme, JPEG sıkıştırma ve gürültü ekleme ataklarına karşı dayanıklılığı yapılan deneylerle gösterilmiştir. Literatürdeki popüler çalışmalardan [40, 42, 54, 89, 108, 110, 119, 138, 139, 144, 145, 146, 147, 170, 171] ile yapılan karşılaştırmalara göre önerilen yöntem ile daha yüksek doğruluk oranı ve daha düşük yanlış negatif değerlerinin elde edildiği deneysel çalışmalarla ispatlanmıştır.

Saldırıdan bağımsız kopyala-yapıştır sahteciliği tespiti isimli 119E045 nolu 1001 TÜBİTAK projesi kapsamında da önerilen ikinci yöntemdeki şema kullanılarak “Kopyala-yapıştır sahteciliği tespiti sistemi” isimli bir yazılım geliştirilmiştir.

5. ÖNERİLER

Kullanım alanı ve önemi giderek artan sayısal görüntülerde gerçekleştirilen sahteciliklerin tespit edilmesi üzerine yapılan çalışmalar literatürde son yıllarda giderek artmaktadır. Sayısal görüntü sahteciliklerini tespit eden çalışmalardaki artışın devamlılığı ve henüz çözülemeyen problemlerin varlığı bu alandaki araştırma potansiyelinin yüksekliğini göstermektedir.

Literatürde önerilen yöntemler, sahte bölgenin hem dokusuz bölge özelliğine sahip olması durumunda hem de sahte görüntünün son işlem ataklarından JPEG sıkıştırma, gürültü ekleme atağı gibi atakları barındırması durumunda sahtecilikleri tespit edememektedir. Literatürdeki bu eksikliğin giderilebilmesi için öncelikle görüntüde bu atak durumlarının varlığının tespit edilebilmesi ve sonrasında bu atakların etkilerini azaltabilme üzerine araştırmalar yapılabilir. Bu atakların negatif etkilerinin azaltılması sonrası dokusuz bölgelerden daha etkin özelliklerin elde edilebilmesi üzerine çalışmalar gerçekleştirilebilir.

Blok tabanlı yöntemler sınıfında görüntünün blok bazlı değerlendirmesinde bloklardan elde edilecek özelliklerin derin öğrenme yöntemlerinden faydalanılabilir. Bu doğrultuda önerilecek çalışmaların küçük boyutlu bloklardan ayırt ediciliği yüksek özelliklerin elde edilmesi için ağ tasarımının bu duruma özgü olması gerekmektedir. Eğitim sırasında dönme, ölçekleme, JPEG sıkıştırma ve gürültü ekleme gibi atak durumlarının da dikkate alınması gerekir.

6. KAYNAKLAR

1. Qureshi, M. A. ve Deriche, M., A bibliography of pixel-based blind image forgery detection techniques, Image Communication, 39 (2015) 46–74.

2. Lian, S. ve Kanellopoulos D., Recent advances in multimedia information system security, Informatica, 33 (2009) 3–24.

3. Rey, C. ve Dugelay, J. L., A survey of watermarking algorithms for image authentication, EURASIP Journal on Applied Signal Processing, 2002, 6 (2002) 613–621.

4. Kundur, D. ve Hatzinakos, D., Digital watermarking for telltale tamper proofing and authentication, Proceedings of the IEEE, 87, 7 (1999) 1167–1180.

5. Om, A. ve Be, K., Passive detection of copy-move forgery in digital images: state-of-the-art, Forensic Science International, 231 (2013) 284–295.

6. Sadeghi, S., Dadkhah, S., Jalab, H.A., Mazzola, G. ve Uliyan, D., State of the art in passive digital image forgery detection: copy-move image forgery, Pattern Analysis and Applications, 21 (2018) 291–306.

7. Ng, T., T. ve Chang, S., F., A model for image splicing, 2004 International Conference on Image Processing, 2004 ICIP '04, Ekim 2004, Singapur, Bildiriler kitabı: 1169-1172.

8. Hsu, Y. F. ve Chang, S. F., Camera response functions for image forensics: an automatic algorithm for splicing detection, IEEE Transactions on Information Forensics and Security, 5, 4 (2010) 816-825.

9. Zhao, X., Li, S., Wang, S., Li, J. ve Yang, K., Optimal chroma-like channel design for passive color image splicing detection, EURASIP Journal on Advances in Signal Processing, 1 (2012) 240.

10. Zhang, Z., Zhou, Y., Kang, J. ve Ren, Y. Study of image splicing detection, Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, Eylül 2008, Şangay, Çin, Bildiriler kitabı: 1103-1110.

11. Qu, Z., Qiu, G. ve Huang, J., Detect digital image splicing with visual cues, International Workshop on Information Hiding, Haziran 2009, Berlin, Heidelberg, Bildiriler kitabı: 247-261.

12. Li, X., Jing, T. ve Li, X., Image splicing detection based on moment features and Hilbert-Huang Transform, 2010 IEEE International Conference on Information Theory and Information Security, Aralık 2010, Beijing, China, Bildiriler kitabı: 1127-1130.

13. Bhanu, B. ve Kumar, A., Copy-move forgery detection using segmentation, 2017, 11th International Conference on Intelligent Systems and Control, Ocak 2017, Coimbatore, Hindistan, Bildiriler kitabı: 224-228.

14. http://forensics.idealtest.org, 01.06.2021

15. https://www.scopus.com, 02.06.2021

16. Warif, N. B. A., Wahab, A.W.A, Idris, M.Y.I., Ramli, R., Salleh, R., Shamshirband, S. ve Choo, K.-K, R., Copy-move forgery detection: Survey, challenges and future directions, Journal of Network and Computer Applications, 75 (2016) 259-278.

17. Yao, H., Qiao, T., Tang, Z., Zhao, Y. ve Mao, H., Detecting copy-move forgery using non-negative matrix factorization, Multimedia Information Networking and Security (MINES 11), Kasım 2011, Shanghai, Çin, Bildiriler kitabı: 591-594.

18. Wu, Q., Wang, S. ve Zhang, X., Detection of image region-duplication with rotation and scaling tolerance, International Conference on Computational Collective Intelligence, Ekim 2010, New York, USA, Bildiriler kitabı: 100-108.

19. Muhammad, G., Al-Hammadi, M. H., Hussain, M., Mirza, A. M. ve Bebis, G., Copy-move image forgery detection method using steerable pyramid transform and texture descriptor, Eurocon 2013, Temmuz 2013, Zagreb, Hırvatistan, Bildiriler kitabı: 1586-1592.

20. Lin, S., D. ve Wu, T., An integrated technique for splicing and copy-move forgery image detection, 2011 4th International Congress on Image and Signal Processing Ekim 2011, Shanghai, Çin, Bildiriler kitabı: 1086-1090.

21. Hussain, M., Muhammad, G., Saleh, S., Q., Mirza, A., M. ve Bebis, G., Copy-move image forgery detection using multi-resolution Weber descriptors, 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, Kasım 2012, Sorento, İtalya, Bildiriler kitabı: 395-401.

22. Wandji, N., D., Xingming, S. ve Kue, M., F., Detection of copy-move forgery in digital images based on AKD, Journal of Computer Science, 10 (2013) 295-302.

23. Bravo-Solorio, S. ve Nandi, A., K., Automated detection, and localization of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Processing, 91, 8 (2011) 1759-1770.

24. Luo, W., Huang, J. ve Qiu, G., Robust detection of region-duplication forgery in digital image, 18th International Conference on Pattern Recognition (ICPR'06), Ağustos 2006, Hong Kong, Çin, Bildiriler kitabı: 746-749.

25. Yong, L., Meishan, H. ve Bogang, L., Robust evidence detection of copy-rotate- move forgery in image based on singular value decomposition, 14th International Conference On Information And Communications Security, Ekim 2012, Hong Kong, Çin, Bildiriler kitabı: 357-364.

26. Sadeghi, S., Jalab, H., A. ve Dadkhah, S., Efficient Copy-Move Forgery Detection for Digital Images, World Academy of Science, Engineering and Technology, 71 (2012).

27. Li, L., Li, S. ve Zhu, H., An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns, Journal of Information Hiding and Multimedia Signal Processing, 4, 1 (2013) 46–56.

28. Wang, J., Liu, G., Li, H., Dai, Y. ve Wang, Z., Detection of image region duplication forgery using model with circle block, International Conference on Multimedia Information Networking and Security, Kasım 2009, Wuhan, Çin, Bildiriler kitabı: 25-29.

29. Liu, G., Wang, J., Lian, S. ve Wang, Z., A passive image authentication scheme for detecting region-duplication forgery with rotation, Journal of Network and Computer Applications, 34, 5 (2011) 1557-1565.

30. Li, L., Li, S., Zhu, H. ve Wu, X., Detecting copy-move forgery under affine transforms for image forensics, Computers and Electrical Engineering, 40, 6 (2014) 1951-1962.

31. Fridrich, A. J., Soukal, B. D. ve Lukáš, A. J., Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop (DFRWS), 2003, 1-10.

32. Popescu, A. ve Farid, H., Exposing Digital Forgeries by Detecting Duplicated Image Regions, Teknik Rapor, TR2004-515, Dartmount Collage, 2004.

33. Huang, Y., Lu, W., Sun, W. ve Long, D., Improved DCT-based detection of copy-move forgery in images, Forensic Science International, 206, 1 (2011) 178-184.

34. Mahdian, B. ve Saic, S., Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants, Forensic Science and International, 171 (2007) 180–189.

35. Kang, X. ve Wei, S., Identifying tampered regions using singular value decomposition in digital image forensics, International Conference on Computer Science and Software Engineering, Aralık 2008, Washington, United States, Bildiriler kitabı: 926–930.

36. Bayram, S., Sencar, H. T. ve Memon, N., An Efficient and Robust Method for Detecting Copy-Move Forgery, IEEE International Conference on Acoustics, Speech and Signal Processing, Nisan 2009, New York, Bildiriler kitabı: 1053 – 1056.

37. Kakar, P. ve Sudha, N., Exposing postprocessed copy–paste forgeries through transform-invariant features, IEEE Transactions on Information Forensics and Security, 7,3 (2012) 1018–1028.

38. Wu, Q., Wang, S. ve Zhang, X., Log-polar based scheme for revealing duplicated regions in digital images, IEEE Signal Processing and Letters 18,10 (2011) 559–562.

39. Muhammada, G., Hussain, M. ve Bebis, G., Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform, Digital Investigation, 9,1 (2012) 49–57.

40. Ryu, S., Kirchner, M, Lee, M. ve Lee, H., Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments, IEEE Transaction on Information Forensics and Security, 8, 8 (2013) 1355–1370.

41. Cozzolino, D., Poggi, G. ve Verdoliva, L., Copy-move forgery detection based on PatchMatch, 2014 IEEE International Conference on Image Processing (ICIP), Ekim 2014, Paris, Fransa, Bildiriler kitabı: 5312-5316.

42. Cozzolino, D., Poggi, G. ve Verdoliva L., Efficient Dense-Field Copy–Move Forgery Detection, IEEE Transactions on Information Forensics and Security, 10, 11 (2015) 2284-2297.

43. Lee, J., Chang, C. ve Chen, W., Detection of Copy–Move Image Forgery Using Histogram of Oriented Gradients, Information Sciences, 321 (2015) 250–262.

44. Fadl, S.M., Semary, N.A., Robust Copy–Move forgery revealing in digital images using polar coordinate system, Neurocomputing, 265 (2017) 57-65.

45. Priyanka, Singh, G. ve Singh, K., An improved block-based copy-move forgery detection technique, Multimedia Tools and Applications, 79 (2020) 13011–1303.

46. Zhong, J., L. ve Pun, C., M., Two-pass hashing feature representation and searching method for copy move forgery detection, Information Sciences, 512 (2020) 675-692.

47. Pun, C.M ve Chung J.L., A two-stage localization for copy-move forgery detection, Information Sciences, 463–464 (2018) 33–55.

48. Lee, J.-C., Copy-Move Image Forgery Detection Based on Gabor Magnitude, Journal of Visual Communication and Image Representation, 31 (2015) 320–334.

49. Bi, X., Pun, C. ve Yuan, X., Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy-Move Forgery Detection, Information Science, 345 (2016) 226-242.

50. Wang, J., Liu, G., Li, H., Dai, Y. ve Wang, Z., Detection of Image Region Duplication Forgery Using Model with Circle Block, Intl. Conference on Multimedia Information Networking and Security, Kasım 2009, Hubei, Bildiriler Kitabı: 25–29.

51. Wu, Q., Wang, S. ve X. Zhang, Detection of image region-duplication with rotation and scaling tolerance, International Conference on Computational Collective Intelligence, Kasım 2010, Kaohsiung, Taiwan, Bildiriler kitabı: 100-108.

52. Liu, G., Wang, J., Lian, S. ve Wang, Z., A passive image authentication scheme for detecting region-duplication forgery with rotation, Journal of Network and Computer Applications, 34, 5 (2011) 1557–1565.

53. Li, L., Li, S. ve Zhu, H., An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns, Journal of Information Hiding and Multimedia Signal Processing, 4,1 (2013) 46–56.

54. Emam, M., Han, Q. ve Niu, X., PCET based copy-move forgery detection in images under geometric transforms, Multimedia Tools and Applications, 75, 18 (2016) 11513–11527.

55. Wang, Xy., Liu, Yn., Xu, H., Wang, P. ve Yang, H.Y., Robust copy–move forgery detection using quaternion exponent moments, Pattern Analysis and Applications, 21 (2018) 451–467.

56. Wang, Y., Kang, X. ve Chen, Y., Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures, Journal of Information Security and Applications, 54, (2020) 102536.

57. Cao, Y., Gao, T., Fan, L. ve Yang, Q., A robust detection algorithm for copy-move forgery in digital images, Forensic Science and International, 214 (2012) 33–43.

58. Shao, H., Yu, T., Xu, M. ve Cui, W., Image region duplication detection based on circular window expansion and phase correlation, Forensic Science and International, 222 (2012) 71–82.

59. Yang, B., Sun, X., Chen, X., Zhang, J. ve Li, X., An efficient forensic method for copy-move forgery detection based on DWT-FWHT, Radioengineering. 22, 4 (2013) 1098–1105.

60. Zhang, J., Feng, Z. ve Su, Y., A new approach for detecting copy-move forgery in digital images, 11th International Conference on Communication Systems, Kasım 2008, Singapore, Bildiriler kitabı: 362–366.

61. Muhammad, G., Hussain, M. ve Bebis, G., Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform, Digital Investigation, 9 (2012) 49–57

62. Peng, F., Nie, Y.Y. ve Long, M., A complete passive blind image copy-move forensics scheme based on compound statistics features. Forensic Science and International, 212 (2011) 21–25.

63. Warif, N. B. A., Wahab, A.W.A, Idris, M.Y.I., Ramli, R., Salleh, R., Shamshirband, S. ve Choo, K.-K, R., Copy-move forgery detection: Survey, challenges and future directions, Journal of Network and Computer Applications, 75 (2016) 259-278.

64. Luo, W., Huang, J. ve Qiu, G., Robust detection of region-duplication forgery in digital image, 18th International Conference on. IEEE, Ağustos 2006, Hong Kong, Bildiriler kitabı: 746-749.

65. Bravo-Solorio, S., Nandi, A. Exposing duplicated regions affected by reflection, rotation, and scaling, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Mayıs 2011, Prag, Çek Cumhuriyeti, Bildiriler kitabı: 1880–1883.

66. Gharibi, F., RavanJamjah, J., Akhlaghian, F., Azami, B., Z. ve Alirezaie, J., Robust detection of copy-move forgery using texture features, 19th Iranian Conference on Electrical Engineering, Mayıs 2011, Tahran, İran, Bildiriler kitabı: 1-4.

67. Hsu, H., C. ve Wang, M., S., Detection of copy-move forgery image using Gabor descriptor, Anti-Counterfeiting, International Conference on Security, and Identification, Ağustos 2012, Taipei, Taiwan, Bildiriler kitabı: 1-4.

68. Davarzani, R., Yaghmaie, K., Mozaffari, S. ve Tapak, M., Copy-move forgery detection using multiresolution local binary patterns. Forensic Science and International, 231 (2013) 61–72.

69. Ustubioglu, B., Baykal, E., Muzaffer, G. ve Ulutas, G., Blur Invariant Image Forgery Detection Method Using Local Phase Quantization, Journal of Energy and Power Engineering, 10, 6 (2016) 358-363.

70. Hu, M.-K., Visual Pattern Recognition by Moment Invariants, IRE Transactions on Information Theory, 8, 2 (1962) 179–187.

71. Bilgehan, M., Ulutas G. ve Ulutas, M., Detection of Copy-Move Forgery Using Krawtchouk Moment, 8th International Conference on Electrical and Electronics Engineering, Kasım 2013, Bursa, Türkiye, Bildiriler kitabı: 311–314.

72. Ryu, S.J., Lee, M.J., Lee, H.K., Detection of copy-rotate-move forgery using Zernike moments, 12th International Conference, Mayıs 2010, Calgary, AB, Canada, Bildiriler kitabı: 51–65.

73. Ryu, S.J., Kirchner, M., Lee, M.J. ve Lee, H.K., Rotation invariant localization of duplicated image regions based on Zernike moments, IEEE Transactions on Information Forensics and Security, 8,8 (2013) 1355–1370.

74. Chen, C. C., Wang, H., ve Lin, C. S., An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection, Multimedia Tools and Applications, 76,24 (2017) 26503-26522.

75. Li, W. ve Yu, N., Rotation robust detection of copy-move forgery, International Conference on Image Processing, ICIP, Eylül 2010, Bildiriler kitabı: 2113–2116.

76. Li, L., Li, S., Wang, J., Copy-move forgery detection based on PHT, World Congr. Inf. Commun. Technol. WICT, Ekim 2012, Bildiriler kitabı: 1061–1065.

77. Li, Y., Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching, Forensic Science and International, 224 (2013) 59–67.

78. Ting, Z. ve Rang-Ding, W., Copy-move forgery detection based on SVD in digital image, 2009 2nd International Congress on Image and Signal Processing, Ekim 2009, Tianjin, Çin, Bildiriler kitabı: 1–4.

79. Zhao, J., Detection of copy-move forgery based on one improved LLE method, Mart 2010, Şangay, Çin, Bildiriler kitabı: 547–550.

80. Meena, K. B. ve Tyagi, V., A copy-move image forgery detection technique based on tetrolet transform, Journal of Information Security and Applications, 52 (2020) 102481.

81. Zhong, J., L. ve Pun, C., M., Two-pass hashing feature representation and searching method for copy move forgery detection, Information Sciences, 512 (2020) 675-692.

82. Priyanka, Singh, G. ve Singh, K., An improved block-based copy-move forgery detection technique, Multimedia Tools and Applications, 79 (2020) 13011–13035.

83. Wang, Y., Kang, X. ve Chen, Y., Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures, Journal of Information Security and Applications, 54 (2020) 102536.

84. Myna, A. N., Venkateshmurthy, M. G. ve Patil, C. G., Detection of region duplication forgery in digital images using wavelet and log-polar mapping, International Conference on Computational Intelligence and Multimedia Applications, Aralık 2007, Sivakasi, India, Bildiriler kitabı: 371-377.

85. Zhao, J. ve Guo, J., Passive forensics for copy-move image forgery using a method based on AKD and SVD, Forensic Science International, 233,1 (2013) 158-166.

86. Lin, H. J., Wang, C., W. ve Kao, Y., T., Fast copy-move forgery detection, WSEAS Transactions on Signal Processing, 5, 5 (2009) 188-197.

87. Sekeh, M., A., Maarof, M., A., Rohani, M., F. ve Motiei, M., Sequential straightforward clustering for local image block matching, World Academy of Science, Engineering and Technology, 50 (2011) 774-778.

88. Ardizzone, E., Bruno, A. ve Mazzola, G., Copy-move forgery detection via texture description, Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, Ekim 2010, Bildiriler kitabı: 59-64.

89. Christlein, V., Riess, C. ve Angelopoulou, E., On rotation invariance in copy-move forgery detection, IEEE International Workshop on Information Forensics and Security, Aralık 2010, Seattle, WA, USA, Bildiriler kitabı: 1-6.

90. Wang, H. ve Wang, H., Perceptual Hashing-based image copy move forgery detection, Security and Communication Networks, 2018 (2018).

91. Liu, G., Wang, J., Lian, S. ve Wang, Z., A passive image authentication scheme for detecting region-duplication forgery with rotation, Journal of Network and Computer Applications, 34,5 (2011) 1557-1565.

92. Zhong, L. ve Xu, W., A robust image copy-move forgery detection based on mixed moments, IEEE International Conference on.Software Engineering and Service Science, Aralık 2013, Beijing, Bildiriler kitabı: 381-384.

93. Wang, J., Liu, G., Li, H., Dai, Y. ve Wang, Z., Detection of image region duplication forgery using model with circle block, International Conference on Multimedia Information Networking and Security, Kasım 2009, Wuhan, China, Bildiriler kitabı: 25-29.

94. Singh, V., K. ve Tripathi, R., C., Fast and efficient region duplication detection in digital images using sub-blocking method, International Journal of Advanced Science and Technology, 35 (2011) 93-102.

95. Chaitawittanun, N. Detection of copy-move forgery by clustering technique, International Conference of Computer Science & Information Technology, 50, 6 (2012), 3948-3959.

96. Bravo-Solorio, S. ve Nandi, A.K., Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Processing, 91,8 (2011) 1759–1770.

97. Khan, E., S. ve Kulkarni, E., A., An efficient method for detection of copy-move forgery using discrete wavelet transform, International Journal on Computer Science and Engineering, 2,5 (2010) 1801–1806.

98. Nguyen, H. C. ve Katzenbeisser, S., Detection of copy-move forgery in digital images using radon transformation and phase correlation, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Temmuz 2012, Piraeus-Athens, Greece, Bildiriler kitabı: 134-137.

99. Zhao, J. ve Guo, J., Passive forensics for copy-move image forgery using a method based on AKD and SVD, Forensic Science International, 233, 1 (2013) 158-166.

100. Bashar, M., Noda, K., Ohnishi, N. ve Mori, K., Exploring duplicated regions in natural images, IEEE Transactions on Image Processing, 99 (2010) 1-40.

101. Ouyang, J., Liu, Y. ve Liao, M. Robust copy-move forgery detection method using pyramid model and Zernike moments, Multimedia Tools and Applications, 78 (2019) 10207-10225.

102. Li, G., Wu, Q., Tu, D. ve Sun, S., A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, Multimedia and Expo, IEEE International Conference on IEEE, Temmuz 2007, Beijing, Çin, Bildirileri kitabı: 1750-1753.

103. Wang, T., Tang, J., Zhao, W., Xu, Q. ve Luo, B., Blind detection of copy-move forgery based on multi-scale autoconvolution invariants, Chinese Conference on Pattern Recognition, Eylül 2012, Heidelberg, Bildirileri kitabı: 438-446.

104. Kang, L. ve Cheng, X., Copy-move forgery detection in digital image, Proceedings of the 3rd International Congress on Image and Signal Processing (CISP ‟10), 2010, Yantai, Çin, Bildiriler kitabı: 2419–2421.

105. Muhammad, N., Hussain, M., Muhamad, G. ve Bebis, G., A non-intrusive method for copy-move forgery detection, Advances in Visual Computing, Ağustos 2011, Berlin, Almanya, Bildirileri kitabı: 516-525.

106. Huang, H., Guo, W. ve Zhang, Y. Detection of copy-move forgery in digital images using SIFT algorithm, Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA), Aralık 2008, Wuhan, China, Bildiriler kitabı: 272–276.

107. Pan, X. ve Lyu, S., Detecting image region duplication using SIFT features, 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, Mart 2010, Dallas USA, Bildiriler kitabı: 1-4.

108. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. D. ve Serra, G., A sift-based forensic method for copy-move attack detection and transformation recovery, IEEE Transactions on Information Forensics and Security, 6,3 (2011) 1099–1110.

109. Shivakumar, B.L. ve Baboo, C., Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors, International Journal of Computer Applications, 27,3 (2011), 1-9.

110. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Tongo, L.D. ve Serra, G., Copy-move forgery detection and localization by means of robust clustering with J-Linkage, Signal Process Image Commun., 28, 6 (2013) 659– 669.

111. Yadav, N. ve Kapdi, R., Copy move forgery detection using SIFT and GMM, NUiCONE, Kasım 2015, Ahmedabad, Hindistan, Bildirileri kitabı: 1–4.

112. Shi Wenchang, Zhao Fei, Qin Bo, Liang Bin, Improving image copy-move forgery detection with particle swarm optimization techniques, China Communications 13(1), 2016, 139 – 149.

113. Shahroudnejad, A. ve Rahmati, M., Copy-move forgery detection in digital images using affine-SIFT, ICSPIS, Aralık 2016, Tehran, İran, Bildirileri kitabı: 1–5.

114. Jin, G. ve Wan, X., An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage, Signal Process., Image Commun., 57 (2017) 113–125.

115. Muzaffer, G. ve Ulutas, G., A fast and effective digital image copy move forgery detection with binarized SIFT, International Conference on TSP, Temmuz 2017, İspanya, Bildiriler kitabı: 595–598.

116. Resmi, M.R. ve Vishnukumar, S., A novel segmentation based copy-move forgery detection in digital images, NetACT, Temmuz 2017, Thiruvanthapuram, Hindistan, Bildirileri kitabı: 346–350.

117. Das, T., Hasan, R., Azam, M.R. ve Uddin, J., A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform, in Proc. IC4ME2, Şubat 2018, Rajshahi, Bangladesh, Bildirileri kitabı: 1–4.

118. Alberry, H. A., Hegazy, A. A. ve Salama, G.I., A fast SIFT based method for copy move forgery detection, Future Computing and Informatics Journal, 3, 2 (2018) 159–165.

119. Li, Y. ve Zhou, J., Fast and effective image copy-move forgery detection via hierarchical feature point matching, IEEE Trans. Inf. Forensics Security, 14, 5 (2019) 1307–1322.

120. Chen, C.-C., Lu, W.-Y. ve Chou, C., H., 'Rotational copy-move forgery detection using SIFT and region growing strategies', Multimedia Tools and Applications, 78 (2019) 18293–18308.

121. Chen, H., Yang, X., Lyu, Y., Copy-Move Forgery detection based on keypoint clustering and similar neighborhood search algorithm, IEEE Access, 8 (2020) 36863 – 36875.

122. Xu, B., Wang, J., Liu, G., Li, H. ve Dai, Y., Image copy-move forgery detection based on SURF, Intlernational Conference on Multimedia Information Networking and Security (MINES), 2010, Bildirileri kitabı: 889–892.

123. Shivakumar, B.L. ve Santhosh Baboo, S., Detection of Region Duplication Forgery in Digital Images Using SURF, International Journal of Computer Science Issues, 8, 4 (2011) 1-10.

124. Kiruthika, K., Devi, S., Mahalakshmi, K. Vijayalakshmi, Detecting Multiple Copies of Copy-Move Forgery Based on SURF, ISSN (Online), 2319 – 8753, 2014, 2276-2281.

125. Al-Hammadi, M.M. ve Emmanuel, S., Improving SURF Based Copy-Move Forgery Detection Using Super Resolution, IEEE International Symposium on Multimedia, , San Jose, Aralık 2016, CA, USA, Bildirileri kitabı: 341-344.

126. Wang, X., Li, S., Liu, Y. Nu, Y., Yang, H. ve Zhou, Z., A new keypoint-based copy-move forgery detection for small smooth regions, Multimedia Tools and Applications, 79 (2017) 23353–23382.

127. Muzaffer, G. ve Ulutas, G. Detection of copy move forgery based on color SURF, Journal of the Faculty of Engineering and Architecture of Gazi University, 34, 3 (2019) 1539-1548.

128. G. Muzaffer, G. Ulutaş ve E. Gedikli, PSO and SURF based digital image forgery detection, 2017 International Conference on Computer Science and Engineering (UBMK), Ekim 2017, Antalya, Türkiye, Bildirileri kitabı: 688-692.

129. Zhu, Y., Shen, X. ve Chen, H., Copy-move forgery detection based on scaled ORB, Multimedia Tools and Applications, 75 (2015) 3221–3233.

130. Muzaffer, G., Makul, O ve Ulutas, G., Copy Move Forgery Detection Using Gabor Filter and ORB, International Conference On Image Processing, Production And Computer Science, Mart 2016, Londra, İngiltere, Bildirileri kitabı: 23-30.

131. Ulutas, G. ve Muzaffer, G., A new copy move forgery detection method resistant to object removal forgery, Mathematical Problems in Engineering, 2016 (2016), 1-19.

132. Yang, H. Y., Qi, S., R., Niu, Y., Niu, P. P. ve Wang, X. Y., Copy-move forgery detection based on adaptive keypoints extraction and matching, Multimedia Tools and Applications, 78 (2019) 34585–34612, 2019.

133. Pandey, R.C., Singh, S.K., Shukla, K. K. ve Agrawal, R., Fast and robust passive copy-move forgery detection using SURF and SIFT image features, 9th International Conference on Industrial and Information Systems, 2014, Bildirileri kitabı: 1-6.

134. Ardizzone, E. Bruno, A. ve Mazzola, G., Copy–Move Forgery Detection by Matching Triangles of Keypoints, IEEE Transactions on Information Forensics and Security, 10, 10 (2015) 2084-2094.

135. Yang, F., Li, J., Lu, W. ve Weng, J., Copy-move forgery detection based on hybrid features, Engineering Applications of Artificial Intelligence, 59 (2017) 73-83.

136. Wang, C., Zhang, Z. ve Zhou, X., An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features, Symmetry, 10 (2018) 706.

137. Prakash, C.S., Panzade, P.P., Om, H. Ve Maheshkar, S., Detection of copy-move forgery using AKAZE and SIFT keypoint extraction, Multimed Tools and Application, 78 (2019) 23535–23558.

138. Zandi, M., Mahmoudi-Aznaveh A. ve Talebpour, A., Iterative Copy -Move Forgery Detection Based on a New Interest Point Detector, Transactions on Information Forensics and Security, 11, 11 (2016) 2499-2512.

139. Silva, E., Carvalho, T., Ferreira, A.ve Rocha, A., Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes, J. Vis. Commun. Image Representation 29 (2015) 16–32.

140. Panzade, P.P., Prakash, C.S. ve Maheshkar, S., Copy-move forgery detection by using HSV preprocessing and keypoint extraction, 2016 International Conference on Parallel, Distributed and Grid Computing (PDGC), Aralık 2016, Waknaghat, India, Bildirileri kitabı: 264-269.

141. Lowe, D., G., Distinctive image features from scale-invariant keypoints, International Journal of Computer Vision, 60, 2 (2004) 91-110.

142. Bay, H., Ess, A., Tuytelaars, T. ve Van Gool, L., Speeded-up robust features (SURF), Computer Vision and Image Understanding, 110, 3 (2008) 346-359.

143. Tralic,D., Zupancic, I., Grgic, S., ve Grgic, M., Comofod 2014; new database for copy-move forgery detection, 2013 55th International Symposium ELMAR, Kasım 2013, Bildirileri kitabı: 49-54.

144. Wang, X., Y., Wang, C., Wang, L., Jiao, L.X., Yang, H. Y. ve Niu, P. P., A fast and high accurate image copy-move forgery detection approach, Multidimensional Systems and Signal Processing, 31 (2020) 857–883,

145. Park, C.S. ve Choeh, J.Y., Fast and robust copy-move forgery detection based on scale-space representation, Multimedia Tools Application, 77 (2018) 16795–16811.

146. Li, J., Li, X., Bin, Y. ve Sun, X., Segmentation-based image copy-move forgery detection scheme, IEEE Transactions on Information Forensics and Security, 10, 3 (2015) 507–518.

147. Pun, C.-M., Yuan, X.-C. ve Bi, X.L., Image forgery detection using adaptive oversegmentation and feature points matching, IEEE Transactions on Information Forensics and Security, 10, 8 (2015) 1705–1716.

148. Lin, C., Lu, W., Sun, W., Zeng, J., Xu, T. ve Lai J.H., Region duplication detection based on image segmentation and keypoint contexts, Multimedia Tools and Applications, 77 (2018) 14241–14258.

149. Wang, C., Zhang, Z., Li, Q. ve Zhou, X. An image copy-move forgery detection method based on SURF and PCET, IEEE Access, 7 (2019) 170032-170047.

150. Liu, Y., Wang, H., Chen, Y., Wu, H. ve Wang, H., A passive forensic scheme for copy-move forgery based on superpixel segmentation and K-means clustering, Multimedia Tools and Applications, 79 (2020) 477–500.

151. Sun, Y., Ni. R. ve Zhao, Y., Nonoverlapping Blocks Based Copy-Move Forgery Detection, Security and Communication Networks, 2018 (2018) 1-12.

152. Meena, K. B. ve Tyagi, V., A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms, Multimedia Tools and Applications, 79 (2020) 8197–8212.

153. Park, J. Y., Kang, T., A., Moon, Y., H., Eom, K., Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram, Symmetry, 12,4 (2020) 492.

154. Yoon, H., Han, Y. ve Hahn, H., Image Contrast Enhancement Based Sub- Histogram Equalization Technique without Over-Equalization Noise, International Journal of Computer Science and Engineering, 3, 2 (2009) 132-138.

155. Pizer, S.M., Amburn, E. P., Austin, J. D. ve Zuidelverd, K., Adaptive Histogram Equalization and Its Variations. Computer Vision, Graphics, and Image Processing, 39 (1987) 355-368.

156. Zuiderveld, K., Contrast Limited Adaptive Histogram Equalization, P. Heckbert: Graphics Gems IV, Academic Press 1994.

157. Reza, M.A., Realization of The Contrast Limited Adaptive Histogram Equaliation (CLAHE) for Real-Time Image Enhancement, Journal of VLSI Signal Processing, 38 (2004) 35–44.

158. Ahmed, N., Natarajan, T. ve Rao, K. R., 1974, Discrete cosine transform, IEEE Trans. Comput., C-32, 90-93.

159. Fischler, M.A. ve Bolles, R.C., Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography, Comm. ACM. 24 (6), Haziran 1981, Bildirileri kitabı: 381-395.

160. Yılmaz İ., Renk uzayları ve dönüşüm algoritmaları, Doktora Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya, 2002.

161. Noboru, O ve Robertson, A. R., Standard and Supplementary Illuminants. Colorimetry, Wiley, Kasım 2015, Bildirileri kitabı: 92–96.

162. Tahaoglu, G., Ulutas, G., Ustubioglu, B., Nabiyev, Vasif, Improved copy move forgery detection method via L*a*b* color space and enhanced localization technique. Multimedia Tools Application 80 (2021) 23419–23456.

163. Tahaoglu, G., Ulutas, G., Ustubioglu, B., Ulutas, M. ve Nabiyev, V, Ciratefi based copy move forgery detection on digital images, Multimedia Tools and Application 1 (2021) 1-14.

164. Manohar, M. ve Ramapriyan, H.K., Connected Component Labeling of Binary Images on a Mesh Connected Massively Parallel Processor. Computer Vision, Graphics, and Image Processing, 45 (1989) 133-149.

165. Ojala, T., Pietikäinen, M. ve Harwood, D., Performance evaluation of texture measures with classification based on Kullback discrimination of distributions, 12th IAPR International Conference on Pattern Recognition,1994, Bildirileri kitabı 1: 582- 585.

166. Ojala, T., Pietikainen, M. ve Maenpaa, T., Multiresolution gray-scale and rotation invariant texture classification with local binary patterns, IEEE Transactions On Pattern Analysis And Machine İntelligence, 24,7 (2002) 971-987.

167. Araújo, S.A. ve Kim, H.Y., Ciratefi: An RST-Invariant Template Matching with Extension to Color Images, Integrated Computer-Aided Engineering, 18, 1(2011) 75-90.

168. Christlein, V., Riess, C., Jordan, J., Riess, C. ve Angelopoulou, E., An Evaluation of Popular Copy-Move Forgery Detection Approaches, IEEE Transactions on Information Forensics and Security, 7, 6 (2012) 1841-1854.

169. Jin, G. ve Wan, X., An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimized J-Linkage. Signal Process. Image Commun., 57 (2017) 113-125.

170. Huang, H.Y. ve Ciou, A.J. Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. J Image Video Proc., 68, 2019 (2019).

171. Vaishnavi, D. ve Subashini, T.S., Application of local invariant symmetry features to detect and localize image copy move forgeries J. Inf. Secur. Appl., 44 (2019) 23-31.

172. Park, J.Y., Kang, T.A., Moon, Y.H. ve Eom, I.K., Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram. Symmetry, 12, 4 (2020), 492.

173. Bi, X. ve Pun, C.M., Fast reflective offset-guided searching method for copy-move forgery detection, Information Sciences, 418–419 (2017), 531-545.

174. Bi, X. ve Pun, C.M., Fast copy-move forgery detection using local bidirectional coherency error refinement, Pattern Recognition, 81 (2018) 161-175.

ÖZGEÇMİŞ

2007 yılında Fatma Kemal Timuçin Anadolu Lisesi'nden mezun oldu. 2007 yılında Erciyes Üniversitesi Bilgisayar Mühendisliği bölümünü kazandı. Erciyes Üniversitesi Yabancı Diller Yüksekokulunda İngilizce Hazırlık eğitimini tamamladıktan sonra 2008 yılında lisans eğitimine başladı ve 2012 Şubat ayında mezun oldu. Haziran 2015'te eğitimini Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimini tamamladı. 2012-2015 yılları arasında Fırat Üniversitesi Yazılım Mühendisliği bölümünde Araştırma Görevlisi olarak başlayan görevini, 2015 yılında Karadeniz Teknik Üniversitesi Bilgisayar Mühendisliği Bölümünde devam ettirmiş ve halen aynı kurumda çalışmaktadır.

Doktora çalışması esnasında TÜBİTAK destekli 119E045 numaralı Saldırıdan Bağımsız Kopyala-Yapıştır Sahteciliği Tespiti adlı projede bursiyer olarak görev aldı. Yabancı dil olarak İngilizce bilmektedir. Başlıca yayınları aşağıda verilmiştir.

Uluslararası hakemli dergilerde yayınlanan makaleler (SCI/SCI-E)

1. Tahaoğlu, G., Ulutaş, G., Üstübioglu, B. ve Nabiyev V., Improved copy move forgery detection method via L*a*b* color space and enhanced localization technique, Multimedia Tools and Applications, 80 (2021) 23419–23456.

2. Tahaoğlu, G. ve Ulutaş, G. Detection of copy move forgery based on color SURF, Journal of The Faculty of Engineering and Architecture of Gazi University, 34 (2019)1540-1548, 2019.

3. Ulutaş, G. ve Tahaoğlu, G., A new copy move forgery detection method resistant to Object Removal with Uniform Background Forgery, Mathematical Problems in Engineering, 2016 (2016) 1-19.

Uluslararası hakemli dergilerde süreci devam eden makaleler (SCI/SCI-E)

1. Tahaoğlu, G., Ulutaş, G., Üstübioglu B., Nabiyev V. ve Ulutas, M, Ciratefi Based Copy Move Forgery Detection on Digital Images, Multimedia Tools and Applications (doi: 10.1007/s11042-021-11503-w, basım aşamasında)

2. Odabaş Yıldırım, E., Tahaoğlu, G., Ulutaş, G., Üstübioğlu, B., Ulutaş, M. ve Nabiyev, V., Color Image Splice Localization based on block classification using transition probability clasification, Journal of Ambigent Intellegent and Humanized Computing (Revizyon sonrası hakem değerlendirmesinde)

Ulusal ve uluslararası konferanslarda sözlü sunumu yapılan bildiriler

1. Tahaoğlu, G., Ulutaş, G., Üstübioğlu, B., A new approach for localization of copy-move forgery in digital images, 44thTelecommunicationand Signal Processing, Brno, Çek Cumhuriyeti, 26 -28 Temmuz 2021, Bildiriler kitabı: 183-186.

2. Tahaoğlu, G., Ulutaş G., Üstübioğlu, B., Ataklara Karşı Dayanıklı Yeni Bir Kopyala Yapıştır Sahteciliği Tespiti Yöntemi, Sinyal İşleme ve İletişim Uygulamaları Kurultayı (SIU2020), Gaziantep, Türkiye, 5 -7 Ekim2020, Bildiriler kitabı: 1-3.

3. Tahaoğlu, G., Ulutaş G., Üstübioğlu B., Copy-Move Forgery Detection with Quadtree Decomposition Segmentation, 43rd International Conference on Telecommunications and Signal Processing (TSP–2020), Milan, İtalya,7 -09 Temmuz 2020, Bildiriler kitabı: 1-5.

4. Tahaoğlu, G., Ulutaş, G., A new deep learning-based method to detection of copy-move forgery in digital images, International Scientific Meeting on Electrical-Electronics and Biomedical Engineering and Computer Science (EBBT), İstanbul, Türkiye, 24 -26 Nisan 2019.

5. Tahaoğlu, G., Erdol, E. S., Ulutaş, G., A Copy-Move Forgery Detection Approach Based on Local Intensity Order Pattern and PatchMatch, 26th IEEE Signal

Processing and Communications Applications Conference (SIU), İzmir, Türkiye, 2 - 5 Mayıs 2018.

6. Aydın Y., Tahaoğlu G., Detection of Copy Move Forgery Technique Based on SIFT and SURF Ulutaş, G. 26th IEEE Signal Processing and Communications Applications Conference (SIU), İzmir, Türkiye, 2 -5 Mayıs2018.