KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANAHTAR NOKTASI VE YAMA EŞLEŞME YÖNTEMLERİ İLE DOKU BAZLI GÖRÜNTÜ SAHTECİLİĞİ TESPİTİ

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Eda Sena ERDÖL

HAZİRAN 2019
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANAHTAR NOKTASI VE YAMA EŞLEŞME YÖNTEMLERİ İLE DOKU BAZLI GÖRÜNTÜ SAHTECİLİĞİ TESPİTİ

Bilgisayar Müh. Eda Sena ERDÖL

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"BİLGİSAYAR YÜKSEK MÜHENDİSİ"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 20 / 05 /2019
Tezin Savunma Tarihi : 13 / 06 /2019

Tez Danışmanı : Doç. Dr. Güzin ULUTAŞ

Trabzon 2019

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalında
Eda Sena ERDÖL tarafından hazırlanan

ANAHTAR NOKTASI VE YAMA EŞLEŞME YÖNTEMLERİ İLE DOKU BAZLI GÖRÜNTÜ SAHTECİLİĞİ TESPİTİ

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 28 / 05 / 2019 gün ve 1806 sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri

Başkan : Doç. Dr. Güzin ULUTAŞ .....

Üye : Prof. Dr. Ahmet Bedri ÖZER .....

Üye : Doç. Dr. Bekir DİZDAROĞLU .....

Prof. Dr. Asim KADIOĞLU
Enstitü Müdürü

ÖNSÖZ

Tez, Karadeniz Teknik Üniversitesi Fen Bilimleri Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Yüksek Lisans Programı'nda yapılan bir çalışmadır.

Çalışmada blok tabanlı yöntemler ve anahtar noktası tabanlı yöntemler incelenerek yöntemlerdeki eksikliklerin giderilmesi, ataklara karşı dayanıklılığın arttırılması ve var olan problemleri iyileştirmek için yeni yöntemler önerilmiştir. Önerilen ilk yöntemde LIOP (Local Intensity Order Pattern) yöntemi kullanılarak özellik vektörleri elde edilir. Daha sonra elde edilen vektörleri eşleştirmek için PatchMatch algoritması kullanılmıştır. Eşleşen vektörlerin sahtecilik yapılan bölgeye ait oldukları var sayılarak boyanmıştır. Kopyala-yapıştır sahteciliğini tespit etmek için önerilen ikinci yöntemde ise, RINBP (Rotation Invariant Neighbors Based Binary Pattern) yöntemi ile doku görüntüsü elde edilmiştir. Daha sonra doku bilgisi üzerinden SIFT (Scale Invariant Feature Transform) yöntemi ile anahtar noktaları çıkartılarak özellik vektörleri elde edilmiştir. Eşleşen vektörlerin sahtecilik yapılan bölgeye ait oldukları varsayılarak işaretleme işlemi gerçekleştirilmiştir. Gerçekleştirilen iki çalışmada daha önceki çalışmalarla kıyaslanarak doğruluk oranı daha yüksek sonuçlar elde edilmiştir. Son gerçekleştirilen çalışmada ise kopyala-yapıştır sahteciliği tespitinde kullanılan ve literatürde var olan veri setleri yerine, farklı olarak ilk defa hiperspektral görüntüler kullanılarak doğruluk oranı yüksek sonuçlar elde edilmiştir.

Öncelikle yüksek lisans tezi danışmanlığımı üstlenerek, gerek günlük hayatta gerekse akademik hayatta yardımlarını esirgemeyen ve yanımda olan, akademisyen olma yolunda her türlü bilimsel katkıyı sağlayan sayın hocam Doç. Dr. Güzin ULUTAŞ'a teşekkürlerimi bir borç bilirim. Hayatımda her konuda yanımda olan ve sevgiyle bana desteğini esirgemeyen, hayatımın kahramanı sevgili eşim Arş. Gör. Hakan ERDÖL'e de ayrıca teşekkür ederim.

Eda Sena ERDÖL

Trabzon 2019

TEZ ETİK BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum "ANAHTAR NOKTASI VE YAMA EŞLEŞME YÖNTEMLERİ İLE DOKU BAZLI GÖRÜNTÜ SAHTECİLİĞİ TESPİTİ" başlıklı bu çalışmayı baştan sona kadar danışmanım Doç. Dr. Güzin Ulutaş'ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuvarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim 13/06/2019.

Eda Sena ERDÖL

İÇİNDEKİLER

Sayfa No

ÖNSÖZ III
TEZ ETİK BEYANNAMESİ IV
İÇİNDEKİLER V
ÖZET VII
SUMMARY VIII
ŞEKİLLER DİZİNİ IX
TABLOLAR DİZİNİ XI
SEMBOLLER DİZİNİ XII
1. GENEL BİLGİLER 1
1.1. Giriş 1
1.2. Sahtecilik Tespitinde Kullanılan Pasif Yöntemler 6
1.2.1. Blok Tabanlı Yöntemler 9
1.2.2. Anahtar Tabanlı Yöntemler 18
1.2.3. Hibrit Yöntemler 21
1.3. Yapılan Çalışmada Kullanılan Yöntemler ve Literatür Araştırması 24
1.3.1. Yerel Yoğunluk Sıra Örüntüsü (Local Intensity Order Pattern, LIOP) 24
1.3.2. Yama Eşleşmesi Algoritması PatchMatch 28
1.3.3. Rotasyondan Bağımsız Komşuluk Temelli İkili Örüntü (RINBP) 30
1.3.4. Ölçekten Bağımsız Öznitelik Dönüşümü (Scale Invariant Feature Transform, SIFT) 35
1.3.5. RANSAC (Random Sample Consensus) 42
1.3.6. Hiperspektral Görüntüleme 43
2. YAPILAN ÇALIŞMALAR VE ÖNERİLEN YÖNTEM 47
2.1. Kopyala-Yapıştır Sahteciliği Tespitinde LIOP ve PatchMatch Tabanlı Yaklaşım 47
2.2. RINBP ve SIFT Tabanlı Kopyala-Yapıştır Sahteciliği Tespiti 50
2.3. SIFT Tabanlı Yöntem ile Hiperspektral Görüntüler Üzerinde Kopyala-Yapıştır Sahteciliği Tespiti 52

3. BULGULAR 55
3.1. Performans Ölçütü Yöntemi 55
3.2. GRIP Veri Seti 56
3.3. Hiperspektral Veri Setleri 58
3.4. LIOP ve PatchMatch Tabanlı Yaklaşım'ın Sonuçları 61
3.5. RINBP ve SIFT Tabanlı Yaklaşım'ın Sonuçları 66
3.6. Hiperspektral Görüntüler Üzerinde Kopyala-Yapıştır Sahteciliği Tespiti Sonuçları 70
4. SONUÇLAR 55
5. ÖNERİLER 76
6. KAYNAKÇA 77
ÖZGEÇMİŞ

Yüksek Lisans Tezi

ÖZET

ANAHTAR NOKTASI VE YAMA EŞLEŞME YÖNTEMLERİ İLE DOKU BAZLI GÖRÜNTÜ SAHTECİLİĞİ TESPİTİ

Eda Sena ERDÖL

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Güzin ULUTAŞ
2019, 82 Sayfa

Sayısal görüntü üzerinde işleme ve düzenleme, teknolojinin gelişmesiyle hızlı ve yaygın hale gelmiştir. Teknolojinin iyi amaçlı kullanımının yanında, görüntülerin gerçekliği üzerinde oynamak gibi kötü amaçlı kullanımı da mümkündür. Sayısal görüntü üzerinde kötü amaçlı olarak kullanılan en yaygın sahtecilik yöntemi, kopyala-yapıştır sahteciliğidir. Kopyala-yapıştır sahteciliği nesneleri kapatmak (ör: olay yeri görüntülerinde cinayetin işlendiği suç aleti ya da suçu işleyen kişinin görüntüsünün gizlenmesi) ya da istenilen nesnelerin sayısını arttırmak (ör: yapılan hava saldırısı görüntüsünde füzelerin ve füzeatarların sayısını arttırmak) için aynı görüntü içerisinden kopyalanan bölgenin yine aynı görüntü içerisine yapıştırılmasıdır. Bu tez çalışmasında, askeri, tıp, kamu ve hukuk gibi önem arz eden alanlarda yapılan kopyala-yapıştır sahteciliği tespiti için önerilen iki çalışma anlatılacaktır. Bunların yanı sıra kopyala-yapıştır sahteciliği tespitinde literatürde daha önce yer almamış ama önemli bir alan olan ve yoğun bilgi içeren hiperspektral uydu veri setleri kullanılarak, görüntü sahteciliği tespiti gerçekleştirilmiştir. Tez kapsamında gerçekleştirilen çalışmalarla literatürde var olan çalışmalar karşılaştırılarak, ataklara karşı dayanıklılık test edilmiştir. Önerilen yöntemlerin doğruluk oranının daha yüksek ve ataklara karşı dayanıklı olduğu deneysel sonuçlar ile rapor edilmiştir.

Anahtar Kelimeler: Sayısal Görüntü İşleme, Kopyala-Yapıştır Sahteciliği, Sahte Görüntü Tespiti, LIOP, PatchMatch, RINBP, LBP, SIFT, RANSAC, Hiperspektral Görüntü.

Master Thesis

SUMMARY

PATTERN BASED IMAGE FORGERY DETECTION BY THE AID OF KEYPOINT AND PATCHMATCH METHODS

Eda Sena ERDÖL

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Assoc. Prof. Güzin ULUTAŞ
2019, 82 Pages

Processing and editing operations on digital images become fast and common with the aid of technological improvements. In addition to the good use of technology, it is also possible to use maliciously, such as editing reality of images. The most common method of vicious editing is the copy-move forgery. Copy-move forgery can be used to cover objects (i.e covering the image of the crime device or the perpetrator of the crime scene in the crime scene images) or increasing the number of objects desired (i.e increasing the number of missiles and missile launchers in the air attack image). In this thesis, two studies which are proposed for the detection of copy-paste forgery in important areas such as military, medical, public and law will be explained. Moreover, Copy-move forgery detection methods are used in hyperspectral satellite image data sets with dense and important information which are not found in literature. The studies carried out within the scope of the thesis were compared with the existing studies in the literature and the resistance to attacks was tested. It has been reported with the experimental results that the accuracy of the proposed methods is higher than conventional methods and resistant to attacks.

Key Words: Digital Image Processing, Copy-Move Forgery, Forged Image Detection, LIOP, PatchMatch, RINBP, LBP, SIFT, RANSAC, Hyperspectral Image.

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1. Hippolyte'nin intihar teşebbüsünü gösteren ilk sahte görüntü [1] 1
Şekil 2. Görüntü doğrulama yöntemleri hiyerarşisi..... 2
Şekil 3. Piksel tabanlı görüntü sahtecilik yöntemlerinin kategorilendirilmesi..... 4
Şekil 4. (a) Gerçek görüntü (b) Kopyalanıp yapıştırılan bölge (c) Sahte görüntü 4
Şekil 5. Scopus tarafından indekslenen kopyala-yapıştır sahteciliği üzerine yapılan çalışmalar [9]..... 5
Şekil 6. Birleştirme sahteciliği yöntemine örnek görsel (a) ilk gerçek görüntü (b) ikinci gerçek görüntü (c) birleştirme sahteciliğinin yapıldığı sahte görüntü..... 5
Şekil 7. Yeniden örnekleme ve enterpolasyon tabanlı görüntü sahteciliği örneği (a) kaynak görüntü (b) oynanmış görüntü (c) b görüntüsündeki parçaların yeniden boyutlandırılıp, konumlarının değiştirilip a görüntüsüne aktarılması sonucu oluşan görüntü [11] 6
Şekil 8. Kopyala-yapıştır sahteciliği tespiti genel akış diyagramı..... 8
Şekil 9. LIOP Tanımlayıcı Vektör Oluşturulması [61] 25
Şekil 10. LIOP Olasılık Dağılım Diyagramı 26
Şekil 11. Ondalık tabanda LBP kodu üretimi..... 31
Şekil 12. LBP'nin farklı gösterimleri (a) 1'e 8'lik (b) 2'ye 16'lık..... 32
Şekil 13. Ondalık tabanda NBP kodu üretimi 33
Şekil 14. Ağaç kabuğu görüntüsüne NBP uygulanması..... 33
Şekil 15. Ondalık tabanda RINBP kodu üretimi [64]..... 34
Şekil 16. İki ölçek arasındaki farkın hesaplanarak ölçek uzayın belirlenmesi [66] 37
Şekil 17. Yerel maksimum ve minimumların bulunması [66] 38
Şekil 18. Anahtar noktaların elenmesi [66]..... 40
Şekil 19. (a) Görüntü gradyanı (b) Anahtar noktası tanımlayıcısı (c) Yerel örüntü histogramı..... 42
Şekil 20. Hiperspektral görüntü dalga boyu 44
Şekil 21. (a) RGB (b) Multispektral (c) Hiperspektral..... 45
Şekil 22. Hiperspektral küp 45
Şekil 23. LIOP+PatchMatch tabanlı çalışmanın akış diyagramı..... 48
Şekil 24. RINBP+SIFT tabanlı çalışmanın akış diyagramı..... 50
Şekil 25. (a) 10. katman görüntüsü (b) 90.katman görüntüsü (c) 110.katman görüntüsü (d) 130.katman görüntüsü..... 53
Şekil 26. (a) Sahte görüntü (b) Görüntünün sahtecilik maskesi..... 54

Şekil 27. GRIP veri seti görüntüsü (a) gerçek görüntü (b) kopyalanan bölge (c) sahte görüntü 56
Şekil 28. GRIP veri setinde (a) JPEG ataklı (b) Gürültü ataklı örnek sahte görüntüler 57
Şekil 29. Hiperspektral Washington D.C.(a) kanal görüntüsü (b) sınıf görüntüsü [72] 59
Şekil 30. Hiperspektral Pavia Center (a) kanal görüntüsü (b) sınıf görüntüsü [73] 60
Şekil 31. University of Pavia (a) kanal görüntüsü (b) sınıf görüntüsü [73] 60
Şekil 32. Gürültü atağına karşı, karşılaştırmalı test sonucu 61
Şekil 33. JPEG sıkıştırma atağına karşı, karşılaştırmalı test sonucu 62
Şekil 34. Ölçekleme atağında, karşılaştırmalı test sonucu 62
Şekil 35. Döndürme atağına karşı, karşılaştırmalı test sonucu 63
Şekil 36. (a) Kalite faktörü 90 olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü 64
Şekil 37. (a) %80 oranında ölçekleme atağına maruz kalmış sahte görüntüsü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü 64
Şekil 38. (a) Standart sapması $ln2$ olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü 65
Şekil 39. (a) 90^o döndürme atağına maruz kalmış sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü 65
Şekil 40. (a) 90^o döndürme atağına maruz kalmış sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi 68
Şekil 41. (a) Standart sapması $ln2$ olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi 68
Şekil 42. (a) %50 oranında ölçekleme atağına maruz kalmış sahte görüntüsü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) sahte görüntünün maskesi 69
Şekil 43. (a) kalite faktörü 20 olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi 69
Şekil 44. Washington D.C. hiperspektral görüntüsünde eşleşme sonucu 71
Şekil 45. Pavia University hiperspektral görüntüsünde eşleşme sonucu 73

TABLOLAR DİZİNİ

Sayfa No

Tablo 1. Literatürde var olan veri setleri 56
Tablo 2. Hiperspektral Veri Setleri 58
Tablo 3. RINBP + SIFT Yönteminin döndürme ataklarına karşı dayanıklılığı 67
Tablo 4. RINBP+SIFT Yönteminin F Ölçütü Performans Sonuçları..... 67
Tablo 5. Tez kapsamında önerilen yöntemlerin karşılaştırılması..... 70
Tablo 6. SIFT Tabanlı Yönteminin Hiperspektral Görüntülerdeki F Ölçütü Performans Sonuçları..... 74

SEMBOLLER DİZİNİ

ADD	Ayrık Dalgacık Dönüşümü (DWT)
AKD	Ayrık Kosinüs Dönüşümü (DCT)
AKD-MKA	Ayrık Kosinüs Dönüşüm Kuantizasyon Katsayıları Ayrıştırma
AWGN	Toplanır Beyaz Gauss Gürültüsü (Additive White Gaussian Noise)
BBF	Best Bin First
DoG	Gauss Uzay Farkı (Difference of Gaussian)
FCMC	Kümeleme için Bulanık C Araçları (Fuzzy C-Means Clustering)
FMD	Fourier Mellin Dönüşümü
GH	Gradyan Histogramı
HOG	Histogram of Gradient (Gradyan Histogramını)
İDD	İkili Dalgacık Dönüşümü
K-D	K-Dimensional Tree
LBP	Yerel İkili Örüntü (Local Binary Patterns)
LBPV	Yerel İkili Örüntü Varyansı (Local Binary Patterns Variance)
LIOP	Yerel Yoğunluk Sıra Örüntüsü (Local Intensity Order Pattern)
LPFD	Log-Polar Fourier Dönüşümü
LPHFD	Log-Polar Hızlı Fourier Dönüşümü
NIR	Kızıl Ötesi (Near Infrared)
ORB	Hızlı ve Döndürülmüş Kısa Yönlü (Oriented Fast and Rotated Brief)
PHD	Polar Harmonik Dönüşümü
RANSAC	Random Sample Consensus
RGB	Red Green Blue
RGB	Red Green Blue
RINBP	Rotasyondan Bağımsız Komşuluk Temelli İkili Örüntü (Rotation Invariant Neighbors Based Binary Pattern)
SIFT	Ölçek Bağımsız Öznitelik Dönüşümü (Scale Invariant Feature Transform)

SURF	Hızlandırılmış Dayanıklı Öznitelikler (Speed up Robust Feature,)
SVD	Tekil Değer Ayrışımı (Singular Value Decomposition)
SWT	Sabit Dalgacık Dönüşümü (Stationary Wavelet Transform)
TBA	Temel Bileşen Analizi
TDA	Tekil Değer Ayrışımı
YUV	Y Luminance, U Chrominance-1, V Chrominance-2

1. GENEL BİLGİLER

1.1. Giriş

Son yıllarda teknolojideki hızlı gelişmeler, insanoğlunun teknolojiyi daha fazla kullanması, sayısal görüntülerin çeşitli alanlarda sıklıkla kullanılmasına sebep olmuştur. Görüntüler üzerinde yapılan sahtecilik çok eski yıllara dayanmaktadır. Eski yıllarda sahtecilik daha çok edebiyat ve sanat eserleriyle sınırlıyken, şimdi insanoğlunun yaşamını çoğu alanda etkilemektedir. Bu alanlardan önemli olanlarının bazıları tıbbi araştırmalar, askeri soruşturmalar, adli ve yargı süreçleridir. Bu alanlarda sayısal görüntülerin doğrulanması büyük önem arz etmektedir.

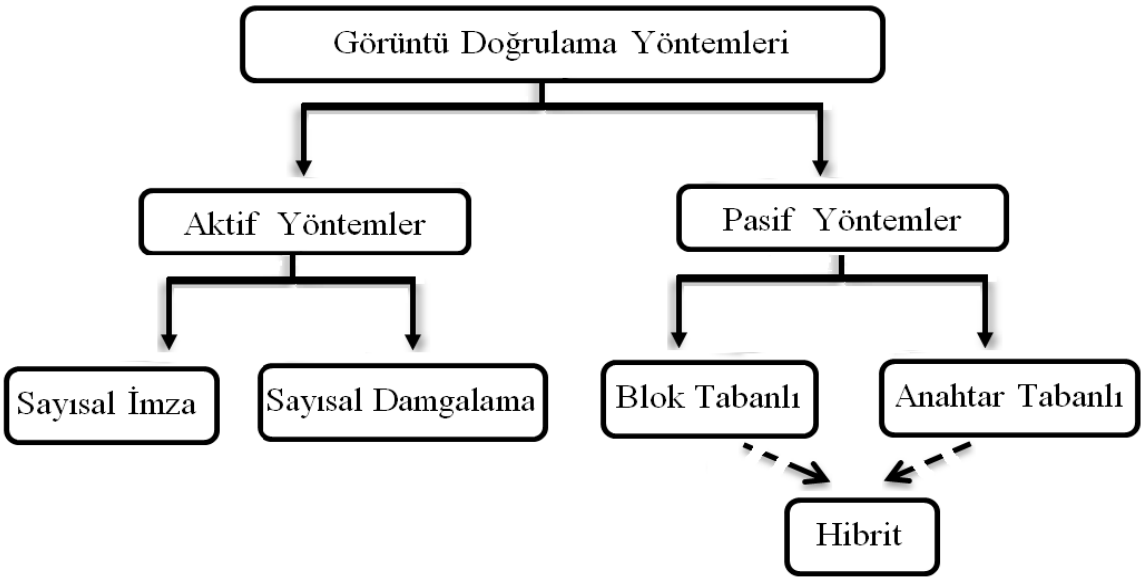
Görüntü sahteciliğinin tespiti konusunda yapılmış ilk çalışma 1840 yılında Hippolyte Bayard adlı kişinin, intihar olayında sunulan sahte görüntüsüdür ve Şekil 1'de gösterilmektedir [1].

Şekil 1. Hippolyte'nin intihar teşebbüsünü gösteren ilk sahte görüntü [1]

Görüntü işleme ve bu alanda yapılan araştırmalar, son yıllarda revaçta olan ve çalışma alanı geniş bir konudur. Görüntülerin delil olarak kullanıldığı ve görüntüler

neticesinde elde edilen kararlar insan hayatını önemli ölçüde etkilediği için, kararların doğruluğu oldukça önemlidir. Sayısal görüntülerde, teknolojinin gelişmesi iyi yönde olduğu gibi görüntünün içeriğini değiştirmek, sahte görüntü oluşturmak veya bölge eklemek, çıkarmak için kötü amaçlıda kullanılmaktadır. Sayısal görüntüler üzerinde değişiklik yapmak sıradan bir bilgisayar kullanıcısı açısından bile oldukça kolaydır. Photoshop, GIMP, Paint.NET, ChocoFlop gibi bir bölümü açık kaynak kodlu ve ücretsiz yazılımlar mevcuttur. Donanım kısmında ise çok yüksek çözünürlüklü dijital kameraların ve video kaydedicilerin gelişmesi görüntüde sahtecilik yapmak isteyen kişilerin işlerini kolaylaştırmaktadır. Hızla gelişen yazılımlar ve donanımlar sayesinde sayısal görüntüler üzerinde iz bırakmadan, normal insan gözüyle anlaşılamayacak görüntü içeriğinde değişiklikler basite indirgenmektedir.

Sayısal görüntülerin doğruluğunu ve güvenilirliğini ispatlamak için birçok farklı yöntem vardır. Şekil 2'de görüldüğü gibi literatürde bu yöntemler aktif ve pasif yöntemler olarak ikiye ayrılmaktadır [2].



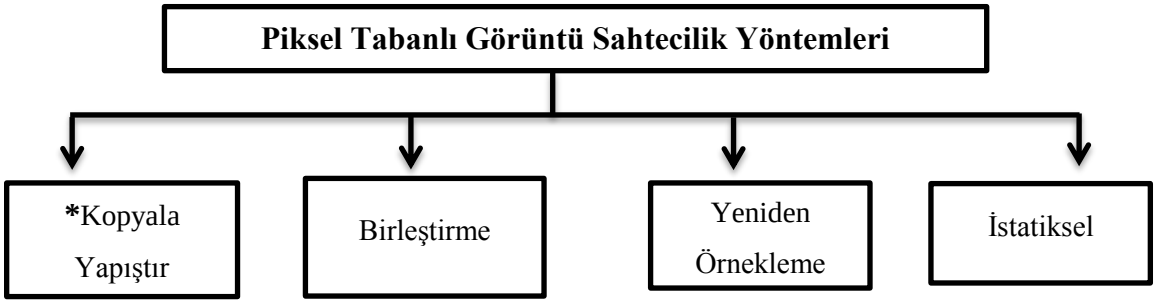
Şekil 2. Görüntü doğrulama yöntemleri hiyerarşisi

Aktif bir yöntem olan sayısal imzalama yöntemi, görüntü üzerinden oluşturulan ve görüntünün özelliklerini içeren imza bilgisinin de görüntü ile gönderilmesiyle oluşturulur. Sayısal imzalama, görüntüyü gönderen kişinin kendi özel anahtarı (private key) ile

dokümanı işaretlemesidir. Daha sonra bu özel anahtardan üretilen ve herkes tarafından bilinen kamusal anahtar (public key), görüntünün gönderileceği alıcıda bulunur. Üretilen kamusal anahtar görüntüyü görüntülemek isteyen kişide bulunur ve görüntüyü açmak için kullanılır. Kamusal anahtar, görüntünün açılmasında kullanılmasının yanı görüntü sahibine erişim yetkisi verir [3]. Dezavantajları ekstra ön işlem gerektirmesi, bilgi oluşturulması ve transferi gibi özel yazılımlara da ihtiyaç duymasıdır.

Diğer bir aktif yöntem olan sayısal damgalama metodunda, damgalama görüntüyü doğrulayabilecek bir araç olarak ele alınmıştır [4]. Bu metotta özel oluşturulmuş bir tür damga bilgisi (parmak izi, mühür vb.) görüntü içine gizlenir. Çıkarılan damga bilgisi gerçek damga test görüntüsünden alınan damga ile karşılaştırılır. Damga bilgisi sayesinde görüntünün değişime uğrayıp uğramadığının kontrolü yapılır [5]. Telif hakkı, parmak izi onayı, gizli iletişim, verinin gerçekliği, dosyaların doğruluğu ve uygunsuz kullanılıp kullanılmadığı gibi alanlarda kullanılmaktadır. Birçok alanda kullanılmasına rağmen, damga bilgisinin görüntülere görüntü oluşum sırasında yerleştirilmesi veya damga oluşturma gibi ön işlemler gerektirdiği için günlük hayatta kullanımı oldukça zordur. Ön işlemleri gerçekleştirebilmek için gerekli olan yüksek çözünürlüklü ve özel donanımlı kameralar piyasada oldukça az ve yüksek maliyetlidir. Bunun yanı sıra damgalama tespitin gerçekleştirilebilmesi için, bazı damgalama metotlarında gerçek görüntüye erişim gereklidir.

Aktif yöntemlerin dezavantajları ve işlem maliyetinin oldukça yüksek olmasından dolayı literatürde pasif yöntemler önerilmiştir. Pasif yöntemlerde görüntünün doğrulanması için orijinal görüntüye ihtiyaç duyulmamaktadır. Pasif yöntemlerde görüntü içerisinde elde edilen veriler ve bunların karşılaştırılmasıyla görüntünün sahte olup olmadığı tespit edilmektedir [6]. Pasif yöntemler kendi arasında piksel tabanlı, kamera tabanlı, format tabanlı, geometrik tabanlı ve fiziksel çevre tabanlı yöntemler üzerinde beş ayrı kategoride incelenmektedir. Piksel bazında görüntülerde yapılan sahtecilikler dört gruba ayrılır ve Şekil 3'te gösterilmektedir [7]. Bu tezde yer alan çalışmalarda piksel tabanlı sahtecilik tespiti yöntemleri kullanılarak, kopyala-yapıştır sahteciliği tespiti yapılmaktadır ve Şekil 2'de pasif tabanlı yöntemlerin içerisinde gösterilmektedir.



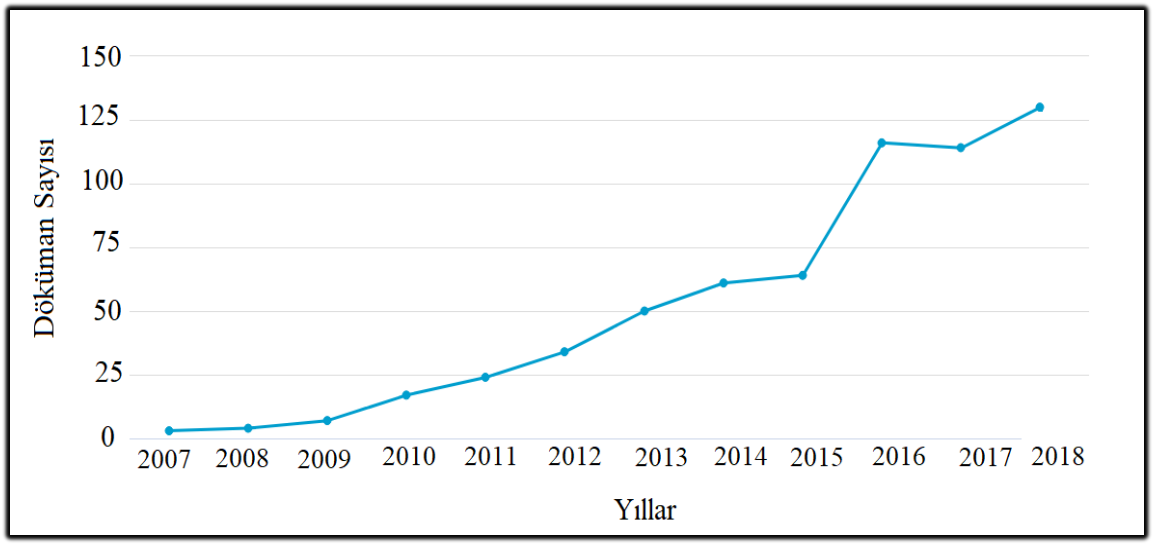
Şekil 3. Piksel tabanlı görüntü sahtecilik yöntemlerinin kategorilendirilmesi

Sahtecilik yöntemlerinden en çok bilineni "kopyalama-yapıştır" olarak adlandırılan, sayısal görüntünün bir kısmının kopyalanarak görüntüdeki istenmeyen nesneleri (suçu işleyen kişi, suç işlenen silah vb.) gizlemek için aynı görüntünün üzerine yapıştırılmasıyla gerçekleştirilmektedir [8]. Bu sahtecilik yöntemi ile görüntüde istenilmeyen bölge veya bölgelerin kapatılması veya gizlenmesi amaçlanmaktadır. Kopyala-yapıştır sahteciliğine örnek görüntü Şekil 4'te verilmiştir. Görüntüde masanın kenar örüntüsü ile masada bulunan silah gizlenmeye çalışılmıştır. Görüntü içerisinden alınan doku sayesinde, tekrar görüntüye yapıştırılan bölgenin insan gözüyle algılanması oldukça zordur.

(a) (b) (c)

Şekil 4. (a) Gerçek görüntü (b) Kopyalanıp yapıştırılan bölge (c) Sahte görüntü

Bu tez içeriğinde, literatürde en çok yer alan kopyala-yapıştır sahteciliği olan görüntülerin tespiti üzerine çalışılmıştır. Şekil 5'te Scopus'dan alınmış yıllara göre kopyala-yapıştır sahteciliği tespiti üzerine yapılan çalışmalar görülmektedir [9].



Şekil 5. Scopus tarafından indekslenen kopyala-yapıştır sahteciliği üzerine yapılan çalışmalar [9]

Diğer bir piksel tabanlı sahtecilik yöntemi olan birleştirme sahteciliği, iki ya da ikiden fazla görüntünün belirli kısımlarının birleştirilerek tek görüntüde toplanmasıdır [10]. Tonlamaların ve renklerin aynı olduğu görüntülerde insan gözüyle algılanması oldukça zordur. Şekil 6'da birleştirme sahteciliğiyle yapılmış örnek görüntü mevcuttur.

(a) (b) (c)

Şekil 6. Birleştirme sahteciliği yöntemine örnek görsel (a) ilk gerçek görüntü (b) ikinci gerçek görüntü (c) birleştirme sahteciliğinin yapıldığı sahte görüntü

Piksel tabanlı üçüncü sahtecilik yöntemi olan yeniden örnekleme yöntemi iki ya da daha fazla görüntüden alınan belirli bölgelerin ölçeklerinin oynanmasıyla (genişletmek-daraltmak, uzatıp-kısaltmak gb.), yeni bir görsel üzerinde birleştirilmesidir. Bu işlem sürecinde komşu pikseller arasındaki benzerlik değerleri hesaplanarak, yeni düzlem

üzerinde yeniden boyutlanmaya gidilir [11]. Yeniden örnekleme ile yapılan sahtecilik yöntemine Şekil 7'de örnek gösterilmiştir.

(a) (b) (c)

Şekil 7. Yeniden örnekleme ve enterpolasyon tabanlı görüntü sahteciliği örneği (a) kaynak görüntü (b) oynanmış görüntü (c) b görüntüsündeki parçaların yeniden boyutlandırılıp, konumlarının değiştirilip a görüntüsüne aktarılması sonucu oluşan görüntü [11]

Piksel tabanlı görüntü sahteciliklerinden sonuncusu olan istatiksel görüntü sahteciliğinde, görüntülerin belirli istatistiksel özelliklerine bakılarak verilerin birbirine yakın olduğu yerlerde görüntü sahteciliği yapılır [12]. Bu sayede insan gözünün fark edemeyeceği şekilde görüntü üzerinde sahtecilik yapılmaktadır.

Bu tezin genel bilgiler kısmında kopyala-yapıştır sahteciliği tespiti yöntemlerinin olumlu olumsuz yönleri ve önerilen yöntemlerle tespit edilen eksikliklerin giderilmesi ile ilgili konular, tez çalışmasında kullanılan bilgiler verilmiştir.

1.2. Sahtecilik Tespitinde Kullanılan Pasif Yöntemler

Kopyala-yapıştır sahteciliği tespiti yöntemleri, görüntü hakkında hiçbir ön bilgi ya da resmin orijinal halinin bilinmesine gerek duymayan çalışmalardır. Kopyala-yapıştır sahteciliği daha öncede bahsedildiği gibi aynı görüntü içeresinde bir veya birden fazla kez yapıldığı için, kurcalanan ya da değiştirilen bölgeler arasında doku, parlaklık ve piksel değerleri gibi özelliklerin benzerlik sağlaması beklenir. Literatürde yer alan çalışmaların temelinde bu teorem vardır.

Şekil 2'de görüldüğü gibi kopyala-yapıştır sahteciliği tespiti yöntemleri, pasif yöntemlerin içerisinde yer alır. Blok tabanlı yöntemler ve anahtar tabanlı yöntemler olmak üzere iki ana başlık altında toplanan sahtecilik tespit yöntemlerine, son zamanlarda literatürde oldukça sık rastlanan ve bu çalışmada da yer alan hibrit yöntemler eklenmiştir.

Genel olarak tüm kopyala-yapıştır sahteciliği yöntemleri akış diyagramı Şekil 8'de verilmiştir. Şekilde görüldüğü ilk olarak görüntü ön işlem (görüntünün gri seviyeye dönüştürülmesi, gürültü azaltma, histogram eşitleme, Ayrık Fourier dönüşümü uygulama gb.) sürecinden geçirilir.

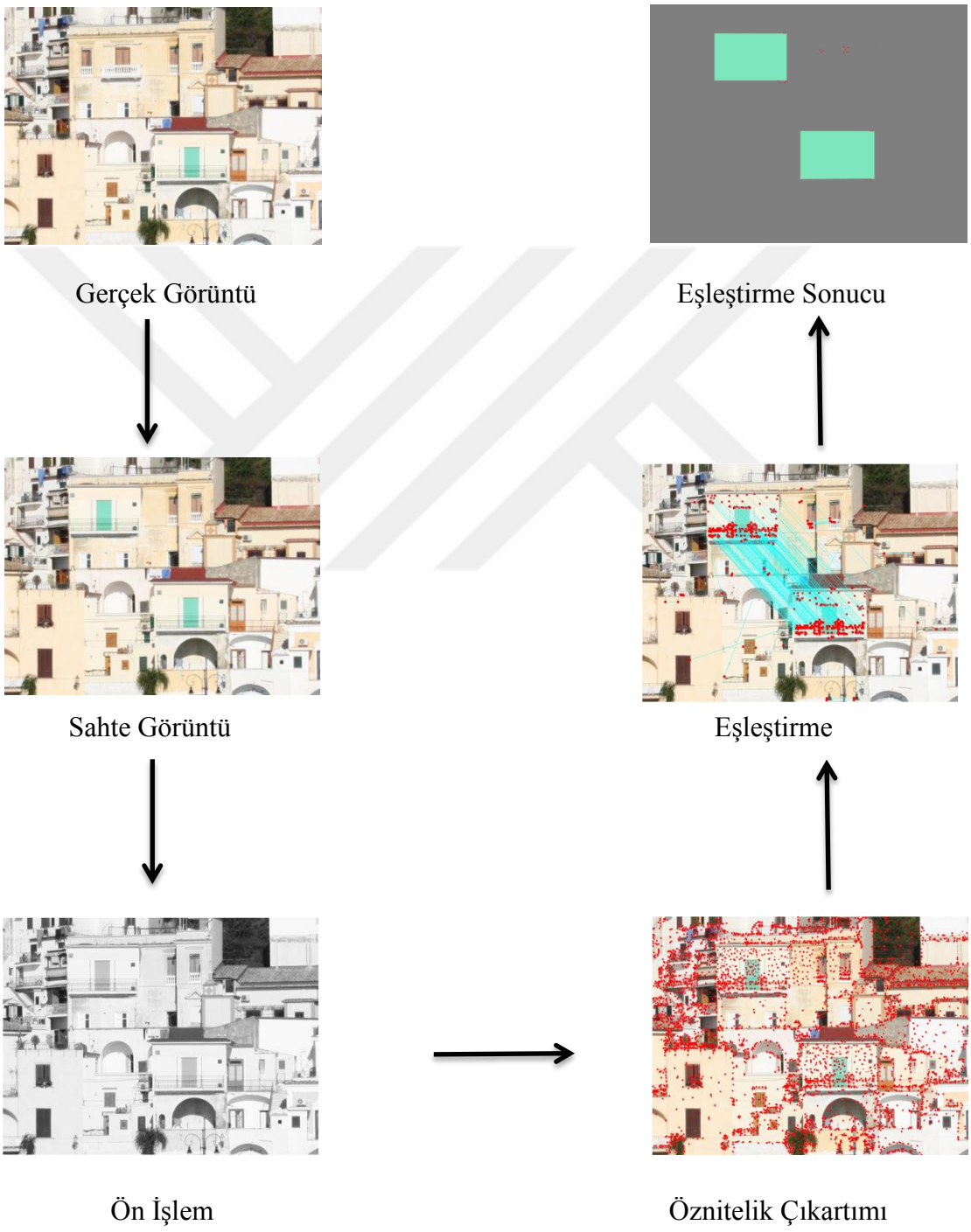
Daha sonraki adımda yöntemin akışını değiştiren seçim yapılır ve öznitelik vektörü oluşturmak için anahtar noktası tabanlı yöntemlerle mi yoksa blok tabanlı yöntemlerle mi devam edileceğine karar verilir. Hibrit yöntemler, anahtar noktası tabanlı ve blok tabanlı yöntemlerin avantajlarını birleştirmek için kullanılan yöntemlerdir. Bu yüzden bu aşamada ya öznitelik çıkarma işlemi anahtar noktasıyla yapılır ya da eşleştirme kısmında anahtar tabanlı çalışan eşleştirme algoritmaları seçilir. Aynı süreç blok tabanlı içinde geçerlidir. Kısaca hibrit yöntemlerde, blok tabanlı yöntem kullanılarak öznitelik oluşturulursa eşleşme kısmında anahtar tabanlı eşleştirme ile çalışan algoritmalar seçilir. Bu süreçte öznitelik çıkartmanın ve eşleştirme yapmanın hangi metotla gerçekleştirileceği yöntemi oluşturan kişinin tecrübesine, yöntemlerin birbiri ile uyumluluğuna ve hangi görüntüler üzerinde hangi ataklara karşı dayanıklı olacağına bağlıdır.

Öznitelik vektörü çıkartıldıktan sonra eşleştirme kısmında, birbiriyle benzerlik gösteren vektörlerde sahtecilik yapılma olasılığı üzerinde durulur. Bu vektörler incelenerek koordinat bilgilerine yani yakınlık uzaklık verilerine bakılır. Literatürde benzer vektörlerin karşılaştırılması yapılmadan önce işlem maliyetini azaltmak için Leksikografi ve Counting Bloom Filters gibi sıralama yöntemleri kullanılmıştır [15,23]. Literatürde ayrıca anahtar noktasından elde edilen öznitelik vektörlerinde, benzer ve yakın komşuları belirlemek için Best-Bin-First arama algoritması kullanılmıştır [13,14]. Eşleştirme aşamasında öznitelik vektörleri arasındaki mesafe Öklid ve Hamming algoritmaları gibi mutlak uzaklık hesaplayan algoritmalar ile ölçülür.

Yanlış eşleştirmelerin giderilmesi, sahtecilik tespitinde önerilen her algoritmada kullanılmaz. Ancak işlem maliyetini azaltmak, özellikle yumuşak geçişli bölgelerde (smooth bölgeler) daha yüksek doğruluk oranı için yapılması önerilir. Yumuşak geçişli bölgeler, görüntü içerisindeki çimenler, yeşillikler, ağaç yaprakları, gökyüzü ve bulut gibi nesnelerin çok olduğu bölgelerdir. Sahtecilik tespitinde, bu bölgelerdeki piksel değerlerinin

oldukça birbirine yakın ve yumuşak geçişlere sahip olmasından dolayı yanlış eşleştirme durumu olasıdır.

Şekil 8'de görüldüğü gibi son olarak benzer vektörler arasındaki mesafe belirlenen eşik değerinin altındaysa ilişkili vektörlerde sahtecilik yapılmıştır denir ve işaretlenir.



Şekil 8. Kopyala-yapıştır sahteciliği tespiti genel akış diyagramı

1.2.1. Blok Tabanlı Yöntemler

Blok tabanlı yöntemlerin genel ismi, öznitelik yani özellik vektörü çıkartırken görüntüyü bloklara ayrıştırmasından gelir. Bu yöntemde bütün resim taranıp, birbirleriyle örtüşen her bloktan özellik vektörü hesaplandığı için işlem maliyeti oldukça yüksektir.

Fridrich, Soukal ve Lukas'a ait olan çalışma, kopyala-taşı sahteciliği alanında literatürdeki ilk çalışmadır [15]. 2003 yılında yapılan çalışmada özellik vektörü oluşturmak için görüntü 8x8'lik bloklara bölünmüş ve her bir bloga Ayrık Kosinüs Dönüşümü (AKD) uygulanmıştır. AKD sonucunda her bloktan oluşan özellik vektörleri ile özellik matrisi elde edilmiştir. Oluşan matris, temeli alfabetik olan Leksikografik algoritması ile sıralanmıştır. Leksikografik sıralamada, a,b,c… gibi büyükten küçüğe sıralanan harfler yerine sayısal 0,1,2… büyükten küçüğe doğru sıralanmıştır. Böyelece benzer blokların oluşturdukları özellik vektörleri yakınlaştırılarak, Öklid uzaklığına bakılmıştır ve kopyala-yapıştır sahteciliği yapılan bloklar tespit edilmiştir. Bu çalışmanın JPEG sıkıştırma ataklarına karşı dayanıklı olduğu tespit edilmiştir. Çünkü yapılan çalışma JPEG sıkıştırmanında temeli olan AKD ile öznitelik vektörü oluşturmaktadır. Çalışmanın dezavantajı ise döndürme ve ölçeklemeye karşı dayanıksız olmasıdır. Ayrıca yapılan ilk çalışma olması ve görüntünün genelinin her bir bloğundan öznitelik çıkarımı, çalışmanın işlem maliyetini oldukça yükseltmiştir.

Popescu ve arkadaşı Farid'in yaptığı çalışmada görüntü sabit boyutlu, küçük alt bloklara bölünerek, her bir sabit bloktan özellik vektörü oluşturulmuştur [16]. Bu yapılan çalışmada küçük alt sabit bloklar 16x16, 32x32 boyutlarından oluşmaktadır. Bunun yanısıra Fridrich ve arkadaşlarının özellik vektörü oluşturmak için kullandığı AKD yöntemini değil, Temel Bileşen Analizi (TBA) yöntemini kullanmışlardır. Fridrich ve arkadaşlarının çalışmasındaki gibi oluşan özellik vektörleri, özellik matrisine aktarılmış, sıralanmış ve aralarındaki uzaklıklara bakılmıştır. Çalışma sonucu JPEG sıkıştırması, gürültü ve bulanıklaştırma ataklarına karşı dayanıklı olduğu test edilmiş ve sonuçlar kısmında gösterilmiştir.

Luo ve arkadaşları yaptığı çalışmada görüntünün renk yoğunluğu bilgisinden yararlanmak için, renkli görüntüyü gri seviyeye dönüştürmeden bir yöntem önermişlerdir. Renkli görüntüyü vxv'lik bloklara ayrıştırarak, görüntünün yoğunluk bilgisi üzerinden

özellik vektörü oluşturmuşlardır [17]. Her blok için 1x7 uzunluğunda özellik vektörleri elde edilmiştir. Özellik vektörünün ilk 1x3'lük boyutunda RGB (red, green, blue) bileşenleri, ardından 1x4 boyutunda ise (Y=0.299 R + 0.587 G + 0.114 B) kanalından elde edilen değerler oluşturmaktadır. Çalışma sonucunda [15] ve [16]'daki çalışmalardan hesaplama karmaşıklığı olarak daha etkin olduğu kanıtlanmıştır. Ataklara karşı dayanıklılık testinde JPEG sıkıştırma, bulanıklaştırma, gürültü ekleme ve bunların birleştirilip uygulandığı ataklarda bile etkili sonuçlar verdiği gösterilmiştir.

Li ve arkadaşları görüntüyü gri seviyeli görüntüye dönüştürerek Ayrık Dalgacık Dönüşümü (ADD) uygulayarak, oluşturdukları alçak frekanslı görüntüyü bloklara ayrıştırmışlardır [18]. Oluşan bloklar üzerinden özellik vektörü çıkarmak için Tekil Değer Ayrışımı (TDA) yani bir matrisin çarpanlarına ayrılma türlerinden biri kullanılmıştır. Her bir blok için oluşturulan min(a,b) özellik vektörleriyle bir matris oluşturmuşlardır. Oluşturulan matrisi Fridrich ve arkadaşlarının çalışmasındaki gibi [15] Leksikografik olarak, sıralayarak birbirine benzer olan vektörler arasındaki mesafeyi minimuma indirgemişleridir. Deneyler sonucu oluşan hata oranını en aza indirmek için ardışıl bloklar arasında belirli bir eşik değeri belirleyerek kaydırma vektörü elde edilmiştir. Kaydırma vektörü ile yanlış eşleştirmelerin giderilmesi amaçlanmıştır. Eğer belirli bir eşik değerini aşan kaydırma vektörü ile ilişkili bloklar varsa, bunlar kopyala-taşı sahteciliğine uğramıştır denilmiştir.

Myna ve arkadaşlarının çalışmasında görüntü boyutunu azaltmak ve işlem maliyetini düşürmek için ilk olarak görüntüye ADD yöntemini uygulanmıştır [19]. Daha sonra görüntü bloklara ayrılarak, blokların her birine log polar transform uygulanarak koordinat sisteminde gösterilmiştir. Sahtecilik yani görüntüde kurcalama işlemi genellikle alçak bantlarda gerçekleştirildiği için, yapılan çalışmada sadece L_oL_o bandı denilen düşük bantlar üzerinde işlem yapılmıştır. Bloklardan oluşan özellik vektörleri ile oluşturulan matris Leksikografik olarak sıralanmıştır. Benzerlik ölçütü olarak da faz kolerasyonu kullanılmıştır. Sadece eşleşen bloklar diğer adımda tekrar işleme sokulur. Boyutu azaltmak için yapılan ön işlem sayesinde daha az hesaplama karmaşıklığına ulaşılmıştır. Çalışmanın sonuçlarında dönme ve ölçekleme ataklarına karşı dayanıklılık olduğu test edilmiştir.

Kang ve Wei'nin çalışmasında bloklardan özellik vektörü çıkartmak için TDA yöntemi kullanılmıştır [20]. Görüntü birbiriyle örtüşen bloklara bölerek, TDA uyguladıktan sonra özellik vektörü boyutu küçültülmüştür. Daha sonra oluşturulan özellik matrisi leksikografik olarak sıralanarak benzer vektörlerin bir araya getirilmesi

sağlanmıştır. Leksikografik olarak sıralamadaki amaç zamansal karmaşıklığını azaltmaktır. Çalışmanın sonucu gürültü ataklarına ve JPEG sıkıştırmaya karşı dayanıklılık gösterirken zamansal hesaplama noktasında çalışma [16]'ya göre daha da verimli olduğu kanıtlanmıştır.

Zhang ve arkadaşlarının çalışmasında görüntü ADD yöntemiyle önce düşük frekanslı dört alt banta dönüştürülmüştür [21]. Daha sonra özellik matrislerinin faz korelasyonları hesaplanarak, piksel eşleştirme ile blokların kopyala-taşı sahteciliğine uğrayıp uğramadığını test etmişlerdir. Çalışmanın yüksek JPEG sıkıştırma ataklarına karşın dayanıklı test edilmiş ve sonuçlar kısmında bu atağa karşı dayanıklı olduğu belirtilmiştir. Ayrıca çalışmada alt bantlarda çalışıldığı için zamansal karmaşıklık ölçümlerinin iyi olduğu belirtilmiştir. Ancak çalışmanın döndürme ve ölçekleme ataklarına karşı dayanıklılığı hakkında bilgi verilmemiştir.

Lin ve arkadaşları daha önce önerilen özellik vektörü çıkartma yöntemlerinde TBA yöntemini kullanmışlardır [22]. Diğer yöntemlerden farklı olarak özellik matrisini sıralarken Radix Sort, yani Taban Sıralaması algoritmasını kullanmışlardır. Daha sonra belirli bir eşik vektörü tanımlamışlardır. Bu vektörün üstünde yüksek frekansa sahip ilişkili bloklarda kopyala-yapıştır sahteciliği yapılmıştır denilip, bu bloklar işaretlenmiştir. Çalışma sonuçlarında sıkıştırma ve gürültü ataklarına karşın dayanıklı olduğu test edilmiştir. Farklı bir sıralama algoritması olan Radix Sort ile çalıştıkları için işlem maliyetinin diğer çalışmalara göre hızlı olduğu söylenmiştir, ancak çalışmada karşılaştırma sonuçlarına yer verilmemiştir.

Bayram ve arkadaşlarının çalışmasında ise görüntü karesel bloklara ayrıştırılıp, bloklara önce Fourier Mellin Dönüşümü (FMD), daha sonra log-polar transformunu uygulanarak özellik vektörü oluşturulmuştur [23]. Log-polar transform metodunu kullanmalarının sebebi döndürme ve ölçeklemeye karşı dayanıklılığı sağlamak içindir. Log-polar uygulanan görüntüde belirli bir faz kayması görülür. Oluşan bu faz kaymasının giderilmesi için, öteleme bağımsız yöntem olan Fourier yöntemi kullanılır. Daha önceki çalışmalarda iki özellik vektörü arasındaki kıyaslamayı öklid uzaklığına bakarak yaparken bu çalışmada Counting Bloom Filtresi kullanılarak kıyaslama yapılmıştır. Bu filtre ile kıyaslamada iki vektör aynı ise uzaysal koordinatlarında aynı yere noktalanır. Eğer aynı yere noktalanan birden fazla vektör varsa, bunlar birbirine eş değer yani kopyala-yapıştır sahteciliği ile oluşturulmuş vektördür denir. Bu yöntem kullanılarak çalışmaya hız kazandırılmıştır. Bunun sebebi özellik matrisinin bir kere taranarak sonuca ulaşılmasıdır.

Bu çalışmanın dezavantajı ise 10^o'den fazla döndürme açısı ataklarına karşı dayanıksız olmasıdır. Bunun sebebi ilk önce görüntüye Fourier Dönüşümü 'nün uygulanmasıdır. Yani oluşan Ayrık Fourier görüntüsü ile gerçek görüntünün birbirine benzemiyor olmasıdır. Eğer döndürme bağımsız yöntem olan log-polar yöntem öncelikli uygulanmış olsaydı ataklara karşı dayanıklılık artırılmış olurdu.

Khan ve Kulkarni'nin çalışmasında zamansal karmaşıklığı iyileştirmek için örtüşen bloklardan oluşan görüntüye öncelikle ADD dönüşümü uygulanmış ve görüntünün özellik vektörünün boyutu küçülmüştür [24]. Blokların içerisindeki en yüksek parlaklık değerine sahip piksel seçilerek özellik matrisi oluşturulmuştur. Amaç düşük kontrast değerlerini işleme katmadan zamansal karmaşıklığı iyileştirmektir. Özellik matrisi sıralandıktan sonra matrisin satırları arasında faz korelasyonu yapılmıştır. Eşleşen bloklar tespit edilerek farklı seviyelerde ADD işlemi gerçekleştirilmiştir. Çalışmanın JPEG ve gürültü ataklarına karşı daha iyi sonuçlar elde etiiği raporlanmıştır. Ancak döndürme ve ölçekleme ataklarına karşın sonuçların istenilen derecede olmadığı belirtilmiştir.

Wu ve arkadaşlarının çalışmasında, Bayram ve arkadaşlarının önerdiği yöntemin [23] işlem adımlarının sırası değiştirilerek yeni bir metot önerilmiştir [25]. Görüntü YCbCr uzayında sabit büyüklükte bloklara bölündükten sonra bu bloklara önce log-polar dönüşüm daha sonra Fourier yani ikisi birlikte Log-Polar Fourier Dönüşümü (LPFD) yöntemi uygulanmıştır. YCbCr uzayında Y kanalı kullanılmıştır. Bunun sebebi görüntü ile ilgili en önemli bilgilerin bu kanalda yer almasıdır. Log-polar yöntemi uygulandıktan sonra oluşan alt bloklar karesel değildir. Çembersel olan alt blokların yarı çapı r olarak belirlenip, blokların boyutu 2r'ye 2r olarak oluşturulmuştur. Log-polar yöntemini uygulamalarının amacı kopyalanıp, genişletme veya döndürme işlemleriyle sahteciliğe uğrayan görüntüyü tespit etmektir. Daha sonra Fourier uygulanması ise log-polar dönüşüm sonucu oluşan faz farkını Fourier'in öteleme bağımsızlığından yararlanmaktır. Fourier sonucu oluşan özellik vektörlerin oluşturduğu matrise Cross-Spectrum uygulanır. Cross-Spectrum, vektörlerin benzerlik oranlarını ikili ikili karşılaştırmasıdır. İki vektörün kıyaslaması sonucu oluşan pik büyüklüklerinin en fazla değere sahip olanları hafızaya kaydedilir. Belirlenen eşik değerini aşan pik değerleri sahte görüntü olarak işaretleniyor. Çalışmanın işlem maliyeti oldukça yüksektir. Bunun sebebi bütün vektörlerin ikili ikili karşılaştırılmasıdır. Çalışmada bu yöntemler gerçekleştirilerek görüntünün döndürme genişletme ve öteleme bağımsız olması hedeflenmiştir. Eşik değeri 0.1 ile 0.5 arasında deneyerek seçilmiştir. 0.3 olarak belirlenen eşik değeri yöntemin oldukça hassas yani etkili olduğunu gösterir. Sonuçlarında

çalışma [23]'e göre çok daha iyi olduğu sunulmuştur. Çalışmanın sonuç kısmında genellikle düz bir zemine sahip görüntüler seçilmiştir. Yani yeşillik bir alan üzerinde bir yaprağın kopyalanıp-yapıştırılması sonucunda yöntemin etkili olup olmadığı bir tartışma konusudur.

Wu ve arkadaşları bir önceki çalışmalarını [25] genişleterek bir sene sonra yeni bir metot önermişlerdir [26]. Yeni metotta, çalışma [25]'dekinden farklı olarak, görüntüye LPFD uygulamak yerine Log-Polar Hızlı Fourier Dönüşümü (LPHFD) uygulanıyor. Buradaki amaç hızlı Fourier dönüşümü uygulayarak, işlem maliyetinin azaltılması ve zamansal karmaşıklığı iyileştirmektir. Daha sonra oluşturulan vektörlerin benzer olup olmadığını tespit etmek için Cross-Spectrum uygulanır. Vektörler arasında 0.1 ve 0.5 arasındaki eşik değerini aşanlar sahteciliğe uğramıştır denilmiştir.

Huang ve arkadaşlarının yaptığı çalışmada görüntünün AKD ile oluşturulmuş 1x16'lık özellik vektörleri kırpma işlemi ile 1x8'lik vektörlere dönüştürülmüştür [27]. Bunun sebebi zamansal karmaşıklık sorununa çözüm bulmaktır. Daha sonra özellik matrisi oluşturulup Leksikografik olarak sıralanmıştır. Önerilen yöntemde özellik vektörlerinin karşılıklı elemanları arasındaki toplamsal fark göz önüne alınarak sabit eşik değeri kullanmaktadır. Benzer vektörler tespit edilerek kopyala-yapıştır sahteciliği tespit yöntemi gerçekleştirilmiştir. Sonuçlara göre JPEG ve bulanıklaştırma ataklarına karşı dayanıklıdır.

Ghorbani ve arkadaşlarının çalışmasında ADD ve Ayrık Kosinüs Dönüşüm-Kuantizasyon Katsayıları Ayrıştırma (AKD-KKA) yöntemi birlikte kullanılarak gelişmiş bir algoritma sunulmaktadır [28]. Görüntü öncelikle zamansal karmaşıklığın azaltılması için ADD yöntemi ile alt bantlara bölünmüştür. Daha sonra alçak bantlarda yani düşük frekanslarda görüntüyü birbiriyle örtüşen bloklara ayırmışlardır. Öznitelik vektörü oluşturmak için kendi önerdikleri AKD-KKA algoritmasını kullanmışlardır. Daha sonraki işlem adımları kopyala-yapıştır sahteciliği tespiti yöntemlerindeki genel adımlar gibi devam etmektedir. Çalışmada işlem maliyeti olarak sonuçların daha iyi olduğu belirtilse de, çalışma yüksek sıkıştırma oranına sahip ataklara karşı dayanıksızdır.

Muhammad ve arkadaşlarının çalışmasında, literatürde ilk olarak özellik vektörü çıkartmak için İkili Dalgacık Dönüşümü (İDD) kullanılmıştır [29]. Bu yöntemde görüntü düşük seviye frekansına sahip LL1 ve yüksek seviye frekansına sahip HH1 bandına bölünmüştür. LL1 ve HH1 bantları üst üste gelecek şekilde birbiriyle örtüşen bloklara ayrıştırılarak genel kopyala-yapıştır sahteciliği tespiti algoritması adımları işlenmiştir. LL1 ve HH1 bantlarına ayrıştırmalarındaki ama ise yüksek frekansa sahip bantlarda benzerlik

oranının düşük olması, düşük seviyeli bantlarda ise benzerlik oranının yüksek olmasıdır. Böylece düşük seviyeli bantlarda kopyala yapıştır sahteciliği tespiti daha kolay ve işlem maliyetini azaltarak tespit edilmiştir. Literatürde yer alan bazı çalışmalara göre iyi olduğu çalışmanın sonuçlar kısmında yer almıştır.

Bravo ve arkadaşlarının yaptığı çalışmada, kopyalanan kısımlara döndürme veya ölçeklendirme atakları yapılsa dahi sahtecilik tespitini gerçekleştirebileceklerini kanıtlamışlardır [30]. Önerilen yöntemde, birbiriyle örtüşen piksel bloklarının log-polar koordinatları eşleştirilir. Daha sonra açı ekseni boyunca toplanır, ölçeklendirme ve dönmeye karşı değişmeyen tek boyutlu (1B) tanımlayıcı özellik vektörü elde edilir. Her bloğun boyut küçültülmüş gösterimi, benzer bölgelerin tespiti için gerçekleştirilen tarama hesaplama maliyetinde olumlu bir etkiye sahip olduğu öne sürülmüştür. Önerilen yöntemin etkinliğini göstermek için Myna [19] ve Pan [43]'ın çalışmalarıyla karşılaştırılmıştır.

Hsu ve Wang tarafından yapılan blok tabanlı çalışmada, özellik vektörü oluşturmak için bloklara Gabor filtresi uygulanmıştır [31]. Özellikle Gabor filtresinin kullanmalarının sebebini, çok küçük ve küçük bölgelerde yapılan kopyala yapıştır sahteciliğini tespit etmek içindir. Daha sonraki işlem adımları kopyala-yapıştır sahteciliği tespiti yöntem adımlarıyla aynıdır. Yani birbiriyle örtüşen blokları Leksikografik olarak sıralıyıp, aralarındaki benzerlik oranına Öklid uzaklık ölçme algoritmasıyla bakılıp en sonunda benzer bölgelerin boyanmasıyla tespit işlemi gerçekleştirilmiştir. Önerilen yöntem literatürde var olan ve özellik vektörü oluşturmak için yine Gabor filtresi kullanılan Gharibi ve arkadaşlarının [32] çalışmasıyla karşılaştırılmıştır. Karşılaştırma sonucunda daha yüksek doğruluk oranı, döndürme ve ölçekleme ataklarına karşı dayanıklıklık sağlandığı gösterilmiştir.

Wandji ve arkadaşı literatürde daha önce de [17] numaralı çalışma tarafından denenmiş olan, görüntü üzerinde ön işlem olan gri seviyeye dönüştürme işlemi olmadan, renkli görüntü üzerinde çalışılmıştır [33]. Renkli görüntü üzerinden birbirleriyle örtüşen bloklara ayrılan görüntüden 10 elemanlı özellik vektörleri oluşturulur. Oluşturulan özellik vektörünün ilk değeri görüntüden oluşturulan YUV (**Y** Luminance, **U** Chrominance-1, **V** Chrominance-2 kısaltmasıdır.) renk uzayından elde edilen Y değeridir. Y bileşini gri seviye, U ve V değeri ise mavi ve kırmızı tabanlı renkliliği temsil eder. Görüntü bu üç değer ile temsil edilir. 10 elemanlı özellik vektörünün geriye kalan 9 elemanını, RGB uzayının gri seviye değer ortalaması, ortalama zıtlık değerleri ve hesaplanan moment değerleri oluşturur. Daha sonra genel blok tabanlı yaklaşımlardaki gibi özellik

vektörleriyle matris oluşturulur, matrisin elemanları Leksikografik sıralanır ve benzer bloklar boyanır. Yapılan çalışmanın sonuçlarında düşük JPEG sıkıştırma, bulanıklaştırma ve gürültü ataklarına karşı sonuçları yer almaktadır. Ancak sonuçlar literatürde yer alan herhangi bir yapılan çalışma ile karşılaştırılmamıştır. Bunun yanı sıra doğruluk ölçütü değeri ile herhangi bir sonuç alınmayıp sadece görüntü görselleri ile sonuçlar verilmiştir.

Li ve arkadaşlarının yaptığı çalışmada görüntü ön işlem olan gürültü filtresinden geçirilir ve literatürde daha önceki [25]. çalışmada görüldüğü gibi çembersel bloklara ayrıştırılır [34]. Özellik vektörü oluşturmak için bloklara Yerel İkili Örüntü (Local Binary Patterns, LBP) uygulanır. Yöntemin diğer adımlarında, blok tabanlı yöntemlerin genel yapısında olduğu gibi özellik vektörleri Leksikografik olarak sıralanır ve eşleştirilir. Çalışmanın sonuçlarında JPEG kalite faktörü, Gauss gürültüsü ekleme ve bulanıklaştırma, döndürme, ölçekleme gibi ataklara karşı dayanıklılık test edilmiş ve test sonuçlarında başarı elde edilmiştir.

Li ve arkadaşları bir yıl sonra tekrar görüntüyü çembersel bloklara ayrıştırarak, özellik vektörü oluşturmak için Polar Harmonik Dönüşümü (PHD) uygulamışlardır [35]. Blok tabanlı sahtecilik tespiti genel adımlarındaki gibi özellik vektörlerini matriste toplamışlardır. Daha sonra özellik matrisini Leksikografik olarak sıralayarak, benzer vektörleri eşleştirmişlerdir. Deneysel bulgularda bir önceki çalışmalarıyla ve literatürde var olan JPEG sıkıştırma, gürültü, döndürme ve ölçekleme ataklarına karşı test sonuçları verilmiştir.

Lee ve arkadaşlarının çalışmasında renkli görüntüye ön işlem uygulayarak gri seviyeli görüntü üzerinde çalışmışlardır [36]. Gri seviyeli görüntüden, Gradyan Histogramını (Histogram of Gradient, HOG) kullanarak özellik vektörü oluşturmuşlardır. Blok tabanlı yöntemlerin genelinde uygulandığı gibi vektörler Leksikografik olarak sıralanıp, benzer vektörler eşleştirilmiştir. Yanlış eşleşmelerin giderilmesi için 16x16 boyutlarında bir çerçeve, tüm görüntü üzerinde gezdirilmiştir. Aynı çerçevede, belirlenen eşik değerinden az eşleşme gerçekleşirse, bu noktaları yanlış eşleştirme olarak değerlendirmişlerdir. Yapılan çalışmada tek bir görüntü üzerinde birden fazla gerçekleştirilen kopyala-yapıştır sahteciliğinin tespit edildiği ispatlanmıştır. Çalışmanın sonuçlarında bulanıklaştırma, döndürme ve piksel parlaklık değişikliği gibi ataklara karşı dayanıklı olduğu test edilmiş ve başarılı gerçekleşen sonuçlar verilmiştir.

Üstübioğlu ve arkadaşlarının çalışmasında görüntü alt bloklara ayrıldıktan sonra görüntüye AKD dönüşümü uygulanmıştır [37]. Oluşturulan alt blokların AKD enerji

olasılık değerleri hesaplanarak 1x10 boyutunda özellik vektörleri oluşturulmuştur. Daha sonra özellik vektörleriyle oluşturulan matris Leksikografik olarak sıralanmıştır. Önerilen yöntemin diğer yöntemlere göre farkı statik bir eşik değeri belirlemek yerine, elde edilen benzerlik oranlarının kullanılarak eşik değeri oluşturmasıdır. Çalışmanın sonuçlarında JPEG ve gürültü ataklarına karşı dayanıklılık test edilmiş ve başarılı olduğu kanıtlanmıştır. Çalışmanın diğer çalışmalardan farkı ise özellik vektörlerini karşılaştırırken belirlenecek olan eşik değerini kendi içinde alacağı tam sayı değer aralığının hesaplanmasıdır.

Moussa'nın önerdiği blok tabanlı çalışma da görüntü birbiri ile örtüşen karesel bloklara bölünür [38]. Daha sonra blokların her biri eşit aralıklı k tane alt bloklara bölünür. Her alt bloğun piksel yoğunluğunun toplamı, kaydırılan matris yardımıyla bir k boyutlu vektör oluşturmak için kullanılır. Oluşturulan vektör, her blok için bir özellik olarak kullanılır. Tüm blokların ortaya çıkardığı özellik vektörleri bir K-D ağaçları'nda (K-Dimensional Tree) saklanır. K-D ağacındaki her bir düğüme karşılık gelen blok, bu düğümün en yakın komşusuna karşılık gelen blok ile kontrol edilir. Bu tip bloklar arasındaki korelasyon önceden belirlenmiş bir eşiğin üstünde ise, iki blok sahte olarak kabul edilir. Önerilen kopyala-yapıştır sahteciliği tekniği, sahtecilik sorununu çözmenin hızlı ve çok basit bir yolunu sunar. Bununla birlikte, geometrik transformasyon durumunda (yani, rotasyon veya ölçek) tespit performansının düşeceği de belirtilmiştir.

Boz ve Bilge önerdikleri blok tabanlı çalışmada LBP ve AKD yöntemlerini bir arada kullanmışlardır [39]. Çalışmada ilk olarak görüntü gri seviyeye çevrilerek, bxb 'lik alt bloklara bölünür. Çalışmada en yüksek değerler 8x8'lik bloklar ile görüntü tarandığında elde edilmiştir. Her bir bloğa LBP yöntemi uygulanarak, görüntü blokları LBP alanlarına dönüştürülmektedir. Daha sonra bloklara AKD yöntemi uygulanarak oluşturulan vektörler öznitelik matrisinde toplanır. Matris Leksikografik olarak sıralanarak benzer vektör bloklarının ardışık sıralanması sağlanarak işlem maliyeti azaltılır. Önce LBP daha sonra da AKD uygulanarak önerilen çalışmanın aydınlatma koşullarına daha az duyarlı özellik vektörleri oluşturması amaçlanmıştır. Çalışmanın sonuçlarında JPEG sıkıştırma, döndürme, ölçekleme ve gürültü ekleme ataklarına karşı sonuçlar değerlendirilmemiştir. Önerilen yöntem literatürde var olan diğer yöntemlerle karşılaştırılmamış, sadece LBP ve AKD'nin tek başına uygulandığı iki çalışma ile karşılaştırılmıştır.

Mahmood ve arkadaşlarının önerdikleri çalışmada, Yerel İkili Örüntü Varyansı (LBPV) ile birlikte daha önce özellik vektörü oluşturmak için kullanılan Sabit Dalgacık Dönüşümü (SWT, Stationary Wavelet Transform) yöntemini bir arada kullanan yeni bir

kopyala-yapıştır sahteciliği tespiti yöntemi yer almaktadır [40]. Yöntem, ön işlem sırasında hedef görüntüyü gri seviyeye dönüştürerek, SWT uygulanır. Daha sonra düşük frekanslı bileşenler işleme devam edilmek için seçilir. Seçilen bant üzerindeki değerlere LBPV yöntemi uygulanarak oluşturulan dairesel bloklardan özellik vektörü elde edilir. Önerilen yöntem CoMoFoD veri seti üzerinde döndürme, bulanıklaştırma, ölçeklendirme, renk azaltma ve parlaklık değişimi gibi ataklara karşı dayanıklılığı test edilmiştir.

Wang ve arkadaşları, LBP ve Tekil Değer Ayrışımı (SVD, Singular Value Decomposition) yöntemini bir arada kullanarak yeni bir sahtecilik tespiti yöntemi önermişlerdir [41]. İlk olarak, yöntem görüntüyü örtüşen bloklara böler ve her bloğu etiketlemek için LBP'yi kullanır. Daha sonra işlenmiş, LBP etiketli görüntüden hesaplanan SVD katsayılarının işaret bilgisini içeren özel bir vektör kullanır. Yani SVD değerleri ortalama Y, Cb, Cr değerleri ile blok için özellik vektörünü oluşturur. Ardından, en büyük N SVD değeri etiketli bloklarda çıkarılır. Son olarak, özellik vektörleri Leksikografik olarak sıralanır ve benzer blokları belirlemek için elemanlar arası benzerlik ölçümü eşik değeri kullanılır. Deney sonuçlarında literatürde var olan bir çalışma ile karşılaştırılma yapılmamış olup kendi ölçütlerine göre çalışma değerlendirilmiştir ve başarılı sonuçlar verilmiştir.

Hosny ve arkadaşları yaptıkları çalışmada, alt görüntü oluşturmak için algılanan nesnenin çevresine bir sınırlayıcı olarak dikdörtgen çizmiştir [42]. Morfolojik operatör ile gereksiz küçük cisimler elimine edilmiştir. Yüksek doğruluk oranına sahip olan PCET (Polar complex exponential transform) momentleri yöntemi kullanılarak, tespit edilen nesneler için özellik vektörleri oluşturmuşlardır. Özellik vektörleri arasındaki öklid uzaklık ve korelasyon katsayısı hesaplanarak, sahtecilik ile kopyalanan nesneleri aramak için kullanılmıştır. Kopyalanan nesnelerle 20 sahte görüntü veri seti daha önce yayınlanmış, literatürdeki çalışmalardan seçilmiştir. Diğer 80 sahte görüntü yazarlar tarafından düzenlenip farklı türdeki nesneler çoğaltılarak oluşturulmuştur. Önerilen yöntemin çoğaltılmış nesne türünü başarıyla tespit ettiği sayısal simülasyonlarla gösterilmiştir. Önerilen yöntem önceden var olan yöntemlerden çok daha hızlı olmasının yanında; Gauss gürültüsü, JPEG sıkıştırma, döndürme ve ölçeklendirme gibi çeşitli saldırılara karşı yüksek sağlamlık göstermiştir.

Literatürde yer alan önemli çalışmalardan çıkarılan sonuç, blok tabanlı yöntemlerin JPEG sıkıştırma atağına karşın oldukça etkili olduğudur. Bunun yanı sıra ölçekleme ve döndürme ataklarına karşı iyi sonuçlar elde edemediğidir.

1.2.2. Anahtar Tabanlı Yöntemler

Literatürde, blok tabanlı yöntemlerde tespit edilen eksiklikleri gidermek ve işlem maliyetini azaltmak için anahtar tabanlı yöntemler önerilmiştir. Yöntemin adından da anlaşıldığı gibi, görüntüden özellik vektörü çıkartmak için bloklara ayrıştırmak yerine, özel olarak belirlenen anahtar noktaları tanımlayıcıları kullanılır. Her anahtar bir piksele karşılık gelmektedir. Renk değişimleri, kenarlar ve dokular anahtar noktası çıkarmak için ideal bölgelerdir.

Anahtar tabanlı yöntemlerin başlangıcı Pan ve Lyu tarafından 2010 yılında yapılmıştır [43]. Çalışmada Ölçek Bağımsız Öznitelik Dönüşümü (Scale Invariant Feature Transform, SIFT) ile anahtar noktası tanımlayıcıları elde edilmiştir. Özellik vektörleri oluşturulduktan sonra eşleştirme için Best Bin First (BBF) algoritması kullanılmıştır. Çalışma sonucunda eşleşen anahtar noktaları gösterilmiştir ve ölçeklendirme ve döndürme ataklarına karşı başarılı olduğu gösterilmiştir. Aynı yıl Pan ve Lyu önerdikleri bir diğer çalışmada sahteciliği tespit etmek için aynı işlem adımlarını takip ettikten sonra eşleştirme kısmında yeni bir yöntem kullanmışlardır [44]. Hatalı eşleştirmelerin giderilmesi ve yüksek doğruluk oranına sahip sonuçlara ulaşmak için Random Sample Consensus (RANSAC) yöntemini metoda eklemişlerdir. Yapılan çalışmanın deneysel sonuçlarında ilk çalışmalarından, Popescu ve arkadaşlarının [16] çalışmasından daha iyi olduğunu ispatlamışlardır.

Bo ve arkadaşları anahtar noktası çıkartmak için yeni bir yöntem olan Hızlandırılmış Dayanıklı Öznitelikler (Speed up Robust Feature, SURF) algoritmasını kullanmışlardır [45]. SURF yöntemi ile anahtar noktaları iki gruba ayrılır ve gruplar arasında en yakın komşular arasındaki oran değerlendirilir. Çalışmanın sonucunda SURF yöntemi ile yanlış eşleştirmeleri özellikle yüksek çözünürlüklü görüntülerde azaldığı tespit edilmiştir. Ayrıca sonuçlarda ölçeklendirme, döndürme, bulanıklaştırma ve gürültü ekleme gibi ataklara karşı dayanıklılık test edilmiş ve başarılı olan sonuçlar değerlendirilmiştir. Yöntemin dezavantajı küçük bölgeler üzerinde yapılan sahtecilikleri tespit edememesidir.

Amerini ve arkadaşlarının yaptığı çalışma literatürde anahtar tabanlı yapılan çalışmanın en önemli olanlarından biridir ve birçok çalışmanın kıyaslama kıstasında yer almaktadır [46]. Anahtar noktası oluşturmak için kullandıkları SIFT yönteminden sonra hiyerarşik kümeleme ve geometrik tahmin dönüşümü yöntemlerini kullanarak daha

kapsamlı özellik vektörleri oluşturmuşlardır. Eşleştirmeyi gerçekleştirdikten sonra daha önceki çalışmalarda yapıldığı gibi yanlış eşleşmelerin giderilmesi için RANSAC metodunu kullanmışlardır. Önerilen yöntemin, aynı görüntü üzerinde bir ve birden fazla yapılan sahtecilikleri tespit ettiği ispatlanmıştır. Deney sonuçlarında önerilen yöntemin JPEG sıkıştırma, döndürme ve gürültü ataklarına karşı başarılı olduğu kanıtlanmıştır. Amerini ve arkadaşlarının yaptığı bir başka çalışmada önceki yaptıkları çalışmayı geliştirmek için eşleştirme adımında geometrik dönüşüm alanında dayanıklı J-Linkage algoritmasını kullanmışlardır [47]. J-Linkage algoritması başlangıçta her anahtar noktasını bir küme olarak alır. Daha sonra aralarında en az uzaklık olan anahtar noktaları birleştirilir. Kümeler arasındaki mesafe hesaplanarak, bütün anahtar noktaları tek bir demet yani tek bir küme içinde kalana kadar devam edilir. Aynı küme içerisinde kalan farklı anahtar noktalarında sahtecilik yapıldığı düşünülerek kaydedilmiştir. Anahtar noktaları kümelenerek sahtecilik yapılan bölge veya bölgelerin tespiti gerçekleştirilmiştir. Daha önceki kendi çalışmalarıyla karşılaştırarak, farklı veri setleri üzerinde önerdikleri yöntemin başarılı olduğunu kanıtlamışlardır.

Yu ve arkadaşları önerdikleri yöntemde anahtar noktalarını elde etmek için Harris Corner yöntemini kullanmışlardır [48]. Harris Corner yöntemini önermelerinin sebebini daha önceki çalışmalarda kullanılan SIFT ve SURF yöntemlerinin smooth (pürüzsüz) bölgelerde özellik çıkarmakta zorlandığı için kopyala-yapıştır sahteciliği tespitinin yapılamaması olduğunu belirtmektedirler. Daha sonra elde edilen anahtar noktalarından özellik tanımlayıcıları elde etmek için Non-Maximal Suppression (NMS) ve Multi-Support Region Order-Based Gradient Histogram (MROGH) algoritmaları birleştirilmiştir. Özellik tanımlayıcılarının eşleştirmesinde k-d ağaçları, 2NN (iki en yakın komşu) komşuluk arama yöntemiyle birlikte kullanılmıştır. RANSAC yöntemi ile hatalı eşleştirmeler giderilip kopyala-yapıştır sahteciliği tespiti yapılmıştır. Çalışmanın sonuçlar kısmında SIFT ve SURF tabanlı yöntemlere göre daha iyi performansa sahip olduğu belirtilmiştir. Ayrıca çalışmanın sonucunda JPEG, gürültü, döndürme ve ölçekleme ataklarına karşı dayanıklılık sonuçları verilmiştir.

Zhu ve arkadaşlarının önerdiği yöntemde anahtar noktası oluşturmak için Hızlı ve Döndürülmüş Kısa Yönlü (Oriented Fast and Rotated Brief, ORB) algoritmasını kullanmışlardır [49]. ORB algoritmasını kullanmalarının sebebini düşük hesaplama maliyeti ve döndürmeye karşı bağımsızlık kazanmak için olduğunu vurgulamışlardır. Ölçeklendirme ataklarına karşı dayanıklılık için ise ilk önce görüntü Gauss ölçekleme

uzayına dönüştürülmüştür. ORB ile anahtar noktaları çıkartıldıktan sonra Hamming uzaklığı ölçerek anahtar noktaları arasındaki benzerlik hesaplanmıştır. Daha önceki çalışmalarda olduğu gibi yanlış eşleştirmelerin giderilmesi için RANSAC algoritması kullanılmıştır. Çalışmanın sonuçlar kısmında JPEG, döndürme, ölçekleme, gürültü ataklarına karşı başarılara yer verilmiştir. Önerilen yöntem Bo [45] ve Amerini'nin [47] arkadaşlarıyla yaptığı çalışmalar ile karşılaştırılmış ve daha başarılı oldukları ispat edilmiştir.

Zandi ve arkadaşları kopyala-yapıştır sahteciliği tespiti için yinelemeli iyileştirme stratejisi kullanan yeni bir yöntem önermişlerdir [50]. Önerdikleri yöntem ile düşük kontrastlı bölgelerde bile anahtar noktası tespiti gerçekleştirdiklerini kanıtlamışlardır. Anahtar noktası tespiti için Zernike Momentleri ve Polar Cosine Transform (PCT) algoritması kullanılmıştır. Segmentasyon tabanlı çalışan yöntemde görüntüyü segmentlere ayırmak için Simple Linear Iterative Clustering (SLIC) algoritması kullanılmıştır. Segmentler oluşturulurken entropi bilgisine başvurulur. Alt segmentler dokusuz (smooth), dokulu (texture) ve daha çok dokulu (strong texture) olarak sınıflandırılır. Segmentler içindeki anahtar noktaları kendi segmentleri içerisinde eşleştirilmiştir. Bu çalışmada yanlış eşleşmenin hızla giderilmesi için yeni bir filtreleme algoritması da önerilmiştir. Son olarak dönüşüm tahmini yapılır ve yanlış eşleştirme olduğu düşünülen eşleştirmeler silinir. Performansın SBU-CM16 adlı diğer çalışmalarla karşılaştırılması için yeni bir veri seti hazırlamışlardır. Veri seti, 800 × 580 boyutunda hem doku içeren hem de pürüzsüz alanlara sahip 240 sahte görüntü içermektedir. Ayrıca, çalışmanın sonucu literatürde var olan Zernike Monentleri, SURF, J-SIFT, GoDeep metodlarıyla anahtar oluşturan diğer çalışmalarla JPEG sıkıştırma, gürültü, döndürme ve ölçekleme ataklarına karşı test edilmiştir.

Warif ve arkadaşları genel geometrik dönüşüm ve yansıma tabanlı saldırılara karşı dayanıklılık için yeni bir anahtar noktası tabanlı yaklaşım önermişlerdir [51]. Ayrıca SIFT-Simetri adı verilen ve SIFT tabanlı kopyala-yapıştır sahteciliğini algılama yöntemini, simetri tabanlı eşleştirme ile yenilikçi bir şekilde birleştirmişlerdir. g2NN ve önerilen simetri eşleştirme tekniğini kullanarak iki aşamalı bir eşleştirme işlemi önermiştir. g2NN tekniği ilk eşleştirme aşamasında ilk kez uygulanmıştır. Daha sonra anahtar noktalarını eşleştirmek için uygulanan simetri eşleştirmesi, simetri büyüklüğünü hesaplamak için ölçek ve faz ağırlık bilgisi kombinasyonuna dayanmaktadır. Deneysel bulgularında SIFT-Simetri yönteminin F ölçütü, %65.3 ortalama F ölçütüne sahip olan bir rotasyon durumu

ile yansıma dışında, basit dönüşüm ve yansıma bazlı ataklar dâhil tüm geometrik dönüşüm durumları için ortalama %80 değerini aştığını göstermişlerdir.

Wang ve arkadaşları görüntüde kilit noktaları diye adlandırdıkları pürüzsüz (smooth) bölgelerde yapılan sahtecilikleri daha iyi tespit etmek için yeni bir anahtar noktası tabanlı yöntem önermişlerdir [52]. İlk olarak, sahte görüntüden rastgele ve düzensiz süper piksel olarak adlandırılan pikseller seçilir. Süper pikseller, yerel bilgi entropisine dayalı olarak düzgün doku ve güçlü doku olarak sınıflandırılırlar. İkinci adımda, anahtar noktaları, süper piksel içerikli uyarlamalı özellik noktaları detektörü kullanılarak, düzgün doku ve güçlü doku olanlar dahil olmak üzere her bir süper pikselden çıkarılır. Kümelere ayrılan anahtar noktaları algoritmanın bir sonraki adımında, kümeler arasındaki uzamsal mesafeyi hesaplanarak, en yakın mesafeye sahip küme çifti için tekrar tekrar aranır ve birleştirilir. Eşleştirme işleminden sonra yanlış eşleştirilen anahtar noktaları RANSAC ile elimine edilir. Çalışmanın deneysel bulguları geometrik dönüşümlere, JPEG sıkıştırma ve beyaz Gauss gürültüsü ekleme gibi çeşitli ataklara karşı test edilmiştir.

Alberry ve arkadaşlarının önerdiği anahtar noktası tabanlı çalışmada SIFT ve Kümeleme için Bulanık C Araçları (Fuzzy C-Means Clustering, FCMC) yöntemi kullanılmıştır [53]. Görüntü gri seviyeye dönüştürüldükten sonra SIFT yöntemi ile anahtar noktaları belirlenir. Gerçek eşleşme adımından önce tespit edilen SIFT ana noktalarının kümelenmesi için FCMC'yi uygulanır. Bu sayede hızlandırılmış bir eşleştirme işlemine yol açan hesaplama karmaşıklığı azaltılır. MICC-220 veri seti kullanılarak test sonuçları verilmiştir. Her ne kadar makale çeşitli veri setlerine karşı bir dizi test sonucu verilse de, literatürde var olan herhangi bir çalışma ile karşılaştırılma yapılmamış ve ataklara karşı dayanıklılık test edilmemiştir.

Literatürde yer alan anahtar noktası tabanlı çalışmalardan çıkarılan sonuç ölçekleme, öteleme ve döndürme ataklarına karşı oldukça etkilidirler. Ancak smooth (pürüzsüz) dediğimiz gökyüzü, yeşillik gibi alanlarda yapılan sahteciliklerde istenilen sonuç aralıklarına ulaşılamamasıdır.

1.2.3. Hibrit Yöntemler

Son olarak literatürde yer alan, blok ve anahtar tabanlı yöntemlerin avantajlarının bir arada kullanılarak oluşturulan kopyala-yapıştır sahteciliği tespiti yöntemlerine hibrit yöntemler denir. Bu yöntemlerin temeli blok tabanlı yöntemlerin dezavantajlı oldukları

yerlerde anahtar tabanlı metotları kullanmak, aynı şekilde anahtar tabanlı yöntemlerin dezavantajlı oldukları yerlerde blok tabanlı metotları kullanarak birbirlerini tamamlamalarını sağlamaktır. Birbirleriyle uyumlu algoritmalar kullanılarak oluşturulan hibrit yöntemler istenilen değer aralıklarında sonuçlar vermektedir.

Christlein ve arkadaşları anahtar noktası tabanlı ve blok tabanlı yöntemleri birleştiren hibrit bir kopyala-yapıştır sahteciliği tespiti tekniği önermişlerdir [54]. Test görüntüleri için kendi oluşturdukları veri setini kullanmışlardır. Bu veri setine ayrı ayrı anahtar noktası tabanlı (SIFT ve SURF) ve blok tabanlı yöntemleri (AKD, PCA, ADD ve Zernike) bir arada kullanarak uygulamışlardır. Bu algoritmaların performansları karşılaştırmışlardır. Sonuçlar, anahtar noktası tabanlı yöntemlerin blok tabanlı yöntemlerden önemli ölçüde daha hızlı olduğunu göstermektedir. Ancak anahtar noktaya dayalı yöntemler genellikle yüksek doğrulukta algılama gerçekleştirmediğini belirtmişlerdir. Bu nedenle, Christlein ve arkadaşları hem anahtar noktası hem de blok tabanlı yöntemlerin bir araya getirilmesi, birçok yönden daha iyi performans sağlayacağını test sonuçları ile göstermişlerdir.

Hashmi ve arkadaşlarının önerdiği çalışmada kopyala-yapıştır sahteciliği tespiti yöntemlerinin dezavantajı olan işlem karmaşıklığını önlemek için ADD tabanlı, SIFT kullanan bir algoritma önerilmiştir [55]. Bu çalışmanın temel amacı, doğru eşleşmeleri artırmak ve sürecin işlem maliyetini azaltmaktır. İlk olarak, eğer görüntü RGB formattaysa, ADD ile gri seviyeye indirgenir. Görüntü bantları LL, LH, HL ve HH olmak üzere dört gruba ayrılır. LL bandı görüntü bilgilerinin en önemli bölümünü içerdiğinden, SIFT yöntemi yalnızca ana özelliği çıkarmak için bu gruba uygulanır. Hibrit algoritmanın SIFT uygulamalarının birinci nedeni, öteleme, ölçeklendirme ve döndürmeden bağımsız olan özellik vektörünü oluşturmaktır. İkinci neden ise, SIFT'in gürültü ataklarına karşı dayanıklı olmasıdır. Önerilen yöntem, MICC-F220 veri setinde 100 görüntü üzerinde test edilmiştir. Sahtecilik tespiti her görüntü için farklılık gösterse de ortalama 2,893 saniye olarak belirtilmiştir. Test görüntüsündeki kopyalanan ve yapıştırılan bölge azaltılırsa, ortalama süre 2 saniye olarak hesaplanır. Çalışma sonuçları sadece Popescu [16], Li [18] ve Zhang'ın [21] çalışmalarıyla karşılaştırılmıştır ve önerilen yöntem daha iyi sonuçlar aldığı kaydedilmiştir. Bununla birlikte, pürüzsüz bölgeler üzerinde nesneleri kapatmanın ne kadar başarılı olduğu test edilmemiştir.

Ardizzone ve arkadaşlarının önerdiği çalışmada blok tabanlı yöntemlerin yerine, anahtar noktalarından oluşturdukları üçgen noktaları karşılaştıran yeni hibrit bir yaklaşım önermişlerdir [56]. Oluşturulan üçgen bölgelerin şekillerine (iç köşelere), içeriğe (renk

bilgisine) ve köşelerine (yerel tanımlayıcılara) göre üretilen özellik vektörlerine göre eşleştirme işlemini gerçekleştirmişlerdir. Bu yöntem, test görüntülerinde meydana gelen yanlış anahtar eşleşmelerinin % 20-25'ini siler. Bu adımdan sonra, üçgenlerin merkezleri hesaplanır ve daha fazla yanlış eşleşmeyi gidermek için merkez kümeye RANSAC uygulanır. Böylece, işlem karmaşıklığının dezavantajı yeni önerilen hibrid yöntemle çözülmektedir. Sonuçlar kendi oluşturdukları veri setleri [57] ve Christlein'in [54] veri setleri ile test edilmiştir. Çalışmanın sonuçları Christlein'in [54] sonuçlarıyla karşılaştırılmış ve önerilen yöntemin daha iyi olduğu kayıt altına alınmıştır.

Tatkare ve arkadaşlarının önerdikleri çalışmada doğruluk performansını arttırmak için SIFT ve Hue Moments yöntemlerinin avantajları bir araya getirilerek yeni bir yöntem öne sürülmüştür [58]. Algılama performansını ölçmek için MICC-F220 ve MICC-F2000 veri setleri kullanılmıştır. Hem SIFT hem de Hue momentlerinin ön işlemden geçirilmesinden sonra öznitelik vektörü elde edilir. Elde edilen özellik vektörlerinin ağırlıklı öklid mesafesi ölçülür. Önerilen yöntemde SIFT ve Hu momentleri seçilmesinin nedenini geometrik transformasyon durumunda (yani, rotasyon veya ölçek) dayanıklı olması olduğu yapılan çalışmada vurgulanmıştır. Çalışma sonuçları, önerilen hibrid sistemin % 92'nin üzerinde bir doğruluk elde ettiğini, SIFT'in ise tek başına % 67'yi ve Hue'nun bireysel olarak % 70 doğruluk elde ettiğini ifade ediyor. Bu çalışmada da hibrit sistemlerin ayrı ayrı yöntemlerin dezavantajlarının en aza indirebileceğini ve daha iyi sonuçlar elde edebileceğini göstermektedir.

Prasad ve arkadaşlarının yaptığı çalışmada SIFT-HOG ve SURF-HOG olarak iki hibrid yönteminin birbiriyle karşılaştırılması gerçekleştirilmiştir. Özellik vektörleri ayrı ayrı SIFT, SURF ve HOG ile elde edilerek hibrit sahtecilik tespiti algoritmalarının sonuçlarının daha iyi olduğunu göstermiştir [59]. SIFT'in faydaları, ölçeklendirme, çeviri ve döndürme bağımsızlığı ve SURF'un HOG'da düşük işlemsel karmaşıklık avantajları ile birleştirilmiştir. Önerilen yöntem, MICC-F220 veri seti üzerinde değerlendirilmiştir. SIFT-HOG test sonuçlarının önerdikleri hibrit yöntemler içinde daha iyi bulunduğu kayıt altına alınmıştır. Ancak, F ölçütü metriği test sonuçlarında açıkça belirtilmemiştir.

Bi ve arkadaşları gerçekleştirdikleri çalışmada hibrit kullanımın iyi bir örneğini göstermişlerdir [60]. Daha önce özellik vektörü oluşturmak için önerilen Geliştirilmiş Tutarlılığa Duyarlı (CSH) yöntemi ile Yerel Hassasiyet Karma (LSH) yöntemini geliştirerek Yerel Çift Yönlü Tutarlılık Hatası (LBCE) yöntemi ile özellik vektörü oluşturmuşlardır. Sadece oluşturulan özellik vektörleri eşleştirme için PatchMatch

algoritmasının eşleştirme kısımlarını kullanmışlardır. Çalışmanın sonuçlarında ilk olarak önerilen PatchMatch [63] yönteminden bazı ataklarda 3 bazı ataklarda 4 kat daha hızlı işlem hızına sahip bir yöntem olduğunu kanıtlamışlardır. Gerçekleştirilen çalışma JPEG sıkıştırma, döndürme, ölçekleme ve gürültü ataklarına karşı test edilmiş ve başarılı sonuçlar kaydedilmiştir. Test sonuçlarında piksel tabanlı F ölçütü değerlerinde JPEG sıkıştırma ve gürültü atakları hariç tüm hesaplamalarda yaklaşık olarak 0.9 değerinde başarılı sonuçlar elde etmişlerdir.

1.3. Yapılan Çalışmada Kullanılan Yöntemler ve Literatür Araştırması

Bu bölümde, yüksek lisans döneminde gerçekleştirilmiş olan çalışmalar ayrıntılı bir şekilde verilecektir. Tez çalışması aşamasında iki adet farklı yöntem gerçekleştirilmiştir. Bunlara ek olarak literatürde sahtecilik alanında denenmemiş bir alanda sahtecilik tespiti yöntemi gerçekleştirilerek, literatüre yeni bir bakış açısı getirilmiştir.

1.3. Yapılan Çalımalar Bölümü'nde ilk olarak kullanılan öznitelik vektörü oluşturmak için kullanılan (LIOP, PatchMatch, RINBP, SIFT) yöntemleri açıklanacaktır. Daha sonraki kısımda yanlış eşleştirmelerin giderilmesi için kullanılan yöntem olan RANSAC açıklanacaktır.

1.3.1. Yerel Yoğunluk Sıra Örüntüsü (Local Intensity Order Pattern, LIOP)

2011 yılında önerilen Yerel Yoğunluk Sıra Örüntü algoritması olan LIOP, kısaca parlaklık sırasına göre piksel parlaklık değerlerinin karşılaştırılmasıyla oluşturulan özellik tanımlamasıdır [61]. Yöntemin temel prensibi parlaklık seviyesi hep aynı tonda değişmesine rağmen alt bölgeler arasındaki parlaklık sıralamasının değişmemesine dayanır.

LIOP algoritmasının işlem basamakları;

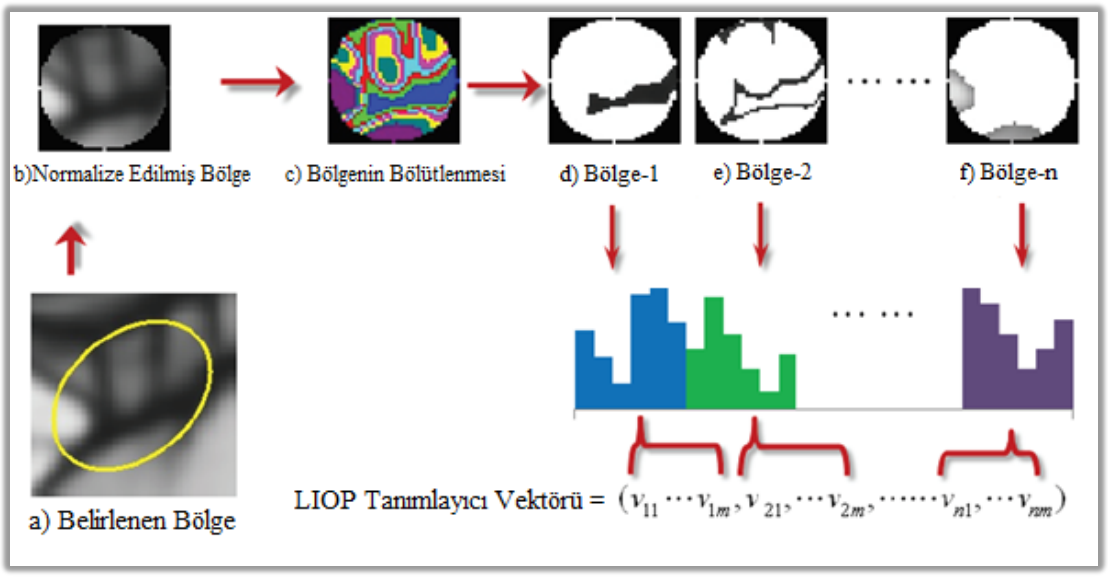
i. Algoritma gürültü ataklarına karşı hassas olduğu için bu dezavantajı ortadan kaldırmak adına öncelikle görüntünün tamamına Gauss filtresi uygulanarak görüntü yumuşatılır.

ii. İkinci adımda özellik vektörlerinin konumunu belirlemek ve komşu pikselleri tahmin etmek için bir bölge dedektörü oluşturulur. Görüntü üzerinde gezdirilen dedektör sayesinde tespit edilen bölgeler farklı boyut ve şekil özelliklerine sahip olurlar. Tespit

edilen bölgelerden eşit tanımlayıcı vektörleri oluşturmak için sabit yarıçap belirlenerek, her bölgenin sabit yarıçaplı bölgelere normalleştirilmesi sağlanır. Bu normalleştirmeden kaynaklanabilecek gürültü ve boşlukların giderilmesi için tekrar her bölgeye Gauss yumuşatma filtresi uygulanır. Bu işlemden sonra oluşturulan her bölge, yerel örüntü olarak adlandırılır. Yerel örüntü bölgeleri eşit şekilde piksel sıraları bozulmadan normalize edilmiş bölgeye indirgenir.

iii. LIOP tanımlayıcı vektörünün oluşturulması için histogram tabanlı yöntem, görüntü üzerinden oluşturulan yerel örüntü bölgelerini alt bloklara böler. Şekil 9. (c)'de görüldüğü gibi her bir farklı bloktan oluşan sıralı bölgeler farklı renklerle ifade edilir.

iv. Görüntünün alt bloklara ayrılmasından sonra, alt bloklar piksel parlaklık değerine göre koyudan (siyah pikseller), parlağa (beyaz pikseller) doğru sıralandırılırlar. Kendi içerisinde bölünen her bir alt blokta sırasıyla histogram hesaplanır ve tanımlayıcı vektöre kaydedilir. LIOP algoritması tüm komşu piksellerin parlaklık sırasını kullanarak tanımlatıcı vektörü oluşturur. Hem bölgelere ayırma hem de LIOP hesabı parlaklık ilişkilerine bağlı olduğu için, oluşturulan tanımlayıcı vektör döndürme, ölçekleme ve tek düze parlaklık değişikliği ataklarına karşı dayanıklıdır.



Şekil 9. LIOP Tanımlayıcı Vektör Oluşturulması [61]

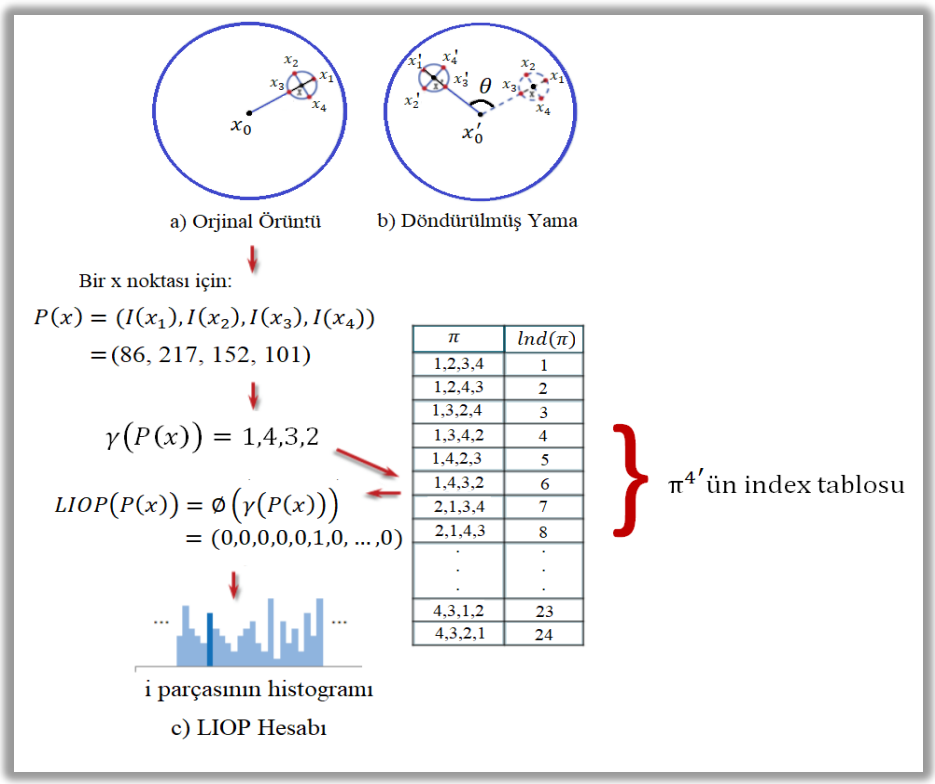
v. $\boldsymbol{P^N} = \{(p_1, p_2, \dots, p_N) : p_i \in R\}$ N boyutlu vektörler olsun ve $\Pi^N = (1,2,\dots,N)$, **P** vektörünün alabileceği indekslerinin olası tüm permütasyonları olsun. γ fonksiyonu ise $\boldsymbol{P^N} \rightarrow \Pi^N$ 'de tanımlı olsun. γ fonksiyonu N elemanlı **P**'yi azalmayan (monoton artan) şekilde sıralasın $(p_{i1} \leq p_{i2} \leq \cdots \leq p_{iN})$. Matematiksel olarak γ(**P**) = π olmaktadır. $\pi = (i_1, i_2, \dots, i_N)$ olmak üzere N=4 için π'nin kombinasyonları Şekil 10.'da verilmiştir.

Şekil 10.'da verilen φ; özellik haritalandırma fonksiyonu π'nin permütasyonları N! boyutlu bir $V_{N!}^{i}$ özellik vektörü oluşturmaktadır. Bu vektörün i elemanı hariç tüm elemanları 0 olup i elemanı 1'dir. φ 'nin matematiksel tanımı eşitlik (1.1)'de verilmiştir.

$$\varphi(\pi) = V_{N!}^{Ind(\pi)} \tag{1.1}$$

Eşitlik (1.1)'de verilen '$(Ind(\pi))$'; π permütasyon tablosundaki indeks vektörüdür ve Eşitlik (1.2)'de gösterilmiştir.

$$V_{N!}^{Ind(\pi)} = (0,\dots,0,\underset{Ind(\pi)}{1},0,\dots,0) \tag{1.2}$$



Şekil 10. LIOP Olasılık Dağılım Diyagramı

Belirtilen $P(x)$ vektörü yerel yama içindeki x noktasının N adet komşu parlaklık örneğini içeren N elemanlı vektördür. x noktası için LIOP hesabı Eşitlik (1.3)'te verilmiştir.

$$\begin{aligned} LIOP(x) &= \varphi(\gamma\,(\mathrm{P(x)})) \\ &= V_{N!}^{Ind(\gamma\,(\mathrm{P(x)})} \\ &= (0,\dots,0,\underset{(Ind(\gamma\,(\mathrm{P(x)}))}{1},0,\dots,0) \end{aligned} \tag{1.3}$$

Eşitlik (1.3)'te verilen $\mathrm{P(x)} = (I_{(x_1)}, I_{(x_2)}, \dots\, I_{(x_N)})$ ve $I_{(x_1)}$'de x noktasının $i.$ komşu örneğinin parlaklığını vermektedir. Toplamda $N!$ sayıda farklı LIOP olduğu için yerel yama $N!$ parçaya bölünür ve her biri bir LIOP ile temsil edilir.

x noktasının N adet komşu örneği x merkezli r piksel yarı çaplı bir çember üzerinde eşit olarak dağıtılır. Döndürme ataklarına karşı dayanıklı olması için ilk nokta radyal yönde yerleştirilir. Merkezi x olan yerel yamada, rotasyon merkezine en uzak noktadaki örnek seçilir. Sonra geri kalan $N-1$ adet örnek noktası çemberin etrafında saat yönünün tersi yönde sıralanır. Örneğin Şekil 10 (b)'de $N = 4$ için döndürmeye karşı dayanıklı örnekleme gösterilmiştir. Şekil 10'da x'in 4 komşu örnekleme noktası olan x_1, x_2, x_3, x_4 döndürüldükten sonra sırasıyla x_1', x_2', x_3', x_4' olarak konumları aynı kalmıştır.

Özellik vektörü, sırasıyla her sıra kutusundaki noktaların LIOP'larını toplayarak ve sonra bunları bir araya getirerek oluşturulur. LIOP özellik vektörü yapısı, Şekil 10'da gösterilmiştir. Matematiksel olarak, yerel yamanın LIOP tanımlayıcısı Eşitlik (1.4)'deki denklem yardımıyla hesaplanır.

$$\text{LIOP özellik vektörü} = (\,\mathrm{öv}_1, \mathrm{öv}_2, \dots, \mathrm{öv}_B)$$

$$\mathrm{öv}_i = \sum_{x \in \mathrm{kutu}_i} \mathrm{LIOP}\,(x) \tag{1.4}$$

B, sıra kutularının sayısı olmak üzere, özellik vektörünün boyutları $N!\,xB$ şeklinde olmaktadır. LIOP özellik vektörünün hem monoton parlaklık değişikliklerinde hem de

görüntü döndürmeye karşı dayanıklıdır. x yerel yamada bir nokta olmak üzere, x' bir monoton parlaklık değişiminden ve görüntü döndürmesinden sonra x noktasını belirtir. $P(x) = \big(I(x_1), I(x_2), \dots, I(x_N) \big)$ ve $P(x') = \big(I(x'_1), I(x'_2), \dots, I(x'_N) \big)$, N boyutlu vektörler olmak üzere, parlaklık sıralaması $I(x_1), I(x_2), \dots, I(x_N)$ yerine $I(x'_1), I(x'_2), \dots, I(x'_N)$ monoton olarak değiştiği için $P(x)$ ve $P(x')$ vektörleri P^N sıralamasında aynı konumlarında kalacaktır. Başka bir değişle, $\gamma(P(x)) = \gamma(P(x'))$'dir. Böylece *LIOP(x)=LIOP(x')* olur.

Benzer parlaklıkların sırası, Gauss gürültüsü nedeniyle birbirine benzemeyenlere göre daha çok değiştiğinden dolayı, daha farklı olan komşu örnek noktalara sahip olan noktaya ait LIOP daha durağandır ve daha büyük bir ağırlık verilmelidir. LIOP özellik vektörlerinin güvenilirliğini arttırmak için Eşitlik (1.5)'de verilen ağırlıklandırma fonksiyonu önerilmektedir.

$$w(x) = \sum_{i,j} sgn\big(\big|I(x_i) - I\big(x_j\big)\big| - T_{lp}\big) + 1 \tag{1.5}$$

Eşitlik (1.5)'de verilen $sgn()$ işaret fonksiyonu ve T_{lp} ise önceden ayarlanmış eşik değeridir. Bu ağırlıklandırma fonksiyonu, farklı örnek çiftlerinin sayısını sayarak komşu x noktası olan nokta noktaları arasındaki yoğunluk farklılıklarını ölçer. Böylece özellik vektörü Eşitlik (1.6)'daki gibi olmaktadır;

$$LIOP \text{ özellik vektörü} = (\text{ö}v_1, \text{ö}v_2, \dots, \text{ö}v_B)$$
$$\text{ö}v_i = \sum_{x \in kutu_i} w(x) LIOP\ (x) \tag{1.6}$$

1.3.2. Yama Eşleşmesi Algoritması (PatchMatch)

PatchMatch görüntü yamaları arasında yaklaşık en yakın komşu eşleşmelerini bulan hızlı bir rastlantısal algoritmadır [62]. PatchMatch algoritmasının süreci 3 aşamada incelenebilir. Bunlar; başlama, yayılma, rastgele aramadır.

i. Başlama**:**

Öncelikle offset alanı Eşitlik (1.7) 'deki gibi rastgele başlatılır.

$$\delta(s) = U(s) - s \tag{1.7}$$

$U(s)$, Ω görüntü desteği üzerinde düzgün dağılımlı, iki boyutlu rastgele bir değişkendir. Algoritmaya başlamadan önce $\delta(s) = 0$ durumu, çözümsüz ve sonuca etkisi olmadığı için atılır. Benzer şekilde, hedeften nispeten uzaktaki eşleşmeler arandığı için, belirli bir eşik değerinden daha küçük olan tüm ofsetleri atılır, daha sonraki tüm gelişmelere dolaylı olarak uygulanan bir koşul olan $\|\delta(s)\|_\infty < T_{D1}$ kullanılır. Çoğu rastlantısal başlangıç ofsetleri kullanışsızdır. Fakat içlerinden bazıları doğru sonuca büyük ihtimalle çok yakındır. PatchMatch'in ana fikri, tüm alanı yinelemeli olarak güncelleyerek sonuca yakın olan ofsetleri hızla yaymaktır.

ii. Yayılma:

Bu aşamada görüntü yukarıdan aşağıya ve soldan sağa taranır. Her piksel için mevcut ofset Eşitlik (1.8)'deki gibi güncellenir.

$$\delta(s) = \arg_{\phi \in \Delta^P(s)} \min D(f(s), f(s + \phi)) \tag{1.8}$$

Eşitlik (1.8)'de verilen yayılma parametresi $\Delta^P(s) = \{\delta(s), \delta(s^r), \delta(s^c)\}$ şeklindedir. Ayrıca tarama sırasına göre s^r ve s^c sırasıyla satır ve sütun boyunca s'den önceki piksellerdir. Uygulamada, algoritma nedensel komşularla ilişkili ofsetlerin eşleştirme kalitesini iyileştirip iyileştirmediğini kontrol eder. Bu nedenle, sabit bir kayma ile bir bölgenin belirli bir pikseli için iyi bir kayma mevcutsa, bu durum bütün bölgeyi aşağıdan ve sağdan doldurarak çok hızlı bir şekilde yayılacaktır. Karmaşık geometrilere sahip görüntülerde, tam yayılma biraz daha fazla yineleme gerektirebilir.

iii. Rastgele Arama:

Yukarıdaki yayılma prosedürü, çok fazla işlem gerektirir ve bu nedenle rastgele başlatmanın kalitesine göre işlem hızı olarak optimum değerden uzaktır. Bu nedenle, yerel minimumda takılı kalma riskini en aza indirmek için, Eşitlik (1.8) denklemini Eşitlik (1.9) olarak güncellenmesinden sonra, mevcut ofset alanının rastgele örneklemesine dayanarak rastgele bir arama aşaması da göz önünde bulundurulur. Bu duruma göre aday ofset fonksiyonu Eşitlik (1.9)'da verilmiştir.

$$\delta_i(s) = \delta(s) - R_i \tag{1.9}$$

Eşitlik (1.9) denkleminde R_i başlangıç pikseli hariç olmak üzere, 2^{i-1} yarıçapı bir kare ızgara üzerinde düzgün dağılımlı, iki boyutlu rasgele bir değişkendir. R_i, iki boyutlu (0,0) değeri hariç {-1, 0, 1}x{-1, 0, 1} değer aralığındadır. Rastgele arama denklemi Eşitlik (1.8)'e uygulanır ve Eşitlik (1.10)'daki eşleştirme fonksiyonu oluşturulur.

Yani uygulamada, bu yeni aday ofsetlerin çoğu $\delta(s)$'e yakındır, ancak küçük olasılıklarla büyük farklılıklar da meydana gelebilir. Böylece rastgele arama için ofset fonksiyonu Eşitlik (1.10)'deki gibi güncellenir.

$$\delta(s) = \arg_{\phi \in \Delta^R(s)} \min D(f(s), f(s+\phi)) \tag{1.10}$$

Bu fonksiyondaki arama parametresi $\Delta^R(s) = \{\delta(s), \delta_1(s), \ldots, \delta_L(s)\}$ şeklindedir. Örneğin 1024x1024 piksellik bir görüntü için $L \leq 10$ seçilsin. Prosedürün tipik olarak birkaç yinelemeden sonra birleştiği göz önüne alındığında, tüm hesaplama yükü, algoritma hızını tam olarak açıklayan tam arama için 10^6'nın aksine, piksel başına 10^2 özellik uzaklık hesaplama işlemine karşılık gelmektedir. Bunun yanında, PatchMatch, en yakın komşu alanın (NNF) çoğunlukla düzenli olduğu ve özellikle bir eşleşmenin arandığı ilgilenilen bölgelere göre düzenli olduğu şeklindeki hipoteze dayanır, aksi takdirde kritik yayılma aşaması temel olarak etkisiz olur [63].

Eşitlik (1.10)'da algoritma rastgele olarak eşleştirme işlemini başladığı için önerilen algoritmanın rastgele tüm görüntüyü taramasıyla, normal algoritmaların tüm görüntüyü taraması arasında hız farkı ortaya çıkmaktadır.

1.3.3. Rotasyondan Bağımsız Komşuluk Temelli İkili Örüntü (RINBP)

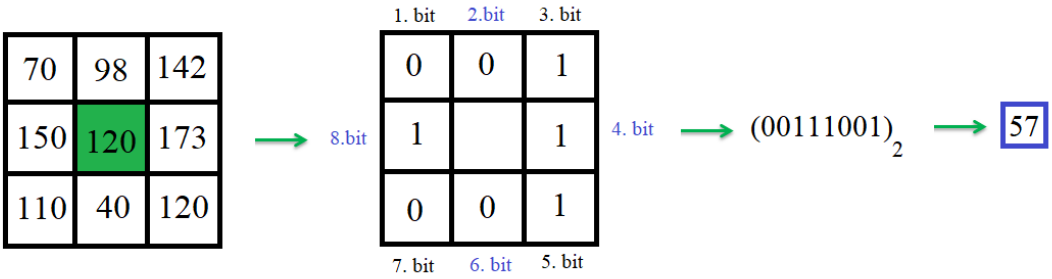
RINBP yöntemi, LBP denilen Yerel İkili Örüntü desen çıkarma operatöründen ilham alınmıştır [64]. Bu yüzden önce LBP gri seviyeli doku operatörünün nasıl çalıştığı anlatılacaktır.

Ojala ve arkadaşları tarafından önerilen çalışmada LBP, ilk kez ayrımsama gücü yüksek desen analizi olarak kullanılmıştır [65]. LBP operatörü, merkez pikselin 3x3'lük komşuluk

bölgesini içeren matriste, komşu pikseller ile karşılaştırma yöntemi ile oluşur. LBP yöntemi ile görüntüdeki her piksel değeri için bir adet LBP kodu üretilir. LBP kodu üretilirken uyulması gereken kural merkez pikseli komşu pikselden büyükse ya da eşitse komşu pikseli '1' değerini alır. Eğer merkez pikseli komşu pikselden küçükse komşu pikseli '0' değerini alır. İkili karşılaştırmadan sonra matrisin sol üst köşesini ilk basamak kabul edilerek, saat yönü sırasıyla LBP kodu oluşturulur. Bu şekilde bir merkez pikseli için üretilen komşu bölgesi LBP kodu, 8 bitten oluşur ve 0-255 değer aralığında yer alır. Oluşan LBP kodunun, decimal yani ondalık sistemdeki değeri, merkez pikseli çevreleyen bölgedeki yerel ikili örüntü bölgesini ifade eder. LBP kodunun hesaplanmasında kullanılan matematiksel denklem Eşitlik (1.11)'de verilmiştir. Denklem içerisindeki s(t) fonksiyonunun değer aralıkları Eşitlik (1.12)'de verilmiştir. Eşitlikte ifade edilen x değeri merkez pikselin konumunu vermektedir. x_i ise i indisli pikselin konumunu ifade etmektedir. $G()$ fonksiyonu pikselin yeğinlik değerini ifade eder ve hesaplama sonucu 0-255 arasında değer alır. Örnek LBP kodunun üretilmesi Şekil 11'de verilmiştir.

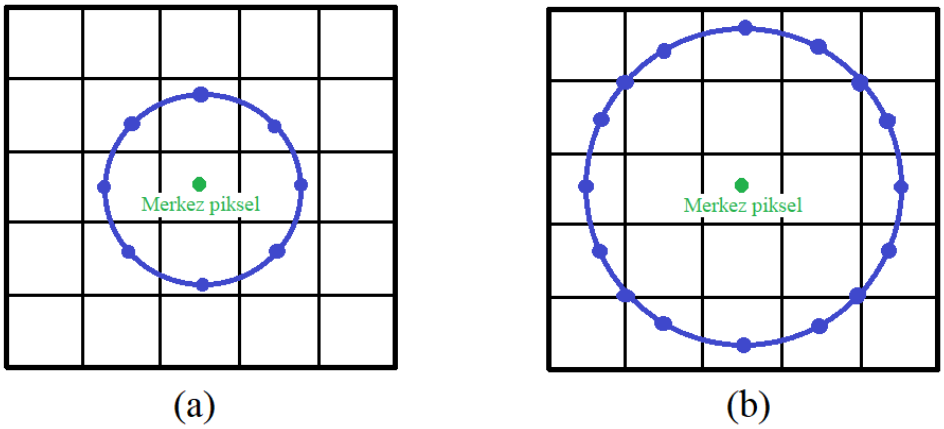
$$LBP(x) = \sum_{i=1}^{8} s(G(x_i) - G(x))\, 2^{i-1} \tag{1.11}$$

$$s(t) = \begin{cases} 1, & t \geq 0 \\ 0, & t < 0 \end{cases} \tag{1.12}$$



Şekil 11. Ondalık tabanda LBP kodu üretimi

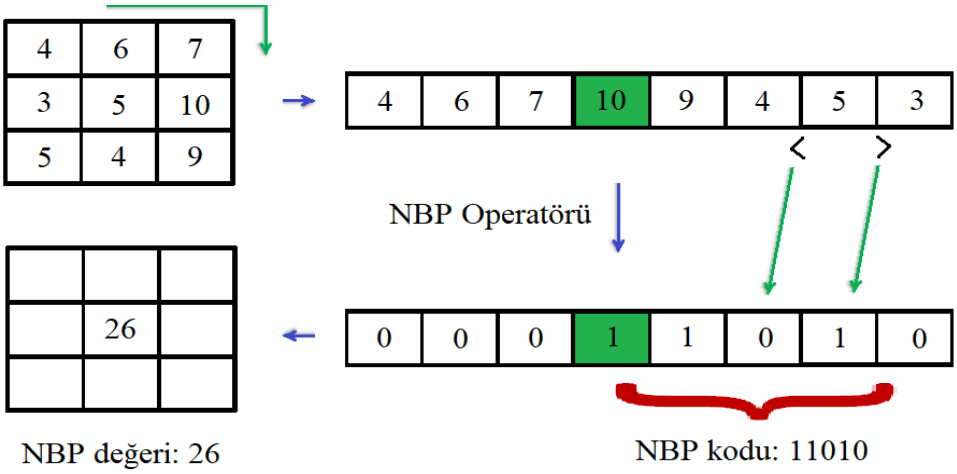
LBP'nin farklı gösterimleri olabilir. Örneğin 1 piksel uzaklık komşuluk için 8 bitlik gösterim Şekil 12.(a)'da gösterilmiştir. Şekil 12.(b)'de 2 piksel uzaklık 16 bitlik komşuluk gösterilmiştir.



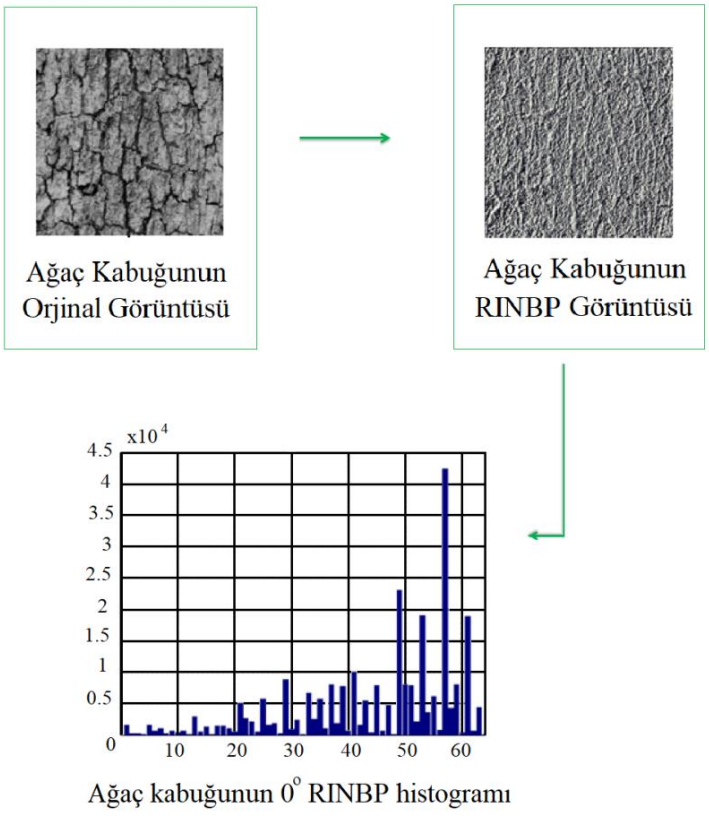
Şekil 12. LBP'nin farklı gösterimleri (a) 1'e 8'lik (b) 2'ye 16'lık

Görüntü üzerine her bir piksel için LBP prosedürü uygulandıktan sonra, 0-255 aralığında değişen piksel değerlerine sahip LBP görüntüsü elde edilir. Her LBP değeri farklı bir piksele karşılık gelir. Bir sonraki aşamada LBP görüntüsünün histogramı alınır. Böylece 256 farklı desenin, belirli bir dokuda ne kadar sıklıkta ortaya çıktığı belirlenir. 256 bitli histogramik dağılım dokunun yapısının tanımlanmasını sağlar.

LBP'den ilham alınarak geliştirilen NBP benzer yapıda çalışmaktadır. NBP yöntemi de komşuluk pikselleri 3x3'lük matris ile tarayarak işleme başlar. Ancak LBP yöntemindeki gibi merkez piksel ile ikili karşılaştırma yapmaz. Yani NBP yönteminde merkez piksel ile karşılaştırma yapılmaz. Karşılaştırma komşu piksellerin kendinden sonra gelen piksel ile karşılaştırılmasıyla gerçekleştirilir. Örneğin, merkez pikselin sol üst komşusunun değeri, merkez pikselin üst orta değeri ile karşılaştırılır. Örnek NBP kodunun üretilmesi Şekil 13'de verilmiştir. Sonuç olarak görüntüdeki piksel değeri 5 olan pikselin NBP'den sonraki karşılığı 26 olacaktır. Tüm piksellere NBP operatörü uygulanarak, NBP görüntüsü elde edilir. LBP yönteminde olduğu gibi, NBP görüntüsünde de histogram hesaplanır ve normalleştirilir. NBP histogramı Şekil 14'de gösterilmektedir ve özellik tanımlayıcı olarak kabul edilir.



Şekil 13. Ondalık tabanda NBP kodu üretimi

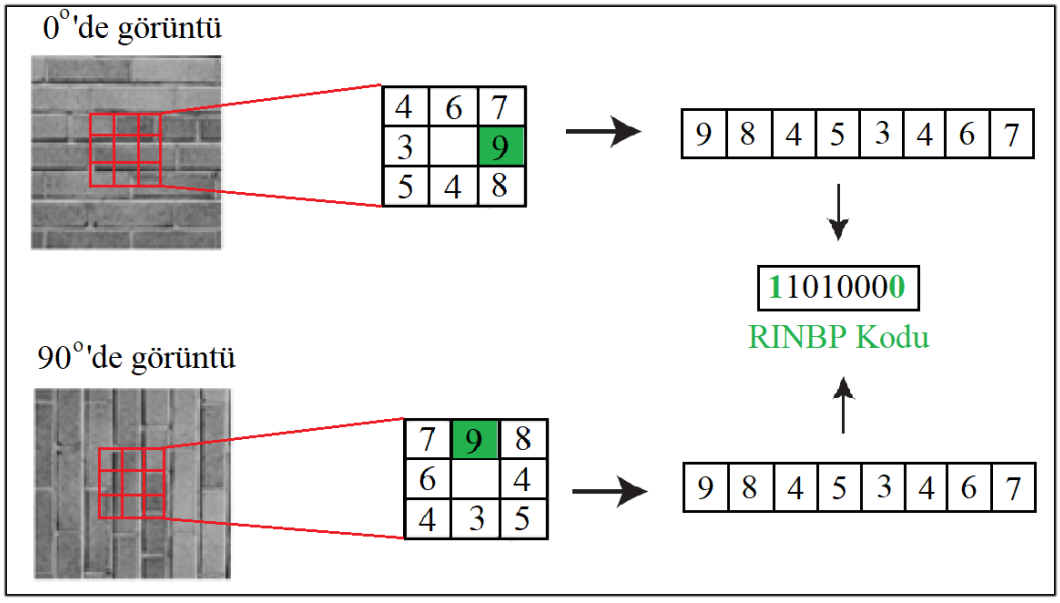


Şekil 14. Ağaç kabuğu görüntüsüne NBP uygulanması

Çıkarılan sonuçlardan da anlaşılacağı gibi, orijinal görüntüdeki küçük bir dönmenin LBP veya NBP ile oluşturulan kodda değişikliğe neden olur. Bu değişikliğin sebebi görüntü üzerinde seçilen merkez pikselin analizine her zaman 3x3'lük gezinti matrisinin sol üst köşesinden başlanmasıdır. Klasik LBP ve NBP yöntemlerinin zayıflığı budur. LBP'nin ve NBP yönteminin dezavantajının ortadan kaldırmak için döndürmeden bağımsız olan RINBP yöntemi önerilmiştir [64].

RINBP yöntemi ilk olarak, merkez pikselin her bir komşusu bir sonraki komşu tarafından denetlenir. Kodlama işlemine en büyük piksel değerine sahip komşudan başlanır. Bu sayede görüntü döndürülse de, desen de ya da dokuda döndürülür.

Kodlama işlemine en büyük komşu pikselden başlandığından, RINBP kodunun ilk bitinin her zaman '1' olacağı bilinmektedir. Aynı şekilde düşünüldüğünde en küçük piksel değeri en sonda kalacağından ve RINBP kodlamasında '0''a dönüşeceği bilmektedir. Şekil 15'de de görüldüğü gibi RINBP kodlamadan sonra ilk bit daima '1' son bit daima '0' olur. Bu bilindiği için önerilen yöntemin ilk ve son bitleri değerlendirmeye alınmaz ve atılır. Sonuç olarak değerli olan RINBP kodu 8 bitten 6 bite düşürülür. Böylece işlem maliyeti azaltılır ve rotasyondan bağımsızlık kazanılır. RINBP histogramının boyutu 64'e eşit olur.



Şekil 15. Ondalık tabanda RINBP kodu üretimi [64]

Şekil 15'de 3x3'lük matriste en büyük piksel değeri olan '9''dan başlanır ve saat yönünde dönülerek, karşılaştırma sıralaması elde edilir. Daha sonraki adımda her bit kendi komşu değeri ile karşılaştırılarak, komşu değerinden büyük veya eşit ise '1' değilse '0' değerini alarak RINBP kodu oluşturulur. RINBP kodunun boyutunu azaltmak için yeşil olan değerleri sileriz. Dolayısıyla elde edilen RINBP kodu, 40'a eşit olan 101000'dir.

Şekil 15'de görüldüğü gibi görüntünün 0^o ve 90^o'deki döndürülmesine rağmen doku bölgesi için elde edilen RINBP kodu aynıdır. Bu da RINBP'nin döndürmeden bağımsız çalıştığının kanıtıdır.

En son işlem olan dokulara ya da cisimlere karşılık gelen RINBP kodlarından, histogramlar çıkarılır. Böylece elde ettiğimiz değerler, özellik vektörlerimizi oluşturur.

1.3.4. Ölçekten Bağımsız Öznitelik Dönüşümü (Scale Invariant Feature Transform, SIFT)

Kopyala-yapıştır sahteciliği tespitinde etkili ve yaygın olarak kullanılan SIFT algoritması, görüntüden öznitelik elde etmek ya da görüntü üzerinde bölge eşleştirilmesi aynı zamanda da cisim takibi için de kullanılan algoritmadır [66]. SIFT algoritmasıyla oluşturulan her anahtar noktası yön, konum ve ölçek bilgisi içermektedir. Bu sayede güvenilir öznitelik elde etmek için kullanılan algoritma, bakış açısı, döndürme, ölçekleme, ışık değişimi ve ötelemeden bağımsız olarak çalışmaktadır.

Literatürde yapılan SIFT algoritmasının [66] çalışma adımları;

i. Ölçek uzayı içerisindeki uç noktaların tespiti: Anahtar noktası tespiti için öncelikle anahtar noktası olabilecek aday noktaların konumlarının ve ölçeklerinin belirlenmesi gerekir. Bunun için ölçek uzayında tanımlı olan istikrarlı noktaların konumları belirlenir. Algoritmanın ilk adımı olarak ölçek uzayı dediğimiz Gauss ölçek uzayının oluşturulması için görüntünün farklı σ değerleri ile Eşitlik (1.13) kullanılarak katlama işlemi gerçekleştirilir.

$$G_\sigma(x,y) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{x^2+y^2}{2\sigma^2}\right] \tag{1.13}$$

Eşitlik (1.13)'da verildiği gibi Gauss ölçek uzayının hesaplanması için sinyallerin farklı ölçeklerde değerlendirilmesi gerekir. Daha çok iki boyutlu görüntüler üzerinde

hesaplanan Gauss ölçek uzayı, Eşitlik (1.14)'de verildiği gibi farklı σ değerlerinin $G(x, y, \sigma)$ ile gösterilen Gauss filtreleri ile katlanmaları sonucu elde edilir.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{1.14}$$

Eşitlik (1.14)'de gösterilen $L(x, y, \sigma)$, Gauss ölçek uzayını ve $I(x, y)$ ise iki boyutlu görüntüyü ifade etmektedir. $I(x, y)$ ile temsil edilen iki boyutlu görüntüde, (x, y) piksel koordinatlarını ifade etmektedir.

Gauss ölçek uzayında anahtar noktaların belirlenmesi için, ölçek uzayı içerisinde farklı σ değerlerine sahip Gauss çekirdeği ile katlamaya girmiş görüntü birbirinden çıkarttırılarak Gauss Uzay Farkı (Difference of Gaussian, DoG) hesaplanır ve Eşitlik (1.15)'de gösterilmiştir.

σ_1 için;

$L1 = G_{\sigma_1}(x, y) * I(x, y)$

σ_2 için;

$L2 = G_{\sigma_2}(x, y) * I(x, y)$

$$L1 - L2 = DoG(x, y, \sigma) * I(x, y) \tag{1.15}$$

Eşitlik (1.15) birinci σ_1 ve ikinci σ_2 ölçekler arasındaki oran k kadardır. Yapılan çalışmada [66] k değeri 1'e yakınsanarak teoride yaklaşım hatasının sıfıra ulaşması sağlanmıştır. Çalışmada k değeri $\sqrt{2}$ alınarak işlemler yapılmıştır. Çalışmada ilk olarak $\sigma_1 = \sigma$ daha sonraki hesaplamalar için $k = \sqrt{2}$ olarak hesaplanarak Gauss çekirdeği ölçek uzayı standart sapma değeri hesaplanarak Eşitlik (1.16)'de verilmiştir.

$\sigma_1 = \sigma$

$\sigma_2 = k\sigma = \sqrt{2}\sigma$

$\sigma_3 = k^2\sigma = 2\sigma$

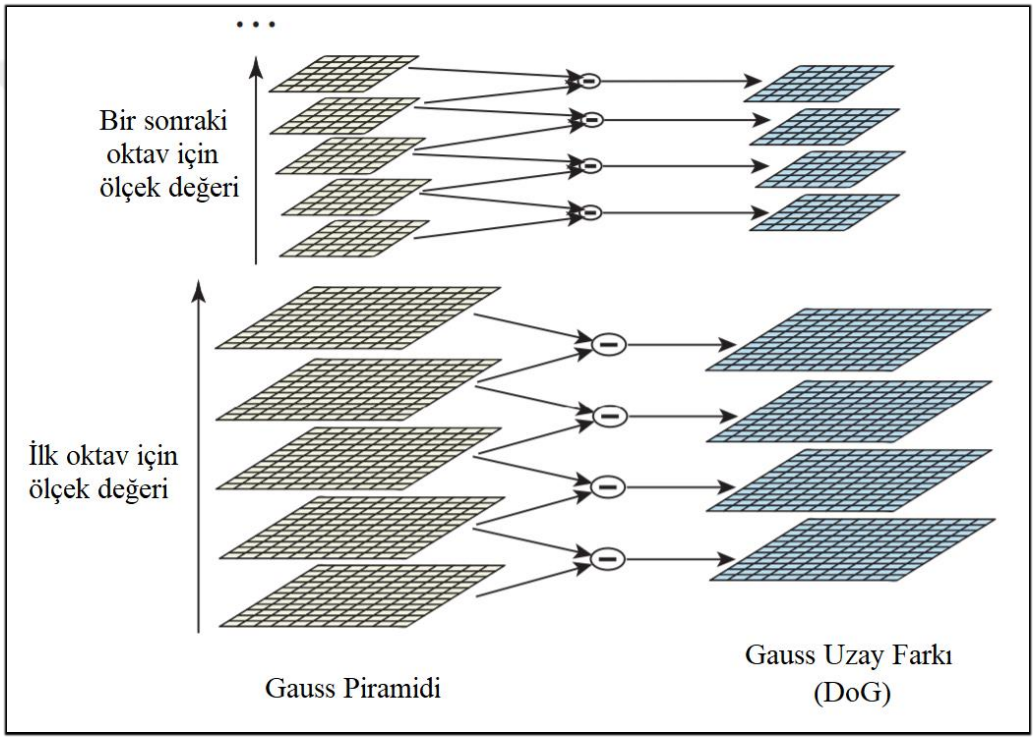
...

…

…

$$\sigma_n = k^{n-1}\sigma = (\sqrt{2})^{n-1}\sigma \tag{1.16}$$

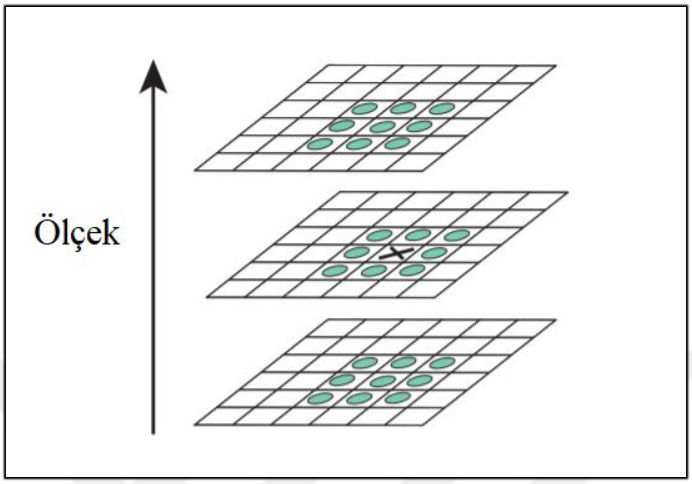
Ölçek uzayı, çarpım faktörü $k = 2^{1/s}$ olarak alınır. Daha sonra her biri $s+3$ adedinde yumuşatılmış görüntü içeren oktav adı verilen serilere ayrılır [66]. İlk seri oluşturulduktan sonra oluşturulan ikinci seri, ilk serinin σ_n kadar alt örneklenmiş ve boyutu yarı oranına indirgenmiş görüntü ile başlar. Bundan sonraki oluşturulacak her seri için bu işlem bir önceki seri kullanılarak oktav sayısı kadar tekrarlanır ve Şekil 16'da gösterilmiştir.



Şekil 16. İki ölçek arasındaki farkın hesaplanarak ölçek uzayın belirlenmesi [66]

Ölçek uzayı belirlendikten sonra görüntüden oluşturulan her bir oktav için Eşitlik (1.15) kullanılarak DoG hesabı yapılır. Uç noktaların belirlenmesi için her bir DoG görüntüsünün kendi ölçek değerlerinin her pikseli çevresinde alt-üst olmak üzere 8 piksel ve komşu ölçekler hizasındaki 9'ar pikselle karşılaştırılır. Toplam 26 piksel ile karşılaştırılma yapılmış olur. Şekil 17'de de gösterildiği gibi karşılaştırma esnasında şayet bir piksel o bölgenin yerel maksimumu veya yerel minimumu ise aday anahtar noktası

olarak belirlenir. Belirlenen oktavlar için görüntü yarı oranına indirilerek yerel maksimum veya yerel minimum olarak tespit edilen aday anahtar noktası koordinatları, içinde bulunduğu oktav indirgenme katsayısı ile çarpılarak kayıt altına alınır.



Şekil 17. Yerel maksimum ve minimumların bulunması [66]

ii. Anahtar noktaların belirlenmesi: Bu işlem adımında aday anahtar noktası olarak belirlenen noktaların kesin konum ve ölçek bilgisinin belirlenmesidir. Gauss uzay farkının gürültüye karşı hassas olması, düşük kontrastlı bölgelerin ve kenarlarda yer alan sıralanmış noktaların tespit edilerek elenmesine olanak sağlar.

Düşük kontrasta sahip aday anahtar noktalarının elenmesi için DoG uzayında $D(x, y, \sigma)$ ölçek uzayı fonksiyonunun ikinci türevinden Taylor serisi kullanılır ve Eşitlik (1.17)'de gösterilmektedir.

$$D(\mathbf{x}) = D + \frac{\partial D^T}{\partial \mathbf{x}}\mathbf{x} + \frac{1}{2}\mathbf{x}^T \frac{\partial^2 D}{\partial \mathbf{x}^2}\mathbf{x} \tag{1.17}$$

Uç noktaların konum bilgisini içeren $\hat{x}$, $D(\mathbf{x})$ eşitliğinin türevinin alınıp, sıfıra eşitlenmesiyle bulunur.

$$\hat{x} = -\frac{\partial^2 D^{-1}}{\partial x^2}\frac{\partial D}{\partial x} \tag{1.18}$$

Lowe yaptığı çalışmada eşik değerini 0.5 olarak belirlemiştir. Eğer hesaplanan değer herhangi bir ölçek uzayında 0.5'den büyük çıkarsa, uç noktasının başka bir örnek uzaya ait ya da yakın olduğu anlamına gelir. Bu durumda aday noktanın yeri eşik değeri kadar değiştirilir ve işlem tekrar gerçekleştirilir. İşlem sonucu 0.5'den küçük çıkan ilk noktada, anahtar noktasının gerçek konumu ve ölçek bilgisi elde edilir.

Düşük kontrastlı bölgelerde kararsız uç noktaların elenmesi için Eşitlik (1.19) kullanılır.

$$D(\hat{x}) = D + \frac{1}{2}\frac{\partial D^T}{\partial x} \tag{1.19}$$

Kenar bölgelerinde bulunan aday anahtar noktalarının bulunduğu koordinat ve ölçekteki DoG görüntüsünün, Hessian matrisi Eşitlik (1.20)'de gösterilmektedir. Bu matris, denklem sisteminin ikinci derece kısmi türevlerinden oluşan matristir. Hessian matrisi ile ikinci türev kullanılarak tepe ve çukur değerler hakkında bilgi edinilebilir.

$$D_{xx} = \frac{\partial^2 D}{\partial x^2}, \quad D_{yy} = \frac{\partial^2 D}{\partial y^2}, \quad D_{xy} = \frac{\partial^2 D}{\partial x \partial y}$$

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \tag{1.20}$$

H matrisinin öz değerleri hesaplanmaktadır. Değersel oranından çıkarım yapılacağı için yalnızca oransal olarak ilgilenmek yeterli olacaktır ve Eşitlik (1.21)'de gösterilmektedir.

α ; En büyük değerdeki öz değeri

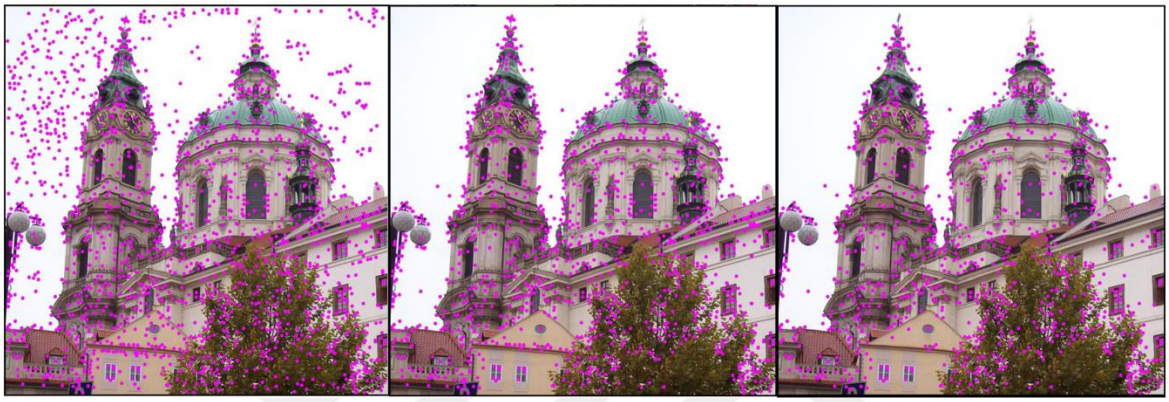
β ; En küçük değerdeki öz değeri

$$Tr(H) = D_{xx} + D_{yy} = \alpha + \beta, \qquad Det(H) = D_{xx}D_{yy} - (D_{xy})^2 \tag{1.21}$$

Eşitlik (1.21)'de hesaplama sonucunda determinantın negatif çıkması durumunda bükümün farklı işarete sahip olmasından dolayı aday noktası elenir.

$$r = \frac{\alpha}{\beta}, \quad \frac{Tr(H)^2}{Det(H)} = \frac{(\alpha+\beta)^2}{\alpha\beta} = \frac{(r\beta+\beta)^2}{r\beta^2} = \frac{(r+1)^2}{r} \tag{1.22}$$

Eşitlik (1.22)'de öz değerlerin eşit olması durumda $(r+1)^2/r$ en küçük değere ulaşır. Bu durumda belli bir eşik değeri altındaki oranını bakmak yeterli olacaktır ve yapılan çalışmada r eşik değeri 10 seçilmiştir. Çalışmada r eşik değerinin altında kalan aday anahtar noktaları elenmiştir. Yapılan işlemler sonucu anahtar noktalarının elenmesine örnek görüntü Şekil 18'te verilmektedir.



Şekil 18. Anahtar noktaların elenmesi [66]

iii. Yön atama işlemi: Anahtar noktası belirleme işleminden sonra döndürme ve ölçekleme ataklarına karşı dayanıklılık sağlamak için bu noktalara yön tayin edilir**.** Her anahtar noktasının, merkezinde kendisinin olduğu düşünülüp, komşu pikseller aracılığıyla gradyan yön ve büyüklük bilgileri hesaplanır. Görüntü içerisinde oluşturulan sahtecilik kısımlarında herhangi bir açı ile döndürme yapılacak olursa, gradyan yönelimleri her piksel bileşeni için eşit dönmeye sahip olacaktır. Bu sayede anahtar noktaları dönme ataklarına karşı bağımsızlık kazanır.

Belirlenen anahtar noktalarına ölçek bağımsızlığı kazandırmak için noktaların ölçek bilgileri kullanılarak elde edilen yumuşatılmış görüntü, anahtar noktalarının yönelimi hesaplamasında kullanılır.

σ ölçekli yumuşatılmış görüntü olan $L(x,y)$ görüntüsü, anahtar noktası etrafındaki her piksel için, gradyan büyüklüğü $m(x,y)$ Eşitlik (1.23) ve $\theta(x,y)$ yönelim açısı hesaplanır Eşitlik (1.24)'de gösterilir.

$$m(x,y) = \sqrt{\left(\left(L(x+1,y) - L(x-1,y)\right)^2 + (L(x,y+1) - L(x,y-1))^2\right)^2} \quad (1.23)$$

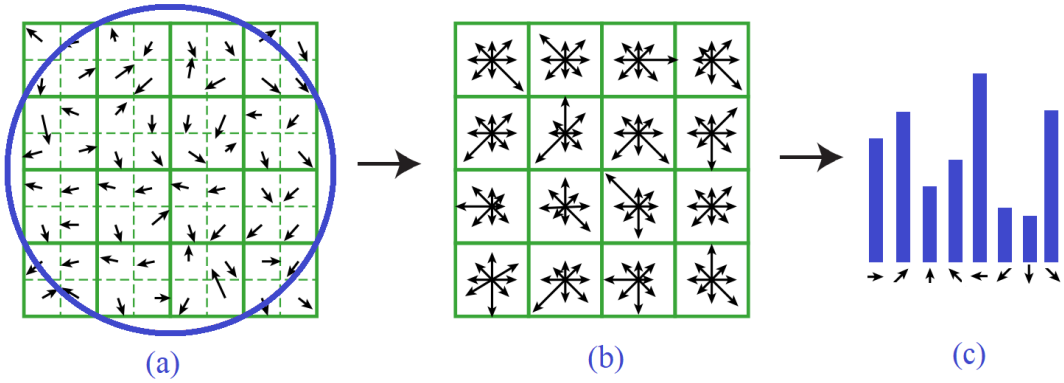
$$\theta(x,y) = \tan^{-1} \frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)} \quad (1.24)$$

Her biri diğerinden 10 derece açı farkına sahip olan 360^o'lik alanı kapsayan 36 adet bin'den oluşan, yön histogramı oluşturulur. Bu histogram, anahtar noktasının üzerinde olduğu σ ölçeğinini 1,5 katı kadar genişlikteki Gauss dairesel penceresindeki anahtar noktalarının gradyan büyüklüklerinin yani $m(x,y)$'nin eklenmesi ile elde edilir. Örneğin pencere içerisindeki pikselin yönelimine en yakın bin'in değerine o pikselin gradyan büyüklüğü eklenir. Bu işlem pencere içerisindeki tüm pikseller için uygulanır.

İşlemler sonucunda elde edilen histogram grafiğinde birden fazla tepe noktası çıkabilir. En yüksek tepe noktasına sahip yönelim açısı baskın değeri vermektedir. Bu değerin %80'inden büyük olan diğer tepe noktalarına sahip yönelimler kullanılarak aynı noktada fakat farklı yönelime sahip anahtar noktalar oluşturulur. Anahtar noktalarının sadece %15'inde gözlemlenebilecek olan bu durum yönelim kararsızlığına sebep olacakmış gibi gözükse de, anahtar noktalarının eşleşmesi için ideal bir yapı oluşturulur. Tepe tepe noktalarının yön değerlerinin daha hassas olarak hesaplanması için tepe noktasına en yakın histogram değerlerinin yön açıları interpolasyon yöntemi ile yeniden hesaplanır. İnterpolasyon sonucu daha doğru bir yön açısı elde edilir.

iv. Anahtar noktası öznitelik tanımlayıcılarının belirlenmesi: Anahtar noktalarının birbirinden ayırmak ve piksellerdeki ışık değişimlerine karşı duyarlılığı ortadan kaldırmak için öznitelik tanımlayıcıları belirlenir. Anahtar noktalarının etrafında 16x16'lık bloklar oluşturulur ve 4x4'lük bloklara bölünür. Bölme işlemi bloklar arasında 45^o olacak şekilde ve sekiz adet yön bilgisi içerecek şekilde olur. İşlem sonucunda toplam 16 adet blok elde edilmiş olur. Her bir okun yönü histogramın yönelim bilgisini, büyüklüğü ise gradyan büyüklüğünün bilgisini vermektedir.

Anahtar noktalarının Gauss pencere ağırlığının, kendi bileşenleriyle kıyaslanarak merkeze olan uzaklık ağırlığının oranına göre örnek histogram alanı etkisi hesaplanır. Şekil 19'da gösterildiği gibi 8 yön bin'inden oluşan 4x4'lük histogram dizisiyle 4x4x8=128 elemanlı öznitelik vektörleri oluşturulur.



Şekil 19. (a) Görüntü gradyanı (b) Anahtar noktası tanımlayıcısı (c) Yerel örüntü histogramı

1.3.5. RANSAC (Random Sample Consensus)

Fischler ve Bolles [67] tarafından önerilen Random Sample Consensus (RANSAC) algoritması, giriş verilerinde fazladan aykırı değerleri elemek için tasarlanmış genel bir parametre tahmin yaklaşımıdır. Bilgisayarla görme topluluğunun istatistik literatüründe benimsemiş olduğu M-tahmin edicileri ve en küçük medyan kareler gibi yaygın olarak kullanılan sağlam tahmin tekniklerinden farklı olarak, RANSAC bilgisayarla görme topluluğu tarafından geliştirilmiştir.

RANSAC, temel model parametrelerini tahmin etmek için gereken minimum sayıdaki gözlem (veri) noktaları kullanarak aday çözümler üreten bir yeniden örnekleme tekniğidir. Fischler ve Bolles [67] 'in belirttiği gibi, bir ilk çözüm elde etmek ve daha sonra aykırı değerleri yok etmek için mümkün olduğunca fazla veri kullanan geleneksel örnekleme tekniklerinden farklı olarak, RANSAC mümkün olan en küçük veri setini kullanır ve bu seti tutarlı (doğru örneklerle) bir şekilde büyüterek ilerler.

Temel algoritmanın ana başlıkları;

1. Model parametrelerini belirlemek için gereken minimum nokta sayısını rastgele seçilir.
2. Modelin parametreleri çözülür.
3. Tüm örnek kümesinden kaç tane örneğin önceden tanımlanmış bir tolerans “ε” ile uyduğunu belirlenir.

4. Eğer aykırı olmayan örnek sayısının setteki toplam sayı noktalarının üzerindeki oranı önceden tanımlanmış bir eşiği τ aşıyorsa, tüm belirlenmiş aykırı olmayan örnek kullanarak model parametrelerini yeniden hesaplanır ve sonlandırılır.
5. Aksi takdirde, 1 ile 4 arasındaki adımları tekrarlanır (en fazla N kez).

Yinelemelerin sayısı, N, rastgele örneklem kümelerinden en az birinin bir aykırı örnek içermediği p (genellikle 0.99'a ayarlanır) olasılığının sağlanması için yeterince yüksek seçilir. "u" alınan örneğin aykırı olmaması olasılığı olsun ve v=1-u ise aykırı olma olasılığı olmak üzere, m ile gösterilen minimum nokta sayısının N kere yinelemesi gerekir, bu durumda p olasılığı Eşitlik (1.25)'de verilmiştir.

$$1 - p = (1 - u^m)^N \tag{1.25}$$

Eşitlik (1.25)'teki denklemi tekrar düzenlenerek N iterasyon sayısı Eşitlik (1.26)'daki gibi bulunur.

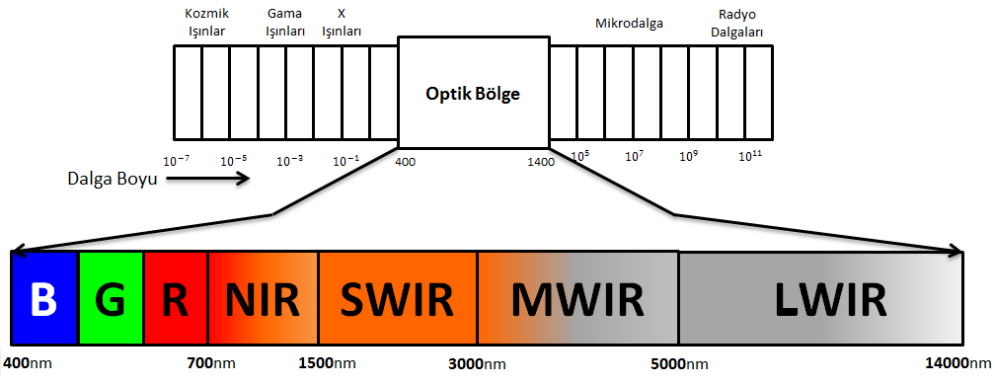
$$N = \frac{\log(1-p)}{\log(1-(1-v)^m)} \tag{1.26}$$

1.3.6. Hiperspektral Görüntüleme

Uzaktan algılama hiçbir fiziksel temas kurmadan, algılanmak istenilen cisimle ilgili veri toplanmasına denir ve kullanılan enerji kaynağına göre ikiye ayrılır. İlki pasif algılama olan uzaktan algılama türünde; algılayıcılar güneş gibi doğal kaynaklardan gönderilen ışınlar ile nesnelerden yayılan ya da yansıyan enerjiyi algılanır. Tez çalışmasında üzerinde durulan ileri multispektral algılayıcılar pasif uzaktan algılama türüne örnektir. İkinci uzaktan algılama türü olan aktif algılamada ise yapay enerji kaynağının çevreye yaydığı enerjinin nesnelerden yansımasını algılar. Aktif uzaktan algılama sistemlerine radar sistemleri örnek verilebilir. Nesnelerin üzerinden yansıyan ya da yayılan ışığın dalga boyu farklı olduğu için biz nesneleri birbirinden ayırt edebiliriz.

Geleneksel görüntüleme sistemleri insan gözünün algılayabileceği dalga boyu aralığında görüntüleme yaparken, hiperspektral görüntüleme insan gözünün

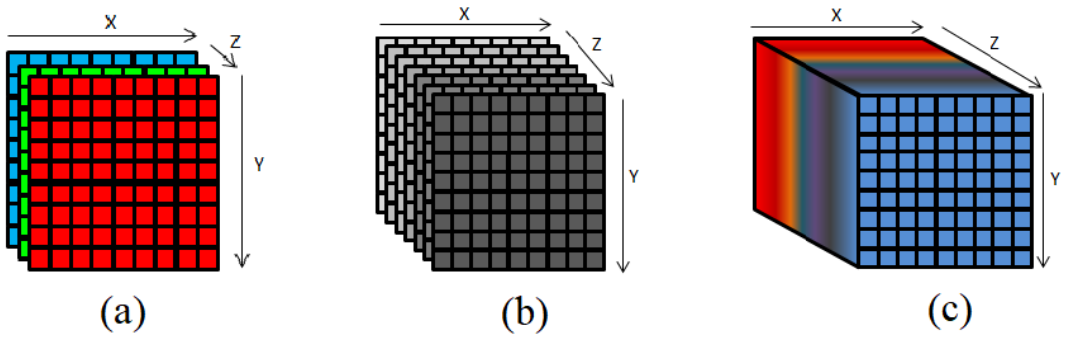
algılayamayacağı dalga boylarını içerir. Hiperspektral görüntüleme sistemleri Şekil 20'de görüldüğü gibi 400nm-14000nm dalga boyu aralığındaki optik bölge denilen alan üzerinde görüntüleme yapmaktadır.



Şekil 20. Hiperspektral görüntü dalga boyu

Şekil 20'de görülen 'B' mavi, 'G' yeşil, 'R' kırmızı dediğimiz RGB bantlarını temsil eder. 400nm-700nm aralığı görülür ışık bölgesi olarak adlandırılır. 700nm-1500nm aralığını, kızıl ötesi denilen NIR (Near Infrared) bölge oluşturur. 1500nm-3000nm aralığını orta dalga kızıl ötesi denilen MWIR (Mid Wave Infrared) bölge oluşturur. 500nm-14000nm aralığını ise uzun dalga kızıl ötesi denilen LWIR (Long Wave Infrared) bölgesi oluşturur.

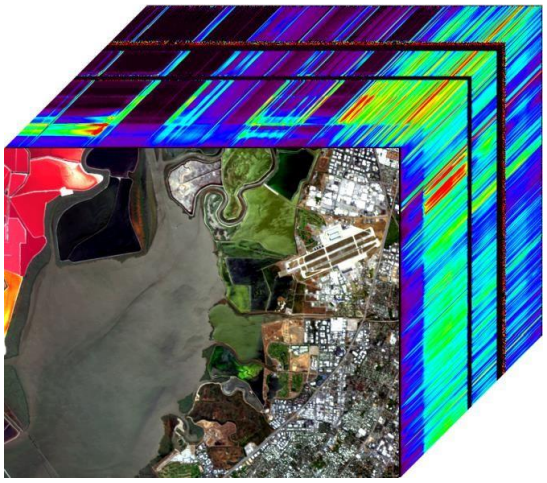
Hiperspektral görüntüler, diğer sayısal görüntüler gibi üç katmanlı RGB boyutunda) olmayıp, görünür dalga boyunun yanında kızıl ötesi ve mor ötesi dalga boylarında görüntü üzerine ekleyerek görüntü üzerinde yeni katmanlar oluşturur. Bu katmanlar sayesinde uydudan görüntülenmek istenilen alan ile ilgili daha fazla veriye sahip oluruz. Şekil 21'de sayısal görüntünün farklı boyutlardaki gösterimine örnek verilmiştir. Şekil 21(a)'da RGB düzleminde ifade edilen görüntü, (b)'de multispektral görüntü ifadesi ve (c)'de aynı şekilde hiperspektral düzlemde görüntü ifadesi verilmiştir.



Şekil 21. (a) RGB (b) Multispektral (c) Hiperspektral

Multispektral görüntüleme tekniğinin geliştirilmesiyle elde edilen hiperspektral görüntüleme insansız hava aracı, uçak, uydu gibi farklı hava araçları üzerinde bulunan özel kameralar tarafından çekilen görüntülerdir [68]. İlk kez 1970 yılından itibaren kullanılmaya başlanan hiperspektral görüntülerin, yaygın kullanımı 2000'li yıllarda başlamaktadır. Hiperspektral sensörler elektromanyetik yansımayı ölçen ve farklı dalga boylarının yansımalarını hiperspektral görüntü olarak veren cihazlardır. Hiperspaktral görüntüler, sensörler art arda gelen bantlardan elde edilen yansımaların yüksek hızla örneklenmesiyle oluşturulur.

Hiperspektral görüntüler, ilk iki boyutu uzamsal diğer boyutu spektral olmak üzere üç boyut içermektedir. Üç boyut içerdiği için hiperspektral küp olarak adlandırılan hiperspektral görüntülere örnek Şekil 22'de gösterilmiştir.



Şekil 22. Hiperspektral küp

Hiperspektral görüntülerin kullanım alanları oldukça geniştir;

*Askeri alanda hedef tespiti vb. amaçlı

*Tarım alanlarında ürün tespiti, tarla sınırları belirlenmesi vb. amaçlı

*Madencilikte yer altı kaynak tespiti ve miktarlarının belirlenmesi amaçlı

*Tıp alanında hastalık ve erken tanı tespiti amaçlı

*Gıda sektöründe besin kalitesi ve ürün çeşitlendirilmesi amaçlı kullanılmaktadırlar.

Literatürde bu kullanım alanlarının dışında sahtecilik alanında da hiperspektral görüntüler kullanılmaktadır. Hiperspektral görüntüler üzerinde teknolojinin ilerlemesiyle sahte evrakların tespiti veya evrak üzerindeki sahteciliğin tespit edilme başarı oranı artmıştır. Literatürde ilk olarak bu teknolojiyi kullanan firma Foster&Freeman olup, Türkiye'de de yerli olarak Forensic XP-4010D ve MSS-2D cihazları TUBİTAK-UEKAE tarafından geliştirilmiştir [69]. Bu çalışmalar gibi hiperspektral kamera teknolojisi kullanılarak akademik anlamda, savunma sanayisi alanında kamuflaj tespiti yöntemi önerilmiştir [70].

Bu tez kapsamında önerilen yöntemde ise ilk defa kopya-yapıştır sahteciliği alanında uydudan elde edilen hiperspektral görüntüler üzerinde sahtecilik tespitinin gerçekleştirilebileceği gösterilecektir. Gerçekleştirilen yöntemine ilişkin açıklama bölüm 2.3.'de anlatılmıştır.

2. YAPILAN ÇALIŞMALAR VE ÖNERİLEN YÖNTEM

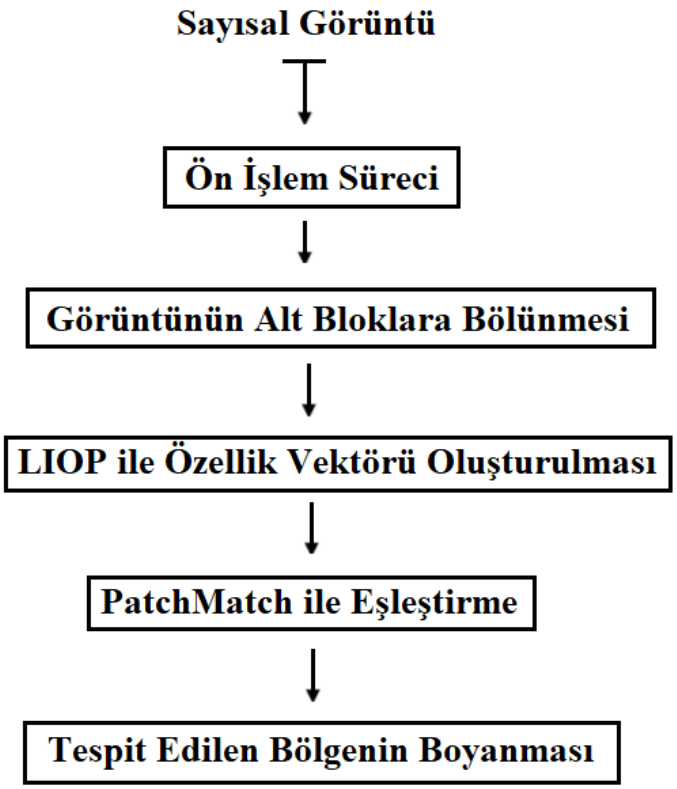
Yüksek lisans dönemi sürecinde; literatürde yer alan kopyala-yapıştır sahteciliği tespiti metotları incelenmiştir. Var olan yöntemlerin eksiklikleri giderilmek için daha etkin ve özgün iki yöntem önerilmiştir. Bunlara ek olarak literatürde kopyala-yapıştır sahteciliği alanında veri seti olarak daha önce hiç kullanılmamış ve teknolojik hayatta önemli bir yere sahip olan hiperspektral uydu görüntüleri üzerinde kopyala-yapıştır sahteciliği tespiti üzerine çalışılmıştır.

2.1. Kopyala-Yapıştır Sahteciliği Tespitinde LIOP ve PatchMatch Tabanlı Yaklaşım

İlk yapılan çalışmada kopyala-yapıştır sahteciliğini tespit etmek için literatürde daha önce özellik çıkarımı için kullanılan LIOP algoritması ve eşleşme kısmında hızlı, etkin, doğru sonuç oranı yüksek olan PatchMatch algoritması birleştirilerek yeni bir yöntem önerilmiştir. Blok tabanlı çalışan, LIOP algoritmasının döndürme ve ölçekleme ataklarına karşı dayanıklılığı kullanılırken, PatchMatch algoritmasının hızlı ve etkinliğinin yanı sıra pürüzsüz (smooth) bölgelerdeki eşleştirme oranının yüksekliğinden yararlanılmıştır.

Önerilen yöntem literatürde daha önce var olan benzer çalışmalar ile karşılaştırılıp, yöntemin ataklara karşı dayanıklılığı test edilmiştir. Sonuçlar kısmında yapılan çalışmanın Gauss gürültü, rotasyon, ölçekleme ve JPEG sıkıştırma atakları uygulandıktan sonra bile yüksek doğruluk içeren görüntü sahteciliği tespiti sonuçları rapor edilmiştir.

Yapılan çalışmaya ilişkin akış diyagramı Şekil 23'de verilmiştir.



Şekil 23. LIOP+PatchMatch tabanlı çalışmanın akış diyagramı

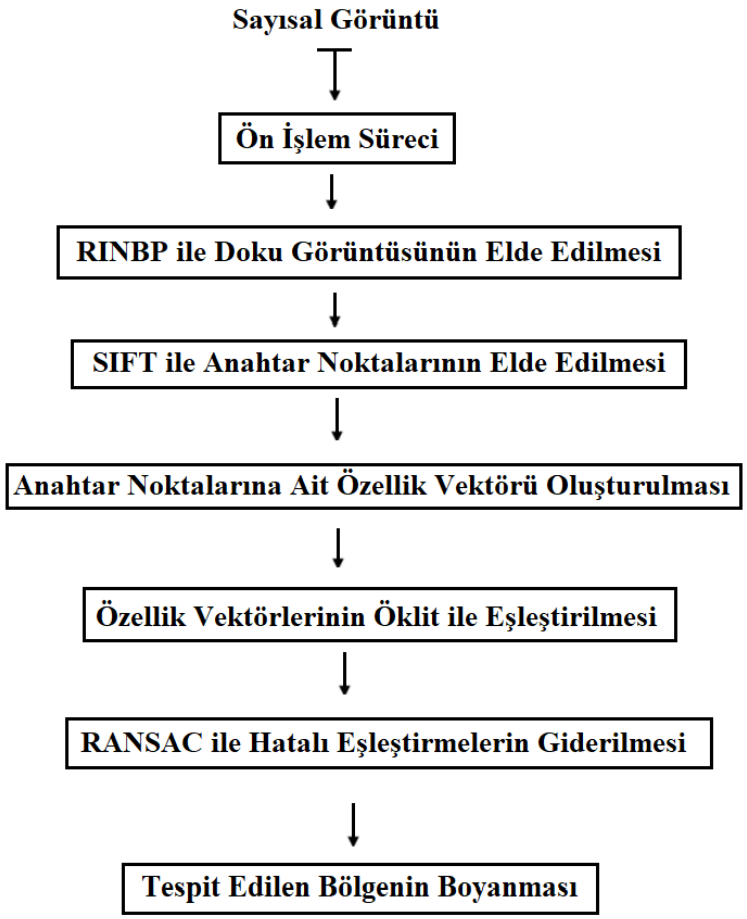
Çalışmanın ilk adımında kopyala-yapıştır sahteciliği tespit edilmek istenen renkli sayısal görüntü, gri seviyeli görüntüye dönüştürülür. Özellik vektörü oluşturabilmek için gri seviyeli görüntü birbiri ile örtüşen 12x12'lik alt bloklara bölünür. Oluşturulan her bir alt bloğa LIOP özellik çıkarma algoritması uygulanır. Böylece 12x12'lik bloklardan eşleştirme işlemine gönderilmek üzere 1x12 boyutta özellik vektörleri oluşturulur. Döndürme ve ölçeklemeden bağımsız olan özellik vektörleri eşleştirme için PatchMatch algoritmasına gönderilir. PatchMatch yönteminde, görüntüden oluşturduğumuz bloklar yama olarak kabul edilir ve birbirine yaklaşık en yakın komşuluğa sahip olan yamalar eşleştirilir. Kullanılan algoritmada başlangıç değeri rastgele seçildiği için işlem maliyeti azalmakta ve eşleştirme hız kazanmaktadır. Eşleştirme sonucunda tespit edilen bölgeler boyanarak kopyala yapıştır sahteciliği tespit edilmiştir. Çalışmanın test sonuçları, bulgular kısmında detaylıca verilecektir.

Önerilen yöntemin genel olarak algoritma basamakları şöyledir;

1. MxN boyutlarındaki sayısal görüntü gri seviyeye dönüştürülmesi için parlaklık ağırlık değerleri Gri seviye $=$ 0.2989 x Kırmızı $+$ 0.5870 x Yeşil $+$ 0.1140 x Mavi şeklinde dönüşüm gerçekleştirilir.
2. Gri seviyedeki görüntü $0 < i \leq M - L$ ve $0 < j \leq N - L$ olmak üzere Blok konumu $= (i: i + L, j: j + L)$ şeklinde tüm görüntüyü LxL boyutunda bloklara bölmektedir.
3. Döngü içinde elde edilen LxL boyutundaki blokların her birine ayrı ayrı Eşitlik (1.3)'teki LIOP özellik vektörü çıkarma işlemi uygulanır.
4. LxL bloklardan LIOP özellik çıkarma yöntemi sonucunda 1xL boyutunda motonon parlaklık değişimine, döndürme ve ölçekleme saldırılarına karşı dayanıklı özellik vektörleri elde edilir.
5. Özellik vektörlerinin temsil ettiği blok konumlarına yerleştirilerek $(\mathrm{M} - \mathrm{L})\mathrm{x}(\mathrm{N} - \mathrm{L})\mathrm{xL}$ boyutlarında 3 boyutlu görüntünün özellik matrisi elde edilir.
6. Özellik vektörleri Eşitlik (1.10)'da verilen PatchMatch algoritması sayesinde tam arama yerine blok başına yaklaşık 10000 kat daha hızlı olan rastgele arama ile eşleşme işlemine tabi tutulur. Böylece minimum uzaklıklı özellik vektörleri aranır.
7. Rastgele aramadan kaynaklanan özellikle lokal minimum uzaklıklar gibi hataları azaltmak için Yoğun Doğrusal Uydurma (Dense Linear Fitting, DLF) algoritması kullanılır.
8. DLF algoritmasında r yarıçaplı dairesel pencere şeklinde Median filtre uygulanmaktadır.
9. r yarıçapındaki komşuluklarla uyma hatası olan ε^2 hesaplanır.
10. ε^2 parametresine T_ε^2 eşik değeri atanır.
11. T_{DS} uzaklık eşik değerinden daha az piksel mesafede bulunan ve eşleşen bölgeler silinir.
12. Az bilgi içeren T_s piksel kare alandan daha küçük olan ve eşleşen bölgeler de kaldırılır.
13. Bu yöntemle hatalı eşleşmelerin çoğu elenmiş olur.
14. Elenmeyen eşleşmelerde yamaların konumlarında eşleşmeyi temsil eden boyama işlemi gerçekleştirilir.

2.2. RINBP ve SIFT Tabanlı Kopyala-Yapıştır Sahteciliği Tespiti

İkinci gerçekleştirilen çalışmada kopyala-yapıştır sahteciliğini tespit etmek için literatürde daha önce denenmemiş bir yöntem olan RINBP doku tespiti algoritması kullanmıştır. Daha sonra elde edilen doku bilgisi üzerinden SIFT yöntemi ile anahtar noktaları çıkartılmıştır. Anahtar noktalarına ait özellik vektörlerinin eşleştirilmesinde ise Öklid yöntemi kullanılmıştır. Yapılan ikinci çalışmaya ilişkin akış diyagramı Şekil 24 ’de verilmiştir.



Şekil 24. RINBP+SIFT tabanlı çalışmanın akış diyagramı

Hamouchene ve arkadaşlarının [64] doku çıkarmak için önerdiği çalışma, literatürde ilk kez sahtecilik tespiti için gerçekleştirdiğimiz çalışmada kullanılmıştır. RINBP algoritmasında açıklandığı gibi 3x3’lük matris tüm matris üzerinde gezdirilerek, RINBP

kodlu doku görüntüsü elde edilmiştir. Köşelerde kalan piksellerin boş komşularının tamamlanması için zero padding (sıfır ile tamamlama) yöntemi kullanılmıştır. RINBP doku görüntüsü elde dilerek, sahtecilik tespitinde gerçekleştirilen döndürme ataklarına karşı dayanıklılık elde edilmiştir.

Çalışmanın daha sonraki adımında RINBP algoritmasından elde edilen doku görüntüsü üzerinden SIFT algoritması ile anahtar noktaları çıkartılmıştır. Gerçekleştirilen çalışmanın son kısmında tespit edilen anahtar noktalarından özellik vektörleri oluşturulmuştur. Özellik vektörlerinin benzerliklerinin ölçülmesi için Öklid mesafe ölçme algoritması kullanılmıştır. Benzerlik ölçümünde uzaklık mesafesi eşik değeri olarak 0.5 kullanılmıştır. Eşik değerini aşmayan özellik vektörleri sahtecilik gerçekleştirilmiştir diyerek işaretlenmiştir. İşaretlenen özellik vektörleri iteratif olarak RANSAC algoritması ile yanlış kararları azaltma işlemine tabi tutulmuştur. Bunun için eşleşen özellik vektörlerinden rastgele örnek seçimi yapılmıştır. Örneklerin büyük ihtimalle doğru olduğu yani birbirine yakın olması gerektiği kabul edilir. Buna göre bir ε tolerans parametresinden daha uzak olma durumu incelenir. ε parametresi görüntüye ve özellik vektörü sayısına göre değişmektedir. Uzak olan özellik vektörleri elimine edilir ve kalan örnek kümesinden yine rastgele örnekleme yapılır. Bu sayede yanlış eşleşmeler büyük ölçüde giderilir. Bu iterasyon N kere tekrarlanır. N parametresinin hesabı Eşitlik (1.26)'da verilmiştir. N iterasyon sonunda eşleşen özellik vektörü kümesi birbiri ile eşleşecek şekilde görselleştirilmiştir. Yani eşleşen özellik vektörleri arası boyanarak kopyalanıp-yapıştırılan bölgenin konumu gösterilmiştir.

Önerilen yöntemin genel olarak algoritma basamakları şöyledir;

---

1. MxN boyutlarındaki sayısal görüntü gri seviyeye dönüştürülmesi için parlaklık ağırlık değerleri $\text{Gri seviye} = 0.2989 \text{ x Kırmızı} + 0.5870 \text{ x Yeşil} + 0.1140 \text{ x Mavi}$ şeklinde dönüşüm gerçekleştirilir.
2. Gri seviyedeki görüntü $0 < i \leq M - L$ ve $0 < j \leq N - L$ olmak üzere Blok konumu $= (i: i + L, j: j + L)$ şeklinde tüm görüntüyü LxL boyutunda bloklara bölmektedir.
3. Kenar bölgedeki piksellerinin etrafında bulunan LxL görüntü parçalarını kullanmak için görüntünün etrafına $(L - 1)/2$ piksel boyutunda sıfır yerleştirme (zero padding) yapılmıştır.

---

4. Görüntüde bulunan her LxL boyutundaki bloğun RINBP algoritmasına göre parlaklık seviyelerine bağlı olarak özellik vektörü çıkarılmıştır.
5. Özellik vektörü en yüksek parlaklık seviyesinden başlayıp saat yönünde bir sonraki parlaklık seviyesinin yüksek ya da düşük olmasını sorgulayarak yüksek ise 1 düşükse 0 değeri ile ikili $1x(L^2 - 3)$ özellik vektörü elde edilmektedir.
6. Özellik vektörü görüntü bloğunun içinde saat yönünde dönmesi ile oluşturulduğu için döndürme ataklarına karşı özellikle dayanıklılığı mevcuttur. Bunun yanında göreceli parlaklık seviyeleri ile oluşturulduğu için tüm piksellerin parlaklıklarının aynı anda artması ya da azalması sıralamayı değiştirmeyeceğinden monoton parlaklık değişimine karşı da dayanıklıdır.
7. Bir sonraki adımda 6. aşamada elde edilen ikili tabandaki vektörler onluk tabana dönüştürülerek yeni görüntü matrisi elde edilir. Bu matrise Bölüm 1.3.4.'te açıklandığı gibi SIFT algoritması ile anahtar noktası tabanlı özellik vektörleri çıkartılır. Çıkartılan özellik vektörleri $LxLx2L = 2L^3$ elemanlı olmaktadır.
8. Çıkarılan özellik vektörleri Leksikografik sıralama ile sıralandıktan sonra Öklid uzaklıkları $d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ olarak hesaplanmıştır.
9. Öklid mesafesi Td eşik değerinden daha yakın olan özellik vektörleri eşleştirilmiştir.
10. Eşleşme sonucunda RANSAC algoritması kullanılarak Eşitlik (1.26)'da verilen N iterasyon sonucunda hatalı eşleşmeler azaltılmıştır.
11. Eşleşme sonucunu görselleştirmek için eşleşen anahtar tabanlı özellik vektörleri mavi ile boyanarak eşleştirilmiştir.

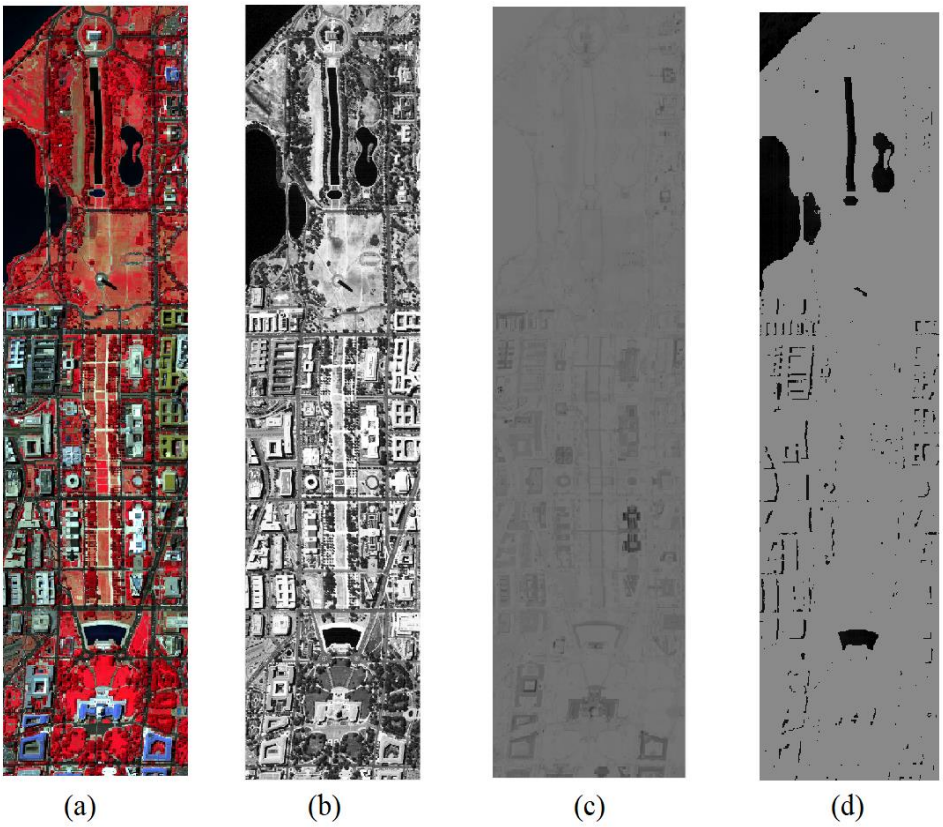
2.3. SIFT Tabanlı Yöntem ile Hiperspektral Görüntüler Üzerinde Kopyala-Yapıştır Sahteciliği Tespiti

Önerilen yöntemde sahtecilik yapılma oranı yüksek olan uydu görüntüleri üzerinde çalışılmıştır. Hiperspektral uydu görüntüleri ile gizlenmek istenen herhangi bir tesis, uçak üssü gibi savunma amaçlı kurulan veya gizli tutulmak istenen bölgeler görüntü içerisindeki herhangi bir alan tespit edilerek kopyala-yapıştır sahteciliği yöntemi uygulanarak kapatılabilir. Başka bir açıdan bakılırsa farklı dalga boyları yaydıkları için hiperspektral görüntüler ile kolayca tespit edilebilen yer altı kaynakları (maden, petrol, doğal gaz)

kopyala yapıştır sahteciliği ile kolayca gizlenebilmektedir. Ayrıca hiperspektral görüntüler askeri alanlarda hedef ve kimyasal/radyoaktif saldırı tespiti, gıda sektöründe besin güvenliği, tıp alanında hastalık tespiti, tarım alanında ürün kalitesinin belirlenmesi amaçlı kullanılmaktadır. Hiperspektral görüntülerin bu denli çok ve doğruluğunun önem teşkil ettiği alanlarda kullanılması sebebiyle doğru verileri içermesi ve üzerinde oynanmamış olması önem arz etmektedir.

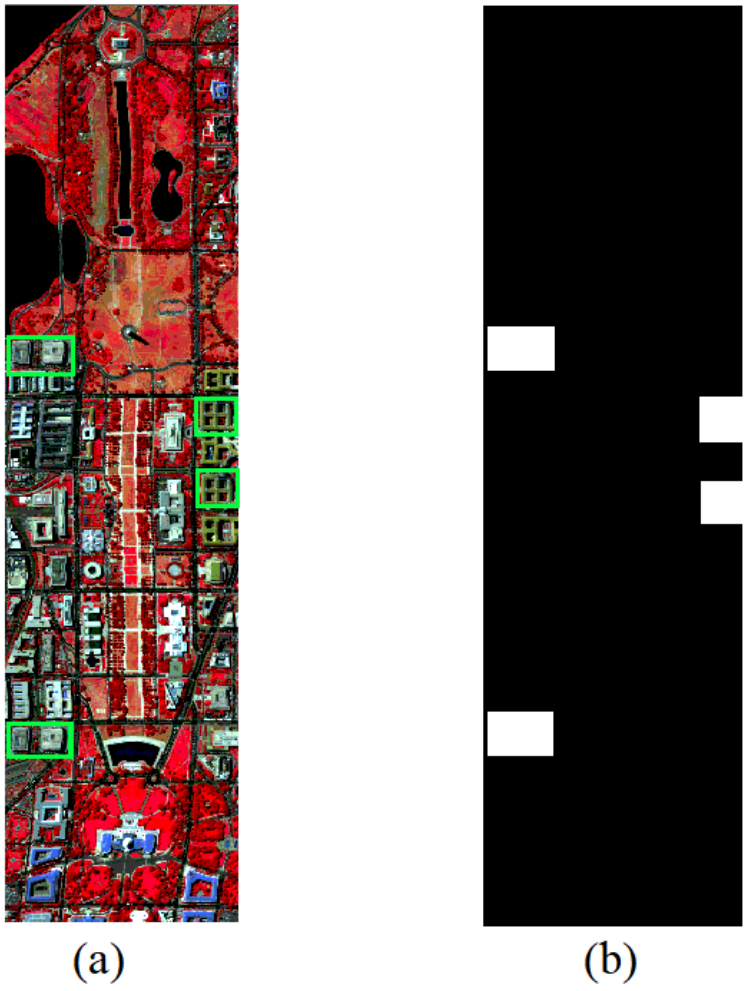
MultiSpecW64 adlı program ile açılan hiperspektral görüntülerin, sadece tek katmanı gözlemlenmektedir. Görüntülerin işlenir hale getirilmesi ve katmanların gözlemlenebilmesi için MatLab programına uygun hale getirilir. İlk işlem basamağında test görüntümüz olan Washington D.C. görüntüsü "1280x307x191" boyutunda ve ".mat" uzantılı olup üzerinde 8 bitlik işlem yapılabilir hale getirilir.

Şekil 25'te hiperspektral görüntünün katmanlarını ve içerdikleri veri bilgilerine ait görsel yer almaktadır.



Şekil 25. (a) 10. katman görüntüsü (b) 90.katman görüntüsü (c) 110.katman görüntüsü (d) 130.katman görüntüsü

İkinci işlem basamağında MatLab programında ".mat" uzantılı DC görüntüsü üzerinde 'for' döngüsü ile 191 katmanın her birine kopyala-yapıştır sahteciliği uygulanmıştır. Sahte görüntü üzerinde yapılan değişiklik çerçeve ile gösterilip belirgin hale getirilip Şekil 26(a)'da verilmiştir. MatLab programında oluşturulan maske görüntüsü ise Şekil 26(b)'de verilmiştir.



Şekil 26. (a) Sahte görüntü (b) Görüntünün sahtecilik maskesi

3. BULGULAR

Tez çalışmasında bu başlık içerisinde gerçekleştirilen çalışmaların deneysel bulguları ve test sonuçları yer almaktadır. Ayrıca performans analiz için kullanın değerlendirme yöntemi olan F ölçütü açıklanacaktır. Yapılan iki çalışmada da F ölçütü ile sonuç değerlendirilmesi gerçekleştirilmiştir.

Bunlara ek olarak bu bölünde test görüntüsü olarak kullanılan üzerinde kopyala-yapıştır sahteciliği uygulanan ve çeşitli ataklar içeren GRIP veri seti ve Hiperspektral veri setleri anlatılacaktır.

3.1. Performans Ölçütü Yöntemi

Yapılan çalışmaların ne kadar doğru sonuç verdiği ve literatürdeki diğer çalışmalara göre başarı ölçütünün nasıl değerlendirildiği bu kısımda verilecektir.

Performans analizi için F ölçütü metriği kullanılmıştır. Bunun sebebi karşılaştırılma yapılan diğer çalışmalarında F ölçütünü kullanması ve literatürde etkin bir geçerliliğe sahip olmasıdır. F ölçütü, Eşitlik (3.1)' de gösterildiği gibi hesaplanmaktadır ve 0-1 aralığında değer almaktadır.

$$\text{F ölçütü} = \frac{2*\text{DP}}{2*\text{DP}+\text{YN}+\text{YP}} \tag{3.1}$$

Eşitlik (3.1)'deki Doğru Pozitif (DP) parametresi; sahtecilik yapılan görüntülerin sahte olarak etiketlendiği görüntü sayısına karşılık gelmektedir. Yanlış Negatif (YN) parametresi; sahte görüntülerin, gerçek görüntüymüş gibi etiketlendiği görüntü sayısına karşılık gelmektedir. Yanlış Pozitif (YP); sahte görüntülerin gerçek görüntü olarak etiketlendiği görüntü sayısına karşılık gelir. Doğru Negatif (DN); gerçek görüntünün gerçek olarak etiketlendiği görüntü sayısına karşılık gelmektedir.

3.2. GRIP Veri Seti

Önerilen yöntemler, Tablo 1.'de de görüldüğü gibi herkese açık çevrim içi erişimli GRIP veri seti üzerinde test edilmiştir [71].

Tablo 1. Literatürde var olan veri setleri

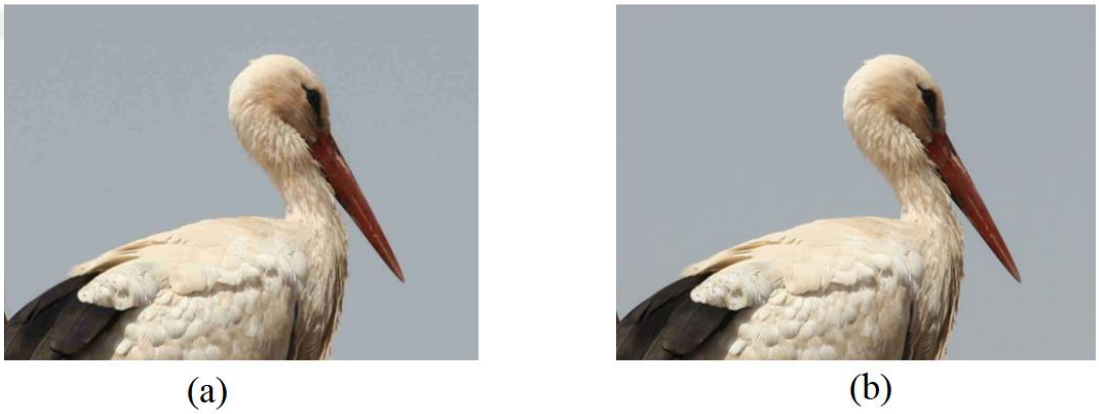
Veri Seti İsmi	Görüntü Boyutu	Orijinal Görüntü Adedi	Atak Tipleri
MICC-F220	722 x 48 800 x 60	220	Çevirme, döndürme, ölçeklendirme ve bunların kombinasyonu
MICC-F600	800 x 533 3888 x 259	600	Çevirme, döndürme, ölçeklendirme ve bunların kombinasyonu
MICC-F2000	2048 x 1536	2000	Çevirme, rotasyon, ölçeklendirme ve bunların kombinasyonu
CoMoFoD	512 x 512 3000 x 200	260	Döndürme, ölçeklendirme, gürültü ve bunların kombinasyonu, JPEG sıkıştırma
GRIP	1024 x 768	3360	Döndürme, ölçekleme, gürültü ekleme ve JPEG sıkıştırtma

GRIP veri setinin kullanılmasının sebebi bütün test edilmek istenilen atakların, görüntülerini içermesidir. Bu veri seti 80 adet gerçek yani kurcalanmamış görüntü içermektedir. Şekil 27'de örneği görüldüğü gibi gerçek görüntü üzerine, yine aynı görüntüden alınmış ve atak derecelerine göre sınıflandırılmış kopyalanıp-yapıştırılan bölgeler eklenmiştir. Şekil 27'de (b)'de gördüğümüz görüntü içerisinden alınmış ve ölçekleme atağı 103 oranında ayarlanmış kurcalanmış bölge görülmektedir.

(a) (b) (c)

Şekil 27. GRIP görüntüsü (a) gerçek görüntü (b) kopyalanan bölge (c) sahte görüntü

GRIP veri seti, insan gözünün dikkatli bakınca anlayabileceği ve sahtecilik yapılan bölgenin tespitini zorlaştırmak için yapılmış ataklar bulunmaktadır. Bunun için yapılmış gürültü atağı örneği Şekil 28'de verilmiştir. Şekil 28 (a)'da insan gözüyle zor fark edilebilecek kalite faktörü 20 olan, JPEG sıkıştırma atağının örnek görüntüsü yer almaktadır. Şekil 28 (b)'de kopyalanıp yapıştırılmadan önce 3x3'lük 0.5 standart sapmaya sahip bir pencere gezdirilerek gürültü üzerine bulanıklaştırma yapılarak yapıştırılan sahte görüntü gösterilmiştir.



Şekil 28. GRIP veri setinde (a) JPEG ataklı (b) Gürültü ataklı örnek sahte görüntüler

GRIP veri seti içerisinde;

* Gauss Gürültüsü) atağı uygulanmış toplam 400 adet sahte görüntü mevcuttur. Bu görüntülerin içerisinde standart sapması 2, 4, 6, 8 ve 10 filtresi uygulanan eşit sayıda görüntü mevcuttur.
* JPEG atağı uygulanmış toplam 720 adet sahte görüntü bulunmaktadır. Bu görüntülerin içerisinde kalite faktörü 20, 30, 40, 50, 60, 70, 80, 90 ve 100 olacak şekilde eşit görüntü bulunmaktadır.
* Ölçekleme atağına maruz kalmış toplam 1120 adet sahte görüntü bulunmaktadır. Bu görüntülerin içerisinde ise eşit miktarda %50, %80, %91, %93, %95, %97, %99, %101, %103, %105, %107, %109, %120 ve %200 oranlarında ölçekleme atağına maruz kalmış görüntü bulunmaktadır.

* Döndürme atağına maruz kalmış toplam 1040 adet sahte görüntü mevcuttur. Bu görüntülerin içerisinde eşit sayıda yer alan 2^o, 4^o, 6^o, 8^o, 10^o, 20^o, 30^o, 45^o, 60^o, 75^o, 90^o, 105^o ve 180^o döndürme atağı uygulanmış görüntü mevcuttur.

80 adet orijinal yani gerçek görüntü ve ataklara maruz kalmış 3280 sahte görüntü ile GRIP veri setinde toplam 3360 görüntü mevcuttur.

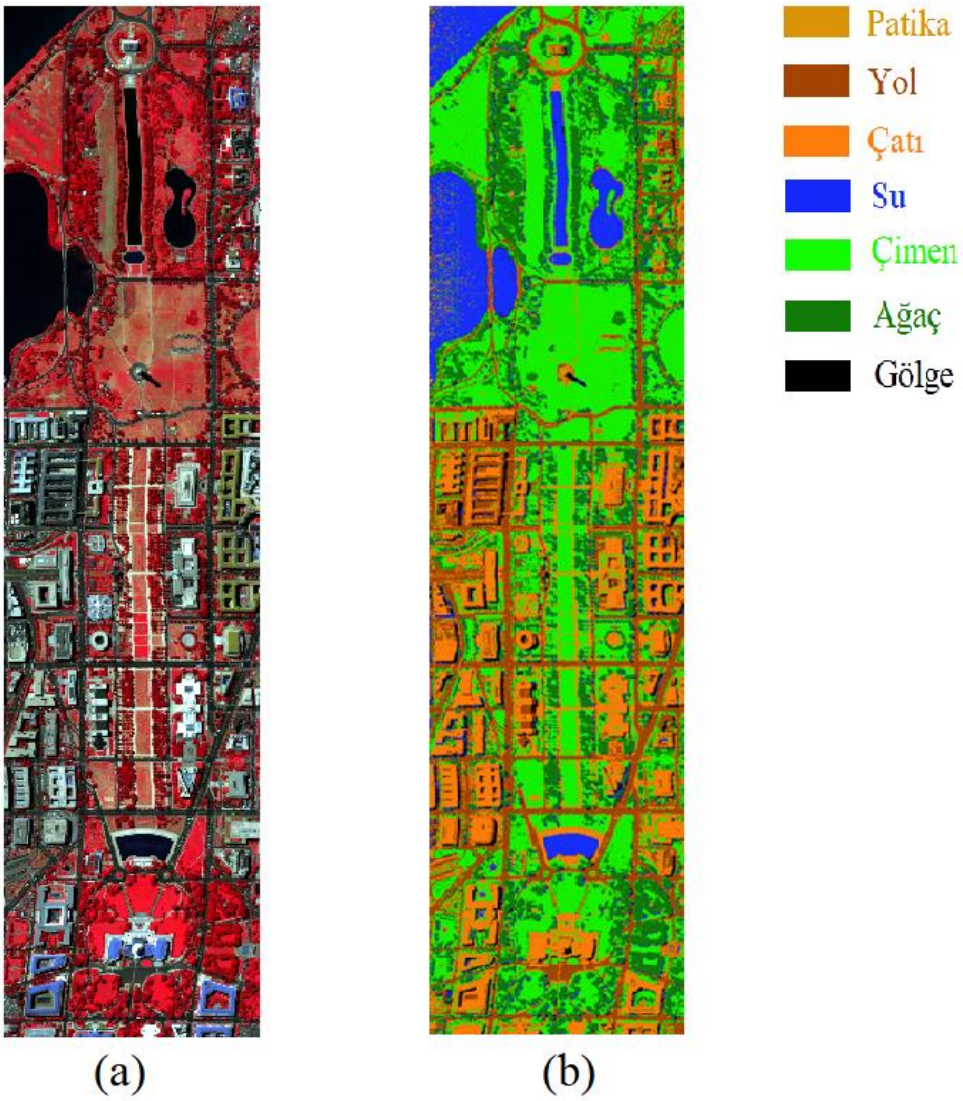
3.3. Hiperspektral Veri Setleri

Bilimsel araştırma amaçlı olarak farklı ülkelere ait farklı uydular üzerindeki hiperspektral kameralar tarafından çekilerek oluşturulan ve ücretsiz olarak sunulan veri setleri Tablo 2'de gösterilmiştir.

Tablo 2. Hiperspektral Veri Setleri

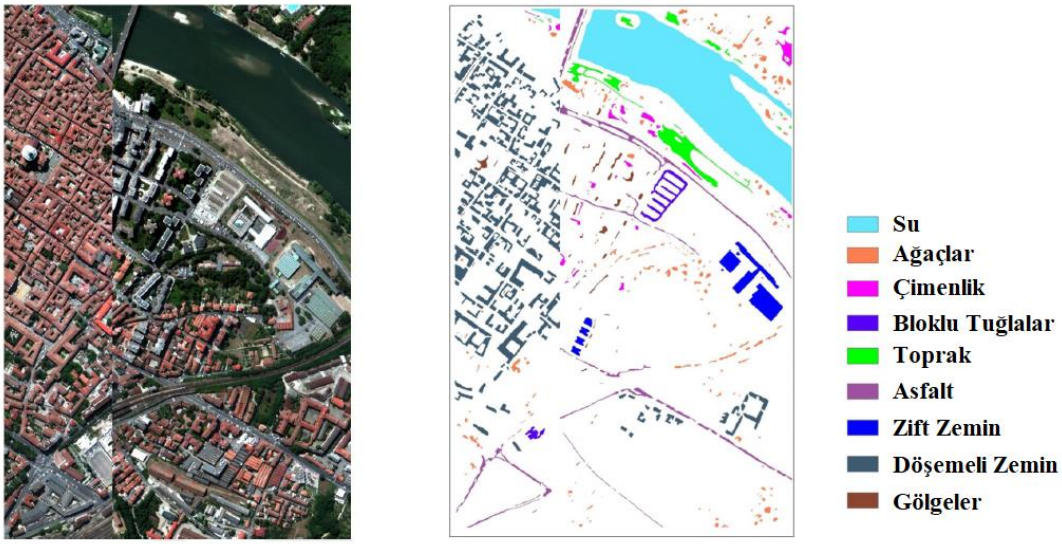
Sensör İsmi	Veri Seti	Bant Adeti	Sınıf Sayısı
AVIRIS	*Indian Pines *Kennedy Space Center *Salina	200 176 204	16 13 16
EO-1	*Botswana	145	14
ROSIS	*Pavia Center *University of Pavia	102 103	9 9
HYDICE	* Washington DC	210	7

Gerçekleştirilen çalışmada Washington District of Columbia üzerinden uydu ile HYDICE (Hyperspectral Digital Imagery Collection Experiment) sistemiyle çekilmiş veri seti kullanılmaktadır [72]. Veri Seti 1995 yılında Ağustos ayında oluşturulmuştur. Görüntü, 0.4-2.4 µm dalga boyu aralığındadır. 210 banttan oluşan veri setinin her bandı 1280x307 piksel içerir. Toplam bant sayısından su soğurma bantları ve gürültülü bantlar çıkartılmıştır. 191 bandı kullanılan görüntü 7 sınıf içermektedir. Bu 7 sınıfı yol, su, çimen, ağaç, çatı, gölge ve patika oluşturmaktadır. Washington D.C. veri seti görüntüsü Şekil 29'da gösterilmektedir.



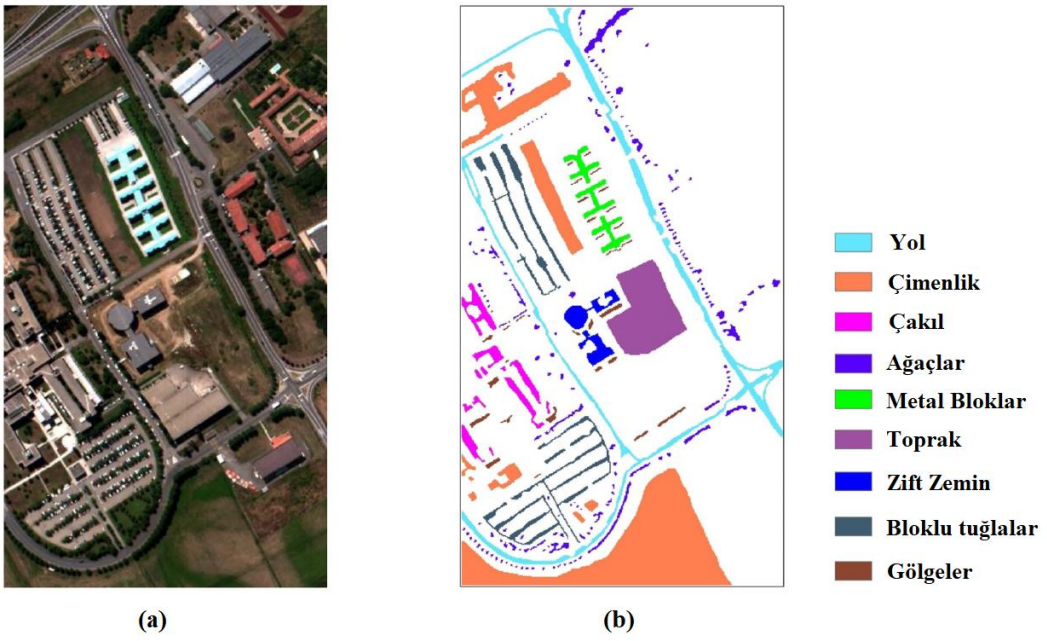
Şekil 29. Hiperspektral Washington D.C.(a) kanal görüntüsü (b) sınıf görüntüsü [72]

Pavia veri setindeki [73] ilk görüntü, İtalya'nın kuzeyindeki Pavia Kent merkezi üzerinden çekilmiştir. Şekil 30'da gösterilen hiperspektral görüntü 102 spektral bant ve 9 sınıf bilgisi içerir.



Şekil 30. Hiperspektral Pavia Center (a) kanal görüntüsü (b) sınıf görüntüsü [73]

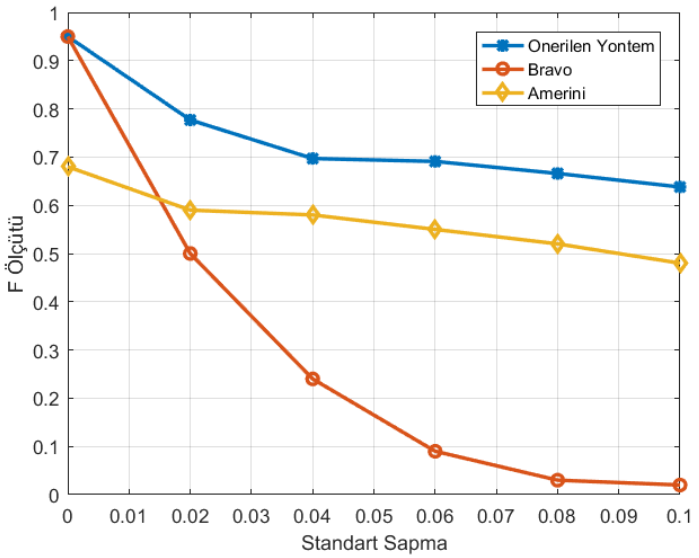
Pavia veri setindeki [73] ikinci görüntü Pavia Üniversitesi üzerinde çekilmiş olup, 103 spektral bant ve 9 sınıf verisi içerir. Şekil 31'de Pavia Üniversitesi'nin hiperspektral görüntüsü yer almaktadır.



Şekil 31. University of Pavia (a) kanal görüntüsü (b) sınıf görüntüsü [73]

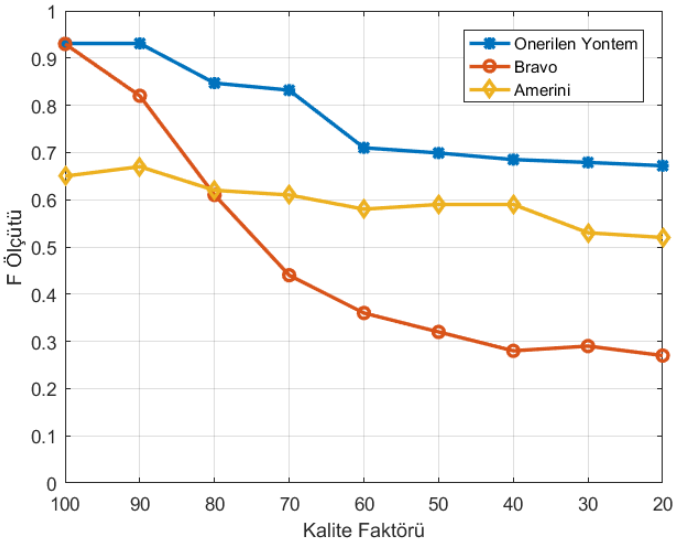
3.4. LIOP ve PatchMatch Tabanlı Yaklaşım'ın Sonuçları

Önerilen ilk yöntemin doğrulama performansı ölçümü için literatürde yer alan Amerini [47] ve Bravo [30] çalışmaları ile kıyaslanmıştır. Amerini ve Bravo'nun çalışmaları önerilen yöntemin gerçekleştirildiği donanım ve F ölçütü aynı şekilde hesaplanarak kıyaslanmıştır. İlk yapılan çalışmanın deneysel bulgularında, yöntemin gürültü atağına karşı test sonuçları verilmektedir. GRIP veri setinde yer alan AWGN gürültü atağına maruz kalmış, sırasıyla standart sapma değerleri $ln(2, 4, 6, 8$ ve $10)$ olan 400 adet sahte görüntü üzerinde test edilmiştir. Şekil 32'de gösterildiği gibi gerçekleştirilen çalışma, Amerini ve Bravo'nun çalışmalarına göre daha iyi performans göstermektedir.



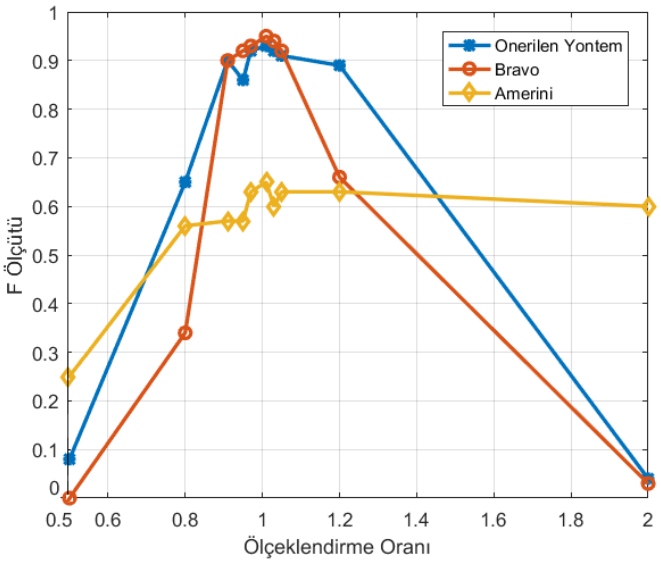
Şekil 32. Gürültü atağına karşı, karşılaştırmalı test sonucu

Gerçekleştirilen ilk çalışmanın ikinci deney bulgularında JPEG ataklarına karşı dayanıklılık test edilmiştir. GRIP veri setinde yer alan kalite faktörü 20, 30, 40, 50, 60, 70 80, 90 ve 100 olan 720 sahte görüntü üzerinde deneysel bulgular incelenmiştir. Amerini, Bravo ve gerçekleştirilen yöntemin test sonuçları Şekil 33'te gösterilmektedir. Gerçekleştirilen yöntemin 20 kalite faktöründe bile diğer çalışmalardan daha iyi sonuç verdiği ispat edilmiştir.



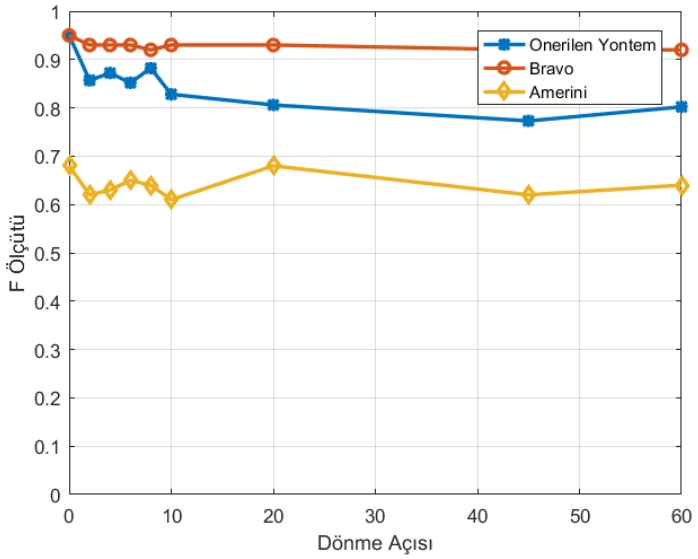
Şekil 33. JPEG sıkıştırma atağına karşı, karşılaştırmalı test sonucu

Gerçekleştirilen çalışmanın üçüncü deneysel bulgularında ölçekleme atağına karşı dayanıklılık test edilmiştir. GRIP veri setinde sırasıyla %50, %80, %93, %107, %120 ve %200 oranlarında ölçekleme atağı ile elde edilmiş 480 adet sahte görüntü kullanılmıştır. Ortalama performans sonuçları Şekil 34'te gösterilmiştir. Gerçekleştirilen çalışmanın ölçekleme ataklarında da yüksek performansa sahip olduğu gösterilmektedir.



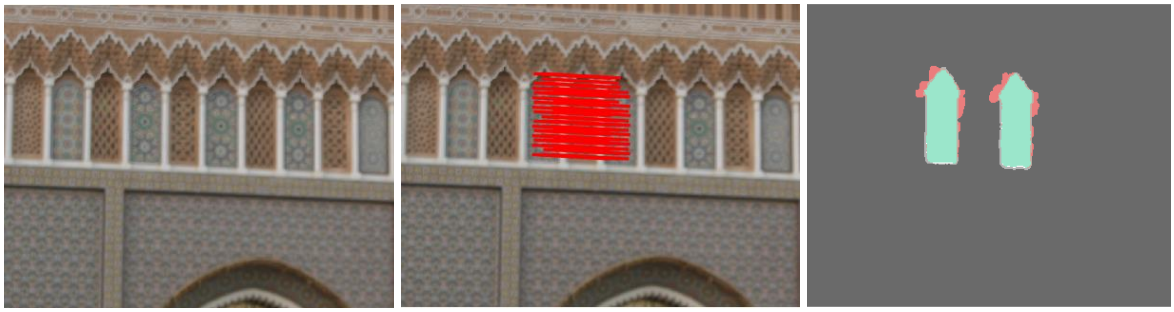
Şekil 34. Ölçekleme atağında, karşılaştırmalı test sonucu

Gerçekleştirilen çalışmanın son deneysel bulgularında yöntemin döndürme atağına karşı performans analizi verilmiştir. GRIP veri setinde olan 2^o, 4^o, 6^o, 8^o,10^o, 20^o, 45^o ve 60^o dönme atağına maruz kalmış, 640 adet sahte görüntü test edilmiştir. Önerilen yöntem Amerini ve arkadaşlarının çalışmasından daha iyi olduğu kanıtlanmıştır. Ancak Bravo ve arkadaşları tarafından gerçekleştirilen çalışma, gerçekleştirilen çalışmaya göre daha yüksek performansa sahiptir. Karşılaştırmalı test sonuçları Şekil 35'de verilmiştir.



Şekil 35. Döndürme atağına karşı, karşılaştırmalı test sonucu

GRIP veri seti görüntüsü üzerinde gerçekleştirilen çalışmanın örnek algoritma çıktısı Şekil 36'da verilmiştir. Şekilde görüldüğü gibi görüntü üzerindeki mozaik desenli pencere dokusu kopyala-yapıştır sahteciliği yöntemiyle kopyalanarak, bir sonraki mozaikli pencere dokusu üzerine yapıştırılmış. Daha sonra sahtecilik tespitini zorlaştırmak için görüntünün kalite faktörü 90 olarak belirlenmiştir. JPEG sıkıştırma atağında, LIOP ve PatchMatch tabanlı yöntem görüntü üzerinde çalıştırılmış ve algoritma sonucu eşleşen vektörler boyanarak sonuç görüntüsü elde edilmiştir. Algoritma çıktısının ölçülmesinde kullanılan F ölçütü, literatürde başarılı olarak kabul edilen bir sonuç olan 0.923 olarak hesaplanmış ve Şekil 36 (c)'de gösterilmiştir.



(a) (b) (c)

Şekil 36. (a) Kalite faktörü 90 olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü

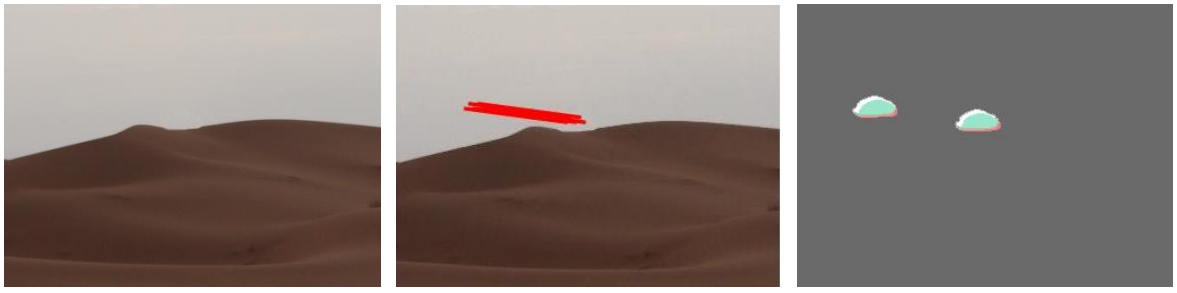
GRIP veri seti üzerinde Şekil 37 (a)'da ölçekleme atağına %80 oranında ölçekleme atağına maruz kalmış test görüntüsü görülmektedir. (b)'de LIOP + PatchMach yöntemini sonucunda eşleşen özellik vektörleri gösterilmektedir. Önerilen yöntem sonucunda F ölçütü bu atağa maruz kalmış görüntülerde, literatürde başarılı olarak kabul edilen bir sonuç olan 0.81 olarak hesaplanmıştır ve Şekil 37 (c)'de gösterilmiştir.

(a) (b) (c)

Şekil 37. (a) %80 oranında ölçekleme atağına maruz kalmış sahte görüntüsü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü

Şekil 38 (a)'da gürültü atağına maruz kalmış standart sapma değeri $ln2$ olan sahte görüntü gösterilmektedir. (b)'de önerilen yöntemin sonucunda, eşleşen özellik vektörleri gösterilmektedir. Test görüntüsü literatürde zor olarak kabul edilen pürüzsüz (smooth)

bölge üzerinde gürültü atağında bile etkili sonuç vermektedir. F ölçütü zor olan test görüntüsünde 0,892 hesaplanmıştır ve Şekil 37 (c)'de gösterilmiştir.



(a) (b) (c)

Şekil 38. (a) Standart sapması $\boldsymbol{ln}2$ olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü

Şekil 39 (a)'da GRIP veri seti içerisinde 90^o döndürme atağına maruz kalmış sahte test görüntüsü yer almaktadır. (b)'de önerilen yöntemin sonucunda, eşleşen özellik vektörleri gösterilmektedir. Test görüntüsü literatürde zor olarak kabul edilen pürüzsüz (smooth) bölge üzerinde gürültü atağında bile etkili sonuç vermektedir. Önerilen yöntemin F ölçütü, literatürde başarılı olarak kabul edilen bir sonuç olan 0.938 olarak hesaplanmış ve Şekil 39 (c)'de gösterilmiştir.

(a) (b) (c)

Şekil 39. (a) 90^o döndürme atağına maruz kalmış sahte görüntü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) F ölçütü hesaplama görüntüsü

3.5. RINBP ve SIFT Tabanlı Yaklaşım'ın Sonuçları

GRIP veri setinde F ölçütünün hesabı için 80 tane orijinal 80 tane sahte görüntü kullanılmıştır. İlk aşamada yalnızca bir görüntü parçasının kopyalanıp yapıştırılması sahte görüntü olarak kabul edilmiştir. Daha sonra kopyalanıp yapıştırılan yamanın üzerinde JPEG sıkıştırma, Gauss gürültüsü ekleme, döndürme ve ölçeklendirme işlemleri uygulanarak algılanması daha zor sahtecilik durumları için tespit algoritması koşturulmuştur. Algoritmanın başarımını ölçmek için F ölçütünden yararlanılmıştır. Önerilen yöntem sahte görüntülerde olduğu gibi orijinal görüntülerde de bazı eşleşmeler yapmıştır. Sahte görüntüde eşleşen özellik vektörleri yaklaşık olarak 300 civarındayken, gerçek görüntülerde bu sayı 0-10 arası değişmektedir. Bu nedenle deneysel olarak bulunan eşik değeri 15 olarak uygulanmıştır. 15 eşleşmenin altındaki görüntüler gerçek görüntü üstü ise sahte görüntü olarak etiketlenmiştir.

Etiketleme aşamasında;

- Sahte olarak etiketlenen sahte görüntüler "Doğru Pozitif" (DP)
- Gerçek olarak etiketlenen sahte görüntüler "Yanlış Negatif" (YN)
- Sahte olarak etiketlenen gerçek görüntüler "Yanlış Pozitif" (YP)
- Gerçek olarak etiketlenen gerçek görüntüler "Doğru Negatif" (DN)

olarak etiketleme gerçekleştirilmiştir.

İkinci yapılan çalışmanın döndürme ataklarına karşı dayanıklılığı vurgulanmıştır. Tablo 3'de GRIP veri setindeki döndürme atağındaki her derece için 80 adet görüntüden toplam 1120 adet test görüntüsü üzerinde, tüm derecelerdeki döndürme ataklarına karşı dayanıklılık test edilmiştir. Test sonucunda elde edilen görüntü seviyesindeki F ölçütü ortalama değerleri verilmiştir.

Tablo 3. RINBP + SIFT Yönteminin döndürme ataklarına karşı dayanıklılığı

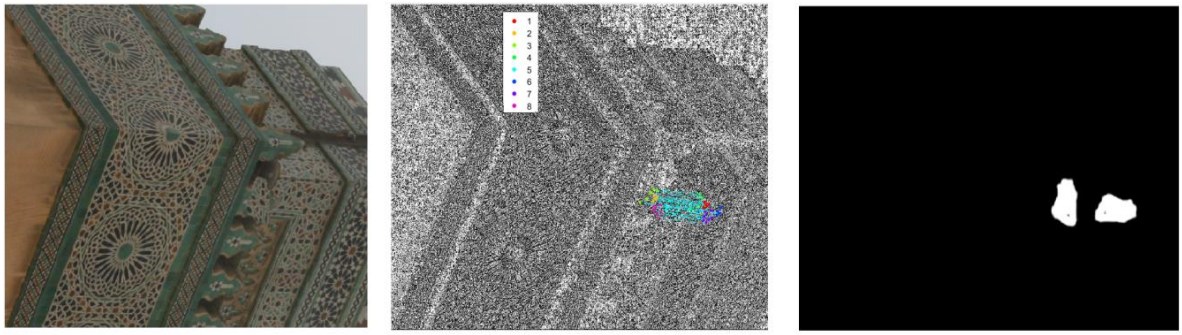
RINBP + SIFT	F Ölçütü	RINBP + SIFT	F Ölçütü
0º	0,968	**30º**	0.93
2º	0.937	**45º**	0.918
4º	0.923	**60º**	0.926
6º	0.942	**75º**	0.917
8º	0.942	**90º**	0.91
10º	0.934	**105º**	0.888
20º	0.913	**180º**	0.901

Önerilen yöntemin görüntü seviyesinde ölçülen F ölçütü değeri sonuçları, literatürde var olan diğer çalışmalar ile karşılaştırılmış olup Tablo 4'te gösterilmektedir.

Tablo 4. RINBP+SIFT Yönteminin F Ölçütü Performans Sonuçları

Yöntemler	F Ölçütü (%)
Bravo 2011 [30]	94,12
Christlein 2012 [54]	67,72
Li 2015 [35]	72,13
Cozzolino 2015 [63]	94,36
Zandi 2016 [50]	86,89
Bi 2018 [60]	96,63
Önerilen Yöntem	96,89

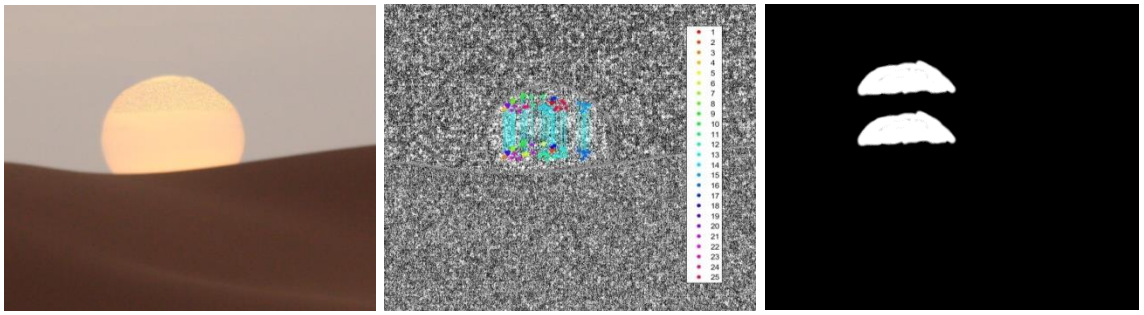
Şekil 40 (a)'da GRIP veri setinde bulunan 90^o döndürme atağına maruz kalmış sahte görüntü görülmektedir. Anahtar noktası tabanlı yapılan çalışmaların sahtecilik tespiti için zor sayılan mimari görüntüde F ölçütü 0,94 olarak hesaplanmıştır. (b)'de yöntemin çıktısında eşleşen anahtar noktaları gösterilmektedir. (c)'de kopyalanıp-yapıştırılan bölgenin gözlemlenebilmesi için 90^o döndürme atağına maruz kalmış görüntünün maskesi yer almaktadır.



(a) (b) (c)

Şekil 40. (a) 90^o döndürme atağına maruz kalmış sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi

Şekil 41 (a)'da GRIP veri setinde bulunan gürültü atağına maruz kalmış standart sapma değeri $ln2$ olan, sahte görüntü görülmektedir. Anahtar noktası tabanlı yapılan çalışmaların sahtecilik tespiti için zor olan pürüzsüz (smooth) bölge içeren görüntüde F ölçütü 0,892 olarak hesaplanmıştır. (b)'de yöntem çıktısında eşleşen anahtar noktaları gösterilmektedir. (c)'de kopyalanıp-yapıştırılan bölgenin gözlemlenebilmesi için sahte görüntünün maskesi yer almaktadır.

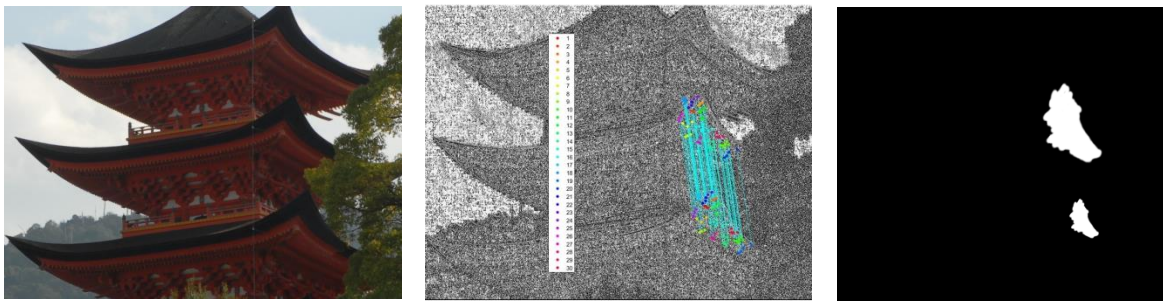


(a) (b) (c)

Şekil 41. (a) Standart sapması $\boldsymbol{ln}2$ olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi

Şekil 42 (a)'da GRIP veri setinde bulunan ölçekleme atağına %50 oranında ölçekleme atağına maruz kalmış test görüntüsü görülmektedir. Anahtar noktası tabanlı yapılan çalışmada mimari görüntüde F ölçütü 0,913 olarak hesaplanmıştır. (b)'de yöntem

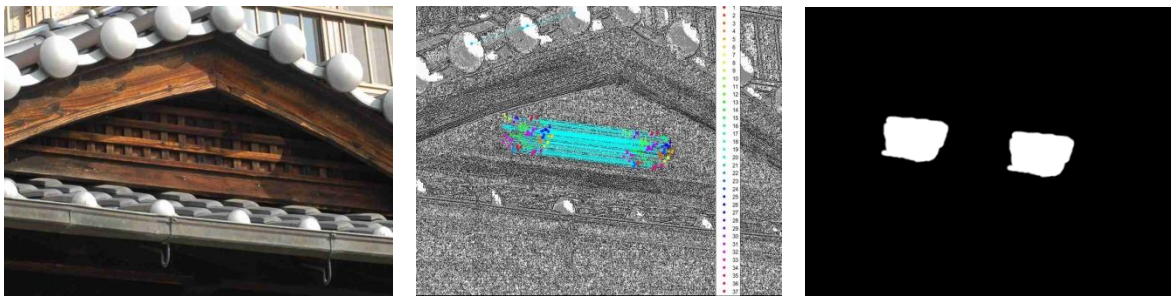
çıktısında eşleşen anahtar noktaları gösterilmektedir. (c)'de kopyalanıp-yapıştırılan bölgenin gözlemlenebilmesi için sahte görüntünün maskesi yer almaktadır.



(a) (b) (c)

Şekil 42. (a) %50 oranında ölçekleme atağına maruz kalmış sahte görüntüsü (b) Önerilen yöntem sonucunda eşleşen özellik vektörleri (c) sahte görüntünün maskesi

Şekil 43 (a)'da GRIP veri setinde bulunan kalite faktörü 20 olarak JPEG formatında sıkıştırılmış olan sahte görüntü görülmektedir. RINBP+ SIFT anahtar noktası tabanlı yapılan çalışmada mimari görüntüde F ölçütü 0,911 olarak hesaplanmıştır. Eşleşen anahtar noktaları (b)'de gösterilmiştir. (c)'de kopyalanıp-yapıştırılan bölgenin gözlemlenebilmesi için sahte görüntünün maskesi yer almaktadır.



(a) **(b)** **(c)**

Şekil 43. (a) kalite faktörü 20 olan sahte görüntü (b) Önerilen yöntem sonucunda eşleşen anahtar noktaları (c) sahte görüntünün maskesi

İlk önerilen çalışma olan LIOP + PatchMatch ve ikinci önerilen çalışma olan RINBP + SIFT yöntemlerinin karşılaştırma tablosu Tablo 5'de verilmiştir. Her iki yöntemde, INTEL i7 4720 HQ işlemcili ve 16 GB DDR3 RAM kapasitesine sahip bilgisayar tarafından gerçekleştirilmiştir. Gerçekleştirilen çalışmaların kodları MATLAB® 2015 programı yardımıyla derlenmiştir.

Tablo 5. Tez kapsamında önerilen yöntemlerin karşılaştırılması

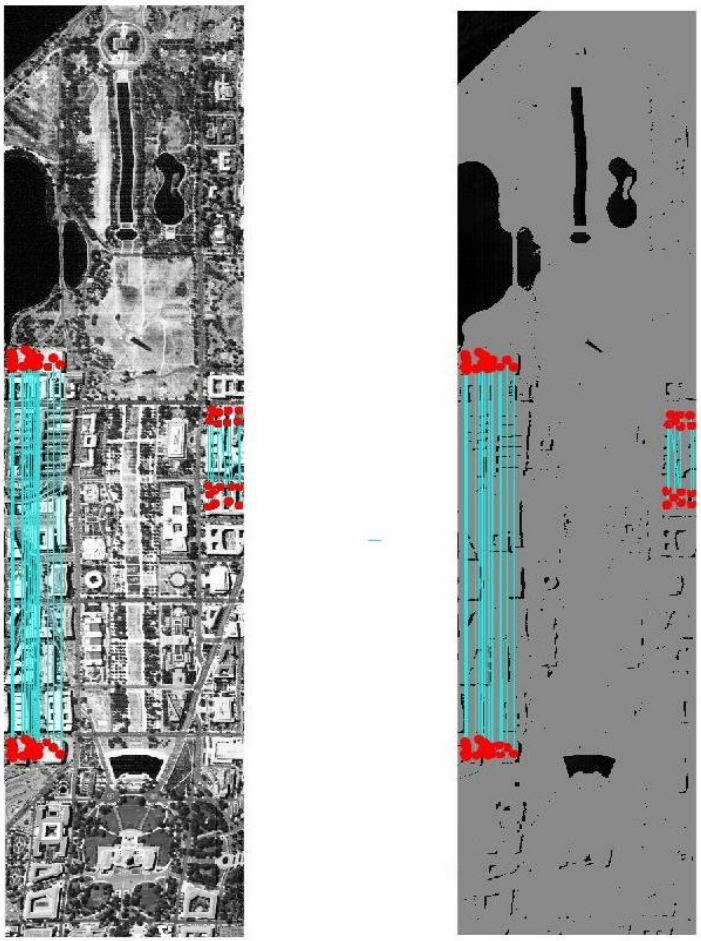
Karşılaştırma Metrikleri	LIOP + PatchMatch	RINBP + SIFT
Doku oluşturma	✓	✓
Döndürme, ölçekleme, gürültü, JPEG sıkıştırma ataklarına karşı dayanıklılık	✓	✓
Yanlış eşleştirmelerin giderilmesi	✓	✓
Bir görüntü üzerinde ortalama hesaplama süresi (sn)	91	514
F ölçütü değeri	Piksel Tabanlı	Görüntü Tabanlı

3.6. Hiperspektral Görüntüler Üzerinde Kopyala-Yapıştır Sahteciliği Tespiti Sonuçları

Bu bölümde hiperspektral görüntüler üzerinde uygulanarak elde edilen sahte görüntüler üzerinde gerçekleştirilen kopyala-yapıştır sahteciliği tespiti sonuçları verilmektir.

Renkli görüntüler kırmızı, yeşil, mavi olmak üzere 3 katman bulundururken, Hiperspektral görüntü veri setinde her görüntü için ortalama 180 katmanda parlaklık verisi bulunmaktadır. Fakat sahtecilik tespiti için her katman bilgi açısından zengin değildir. Bazı katmanlar sadece tek parlaklık seviyesi olurken (örneğin 120 parlaklık seviyesi ile sadece gri görünen katmanlar) diğer katmanlar geniş bir histogram aralığı içermektedir. Geniş histogram aralığı içeren katmanlar SIFT algoritması ile daha çok anahtar noktası üretmektedir. Bu nedenle daha zengin bilgi içerdiği şeklinde yorumlanmıştır. Örneğin Washington D.C. hiperspektral görüntüsü için 25 farklı katmanda SIFT algoritması çalıştırılmıştır. Katmanlar arasında eşleşen anahtar noktaları karşılaştırılarak 10x10 piksel etrafında diğer katmanlarda eşleşme olup olmadığı araştırılmıştır. Doğru verilen eşleşme kararlarında anahtar noktasının en az 10 katmanda aynı anahtar noktasıyla eşleştiği gözlemlenmiştir.

Şekil 44'de önerilen yöntem ile gerçekleştirilen test sonucu verilmiştir. (a)'da hiperspektral görüntünün 90. katmanındaki görüntü bandı üzerindeki eşleşen anahtar noktaları gösterilmektedir. (b)'de aynı hiperspektral görüntünün 130. katmanındaki eşleşme sonucu gösterilmektedir.



(a) (b)

Şekil 44. Washington D.C. hiperspektral görüntüsünde eşleşme sonucu

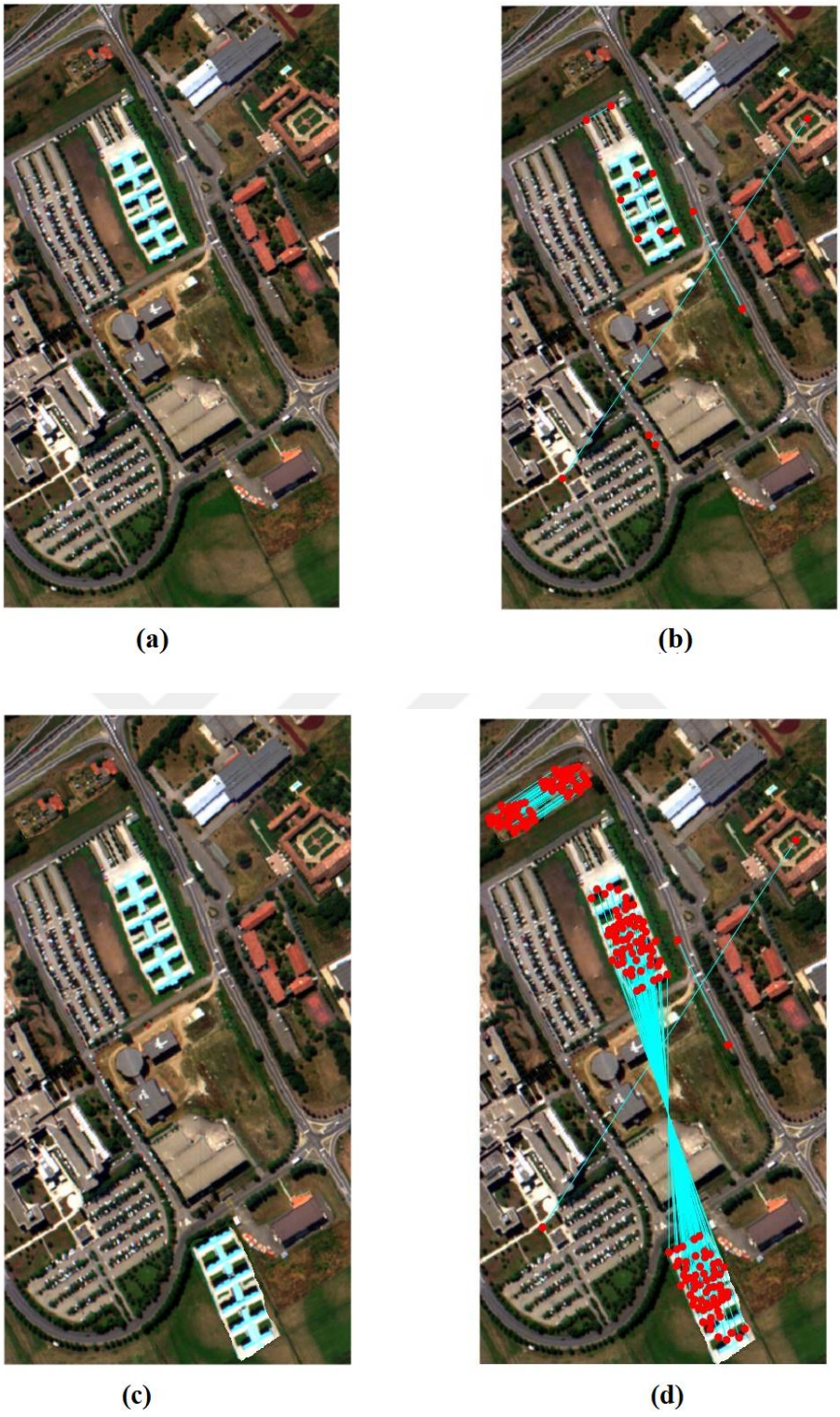
Hiperspektral görüntü veri setinde görüntü sayısı oldukça azdır. Bu nedenle görüntü etiketleme olarak doğruluk ölçümü hassas değildir. Çünkü bir görüntünün yanlış etiketlenmesi F ölçütünü yaklaşık %20 düşürmektedir. Bu nedenle Hiperspektral görüntülerde anahtar noktası tabanlı F ölçütü ile başarım incelenmiştir. Hiperspektral görüntülerde 3 adet orijinal görüntünün her katmanında aynı konumdaki bölgeler kopyalanarak yine her katmanda aynı olan farklı bir bölgeye yapıştırılarak sahte görüntüler ve maske oluşturulmuştur. Önerilen yöntem örneğin Pavia University hiperspektral

görüntüsüne uygulandığında, görüntüde toplamda 4344 adet anahtar noktası bulunmuştur. Bulunan anahtar noktalarının özellik vektörleri leksikografi sıralamasından sonra Öklid uzaklığı kullanılarak eşleşmeler yapılmıştır. Eşleşme algoritmasının çıktısında 356 adet anahtar noktası eşleşmesi gerçekleşmiştir. 12 tane anahtar noktası maskenin dışında eşleşmiştir. 344 tanesi maskenin içinde eşleşmiştir. 6 adet anahtar noktası maskenin içinde olmasına rağmen eşleşmemiştir. Bunların haricinde maskenin dışında kalıp eşleşmeyen 3982 adet anahtar noktası bulunmuştur. F ölçütünü hiperspektral görüntü için hesaplarken kullanılan parametreler;

- Maskenin içinde kalıp eşleşen anahtar noktaları (DP)
- Maskenin içinde kalıp eşleşmeyen anahtar noktaları (YN)
- Maskenin dışında kalıp eşleşen anahtar noktaları (YP)
- Maskenin dışında kalıp eşleşmeyen anahtar noktaları (DN)

olarak belirlenmiştir. Bu parametreler ölçümlerine göre Pavia University test görüntüsünün F ölçütü %97,45 bulunmuştur. F ölçütünün %97,45'lik değeri görüntünün %97,45 ihtimal olasılığında sahte olduğu yönünde yorumlanmıştır.

Şekil 45 (a)'da Pavia University hiperspektral görüntüsü verilmiştir. Eşleşen noktalar (b)'de verilmiştir. (a) görüntüsünün her katmanında aynı konumlar arası kopyala-yapıştır sahteciliği ve kopyalanan yama üzerinde döndürme işlemi uygulanarak (c) görüntüsü elde edilmiştir. Döndürme saldırısına rağmen önerilen algoritma ile (c) görüntüsünde eşleşen 356 tane anahtar noktası bulunmuştur. Elde edilen eşleşme sonucu (d)'de verilmiştir. Eşleşen anahtar noktası sayılarındaki fark, önerilen algoritmanın güvenilirliğini göstermektedir.



Şekil 45. Pavia University hiperspektral görüntüsünde eşleşme sonucu

Tablo 6‘da kullanılan hiperspektral görüntüler üzerinden hesaplanan F ölçütü değerleri verilmiştir.

Tablo 6. SIFT Tabanlı Yönteminin Hiperspektral Görüntülerdeki F Ölçütü Performans Sonuçları

Veri Seti	**F Ölçütü (%)**
Washington D.C.	96,06
Pavia University	97,45
Pavia Center	96,8

4. SONUÇLAR

Yüksek lisans çalışması kapsamında gerçekleştirilen işlemler ve elde edilen bulgular neticesinde kopyala-yapıştır sahteciliği tespitinde blok tabanlı algoritmaların döndürme ve ölçekleme ataklarına karşı dayanıksız olduğu, anahtar noktası tabanlı algoritmaların ise pürüzsüz bölge içeren görüntülerde yanlış eşleştirme yaptığı ve kötü sonuçlar verebildiği gözlemlenmiştir. Buradan yola çıkarak eksikliklerin giderilmesi ve ataklara karşı dayanıklı iki çalışma gerçekleştirilmiştir.

Gerçekleştirilen ilk çalışmada literatürde en sık kullanılan görüntü sahtecilik türü olan kopyala-yapıştır sahteciliği tespiti için etkin bir çalışma gerçekleştirilmiştir. LIOP ve PatchMatch tabanlı çalışmada ataklara karşı dayanıklı ve etkin bir sahtecilik tespit sistemi geliştirilmiştir. Gerçekleştirilen çalışma literatürde referans olarak oldukça sık kullanılan Amerini [47] ve Bravo'nun [30] çalışmaları ile aynı veri seti üzerinde kıyaslanma yapılarak karşılaştırılmıştır. Gerçekleştirilen yöntem ile döndürme, ölçekleme, gürültü ekleme ve JPEG atakları dahi uygulansa görüntü üzerindeki bir veya birden fazla yapılan kopyala-yapıştır sahteciliğinin tespit edildiği kanıtlanmıştır. Gerçekleştirilen çalışmanın, döndürme ataklarında Bravo ve arkadaşlarının yaptığı çalışmaya oranla daha düşük sonuç verdiği gözlemlenmiştir. Bu sebeple RINBP ve SIFT tabanlı ikinci bir çalışma önerilerek döndürme atağına karşı dayanıklılık kazandırılmıştır.

RINBP ve SIFT tabanlı gerçekleştirilen ikinci çalışmada döndürme ataklarında oldukça etkili bir yöntem önerildiği kanıtlanmıştır. Gerçekleştirilen çalışmanın sadece döndürme ataklarına karşı değil, literatürde var olan diğer çalışmalara kıyasla iyi bir çalışma olduğu gözlemleniştir.

Literatürde daha önce kopyala-yapıştır sahteciliği üzerinde hiç denenmemiş ancak birçok dalda önemli bir yere sahip hiperspektral görüntüler üzerinde sahteciliği tespiti denenerek literatüre yeni bir bakış açısı getirilmiştir. Test görüntüsü sonuçlarından da anlaşıldığı gibi her bir katmanda farklı doku özelliklerinden elde edilen anahtar noktaları ile başarılı sonuçlar elde edilmiştir.

5. ÖNERİLER

Literatür çalışması ve önerilen yöntemlerden de anlaşıldığı gibi hibrit ve dinamik yöntemlerin deneysel bulguları diğer yöntemlere göre daha iyidir. Daha sonraki çalışmalarda tüm ataklara karşı başarılı hibrit yöntemler geliştirilebilir.

Sahtecilik tespiti için önerilen yöntemlerin işlem maliyetleri hesaplanarak, literatürdeki diğer çalışmaların hesaplama maliyetleri ile karşılaştırılma yapılabilir. Böylece yeni bir karşılaştırma metriği elde edilmiş olur.

Hiperspektral görüntüler üzerinde çeşitli ataklar uygulanarak yeni veri seti görüntüsü elde edilebilir. Elde edilen ataklı görüntüler üzerinde test bulguları incelenebilir. Ataklara karşı dayanıklılık literatürde var olan diğer çalışmalar ile karşılaştırılabilir.

6. KAYNAKÇA

1. Qureshi M. A. ve Deriche M., A bibliography of Pixel-Based Blind Image Forgery Detection Techniques, Signal Processing: Image Communication, 39 (2015) 46-74.

2. Muzaffer G., Karaagacli E.S. ve Ulutas G., Recent keypoint based copy move forgery detection techniques, International Artificial Intelligence and Data Processing Symposium (IDAP),Eylül, 2017, Malatya, Bildiriler Kitabı: 1-7.

3. Oral M., Furat M., Veri Saklama Yöntemleri Sayısal Görüntülerin Damgalanması, Amaçları Ve Uygulama Alanları, İletişim Teknolojileri Ulusal Sempozyumu (ITUSEM), Ekim 2007, Adana, Bildiriler Kitabı: 195-200.

4. Cox, I. J., Miller, M. L. ve Bloom, J. A., Digital Watermarking and Setenography, Multimedia Information and Systems, Haziran, 2002, San Francisco, Bildiriler kitabı: 41-83.

5. Rey, C. ve Dugelay, J. L., A Survey of Watermarking Algorithms for Image Authentication, EURASIP Journal on Applied Signal Processing, 50 (2002) 613-621.

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

7. Boz A. , Dijital Görüntülerde Kopyala Taşı Sahteciliği Tespiti Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2016.

8. Chihaoui T., Bourouis S. ve Hamrouni K., Copy-move image forgery detection based on SIFT descriptors and SVD-matching, 2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), 2014, 125-129.

9. https://www.scopus.com/home, 15 Ocak 2019.

10. Ng T. ve Chang S., A model for image splicing, International Conference on Image Processing (ICIP '04), Temmuz 2004, Singapore, Bildiriler Kitabı: 169-1172.

11. Mahdian B. ve Saic, S., Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security, 3 (2008) 103-113.

12. Farid H. ve Lyu S., Higher-Order Wavelet Statistics And Their Application To Digital Forensic, 3th Computer Vision and Pattern Recognition Workshop, Haziran 2003, USA, Madison, Bildiriler Kitabı: 132-138 .

13. Huang H., Guo Q. ve Zhang Y., Detection of copy-move forgery in digital images using SIFT algorithm, Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Aralık 2008, Wuhan, 272-276.

14. Pan X. ve Lyu S., Region duplication detection using image feature matching, IEEE Transactions On Information Forensics And Security, 5, 4 (2010) 857-867.

15. Fridrich, A. J., Soukal, B. D. ve Lukas, A. J., Detection of copy-move forgery in digital images, Proceedings of Digital Forensic Research Workshop, Ağustos, 2003, USA, Trumansburg, 15-18 .

16. Popescu, A. ve Farid, H., Exposing Digital Forgeries by Detecting Duplicated Image Regions, Tech. Rep., Dartmount Collage, 2004.

17. Luo, W., Huang, J. ve Qiu, G., Robust Detection of Region Duplication forgery in Digital Images, 18th International Conference on Pattern Recognition (ICPR'06), Ağustos 2006, Hong Kong, 746-749.

18. 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, IEEE International Conference on Multimedia and Expo, Beiijing, Temmuz 2007 .

19. Myna, A. N., Venkateshmurthy M. G. ve Patil C. G., Detection of Region Duplication Forgery In Digital Images Using Wavelets and Log-polar Mapping, IEEE Int. Conf. Computational Intelligence and Multimedia Applications, Aralık 2007, Sivakasi, Tamil Nadu, , 371-377.

20. Kang, X. ve Wei, S., Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensic, International Conference on Computer Science and Software Engineering, Aralık 2008, Çin, Wuhan, 926-930.

21. Zhang, J., Feng, Z. ve Su, Y., A new approach for detecting Copy-Move forgery in digital images. 11th IEEE Singapore International Conference on Communication Systems, Kasım 2008, Guangzhou, 362-366.

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

23. 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, 1053-1056.

24. Khan, S. ve Kulkarni, A., Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform, International Conference & Workshop on Emerging Trends in Technology, Şubat 2010, New York, 31-36.

25. Wu Q., Wang S. ve Zhang X., Detection of Image Region-Duplication with Rotation and Scaling Tolerance,) Computational Collective Intelligence, Technologies and Applications, 6421 (2010) 100-108.

26. Wu Q., Wang S. ve Zhang X., Log-Polar Based Scheme for Revealing Duplicated Regions in Digital Images, IEEE Signal Processing Letters, 18, 10 (2011) 559-562.

27. Huang Y., Lu, W., ve Long, D., Improved DCT Based Detection of Copy-Move Forgery im Images , Forensic Science International, 206 (2011) 178-184.

28. Ghorbani M., Firouzmand M. ve Faraahi A., DWT-DCT (QCD) based copy-move image forgery detection, 18th International Conference on Systems, Signals and Image Processing, Sarajevo, 2011, 1-4.

29. Muhammad G., Hussain M., Khawaji K. ve Bebis G., Blind copy move image forgery detection using dyadic undecimated wavelet transform, 17th International Conference on Digital Signal Processing (DSP), 2011, Corfu, 1-6.

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

31. Hsu H. ve Wang M., Detection of copy-move forgery image using Gabor descriptor, Anti-counterfeiting, Security and Identification, Mayıs 2012, Taipei, 1-4.

32. 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, Ağustos 2011, Tehran, 1-4.

33. Wandji, N. D. ve Xingming, S., Robust Detection of Copy-Move Forgery in Color Images, Proceedings of the International Conference on Image Processing, Computer Vision and Pattern Recognition (IPCV), Haziran 2013 Las Vegas, Nevada USA, 492-495.

34. 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.

35. Li, L., Li, S., Zhu H. ve Wu X., Detecting Copy-Move Forgery Under Affine Transforms for image Forensics, Computer & Electrical Engineering on Elsevier, 40, 6 (2014) 1951-1962.

36. Lee J. C., Chang C. P. ve Chen W. K., Detection of Copy-Move Image Forgery Using Histogram of Orientated Gradients, Information Sciences, 3, 21 (2015) 250-262.

37. Üstübioğlu, B., Ulutaş G., Nabiyev V. ve Ulutaş M., Image forgery detection based on energy probability, 23nd Signal Processing and Communications Applications Conference (SIU), Eylül 2015, Malatya, 919-922.

38. Moussa M. A., A fast and accurate algorithm for copy-move forgery detection, Proc. ICCES, Ocak 2015, Cairo, 281–285.

39. Boz A. ve Bilge H.Ş., Copy-move image forgery detection based on LBP and DCT, 24th Signal Processing and Communication Application Conference (SIU), Eylül 2016, Zonguldak, Bildiriler Kitabı: 561-564.

40. Mahmood T., Irtaza A., Mehmood Z. ve Mahmood M. T., Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images, Forensic Science International, 279 (2017) 8-21.

41. Wang Y., Tian L. ve Li C., LBP-SVD based copy move forgery detection algorithm, IEEE International Symposium on Multimedia (ISM), Mayıs 2017, Taichung, 553-556.

42. Hosny K. M., Hamza H. M. ve Lashin N. A., Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators, Imaging Science Journal, 66, 6 (2018) 330–345.

43. Pan, X. ve Lyu, S., Detecting Image Region Duplication Using SIFT Features, International Conference on Acoustics, Speech and Signal Processing, Ocak 2010, Dallas, 1706-1709.

44. Pan, X. ve Lyu, S., Region Duplication Detection Using Image Feature Matching, IEEE Transactions on Information Forensics and Security, 5 (2010) 857-867.

45. Bo, X., Junwen, L., Guangjie, L. ve Yuewei, D., Image Copy-Move Forgery Detection Based On SURF, International Conference on Multimedia Information Networking and Security, Ekim 2010, Nanjing, Jiangsu, 889–892.

46. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. 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.

47. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A., Tongo, L. ve Serra, G., Copy- move forgery detection and localization by means of robust clustering with J-linkage, Signal Processing : Image Communication, 28 (2013) 659-669.

48. Yu, L., Han, Q. ve Niu, X., Feature point-based copy-move forgery detection: covering the non-textured areas, Multimedia Tools and Applications, 75, 2 (2014) 1159–1176.

49. Zhu Y., Shen X. ve Chen H., Copy-move Forgery Detection Based on Scalled ORB, Multimedia Tools and Applications, 75, 6 (2015) 1-15.

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

51. Warif N. B. A., Wahab A. W. A., Idris M. Y. I., Salleh R. ve Othman F., SIFT-symmetry: A robust detection method for copy-move forgery with reflection attack, Journal of Visual Communication and Image Representation, 46 (2017) 219–232.

52. Wang X.-Y., Li S., Liu Y.-N., Niu Y., Yang H.-Y. ve Z.-L Zhou, A new keypoint-based copy-move forgery detection for small smooth regions, Multimedia Tools and Applications, 76, 22 (2017) 23353–23382.

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

54. 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.

55. Hashmi M. F., Hambarde A. R. ve Keskar A. G., Copy move forgery detection using DWT and SIFT features, 13th International Conference on Intellient Systems Design and Applications, Kasım 2013, Bangi, 188-193.

56. 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.

57. http://www.dicgim.unipa.it/cvip/, Ardizzone dataset, Eylül 2017.

58. Tatkare K. A. ve Mane V., Fusion of SIFT and hue moments features for cloning tamper detection, International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Mayıs 2015, Davangere, 409-414.

59. Prasad S. ve Ramkumar B., Passive copy-move forgery detection using SIFT, HOG and SURF features, IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Nisan 2016, Bangalore, 706-710.

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

61. Wang, Z., Fan, B. ve Wu, F., Local Intensity Order Pattern for Feature Description, IEEE International Conference on Computer Vision (ICCV 2011), Mayıs 2011, Barcelona, 603-610.

62. Barnes C., Shechtman E., Finkelstein A. ve Goldman D.M., Patch-Match: a randomized correspondence algorithm for structural image editing, ACM Transactions on Graphics (Proc. SIGGRAPH), 28, 3 (2009) 48-72.

63. 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.

64. Hamouchene I. ve Aouat S., A cognitive approach for texture analysis using neighbors-based binary patterns, IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing, Mayıs 2014, London, 94-99.

65. Ojala T., Pietikainen M. ve Maenpaa T., Gray scale and rotation invariant texture classification with local binary patterns, Computer Vision, ECCV Proceedings, Lecture Notes in Computer Science 1842, Nisan 2000, Springer, 404-420.

66. Lowe, D.G., Distinctive Image Features from Scale-Invariant Keypoints, International Journal of Computer Vision, 2, 60 (2004) 91-110.

67. Fischler, M. A. ve Bolles, R. C., Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography, Communications of the ACM, 24, 6 (1981) 381-395.

68. Perkinson, M.C., Lobb, D., Cutter, M. ve Renton, R., Low Cost Hyperspectral Imaging from Space, 5th IAA Symposium on Small Satellites for Earth Observation, 2-6 April 2001, Berlin, 102-108 .

69. Karaca, A.C., Ertürk, A., Güllü, M.K., Elmas M. ve Ertürk S., Hiperspektral Görüntüleme Sistemi ile Adli Belgelerdeki Bulguların Analizi, 20. IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı , 2012, Muğla.

70. Karaca, A.C., Ertürk, A., Güllü, M.K., Elmas M. ve Ertürk S., Hiperspektral Görüntüleme ile Kamuflaj Tespiti, 6. Savunma Teknolojileri Kongresi (SAVTEK 2012),Haziran, 2012, Ankara.

71. http://www.grip.unina.it, 12 Nisan 2017.

72. Fauvel, M., Chanussot, J. ve Benediktsson, J. A., Kernel principal component analysis fort he classification of hyperspectral remote sensing data over urban areas, EURASIP Journal on Advances Signal Proccessing, 19, 80 (2009) 384-403.

73. Mura, D.D., Villa, A., Benediktsson, J.A., Chanussot, J. ve Bruzzone, L., Classification of hyperspectral images by using extended morphological attribute profiles and independent component analysis, IEEE Geoscience and Remote Sensing Letters, 8, 3 (2011) 542-546.

ÖZGEÇMİŞ

1992 yılında Elazığ'da doğdu. İlkokul, ortaokul ve lise öğrenimini Elazığ'da tamamladı. 2010 yılında Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde lisans programına başladı. 2011 yılında Esenboğa Havalimanı Bilgi İşlem Biriminde gönüllü stajyer olarak üç ay boyunca çalıştı. 2012 yılının yaz stajını Ortadoğu Teknik Üniversitesi Teknokent bünyesinde bulunan AMP Yazılım'da tamamlamıştır. 2013 yılının yaz stajını Bilkent Teknokent bünyesinde bulunan Microsoft firmasında tamamlamıştır. "Mobil Cihazlarda Otobüs Takibi Ve NFC İle Ücret Ödeme" adlı proje ile 2014-TÜBİTAK 2241/A Sanayi Odaklı Lisans Bitirme Tezi Destekleme programında destek kazanıp, 2241/B Sanayi Odaklı Lisans Bitirme Projeleri Yarışmasında finalist olmuştur. 2014 yılında Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun olup, Microsoft-Ankara bünyesinde bulut teknolojileri biriminde göreve başlamıştır. 2016 yılında Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans öğrenimine başladı.

Akademik olarak yaptığı çalışmalar;

*A Copy-Move Forgery Detection Approach Based On Local Intensity Order Pattern And Patchmatch -2018,

*Recent Keypoint Based Copy Move Forgery Detection Techniques -2017,

*Lokasyon Bazlı CAPTCHA -2016,

*Pcap Paketler İle Restfull Apı'yi Gerçek Zamanlı Dinleme -2016,

*Modüler Sistemlerde Kurumsal Uygulamaları Çalıştırma -2015,

*Çölyak ve Fenilketonüri Hastaları için Barkod Destekli Ürün Mobil Satın Alma Rehberi -2015.