

**KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**



TRABZON



KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ORCID : - - -

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce

Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : / /

Tezin Savunma Tarihi : / /

Tez Danışmanı :

ORCID : - - -

Trabzon

ÖNSÖZ

“Videolarda Çerçevesel Arası Sahteciliklerin Tespiti” isimli bu tez Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Doktora Programı’nda hazırlanmıştır.

Video sahteciliklerinin tespiti, artan video kullanımına olan güvenin sağlanması için araştırılması gereken siber güvenlik alanındaki popüler konulardan biridir. Sosyal medyanın etkin ve yoğun bir şekilde kullanıldığı günümüz dünyasında sahte videoların hızla yayılımı, ülkeler gibi geniş kitlelerin kısa sürede bu videolardan etkilenmesine ve bir panik ortamının oluşmasına neden olmaktadır. Sahtecilik tespiti, kişilerin ve nesnelerin kimliklendirildiği sigorta şirketleri, güvenlik sistemleri gibi çoklu ortam verilerini kullanan sistemlerin güvenilirliğinin sağlanması için anahtar görevi görmektedir. Dolayısıyla toplumları etkileyen, mahkemelerde delil niteliği taşıyan videoların, bütünlüklerinin ve doğruluklarının araştırılması gerekmektedir. Bu tez çalışması kapsamında, videolar üzerinde yapılan çerçeveler arası sahteciliklerin tespitini gerçekleştiren bir doğrulama sistemi yapılmıştır. Sistemin gerçekleştirilmesi sırasında, literatürdeki açıklıkları giderebilecek ve yeni çalışmalara yol gösterebilecek yeni yaklaşımlar önerilmiştir.

Lisans eğitimimden bu yana danışmanlığımı üstlenen her türlü destek, ilgi ve tecrübelerini esirgemeyen Saygıdeğer Hocam Doç. Dr. Güzin ULUTAŞ’ a teşekkürü bir borç bilirim. Tez izleme komitemde bulunan ve önerileriyle tezimin son halini almasına katkı sağlayan Sayın Prof. Dr. Murat EKİNCİ ve Sayın Doç. Dr. Önder AYDEMİR hocalarıma teşekkürlerimi sunarım.

Bu süreçte sürekli yanımda olan, her türlü sevincime ve stresime ortak olan eşim Hakan BOZKURT’ a, oğlum Muhammed Bera BOZKURT’ a ve değerli aileme çok teşekkür ederim.

Bu tez çalışmasının bundan sonraki çalışmalara katkı sağlamasını temenni ederim.

Işıl BOZKURT

Trabzon 2023

TEZ ETİK BEYANNAMESİ

Doktora Tezi olarak sunduğum “Videolarda Çerçevesel Arası Sahteciliklerin Tespiti” 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. 24/07/2023

Işıl BOZKURT

İÇİNDEKİLER

	<u>Sayfa No</u>
ÖNSÖZ	III
TEZ ETİK BEYANNAMESİ	IV
İÇİNDEKİLER	V
ÖZET.....	VIII
SUMMARY	IX
ŞEKİLLER DİZİNİ.....	X
TABLolar DİZİNİ	XVI
SEMBOLLER DİZİNİ.....	XVII
1. GENEL BİLGİLER.....	1
1.1. Giriş.....	1
1.2. Sahte Video Oluşturma Teknikleri	6
1.2.1. Derin Sahte Video Üretimi	7
1.2.2. Konumsal Sahtecilikler	8
1.2.3. Zamansal Sahtecilikler	9
1.3. Sahtecilik Tespit Teknikleri	9
1.3.1. Derin Sahte Video Tespit Teknikleri	11
1.3.2. Çerçeve İçi Sahtecilik Tespit Teknikleri.....	13
1.3.3. Çerçeveler Arası Sahtecilik Tespit Teknikleri	14
1.3.3.1. Öznitelik Çıkarımına Dayalı Tespit Teknikleri.....	15
1.3.3.1.1. Sıkıştırma Kalıntılarına Dayalı Tespit Teknikleri.....	16
1.3.3.1.2. Gürültü Kalıntılarına Dayalı Tespit Teknikleri.....	17
1.3.3.1.3. Hareket Özniteliğine Dayalı Tespit Teknikleri.....	18
1.3.3.1.4. İstatistiksel Özniteliklere Dayalı Tespit Teknikleri.....	20
1.3.3.2. Öğrenmeye Dayalı Tespit Teknikleri.....	24
1.3.3.3. Hibrit Yöntemler (Öznitelik ve Öğrenme Tabanlı)	26
2. YAPILAN ÇALIŞMALAR.....	30
2.1. Tekrarlama Sahteciliği Tespit Yöntemleri	31
2.1.1. Doku Tabanlı Tekrarlama Sahteciliği Tespiti	31
2.1.1.1. Yerel İkili Örüntü Algoritması	31
2.1.1.2. Weber Yerel Tanımlayıcı Algoritması	34
2.1.1.3. Yapısal Benzerlik Metriği	38

2.1.1.4.	Tekrarlama Sahteciliği Tespiti için Önerilen Doku Tabanlı Yaklaşım	40
2.1.2.	Kenar Algılamaya Dayalı Tekrarlama Sahteciliği Tespiti	42
2.1.2.1.	Canny Algoritması.....	43
2.1.2.2.	LoG Algoritması.....	46
2.1.2.3.	Tekrarlama Sahteciliği Tespiti İçin Önerilen Kenar Algılamaya Dayalı Yaklaşım	48
2.2.	Sıkıştırılmaya Dayanıklı Tekrarlama Sahteciliği Tespit Yöntemleri	52
2.2.1.	Frekans Düzleminde Kullanılan Teknikler.....	53
2.2.1.1.	AKD Algoritması	53
2.2.1.2.	ADD Algoritması	55
2.2.1.3.	Frekans Düzlemine Dayalı Önerilen Yöntem	56
2.3.	Çerçeveler Arası Tüm Sahteciliklerin Tespit Yöntemi	62
2.3.1.	Silme Sahteciliği Tespiti.....	63
2.3.1.1.	Tepe Sinyal Gürültü Oranı	64
2.3.1.2.	TSGO' ya Dayalı Silme Sahteciliği Tespit Yöntemi.....	65
2.3.2.	Çerçeveler Arası Dört Tür Sahtecilik Tespit Yöntemi	67
2.3.2.1.	Piramitsel Yönlendirilmiş Gradyanlar Histogramı Algoritması.....	67
2.3.2.2.	Çerçeveler Arası Dört Sahteciliğe Çözüm Sunulan Yaklaşım	70
3.	BULGULAR VE İRDELEME	85
3.1.	Kullanılan Veri Setleri.....	85
3.2.	Kullanılan Performans Değerlendirme Ölçütleri.....	87
3.3.	Gerçekleştirilen Yöntemlerin Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar	88
3.3.1.	Tekrarlama Sahteciliği Tespiti İçin Önerilen Doku Tabanlı Yaklaşım Sonuçları.....	89
3.3.2.	Tekrarlama Sahteciliği Tespiti için Önerilen Kenar Algılamaya Dayalı Yaklaşım Sonuçları	94
3.3.3.	Sıkıştırılmış Videolarda Frekans Düzlemine Dayalı Tekrarlama Sahteciliği Tespit Sonuçları.....	99
3.3.4.	Çerçeveler Arası Sahteciliklere Çözüm Sunmak İçin Önerilen Çalışma Sonuçları.....	112
3.3.4.1.	Silme Sahteciliği Tespit Yöntemi Sonuçları	112
3.3.4.2.	Silme, Tekrarlama, Ekleme ve Karma Olmak Üzere Çerçeveler Arası Sahteciliklerin Tespitine Yönelik Önerilen Çalışma Sonuçları	116

3.4.	Tez Kapsamında Önerilen Yöntemlerin Karşılaştırılması.....	124
4.	TARTIŞMA VE SONUÇLAR.....	126
5.	ÖNERİLER	128
6.	KAYNAKLAR.....	130
ÖZGEÇMİŞ		



Doktora Tezi

ÖZET

VIDEOLARDA ÇERÇEVELER ARASI SAHTECİLİKLERİN TESPİTİ

Işıl BOZKURT

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Güzin ULUTAŞ
2023, 143 Sayfa

Bir olay ya da nesneyi gizlemek veya video akışını değiştirerek izleyeni yanıltmak için video sahtecilikleri yapılmaktadır. Video sahtecilikleri içerisinde, çerçeveler arası sahtecilik türleri en sık kullanılan sahtecilik türlerindendir. Tez kapsamında videolarda gerçekleştirilen çerçeveler arası sahteciliklerinin tespitine yönelik problemler araştırılmış ve çözümüne yönelik yeni yöntemler önerilmiştir. Çalışmalar hem mevcut olan hem de tez kapsamında oluşturulan yeni veri tabanı üzerinden denenerek test edilmiştir. Literatürde sıkça kullanılan ortak veri tabanları ve özel olarak hazırlanan gerçekçi video örnekleri kullanılmıştır. İlk olarak doku ve kenar algılamaya dayalı yöntemler ile tekrarlama sahteciliği, sıkıştırılmamış videolar üzerinden tespit edilmiştir. İkinci olarak sıkıştırılmış videolarda çalışabilen tekrarlama sahteciliğinin tespitine yönelik frekans tabanlı bir yaklaşım önerilmiştir. Önerilen yöntem bulanıklaştırma ataklarına karşı test edilmiş başarılı sonuçlar alınmıştır. Üçüncü olarak birden fazla sahteciliğin tespitine yönelik yaklaşımlar önerilmiştir. Bu amaçla silme sahteciliğinin tespiti için benzerlik tabanlı ve çerçeveler arası tüm sahteciliklerin çözümü için hibrit tabanlı yaklaşım tasarlanmıştır. Hibrit çalışma sıkıştırma ataklarına karşı dayanıklı hale getirilmiştir.

Anahtar Kelimeler: Video sahteciliği tespiti, Pasif sahtecilik tespiti, Çerçeveler arası sahteciliklerin tespiti.

PhD. Thesis

SUMMARY

DETECTION OF INTER-FRAME FORGERIES IN VIDEOS

Işıl BOZKURT

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Assoc. Prof. Güzin ULUTAŞ
2023, 143 Pages

Video forgeries are used to hide an event or object, or to mislead the viewer by altering the flow of the video. Among video forgeries, inter-frame forgeries are among the most common types of forgeries. In this thesis, the problems of detecting inter-frame forgeries in videos are investigated and new methods are proposed to solve them. The studies were tested on both the existing database and the new database created within the scope of the thesis. Common databases commonly used in the literature and specially prepared realistic video examples were used. Firstly, texture and edge detection methods are used to detect repetition forgery in uncompressed videos. Secondly, we propose a frequency-based approach to detect duplication forgery that works on compressed videos. The proposed method was tested against blurring attacks and successful results were obtained. Thirdly, approaches to detect multiple forgeries have been proposed. For this purpose, we designed a similarity-based approach for the detection of deletion forgery and a hybrid approach for the resolution of all inter-frame forgeries Hybrid operation is made resistant to compression attacks.

Key Words: Video Forgery Detection, Passive Forgery Detection, Interframe Forgery Detection.

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1. 1.	Çerçeveler arası sahtecilik örneği (a) Orjinal video çerçeveleri (b) Tekrarlama sahteciliği yapılmış video çerçeveleri (c) Karma sahteciliği yapılmış video çerçeveleri.....	4
Şekil 1. 2.	Basında çıkan dezenformasyon haberleri (a) [13] (b) [14].....	5
Şekil 1. 3.	(a) Orjinal video çerçeveleri (b) Derin sahte uygulaması kullanılarak yapılmış sahte video çerçeveleri.....	6
Şekil 1. 4.	(a) Orijinal video çerçeve dizisi, (b) Silinen F7, F8, F9 video çerçeve dizisi, (c) Eklenen F6, F7, F8 video çerçeve dizisi, (d) Tekrarlanan F1=F7, F2=F8, F3=F9 video çerçeve dizisi, (e) Karılan F1=F9, F2=F8, F3=F7 video çerçeve dizisini göstermektedir	10
Şekil 1. 5.	Pasif sahtecilik tespit tekniklerinin sınıflandırılması.....	15
Şekil 2. 1.	Komşuluk değerlerine göre merkez piksel etiketinin atanması.....	32
Şekil 2. 2.	Video_34'e ait YİÖ öznelilik histogramlarının hata kareleri farkının gösterilmesi (a) Video-34 132. çerçeveye ait görsel (b) Video-34 434. çerçeveye ait görsel (c) Video çerçevelerinin hata kareleri farkı	33
Şekil 2. 3.	Weber algoritması filtreleri (a) DU hesabında kullanılan filtreler (b) YO' nun hesaplanması için kullanılan filtreler.....	34
Şekil 2. 4.	(a)VTL veri tabanından Akiyo videosunun 10 numaralı çerçevesi (b) Çerçeveye ait gri görüntü (c) Vs00 görüntüsü (d) Vs01 görüntüsü (e) Vs10 görüntüsü (f) Vs11görüntüsü	35
Şekil 2. 5.	WYT histogramının oluşturulması (a) Akiyo 10. çerçeveye ait DU histogramı (b) Akiyo 10. çerçeveye ait YO histogramı (c) Akiyo 10. çerçeveye ait WYT histogramı	36
Şekil 2. 6.	WYT algoritması hata kareleri farkı (a) 10 numaralı çerçeve (b) 220 numaralı çerçeve (c) WYT algoritması öznelilikleri hata kareleri farkı.....	38
Şekil 2. 7.	Web_Test veri tabanından alınan video çerçeve örneklerinin YBM kıyaslamalarının gösterimi (a) Beş_hırsız videosundan alınan 1. çerçevenin (b) Beş_hırsız videosundan alınan 1499. çerçevenin (c)Sakin_hırsız videosundan alınan 1650. çerçevenin görselleri	39
Şekil 2. 8.	Önerilen yöntemin genel blok diyagramı	41

Şekil 2. 9.	(a) YİÖ ile çıkarılan öznitelik histogramı (b) WYT ile çıkarılan öznitelik histogramı (c) YİÖ ile tespit edilen çerçevelerin ikili gösterimi (d) WYT ile tespit edilen çerçevelerin ikili gösterimi.....	42
Şekil 2. 10.	Canny algoritmasının uygulama adımları (a) 170. çerçeveye ait görsel (b) Gauss filtresinden geçirilen görüntünün çıktısı (c) x filtresi konvolüsyon sonucu (d) y filtresi konvolüsyon sonucu (e) Maksimum olmayan noktaların bastırılması sonrası (f) Eşik uygulaması sonrası	45
Şekil 2. 11.	Laplasyan filtresi için kullanılabilecek iki farklı matris	46
Şekil 2. 12.	LoG filtresi	47
Şekil 2. 13.	LoG algoritması ile (a) 0.1 (b) 0.3 (c) 0.5 standart sapma değerleri için elde edilen görseller.....	47
Şekil 2. 14.	Kenar algılamaya dayalı algoritmanın genel adımları.....	49
Şekil 2. 15.	V25 için alınan; (a) YCbCr renk uzayından Y renk kanalına ait görsel, (b) Görsele ait Canny algoritması uygulanmış görüntüsü, (c) LoG filtresinden geçirilmiş görüntüsü, (d) Canny ve LoG filtresinin birlikte uygulandığı çıktı görüntüleri.....	50
Şekil 2. 16.	(a) Korelasyon fark görüntüsü, (b) üst üçgensel matrisi	52
Şekil 2. 17.	8x8'lik blok üzerinden AKD frekansları ve zigzag tarama	54
Şekil 2. 18.	(a) Orijinal görüntü (b) AKD uygulanan görüntü	55
Şekil 2. 19.	Veri tabanından alınan gri bir görüntüye ait ADD dönüşümün görsel sonuçları.....	56
Şekil 2. 20.	Frekans düzlemine dayalı tekrarlama sahteciliği tespit çalışması genel adımları	57
Şekil 2. 21.	Renkli görüntülerin gri seviyeye dönüştürülmesi ve bloklara ayrılması	58
Şekil 2. 22.	x ve y yönünde uygulanan Prewitt algoritması filtreleri	59
Şekil 2. 23.	Ayırt edici özniteliklerin görselleştirilmesi (a) Elde edilen "M " görüntüsü (b) Prewitt' li ikili görüntü (c) Prewitt Algoritması sonrasında elde edilen kenar çizgileri.....	59
Şekil 2. 24.	Öznitelik görüntüsündeki 1 değerli piksellerin histogramı	60
Şekil 2. 25.	Yapıştırılma konumunun tespiti için otomatik eşik belirleme.....	60
Şekil 2. 26.	Gruplar arasındaki ilişkinin korelasyonları incelenerek değerlendirilmesi	61

Şekil 2. 27.	Sahteciliğe aday çerçeveler içerisinde yanlış pozitiflerin elenmesi 62
Şekil 2. 28.	SULFA veri tabanından alınan video örnekleri(a) can_220_flap (1) videosu 61.çerçeve (b)can_220_flap (2) videosu 331.çerçeve (c) video18_can_220_garden (4) videosu 1.çerçeve..... 64
Şekil 2. 29.	Çerçevelere ait TSGO' larının kıyaslanması 65
Şekil 2. 30.	Silme sahteciliği tespit algoritmasının genel adımları..... 65
Şekil 2. 31.	(a) Orijinal videoya ait öznitelik gösterimi (b) Silme sahteciliği yapılan videoya ait öznitelik gösterimi..... 67
Şekil 2. 32.	PYGH algoritması ile öznitelik çıkarımı 68
Şekil 2. 33.	“(a) nik_s3000_bridge (1)” videosu çerçeve görüntüsü (b) Seviye-0 için histogram (c) Seviye-1 için histogram (d) Seviye-2 için histogram 69
Şekil 2. 34.	Çerçeveler arası sahtecilik tespit yönteminin adımları..... 71
Şekil 2. 35.	Hibrit yöntem için sahtecilik türünün tespiti için önerilen yöntem (a) Toplam tepe sayısının araştırılması, (b) Sahtecilik türünün belirlenmesi 73
Şekil 2. 36.	Eşleşen çiftlerin sayısının bulunması 74
Şekil 2. 37.	(a) V2 videosuna ait çerçeve örneği (b)Silme sahteciliğine ait görselin öznitelik vektörü grafiği (c) V4 videosuna ait çerçeve örneği (d) Ekleme sahteciliğine ait görsel öznitelik vektörü grafiği 75
Şekil 2. 38	Ekleme sahteciliği mevcut videonun arasına yapıldığı durumda 76
Şekil 2. 39.	Ekleme sahteciliği mevcut videonun sonuna yapıldığı durumda 77
Şekil 2. 40.	İkiden fazla video art arda eklendiğinde elde edilen görseller 77
Şekil 2. 41.	Tekrarlama sahteciliğinin yapıldığı videoya ait öznitelik grafikleri (a) V18 videosuna ait çerçeve (b) Tekrarlama sahteciliği öznitelik vektörü grafiği (c) Tekrarlama sahteciliğinde eşleşen noktalara ait grafik..... 78
Şekil 2. 42.	Karma sahteciliği örneği (a) V16 videosuna ait çerçeve (b) Karma sahteciliğine ait öznitelik vektörü grafiği (c) Karma sahteciliğinde eşleşen çerçeveler 79
Şekil 2. 43.	Tekrarlama sahteciliği videonun sonunda yapıldığında oluşturulan öznitelik vektörü grafikleri (a) Akiyo videosuna ait görsel (b) 1. çerçeve ile diğer çerçevelerin YBM kıyaslaması sinyal grafiği (c) Ardışık çerçevelerin özniteliklerinin YBM ile kıyaslanması 81

Şekil 2. 44.	Tekrarlama sahteciliği öznitelik kıyaslama görselleri	83
Şekil 3. 1.	Web-test oluşturulurken kullanılan orijinal video çerçeve örnekleri	85
Şekil 3. 2.	Farklı kalitelerde sıkıştırılmış sahte can_220_book videosu ile sıkıştırılmamış sahte haldeki video çerçevelerinin ortalama TSGO değerlerinin grafiği	86
Şekil 3. 3.	(a) Orijinal ve (b) bulanıklaştırma atağı uygulanmış çerçeve görselleri	87
Şekil 3. 4.	Tez kapsamında çözüm sunulan problemler, çözüm yaklaşımları ve kullanılan algoritmalar	89
Şekil 3. 5.	Tez kapsamında yapılan çalışmaların kıyaslandığı çalışmalar, kullanılan veri tabanları ve pozitif üstünlükleri	91
Şekil 3. 6.	Fadl vd. önerdiği veri tabanından alınan (a) v29 ve (b) v30 ait görsel örnekler	91
Şekil 3. 7.	(a) YİÖ algoritmasına dayalı önerilen çalışmanın analiz sonuçları (b) WYT algoritmasına dayalı önerilen çalışmanın analiz sonuçları	93
Şekil 3. 8.	YİÖ- WYT kıyaslaması	93
Şekil 3. 9.	Önerilen yöntem ve doku tabanlı diğer çalışma ile kıyaslanması ...	93
Şekil 3. 10.	Kenar çıkarımına dayalı algoritmanın v29 üzerinden uygulanan görüntü çıktıları (a) Canny görüntüsü (b) LoG görüntüsü (c) Canny ve LoG' un birleştirilmiş görüntüsü (d) Elde edilen özniteliklerin korelasyon grafiği (e) Gruplar arası korelasyon değerlerinin ikili görüntüsü (f) İkili görüntünün üst üçgensel matris imgesi (g) Tekrarlanan sahte çerçeve çiftleri	95
Şekil 3. 11.	Kenar özniteliklerine dayalı tekrarlama sahteciliği tespit yöntemi Fadl vd.' nin veri tabanında [126] kıyaslanması	97
Şekil 3. 12.	Kenar özniteliklerine dayalı tekrarlama sahteciliği tespit yöntemi SULFA ve VTL veri tabanlarında, [175] ve önerilen çalışmaların kıyaslanması	98
Şekil 3. 13.	Orjinal can_220_book videosuna ait (a) Sıkıştırılmamış orijinal videonun, (c) Sıkıştırılmamış sahte videonun, (e) H264 crf30 kalite faktörü ile sıkıştırılmış sahte videonun (g) MPEG-4 QS21 kalite faktörü ile sıkıştırılmış sahte videonun; AKD öznitelikleri alınmış ikili M görüntüsü (b) Sıkıştırılmamış orijinal videonun, (d) Sıkıştırılmamış sahte videonun (f) H264 crf30 kalite faktörü ile sıkıştırılmış sahte videonun, (h) MPEG-4 QS21 kalite faktörü ile	

	sıkıştırılmış sahte videonun; Prewitt algoritması uygulanmış görüntüsü	100
Şekil 3. 14.	Kaynak çerçeve tespit sonuçları	102
Şekil 3. 15.	Sıkıştırılmamış sabit ve hareketli kamera ile çekim yapılan videolarda elde edilen tespit sonuçları.....	103
Şekil 3. 16.	Sıkıştırılmış sabit ve hareketli kamera ile çekim yapılan videolarda elde edilen tespit sonuçları	103
Şekil 3. 17.	(a) MPEG-4 (b) H.264 ile sıkıştırılmış videolar için farklı kalite oranlarında sıkıştırma etkisinin izlenmesi	105
Şekil 3. 18.	Sıkıştırılmış ve sıkıştırılmamış videolarla olan tespit kıyaslaması sonuçları.....	106
Şekil 3. 19.	Bulanıklaştırma ataklarına karşı elde edilen sonuçlar	107
Şekil 3. 20.	Ren vd. çalışması ile ortak veri tabanı kullanılarak tekrarlama sahteciliği tespit sonuçları	108
Şekil 3. 21.	Wei vd. çalışması ile ortak veri tabanı kullanılarak tekrarlama sahteciliği tespiti sonuçları	108
Şekil 3. 22.	Algoritması koşulan çalışmalar ile kıyaslama sonuçları	109
Şekil 3. 23.	AKD tabanlı yöntemlerin kıyaslanması	110
Şekil 3. 24.	AKD ve ADD yöntemlerinin kıyaslamalı sonuçları.....	110
Şekil 3. 25.	Önerilen yöntemin hangi açılardan incelendiğinin gösterilmesi ...	111
Şekil 3. 26.	(a) 160. çerçevede silme sahteciliği yapılan can_220_garden (1) videosunun çerçeve örneği (b) TSGO grafiği (c) TSGO' ların değişim grafiği	114
Şekil 3. 27.	Silme sahteciliğinin farklı sıkıştırma metriklerinden elde edilen sonuçları.....	115
Şekil 3. 28.	PYGH' lı çalışmanın farklı veri tabanlarından alınan sonuç kıyaslamaları.....	116
Şekil 3. 29.	Web-test veri tabanından alınan sonuçlar.....	117
Şekil 3. 30.	Web-test' teki SULFA veri tabanından alınan sonuçlar.....	118
Şekil 3. 31.	Fadl vd.' in [126] kullandığı veri tabanından alınan sonuçlar	119
Şekil 3. 32.	Ren vd.' nin [124] kullandığı veri tabanından alınan sonuçlar	119
Şekil 3. 33.	Shelke vd. kullandığı veri tabanından alınan sonuçlar	120

Şekil 3. 34.	Fadl vd.' nin önerdiği veri tabanından elde edilen sahtecilik tespit sonuçları.....	121
Şekil 3. 35.	Fadl vd. çalışması ile üç tür sahteciliğin kıyaslama sonuçları.....	121
Şekil 3. 36.	Sahtecilik türlerinin tespit başarısı	123
Şekil 3. 37.	Çerçeve düzeyinde elde edilen tekrarlama ve ekleme sonuçları ...	124



TABLÖLAR DİZİNİ

	<u>Sayfa No</u>
Tablo 1. 1. Video sahteciliği algılama alanındaki yayınların yıllara göre dağılımları.....	2
Tablo 1. 2. Kaynak olarak kullanılan veri tabanları.....	28
Tablo 1. 3. Literatürde kullanılan veri tabanları	29
Tablo 3. 1. Kenar özniteliklerine dayalı tekrarlı sahteciliği tespit yöntemi Web-test ve Fadl vd.' nin veri tabanlarında önerilen çalışmaların kıyaslanması	98
Tablo 3. 2. Farklı blok boyutlarına göre değerlendirme sonuçları.....	99
Tablo 3. 3. Farklı sıkıştırma kalitelerine göre elde edilen değerlendirme sonuçları.....	102
Tablo 3. 4. MPEG-4 ve H.264' e göre ortalama koşma süreleri	106
Tablo 3. 5. Kıyaslanan çalışmaların ortalama koşma süreleri	109
Tablo 3. 6. Wei vd.' nin önerdiği veri tabanına göre kıyaslama sonuçları.....	113
Tablo 3. 7. Önerilen çalışma ile Fadl vd. 'nin çalışmasının karma sahteciliği tespit sonuçları	122
Tablo 3. 8. Tez kapsamında yapılan çalışmaların kıyaslaması	125

SEMBOLLER DİZİNİ

ADD	Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform- DWT)
AKD	Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform- DCT)
BTESA	Bölge Tabanlı Evrişimli Sinir Ağı (Region-Based Convolutional Neural Network-RCNN)
ÇKA	Çok Katmanlı Algılayıcı (Multilayer Perceptron- MLP)
ÇÜA	Çekişmeli Üretici Ağ (Generative Adversarial Network-GAN)
DAA	Doğrusal Ayırma Analizi (Linear Discriminant Analysis-LDA)
DE	Diferansiyel Uyarım (Differential Excitation)
DN	Doğru Negatif (True Negative-TN)
DO	Doğruluk Oranı (Detection Accuracy-DA)
DP	Doğru Pozitif (True Positive-TP)
DU	Duyarlılık (Recall-RR)
ESA	Evrişimli Sinir Ağı (Convolutional Neural Network-CNN)
FÇG	Foton Çekim Gürültüsü (Photon Shot Noise-PSN)
FTD	Foto-Tepki Düzensizliği (Photo-Response Non- Uniformity-PRNU)
GO	Gradyan Oryantasyonu (Gradient Orientation)
GP	Gradyan Piramidi (Gradient Pyramid)
GSEM	Gri Seviye Eş Oluşum Matrisi (Gray Level Co_occurence Matrix)
GSF	Gürültü Seviyesi Fonksiyonu (Noise Level Function-NLF)
HDKO	Hareket Dengelemeli Kenar Oluşumu (Motion Compensated Edge Artifact-MCEA)
HH	Yüksek-Yüksek Alt bant (High-High Subband)
HL	Yüksek-Alçak Alt bant (High-Low Subband)
IFCN	Uluslararası Doğruluk Kontrol Ağı (International Fast- Checking Network)
IVY Lab	Görüntü ve Video Sistem Laboratuvarı (Image and Video systems Lab)
KE	Keskinlik (Precision-PR)
KEYK	K-En Yakın Komşuluk (K- Nearest Neighbour-KNN)
KYM	Kırmızı Yeşil Mavi (Red Green Blue-RGB)

	LASIASTA-Segmentasyon Algoritmalarının İntegral Değerlendirilmesi için Etiketli ve Açıklamalı Diziler (Labeled and Annotated Sequences for Integral Evaluation of Segmentation Algorithms)
LH	Alçak-Yüksek Alt bant (Low-High Subband)
LL	Alçak-Alçak Alt bant (Low-Low Subband)
LoG	Gauss' un Laplası (Laplacian of Gaussian)
LR	Lojistik Regresyon (Logistic Regression)
MFCN	Çok Amaçlı Evrişimli Sinir Ağı (Multi- task Fully Convolution Network)
OKH	Ortalama Karesel Hata (Root Mean Square Error-RMSE)
PYGH	Piramitsel Yönlendirilmiş Gradyanlar Histogramı (Pyramid of Histogram of Oriented Gradients-PHOG)
REWIND	Görsel İşitsel Verilerin- Sesin Tersine Mühendisliği (Reverse Engineering of Audio- Visual Content Data)
RFD	Renk Filtresi Dizisi (Color Filter Array-CFA)
RGY	Resim Grubu Yapısı (Group of Picture-GOP)
SÖG	Sensör Örüntü Gürültüsü (Sensor Pattern Noise-SPN)
SULFA	Surrey Üniversitesi Sahtecilik Analizi Kütüphanesi (Surrey University Library for Forensic Analysis)
ŞBC	Şarj Bağlantılı Cihaz (Charged Coupled Device-CCD)
TDTVD	Uzamsal Düzlemde Kurcalanmış Video Veri Seti (Temporal Domain Tampered Video Dataset)
TSA	Tekrarlayan Sinir Ağı (Recurrent Neural Network-RNN)
TSGO	Tepe Sinyal Gürültü Oranı (Peak Signal-to-Noise Ratio-PSNR)
UKSB	Uzun-Kısa Süreli Bellek (Long Short-Term Memory-LSTM)
ÜKÖS	Üçgensel Kutuplu Özellik Sınıflandırma (Triangular Polarity Feature Classification-TPFC)
VLFD	Çerçeve Tekrarlama için Video Adli Bilişim Kütüphanesi (Video Forensics Library for Frame Duplication)
VTD	Video Tahrif Verileri (Video Tampering Data)
VTL	Video İz Kütüphanesi (Video Trace Library)
YBM	Yapı Benzerliği Metriği (Structural Similarity-SSIM)
YGH	Yönlendirilmiş Gradyanların Histogramı (Histogram of Gradients-HOG)

YİÖ	Yerel İkili Örüntü (Local Binary Pattern-LBP)
YN	Yanlış Negatif (False Negative-YN)
YOK	Yığınlanmış Otomatik Kodlayıcı (Stacked Auto Encoders-SAE)
YP	Yanlış Pozitif (False Positive-FP)



1. GENEL BİLGİLER

1.1. Giriş

Gelişen teknoloji ile çoklu ortam verileri günlük hayatta önemli bir yer edinmiştir. Bu verilerden olan videolar, yaşanmış olayların önemli canlı kanıtlarıdır. Depolama ve iletim sorunları çözülebilir hale geldikçe özellikle sosyal medya uygulamalarında veya güvenlik uygulamalarında kişilerin kendilerini ifade etmelerinde videoların önemini daha da artırmaktadır. Kişilerin ve firmaların toplumu yönlendirme ve bilgilendirme amacıyla bir çeşit reklam pazarı olarak kullandıkları sosyal medya uygulamaları ile haberlerin hızla yayılımı, ülkeler gibi geniş kitlelerin kısa sürede bu haberlerden etkilenmesine ve bir panik ortamının oluşmasına neden olmaktadır [1]. Bu yüzden de bu tarz videoların güvenilir kaynaklardan alındığının ve bütünlüklerinin korunduğunun tespit edilmesi gerekmektedir.

Videolar üzerinde değişim yapılabilmesini sağlayan uygulamalar telefon kullanan herkes tarafından kolaylıkla kullanılabilir. Yapılan değişimler, videoların kullanım amacına göre önem arz etmektedir. Örneğin bir video mahkemede delil olarak kullanılacaksa veya toplumu bilgilendirecek bir haber programında gösterilecekse veya içeriği askeri ya da siyasi bir konuyu içeriyorsa bu tür videoların güvenilirliği kesinlikle kontrol edilmelidir. Elektronik bir delilin ceza yargılamasında kullanılabilmesi için doğruluğunun ve veri bütünlüğünün korunmuş olması gerekmektedir [1]. Aksi halde 5271 sayılı Türk Ceza Muhakemesi Kanuna göre delil olarak kullanılamazlar [2]. Bu bağlamda, yargıdan beklenen, çağın teknik gelişmelerini yakından izleyerek, bu gelişmeleri hukuk alanı ile birleştirerek adil bir hüküm verebilmesidir [3]. Bilgisayar bilimcilerinden beklenen ise Prof. Edmond Locard'ın "Değişim Prensibi" teoreminden de yola çıkarak, yapılan her değişim işleminin bıraktığı izleri teorik bir şekilde tespit edebilmektir [4]. Ancak örneğin bir film senaryosunun çekiminde her türlü değişim işlemi kullanılabilir, bu tür videolar sahtecilik tespiti konusunda irdelenmeyi gerektirmez [6].

Video verilerinin güvenliği literatürde, kullanıcı erişim kontrolü, görsel güvenlik sistemleri ve kullanılan video verilerinin doğrulanması olarak üç ana başlık altında incelenebilir [7]. Kullanıcı erişim kontrolü alanındaki çalışmalar videoların yetkilendirme ve kimlik doğrulama amacıyla kullanıldığı alanlar ile ilgili çalışmaları kapsamaktadır. Video verilerinin gizliliği yetkisiz kullanıcılardan korumak için yapılan çalışmalar

şifreleme yöntemleri ve veriyi koruma yöntemleri olarak görsel güvenlik altında incelenmektedir [7]. Video sahteciliklerinin tespiti alanındaki çalışmalar ise video verilerinin doğrulanması ve bütünlerinin korunması üzerine yapılan çalışmalardır.

Video sahteciliklerinin tespiti son yılların popüler konularındandır. “Video forgery detection” (Video sahtecilik tespiti) anahtar kelimeleri ile taranan sonuçlar dikkate alındığında Tablo 1.1.’ de elde edilen yayın sıralamasının yıllara göre dağılımı gösterilmiştir. Burada 2022 yılı içerisindeki 59 makalenin 37 makalesi öğrenme tabanlı çalışmaların kapsamında yer almaktadır. İkinci satır boyunca yapılan çalışmalar öğrenme tabanlı çalışmaların sayısını göstermektedir. Bu sıralama yapılırken önde gelen veri tabanlarından olan Scopus’un taradığı, Springer, IEEE Xplore, ACM Digital Library veri tabanlarının altında, yayın kalitesi yüksek makalelerin dağılımı verilmiştir [8].

Tablo 1. 1. Video sahteciliği algılama alanındaki yayınların yıllara göre dağılımları

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
1	2	3	5	3	4	3	15	17	19	21	34	36	59
-	-	-	-	-	-	-	1	1	1	3	11	16	37

Videolar çerçeve olarak tanımladığımız görüntü dizilerinin art arda sıralanmasıyla oluşmaktadır [9]. Belli bir süre içerisinde çerçevelerin görüntülenmesi akış oluşturmaktadır. Videolarda yapılan değişimler çerçeve içlerinde yapılabildiği gibi zamansal düzlemde akış düzeyinde de yapılabilir. Literatürde yapılan sahtecilikler konumsal ve uzamsal sahtecilikler olarak tanımlanmaktadır [10]. Bazı çalışmalarda bu sahteciliklerin her ikisi birlikte kullanılarak yapılabildiği gibi derin öğrenme teknikleri ile de sahtecilik yapılabilmektedir. Genel olarak, sahtecilik yapan kişiler tarafından videoların akışının bozulmaması dikkate alınır. Video akışı videonun oynatıldığı ortama ve izleyen kişinin algılamasına göre değişmektedir. Örneğin çok yavaş hareketin olduğu videolarda saniyede 10 çerçeve (görüntü) oynatılması algıyı bozmazken, hareketin hızlı olduğu videolarda saniyede 24 çerçeve dahi yeterli olmayabilir. Sanal gerçeklik videoları düşünülürse saniyede yaklaşık 500 çerçeve olması gerekmektedir [11]. Standart olarak kabul edilen değerler örneğin sinema ortamında oynatılan bir film için 24fps iken televizyon ortamında oynatılan bir video için 29.97fps veya 25fps olabilmektedir [12]. Dolayısıyla veri tabanı oluşturulurken bu bilgi göz önünde bulundurulmalıdır.

Sahtecilik işlemlerinin tespiti için, en azından insan gözünün algılayamayacağı şekilde yapıldığı düşünülen 24-30fps aralığında kombinasyonlara bakmak gereklidir.

Kötü niyetli kişiler videolarda daha çok akış düzeyinde yani zamansal düzlemde yapılan değişimleri tercih etmektedirler. Çünkü videolarda değişim işleminin görüntü düzeyinde yani bölgesel olarak yapıldığı durumlarda, video akışını bozmamak adına yapılan bölgesel değişim tüm videoya uygulanmalıdır. Yapılan sahteciliğin, sahnelerdeki uyumunun bozulmaması için, bulanıklaştırma gibi son işlemler yapılmalıdır. Bu da çerçeve düzeyinde uğraşmaktan daha zordur [13]. Hem zaman almakta hem de uzmanlık gerektirmektedir. Videolar üzerinde yapılan sahteciliğin fark edilebilir olması, sahtecilik yapan kişiler tarafından istenmeyen bir durumdur. Çünkü fark edilmesi kanıtın direk şüpheli konumunda değerlendirilmesine neden olur. Örneğin bir hırsızlık anının kaydedildiği video senaryosunu düşünelim. Hırsızlık yapan şahıs kendisinin bulunduğu çerçeveleri kapatmak için sabit sahneli çerçevelerden kopyalama yaparak bulunduğu çerçevelerin üzerine yapıştırma işlemi gerçekleştirebilir. Bu şekilde olay yerinde hiç bulunmamış izlenimi verebilir. Şekil 1.1.' de YouTube' dan alınmış bir videonun bu senaryoya ait çerçeveler arası sahtecilikler yapılarak oluşturulmuş görüntüleri bulunmaktadır [14]. Şekil 1.1. (a)' daki orijinal videoda sahnedeki iki bayanın tavukları besleyip sonra da beslediği tavuğu heybesine koyarak sahneden uzaklaştığı görülmektedir. Şekil 1.1.(b)' de tavuğun heybeye konulduğu çerçeveler, tavuğun beslendiği sahneler ile kapatılmıştır. Bunun için 1050. ile 1155. çerçeveler arası 106 çerçeve, 1250-1355 arası 106 çerçevenin üzerine yapıştırılarak, ilgili sahnenin kapatılması sağlanmaktadır. Şekil 1.1. (c)' de sabit sahneli çerçeveleri içeren, yani bayanların sahnede hiç bulunmadığı çerçevelerden kopya yapılarak kapatma işlemi yapılabileceği gibi, bayanların bulunduğu sahneler silinerek, sahnede bayanların hiç bulunmadığı izlenimi verilerek de kapatma işlemi yapılabilir. Farklı bir senaryoda mahkemede tavuğun sahibi birden fazla tavuğunun çalındığını iddia ederek hırsızlığın yapıldığı sahneyi de çoğaltabilir. Şekil 1.1.' de çerçeveler arası sahteciliklere ilişkin senaryolardan örnekler canlandırılmıştır.

Videolar görüntülere göre işlenme zamanı bakımından fazla zaman aldığı için kullanılacak olan öznitelik çıkarım yöntemlerinin efektif olması gerekmektedir. Videolarda işlenecek olan çerçeve sayısının bilinmemesi veya yüksek olması literatürde bu alanda yapılan çalışmaların zaman bakımından kıyaslanmaları gerekliliğini de ortaya çıkarmıştır. Boyut azaltma teknikleri işlem zamanından tasarruf amacıyla kullanılsa da gerçekleşen veri kaybı ile ayırt edici öznitelik arasında dengenin sağlanması da önemlidir.



(a)



(b)



(c)

Şekil 1. 1. Çerçeveler arası sahtecilik örneği (a) Orjinal video çerçeveleri (b) Tekrarlama sahteciliği yapılmış video çerçeveleri (c) Karma sahteciliği yapılmış video çerçeveleri

Yakın zamanda korona virüs için sosyal medya da yayılan dezenformasyonlar toplumu korkutmuştur. Şekil 1.2. (a)' da toplumu korkutan haberin aslında lisede olan bir uygulamanın videosu [15], Çin'de farklı bir çetenin çökertilmesi esnasında çekilen bir video [16] olduğu ispatlanmıştır [17]. Ülkemizde bu infodeminin önüne geçmek için asılsız haberleri kanıtlayan IFCN, bağlı teyit.org gibi platformlar mevcuttur [18].



(a)



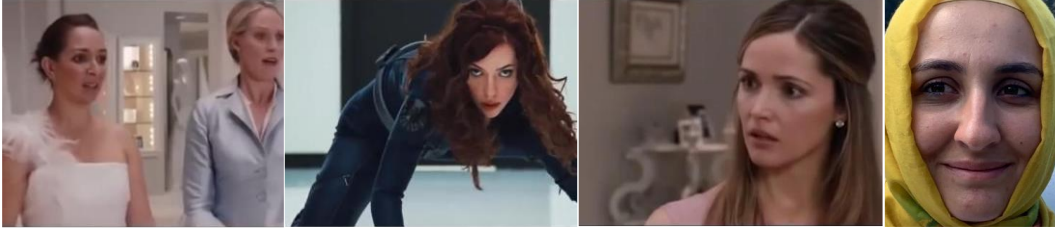
(b)

Şekil 1. 2. Basında çıkan dezenformasyon haberleri (a) [13] (b) [14]

Yine günümüzde oldukça popüler olan derin sahte yüz değiştirme algoritmalarının artışı gerek kullanıcı doğrulama sistemlerinin saptırılması gerekse yetkilendirme sistemlerinin kandırılması amacıyla kullanılabilecek birer tehdit unsurudur [19]. Şekil 1.3. (a) da orijinal görüntüleri verilen video çerçevelerinin FAKEMEAPP uygulaması ile Şekil 1.3. (b) de derin sahte ile yapılmış yüz değişim işlemi görülmektedir. Yapılan tüm video sahteciliklerin tespiti siber güvenlik altındaki sahtecilik biliminin kapsamında videoların doğrulanması gerekliliğini açıkça göstermektedir.

Videolar boyutlarının yüksek olması dolayısıyla kayıt işleminden sonra genellikle sıkıştırılarak depolanırlar. Yaygın kullanılan video sıkıştırma standartları MPEG-4, H.264'tür [20-21]. Sıkıştırma işlemlerinde kullanılan resim grubu yapısına RGY (GOP) denilmektedir [22]. Literatürde silme sahteciliğinin tespiti için önerilen çalışmalar, RGY boyutunun katları şeklinde silme işlemi yapıldığı zaman başarılı olamamaktadırlar [23-24]. Sıkıştırılma oranının artması çerçeve özniteliklerinin birbirinden farklılaşmasına, veri kaybının artmasına neden olmaktadır. Bu da tekrarlama sahteciliklerinin bulunmasını zorlaştırmaktadır.

Sahtecilik tespiti karşıtı teknikler, sahtecilik işleminin ardından yapılan değişimleri kapatmak amacıyla veya tespit tekniklerinin gerekli sürede gerçekleştirilememesi için kötü niyetli kişiler tarafından kullanılan tekniklerdir. Bu teknikler sahtecilik tespitinin yapılmasını zorlaştıran tekniklerdir [25].



(a)



(b)

Şekil 1. 3. (a) Orjinal video çerçeveleri (b) Derin sahte uygulaması kullanılarak yapılmış sahte video çerçeveleri

Literatürde bu tür saldırılar manipölasyon ve çarpıtma teknikleri, veri gizleme teknikleri, kanıt toplanmasının önlenmesi, yasal mevzuatı kullanarak kötü niyetli eşleştirme uygulamaları, adli analiz karmaşıklığının artırılması, güvenilirliği etkileyen kanıtlar ve adli yaklaşım ve araçlara saldırmak şeklinde yedi farklı yaklaşım altında sınıflandırılmışlardır [26]. Sitara vd. sunduğu bir çalışmada pasif yaklaşımların bulunmasını zorlaştırmak amacıyla sahtecilik tespiti karşıtı tekniklerden sayabileceğimiz, videolarda sahtecilik işleminden sonra, videonun çözünürlüğünün büyütülmesini tespit etmeyi amaçlamışlardır [27]. Doğal çekim sırasındaki büyütme işlemi gibi olduğunu düşündüren ve yapılan sahteciliğin aslında orijinal videoda kullanılan büyütme olmadığını tespit etmişlerdir. Farklı bir çalışmada Fadl vd. sahtecilik sonrası yapılan izlerin algılanamaması için bulanıklaştırma etkilerine karşı gerçekleştirdikleri çalışmalarını test etmişlerdir [28].

1.2. Sahte Video Oluşturma Teknikleri

Videolarda sahtecilik işleminin amacı giriş bölümünde de bahsedildiği gibi bir olayın veya nesnenin kapatılması, gizlenmesi veya birden fazla tekrarlanmış gibi gösterilmesidir.

Sahte videoların oluşturulması için videoyu oluşturan çerçeve dizilerinin arasında yani zaman eksenini boyunca ilerleyen çerçeveler üzerinde oynama yapılabileceği gibi çerçeve içerisinde yani konumsal düzlemde de kurcalamalar gerçekleştirilebilir. Bu işlemler manuel olarak yapılabildiği gibi derin öğrenme teknikleri ile de gerçekleştirilebilir. Derin öğrenme teknikleri ile oluşturulan sahte videolar, son kullanıcıya sunulan uygulamalar düşünüldüğünde, oluşturulan sahte görüntüler kadar kaliteli olmamakta dolayısıyla tam anlamıyla sahtecilik yapan kişiler tarafından sahteciliğin amacına hizmet edememektedir. Ancak derin öğrenme tekniklerinin gelişmesine bağlı olarak gelecekte bu tür sahtecilikler de istenilen başarıya ulaşacaktır. Sahte video üretme teknikleri konumsal sahtecilikler, zamansal sahtecilikler ve derin sahte video üretimi olarak sınıflandırılabilir.

1.2.1. Derin Sahte Video Üretimi

Derin sahte veriler derin öğrenme teknikleri kullanılarak oluşturulmuş gerçeğe yakın video veya görüntülerdir. Film sektörü veya sanal gerçeklik uygulamalarında önceden beri kullanılan derin öğrenme teknikleri, gereken kostüm veya sahne değişikliklerinin masraflarını aza indirmek için kullanılsalar da bu videoların kötüye kullanılma riski korkutucu boyutlarda olabilecek düzeydedir [29]. Derin sahte videoların üretiminde üç tür yaklaşım bulunmaktadır. Bunlardan ilki mevcut videoların referans kabul edilen başka videoya dönüştürülmesi işlemi yani kukla ustası tekniğidir [30]. Bu teknik ile kaynak kişinin özellikleri öğrenilerek, hedef kişinin özelliklerinin kaplaması sağlanır. Böylece hedef kişi kaynak kişinin taklidini yapmış olur. İkincisi sadece yüz ifadeleri değiştirilerek yapılan sahte kimlikli veya sahte anlamlı videolardır [31]. Üçüncüsü de videodaki ağız hareketlerini ses kaydına uydurarak dudak uyumu sağlanılmaya çalışılmaktadır [32]. Bu videoların yapımında otomatik kodlayıcılar ve çekişmeli üretici ağlar (ÇÜA) kullanılmaktadır.

Derin ağların görüntü üretebilen ilk modeli ÇÜA 2014 yılında kullanılmıştır [33]. 2018 başlarında ona OpenFace, SwapFace2Face Fake App gibi çeşitli uygulamalarda eşlik ederek ilerlemesini sağlamıştır [34]. ÇÜA alt yapısında ayırıcı (kod çözücü) ve üretici(kodlayıcı) olarak iki farklı derin ağı sahiptir [35]. Üretici derin ağı ürettiği görüntüyü, ayırıcı ağı ayırmadan diye üretilen sahte görüntü gerçek görüntü gibi ayırıcı ağı verilir. Ayırıcıdan elde edilen görüntü de yüksek hata ile üretici tarafından eğitilerek rekabetçi bir ortamda en mükemmele ulaşılması hedeflenir. Üretici girişte verilen girdinin

öznitelik haritasını çıktı olarak döndürür. Ayırıştırıcı ise üreticinin tersi yönde çalışarak, üreticiden öznitelik vektörünü alarak en yakın eşleşmeyi çıktı olarak verir. Temelde bu şekilde çalışan derin sahte ağların kiminde hedef ve kaynak görüntüler için aynı kodlayıcı kullanılmakta, çıkışta ise farklı ayırıştırıcılar ile eğitim yapılmaktadır [36]. Kiminde ise kodlayıcı ve kod çözücüler ortak; ancak ara katmanlar eklenmiştir [37]. Bir diğerinde derin öğrenmenin iki farklı kaybindan yararlanılarak farklı ağ yapıları kullanılmış ve algısal kayıp sayesinde daha doğal ve yüksek kaliteli videolar üretilmesi sağlanmıştır [38]. Kayıp fonksiyonları gerçek ve yeniden üretilen girdiler arasındaki farkı hesaplamak için kullanılmaktadır. Üretici ve ayırıştırıcılar arasındaki kaybı azaltmak için optimize edicilerde kullanılmaktadır. Tüm değişkenler farklı farklı ağlar veya optimize ediciler kullanılarak derin sahte verilerin üretilmesinde çeşitli uygulamalar gün geçtikçe çeşitlilik kazanmakta ve daha yüksek başarılar elde etmektedir.

1.2.2. Konumsal Sahtecilikler

Video çerçeveleri içerisinde yapılan sahtecilikler bu gruba dahil edilmektedir. İç boyama işlemleri ile yapılan sahtecilikler, görüntüdeki sadece nesne veya dokuların olduğu bölümlerin silinmesi, kopyalanması veya farklı videolardan nesne eklenmesi örnek olarak verilebilir [39]. Bunun dışında çerçevelerin kenar kısımlarında bulunan nesnelerin silinebilmesi için video boyutlarından kırılma yapılabilir [40]. Kırılan yerler yeniden eski video boyutlarına getirilebilir. Aynı video içerisinde bir nesnenin veya dokunun kopyalanarak videonun farklı bir yerine yapıştırılması durumunda homojen kaynak kullanılarak; iki farklı videodan birleştirme yapıldığında ise heterojen kaynaklar kullanılarak sahtecilik yapılır. Literatürde, kopyası alınan bir nesnenin yeni bir bölgeye yapıştırılması ile ekleme sahteciliği yapıldığı kabul edilmektedir. Ancak bir nesnenin veya olayın kapatılması veya gizlenmesi için bir yamanın kopyalanıp yapıştırılması ise tekrarlama sahteciliği olarak tanımlanabilir [41]. Temelde piksel ve blok düzeyinde gerçekleştirilen değişimlere rötuşlama, yeniden örnekleme, şekil değiştirme gibi işlemlerde örnek verilebilir. Yeniden örnekleme bir görüntüdeki piksel sayısının artırılması veya azaltılmasıyla görüntü örneğinin başka bir örneğe dönüştürülmesidir [42]. Yatay ve dikeyde piksellerin aynalamasının yapılması, döndürme ve ölçekleme işlemleri de yeniden örneklemenin bir parçasıdır. Rötuşlama ise görüntüde istenmeyen yerleri gidermek için

kullanılır. Yapılan sahtecilik işlemlerinin örtülmesi için kontrast artırma, bulanıklaştırma gibi işlemler yapılarak sağlanır.

Konumsal sahteciliklerde aslında görüntü sahteciliklerinde kullanılan sahtecilik teknikleri kullanılsa da video boyunca birden fazla çerçeve için aynı sahteciliğin yapılması durumu fark edilebilirliğini artırmaktadır. Dolayısıyla yapılan sahtecilikler her çerçeve için ayrı ayrı düzenlenmelidir. Hareketsiz videolara durağan bir nesnenin yerleştirildiği videolarda dahi derinlik bilgisinin kazandırılabilmesi için bir çerçeveye yerleştiren görüntü diğer çerçevelere uymayabilir. Nesneleri sahnelerle uyumunun sağlanması için kullanılan yeşil ya da mavi ekran teknikleri kullanılarak yapılan sahte video üretim tekniklerini de bu gruba dahil edebiliriz [43-47].

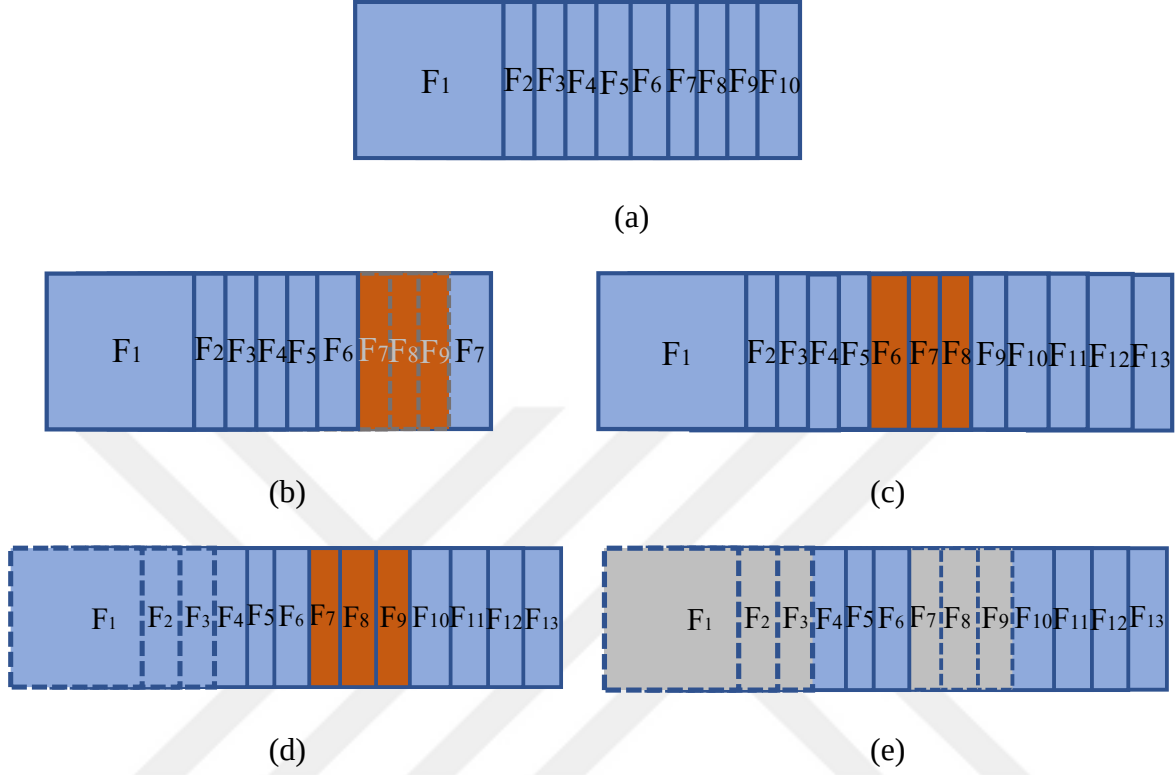
1.2.3. Zamansal Sahtecilikler

Video, zaman ekseninde çerçevelerin belli sayıda gösterilerek, görüntüye hareketlilik katılması ile oluşur. Videoları oluşturan bu görüntü dizilerinde silme, ekleme, tekrarlama veya karma yani yer değiştirme gibi işlemler yapılarak sahnedeki bir nesne veya olayın gizlenmesi veya tekrar edilmesi sağlanmaktadır [48]. Saldırganların çerçeveler arası yani zamansal sahtecilikleri yaparken kullandıkları yöntemler Şekil 1.4.' te gösterilmektedir. Bu tez kapsamında da literatürdeki boşluklarının giderilmeye çalışıldığı sahtecilikler zamansal sahteciliklerdir.

1.3. Sahtecilik Tespit Teknikleri

Videolarda yapılan sahteciliklerin doğrulanması gerekliliği günümüzün en önemli konularından biridir. Saldırganlar tarafından yapılan bozulmalar yüzünden, izlenen hiçbir şeyin doğruluğundan emin olunamadığı zamana doğru gidilmektedir. Dolayısıyla yapılan bu atakların tespiti gerekmektedir. Video sahtecilik işlemlerinin tespiti aktif ve pasif doğrulama yöntemleri ile gerçekleştirilmektedir [49]. Aktif sahtecilik yöntemleri verilerin doğrulanması için bir ön çalışma gerektirmektedir [50]. Sahtecilik tespitinin aktif yöntemlerle yapılabilmesi için videoların orijinal hallerinin de bulunması gerekliliği vardır. Her videoya uygulanması bir maliyet ortaya çıkardığından ve tüm videoların orijinal hallerinin bulunmaması nedeniyle pasif tespit tekniklerine göre daha az tercih edilirler.

Aktif sahtecilik tespit teknikleri sayısal imza ve damgalama yapılarak oluşturulmaktadır [51].



Şekil 1. 4. (a) Orijinal video çerçeve dizisi, (b) Silinen F7, F8, F9 video çerçeve dizisi, (c) Eklenen F6, F7, F8 video çerçeve dizisi, (d) Tekrarlanan F1=F7, F2=F8, F3=F9 video çerçeve dizisi, (e) Karılan F1=F9, F2=F8, F3=F7 video çerçeve dizisini göstermektedir

Aktif teknikler kimlik doğrulama, kopya kontrolü, dış müdahalelerin engellenmesi, fikri mülkiyet hakkı ve telif haklarının ihlalini engellemek amacıyla geliştirilmiştir [52].

Sayısal imza ilk olarak Diffie ile Helman tarafından oluşturulmuş sonrasında Rivest, Shamir ve Adleman tarafından şu anki haline şekillendirilmiştir [53]. Sayısal imza, imzanın oluşturulması ve doğrulanması bakımından iki aşamalıdır. İlk olarak imzalanacak olan verinin bir özet değeri oluşturulur. Bu özet değeri imza sahibinin özel anahtarı ile şifrelenerek, imzası oluşturulmuş olur. Doğrulama aşamasında ise imzayı alan taraf göndericinin açık anahtarı ile şifreyi çözerek kişi bilgisini doğrulamayı sağlar. İkinci olarak da açık anahtarla çözülen verinin tekrar özet değeri alınarak, gelen belgenin özet değeri kıyaslanır; eğer belge değişime uğramış ise özet değerleri eşleşemeyecektir, bu da belge de oynama yapıldığını, yani belgenin orijinal olmadığını göstermektedir [54]. Görüntü

sahteciliklerinin doğrulanmasında mevcut görüntü sütunlarının imzasını oluşturularak en anlamsız bitine doğrulamanın sağlanması için imza gömülür. Bu çalışma ile farklı sahtecilik türlerine karşı başarıyla tespit gerçekleştirilmiştir [55]. H264/AVC videolar üzerinde RGY uzunluğunun 10 olarak ayarlandığı videolarda, her RGY için imza oluşturularak sahtecilik tespiti gerçekleştirilmiştir [56].

Damgalama yönteminde verinin içerisine gizlenen damga, veride herhangi bir tahrifat oluşması durumunda değişikliğe uğrayarak veride oynama yapıldığını kanıtlar [57]. Damgalama yapılabilmesi için istenilen amaca ve uygulamaya göre maliyet, dayanıklılık, kapasite ve algılabirlik gibi gereksinimler vardır [58]. Bu gereksinimlerin karşılanabilmesi için oluşturulan damgalı veri ile orijinalinin aynı olduğuna dikkat edilmeli bu amaçla da damganın ekleneceği verinin kapasitesine dikkat edilmelidir. Damga işlemi için çok büyük boyutlu verilerin kullanılması hem oluşturulan damganın ortaya çıkmasına hem de maliyet açısından donanım ihtiyaçlarına neden olacaktır [59]. Donanım ihtiyacının düşürülmesi için damga boyutunun küçültülmesi de dayanıklılığını düşürecek bu da güvenliğinin ihmal edilmesine neden olacaktır [60]. Bu yüzden aktif teknikler kullanılırken kullanılan algoritmaların gereksinimleri de göz önünde bulundurularak araştırmacılar ve kullanıcılar tarafından sahtecilik tespitinde çok tercih edilmezler [61].

Pasif tespit teknikleri videoların kendi doğasından kaynaklanan istatistiksel öznitelikleri kullanır. Yapılan sahteciliğin tespiti için videoların orijinal hallerinin olmasını gerektirmez. Bu yüzden de her türlü video için uygulanabilirliği yüksek olan bu tespit teknikleri araştırmacılar tarafından da sıklıkla tercih edilir. Bu teknikler üç farklı sınıf altında incelenebilir. Bunlar derin sahte video tespit teknikleri, çerçeve içi sahtecilik tespit teknikleri, çerçeveler arası sahtecilik tespit teknikleridir.

1.3.1. Derin Sahte Video Tespit Teknikleri

Derin sahte video tespit teknikleri henüz gelişiminin başlangıç aşamasındadır. Bunun birincil nedeni olarak video veri tabanlarının henüz yeterli düzeyde olmaması [62] ikinci nedeni ise video işlemenin zaman ve donanım açısından maliyetli olması verilebilir. Bu etkenler göz önünde bulundurulduğunda derin sahte video alanında yapılan çalışmaların çoğunluğu çerçeve içlerindeki yüz manipülasyonlarının tespitini gerçekleştirmektedir. Çerçeveler arası sahteciliklerin tespitinde ise ek algoritmalar yardımıyla veya anahtar çerçeve çıkarılarak onlar üzerinden tespit gerçekleştirilmektedir.

Yüz sahteciliklerinin tespitinde önerilen yöntemler, doku tabanlı yöntemler, yüz bölümlerinin hareketine dayalı; göz kırpma hareketlerinin sıklığı [63-65], dudak hareketi [66] gibi yöntemler ve son olarak da aydınlatma ve gürültü kalitesine dayalı yöntemler olarak üç sınıf altında incelenebilir [67].

Koopman vd., derin sahte videoları ayırmak için FTD tabanlı, videolardan çıkarılan yüzlerin gruplandırılarak ortalama normalize edilmiş çapraz korelasyonu ile bir yöntem önermişlerdir [68]. Afchar vd., MesoNet ağını önererek videolarda gerçekleştirilen dudak hareketi ve yüz değişim derin sahte videolarına çözüm sunmayı hedeflenmişlerdir [69]. Suratkar ve Kazi öncelikle videolardan yüzleri algılamış ve sonrasında bu yüzleri transfer öğrenmeye dayalı yaklaşımları kullanarak eğitime tabi tutmuştur [70]. Çalışmalarını dört farklı veri setinde test ederek sonuçlarını rapor etmiştir. Guera vd. çerçeve düzeyinde ESA ile öznitelik çıkararak bu öznitelikleri TSA vermiştir. Yüz değişim sahteciliklerini tespit eden çalışma 600 video üzerinden test edilerek başarılı sonuçlar elde edilmiştir [71]. Amerini vd. videoların sahte ve orijinal olduğuna karar vermek için çerçevelerin optik akış özniteliklerini çıkararak bunları ESA ağına vermiştir [72]. Verde ve ark. birbirinden farklı iki videonun zamansal düzlemde birleştirilmesinin algılanmasına yönelik farklı kodex yapılarına sahip videoların algılanması için ESA ile eğitim yapmıştır [73]. Pessoa ve ark yine kodex türünün belirlenmesi için ESA tabanlı nicel bir yaklaşım sunmuştur. Geçmiş çalışmalardan farklı olarak ham olarak kodlanmış tüm bit akışını girdi olarak kabul edip herhangi bir piksel verisinin kodunu çözmeden sınıflandırma sağlamışlardır [74]. Vinolin ve Sucharitha DCT ve Öklid uzaklığını kullanarak anahtar çerçeveleri çıkarmış ve anahtar çerçevelerden Viola Jones algoritması ile yüz tespitini gerçekleştirmiştir [75]. Sonrasında 3B etkisi ile doku özniteliklerini kullanarak ışık etsini incelemiş ve bunlar arasındaki uzaklıkları derin ESA ağına girdi olarak vermiştir. Yöntem anahtar çerçeve çıkarma yaklaşımı ile derin sahtecilik tespit yöntemlerini kullanarak videoların sahte olup olmadığına karar vermektedir. Long vd. ise çerçeveler arası silme ve tekrarlama sahteciliğini daha önce Chengjiang'ın 3B evrişim [76] ağını kullanarak silme sahteciliğine çözüm sunduğu çalışmayı baz alarak yeni bir yaklaşım sunmuşlardır [77]. Ağdan alınan çıktı puanlarını güven puanı olarak kullanıp bir tepe saptama adımı belirlemiş ve çıktı puanı eğrilerine dayalı bir ölçek terimi olarak kullanmışlardır. Tekrarlama sahteciliği için de i3D modelini kullanarak eşleşmeleri tespit etmişlerdir.

Derin video tespit tekniklerine olan ilgi veri sayısı artıkça her geçen gün daha da popülerleşmektedir. Günümüzde kullanılan teknikler ile henüz gerçek yaşamda

kullanılabilecek uzunlukta derin sahte videoları üretmek, donanım kalitesi yüksekliği ve süre uzunluğu bakımından işlenme zorluğu olduğu için kısa süreli veri tabanları üzerinden çalışmalar gerçekleştirilmektedir. Derin sahte videoların doğrulanması gelecekte önemli konulardan biri olsa da şimdilik yapılan ataklar göz önünde bulundurulduğunda çerçeve içi ve çerçeveler arası sahteciliklerin tespiti popülerliğini korumaktadır.

1.3.2. Çerçeve İçi Sahtecilik Tespit Teknikleri

Videolar çerçeve olarak adlandırdığımız görüntü dizilerinden oluşmaktadır. Çerçeve içi sahtecilikler; çerçeve içerisine bir nesnenin eklenmesi, çerçeveden bir nesnenin kaldırılarak iç boyama teknikleri ile yerinin doldurulması [78] veya iki görüntünün birleştirilerek oluşturulması şeklinde sınıflandırılabilir. Ekleme sahteciliklerinde kaynak videodan alınan görüntü ile yapıştırılan yani hedef videonun arka planı arasındaki tutarsız bilgiler sahtecilik tespiti için kullanılmaktadır. Literatürde ekleme sahteciliklerinin etkin bulunması için çeşitli teknikler önerilmiştir. Konumsal ve zamansal blok korelasyonu [79], çerçeve değişim algılayıcısı [80], TSA [81] ve ESA [82] kullanılarak önerilen yöntemler bunlardan bazılarıdır.

Sahtekâr kişilerin izleyeni yanıltmak amacıyla konumsal sahtecilikleri kullanarak oluşturduğu bu tarz sahte videolar, çoklu ortam düzenleme yazılımları ile kolayca yapılamaz. Bu yüzden de çerçeveler arası sahteciliklere göre daha az tercih edilirler. Yapılan tespit teknikleri genellikle kaba kuvvet teknikleri, blok tabanlı ve anahtar noktası tabanlı yöntemler ile çözülmektedir. Kaba kuvvet teknikleri; kapsamlı ve otokorelasyon teknikleri olarak incelenmektedir [83]. Bu tekniklerde dairesel bir pencerenin kaydırılması ile kapsamlı arama yapılırken, konum değişikliği tespiti için seri şekilde korelasyon bilgisine bakılarak tespit gerçekleştirilir. Blok tabanlı yöntemler de çerçeveler örtüşen veya örtüşmeyen bloklara ayrılarak görüntü öznitelikleri çıkarılır ve bu özniteliklerin kıyaslaması yapılır. Anahtar noktası tabanlı teknikler ise çerçevelerden çıkarılan yerel öznitelikleri (kenar, köşe noktaları ... gibi), tanımlayıcılar ile ifade etmektedir. Sonrasında bu tanımlayıcıları benzer öznitelikleri bulmak için sınıflandırıp karşılaştırmaktadır.

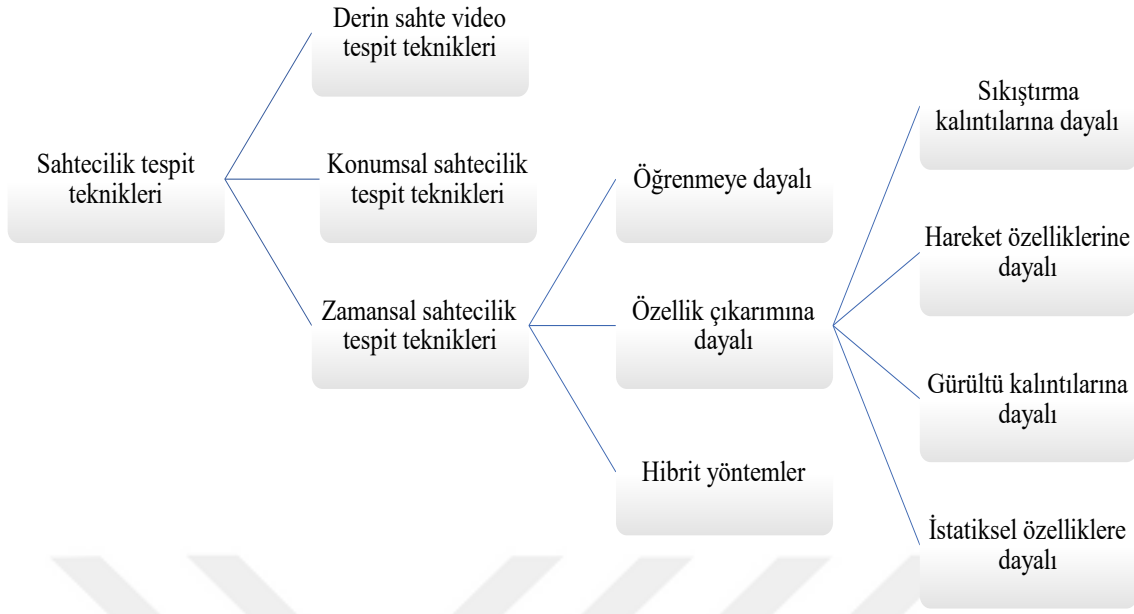
Literatürde yapılan çerçeve içi sahtecilik tespit teknikleri genelde hem konumsal hem de zamansal boyutta yapılan sahteciliklerin tespitine yönelik çalışmaları kapsamaktadır. Bu alanda yapılan çalışmaların öncüsü sayılan Wang vd. yapmış olduğu çalışma ilk olarak çerçeve içerisinde örtüşen blokların korelasyonuna, sonrasında da gruplandırılan çerçeveler

arası korelasyona bakarak tekrarlama sahteciliğine çözüm sunmayı hedeflemiştir [84]. Bu çalışmayı referans alan Lin vd. korelasyon ilişkisini incelerken renk bilgisinden faydalanmışlardır [85]. Singh vd. anomali noktalarını hesabına dayalı hem çerçeveler arası hem de çerçeve içi sahteciliklerin tespitini gerçekleştirmişlerdir [86].

1.3.3. Çerçeveler Arası Sahtecilik Tespit Teknikleri

Çerçeveler arası sahtecilik tespit teknikleri bu tez kapsamında dört tür sahteciliğe çözüm bulmayı amaçlayan zamansal boyutta yapılan sahteciliklerin tespitini gerçekleştirmektedir. Kullanılan yöntemlerin algoritmik farkları göz önünde bulundurulduğunda bu alanda yapılan çalışmalar üç farklı sınıf altında incelenebilir. Bunlar öznitelik çıkarımına dayalı tespit teknikleri, öğrenmeye dayalı tespit teknikleri ve hibrit yöntemlerdir. Şekil 1.5. bu sınıflandırmaların şematik olarak gösterimini yapmaktadır. Öznitelik çıkarımına dayalı tespit tekniklerini de kullanılan algoritmaların farklılıklarına göre dört sınıfa ayırabiliriz. Bu yöntemlerin avantaj ve dezavantajları ilerleyen bölümlerde detaylı olarak anlatılmaktadır.

Çerçeveler arası sahtecilik tespit tekniklerini zamansal, çerçeve içi sahtecilik tespit tekniklerini de konumsal sahtecilik tespit teknikleri olarak adlandırabiliriz. Genel olarak bakıldığında pasif sahtecilik tespit tekniklerinin uygulanması için ön işleme, öznitelik çıkarımı, öznitelik kıyaslaması ve sahteciliğin tespiti, son olarak da mevcut sahteciliğin türünün belirlenmesi ve konumlandırılması aşamalarından geçirmekteyiz. Ön işleme ile gerek olmadığı düşünülen verilerin kaldırılması ve kullanılacak öznitelik algoritmalarının dayanıklılığının artırılması hedeflenir. Öznitelik çıkarımı için KYM renk uzayı yerine gri renk uzayının kullanılması, video çerçevelerinin tamamı yerine bloklara ayrılarak ilgili blokların kullanılması veya her çerçevelerden tek tek öznitelik çıkarmak yerine grupta yapılarak öznitelik çıkarılması ön işleme adımlarına örnek olarak verilebilir. İkinci aşamada sahteciliği başarıyla tespit edebilecek ve işlenen her çerçeve için ayırt edicilik sağlayan öznitelik koleksiyonları çıkarılır. Bazı çalışmalarda kullanılan özniteliklerin, tespit etkisini düşürmeyecek şekilde optimize edilmesi gerçekleştirilir. Burada amaç işlem süresinden kazanç elde etmek için öznitelik boyutunu düşürmektir. Üçüncü aşamada çıkarılan özniteliklerin çeşitli teknikler ile sahte ya da orijinal olduğunun belirlenebilmesi için kıyaslamasının yapılmasıdır.



Şekil 1. 5. Pasif sahtecilik tespit tekniklerinin sınıflandırılması

Kıyaslama sırasında uzaklık metrikleri, kalite metrikleri, benzerlik analizleri, sınıflandırma veya kümeleme teknikleri gibi teknikler kullanılmaktadır. Dördüncü aşama olan son aşamada da sahteciliğin hangi tür sahtecilik olduğu belirlenmekte ve yapılan sahteciliğin konumunun tam olarak bulunması sağlanmaktadır.

1.3.3.1. Öznitelik Çıkarımına Dayalı Tespit Teknikleri

Öznitelik çıkarımına dayalı sahtecilik tespit teknikleri araştırılan videoları sahte kabul etmektedir. Test edilen videoların sahte olup olmadıkları, bu değerlendirmeye bağlı olarak çerçeve düzeyinde gerçekleştirilmektedir. İncelenen videolarda herhangi bir ize rastlanılmadıysa videolara orijinal denilmekte ancak yapılan çalışmalarda bununla ilgili doğruluk oranı belirtilmemektedir. İlgili çerçevelerde komşuluk ilişkileri incelenerek şüpheli alanların tespit edilmesi ise videonun sahte olarak tanımlanmasını sağlamaktadır. Öznitelik çıkarımına dayalı tespit teknikleri de kendi içerisinde; sıkıştırma kalıntılarına dayalı tespit teknikleri, gürültü kalıntılarına dayalı tespit teknikleri, hareket özniteliklerine dayalı tespit teknikleri ve istatistiksel özniteliklere dayalı tespit teknikleri olarak sınıflandırılmaktadır.

1.3.3.1.1. Sıkıştırma Kalıntılarına Dayalı Tespit Teknikleri

Videolar depolama ve iletim işlemleri için genellikle sıkıştırılarak kullanılırlar. Dolayısıyla sahtecilik yapacak kişi ilk olarak sıkıştırılmış videonun kodunu çözecek ve ardından sahtecilik yapacaktır. Sonra da yapılan işlemin fark edilmemesi için videoyu tekrar sıkıştıracaktır. Araştırmacılar tarafından yapılan bu yeniden sıkıştırma işlemi sahtecilik tespiti için kullanılmıştır. Çünkü bir video ikinci kez sıkıştırıldığı zaman sıkıştırmada kullanılan periyodik öznitelikler, niceleme parametreleri, AKD katsayıları veya RGY öznitelikleri değişime uğrayarak tespit için izler oluşturacaktır [39].

Sıkıştırma işlemlerinde kullanılan çerçeve grubu yapısına RGY denilmektedir. RGY yapısı sabit şekilde sıralanan I (intra coded frame), B (bipredictive coded frame), P (predictive coded frame) çerçevelerinden oluşmaktadır. İkinci sıkıştırma işleminin ardından, sahtecilik yapılan çerçevelerdeki RGY yapısının tutarsızlığı yapılan sahteciliğin tespitinde sıklıkla kullanılmıştır. Bir video dizisinde videoya çerçeve düzeyinde ataklar uygulandığında araya giren veya aradan çıkan yeni çerçevelerin ikinci sıkıştırma işlemi sonrasında sıralamalarında değişiklik olur. Bu işlem sıkıştırma sonrası video içerisinde periyodik düzenin bozulmasına neden olmakta ve sahteciliğin fark edilmesini sağlamaktadır. Wang vd.'nin önerdiği ekleme ve silme sahteciliğinin tespitine yönelik çalışma bunun iyi bir örneğidir [87]. Bu tarz yöntemlerin dezavantajı RGY sayısının katları şeklinde ekleme ya da silme sahteciliği yapıldığı zaman sahtecilik tespitinin yapılamamasıdır. Wang vd. bir diğer çalışmada niceleme parametrelerindeki sapmaları kullanmışlardır [88]. Yöntem ile makro blok seviyesinde çift nicelemeyi tespit ederken ikinci sıkıştırmanın kalitesi birinci sıkıştırmanın kalitesinden yüksek olduğunda etkili bir tespit yapabilmektedir. Yöntem ayrıca yeşil ekran sahteciliklerinin tespiti için de kullanılabilir. Su vd. I çerçevelerinin AKD katsayılarının histogramına dayalı farklı türde video kodlama sistemlerinin ihtiyaçlarına cevap verebilen bir yöntem önermişlerdir [89]. Yöntem yavaş içerikli videolarda başarısız olmaktadır. Aghamaleki vd. farklı RGY yapıları ve uzunluklarını içeren videolarda ekleme ve silme sahteciliğine çözüm önerisi sunmuş ve çift sıkıştırmayı algılayabilmişlerdir [90]. P çerçevelerindeki niceleme hatalarını tespit etmek ve kalıntı hatalarını azaltmak için dalgacık tabanlı bir algoritma önermişlerdir. Yöntemin başarısı sıkıştırma oranı artıkça azalmakta ve arka planı sabit videolar için efektif olarak çalışmaktadır. Çift sıkıştırma işleminin algılanması sahteciliğin tespitinde kullanılan önemli özelliklerden biri olduğu için son yıllarda yapılan çalışmalar videoların

iki kere sıkıştırmaya tabi olup olmadığını test etmektedir. Mahfoudi vd. gerçek zamanlı videolarda AKD katsayılarının analizine dayalı 2 kere sıkıştırılmış videoların algılanmasını amaçlamaktadır [91]. AKD katsayılarının sıfır ortalamalı Laplasyan dağılımı ile kabaca tahmin edilebileceğini ve ölçek parametresinin niceleme parametresine bağlı olduğunu göstermişlerdir.

1.3.3.1.2. Gürültü Kalıntılarına Dayalı Tespit Teknikleri

Video kayıt cihazları, kayıt işlemini gerçekleştirirken birtakım (renk filtresi türü, lens türü, geri mozaikleme tekniği veya sıkıştırma parametreleri gibi) izler bırakır. Bu izler kamera kaydının yapıldığı cihazın tanımlanmasında kullanılabilir. Buradan yola çıkarak tek bir kamera tarafından kaydedilen videoların bütünlük arz edeceği düşünülerek, farklı kamera etkisinin bulunduğu videolar kurcalanmış video sınıfına dahil edilmektedir. Sahtecilik tespit işlemi, kayıt esnasında video kayıt parametreleri (tarama yapısının kullanılması veya renk kanalları gibi) ve gürültü etkilerine (desen gürültüsü veya gürültü kalıntıları gibi) göre gerçekleştirilebilir [49].

Literatürde Bayram vd. kamera kaynağının belirlenmesinde kullanılan görüntü özniteliklerini dalgacık alan istatistikleri, renk öznitelikleri ve görüntü kalitesi metrikleri olarak üç sınıfa ayırmıştır [92]. Bu teknikler benzer özelliklere sahip kameralar kullanılarak oluşturulmuş videolarda tespit gerçekleştirememektedirler. Ekleme sahteciliğinin çözümüne yönelik De vd. tüm çerçevelerin, ŞBC kamera gürültüsüne dayalı, ortalama gürültüsü hesaplayarak, ortalama gürültüden fazla olanları sahte olarak etiketlemişlerdir [93]. Mondaini vd. konumsal ve zamansal boyutta ekleme sahteciliklerine ve kopyala yapıştır sahteciliğine çözüm bulmak için sensör patern gürültüsüne dayalı bir yaklaşım önermişlerdir [94]. Yöntem sabit arka planlı sıkıştırılmamış videolar için etkin olarak çalışmaktadır. Bayram vd. videolarda tekrarlama sahteciliğinin tespiti için çeşitli ataklar altında başarılı sonuçlar üretebilen FTD tabanlı bir yöntem önermişlerdir [95]. Kobayashi vd. ekleme sahteciliklerinin tespiti için gürültü tutarsızlıklarına dayalı iki yöntem önermişlerdir. İlk çalışmada foton atış gürültüsünden (FÇG) faydalanan doğruşal gürültü seviyesi fonksiyonunu (GSF) formülize etmiştir [96]. İkinci çalışmada doğruşal olmayan GSF yardımıyla manipölasyonların tespitini gerçekleştirmişlerdir [97]. İki yöntem de tamamen gürültü özniteliklerine dayalı olduğu için ve MPEG-4 ve H.264 gibi kodex yapılarının gürültü bilgisini ortadan kaldırması sıkıştırılmış videolarda yöntemlerin

performansını düşürmüştür. Taşpınar vd. FTD tabanlı kamera kaynağının belirlenmesini engelleyen ve renkli görüntülerin yeniden boyutlandırılmasında kullanılan algoritmaya karşı kameraların yine de bir parmak izi bırakabildiği bir yöntem önermişlerdir [98]. Kamera kaynağının belirlenmesinde kullanılan bir tür parmak izi çıkarılarak eğitilen sinir ağı modelini öneren Verdoliva vd. de sahtecilik tespiti için ses izi yaklaşımını önermişlerdir [99]. Yöntem herhangi bir ince ayar yapılmamış ve sıkıştırılmamış videolar üzerinden test edilmiştir.

Gürültü olarak adlandırdığımız ve kullanılan kameranın lens ve sensörüne göre değişen görüntü oluşumu esnasında oluşan öznitelikler kamera kaynağının belirlenmesinde kullanılan önemli özniteliklerdendir. Bu öznitelikler, lenslerin üretim esnasında yüzeylerinde meydana gelen düzensizliklerden kaynaklanır. Oluşan görüntünün kamera kaynağını tespit ederken kullanılan bu özniteliklerin dışında renk filtresi dizisi (RFD) interpolasyonu ve görüntü öznitelikleri de kamera kaynağının tespitinde kullanılan algılama tekniklerine dahil edilmektedir [42]. Bu alanda yapılan çalışmaların dezavantajı sürekli gelişen teknolojik cihazların, tanımlama yapılabilmesi için sürekli incelenmesini gerektirir.

1.3.3.1.3. Hareket Özniteliklerine Dayalı Tespit Teknikleri

Hareket öznitelikleri video çerçeveleri arasındaki zamana dayalı tutarlı ilişkilere göre çıkarılan özniteliklerdir. Belirlenen bir kaynaktan alınan verilerin, sahne üzerinde bir noktadan başka noktaya kayması ve bu esnada nesnenin yer değiştirmesi, hızı veya yönünün izlenmesi hareket tespitinin kapsamına girer. Hareket özniteliklerine dayalı çalışmaların uygulanmasında; sahnenin ışık değişimleri, nesne şekillerinin tam olarak belirlenememesi, karmaşık nesne hareketleri, nesnelerin birbirini kapatması, nesnenin hızı ve ortamın yapısal bozulması (gürültü eklenmesi gibi) karşılaşılan problemleridir [100].

Literatürdeki çalışmalar incelendiğinde HDKO tabanlı yaklaşım Su vd. tarafından silme sahteciliği [101], Dong vd. tarafından ekleme ve silme sahteciliği tespiti için kullanılmıştır [102]. HDKO tekniği ile ardışık çerçeveler arasındaki korelasyon bilgisindeki tutarlılığın bozulmasına göre tespit işlemi gerçekleştirilmiştir. Bu yöntemler çerçevelerdeki silme sayısının artmasının algılama doğruluğunu da artıracak ancak yavaş hareket içeren videolarda veya sabit kameralı videolarda yöntemin etkisiz kalacağını

ortaya çıkarmışlardır. Ayrıca bu teknikler RGY sayısının katları şeklinde çalıştığında da etkisiz kalmakta sabit RGY uzunluklu videolarda çalışmaktadırlar.

Sahtecilik tespitinde kullanılan bir diğer öznelik optik akıştır [103-111]. Optik akış ardışık görüntülerdeki piksellerin yer değiştirmesi olup hareketin yönünü ve hızını belirlemede kullanılır. Hareketin tespiti için kullanılan bu tekniğin klasik yöntemlerinde takibi yapılan pikselin renginin sabit kaldığı ve düşük hızlı olduğu varsayılmaktadır [104]. Bu yüzden de sahtecilik tespiti çalışmalarında aksi durumları içeren videolar için dayanıklı bir algoritma üretmek zordur. Optik akışı kullanarak Chao vd. ekleme ve silme sahteciliğinin tespit edilmesini amaçlamışlardır [103]. Yöntem mevcut veri tabanlarını kullanarak iki veri tabanı oluşturmuş ve hareketli bir pencere oluşturarak, pencere içerisindeki ilk ve son çerçeve arasındaki fark ile ekleme sahteciliğini; bitişik çerçeve arasındaki optik akışı hesaplayarak da silme sahteciliğini tespit etmektedir. Singh ve Aggarwal optik akış tutarsızlığı ile kamera gürültüsü etkisini bir arada kullanarak videolara nesne eklenmesi ve videodan nesne çıkarılmasında kullanılan kopyala yapıştır sahteciliği tespitini gerçekleştirmişlerdir [111]. Optik akış için Horn ve Schunk metodunu ve gürültü tespiti için de Sensör Örüntü Gürültüsü ve Foto-Tepki Düzensizliğini kullanmışlardır. Yöntem sadece kopyala yapıştır sahteciliklerine çözüm sunmaktadır. İki ayrı algoritma için ayrı ayrı sonuç rapor etmişlerdir.

Bir video dizisinin ardışık çerçeveleri birbirleriyle yüksek oranda ilişkilidir. Dolayısıyla uzamsal ve zamansal alanda bu fazlalıkları optimize etmek için videolar hareket vektörlerini kullanarak yeniden kodlanır. Hareket vektörleri, bir videodaki makro blokları temsil etmek için kullanılır ve mevcut çerçeve ile referans çerçeve arasında bir ara sapma (tahminleme) sağlayan hareket kalıntısı olarak da adlandırılan iki boyutlu vektörlerdir. Kanherla vd. bu hareket vektörlerini Markov Modelleri kullanarak SVM sınıflandırıcısına vermiş ve örüntü tanıma gerçekleştirmiştir [112]. Bu şekilde iç boyama sahteciliği ile oluşturulan sahte videoların tespiti gerçekleştirilmiştir. Yöntem hareketli arka plan ve değişen uzunluklu RGY yapısına sahip videolar için uygun değildir. Zhang vd. hareket vektör piramitlerinin tutarlılığını ve varyasyon faktörünü kullanarak çerçeve silme ve tekrarlama sahteciliğine çözüm bulmaktadır [113]. Yöntem hareket vektörleri ile Gauss piramidini birleştirerek hareket vektör piramidini oluşturmuştur. Yöntem sadece sabit arka planlı videolar üzerinden testler gerçekleştirilerek tespit gerçekleştirmiştir. Yu vd. silme sahteciliğinin tespiti için videolardaki ani değişiklikleri yakalamayı hedeflemişlerdir [114]. 6 alt küme üzerinden oluşturdukları veri setlerinde farklı RGY

seviyesinde testler gerçekleştirmişlerdir. Tahmin kalıntılarındaki varyasyon büyüklüğünü ve makro blokların sayısını ölçmek için yeni bir öznitelik geliştirmişlerdir.

Bakas vd. P çerçevelerindeki anormal noktaları tespit ederek, ikinci adımda bu noktaların doğrulanması ve sahteciliğin tam yerinin saptanması ve son olarak da yapılan sahtecilik türünün tespiti için üç modülden oluşan bir yöntem önermişlerdir [115]. Yöntem anormal noktaların tespitini hareket vektörlerini kullanarak gerçekleştirir. Yöntem RGY uzunluğundan ve sıkıştırmadan etkilenmediğini deneysel sonuçlarında ifade etmiştir. Kharat vd. tekrarlama sahteciliğine yönelik I ve P çerçevelerinden çıkarılan hareket vektörlerini kullanmaktadır [116]. Hareket vektörlerini içeren hareket bloklarının görüntüsü alınmaktadır. Bu görüntülerden bir vektör oluşturularak vektördeki ani değişimler sahteciliğin yapıldığı yerleri göstermektedir. Yöntem sabit arka planlı videolarda çalışmaktadır. Bunlar dışında hareketli nesnelerin hızını kullanarak, hız alanı dizisi için blok tabanlı çapraz korelasyonu kullanan Wu vd. silme ve tekrarlama sahteciliğine yönelik yöntem geliştirmişlerdir [117]. Sitara ve Mehtre dört tür sahteciliğe hız alanını ve P çerçevelerinin tahmin izlerini kullanarak çözüm bulmayı hedeflemişlerdir [118]. Yöntem arka planı sabit olan videolar üzerinden test edilmiş ve farklı sıkıştırma kaliteleri için test edilmemiştir.

Hareket tespitinin başarılı sonuçlandırılması videolarda izlenen nesnenin hareketinde meydana gelen değişimlerin saptanmasında da ipucu olarak kullanılmıştır. Sahtecilik tespiti alanındaki çalışmalar hareket tespitinde karşılaşılan problemlerden ötürü kısıtlı kalmaktadır. Sahtecilik tespitinde; hareket kalıntıları, optik akış, hareket vektör piramitleri, hız alan yoğunluğu ve hareket dengelemeli kenar oluşumları (HDKO) kullanılan yöntemlerdir.

1.3.3.1.4. İstatistiksel Özniteliklere Dayalı Tespit Teknikleri

Video sahteciliklerinin tespitinde en sık kullanılan pasif sahtecilik türleri istatistiksel özniteliklere dayalı yöntemlerdir. Bu yöntemler çıkarılan doku tabanlı, kenar tabanlı, frekans tabanlı, moment tabanlı, anahtar noktası tabanlı ve korelasyon tabanlı istatistiksel özniteliklere dayalı tutarsızlıkların tespitini gerçekleştirmektedir.

Korelasyon tabanlı istatistiksel öznitelikleri kullanarak hem zamansal hem konumsal sahteciliklerin tespitine yönelik çözüm sunan Wang ve Farid çerçeveleri örtüşen bir şekilde gruplandırarak kaba kuvvet şeklinde sahtecilik tespiti yapmayı hedeflemiştir. Ancak

yöntem çok yavaş çalışmaktadır [84]. Lin vd. tekrarlama sahteciliğinin tespit etmeyi amaçlamıştır. Bunun için öncelikle KYM renk uzayındaki iki bitişik çerçevenin histogram farkını özellik olarak kabul etmişlerdir [85]. Sonrasında zamansal ve konumsal korelasyon ilişkisine göre tespit işlemini gerçekleştirmişlerdir. Singh vd. her çerçeveyi dörde bölerek elde ettiği alt bloklardan dokuz öznitelik çıkarmış bunları sıralayarak, Kök Ortalama Karesel Hata değerini hesaplamışlardır [121]. Şüpheli bulunan çerçeveler arasındaki korelasyon değeri ile de tekrarlama sahteciliğinin tespitini yapmışlardır. Wei vd. komşu çerçeveler arasındaki benzerliği açıklamak için korelasyon fonksiyonunun bir ölçüsü olan karşılıklı bilgiyi kullanmıştır [122]. Yöntem tekrarlama, silme ve ekleme sahteciliklerine çözüm sunmaktadır. Çerçevelerin ve çerçeve içerisinde blokların Haralick özniteliklerinin korelasyon bilgisine göre üç tür sahteciliğe çözüm sunmayı hedefleyen Bakas vd. RGY sayısının katları boyutunda yapılan sahteciliğe ve çeşitli sıkıştırma oranlarına dayanıklı bir çalışma önermişlerdir [123]. İlk adımda silme ve ekleme sahteciliğine bakılmıştır. Her çerçevenin gri seviye eş oluşum matrisleri (GSEM) hesaplanmış ve belirlenen eşğin üzerinde olanlar orijinal çerçeve olarak kabul edilirken eşğin altında kalanlar pik sayısı bir tane ise silme iki tane ise ekleme sahteciliği var kararına varılmıştır. Eşğin altında kalan korelasyon katsayılarından eşit çiftler varsa tekrarlama sahteciliği tespit edilmiştir. Ren vd. ilk olarak video çerçevelerini örtüşen gruplara ayırır ve bu alt grupların gelişmiş Levenshtein uzaklığını hesaplar [124]. Bu uzaklık ne kadar yüksek olursa çerçeve çiftleri arasındaki benzerlik o kadar düşük olur. Alt dizilerin ölçüm mesafeleri eşit çıkarsa bu durumda da her bir alt dizinin içindeki elemanlarının ölçümü yapılır. Eğer uzaklık sıfır ise iki çerçeve birbirinin kopyasıdır. Eşik kullanılan yöntemlerde, eşik değerleri belirli koşullar için kalibre edilirken her durum için çalışmamaktadır. Bu da yöntemlerin genelleştirilmesini engeller. Dolayısıyla eşik kullanılan çalışmaların dinamik eşik olacak şekilde tasarlanması gerekmektedir.

Görüntü içerisinde kenar, piksel yoğunluğundaki değişim, nesne sınırları veya nesnelere ait gölge ve yansıma sınırları, aydınlatma değişimleri olarak tanımlanabilir. Kenar tespiti dikey ve yatay yönde uygulanan filtrelerle en kolay şekilde tespit edilir. Kenar bulma algoritmaları kullanılarak sahtecilik tespiti yapan çalışmalardan Aloraini vd. videolarda bulunan nesnelerin silme sahteciliğinin tespitine yönelik uzamsal ayrıştırma, zamansal filtreleme ve sıralı analiz kullanan bir yaklaşım önermiş sıkıştırılmış ve düşük çözünürlüklü videolara karşı da sağlamlığını göstermişlerdir [125]. Yöntem kaldırılan nesnelerin boyutu bilinmediğinden her çerçeveye Laplas piramidi uygular. Her seferinde

çerçeve boyunu yarıya indirerek minimum ölçeğe ulaşana kadar işlemi tekrarlar, böylece kenarları farklı ölçeklerde temsil eden çok ölçekli videolar oluşturur. Fadl vd. dört tür sahteciliğe çözüm sunmuşlardır [126]. Yöntem YGH algoritmasını ekleme ve silme sahteciliğinin tespitinde, hareket enerji görüntüsünü (MEI) tekrarlama ve karma sahteciliğinin tespitinde kullanmıştır. Yöntem hareket enerji görüntülerini çıkarmak için Canny kenar bulma algoritmasını kullanmaktadır.

Doku tabanlı algoritmalar seyrek alan ve yoğun alan tanımlayıcı teknikler olarak iki bölümde incelemektedir [127]. Yoğun alan tanımlayıcılar piksel düzeyinde öznitelik çıkarırken (YİÖ, LPQ, WYT, ... gibi), seyrek tanımlayıcılar ilgi noktalarını algılayarak, yerel bir örnek üzerinden değişmez öznitelikleri tanımlayan tekniklerdir (SIFT, SURF, YGH, ... gibi). Liao vd. doku öznitelikleri bakımından kontrast, bulanıklık, doğrusallık, açısallık, pürüzlülük ve büyüklük gibi değişik öznitelikleri inceleyen Tamura Özniteliklerinden faydalanılarak tekrarlama sahteciliğine çözüm sunmayı hedeflemişlerdir [128]. Çıkarılan özniteliklerden öz vektör matrisleri çıkarılmakta, komşu vektörler arasındaki değişimin hesaplanması için özvektörler sıralanmaktadır ve aralarındaki farka göre tekrarlama sahteciliğine çözüm bulunmaktadır. Tralic vd. hücrel otomata modeli ile YİÖ özniteliklerini kullanarak kopyala yapıştır sahteciliğine çözüm bulmayı hedeflemiştir [129]. Yöntem video çerçevelerini örtüşen bloklara bölerek her bloğa hücrel otomata uygular. Sonrasında YİÖ uygulayarak elde edilen ikili değerleri bir kural dizisine dönüştürülerek histogramlarından sahteciliğin tespitini gerçekleştirir. Saddique vd. kurcalanan video çerçevelerinin dokusu ve mikro desenlerinden meydana gelen tutarsızlıkları, ardışık çerçevelerin farkını alarak, sahte olup olmadıklarını ise destek vektör makineleri (DVM) kullanarak gözlemlemiştir [130]. Önerdikleri yöntem ile ardışık çerçeve farkı ve ayırt edici dayanıklı yerel ikili modeli kullanarak, segmentlere ayrılan videoların tekrarlama ve birleştirme sahteciliklerine karşı dayanıklılıkları test edilmiştir. Shelke vd. iki farklı doku tabanlı teknik kullanarak birden fazla sahteciliğe aynı videolar üzerinden tespit edebilen bir yöntem önermişlerdir [131]. Yöntem üç veri tabanından alınan videolar üzerinden test edilmiştir. Gürültüye maruz kalan videolar için önerilen yöntem dayanıklıdır. Shehnaz ve Kaur ekleme, silme ve tekrarlama sahteciliğine YİÖ histogramlarını çıkarıp bunlar arasındaki benzerliği histogram kesişme metriğine göre hesaplar [132]. Bu komşu metrik değerlerinin farklılıkları sabit uzunluklu öznitelik vektörü elde etmek, değişken uzunluklu videolar için uygulanabilir bir yöntem sunabilmek için kullanılır. Yöntem sahtecilik kararını DVM sınıflandırıcısını kullanarak gerçekleştirir.

Seyrek tanımlayıcılardan olan anahtar noktası tabanlı yöntemleri sahtecilik tespitinde kullanan birçok çalışma mevcuttur; ancak bunlardan çok azı video sahtecilikleri alanında kullanılmıştır. Bunun nedeni videolar çok sayıda görüntüden oluştuğu için öznitelik çıkarımının zaman alması ve sabit sahneli çerçevelerde ayırt ediciliğin düşük olmasından kaynaklanmaktadır. Pandey vd. konumsal düzlemde kopyala yapıştır sahteciliğinin tespiti için SIFT öznitelik çıkarım tekniğini kullanırken, zamansal düzlemde tekrarlama sahteciliğinin tespitinde gürültü kalıntısı ve korelasyonu kullanmıştır [133]. Ulutaş vd. tekrarlama sahteciliğinin çözüm bulmak için çerçevelerden çıkarılan SIFT özniteliklerini Kelime Çantası (BOW) kullanarak modellemiş ve bunlar arasındaki benzerliği Öklid uzaklığını kullanarak kıyaslamıştır [134]. Bulunan aday çerçeveler arasından TSGO değerlerine göre sahte çiftlerin tespitini gerçekleştirmişlerdir. Zhao vd. [135] üç tür sahteciliğe çözüm sunmak için HSV renk uzayına çevirdikleri çerçevelerin histogram farklarına dayalı olarak ekleme ve silme sahteciliğine çözüm bulmuşlardır. Tekrarlama sahteciliğinin tespiti için SURF ile öznitelik çıkarımı yaparak bunları FLANN algoritması ile eşleştirmiştir. Kharat vd. tekrarlama sahteciliğinin tespiti için TSS algoritması ile şüpheli çerçevelerin tespitini gerçekleştirmiş sonrasında tüm çerçevelerin SIFT ile özniteliklerini çıkarmış ve RANSAC algoritmasını kullanarak eşleşen çerçeve çiftlerini şüpheli çerçeveler arasından seçmiştir [116].

Genellikle görüntü sahteciliklerinin tespitinde kullanılan moment öznitelikleri verilerin çeşitli değişmezlik özelliklerini kullanarak tanımlanır. Video üzerinde çerçeve içerisinde yapılandırılan bölgede ölçekleme veya öteleme gibi geometrik bozulmalara karşı dayanıklılık sağlayan Zernike momentleri video sahteciliklerinin tespitinde Liu vd. tarafından öznitelik çıkarımı için kullanılmıştır [120]. Yöntem kabadan inceye doğru iki aşamalı üç tür sahteciliğe çözüm sunan bir doğrulama mekanizması sağlamaktadır. Yöntem kromatik renk uzayı üzerinden Zernike momentlerini ve Tamura kabalık doku özelliğini kullanarak aday çerçeveleri bulmuş ve sonrasında da en yakın komşuluk algoritması ile anomali noktaları üzerinden sahtecilik tespitini gerçekleştirmiştir. D'Amiano vd. videolara eklenen veya video içerisinde tekrarlanan nesnelerin tespitini gerçekleştirmek için yoğun alan doku yaklaşımı önermişlerdir [138]. Yöntem yama eşleme algoritmasının yapısında dönmeden bağımsızlık sağlayan Zernike ortonormal açısıl fonksiyonu kullanarak videolar üzerinde hızlı eşleme yapabilen bir yöntem tasarlamasını sağlamış ancak gerçek hayatta çalışabilecek kadar hızlı olmayan bir çalışma ortaya çıkarmıştır.

İstatistiksel özniteliklere dayalı tespit yöntemlerinin son sınıfı olarak adlandırılan frekans tabanlı teknikler, sahtecilik işleminden sonra videoların sıkıştırılması ile kaybedilen sahtecilik izlerinin bu izlere bağlı olmaksızın çıkarılan özniteliklerini elde etmek amacıyla kullanılan yöntemlerdir. Sıkıştırma algoritmaları, yüksek frekans bileşenlerinin atılmasını, bu işlem esnasında da sıkıştırmanın en iyi olmasını ve veriyi de en iyi şekilde temsil edebilecek düzeyde olmayı hedeflerler. Sahtecilik işlemleri yapıldıktan sonra sıkıştırma uygulandığında yüksek frekans bileşenleri kaybolur. Öyleyse çıkarılacak öznitelikler yüksek frekans bileşenlerinden çıkarılmamalıdır. Bunun için de uygulanacak yöntemler ilk olarak çerçevelerin ayrık kosinüs dönüşümü, Fourier dönüşümü veya dalgacık dönüşümü gibi tekniklerle frekans düzlemine dönüştürülmesini hedefler. Böylece kalan bileşenler sahte ve orijinal verinin ayırt ediciliği için kullanılabilir. Bu yaklaşımdan yola çıkarak Bozkurt vd. AKD tabanlı özniteliklerin ikili görüntü matrislerini çıkararak, doğru eğiminden faydalanıp, matematiksel bir yaklaşım öne sürmüşlerdir [139]. Fadl vd. sabit sahneleri temsil eden çerçeveleri seçmek ve diğerlerini elemek için artık çerçevelerin standart sapmasına ve AKD kat sayılarının entropisine dayalı öznitelik analizi yapmıştır [140]. Yöntem tekrarlama sahteciliğini hem tek çerçeve hem de alt grup düzeyinde tespit etmektedir. Singh vd. yine AKD özniteliklerinden faydalanarak hem çerçeve içi düzenli ve düzensiz sahte bölgelere, hem de çerçeveler arası sahteciliğe çözüm bulmayı hedeflemişlerdir [141]. Jin vd. AKD katsayılarının yüksek frekans bileşenlerinin periyodikliğinden faydalanarak MPEG-2 videolar üzerinden ekleme ve silme sahteciliğinin tespitini gerçekleştirmeyi hedeflemişlerdir [142].

1.3.3.2. Öğrenmeye Dayalı Tespit Teknikleri

Makine öğrenmesi, insan öğrenme şeklini taklit ederek, belirli görevler için veriler üzerinden eğitilen ve bir ağ modeline oturtulan, test verilerinin tahminlemesi, sınıflandırılması ve kümelenmesi için kullanılan bir analiz yöntemidir. Kullanılan algoritmalar karmaşık öznitelikleri otomatik olarak öğrenme yeteneğine sahiptirler. Veriye dayalı olarak analiz yapan bu yöntemlerin uygulanabilmesi için çok miktarda veriye ihtiyaç vardır. Video sahteciliklerinin tespiti alanında yeterli veri tabanlarının oluşturulamamış olması bu alanda kullanılan yöntem sayısının az olmasına neden olmuştur. Oluşturulan veri tabanlarının sayısı artıkça önerilen yöntem sayısı da artacaktır.

Bu durum, bu alanda yapılan çalışmaların kısıtlanmasına da neden olmaktadır. SVM, KEYK, LR, DDA, ÇKA literatürde kullanılan öğrenme tabanlı tekniklerdir.

Shanableh tarafından çerçeve silme sahteciliğinin tespitine yönelik tahmin artıkları, niceleme ölçekleri, makro blok yüzdesi ve TSGO değerinin tahminini kullanarak makine öğrenmesine dayalı bir yaklaşım önerilmiştir [143]. Wang vd. gri seviye korelasyon katsayılarının tutarlılık (CCCoGV) özniteliklerini çıkararak normalizasyon ve kuantalama yaptıktan sonra DVM sınıflandırıcısı ile ekleme ve silme sahteciliklerinin tespiti gerçekleştirmişlerdir [144]. Hong vd. en son kodek bileşeni HEVC ile kodlanmış videolar için silme sahteciliğinin tespitine yönelik iki bölümden oluşan bir şema önermişlerdir [145]. İlk bölümde sıkıştırma etkisine dayalı öznitelikler çıkartılmış, ikinci kısımda DDA, KEYK ve ÇKA sınıflandırıcıları kullanarak manipüle edilmiş videolardan çıkarılan özniteliklerdeki çerçeve değişikliğine odaklanmışlardır. Huang vd. ekleme ve silme sahteciliğine çözüm olarak ÜKÖS yaklaşımını kullanmışlardır. Yöntemde 3 katlamalı çapraz validasyon ile farklı veri tabanlarından aldığı sonuçları sunmuşlardır [146].

Klasik öğrenme tekniklerinin yanında kullanılan katman sayısının artması derin öğrenme yaklaşımını geliştirmiştir. Bu da araştırmacıların video sahteciliklerinin tespitinde ESA, MFCN, BTESA, TSA, UKSB, Auto Encoder, YOK gibi derin sinir ağlarının kullanılmasını da sağlamıştır. Yao vd. girdi görüntü yamalarından, yüksek boyutlu öznitelikleri otomatik olarak ESA ile çıkararak nesne tabanlı sahteciliğin tespitini hedeflemişlerdir [147]. Mevcut ESA modellerinden farklı olarak eğitim için mutlak fark, maksimum havuzlama ve yüksek geçişli filtre katmanları olarak üç ön işleme katmanından geçirilen çerçeveler kullanılmıştır. Kono vd. tarafından nesne kaldırma sahteciliğini algılamak için uzamsal ve konumsal tutarlılığa bağlı Evrişimli Uzun Kısa Süreli Bellek (ConvUKSB) modeli önerilmiştir [148]. Yöntem konumsal düzeyde ESA, zamansal düzeyde TSA kullanarak hem sabit hem hareketli videolar için başarılı sonuçlar elde etmiştir. Hong vd. iki bölümden oluşan şemalarında çerçeve sime sahteciliğine çözüm bulmayı amaçlamışlardır [149]. İlk bölümde kodlama bilgisine dayalı öznitelik çıkarılmaktadır. İkinci bölümde DDA, KEYK, ÇKA gibi sınıflandırıcıları kullanarak videonun orijinalliği test edilmiştir. Fadl vd. 2D-ESA modelini kullanarak konumsal ve uzamsal düzlemde çerçeveler arası sahteciliği tespit etmek için her bir sahneden tek bir görüntü oluşturmayı amaçlamaktadırlar [150]. Sonrasında derin öğrenme özniteliklerini üretmek için YBM bilgisinden faydalanmışlardır. Silme, ekleme ve tekrarlama sahteciliğine çözüm bulmayı hedeflemişlerdir. Derin öğrenme yaklaşımları veri odaklı

özmler olduėu iin yksek boyutlu mevcut veri tabanlarından yeni bir sahte veri tabanı oluřturmuřlardır. Ancak mevcut veri tabanı eriřim aık olarak sunulmamaktadır.

1.3.3.3. Hibrit Yntemler (znitelik ve ėrenme Tabanlı)

Yeni bir yaklařım tr olan hibrit alıřmalarda video btnlėn vurgulamak iin sadece video ieriklerinden ıkarılan znitelikler deėil, tm video dosyalarında gizli olan bilgiler de kullanılmaktadır. Videolar diske kaydedilirken kap(container) olarak adlandırılan kod özme yazılımlarını kullanmaktadırlar. Bu yazılımlar videonun ses grnt ve alt yazı gibi akıřlarını ve meta verilerini kapsamaktadır. Yang vd. nerdiėi alıřmada videoların orijinal olup olmadıėının tespitini videolarda kayıt iřlemi yapılırken kullanılan iřletim sisteminin, dzenleme uygulamasının ve kullanılan deėiřim yapılan sosyal medya platformunun belirlenmesini Karar Aėaları ile saėlamaktadır [151]. Xiang vd. MPEG-4 videolara ait en yakın komřuluk algoritmasına gre videoların sahte ya da orijinalliėinin tespiti iin yine meta verilerden elde edilen zellikleri kullanmıřlardır [152]. Altınıřık vd. da ierik analizine alternatif olarak meta verileri kullanarak sınıflandırma yapılan alıřmada kurcalamanın tespit edilebileceėini, iki seviyeli bir yntem ile gstermiřlerdir [153]. İlk seviyede meta veri aėalarının topolojik zelliklerini sınıflandırmıř ikinci seviyede kamera modelini tanımlamak iin dosya meta verilerini bir znitelik vektr ile eřleřtirmiřlerdir.

Hibrit yntemler doėrulaması yapılan videonun eřitli zniteliklerini kullanarak orijinal ve sahte olduėuna karar verirken bir hesaplama maliyeti de gerektirir. nk arařtırılan videonun mevcut tm referans kapsayıcılarla farklılıėının kontrol edilmesini gerektirir. Ayrıca yapılan sahteciliklerin lokalizasyonu iin de aıklanabilirlik saėlamazlar.

1.4. Veri Setleri

Video sahteciliklerinin tespitinde karřılařılan en nemli problemlerin bařında karřılařtırmalı deneysel analiz yapılacak kamuya aık veri setlerinin ok kısıtlı olması gelmektedir. Mevcut veri kmeleri genellikle sahtecilik iermeyen orijinal videolardan ierip, arařtırmacılar tarafından tek tip sahtecilik yapılarak kullanılmaktadırlar. Literatrde incelenen ok az veri seti hem drt tr sahteciliėi iermekte hem de aık halde

bulunmaktadır. Mevcut veri setleri genellikle sabit arka plan içeren videolardan oluşmaktadır. Veri tabanlarında kullanılan ekleme sahteciliği yapılan videolar genellikle aynı video içerisinden kopyalanan çerçevelerin, tekrar aynı video içerisine yapıştırılması ile oluşturulmaktadır. Bu şekilde toplam çerçeve sayısı artacak şekilde aslında tekrarlama sahteciliği yapılmış olunmaktadır. Ekleme sahteciliği için iki farklı videonun birleştirilmesi gerekmektedir. Literatürde istatistiksel tabanlı sahtecilik tespit yöntemlerinde kullanılan videolardan Fadl vd.'nin önerdiği çalışma [126] içerisinde kullanılan ekleme videoları iki farklı videonun birleştirilmesi ile oluşturulmuştur. Fakat içerisinde beş adet ekleme videosu bulunmaktadır.

Video sahteciliklerinin tespitinde işlem süresi önemli bir sorundur. Çünkü bir güvenlik kamerasından alınan kayıtların incelenmesi gerekliliği göz önünde bulundurulduğunda koşma süresi saatler sürebilir. Dolayısıyla önerilen yöntemlerin dayanıklılığını test edebilmek için yüksek çözünürlüklü ve video kayıt süresi uzun olan videolarda ele alınmalıdır. Ancak literatürdeki veri setleri genellikle düşük çözünürlüklü ve kısa uzunluktaki videolar için tasarlanmıştır. Mevcut veri setlerinin kasıtlı gürültü ekleme, sıkıştırma, parlaklık değişikliği gibi son işlem adımlarını içeren örnekleri genellikle çalışma yapan araştırmacılar tarafından oluşturulmakta ve erişime açık halde bulunmamaktadır. Veri seti oluşturma zaman alan bir süreç olduğu için son işlemlere dayalı test edilen yöntemlerin sayısı sınırlı kalmaktadır.

Shelke vd. üç farklı veri setini kullanarak doku tabanlı yöntemlerini test etmek için önerdikleri çalışmalarında her iki 15 video için aynı konumlarda gerçekleştirdiği sahtecilikler üzerinden doğruluk oranını hesaplamıştır [154]. Videoların 10 tanesi 320x240, 20 tanesi 640x480 çözünürlüklüdür. VLFD (Çerçeve Tekrarlama için Video Adli Bilişim Kütüphanesi) Sharma ve Kanwal tarafından Hu momentleri ile öznitelik çıkardıkları videolarda tekrarlama sahteciliğine çözüm bulabilmek bu doğrultuda da sınıflandırma yapmak için veri setini önermişlerdir [155]. Veri seti 210 videodan oluşmaktadır. Bunlardan 110 tanesi 3840x2160, 100 tanesi 1920x1080 çözünürlüklüdür. Panchal ve Shah, TDTVD (Uzamsal Düzlemde Kurcalanmış Video Veri Seti) için 40 orijinal videodan toplam 210 kurcalanmış video oluşturmuşlardır [156]. Veri tabanlarında; ekleme silme ve tekrarlama sahteciliği bulunmaktadır. Fadl vd. 2020 yılında oluşturdukları veri tabanı için 5 silme, 5 ekleme, 9 karma, 10 tekrarlama ve 3 tane de hem karma hem tekrarlama sahteciliğinin yapıldığı videolardan oluşmaktadır [126].

Araştırmacılar tarafından oluşturulan yeni veri tabanlarının birçoğu mevcut veri tabanlarının kurcalanması ile oluşturulmaktadır. Bu şekilde kullanılan bazı veri tabanları ve çözünürlükleri Tablo 1.2.' deki gibi örneklendirilmiştir;

Tablo 1. 2. Kaynak olarak kullanılan veri tabanları

Veri Tabanı İsmi	Çözünürlüğü
REWIND [157]	320x240
VTL [158]	176x144, 352x288
VTD [159]	1280x720
SULFA [160]	320x240
UCF101 [161]	-
LASIASTA [162]	288x352
VIRAT [163]	720x1280
IVY LAB [164]	576x704

SULFA sahtecilik tespiti alanında en çok kullanılan, orijinal ve sahte video içeren veri tabanıdır [160]. UCF101 insan hareketlerinin beş sınıfa ayrıldığı 101 farklı hareket içeren veri setidir. VIRAT veri seti çeşitli sahnelerde çekilmiş ve gerçekçi sahnelerden oluşan, videolardan oluşmaktadır [163].

Tablo 1.3.' de çerçeveler arası sahteciliklerin tespitinde kullanılan veri tabanları verilmiştir. Bunlar dışında sahtecilik tespiti kapsamında kamera türlerinin belirlenmesi veya çerçeve içi sahteciliklerin tespiti alanında kullanılmak üzere sunulan veri tabanları da mevcuttur.

Tez kapsamında da literatürde kullanılan veri tabanlarındaki eksiklikler göz önünde bulundurularak 20 tane SULFA veri tabanından alınan, 17 tane VTL veri tabanından iki farklı çözünürlükte alınan, 15 tane YouTube videoları kullanılarak oluşturulan toplam 69 orijinal video üzerinde değişiklikler yapılarak yeni bir veri tabanı oluşturulmuştur. Sahte çerçevelerin oluşturulmasında farklı sayılardaki ve rastgele konumlardaki çerçevelerde sahtecilik senaryosu oluşturulmuştur. Veri tabanı içerisinde farklı sıkıştırma kalite oranlarında ve farklı kodek yapılarında videolar oluşturulmuştur. Bulanıklaştırma ataklarının dayanıklılığının testi için, sahte videolar üzerinde bulanıklaştırma filtresi

uygulanmıştır. Bölüm 3.1.’ de kullanılan ve oluşturulan veri tabanlarından detaylı olarak bahsedilmektedir.

Tablo 1. 3. Literatürde kullanılan veri tabanları

Sıra	Yılı	Veri tabanı	Video sayısı	Kullanılan kaynak
1	2022	Shelke ve Kasana [154]	30-Orijinal	SULFA REWIND VTL
2	2021	Bakas [115]	43-Orijinal	VTD LASIESTA UCF101
3	2021	Fadl vd. [126]	100-Orijinal 420-Silme 287-Ekleme 62-Tekrarlama	VIRAT SULFA LASIESTA IVY LAB
4	2021	Sharma ve Kanwal [155]	200-Orijinal 200-Sahte	Kendileri oluşturdu.
5	2020	Panchal ve Shah [156]	40 Orijinal	SULFA VTD
6	2020	Fadl [126]	28-Orijinal 32-Sahte	SULFA LASIESTA IVY LAB
7	2018	Ulutaş [134]	Tekrarlama	SULFA

2. YAPILAN ÇALIŞMALAR

Videoların güvenilirliğinin sağlanması, kanıt olarak kullanılabilmesi için doğrulanmaları gerekmektedir. Doğrulama işleminin gerçekleştirilmesi için videoların orijinal hali bulunamayabilir. Son kullanıcılar tarafından kolaylıkla kullanılabilen düzenleme yazılımları ile özellikle çerçeveler arasında yapılan sahtecilikler videoların kurcalanmasını kolaylaştırmaktadır. Videolar büyük boyutlu veriler oldukları için işlem zamanı uzun sürmekte ve genellikle sıkıştırılarak depolanmaktadırlar. Dolayısıyla bu problemlere çözüm bulabilmek için tez kapsamında videoların pasif sahtecilik tespit teknikleri içerisinde, öznitelik çıkarımına dayalı istatistiksel tespit teknikleri kullanılarak doğrulanmalarının yapılması amaçlanmıştır. Bu doğrultuda yapılanlar aşağıdaki gibi sıralanmıştır;

1. İlk olarak tekrarlama sahteciliğine çözüm bulunması
2. Tekrarlama sahteciliği için önerilen çalışmanın sıkıştırmaya karşı dayanıklı hale getirilmesi
3. İkinci olarak silme sahteciliğine çözüm bulunması
4. Son olarak da çerçeveler arası tekrarlama, ekleme, silme ve karma sahteciliklerinin tamamına çözüm bulunması ve bunların son işlem ataklarına dayanıklı hale getirilmesi

Önerilen yöntemlerin işlem zamanı bakımından efektif çalışabilmesi videoların ön işleminden geçirilmesi ve kullanılan öznitelik çıkarım algoritmalarının ayırt edici ve hızlı çalışabilecek şekilde tasarlanması üzerine durulmuştur. Tespit yöntemlerinin gerçekleştirilen sıkıştırma, bulanıklaştırma gibi son işlem ataklarına karşı dayanıklı olması sağlanılmaya çalışılmıştır. Bu kapsamda da üç çalışma önerilmiştir.

Tekrarlama sahteciliğinin tespitine yönelik yapılan çalışmada doku tabanlı ve kenar tabanlı yöntemler kullanılmıştır. Doku tabanlı yöntemler ile WYT, YİÖ ve PYGH algoritmalarından alınan sonuçlar gözlemlenmiştir. Tekrarlama sahteciliğini başarıyla tespit eden bu çalışmalarda kullanılan videoların sıkıştırma gibi son işlem adımlarına maruz bırakıldığında tanılama oranının düştüğü gözlemlenmiş ve çalışmaların sıkıştırmaya dayanıklı hale getirilmesi için bir sonraki çalışmada frekans tabanlı yöntemler kullanılmıştır. Frekans düzlemine çevirmek için çerçevelerin AKD ve ADD öznitelikleri

ıkarılarak yeni bir yaklaşımla elde edilen znitelikler ikili grsellere dnştrlmş ve farklı kalite ve sıkıştırma standartlarında testler gerekleştiriłmiştir. Sonrasında tekrarlama sahtecilięi ek olarak silme sahtecilięine zm nerilmiştir. Son alıřmada da sadece tekrarlama sahtecilięi deęil literatrde bahsi geen ereveler arası tm sahteciliklere zm sunan yeni bir yaklaşımla sunulmuştur.

2.1. Tekrarlama Sahtecilięi Tespit Yntemleri

Tekrarlama sahtecilięi olay veya nesnelerin kapatılmasında, aynı video ierisinden, erevelerin kopyalanarak mevcut erevelerin zerine veya arasına yapıştırılması ile gerekleştirilir. Bu kurcalama iřlemi ile mevcut video zelliklerinde meydana gelen sapmalar yapılan sahtecilik iřlemlerinin bulunması iin kullanılmaktadır. Buradan yola ıkararak videolardan doku tabanlı ve kenar tabanlı znitelikler ıkarılmıştır.

2.1.1. Doku Tabanlı Tekrarlama Sahtecilięi Tespiti

Doku tabanlı tekniklerin ereyi temsil edebilecek ayırt edici znitelikleri avantaj olarak dřnlerek tekrarlama sahtecilięine iki farklı doku tabanlı algoritma ile zm sunulmuştur. Bu amala kullanılan Yİ ve WYT algoritmalarının detaylarından Blm 2.1.1.1. ve 2.1.1.2.’ de bahsedilmiştir. Doku tabanlı kullanılan yntemlerin ataksız videolar iin ayırt edici znitelik olarak kullanılabileceęi alıřma sonrası elde edilen bařarılı sonular ile gzlemlenmiştir. nerilen yntemin detaylarından Blm 2.1.1.3.’ de bahsedilmiştir.

2.1.1.1. Yerel İkili rnt Algoritması

Yerel İkili rnt (Yİ) algoritması grnt iřleme uygulamalarında sıka kullanılan parlaklık deęiřimine karřı duyarlılıęı dřk olan bir algoritmadır. Gri grntler zerinde uygulanan algoritma Ojala vd. tarafından nerilmiştir [165]. Yntem merkez piksel deęerleri (P_m) ile komřu pikseller (P_k) arasındaki iliřkiyi ikilik sistem ile karřılařtırmalı olarak Eřitlik 2.1. ve Eřitlik 2.2.’ deki gibi iliřkilendirir. Eřitlik 2.2.’ de

gösterilen D değeri ikili gösterimdeki sayı değerlerini göstermektedir. Sırasıyla bakılan komşuların 8 komşuluğu $i=0$ ' dan başlanarak 7' ye kadar ilerler.

$$D = \{P_m \leq P_k \text{ ise } 1 \text{ veya } P_m > P_k \text{ ise } 0\} \quad (2.1)$$

$$LBP(P_m) = \sum_{i=0}^k D \times 2^i \quad (2.2)$$

Eşitlik içerisinde kullanılan P_m merkez pikselin, P_k komşu piksellerin yoğunluk değerlerini temsil etmektedir. Şekil 2.1.' de görüldüğü gibi $(P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7)$ değerleri piksel yoğunluk değerlerini göstermektedir. Komşu piksel değeri merkez pikselin değerinden küçükse sıfır, büyük veya eşitse 1 değeri atanır. Elde edilen 8 bitlik ikili sayının onluk değeri merkez pikselin yeni değerinin belirlenmesini sağlar. Her piksel için pencere kaydırılarak merkez piksel değerleri güncellenmektedir. Standart olarak kabul edilen YİÖ algoritmasının dışında komşuluk sayısı ve komşuluklara olan uzaklıklara göre uygulamalarında çeşitlilikler sağlanabilir. Bu elde edilecek verinin büyüklüğü ile işlem zamanı arasındaki dengeye göre uygulama alanlarına bağlı olarak çeşitlilik gösterebilir.

P_0	P_1	P_2	19	220	17	0	1	0			
P_7	P_m	P_3	56	129	143	0	?	1	(01010010) ₂		82
P_6	P_5	P_4	168	76	244	1	0	0			

Şekil 2. 1. Komşuluk değerlerine göre merkez piksel etiketinin atanması

YİÖ histogramı, görüntüdeki piksellerin özniteliklerini hesaplamak için kullanılmaktadır. Özniteliklerin hesaplanması esnasında her piksel ve bitişigindeki piksellerden ikili örüntüler elde edilir. İkili örüntü, görüntüdeki merkez piksel ve onun bitişik piksellerinin ikili değerlerinden oluşmaktadır. Eğer ikili örüntüde en fazla iki kez 0-1 veya 1-0 geçişi varsa, bu örüntü tekdüze (uniform) olarak isimlendirilir. Bu örüntülerin tekdüze olup olmadığı kontrol edilir. Tekdüze olmayan örüntüler tek bir sütun ile gösterilmekte, tekdüzeler ise ayrı sütunlarda gösterilmektedir. Bu işlem sonucunda, her hücre için öznitelik boyutu 256'dan 59'a kadar azaltılabilir. 58 tekdüze, 1 tane tekdüze olmayan ikili örüntüler YİÖ histogramının oluşturulmasında kullanılır. Şekil 2.2.' (a) ve

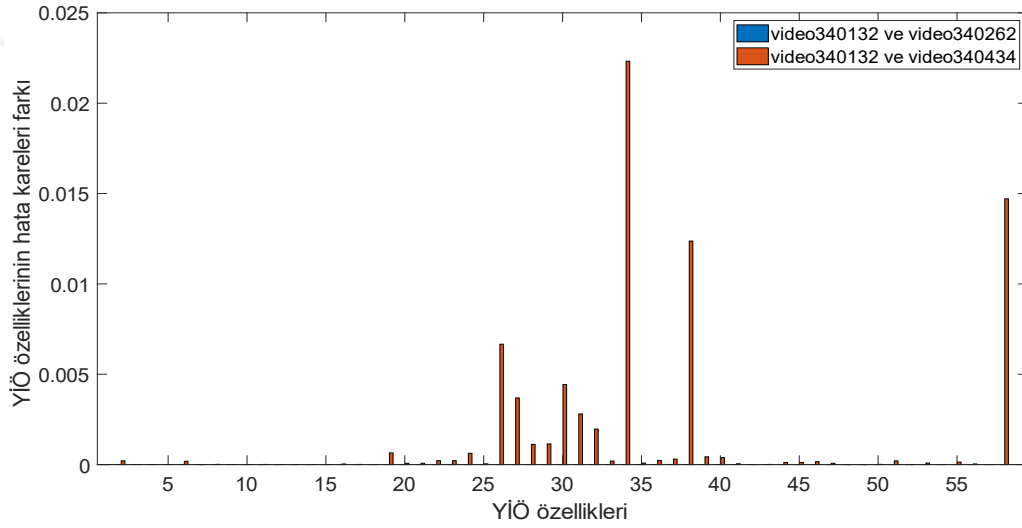
Şekil 2.2. (b)' de sırasıyla veri tabanından alınan “can_220_room (3)” örnek çerçeveler gösterilmektedir.



(a)



(b)



(c)

Şekil 2. 2. Video_34'e ait YİÖ öznitelik histogramlarının hata kareleri farkının gösterilmesi (a) Video-34 132. çerçeveye ait görsel (b) Video-34 434. çerçeveye ait görsel (c) Video çerçevelerinin hata kareleri farkı

Şekil 2.2 (c)' de 262. çerçeve 132. çerçevenin kopyası olup öznitelikler aynı olduğu için hata kareleri farkı sıfır olmaktadır ancak birbirinden farklı olan 132. çerçeve ile 434. çerçevenin hata kareleri farkı kırmızı ile gösterilen sütunlardaki gibi yüksek çıkmaktadır. Şekil 2.2.' de görüldüğü gibi birbirinin kopyası olan çerçeveler için YİÖ öznitelikleri çıkarılarak tespit edilebilir. YİÖ algoritması uygulandığında birbirinin kopyası olan çerçevelerde hata kareleri farkının sıfır olduğunu gözlemlenmektedir. Şekil üzerinde x eksenini 59 tane özelliği gösterirken, y sütunu ise kullanılan iki farklı görüntüdeki özniteliklerin hata kareleri farkının değerlerini göstermektedir.

2.1.1.2. Weber Yerel Tanımlayıcı Algoritması

Merkez piksel etrafındaki komşu pikseller ile yoğunluk farkını inceleyerek değişimi tespit edebiliriz. Değişim insan gözünün algıladığı örüntünün bulunmasını sağlar. Diferansiyel uyarım (DU) ve yönelim oryantasyonu (YO- ϕ) olarak iki bileşen kullanılarak hesaplanan Weber Yerel Tanımlayıcı (WYT) algoritması kenar algılama, gürültü ve aydınlatma gibi değişikliklere karşı dayanıklı sağlam yerel doku özneteliklerindendir [166]. DU her pikselin WEBER Yasasına göre yoğunluk değerini nicelendirir. Weber Yasası mevcut ortamda fark edilebilir bir özelliğin algılanabilmesi için ortamdaki uyaran değerler ile oranının sabit olduğunu söyler. Merkez piksel P_c 'nin komşu pikseller ile farkının, merkez piksel parlaklığına oranlanması ile DU'nun karşılık düştüğü açı bulunur.

$$DU(P_c) = \arctan \sum_{i=0}^{N=l} \frac{P_i - P_c}{P_c} \quad (2.3)$$

$$\phi(P_c) = \arctan \left(\frac{P_7 - P_3}{P_5 - P_1} \right) \quad (2.4)$$

Piksel P_c 'nin i . komşuluğu P_i 'dir. Eşitlik 2.3 'de gürültüden kaynaklanabilecek çok hızlı değişimleri kontrol etmek için arctan işlevi kullanılır. (DU) Şekil 2.3. (a)'da ki $f00$ ve $f01$ filtreleri kullanılarak hesaplanır. Eşitlik 2.4 de P_5 aşağı komşuluğu, P_1 yukarı komşuluğu, P_7 sol komşuluğu, P_3 sağ komşulukları göstermektedir. Yönelimleri de Şekil 2.3. (b)'deki $f10$ ve $f11$ filtreleri kullanılarak hesaplanır.

+1	+1	+1
+1	-8	+1
+1	+1	+1

f_{00}

0	0	0
0	+1	0
0	0	0

f_{01}

+1		-1

f_{11}

	-1	
	+1	

f_{10}

(a)
(b)

Şekil 2. 3. Weber algoritması filtreleri (a) DU hesabında kullanılan filtreler (b) YO'nun hesaplanması için kullanılan filtreler

Şekil 2.4. (a) VTL veri tabanından alınan “Akiyo.qcif” videosunun 10. çerçevesine aittir. Şekil 2.4. (b)’ de çerçeveye ait gri görüntü; Şekil 2.4. (c)’ de $f00$ filtresi ile yapılan görüntü konvolüsyonu, V_s^{00} ; Şekil 2.4. (d)’ de $f01$ filtresi ile yapılan görüntü konvolüsyonu, V_s^{01} ; Şekil 2.4. (e)’ de $f10$ filtresi ile yapılan görüntü konvolüsyonu, V_s^{10} . Şekil 2.4. (f)’ de ise $f11$ filtresi ile yapılan görüntü konvolüsyonu, V_s^{11} ait çıktılar gösterilmektedir.



(a)



(b)



(c)



(d)



(e)



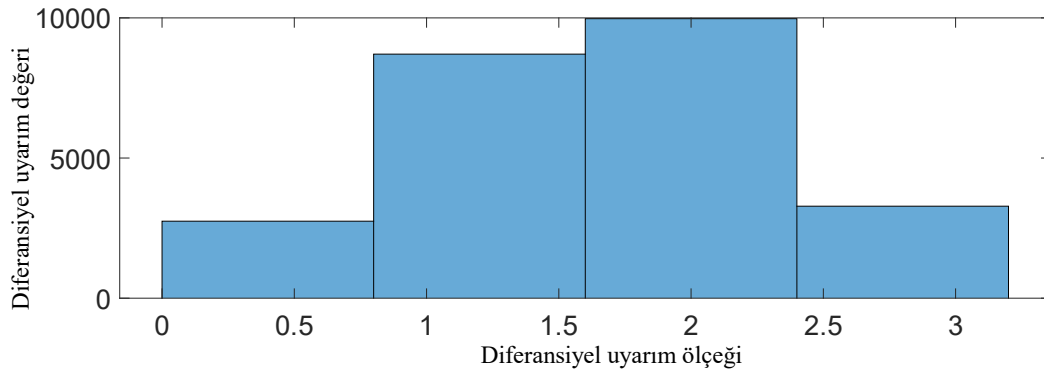
(f)

Şekil 2. 4. (a)VTL veri tabanından Akiyo videosunun 10 numaralı çerçevesi (b) Çerçeveye ait gri görüntü (c) V_s^{00} görüntüsü (d) V_s^{01} görüntüsü (e) V_s^{10} görüntüsü (f) V_s^{11} görüntüsü

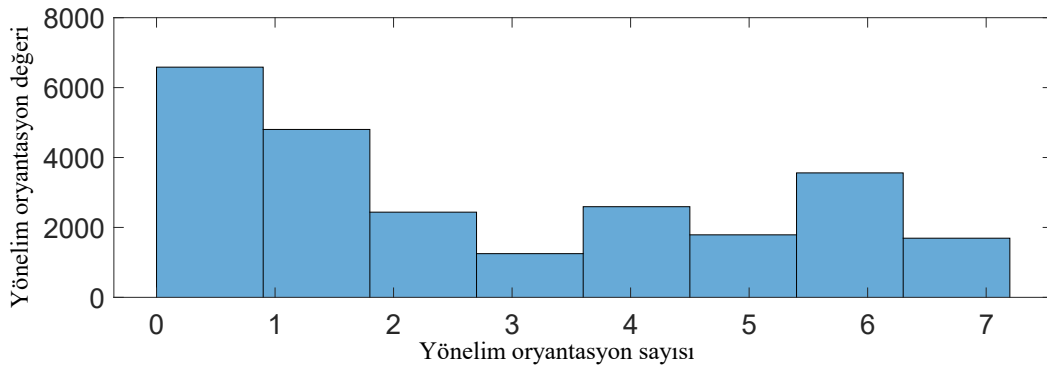
YO' nun karşılık düştüğü açı değerleri 8 farklı yönde Eşitlik 2.5'te gösterilen niceleme kullanılarak gerçekleştirilir, burada V_s^{11} ve V_s^{10} , f_{11} ve f_{10} filtrelerinden geçirilmiş olan değerleri göstermektedir. Niceleme işlemi histogram hassasiyetini artırmak için yapılır. DU ve YO histogramları çıkarıldıktan sonra DU değerleri baskın yönler göre gruplandırılarak WYT histogramı çıkarılır.

$$\phi(P_c) = \theta \in [-\pi/2, \pi/2] \rightarrow \theta' \in [0, 2\pi]$$

$$\phi(P_c) = \begin{cases} \theta, & V_s^{11} > 0, V_s^{10} > 0 \\ \theta + \pi, & V_s^{11} > 0, V_s^{10} < 0 \\ \theta - \pi, & V_s^{11} < 0, V_s^{10} < 0 \\ \theta, & V_s^{11} < 0, V_s^{10} > 0 \end{cases} \quad (2.5)$$



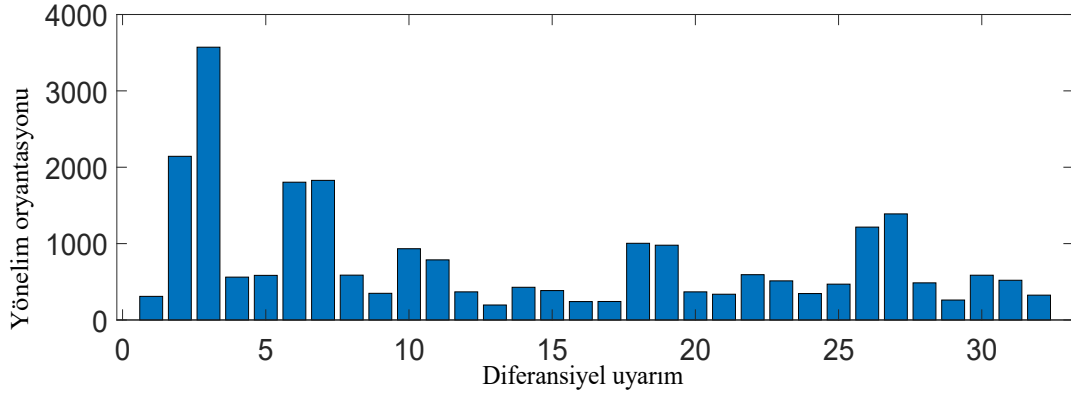
(a)



(b)

Şekil 2. 5. WYT histogramının oluşturulması (a) Akiyo 10. çerçeveye ait DU histogramı (b) Akiyo 10. çerçeveye ait YO histogramı (c) Akiyo 10. çerçeveye ait WYT histogramı

Şekil 2.5.' in devamı



(c)

Şekil 2.5.' de Akiyo görüntüsüne ait WYT histogramı ve histogramın çıkarılmasında kullanılan DU ve YO histogramları gösterilmektedir. WYT histogramında, yatay eksen DU, dikey eksen YO ile temsil edilir. Bu histogram, doku tanımlayıcısı olarak kullanılan WYT tanımlayıcısıdır. WYT ile 8 yönelimde 4 farklı ölçekte niceleme yapılarak her çerçeve için 1×32 boyutlu öznitelik çıkarılmaktadır.

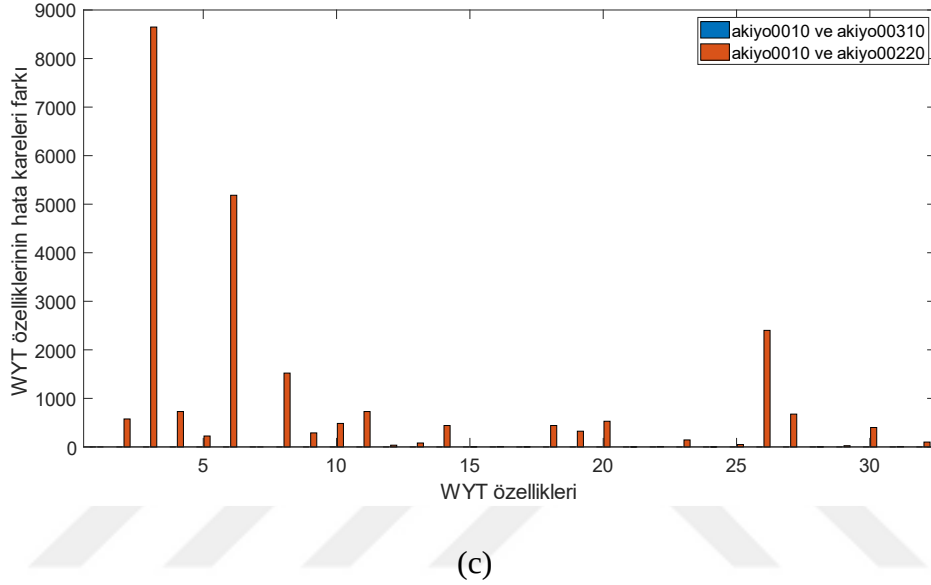
Şekil 2.6.' da VTL veri tabanından alınan "Akiyo.gif" videosu için görseller verilmektedir. Bu videonun seçilmiş olma nedeni sabit arka planlı ve sadece sunucunun konuşma hareketlerinin olduğu bir video olmasıdır. 10 ve 310 numaralı iki çerçeve birbirinin kopyasıdır. Bu yüzden tek şekil ile gösterilmektedir. 10 ve 310 numaralı çerçeveler Şekil 2.6. (a)' da ve 220 numaralı çerçeve ise Şekil 2.6. (b)' de gösterildiği gibidir. Şekil 2.6. (c)' de 10. ile 310. çerçevelere ve 10. ile 220. çerçevelere WYT algoritması uygulandıktan sonra elde edilen hata kareleri farkı gösterilmektedir. Birbirinin kopyası olan çerçevelerin hata kareleri farkı Şekil 2.6. (c)' de görüldüğü gibi sıfır çıkmaktadır, bu yüzden mavi ile gösterilen sütunlar şekilde görülmemektedir. Kırmızı ile belirtilen sütunlar ise farklı çerçevelerden elde edilen WYT histogramının hata kareleri farkını göstermektedir. Sonuç olarak doku tabanlı öznitelik çıkarımı için kullanılan WYT algoritması ayırt edici bir öznitelik olarak kullanılabilir bir özniteliktir. Bu amaçla YİÖ ve WYT algoritmalarının kıyaslanmasını içeren yeni bir çalışma ile bu algoritmaların üstünlüklerinin belirlenmesi amaçlanmaktadır.



(a)



(b)



(c)

Şekil 2. 6. WYT algoritması hata kareleri farkı (a) 10 numaralı çerçeve (b) 220 numaralı çerçeve (c) WYT algoritması öznetelikleri hata kareleri farkı

2.1.1.3. Yapısal Benzerlik Metriği

Algıya dayalı olan Yapısal Benzerlik Metriği (YBM), iki görüntü arasındaki benzerliği ölçmek için kullanılan kalite metriği olarak tanımlanmaktadır [167]. YBM değeri parlaklık (I), kontrast (c) ve yapı değerlerine (s) göre yine iki çerçeve arasındaki benzerliği $[0, 1]$ aralığında ölçmektedir. Eşitlik 2.6 ile Eşitlik 2.10 arasındaki formüllerde hesaplanması gösterilmektedir. μ_x ve μ_y sırasıyla x ve y görüntülerindeki piksellerin ortalamalarını, σ_x^2 ve σ_y^2 sırasıyla x ve y görüntülerinin varyansını ifade etmektedir. c_1, c_2, c_3 sabit katsayılarıdır. α, β, γ parlaklık, kontrast ve yapı elemanı değerlerini ağırlıklandırmaya yarayan sabit katsayı değerleridir ve varsayılan olarak 1 değeri atanmaktadır. YBM sonucu ne kadar 1'e yakınsa yöntemde kıyaslaması yapılan

öznitelikler birbirine o kadar benziyor demektir. Bu da tekrarlama sahteciliği için yöntemin başarılı olduğunu göstermektedir.

$$l(x, y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} \quad (2.6)$$

$$c(x, y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} \quad (2.7)$$

$$s(x, y) = \frac{\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3} \quad (2.8)$$

$$c_3 = \frac{c_2}{2} \quad (2.9)$$

$$YBM(x, y) = [l(x, y)^\alpha \cdot c(x, y)^\beta \cdot s(x, y)^\gamma] \quad (2.10)$$

Şekil 2.7.'de 3 görüntü arasındaki YBM değerlerine ait grafik gösterilmektedir. Bu görüntüde Şekil 2.7. (a)' da ki görüntü ve kopyası ile YBM değeri hesaplanmış ve grafiğin ilk sütununda görüldüğü gibi 1 değeri elde edilmiştir. Şekil 2.7. (b)' de ve Şekil 2.7. (a)' da aynı video içerisinde alınmış farklı çerçeveler gösterilmektedir. Bu iki çerçeveye ait YBM değeri grafiğin ikinci sütununda, yaklaşık olarak %96'lık değer ile gösterilmektedir. Şekil 2.7. (c)' de ise farklı bir videodan alınan çerçeve örneği gösterilmektedir. Son sütunda ise Şekil 2.7. (a) ile Şekil 2.7. (c)' nin YBM değeri hesaplanmıştır ve yaklaşık olarak %21' lik bir değer elde edilmiştir. Grafik üzerindeki x eksenleri yapılan YBM kıyaslamalarını, y eksenleri ise YBM değerlerini göstermektedir.



(a)



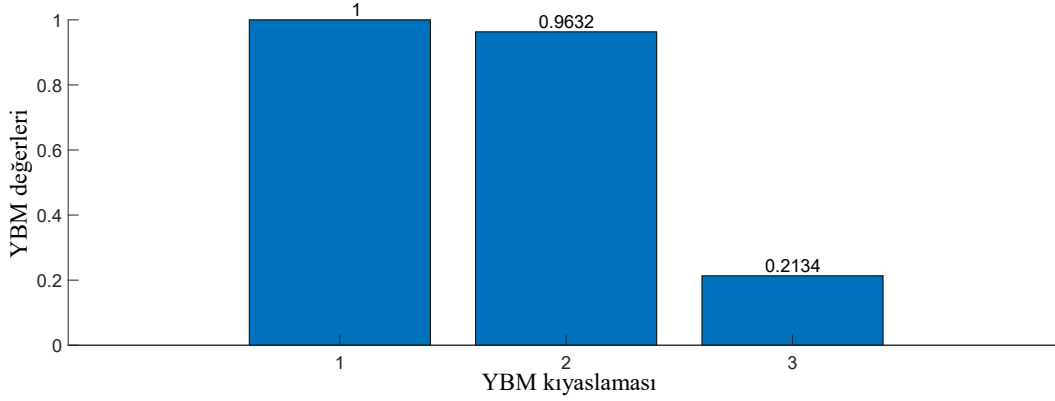
(b)



(c)

Şekil 2. 7. Web_Test veri tabanından alınan video çerçeve örneklerinin YBM kıyaslamalarının gösterimi (a) Beş_hırsız videosundan alınan 1. çerçevenin (b) Beş_hırsız videosundan alınan 1499. çerçevenin (c) Sakin_hırsız videosundan alınan 1650. çerçevenin görselleri

Şekil 2.7.' in devamı

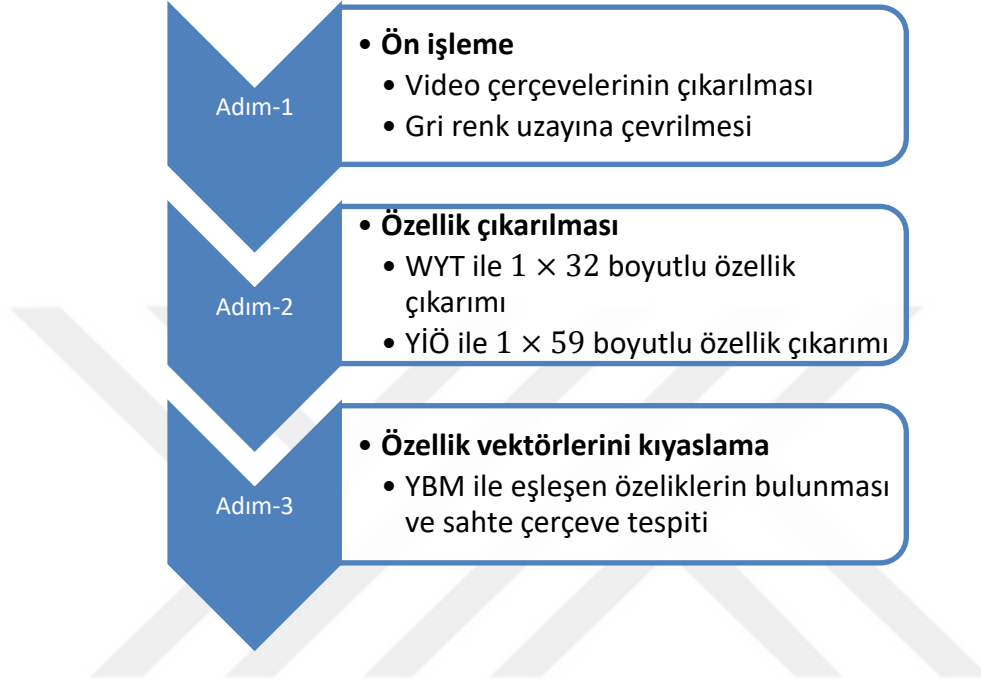
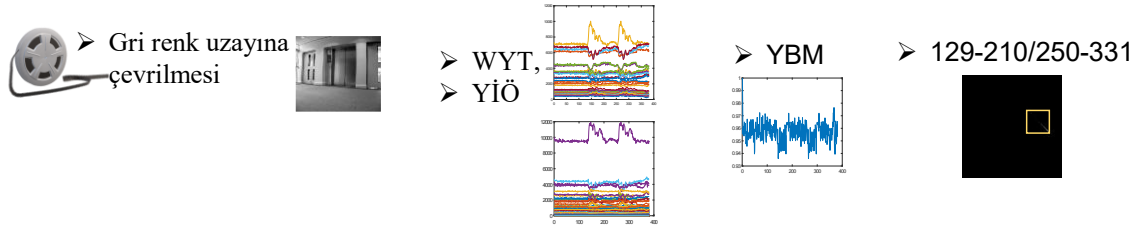


(d)

Şekil 2.7.'de de görüldüğü gibi aynı olan çerçevelerin YBM değeri 1 çıkarken benzerlik değeri düştükçe YBM değeri de düşmektedir. YBM değeri çalışma kapsamında çıkarılan özniteliklerin kıyaslanması için kullanılmaktadır.

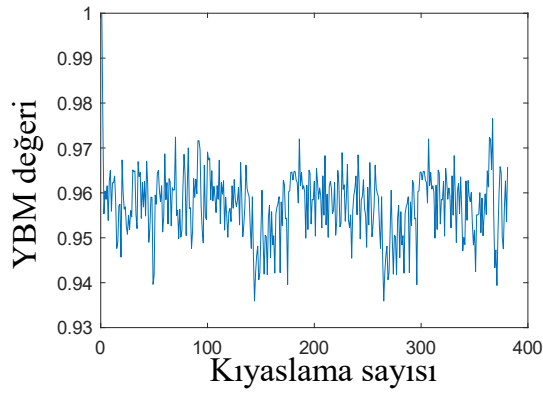
2.1.1.4. Tekrarlama Sahteciliği Tespiti İçin Önerilen Doku Tabanlı Yaklaşım

Bu bölümde doku tabanlı öznitelik çıkarım algoritmalarının avantajlarından faydalanılarak önerilen yöntemin detaylarından bahsedilecektir. Algoritma üç adımda, tekrarlama sahteciliğine iki farklı doku tabanlı algoritma kullanarak çözüm sunmayı hedeflenmektedir. İlk aşamada video çerçevelerinden elde edilen her bir çerçeve KYM uzayından gri renk uzayına dönüştürülmektedir. Sonrasında her bir çerçeve için öznitelik vektörü oluşturulmaktadır. Öznitelik çıkarmak için doku tabanlı YİÖ ve WYT algoritmaları kullanılmaktadır. Kullanılan her iki algoritmada, yoğun yerel tanımlayıcı olarak tanımlanan sınıfa dahildir [15]. Bu sınıftaki öznitelik çıkarım teknikleri görüntüden piksel düzeyinde öznitelik çıkarmaktadır. İncelenen her çerçeve için komşu piksellerle olan ilişkisi gözetilmektedir. Kullanılan algoritmalarda her iki doku tabanlı yöntem için merkez pikselin etrafındaki 3×3 lük kare komşuluk kullanılmaktadır. Üçüncü aşamada birinci çerçevenin öznitelik vektörü referans seçilerek, geri kalan çerçevelerle YBM kıyaslamasına bakılmaktadır. Önerilen yöntemin blok diyagramı Şekil 2.8.' de verildiği gibidir. İlk kısım görsel olarak ikinci kısım adımlar şeklinde gösterilmektedir.

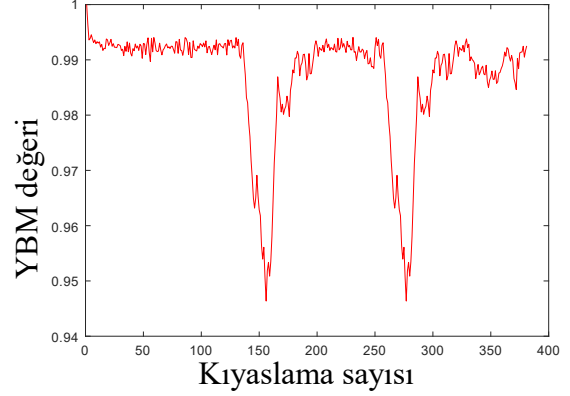


Şekil 2. 8. Önerilen yöntemin genel blok diyagramı

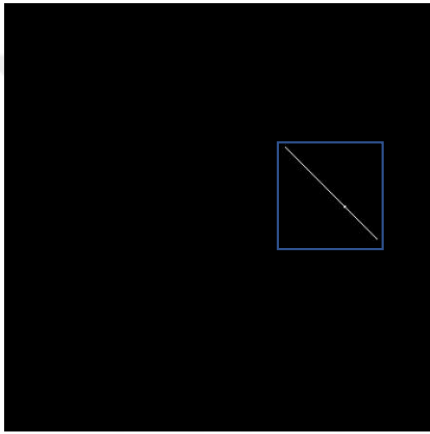
Yöntemin öznelik çıkarımında kullanılan algoritmaların detaylarından önceki bölümlerde bahsedilmektedir. Bu özneliklere ait Fadl veri tabanından alınan video 17' ye ait Şekil 2.9. (a)' da YİÖ özelliği kullanılarak ve Şekil 2.9. (b)' de ise WYT özelliği kullanılarak elde edilen YBM histogramlarının çıktı örnekleri gösterilmektedir. Burada x eksenleri çerçeve sayısının bir eksiği kadar yapılan kıyaslamayı, y eksenini ise yapılan kıyaslamaların YBM değerlerini göstermektedir. Kıyaslama işlemi 1. çerçevenin özelliği referans kabul edilerek yapılmıştır. Şekil 2.9 (c) ve (d)' de tekrarlama sahteciliği yapılan çerçevelerin korelasyon sonucu ikili görüntülerine ait görsel verilmektedir. Görsel üzerindeki doğru parçaları eşleşen noktaları, yani kopyalamanın yapıldığı kaynak çerçeve ve yapıştırmanın yapıldığı hedef çerçevelerin konumlarını göstermektedir. Bu görselde bulunan doğru parçaları kopyalamanın ve yapıştırmanın yapıldığı çerçeveler arasındaki fark sabit olduğundan doğru eğimi için kullanılır. İki noktası ve eğimi bilinen doğru denkleminde yola çıkarak görsel amaçlı çizdirilmiştir. Doğru parçaları dikkat çekmesi için kutu içerisine alınmıştır.



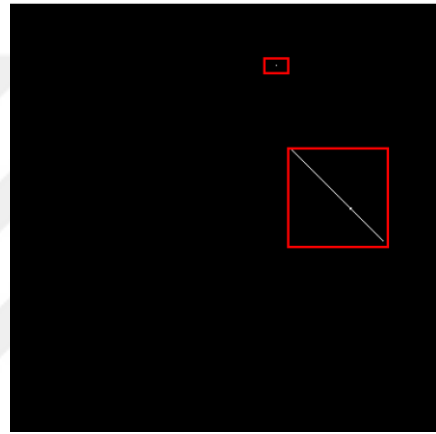
(a)



(b)



(c)



(d)

Şekil 2. 9. (a) YİÖ ile çıkarılan öznelilik histogramı (b) WYT ile çıkarılan öznelilik histogramı (c) YİÖ ile tespit edilen çerçevelerin ikili gösterimi (d) WYT ile tespit edilen çerçevelerin ikili gösterimi

Bu çalışma ile tekrarlama sahteciliğine doku tabanlı iki farklı yaklaşım sunularak başarılı sonuçlar elde edilmiştir. Üçüncü bölümde yöntemin denendiği veri tabanlarından alınan kıyaslamalı sonuçları verilmektedir.

2.1.2. Kenar Algılamaya Dayalı Tekrarlama Sahteciliği Tespiti

Doku tabanlı yaklaşım dışında görüntü içerisindeki nesnelerin ikili görüntülerinin oluşturularak elde edilen görüntüler üzerinden kenar bulma algoritmalarıyla tekrarlama sahteciliğinin yapılabilmesi için ikinci bir çalışma önerilmiştir. Kenar nesnelerin tanımlanması için keskin geçişlerin olduğu piksellerin gruplandırılması işlemidir.

Kenar bulma işleminde sahne içerisindeki nesnelerin gürültülerini temizlemek veya azaltmak, görüntünün yumuşatılması için LoG filtresi ve Canny algoritması birlikte uygulanmıştır [168]. Ayrıca kenar algılarken, köşe noktalarının ve birleşim noktalarının algılamasında LoG algoritmasının kullanılması kenar bulma başarısını artırmaktadır. Bu yüzden bükülme (sıfır geçiş) noktalarının bulunmasında Gauss' un ikinci türevini kullanan LoG algoritması da kullanılmıştır. Bölüm 2.1.2.1. ve 2.1.2.2.' de kullanılan algoritmaların detaylarından bahsedilmektedir.

2.1.2.1. Canny Algoritması

Kenar algılama yöntemleri, parlaklık yoğunluğu ve renk değişimlerinin algılanması için kullanılmaktadır. Canny algoritması ile görüntü yüzeyindeki kenarların algılanması için gradyan değerleri, gri görüntüler üzerinden Gaussian filtresi kullanılarak uygulanır. Algoritma sinyal gürültü oranını optimize edecek şekilde 4 aşamadan oluşmaktadır [169]. Bunlar filtre uygulayarak yumuşatma, gradyan hesaplama, maksimum olmayan noktaların bastırılması ve eşikleme şeklindedir. Canny algoritmasında, gradyan vektörü yönünde, şiddeti yerel maksimum olan noktalar kenar noktasını temsil eder. Kenar piksellerinin çizgilerini inceltmek için eşikleme yöntemiyle maksimum olmayan noktaların bastırılması gerçekleştirilir.

Adım 1: $I[x, y]$ görüntüsünün, " $\sigma = 1$ " yumuşatma derecesi kullanılarak $G[x, y, \sigma]$ filtresi ile konvolüsyonu ile $S[x, y]$ görüntüsü oluşturulur. Gürültünün kaldırılması için yumuşatma işlemi yapılır. Eşitlik 2.11, Eşitlik 2.12' nin formüle edilmiş halini göstermektedir.

$$S[x, y] = I[x, y] * G[x, y, \sigma] \quad (2.11)$$

$$S[x, y] = \frac{1}{159} \begin{bmatrix} 2 & 4 & 5 & 4 & 2 \\ 4 & 9 & 12 & 9 & 4 \\ 5 & 12 & 15 & 12 & 5 \\ 4 & 9 & 12 & 9 & 4 \\ 2 & 4 & 5 & 4 & 2 \end{bmatrix} * I[x, y] \quad (2.12)$$

Adım 2: $S[x, y]$ ' nin sonlu farklar yaklaşımıyla x ve y piksellerindeki kısmi türevleri alınarak gradyan büyüklüğü $M[x, y]$ ve her bir noktanın eğimi $Q[x, y]$ bulunur. Eşitlik 2.14, Eşitlik 2.13' ün; Eşitlik 2.16, Eşitlik 2.15' in filtrelerini göstermektedir.

$$P[x, y] \approx (S[x, y + 1] - S[x, y] + S[x + 1, y + 1] - S[x + 1, y])/2 \quad (2.13)$$

$$P[x, y] = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} * S[x, y] \quad (2.14)$$

$$R[x, y] \approx (S[x, y] - S[x + 1, y] + S[x, y + 1] - S[x + 1, y + 1])/2 \quad (2.15)$$

$$R[x, y] = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * S[x, y] \quad (2.16)$$

$$M[x, y] = \sqrt{P[x, y]^2 + R[x, y]^2} \quad (2.17)$$

$$Q[x, y] = \arctan(R[x, y], P[x, y]) \quad (2.18)$$

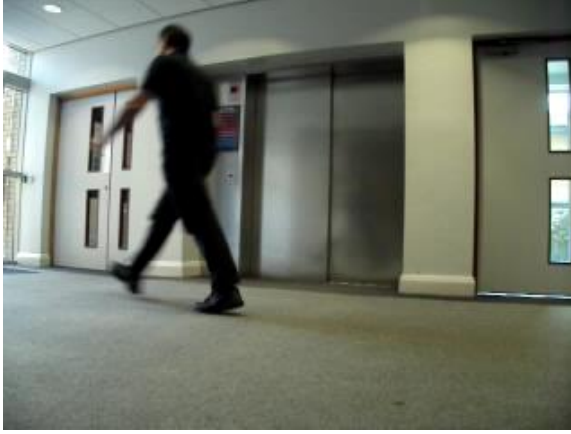
Adım 3: Maksimum olmayan noktaların bastırılması gerçekleştirilir.

Adım 4: Bu adımda hatalı kenarların elenmesi için belirlenen eşik değerinin altında kalan noktaların sıfırlanması gerçekleştirilir. Eşik değeri görüntüye göre otomatik seçilmektedir.

Eşik değerinin seçilmesi deneysel olup; küçük seçilmesi durumunda yanlış kenarlar oluşurken, büyük seçildiğinde de mevcut kenarların kaybolmasına neden olunur.

Fadl veri tabanından alınan V17 isimli videonun 170. çerçevesine ait Şekil 2.10.' da adım adım Canny ile elde edilmiş kenar görüntüsü görülmektedir.

İlk olarak Şekil 2.10. (a)' da video çerçevesine ait görsel verilmektedir. Şekil 2.10. (b)' de adım 1' deki Gauss filtresinden geçirilmiş, sonrasında Şekil 2.10. (c) ile yatay ve Şekil 2.10. (d) ile dikey yönde konvülasyonlardan geçirilmiş görseller gösterilmektedir. Algoritmanın üçüncü aşaması maksimum olmayan noktalar bastırıldığında elde edilen görsel Şekil 2.10. (e)' deki gibidir. Canny algoritması çift eşikleme kullanan kenar belirleme yöntemlerindendir. Eşikleme işleminde kullanılan eşik değeri büyük seçilirse bu durumda ince kenarlar algılanamayacak, küçük seçilirse de tam tersi görüntüdeki kenar olmayan gürültü kısımları dahi kenar olarak algılanacaktır. Dolayısıyla bu algoritma iki eşik kullanarak eşikleme problemine çözüm sunmaktadır. Algoritmanın son aşamasında ise görüntüye göre belirlenen eşik değerinden geçirilen yöntemin sonuç çıktısı Şekil 2.10. (f)' de gösterilmektedir.



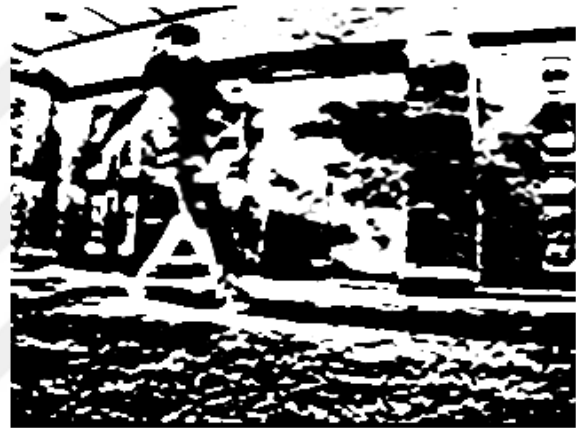
(a)



(b)



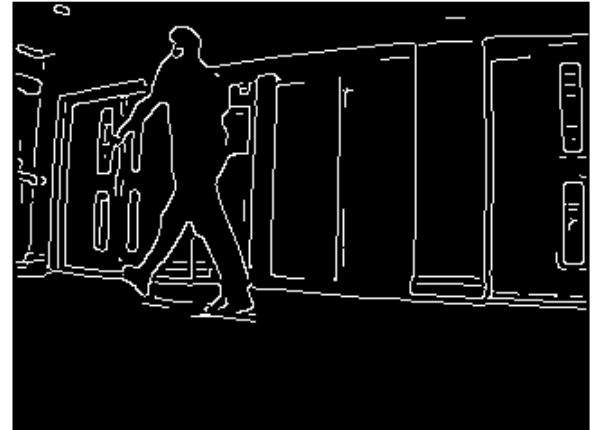
(c)



(d)



(e)



(f)

Şekil 2. 10. Canny algoritmasının uygulama adımları (a) 170. çerçeveye ait görsel (b) Gauss filtresinden geçirilen görüntünün çıktısı (c) x filtresi konvolüsyon sonucu (d) y filtresi konvolüsyon sonucu (e) Maksimum olmayan noktaların bastırılması sonrası (f) Eşik uygulaması sonrası

2.1.2.2. LoG Algoritması

LoG algoritması Gaussian fonksiyonu ile görüntüyü düzgünleştirip, gürültüyü kaldırırken, Laplasyan fonksiyonu ile de görüntünün türevini alarak parlaklık değişimlerinin olduğu yerleri ortaya çıkarır [170]. Laplasyan filtresi için kullanılan iki ayrı yaklaşım filtreleri Şekil 2.11.' de görüldüğü gibidir. Bu filtreler gürültüye karşı çok hassastırlar. Bunu engellemek için Laplas filtresinden önce Gauss ile yumuşatma yapılır. Böylece yüksek frekans gürültü bileşenleri azaltılmış olunur.

0	-1	0	-1	-1	-1
-1	+4	-1	-1	+8	-1
0	-1	0	-1	-1	-1

Şekil 2. 11. Laplasyan filtresi için kullanılabilecek iki farklı matris

Piksel değerleri x, y olan I görüntüsüne Eşitlik 2.19' daki gibi Laplasyan fonksiyonu uygulanmaktadır.

$$L(x, y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2} \quad (2.19)$$

Gauss filtresi, görüntüdeki her piksel değerini, kendisi ve etrafındaki piksel değerlerinin ağırlıklı ortalamasıyla değiştirir. Bu ağırlık Gauss dağılımına göre belirlenir. Daha uzak olan piksellerin ağırlıkları daha azdır. Laplasyan filtresi ise bir pikselin değerini, kendisi ve etrafındaki piksellerin değerleri arasındaki farkların toplamı olarak belirler. Ancak; Laplasyan filtresi gürültüye karşı hassas olduğundan önce Gauss uygulanarak düzgünleştirilen görüntüye Laplasyan uygulanır. İki boyutlu sıfır merkezli LoG fonksiyonu da Eşitlik 2.20'de gösterilmiştir.

$$LoG(x, y) = -\frac{1}{\pi\sigma^4} \left[1 - \frac{x^2 + y^2}{2\sigma^2} \right] e^{-\frac{x^2 + y^2}{2\sigma^2}} \quad (2.20)$$

Aslında aritmetik işlemlerin azaltılması için Gauss ile Laplace filtrelerinin hibritleştirilmesi sonucu Şekil 2.12.' deki filtrede uygulanabilir. Bu filtre için Gauss standart sapması $\sigma=1.4$ seçilerek işlem yapılmıştır.

0	1	1	2	2	2	1	1	0
1	2	4	5	5	5	4	2	1
1	4	5	3	0	3	5	4	1
2	5	3	-12	-24	-12	3	5	2
2	5	0	-24	-40	-24	0	5	2
2	5	3	-12	-24	-12	3	5	2
1	4	5	3	0	3	5	4	1
1	2	4	5	5	5	4	2	1
0	1	1	2	2	2	1	1	0

Şekil 2. 12. LoG filtresi

Gauss standart sapması düşürüldüğü zaman Gauss darlaşacaktır. Bu da yumuşatma etkisinin azalmasına neden olacaktır [168].

Şekil 2.13' de LoG algoritmasının farklı standart sapmalarına ilişkin görseller verilmektedir. Algoritma da kullanılan standart sapma değerlerinin değiştirilmesine bağlı olarak büyük sigma değeri daha fazla düzgünleştirmeye neden olmakta ve kenarlardaki değişimler Şekil 2.13.' deki gibi güncellenmektedir. Örnek olarak verilen görüntülerde sigma değeri sırasıyla 0.1, 0.3 ve 0.5 olarak seçilmiştir.



(a)



(b)



(c)

Şekil 2. 13. LoG algoritması ile (a) 0.1 (b) 0.3 (c) 0.5 standart sapma değerleri için elde edilen görseller

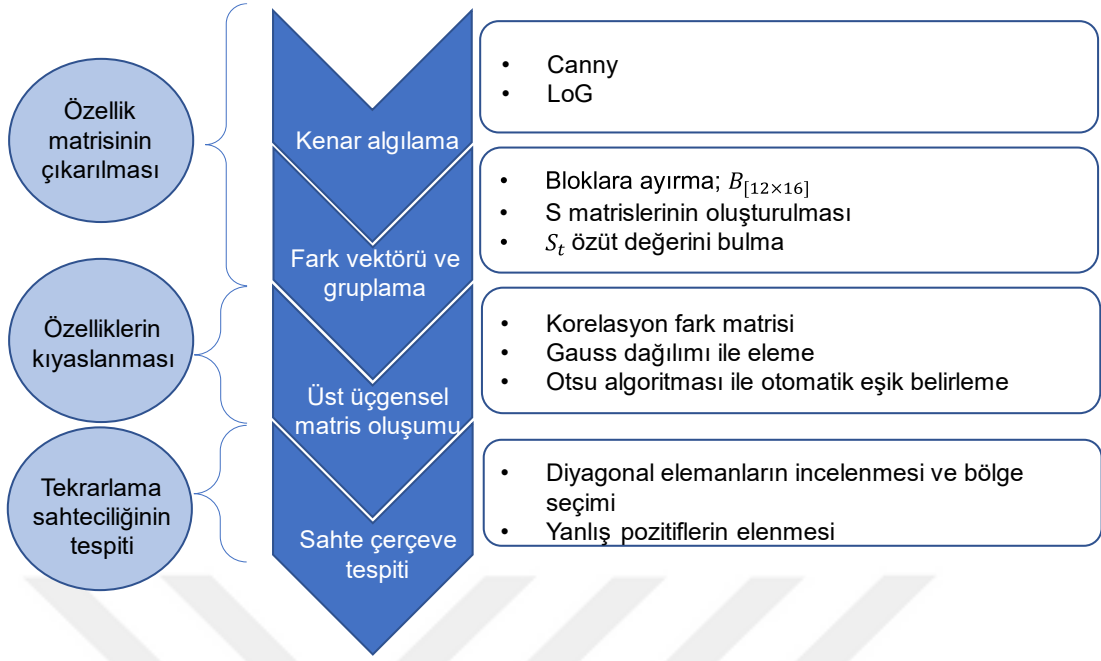
LoG algoritması uygulandıktan sonra eşik değerine göre kenarlar belirlenir. Eşik değerinin üzerinde olanlar kenar kabul edilirken, altında kalanlar kenar olarak seçilmezler. Algoritmanın son aşamasında en belirgin kenarların korunması maksimum olmayan noktaların bastırılması gerçekleştirilir.

2.1.2.3. Tekrarlama Sahteciliği Tespiti İçin Önerilen Kenar Algılamaya Dayalı Yaklaşım

Çerçeveler arası kurcalama işlemi, ardışık çerçevelere ait nesnelerin tutarlı özniteliklerinde, sapmalara neden olmaktadır. Nesnelerin algılanması için nesnelere ait kenarların belirlenmesi gerekmektedir. Bu çalışma ile nesne kenarlarından elde edilen öznitelikler ile çerçeveler arası tekrarlama sahteciliğine çözüm bulmak amaçlanmıştır. Yöntem üç aşamadan oluşmaktadır. İlk aşamada LoG ve Canny algoritması bir arada kullanılarak nesnelere ait kenarlar belirlenmektedir. Ardışık çerçevelerde tekrarlama sahteciliğinin yapılması herhangi bir olayı veya nesneyi kapatmamaktadır. Dolayısıyla da sahtecilik yapmak isteyen kişilerin amacına hizmet etmeyecektir. Bu göz önünde bulundurularak ardışık çerçevelerden elde edilen öznitelikler gruplandırılmış ve mevcut videolar sabit uzunlukla alt gruplara ayrılmıştır. Gruplama yapılması aynı zamanda durağan sahnelerdeki benzerliğin yüksek olması dolayısıyla yanlış pozitiflerin artmasını engellemiştir. Yöntemin ikinci aşamasında alt gruplar arasındaki korelasyon değerleri hesaplanmış ve görsel matrisi oluşturulmuştur, yüksek korelasyonlu gruplar aday olarak belirlenen sahte çerçeve grubuna dahil edilmiştir. Son aşamada aday çerçeveler arasından yanlış pozitif olanların elenmesi gerçekleştirilmiştir. Yöntemin adımları Şekil 2.14.' de gösterildiği gibidir. Yöntem üç ana aşamadan oluşmaktadır. Kenar algılama ve fark vektörlerinin oluşturulması öznitelik matrisinin çıkarılması için, üst üçgensel matris oluşumu özniteliklerin kıyaslanması için, sahte çerçeve tespiti de tekrarlama sahteciliğinin tespiti için kullanılan yöntemler Şekil 2.14.' de adım adım gösterildiği gibidir.

Video içerisindeki tüm çerçeveler bloklara bölünmektedir. Ardışık çerçeve blokları arasında bir fark hesaplamak amacıyla ardışık iki çerçevenin aynı sıradaki bloklarının Eşitlik 2.21 kullanılarak xorlarına bakılır.

$$S_1 = B_1^1 \oplus B_2^1 \quad (2.21)$$



Şekil 2. 14. Kenar algılamaya dayalı algoritmanın genel adımları

Burada B_1^1 ile 1. çerçevenin 1. bloğu, B_2^1 ile 2. çerçevenin 1. bloğu ve S_1 ile de 1. bloklara ait xor matrisi gösterilmektedir. Bir videonun boyutunu 240×320 olarak düşünersek her blok boyutu 12×16 olursa elde edilen toplam blok sayısı 400 olacaktır. Her ardışık iki çerçeve için 400 bloklu S matrisi oluşturulmuştur. S matrisinin içerisinde 0 ve 1'lerden oluşan çerçeve blokları arası farklılıklar bulunmaktadır. Bu farklılıkların toplamı bize iki ardışık çerçeve arasındaki değişimi göstermektedir. Her bloktan elde edilen değişim aslında iki ardışık çerçeveden çıkarılmış fark özüt değeri olarak nitelendirilebilir. Eşitlik 2.22 ile hesaplanan özüt değerleri iki ardışık çerçeve özniteliklerine bakılarak elde edilecek öznitelik matrislerini oluşturacaktır. Sonrasında matrisler vektöre dönüştürülerek kullanılmaktadır.

$$S_t = \sum_{j=1}^{16} \sum_{i=1}^{12} x \quad (2.22)$$

Şekil 2.15 (d)' de görüldüğü gibi elde edilen ikili görüntü her çerçeve için kullandığımız öznitelikleri göstermektedir. Şekil 2.15 (b) ve Şekil 2.15 (c) ise kenar filtrelerinin ayrı ayrı uygulanmış halini göstermektedir.



(a)



(b)



(c)



(d)

Şekil 2. 15. V25 için alınan; (a) YCbCr renk uzayından Y renk kanalına ait görsel, (b) Görsele ait Canny algoritması uygulanmış görüntüsü, (c) LoG filtresinden geçirilmiş görüntüsü, (d) Canny ve LoG filtresinin birlikte uygulandığı çıktı görüntüleri

Öznitelik vektörlerinden oluşan matrisin satırları çerçeve sayısı kadar olup, sütunları blok sayısı kadardır. Öznitelik vektörlerinin birbirleri ile kıyaslandığında art arda gelen bu çerçeveler özellikle sabit sahneli videolarda çok benzer çıkabilmektedir. Bunun üstesinden gelmek için öznitelik vektörlerini birebir benzerliği yerine, ardışık çerçeve gruplarının özniteliklerinin benzerliğini öne çıkarmak amacıyla gruplandırma yapılmıştır. Böylece iki çerçeve farkı yerine çerçeve gruplarının farkı incelenmiş olacaktır. Bu farkın hesaplanmasında Pearson korelasyon katsayısı Eşitlik 2.23 ile hesaplanmaktadır. Korelasyon iki değişken arasındaki lineer ilişkinin ölçülmesinde kullanılır. Burada amaç x ve y ile gösterilen değerlerin, doğrusal biçimde ne kadar tutarlılık gösterdiğini ifade eder. $\bar{x}$

ve $\bar{y}$, $\bar{x}$ ve $\bar{y}$ verilerinin ortalama deęerlerini gstermektedir. Her deęiřkenden ortalamalarının ıkarılıp, sonra bu deęerlerin arpımlarının toplamı, x ve y deęiřkenleri arasındaki ortak deęiřim miktarını hesaplamak iin kullanılmaktadır.

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (2.23)$$

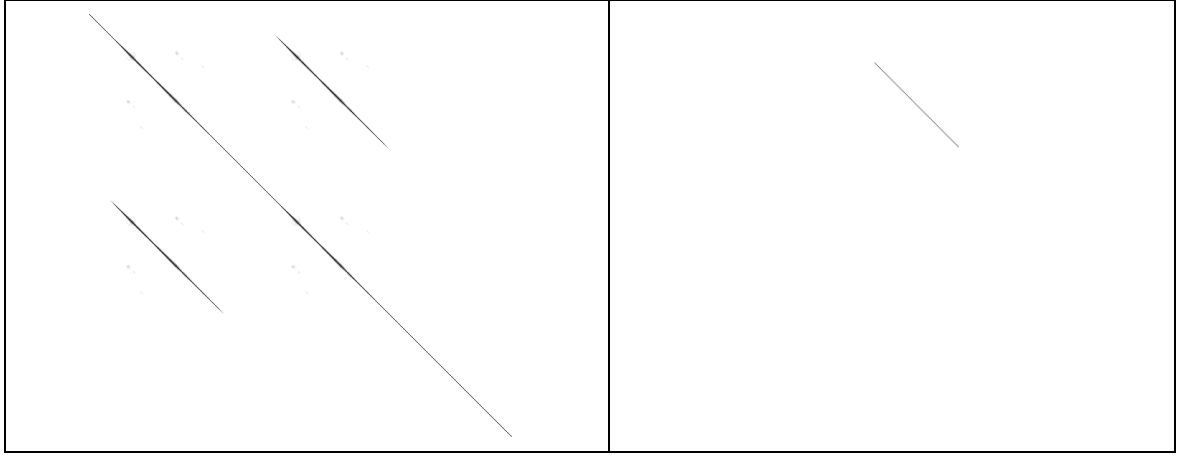
Hesaplanan korelasyon katsayılarının farklarının grnts řekil 2.16.' da gsterildięi gibidir. Tm znitelik vektrlerinin sayısı kadar korelasyon iřlemi yapılacaęı iin bu fark matrisine ait řekil 2.16. (a)' daki grselde satır ve stn sayısı znitelik vektrnn sayısı ile grup sayısının farkı kadar olmaktadır. Simetrik olan bu matrisin, sadece st gensel blgesi kullanılmaktadır.

Korelasyon fark matrisi grnts oluřturulmasının sebebi bu grnt zerinden sahtecilik yapılan eřleřmelerin yani izginin tespit edilmesidir. Bu amala grnt zerindeki beyaz pikseller dięer bir deyiřle yksek korelasyonlu ereve eřleřmeleri elenmiřtir.

řekil 2.16. zerinde siyah renkli kısımlar farkların sıfıra yakın olduęu kısımları gstermektedir. řekil 2.16. (b)' de korelasyon fark matrisi zerindeki křegen oluřturan siyah piksel deęerleri, tekrarlama sahtecilięine aday korelasyon eřleřmelerini gstermektedir. Kopyalanan ve yapıřtırılan erevesel arası fark sabit olduęundan, sahte erevesel korelasyon grnts zerinde -45°'lik bir doęru oluřturması beklenilir.

Sahte blgeleri gsteren doęrunun bulunması iin olasılık yoęunluk fonksiyonundan ve Otsu algoritmasından faydalanılmaktadır. Son ařama da diyagonal elemanların incelenmesi iin blge seimi yapılmaktadır. Elde edilen sonu grnts řekil 2.16 (b)' deki gibidir.

nerilen yntemin bu ařamasına kadar sahte olabilecek aday vektrn oluřturulması saęlanmaktadır ancak mevcut doęru zerindeki tm noktaların aslında sahte erevesel oluřmadıęı gzlemlenmiřtir. Hatalı bulunan erevesel elenmesi iin aday olarak belirlenen bu erevesel bařlangı ve bitiř konumlarındaki erevesel ile aralarındaki YBM hesaplanmaktadır.



(a)

(b)

Şekil 2. 16. (a) Korelasyon fark görüntüsü, (b) üst üçgensel matrisi

Doğru boyunun fazla olması ve eksik olması şeklinde iki farklı durum söz konusudur. Bu fazlalıkların elenmesi için deneysel olarak belirlenen eşik değerine göre kıyaslama yapılmaktadır. Eşik değerinden büyük olan çerçeveler sahte çerçeve, eşik değerinin altında kalanlar orijinal çerçeve olmaktadır.

Eğer fazla bulunan konumlar doğrunun başlangıcındaysa ve YBM değeri eşikten küçükse, aslında başlangıç o konum değil bir sonraki konum olacaktır; dolayısıyla başlangıç konumu artırılır. Eğer bitiş konumda ise ve yine eşikten küçükse bu sefer de bitiş konumu o konum değil bir önceki konum olacaktır.

Eksik bulunma durumunda da doğrunun başlangıç ve bitiş durumuna göre eşik değerinin üzerinde kalanlar sahte olarak etiketlenir. Başlangıçta ise azaltılır, bitiş konumda ise artırılabacaktır. Bu çalışmada tekrarlama sahteciliğini yapmak için örtüşen şekilde yapıştırma yapılmadığı ve en az 10 çerçeve sonuna yapıştırma yapıldığı varsayılmıştır.

Bu varsayım, sahtecilik yapan kişilerin sahne üzerinde değişiklik yapmak isteyeceği, dolayısıyla yakın çerçeveler üzerinde oynama yapılması durumunda hedefine ulaşamayacağı düşüncesinden kaynaklanmaktadır.

2.2. Sıkıştırma Dayanıklı Tekrarlama Sahteciliği Tespit Yöntemleri

Sıkıştırma işleminin temelinde kullanılan AKD ile yüksek frekans bileşenleri atılarak, atılan bu bileşenlerin öznetelik çıkarımına dahil edilmemesi sıkıştırma karşı

dayanıklılık sağlamaktadır. Bu doğrultuda amaç mevcut verileri frekans düzlemine dönüştürerek yüksek frekans bileşenlerinden bağımsız olmaları amaçlanmıştır.

2.2.1. Frekans Düzleminde Kullanılan Teknikler

Sıkıştırma işleminin amacı görselin kalitesinin en az etkilenecek şekilde, gözün fark etmediği piksel değerlerinin atılarak, minimum kapasitenin sağlanmasıdır. Videolarda B ve P çerçevelerinde kullanılan sıkıştırma standartlarının temel amacı da bu şekilde yüksek frekans bileşenlerinin atılmasıdır. Yüksek frekans bileşenleri atılınca, geriye kalan veriler daha az kayıplı olarak kullanılabilecek öz nitelikler olduğu için, bunlar üzerinden çıkarılan öz nitelikler de sıkıştırmanın meydana getirdiği kayıptan etkilenmemektedir. Buradan yola çıkarak AKD ve ADD algoritması ile frekans düzlemine dönüştürülen videoların düşük frekans bileşenleri referans öz nitelik olarak seçilerek kıyaslamaları yapılmakta ve önerilen yöntemin sıkıştırmaya karşı dayanıklılığı sağlanmaktadır.

2.2.1.1. AKD Algoritması

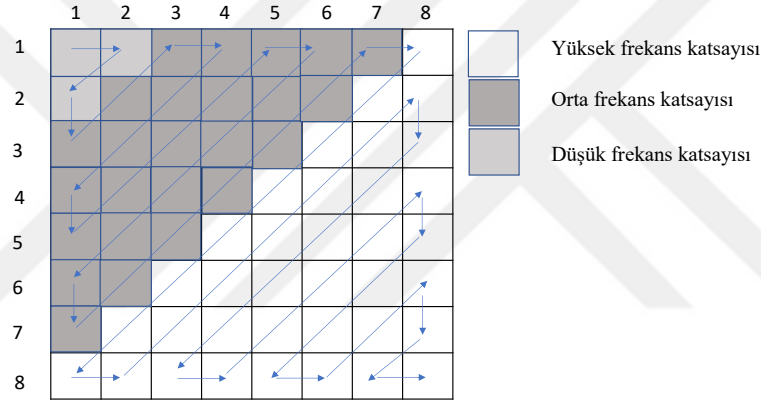
Nasir Ahmed tarafından önerilen ve sinyal işleme, görüntü işleme, veri sıkıştırma uygulamalarında kullanılan AKD algoritması ile görüntünün farklı frekans bantlarına ayrıştırılması gerçekleştirilmektedir [171]. Bu frekans bantları ile düşük, orta ve yüksek katsayılar oluşturulmaktadır. Ayrıştırma sonucunda görüntünün bilgi içeriğinin çoğu düşük frekans katsayıları ile temsil edilmektedir. JPEG sıkıştırmanın temelinde AKD dönüşümü ve katsayıların zigzag taranması kullanılmaktadır.

$$F(u, v) = \frac{1}{\sqrt{MN}} \alpha(u) \alpha(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \cos\left(\frac{(2x+1)u\pi}{2M}\right) \cos\left(\frac{(2y+1)v\pi}{2N}\right) \quad (2.24)$$

$$\alpha(u) = \begin{cases} 1/\sqrt{2}, & u = 0 \\ 1, & u = 1, 2, \dots, M-1 \end{cases} \quad (2.25)$$

$$\alpha(v) = \begin{cases} 1/\sqrt{2}, & v = 0 \\ 1, & v = 1, 2, \dots, N-1 \end{cases} \quad (2.26)$$

Düşük frekanslı katsayıların ön planda tutulmasını sağlayan zigzag tarama sayesinde, yüksek frekans bileşenlerinden bağımsız işaret bilgisi çıkarılmakta, çıkarılan özniteliklerin sıkıştırma ataklarına karşı etkinliği sağlanmaktadır. Eşitlik 2.24 ile $M \times N$ boyutlu $f(x,y)$ görüntüsüne, dönüşüm uygulandığında elde edilen $F(u,v)$ katsayıları göstermektedir. Şekil 2.17.' de AKD ile elde edilen frekans bileşenleri üzerindeki zigzag taramanın gösterimi yapılmıştır. Açık gri hücreler düşük frekans bileşenlerini, koyu gri bölümler orta frekans aralığını, beyaz kısımlarda yüksek frekans bileşenlerini göstermektedir. Mavi oklar ile de zigzag taramanın sırayla düşük frekanstan yüksek frekansa göre ilerlemesini göstermektedir. İlerleme sonucunda oluşan vektörün ilk elemanları yüksek frekanslı elemanlarını içermektedir.



Şekil 2. 17. 8x8'lik blok üzerinden AKD frekansları ve zigzag tarama

Şekil 2.18.' de SULFA veri tabanından alınan can_220_flap (2) videosuna ait AKD dönüşümü çıktısı gösterilmektedir. Şekil 2.18. (a)' da orijinal görüntü, Şekil 2.18. (b)' de AKD' si alınmış görsel gösterilmektedir. İki görüntü arasındaki kalite kaybı açıkça fark edilebilmesine rağmen görüntü yine de tanımlanabilir halde bulunmaktadır. Ancak AKD' si alınan görüntü de mevcut verilerin yaklaşık %85' i atılmıştır.

Girdi görüntüsünün AKD katsayıları hesaplanırken, 8×8 ' lik bloklara ayrılmakta ve 64 adet katsayı elde edilmektedir; ancak bunlardan sadece ilk 10 tanesi alınmakta geri kalanı ise sıfırlanmaktadır. Dolayısıyla elde edilen görüntü kalitesinde bozulma olmaktadır. AKD' si alınan görüntü elde edilirken şekilde gösterebilmek için ters AKD fonksiyonu kullanılmaktadır [172]. Önerilen yöntem içerisinde çerçeve bloklarının ortalamalarının AKD' si alınarak, AKD sonuçları özellik vektörü olarak kullanılmaktadır.



(a)



(b)

Şekil 2. 18. (a) Orijinal görüntü (b) AKD uygulanan görüntü

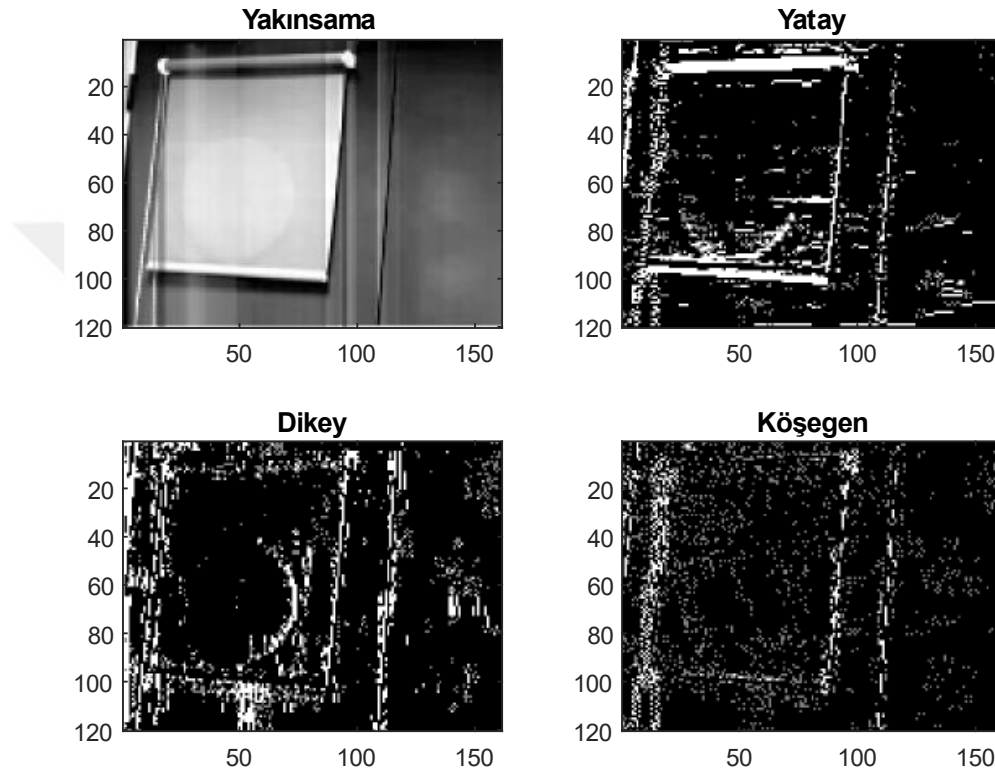
2.2.1.2. ADD Algoritması

Dalgacık Dönüşümü, zaman frekans analizi yapan istatistiksel bir yöntemdir. Mallat tarafından önerilen Ayrık Dalgacık Dönüşümü görüntüye uygulandığında hem uzamsal hem de frekans bilgisinin edinimini sağlar [173]. ADD işlenmiş görüntünün çok seviyeli ayrıştırılmasını sağlayarak ayırt edici özneliklerin verimli şekilde çıkarılmasını sağlar. Yüksek ve alçak geçişli filtreler uygulayarak girdi sinyallerini alt bileşenlerine ayırır. Alçak geçiren filtre görüntünün yaklaşık bilgilerini ve düzgün renk değişimlerini, yüksek geçiren filtre keskin değişimlerin olduğu kenar gibi detayları çıkarır. Filtreden çıkan katsayıların örnek sayısı, alt örnekleme yapıldığından yarıya düşmektedir.

Görüntü için kullanılan 2 boyutlu ADD tek boyutlu durumda kullanıldığı gibidir [174]. İki boyutlu ADD girdi görüntüsünü dört alt banda ayırır. Bunlar j seviyesinde katsayıların üç bileşeni ve $j+1$ seviyesindeki yaklaşımdır. Yatay ve dikey yönlerde düşük frekans bileşeni LL (cA-girdi resminin daha küçük ölçekli formunu), yatay yönde düşük frekans bileşeni ve dikey yönde yüksek frekans bileşeni LH (cV-Vertical), yatay yönde yüksek frekans bileşeni ve dikey yönde düşük frekans bileşeni HL (cH-Horizontal) ve son olarak da her iki yönde yüksek frekans bileşeni HH (cD-Diagonal) şeklinde çıktılar üretilir. Şekil 2.19.' da veri tabanından alınan video 8' e ait dönüşüm görsel Matlab çıktıları verilmiştir. ADD görüntülerin çok seviyeli gösterimini sağladığı için özneliklerin detaylı

incelenebilmesini sağlamakta ve ayırt ediciliğini artırmaktadır. Küçük bir parça ile görüntünün temsil edilmesi tüm görüntünün kullanılmasından daha avantajlıdır.

Ayrıca dönüşüm kodlamaları görüntülerin katsayılar aracılığıyla temsil edilmesini sağlamakta ve bu sayede görüntü elemanları arasındaki korelasyon azaltılarak fazla bilginin devamlı kodlanmasına gerek duyulmamaktadır.



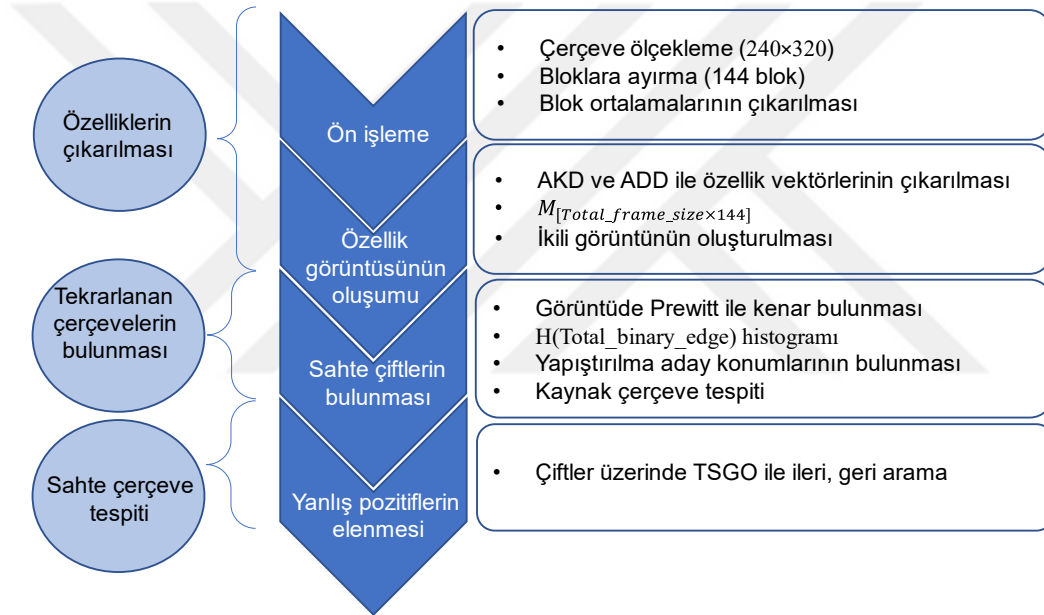
Şekil 2. 19. Veri tabanından alınan gri bir görüntüye ait ADD dönüşümün görsel sonuçları

2.2.1.3. Frekans Düzlemine Dayalı Önerilen Yöntem

Önerilen yöntem, tekrarlama sahteciliği yapılan videoların son işlem ataklarından olan sıkıştırma ve bulanıklaştırma işlemlerine dayanıklı olması için geliştirilmiştir. Yöntem, ön işleme ve öznitelik görüntüsünün oluşumu ile özniteliklerin çıkarılması, sahte çiftlerin bulunması ile tekrarlanan çerçevelerin bulunması ve yanlış pozitiflerin elenmesi ile sahte çerçevelerin tespiti olarak üç kısımdan oluşmaktadır. Öznitelik vektörlerinin oluşumunda AKD ve ADD algoritmaları kullanılmaktadır. Bu öznitelik vektörlerinin çerçeve numaralarına göre alt alta sıralanmasıyla ikili görüntüler oluşturulmaktadır. Bu

görüntüler üzerindeki düzensiz noktaları bulmak için kenar bulma algoritmaları kullanılmaktadır. Düzensiz bölgeler üzerinde tekrarlanan çerçeveler ve kaynak çerçeveler eşler halinde tespit edilmektedir. Son aşamada da eşleşen çiftler üzerinde ileri geri arama yapılmaktadır. Düzensiz bölgeler, video dosyasında yapılmış olabilecek kurcalama işlemlerinin izlerini göstermektedir. Video içerisinde sahte çerçeveye ait eşleşen çerçeve, kaynak çerçeve olarak adlandırılmaktadır.

Yöntem içerisinde elde edilen özniteliklerden ikili görüntü oluşturularak, görüntüde bulunan kenarların sahte bölgelerinde bulunmasında kullanılması yöntemine ait özgün değeri vermektedir.



Şekil 2. 20. Frekans düzlemine dayalı tekrarlama sahteciliği tespit çalışması genel adımları

Yöntem hem kaynak çerçevelerin hem de tekrarlanan çerçevelerin tespitini gerçekleştirmektedir. Yöntemin aşamaları aşağıda adım adım anlatılmıştır.

1. Çerçeveler KYM uzayından gri renk uzayına dönüştürülür. Çerçeve boyutları ($N_c \times M_c$); örneğin 240×320 olacak şekilde ölçeklenir. Her bir çerçeve örtüşmeyen 144 bloğa ($N_b \times M_b$) ayrılır. Şekil 2.21.'de bu aşama SULFA veri tabanından alınan video çerçevesine ait görsel üzerinden örneklendirilmektedir. Elde edilen blok sayısına ait denklem Eşitlik 2.27' de gösterildiği gibidir.

$$\text{Blok_sayısı} = (N_c/N_b) \times (M_c/M_b) \quad (2.27)$$

Girdi görüntülerini elde edilen videoların her bir karesi bloklara ayrılarak bir sonraki adımda blokların ortalaması alınır.



Şekil 2. 21. Renkli görüntülerin gri seviyeye dönüştürülmesi ve bloklara ayrılması

2. Blokların ortalaması (μ) alınır ve elde edilen vektörlere (V) AKD veya ADD fonksiyonu uygulanır ve elde edilen öznitelik vektörlerinin alt alta sıralanması ile tüm çerçevelerin özniteliklerinden $M_{[Toplam_çerçeve_sayısı \times 144]}$ boyutlu görüntü oluşturulur. Şekil 2.23 (a) ile oluşturulan ikili görüntünün yatayda boyutu 144 olup her bir çerçeveden elde edilen özniteliklerin sıralamasıdır. Düşeyde toplam çerçeve sayısı kadar boyutu vardır. Eşitlik 2.28' de μ_b ile her bloğa ait ortalama, V_i ile de her çerçeveye ait öznitelik vektörleri gösterilmektedir. Buraya kadar olan aşamada ilgili videodan görüntü şeklinde öznitelik çıkarılmıştır. Bir sonraki aşamada tekrarlanan çerçevelerin bulunması için algoritmanın ikinci aşamasına geçilmektedir.

$$V_i = \text{fonksiyon_AKD} \forall (\mu_1, \dots, \mu_{144}) \quad (2.28)$$

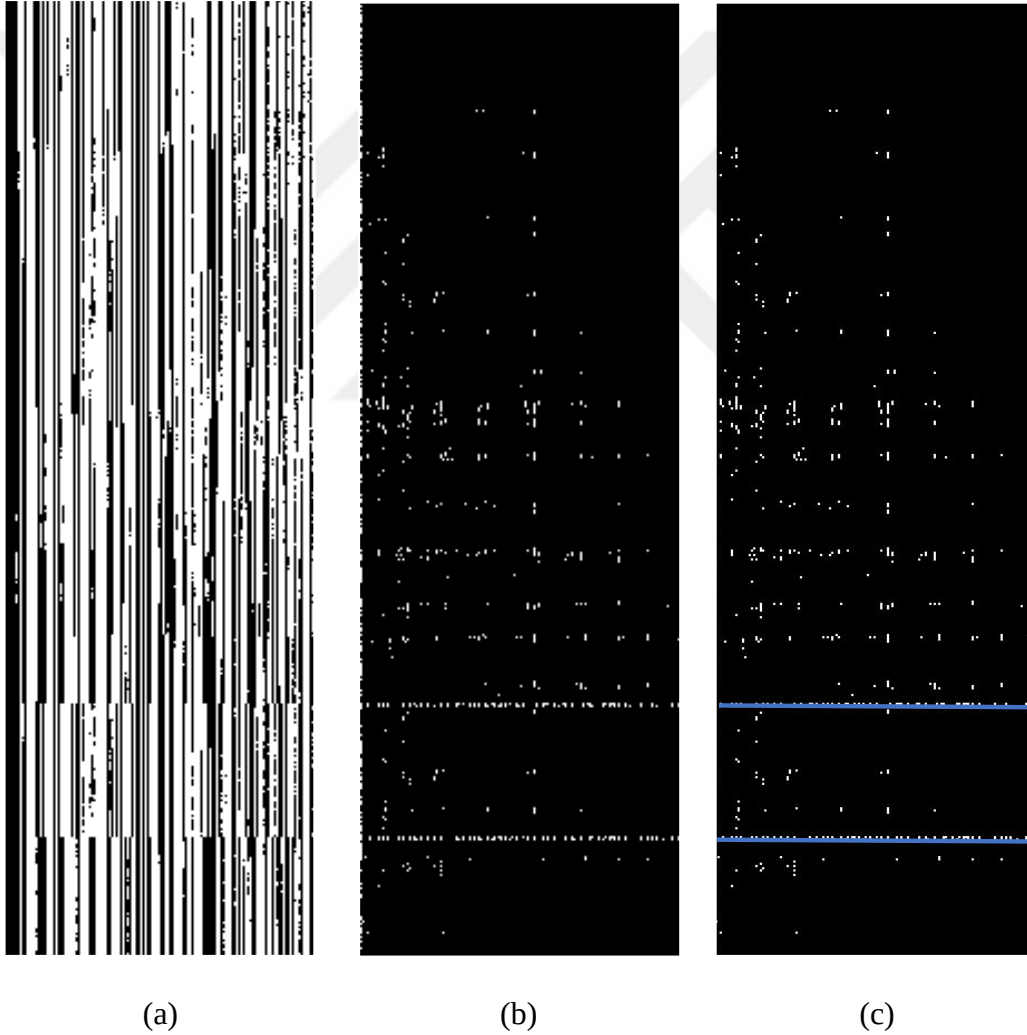
$$M_{[Toplam_çerçeve_sayısı \times 144]} = [V_1 \dots V_{çerçeve_sayısı}]$$

3. "M" Görüntüsü ikili hale dönüştürülür ve sahteciliğin yapıldığı yerdeki aykırı çizgiler yatay yönde Prewitt algoritması ile bulunur. Kullanılan Prewitt Algoritmasına ait filtreler Şekil 2.22.' de gösterildiği gibidir. Şekil 2.23. (b)' de

Prewitt algoritmasından geçirilmiş ikili görüntünün görseli verilmektedir. Kenar kısımları mavi ile Şekil 2.23. (c)' de belirginleştirmek amacıyla gösterilmektedir.

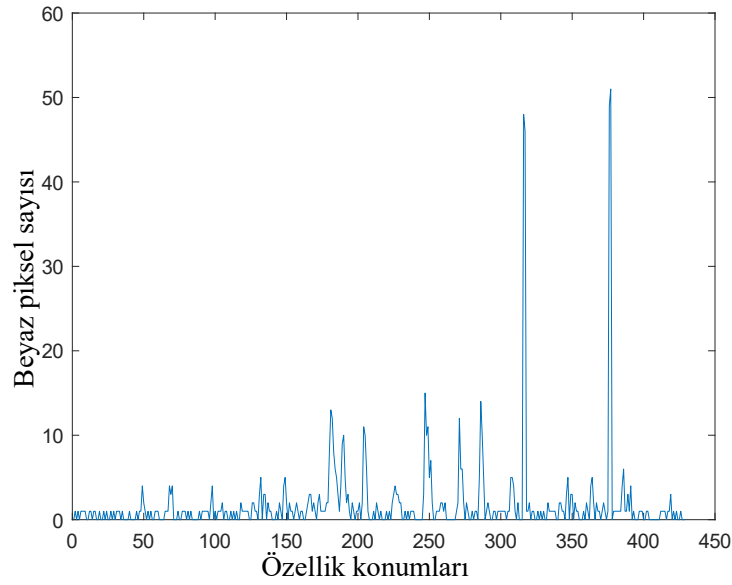
-1	0	+1	+1	+1	+1
-1	0	+1	0	0	0
-1	0	+1	-1	-1	-1

Şekil 2. 22. x ve y yönünde uygulanan Prewitt algoritması filtreleri



Şekil 2. 23. Ayırt edici öznelitliklerin görselleştirilmesi (a) Elde edilen "M" görüntüsü (b) Prewitt' li ikili görüntü (c) Prewitt Algoritması sonrasında elde edilen kenar çizgileri

4. İkili görüntü üzerinde çizginin olduğu yerlerde 1'lerin toplam sayısına göre $H(\text{Total_binary_edge})$ bir histogram çizdirilir ve buradaki zirve değerleri 20 çerçeve farkla çizdirilir. Şekil 2.24' de histograma ait görsel örnek görsel verilmiştir. Görselde y eksenini 1'lerin toplam sayısını, x eksenini ise çerçeve sayısının 20 eksiğini göstermektedir.



Şekil 2. 24. Öznitelik görüntüsündeki 1 değerli piksellerin histogramı

5. Sonrasında yapııştırılma konumu adayları olarak elde edilen tepe değerlerinin ($f(x)$) standart sapma ve ortalamaları hesaplanmaktadır. Ortalama değerinden ($\mu_{f(x)}$), bir standart sapma ($\sigma_{f(x)}$) kadar büyük olan tüm pik konumları yapııştırılma konumu adaylarına ($C(y)$) dahil edilmektedir.

```

f(x) = [x1, x2, x3, ..., xn]
for i=1: n
    if xi > μf(x) + σf(x)
        C(y) = loc(xi)
    end

```

Şekil 2. 25. Yapııştırılma konumunun tespiti için otomatik eşik belirleme

6. Elde edilen aday pik değerlerinden hangisinin yapılan sahteciliğin konumu olduğu Şekil 2.26.'daki gibi belirlenir. Burada r_i sıradaki satırı, t seçilecek grup boyutunu ifade etmektedir. Aday yapıştırılma konumları da y_k değerleridir. Bu işlem için her pikin t adet komşuluğu alınarak daha önce oluşturulmuş olan öznitelik matrisi içerisinde arama yapılır. Arama sonucu eşleşme oranları birer listede tutulmaktadır. Her bir listenin maksimum değerleri elde edilir. Maksimum değerlerin kıyaslanması sonucunda en büyük değere sahip liste sahtecilik içeren liste olarak belirlenir. Bu listenin oluşturulmasında kullanılan pik değeri de sahteciliğin yapıldığı konumlardan biridir. Arama işlemi esnasında, pikin yakın olduğu konumlardaki korelasyon değerleri çok yüksek çıkacaktır. Ancak bu noktalar eşleşen noktalar olamayacağı için maksimum değer araması yapılırken, değerlendirilmeye alınmazlar.

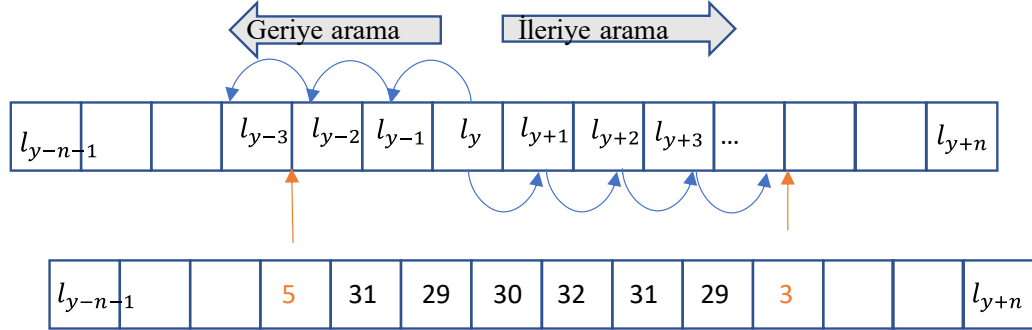
$$C(y) = [y_1, y_2, \dots, y_k]$$

Her bir aday için:
 $korelasyon([y_k: y_k + t], [r_i: r_i + t])$

Şekil 2. 26. Gruplar arasındaki ilişkinin korelasyonları incelenerek değerlendirilmesi

7. Seçilen yapıştırma konumunun karşılık değeri aranır. Bu aşamada seçilen yapıştırma konumundaki çerçeve, videodaki tüm çerçeveler ile kıyaslanır. Çerçeve kıyaslama için YBM değerlendirmesi kullanılmaktadır. Yapıştırma konumunun 30 çerçeve yakınındaki bölgeler değerlendirmeye alınmaz. En yüksek eşleştirme değerine sahip çerçeve, yapıştırılan konumun kopyalandığı yer olarak seçilmektedir.
8. Bu aşamaya kadar hem kopyalama hem de yapıştırma bölgelerine ait çerçeve konumları belirlenmiştir. Bu yapıştırma konumu etrafında sahte kaç adet çerçeve daha bulunduğu incelenmelidir. Bu amaçla seçilen yapıştırma konumunun öncesindeki ve sonrasındaki çerçevelere bakılır. Burada yapıştırmanın başlangıç ve bitiş konumlarında bitişik çerçevelerle benzerliklerinin ani düşüşünden faydalanılır. Dolayısıyla yapıştırma konumundan itibaren bitişik çerçevelerle TSGO

kıyaslamaları yapılır. Eğer ani bir değer düşüşü yoksa bu konum da sahte çerçeveler grubuna dahil edilir.



Şekil 2. 27. Sahteciliğe aday çerçeveler içerisinde yanlış pozitiflerin elenmesi

Kopyalama konumu da kopya çerçevenin bitişiğindeki çerçeve olarak belirlenir. Ani değer düşüşü varsa tüm sahte çerçevelerin bulunduğu kabul edilir. Bu arama işlemi Şekil 2.27.' deki gibi hem ileri hem de geri yönlü olarak yapılır. Böylece hem yapıştırma noktasından önceki hem de sonraki sahte çerçeveler tespit edilmiş olur.

Yöntem kaynak çerçevelerin bulunmasını ve tekrarlama sahteciliğinin tespitini yüksek doğruluk oranı ile gerçekleştirmektedir. Elde edilen sonuçlar görüntülerin blok boyutuna, bulanıklaştırma, kodek türü, kalite oranı gibi sıkıştırma etkenlerine, videoların hareketli ve sabit kamera ile çekilmiş olması gibi birçok alternatif yönünden değerlendirilmiştir. Yöntemin sonuçları Bölüm 3.3.3.' de verilmektedir.

2.3. Çerçeveler Arası Tüm Sahteciliklerin Tespit Yöntemi

Tezin bu aşamasına kadar olan bölümlerde tekrarlama sahteciliğine çözüm bulunmaya ve bu çözümlerin son işlem ataklarına karşı dayanıklılıklarının artırılmasına çalışılmıştır. Bundan sonraki aşamalarda ise sadece tekrarlama sahteciliği değil literatürde bahsi geçen çerçeveler arası tüm sahteciliklere çözüm bulunması amaçlanmıştır.

İlk olarak çerçevelerden çıkarılan özniteliklerin histogramındaki ani sapma değerlerinin incelenmesine dayalı silme sahteciliği tespiti gerçekleştirilmiştir. Silme sahteciliğinin tespiti üzerine yapılan çalışmalar çıkarılan öznitelik histogramlarındaki belirlenen eşiği geçen tepe noktalarının sayısının tek olmasına dayalı tespit

gerçekleştirmektedir. Burada eşik değerinin mevcut veri tabanlarına göre statik belirlenmesi yöntemlerin genelleştirilmesi problemini ortaya çıkarmaktadır.

Tek sayıda silme sahteciliği dışında videolarda birden fazla sayıda silme sahteciliği de yapılabilir veya tekrarlama sahtecilikleri video dizilerinin başında ya da sonunda gerçekleştirilebilir; bu durumlarda tek sayıda tepe noktasının incelenmesi en önemli ikinci problem olarak ortaya çıkmaktadır. Bu problemlerinden üstesinden gelmek ve videolarda gerçekleştirilen çerçeveler arası diğer sahteciliklerinde türünü tespit edebilmek için diğer bir yöntem geliştirilmiştir. Bu yöntem anomali tespitine dayalı, ayırt edici öznitelikler kullanılarak, çerçeveler arası farklı tür sahteciliklere çözüm sunulabilecek şekilde geliştirilmiştir. PYGH algoritmasına dayalı öznitelik çıkarılarak tüm sahteciliklere çözüm bulunması bu doğrultuda literatüre katkı sağlanmıştır. Önerilen yöntemin sıkıştırma ataklarına karşı dayanıklılığını artırmak amacıyla PYGH algoritması uygulanmadan önce video çerçevelerine ADD dönüşümü uygulanarak da ikinci bir yaklaşım sunulmuş ve kıyaslamaları karşılaştırmalı olarak verilmiştir.

2.3.1. Silme Sahteciliği Tespiti

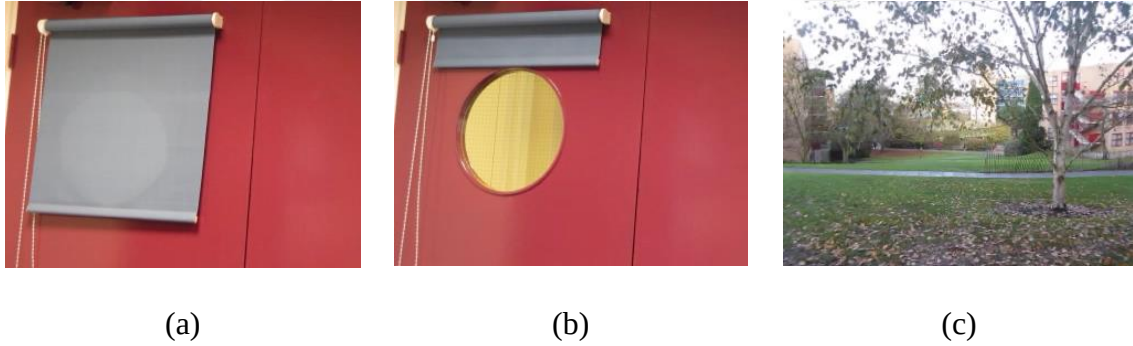
Çerçeveler arası sahtecilikler içerisinde olayların kapatılması için kullanılan en kolay sahtecilik türlerinden olması, silme sahteciliğinin tespiti üzerine yapılan çalışmalarında sayısını artırmıştır. Silme sahteciliği videoda geçen olayın gösterilmemesi için çerçevelerinin video dizisinden atılması sağlanmaktadır. Silme işlemi ya olayın başlangıcından sonuna kadar olan tüm sahnenin silinmesi ya da sadece ilgili hareketin silinmesi şeklinde gerçekleştirilmektedir. Tüm sahnenin silinmesi RGY' nin katları şeklinde silmeye neden olmaktadır. Bu da yapılan sahtecilik işleminin bulunmasını zorlaştırmaktadır. Bu çalışma ile de silme sahteciliğinin yapıldığı konum, TSGO algoritmasına dayalı olarak tespit edilmektedir. Yöntemde kullanılan TSGO algoritmasından Bölüm 2.3.1.1'de, yöntemin detaylarından ise Bölüm 2.3.1.2'de bahsedilmektedir. Silme sahteciliklerinin tespitine yönelik hızlı bir çözüm üretmenin amaçlandığı yöntemde farklı sıkıştırma formatlarında ve kalite oranlarında rastgele konumlarda sahtecilik yapılan videolar üzerinden testler gerçekleştirilmektedir. Sahtecilik yapılan çerçeve sayısı 50 çerçeveden başlanarak 10 çerçeveye kadar düşürülmekte ve rastgele konumlarda sahtecilik yapılarak algoritmanın dayanıklılığı test edilmektedir.

2.3.1.1. Tepe Sinyal Gürültü Oranı

Tepe Sinyal Gürültü Oranı (TSGO), iki farklı görüntü arasındaki kalite etkisinin, kaliteyi etkileyen hata gürültüsü arasındaki oranı hesaplamak için kullanılmaktadır. Bu ölçüt ile iki görüntünün birbirine ne kadar benzediği hesaplanmaktadır. Yüksek olması durumu iki görüntünün daha çok benzediği anlamına gelmektedir. Eşitlik 2.29’da N ve M görüntülere ait satır ve sütun bilgisini, L maksimum parlaklık değerini, I_1 ve I_2 ise TSGO hesaplanacak iki görüntüyü temsil etmektedir.

$$TSGO = 10x \log_{10} \left(\frac{L^2}{\frac{1}{M \times N} \times \sum_{i=1}^M \sum_{j=1}^N (I_1(i, j) - I_2(i, j))^2} \right) \quad (2.29)$$

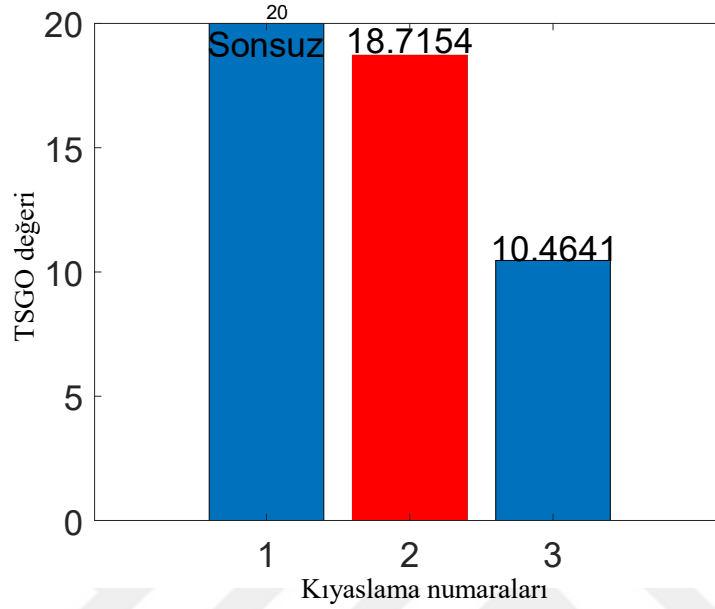
Şekil 2.28.’ de SULFA veri tabanından alınan can_220_flap (1), can_220_flap (2), can_220_garden (4) videolarına ait çerçeve örnekleri ve Şekil 2.29.’ da da bunlar arasındaki TSGO’ ları gösterilmektedir.



Şekil 2. 28. SULFA veri tabanından alınan video örnekleri(a) can_220_flap (1) videosu 61.çerçeve (b)can_220_flap (2) videosu 331.çerçeve (c) video18_can_220_garden (4) videosu 1.çerçeve

Şekil 2.29’da görüldüğü gibi birbirinin aynısı olan çerçeveler için TSGO sonsuz çıkarken birbirinden bağımsız çerçeveler için TSGO düşmektedir. Şekil 2.29.’ da 1 numaralı sonsuz olan sütun: Şekil 2. 28. (a)’ daki görselin kendisiyle kıyaslamasını, 2. Sütun: Şekil 2.28. (a) ile Şekil 2.28. (b)’deki görsellerin kıyaslanmasını, 3. sütun da: Şekil 2.28. (a) ile Şekil 2.28. (c)’ deki görsellerin TSGO kıyaslamalarını göstermektedir.

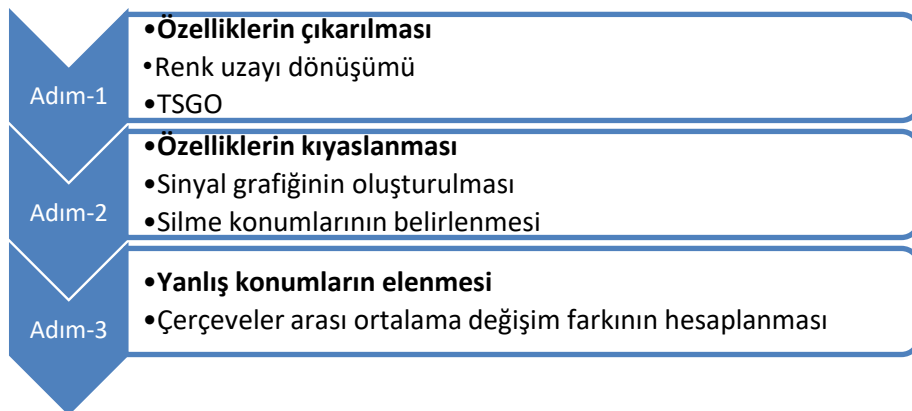
Dolayısıyla silme işleminin yapıldığı bir videoda ardışık çerçevelerin TSGO' larında değişim olması beklenmektedir.



Şekil 2. 29. Çerçevelere ait TSGO' larının kıyaslanması

2.3.1.2. TSGO' ya Dayalı Silme Sahteciliği Tespit Yöntemi

Silme sahteciliğinin tespit performansı yapılan sahteciliğin konumunun bulunmasına göre gerçekleştirilmiştir.



Şekil 2. 30. Silme sahteciliği tespit algoritmasının genel adımları

Yöntem içinde kullanılan videoların tamamının sahte olduğu varsayılmış ve hangi konumda sahtecilik yapıldığının üzerine çalışılmıştır. Yöntemin işlem adımları aşağıdaki gibidir. İşlem adımları Şekil 2.30.' da gösterilmektedir.

Adım 1- Özniteliklerin çıkarılması:

- Video çerçeveleri gri renk uzayına dönüştürülmektedir
- Ardışık çerçeveler arası TSGO hesaplanmakta ve çerçeve sayısından 1 eksik sayıda öznitelik içeren bir vektör elde edilmektedir.

Adım 2- Özniteliklerin kıyaslanması:

- Öznitelik vektörlerine ait histogram çıkarılarak, histogram içerisindeki ani değişim olan tepe noktalarının konumları silinmeye aday çerçeveler olarak belirlenir.

Adım 3- Yanlış konumların elenmesi:

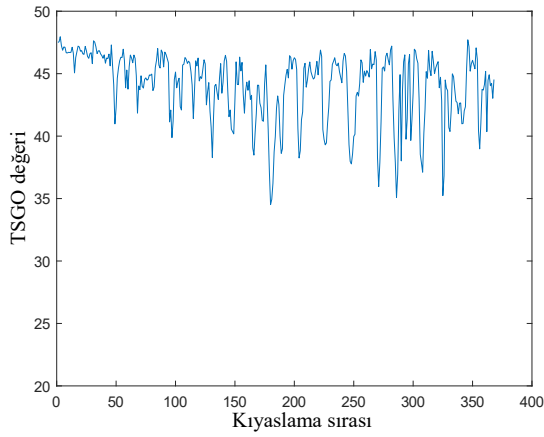
- Aday çerçevelerin bir önceki ve bir sonraki komşuları ile TSGO farkları alınarak ortalama değişimleri Eşitlik 2.30 kullanılarak hesaplanmıştır.

$$d = \frac{(TSGO(i + 1) - TSGO(i)) + (TSGO(i) - TSGO(i - 1))}{2} \quad (2.30)$$

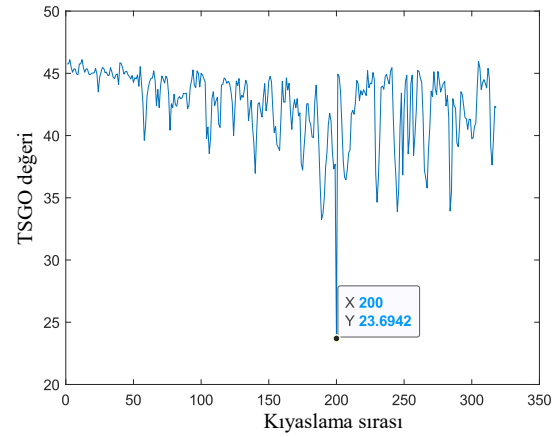
TSGO' ları arasındaki değişim eşik değerinden büyükse aday çerçeveler arasında bulunan ilgili çerçeve, silmenin yapıldığı konum olarak tespit edilmiştir. Eşik değerinden büyük değilse en düşük TSGO değerine sahip çerçeve silmenin yapıldığı yer olarak bulunmuştur.

Yöntem içerisinde çerçeveler arasındaki benzerlik ilişkisini ölçmek için kullanılan TSGO değeri iki görüntü aynı olduğunda sonsuz değer almaktadır. Kullanılan videolar içerisinde birbirini bir kere tekrarlayan bazı çerçeveler olduğu anlaşılmış ve TSGO sonsuz çıkan bu tarz çerçevelerin değişimleri olmadığı düşünülerek, değişim vektöründeki değerlerine sıfır atanmıştır.

Orijinal videoda çerçevelerin TSGO değerleri birbirine çok yakındır. Silinen çerçeveler aradan çıktığında art arda gelen çerçeveler arasında oluşan tepe noktasının minimum olmasının nedeni benzerliklerinin az olmasıdır. Şekil 2.31.' de orijinal ve 200 numaralı konumdan silme sahteciliği yapılan videolara ait öznitelik görüntüleri verilmektedir.



(a)



(b)

Şekil 2. 31. (a) Orijinal videoya ait öznitelik gösterimi (b) Silme sahteciliği yapılan videoya ait öznitelik gösterimi

2.3.2. Çerçeveler Arası Dört Tür Sahtecilik Tespit Yöntemi

Bu bölüme kadar tekrarlama, tekrarlanan çerçeveleri ekleme ve silme sahteciliğinin çözümüne yönelik çalışmalar anlatıldı. Çerçeveler arası diğer bir sahtecilik olan çerçeve karma ile, tek bir video içinde kopyalanan çerçevelerin konumları değiştirilerek yapıştırılma işlemi yapılmaktadır. Böylece olay akışı, tersine yapılmış izlenimi verilerek sahtecilik yapılmaktadır. Son yıllarda tespiti gerçekleştirilen bu sahtecilik türü bazı araştırmacılar tarafından tekrarlama sahteciliği olarak görülmektedir, ancak eşleşen çift grupları şeklinde arama yapan tekrarlama sahteciliği çalışmaları karma sahteciliğini tespit edememektedir. Bu çalışma ile Piramitsel Yönlendirilmiş Gradyanlar Histogramı (PYGH) algoritması kullanılarak çerçeveler arası tüm sahteciliklere çözüm sunabilen bir çalışma önerilmektedir. Bölüm 2.3.2.1' de PYGH algoritmasından, Bölüm 2.3.2.2' de önerilen yaklaşımdan bahsedilmiştir.

2.3.2.1. Piramitsel Yönlendirilmiş Gradyanlar Histogramı Algoritması

Görüntünün farklı seviyelerde alt bloklara ayrılarak, her seviyeden elde edilen özniteliklerin birleştirilmesi ile oluşturulan Yönlendirilmiş Gradyanların Histogramı (YGH) algoritması gri renkli görüntüler üzerinden çalışan doku tabanlı bir algoritmadır.

YGH algoritması görüntülerdeki şekillerin tanımlanması amacıyla kullanılmaktadır. Piramitsel Yönlendirilmiş Gradyanlar Histogramı (PYGH) algoritması farklı blok seviyelerinde uygulandığı için YGH' a kıyasla daha ayırt edici olmaktadır.

Önerilen yöntem içerisinde iki seviyeli YGH algoritması kullanılmıştır. Sahtecilik tespiti çalışmalarında PYGH algoritması daha önce kullanılmamıştır. Eşitlik 2.31 ve Eşitlik 2.32 ile yatay ve düşey yönde F çerçevesi üzerinde her bir noktanın Sobel filtreleri kullanılarak gradyan değerleri hesaplanır. Eşitlik 2.33' de m ile gradyanların büyüklüğü, Eşitlik 2.34' de Q ile gradyanın açısı hesaplanır. 180 ile 360 dereceler arasındaki açı değerleri 8 eşit parçaya bölünerek her parçanın ait olduğu açı değerine göre gradyan büyüklüğü eklenerek histogramı çıkarılır. En son aşamada da blok içerisinde oluşturulan tüm değerlerin birleştirilmesi ile elde edilen histogramın normalizasyon gerçekleştirilir.

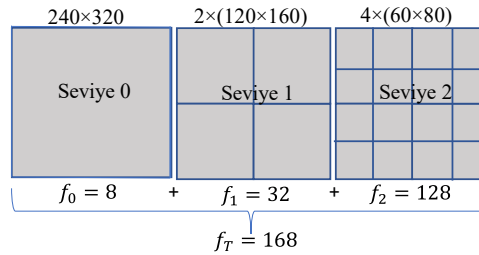
$$g_x(x, y) = F(x + 1, y) - F(x - 1, y) \quad (2.31)$$

$$g_y(x, y) = F(x, y + 1) - F(x, y - 1) \quad (2.32)$$

$$m(x, y) = \sqrt{g_x(x, y)^2 + g_y(x, y)^2} \quad (2.33)$$

$$Q(x, y) = \arctan \frac{g_x(x, y)}{g_y(x, y)} \quad (2.34)$$

PYGH algoritması girdi olarak verilen görüntünün şekilsel özelliğini döndürmektedir. İlk olarak seviye sıfırda tüm çerçeveye $[240 \times 320]$ YGH uygulanarak $f_0 = 8$ tane öznitelik çıkarılır. Sonrasında seviye bire yani çerçevenin dörde bölünmüş halinden, her bloktan 8 öznitelik çıkaracak şekilde $4 \times 8 = f_1 = 32$ öznitelik çıkarılır. En son seviye üzerinden yani görüntünün on altı eş parçasından $16 \times 8 = f_2 = 128$ öznitelik çıkarılır. Şekil 2.32.' de görüldüğü gibi çıktı olarak 1×168 boyutlu vektörler elde edilir.

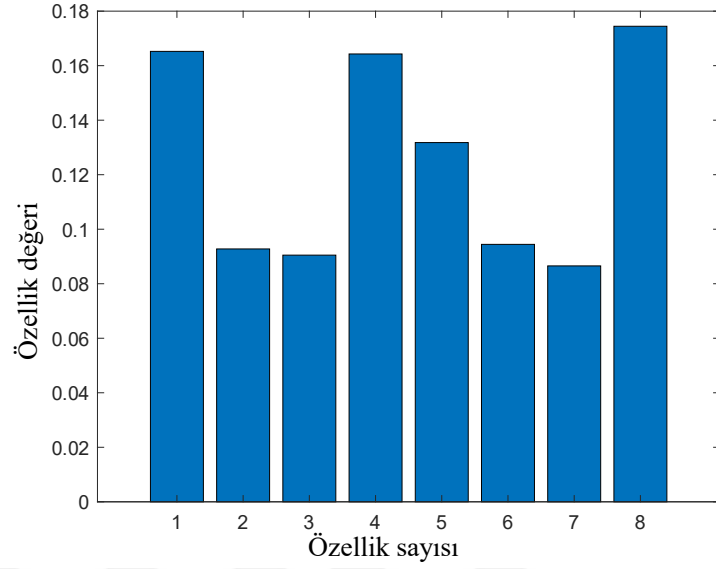


Şekil 2. 32. PYGH algoritması ile öznitelik çıkarımı

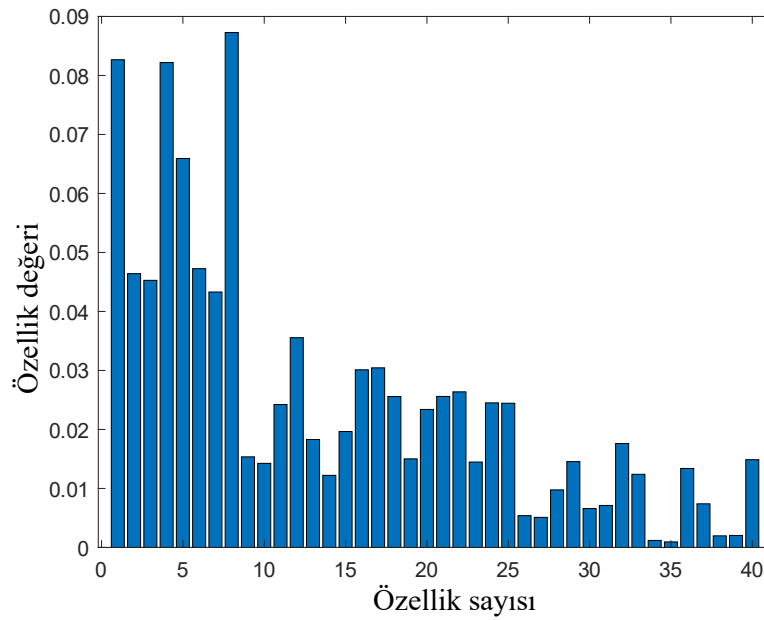
Şekil 2.33.' de SULFA veri tabanından alınan nık_s3000_bridge (1) isimli videonun 1 numaralı çerçevesinden elde edilen üç farklı seviye için çubuk diyagramları gösterilmektedir.



(a)



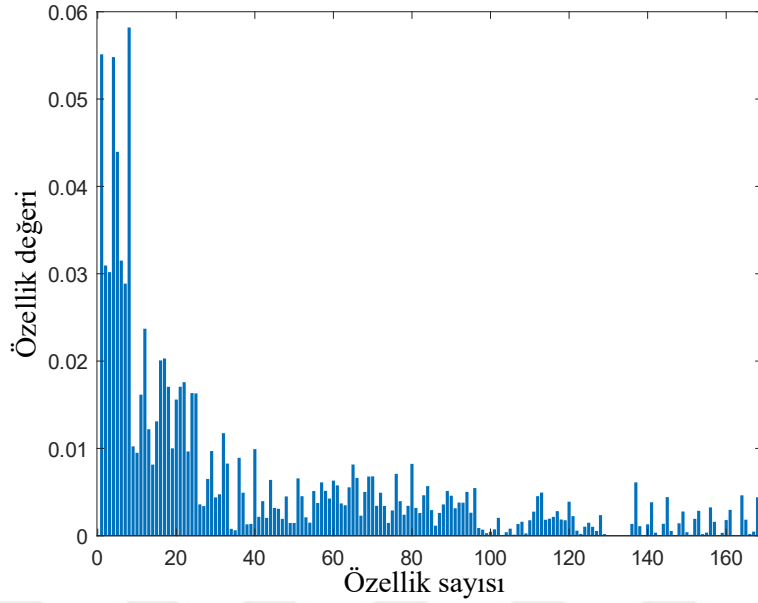
(b)



(c)

Şekil 2. 33. “(a) nık_s3000_bridge (1)” videosu çerçeve görüntüsü (b) Seviye-0 için histogram (c) Seviye-1 için histogram (d) Seviye-2 için histogram

Şekil 2.33.' ün devamı



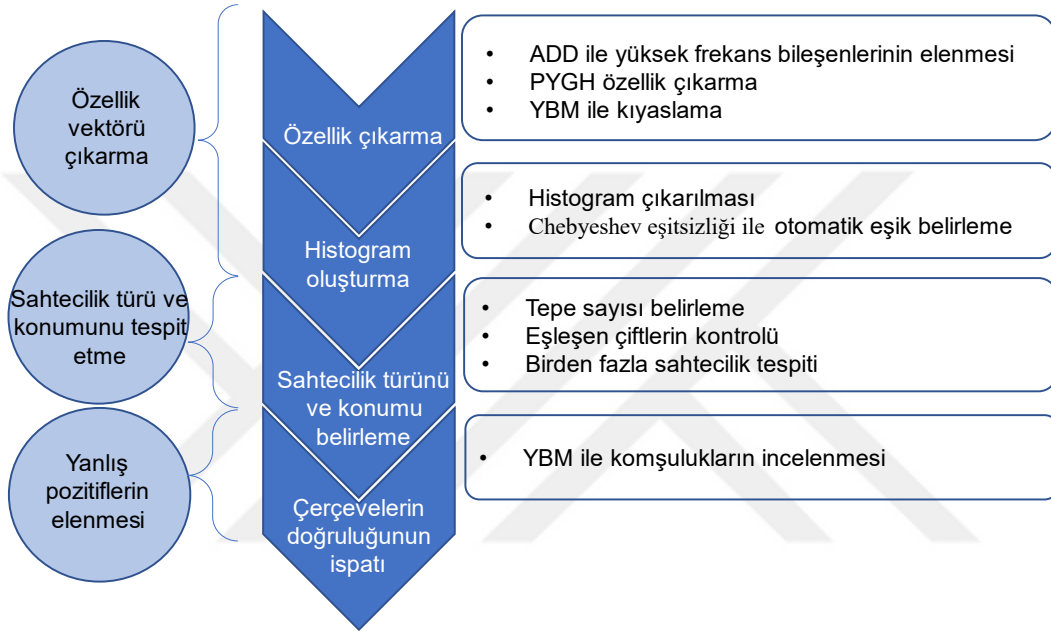
(d)

Yatay eksenler özellik sayısını, dikey eksenler özelliklerin değerlerini ifade etmektedir. Seviye 0 için 8 öznitelik, seviye 1 için toplamda $8 + 32 = 40$ öznitelik, seviye 2 için toplamda $40 + 128 = 168$ elde edilmektedir.

2.3.2.2. Çerçeveler Arası Dört Sahteciliğe Çözüm Sunulan Yaklaşım

Zamansal boyutta yapılan sahteciliklerin tamamı için çözüm sunulan bu çalışma ile ilk olarak yapılan kurcalama işlemlerinde akıştan alınan görüntülerden nasıl öznitelik çıkarımı yapıldığını ve bu özniteliklerin birbirleriyle nasıl kıyaslandığı açıklanmaktadır. Yöntemde dört farklı çerçeve kurcalama sahteciliği, literatürde bahsi geçen üç farklı veri tabanı ve Web-test üzerinden test edilerek denenmiştir. Bu çalışmanın katkısı, yapılan sahteciliklerin sayısının birden fazla olması durumunda çözüm sunabilmekte ve literatürdeki çalışmalardan farklı olarak her sahtecilik işlemi kendi içinde tek tek incelenmektedir. Şüpheli çerçevelerin, komşulukları ile ilişkileri incelenmektedir. Örneğin bir videoda iki kere silme işlemi yapılabilir veya diğer çerçeveler arası sahtecilik türlerinden biri aynı anda olabilir şeklinde diğer çerçeveler arası sahtecilikleri de test edecek şekilde algoritma koşulmaktadır. Yöntemin çalışma prensibine ait çalışma adımları Şekil 2.34.' de gösterildiği gibi öznitelik vektörünün oluşturulması ve sahtecilik türü ile

konumunun tespit edilmesi son olarak da yanlış bulunan sahte çerçevelerin doğruluğunun tespiti olarak üç ana aşamadan oluşmaktadır. Yöntem ilk olarak sıkıştırılmamış videolarda test edilmiş, sonrasında sıkıştırmaya da dayanıklılığının artırılmaması için daha önceki çalışmalarda sağlanan başarılar değerlendirilerek ADD’ nin yüksek frekans bileşenleri elenerek sıkıştırılmış videolarda test edilmiş ve başarılı sonuçlar alınarak yöntemin performansı iyileştirilmiştir.



Şekil 2. 34. Çerçeveler arası sahtecilik tespit yönteminin adımları

Video sahteciliklerinin tamamına çözüm bulan yöntemlerden farklı olarak önerilen çalışmamızda elde edilen anomali noktalarının her biri ayrı ayrı incelenmektedir. Yöntem ile farklı videolardan çerçeve ekleme, çerçeve silme, çerçeve tekrarlama ve çerçeve karma şeklinde dört farklı sahtecilik tipine çözüm önerisi sunulmaktadır. Amaçlanan algoritma dört kısımdan oluşmaktadır. İlk iki aşamada video çerçevelerinin öznitelik vektörleri çıkarılmaktadır. Özniteliklerin birbirlerinden ne kadar farklı olduğunu ölçmek için ayrı ayrı YBM değerleri hesaplanmaktadır. Videolarda anormal bir durum olup olmadığı bu videolardan elde edilen sinyal grafiklerinden çıkarılan tepe noktalarına göre karar verilir. Ani oluşan bir anormallik durumuna kullanılan Chebyeshev eşitsizliği algoritması ile belirlenen eşik değeri t ile karar verilir. Eşitsizliğin hesaplanması Eşitlik 2.35 ile gösterilmektedir.

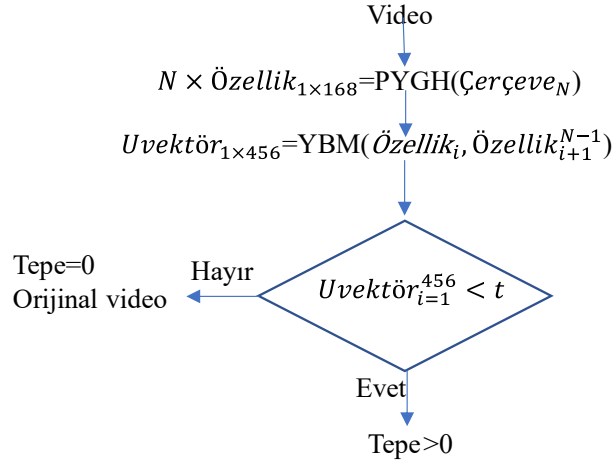
$$T_1 = \mu_1 - p_1 * \sigma_1 \quad (2.35)$$

Belirlenecek olan rastgele eşik değerinin veri kümesinde mevcut elemanlar içerisinde seçilme olasılığı $p > 0$ olmak üzere ortalama μ_1 ve standart sapmaya σ bağlı olarak bulunabilir. Bu eşitsiliğe göre eşik değeri olarak belirlenen değer olan T_1 , ortalamadan p kadar standart sapma uzaktadır. Burada kullanılan p_1 değeri de veri setinde kullanılan videolara göre belirlenmiştir.

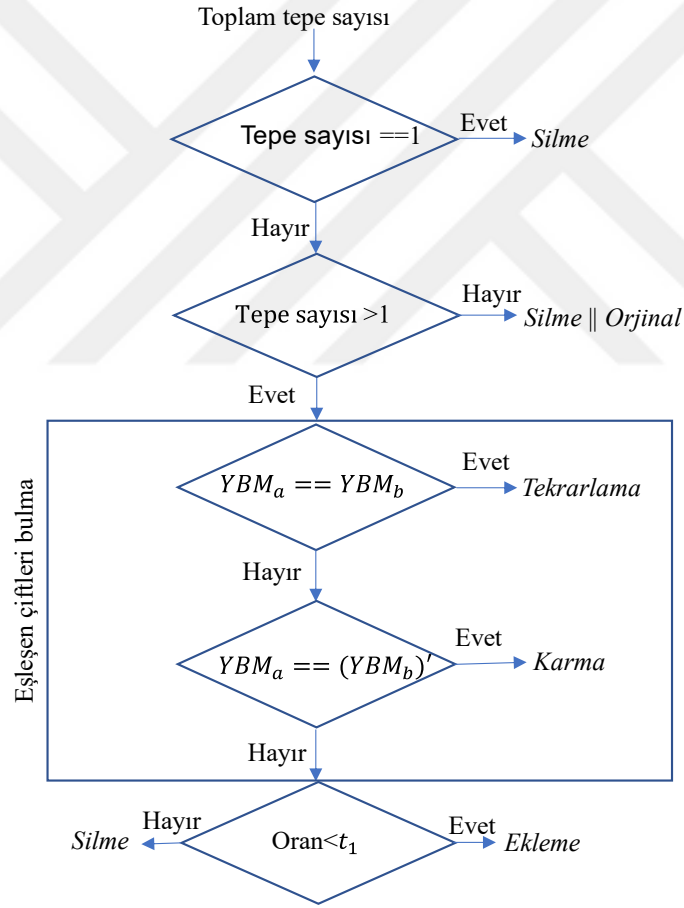
Belirlenen eşik değerinden büyük olan tepe noktaları çerçevelerin öznitelikleri arasında herhangi anormal bir durum olmadığını yani çerçevelerin orijinallik durumunu göstermektedir. Eşik değerinin altında kalan tepe noktaları ise videonun şüpheli bir video olduğunu göstermektedir. Bu çalışma ile videoların ne kadarının orijinal ne kadarının sahte olduğuna karar veren bir değerlendirme sayesinde literatüre katkı sağlanmıştır. Videoda yapılan sahteciliğin belirlenmesi için algoritmanın üçüncü aşamasına geçilmektedir.

Çalışmanın üçüncü aşamasında birden fazla aynı sahtecilik tekrar edilmiş ise yapılan sahteciliğin sayısının kontrolü yapılmaktadır. Son aşamada ise yanlış bulunan noktaların elenmesi gerçekleştirilmektedir.

Yöntem hangi tür sahtecilik yapıldığına karar verirken Şekil 2.35. (a)'daki gibi öncelikle elde edilen tepe noktalarının sayısını, sonrasında ise tepe noktalarının konumları ile çevre komşuları arasındaki ilişkiyi hesaplanmaktadır. Tepe sayısı sıfır ise video orijinaldir. Tepe noktalarının olduğu yer çerçeve özniteliklerinin değişim gösterdiği konumlar olarak değerlendirilmektedir. Şekil 2.35. (b)'de görüldüğü gibi öznitelik sinyallerinde tepe sayısı 1 ise mevcut video çerçeveleri içerisinde tepe noktasının olduğu yerde tek bir sapma olmaktadır. Tepenin komşu çerçevelerle ilişkisi incelendiğinde uzak bir ilişki varsa bu noktada silme sahteciliği bulunmaktadır; ancak aralarında yakın ilişki varsa bu durumda tepe noktası video içerisindeki nesnelerin hareketinden kaynaklanmaktadır ve orijinal video kararı verilmektedir. Ancak tepe sayısı birden fazla ise bu durumda öncelikle tekrarlama ve karma sahtecilikleri var mı şeklinde arama devam etmektedir. Eğer bu sahteciliklerden biri varsa çerçevelerin birbirleri ile eşleşmelerinin de bulunması gerekmektedir. Eğer eşleşen herhangi bir çerçevesi yoksa ekleme veya birden fazla sayıda silme yapılmış veya orijinal video olabilir. Bu yüzden elde edilen tepe noktalarının komşuluklarıyla olan ilişkileri tek tek incelenmektedir. Burada kullanılan t_1 eşikinin detaylarından Eşitlik 2.35.'de bahsedilmektedir.



(a)

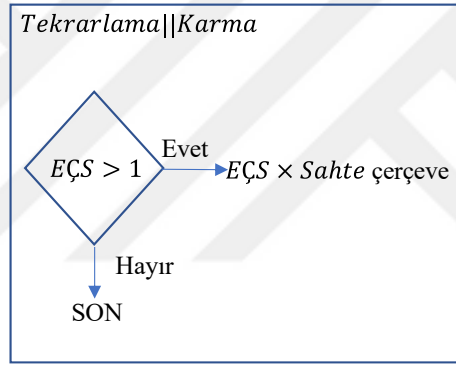


(b)

Şekil 2. 35. Hibrit yöntem için sahtecilik türünün tespiti için önerilen yöntem (a) Toplam tepe sayısının araştırılması, (b) Sahtecilik türünün belirlenmesi

Şekil 2.35 (b)' de gösterildiği gibi eşleşen çiftleri bulma kısmına girildiği zaman yani pik sayısı birden fazla ise öncelikle pik değerlerinin eşi var mı diye kontrol edilir. Eğer aynı özellikte iki çerçeve varsa bu durumda ya tekrarlama ya da karma sahteciliği yapılmış olabilir. Eşleşen çiftler varsa; bu çiftlerden önceki veya sonraki çerçevelerden de video içerisinde tekrar edilmiş demektir. Dolayısıyla yan çerçevelerde öznelik matrisinde aranır. Bulunan tepe değeri yapılan sahteciliğin sonu ya da başı olabilir. Bu nedenle de hem o konumun öncesi hem de sonrası ile eşleşme var mı diye kontrol edilir.

Eşleşme varsa bu durumda eşleşmelerin sayısı incelenmektedir. Eşleşmenin kaç tane olduğu Şekil 2.36.' daki gibi kontrol edilir. Kontrol sonucu elde edilen eşleşme sayısı kadar sahtecilik yapıldığı tespit edilir. Bu sayı Şekil 2.36.' da *EÇS* (Eşleşen Çerçeve Sayısı) ile ifade edilmiştir.

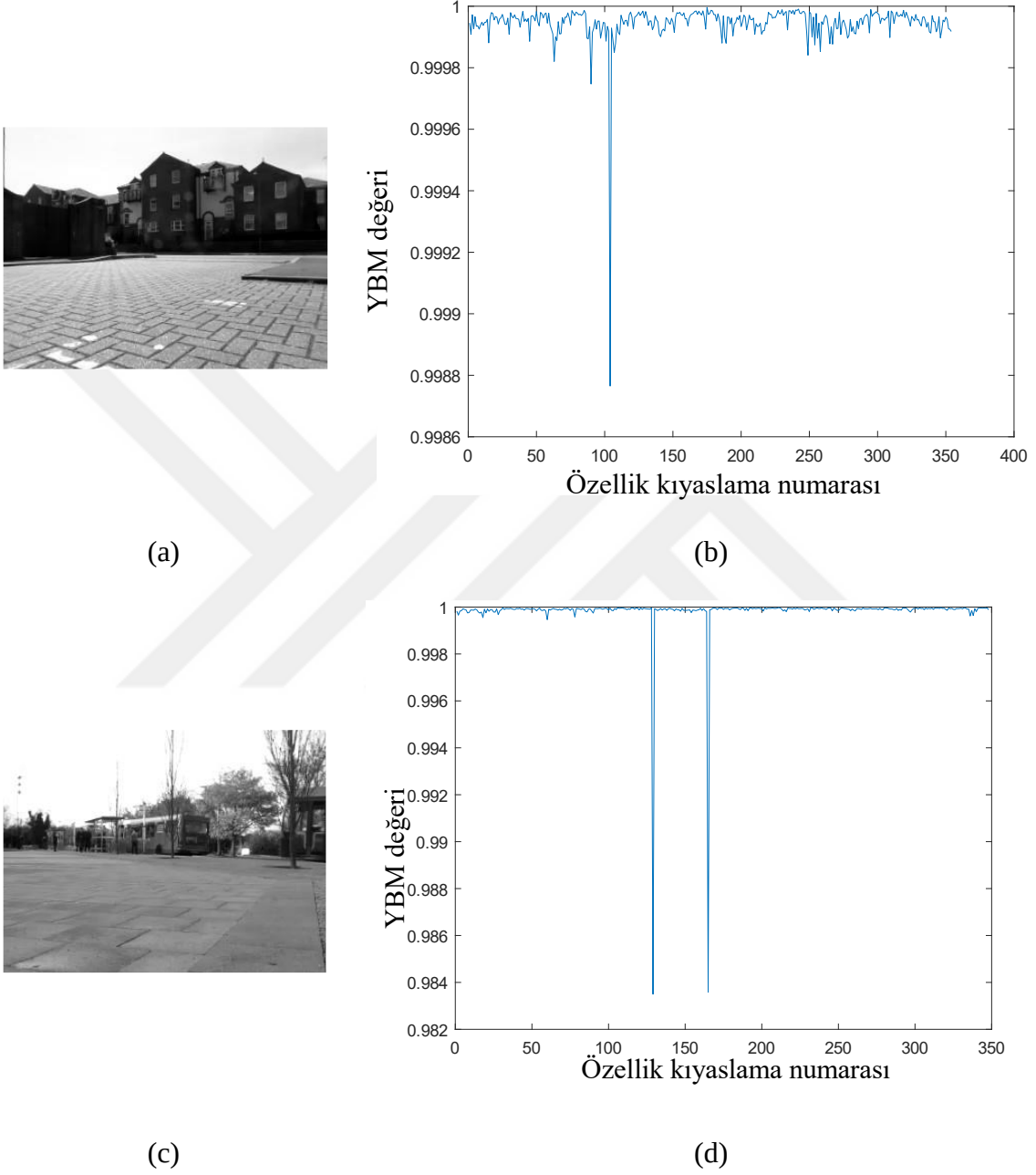


Şekil 2. 36. Eşleşen çiftlerin sayısının bulunması

Her çerçeve için eşleşme sayısı ile eşleşen çerçevelerin indeks değerleri de kontrol edilir. Eğer indeks değerlerinde sıralı bir şekilde artma veya azalma varsa “tekrarlama sahteciliği”, sıralı değil de karmaşık şekilde eşleşme varsa bu durumda da “karma sahteciliği” yargısına varılır. Eşleşme yoksa bu durumda bir sonraki aşamaya geçilir.

Fadl vd.’ nin önerdiği videolardan [126] alınan silme için V2 ve ekleme için V4 çerçeve örnekleri sırasıyla Şekil 2.37. (a) ve Şekil 2.37. (c)’ de elde edilen öznelik vektörleri çıktısı gösterilmektedir. Silme sahteciliğinde video akışı içerisinde 105 ile 110 numaralı çerçeveler arası 5 çerçevenin atılması ile geriye kalan video çerçevelerinin öznelikleri arasında farklılık Şekil 2.37. (b)’ de görüldüğü gibi tek bir noktada ani değişime neden olmaktadır. Şekilde görüldüğü gibi sadece 5 çerçeve silme işlemi hareketli

video olması dolayısıyla bu kadar ani değişime neden olurken; sabit sahneli videolarda yine değişime neden olacak fakat bu kadar bir sıçrama olması beklenmeyecektir.



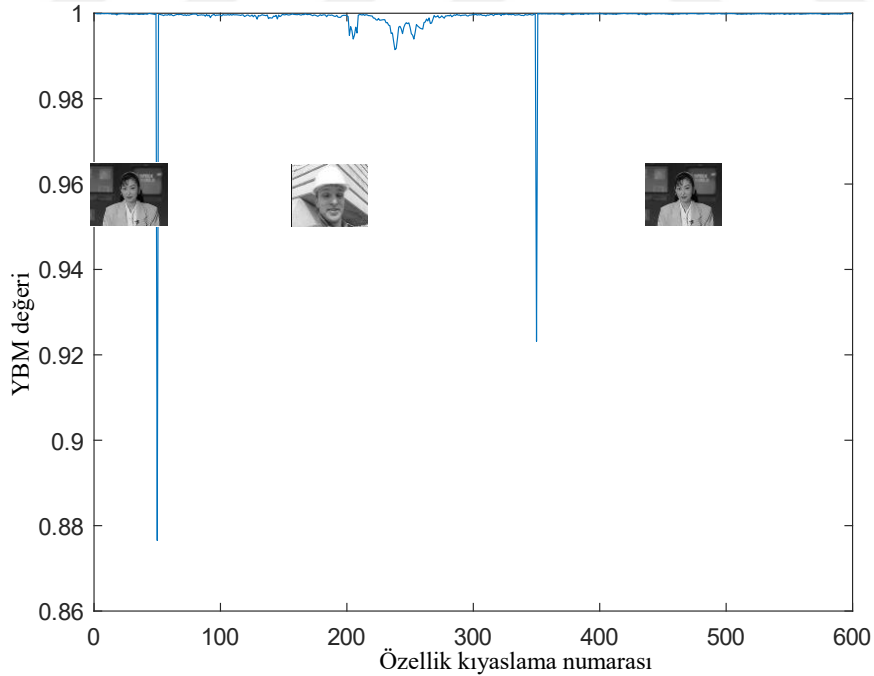
Şekil 2. 37. (a) V2 videosuna ait çerçeve örneği (b) Silme sahteciliğine ait görselin öznelilik vektörü grafiği (c) V4 videosuna ait çerçeve örneği (d) Ekleme sahteciliğine ait görsel öznelilik vektörü grafiği

Ekleme yapılan videolarda hem eklemenin yapıldığı başlangıç konumunda hem de bitiş konumunda farklılık olacağı için ani oluşum Şekil 2.37. (d)'deki gibi iki ayrı tepe

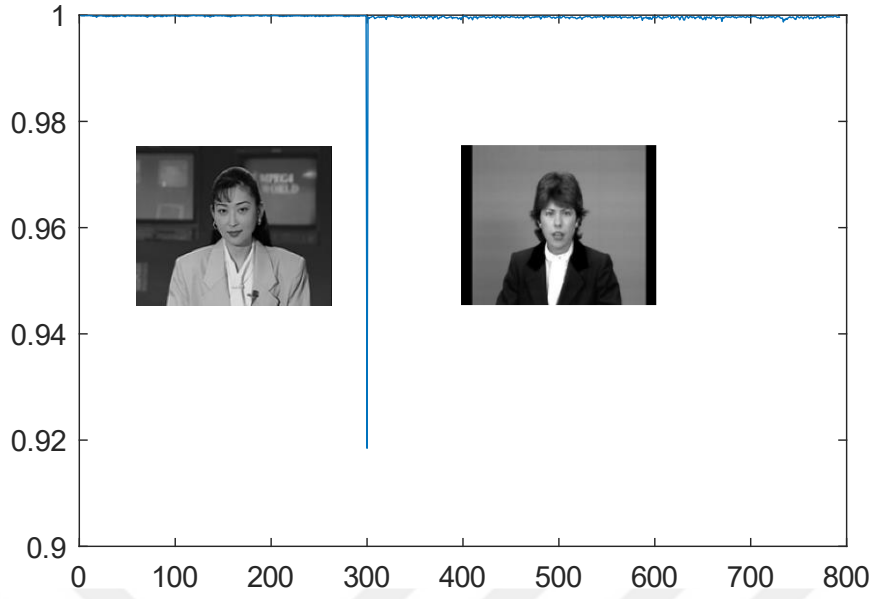
noktası oluşmasına neden olmaktadır. Bu video içerisinde 130 ile 165 arasına ekleme işlemi yapılmıştır. Algoritmanın literatürdeki diğer çalışmalardan farkı elde edilen bu iki tepe noktasının aslında ekleme değil birden fazla silme işlemi de yapılmış olabileceği veya tekrarlama ya da karma sahteciliğini de inceleyerek değerlendirme yapmasıdır. Bir sonraki örnek için yapılabilecek ekleme örnekleri gösterilmektedir.

Ekleme işlemi iki farklı videodan araya sona veya ikiden fazla videonun birleştirilmesi şeklinde yapıldığında elde edilen öznelite grafiklerinin dağılımı Şekil 2.38.' de verilmiştir.

Şekil 2.37 ideal olarak beklenen öznelite grafiği iken, Şekil 2.38., Şekil 2.39. ve Şekil 2.40. literatürde daha önce incelenmemiş olası ihtimalleri içermektedir. Literatürde yapılan ekleme sahtecilikleri genellikle aynı video içerisinde kopyalanarak yapılan ve çerçeve sayısını artıran tekrarlama sahteciliği örnekleri üzerinden test edilmektedir. Kaynak kameraların tespitine yönelik çalışmalarda bu çalışmada örneklendirildiği gibi farklı videoların birleştirilmesiyle elde edilen sahte videolar üzerinden araştırma yapılmaktadır.

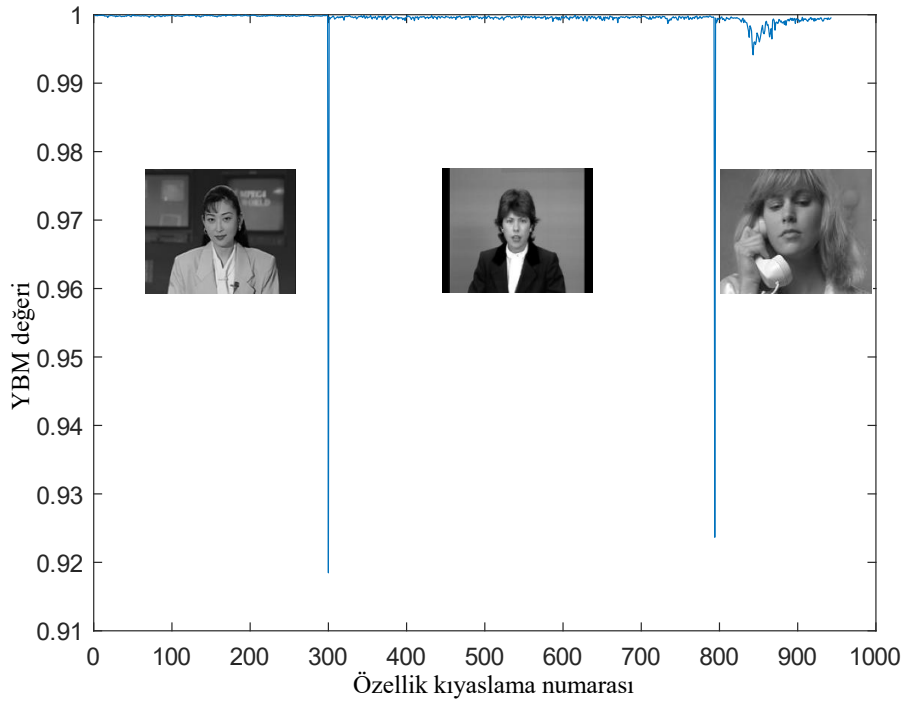


Şekil 2. 38. Ekleme sahteciliği mevcut videonun arasına yapıldığı durumda



Şekil 2. 39. Ekleme sahteciliği mevcut videonun sonuna yapıldığı durumda

Şekillerde gösterilen ihtimaller düşünüldüğünde; ekleme sahteciliği ile oluşan tepe noktası sayısı her zaman iki olmamakla beraber her iki tepe sayısının oluştuğu öznelilik vektörü sadece iki videonun birleştirilmesi ile değil, Şekil 2.39.'daki gibi iki veya Şekil 2.40.'daki daha fazla videonun birleştirilmesi ile de sağlanabilir.

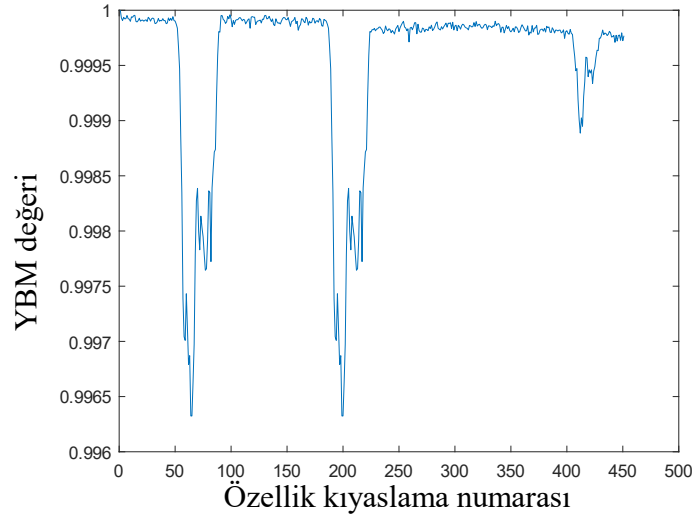


Şekil 2. 40. İki den fazla video art arda eklendiğinde elde edilen görseller

Bu çalışma geliştirilirken sadece öznitelik sinyal grafiğindeki tepe sayısı değil oluşan aday tepe noktalarının her biri ayrı ayrı incelenmektedir. Şekil 2.39. ile gösterilen iki videonun birleştirilmesi ile ekleme sahteciliğinin yapıldığının veya video sonundan yapılan silme sahteciliğinin ayrımını yapmak çok zordur. Algoritma bu tarz sahtecilik için ilgili tepe değerini silme sahteciliği olarak sonuçlandırmaktadır. Videolar ayrı ayrı sahnelerin birleştirilerek oluşturulduğu tek parça bir video gibi olmaktadır. Çünkü eklemenin yapıldığı konum ve bu konumun sonrası birbiri ile ilişkili, eklemenin yapıldığı kısım ve öncesi de yine birbiri ile ilişkili olacaktır. Algoritma sadece sahne geçişlerinden dolayı birleşim noktalarını bulabilecektir.



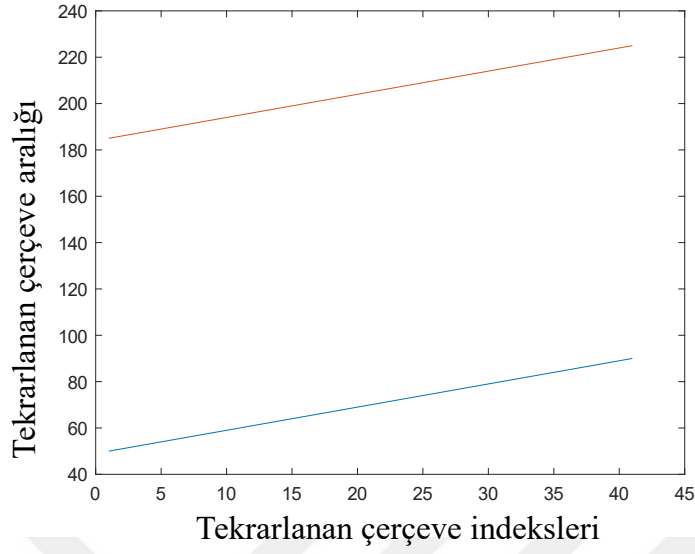
(a)



(b)

Şekil 2. 41. Tekrarlama sahteciliğinin yapıldığı videoya ait öznitelik grafikleri (a) V18 videosuna ait çerçeve (b) Tekrarlama sahteciliği öznitelik vektörü grafiği (c) Tekrarlama sahteciliğinde eşleşen noktalara ait grafik

Şekil 2.41.'in devamı



(c)

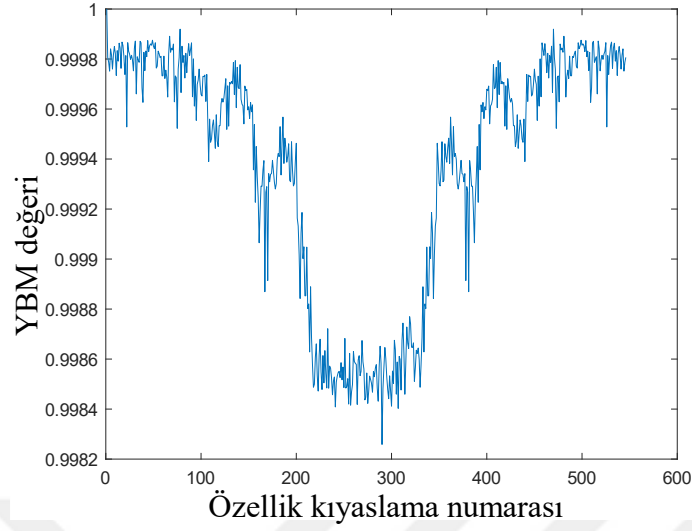
Şekil 2.41.' de tekrarlama ve Şekil 2.42.' de karma sahteciliklerine ait kullanılan veri tabanından alınan örnek görüntüler, elde edilen öznitelik vektörleri ve algoritmanın tespit ettiği sahtecilik konumlarına ait eşleşen noktaların grafikleri çizdirilmiştir. Tespit sonucu elde edilen grafiklerden de görüldüğü gibi tekrarlama sahteciliğinde; kopyalanan çerçeveler aynı sıralama ile videonun farklı bir bölgesine yapıştırıldığı için doğruları oluşturan konumların Şekil 2.41. (c)' deki gibi birbirine paralel şekilde arttığı gözlemlenmektedir. Tekrarlama sahteciliğinde kırmızı ile gösterilen kopyalanan çerçevelerin konumları artarken, mavi ile gösterilen çerçevelerin konumları da artmaktadır.



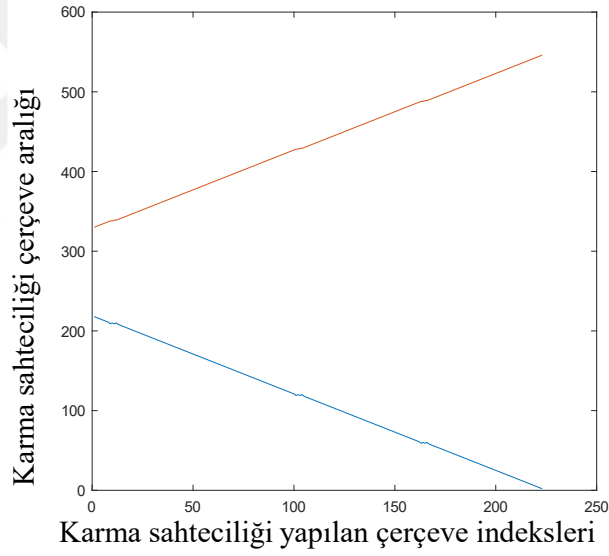
(a)

Şekil 2. 42. Karma sahteciliği örneği (a) V16 videosuna ait çerçeve (b) Karma sahteciliğine ait öznitelik vektörü grafiği (c) Karma sahteciliğinde eşleşen çerçeveler

Şekil2.42.' in devamı



(b)



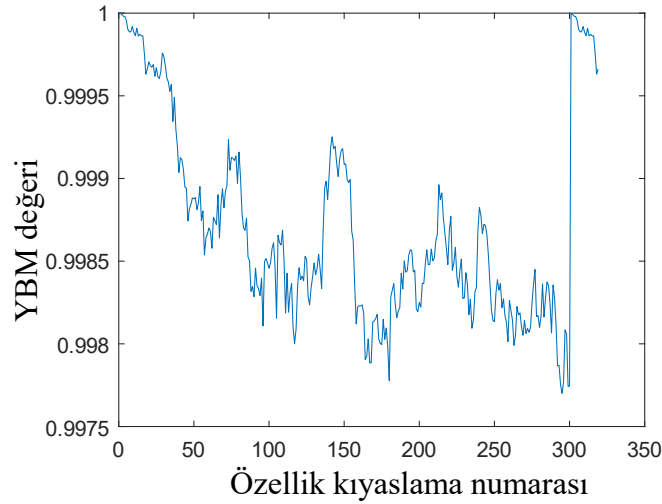
(c)

Karma sahteciliğinde kopyalanan video çerçevelerinin sıralaması değiştirildiği için kırmızı ile gösterilen kaynak çerçevelerin konumları artarken, mavi ile gösterilen hedef çerçevelerin konumları Şekil 2.42. (c)' deki gibi azalmaktadır. Şekil 2.41. içerisinde kullanılan videolar Fadl vd.' nin önermiş olduğu veri tabanından [126] alınan video örnekleridir. Şekil 2.41. (a)' da kullanılan V18 isimli videoda, 145 ve 185 arası 40 çerçeve 50. çerçeveden sonraya yapıştırılmıştır. Böylece Şekil 2.41. (b)' de elde edilen simetrik tepe noktalarına ait görsel oluşmaktadır. Şekil 2.41. (b) ve Şekil 2.42. (b)'de yatay eksen

iki çerçeve arasındaki ilişki sıralamasını, düşey eksen ise bunlar arasındaki çıkarılan PYGH özniteliklerinin YBM ile kıyaslamalarının değerini göstermektedir. Şekil 2.41. (c)' deki gibi 51.çerçeve 186. çerçeve ile eşleşmektedir. Şekil 2.41. (c) ve Şekil 2.42. (c)' de yatay eksen toplam kopyalanan çerçeve sayısını, düşey eksen ise eşleşen çerçeve numaralarını göstermektedir. Şekil 2.42. (a)' da kullanılan V16 isimli karma sahteciliği yapılan videoda 1. çerçeveden sonraya 217 çerçeve tersten yapıştırılmıştır. 218. çerçevenin karşılığı 330. çerçeveye denk gelmektedir. Şekil 2.43.' de aynı video içerisinde kopyalanan çerçevelerin videonun sonuna ekleme yapılarak yapıştırıldığında elde edilen grafik gösterilmektedir. Bu video Ren vd. [124] önermiş olduğu çalışmada kullandıkları veri setinden alınmış bir videoya aittir. Video da ilk 20 çerçeve kopyalanarak videonun sonuna yani 300. çerçeveden sonraya yapıştırılmıştır.



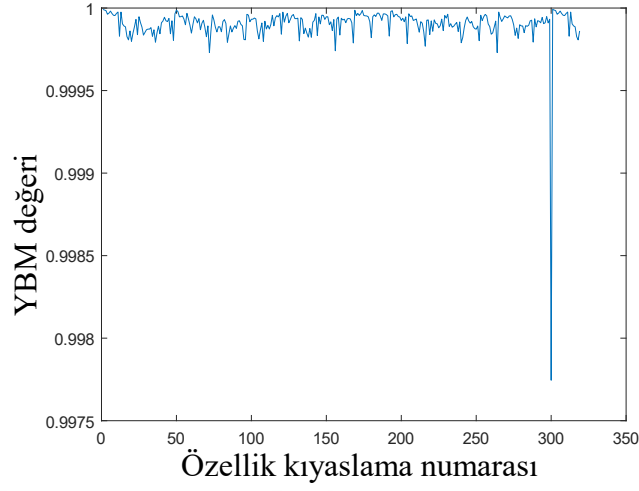
(a)



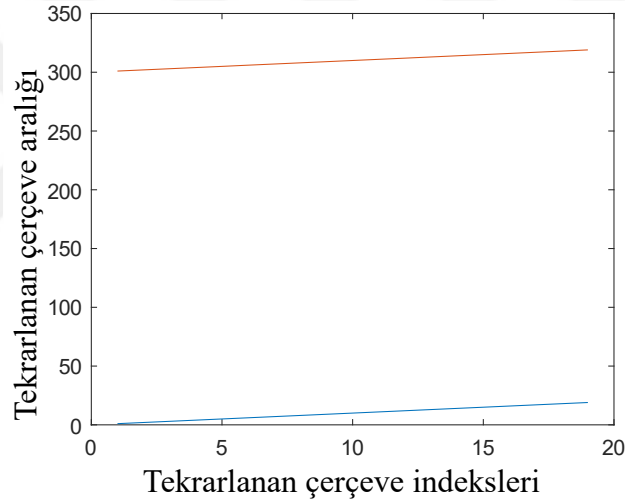
(b)

Şekil 2. 43. Tekrarlama sahteciliği videonun sonunda yapıldığında oluşturulan öznitelik vektörü grafikleri (a) Akiyo videosuna ait görsel (b) 1. çerçeve ile diğer çerçevelerin YBM kıyaslaması sinyal grafiği (c) Ardışık çerçevelerin özniteliklerinin YBM ile kıyaslanması

Şekil 2.43.'ün devamı

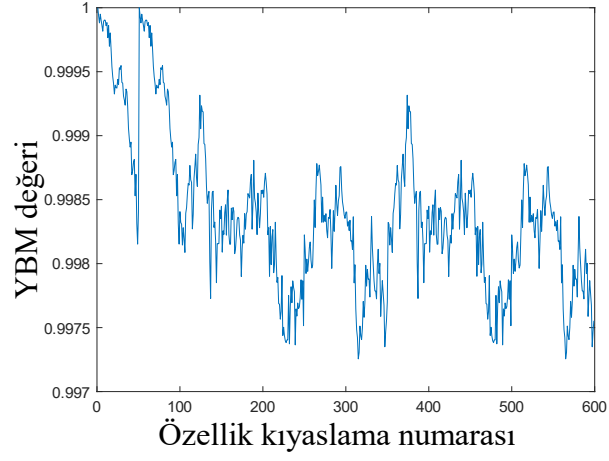


(c)

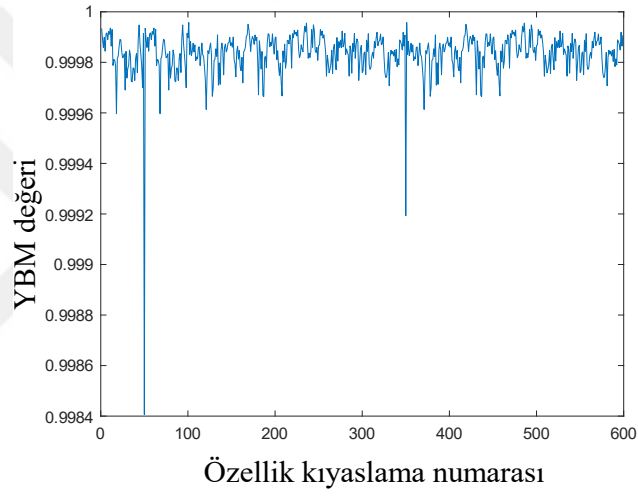


(d)

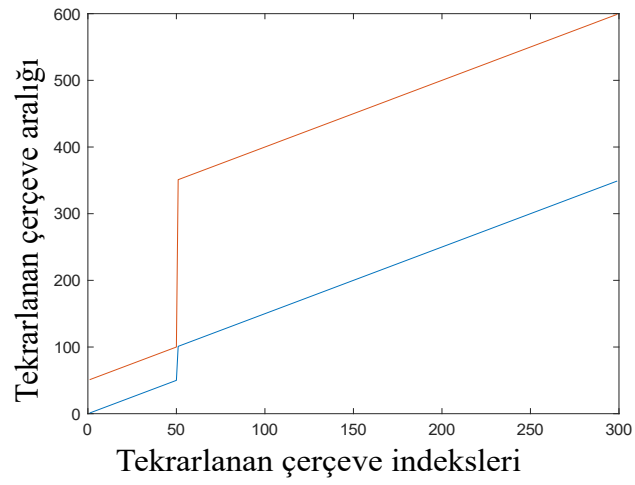
Şekil 2.44.' de aynı “Akiyo” videosunun [158] içerisine 50. çerçeveden sonra tekrar videonun tamamı yapıştırılarak sahtecilik yapılmıştır. Böylece yapıştırılan konunun 51. ve 101. çerçeveleri arası ilk 50 çerçeveyle eşleşmektedir. Sahte videonun 101. çerçevesi de yine sahte videonun 351. çerçevesi ile eşleşmektedir. Şekil 2.44. (a)' da PYGH algoritması ile elde öznitelik vektörlerinin 1. çerçeveye ait öznitelik ile diğer çerçevelerin YBM kıyaslamasına ait sinyal grafiği gösterilmektedir. Bu grafik tekrarlanan sahnelerin özniteliklerinin birbiri ile benzerliğini göstermek için çizdirilmiştir. Şekil 2.44. (b)' de algoritmanın içerisinde kullanılan ardışık çerçevelere ait özniteliklerin kıyaslanması gösterilmektedir.



(a)



(b)



(c)

Şekil 2. 44. Tekrarlama sahteciliği öznelitik kıyaslama görselleri

Şekil 2.44. (b)' de yatay eksen çerçeve kıyaslamalarının numaralarını, düşey eksen ardışık çerçevelerin PYGH özniteliklerinin YBM kıyaslamalarına ait büyüklük değerlerini göstermektedir. Şekil 2.44. (c) tekrarı yapılan çerçevelerle 300 çerçeve içeren video toplamda 600 çerçeve içeren video olmaktadır. Düşey eksen de kırmızı çizgi yapıştırılan çerçeve konumlarını, mavi çizgi kopyalanan çerçeve konumlarını göstermektedir. Yatay eksen de tekrar edilen sahte çerçeve sayısını göstermektedir.

Algoritmamız içerisinde eşleşme ile ilgili herhangi bir sahtecilik olup olmadığı araştırılmaktadır. Tekrarlama veya karma sahteciliği için eşleşme noktası sahteciliğin varlığını ya da yokluğunun bir göstergesi olabilir; ancak ekleme ve silme için böyle bir dayanak bulunmamaktadır. Bu yüzden ikinci bir eşik noktası belirlemeye ihtiyaç duyulmaktadır. Tekrarlama ve karma sahteciliğinde aynı video içerisinden yapıştırılma yapıldığı için ekleme ve silme sahteciliği yapıldığı durumda komşu çerçevelerle olan benzerlik ilişkisi daha az olacak ve aralarındaki fark daha yüksek olacaktır. Buna dayanarak incelenen pik noktalarının çerçevesi ile yanındaki çerçevelerin benzerlik oranına göre bir inceleme yapılmaktadır. Deneysel olarak belirlenen eşik değeri, Eşitlik 2.36' daki gibi hesaplanan oran değeri ile kıyaslanır.

$$t_1 = \frac{ortalama(YBM_{a+2}, YBM_{a+1})}{ortalama(YBM_{a-2}, YBM_{a-1})} \quad (2.36)$$

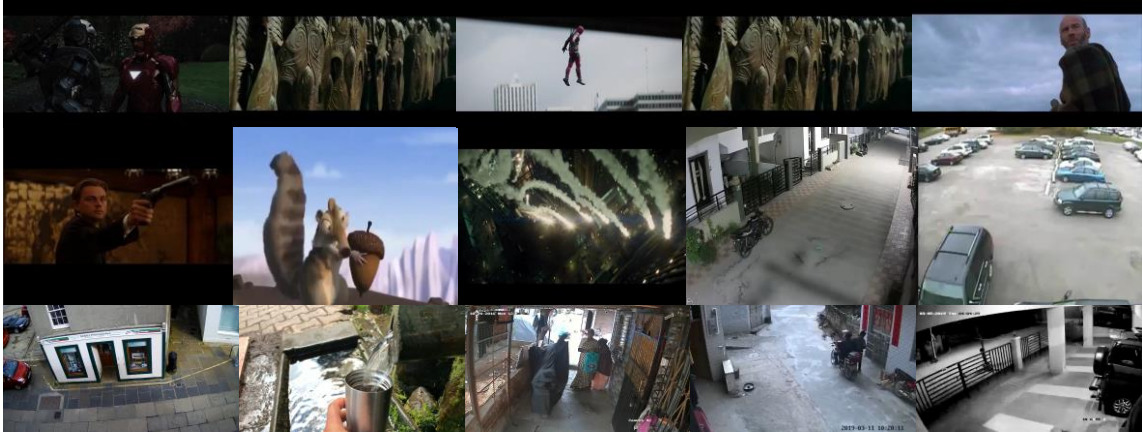
Ekleme sahteciliği için farklı iki video birleştirildiği düşünülünce, bunlar arasındaki benzerlik oldukça düşük çıkacaktır. Diğer bir deyişle tepe noktasının öncesi ve sonrasındaki çerçevelerin farkı yüksek, benzerliği düşük çıkacaktır. Silme durumunda ise yine ardışık çerçeveler arası benzerlik farkı oluşacaktır. Ancak silmenin yapıldığı videoda farklı bir videodan görüntü alınmadığı için benzerlik farkı eklemeye göre az olacaktır.

3. BULGULAR VE İRDELEME

Bu bölüm doktora tezi kapsamında yapılan çalışmaların deneysel sonuçlarının literatürdeki diğer çalışmalarla avantaj ve dezavantajlarına göre kıyaslanmasını kapsamaktadır. Bölüm 3.1’ de kullanılan veri setlerinden, Bölüm 3.2’ de kullanılan performans ölçütlerinden bahsedilmektedir. Sonrasında gerçekleştirilen yöntemlerin literatürdeki veri tabanlarında ve oluşturulan veri tabanında değerlendirilmesi yapılmaktadır. Son bölümde ise önerilen yöntemlerin karşılaştırılması verilmektedir.

3.1. Kullanılan Veri Setleri

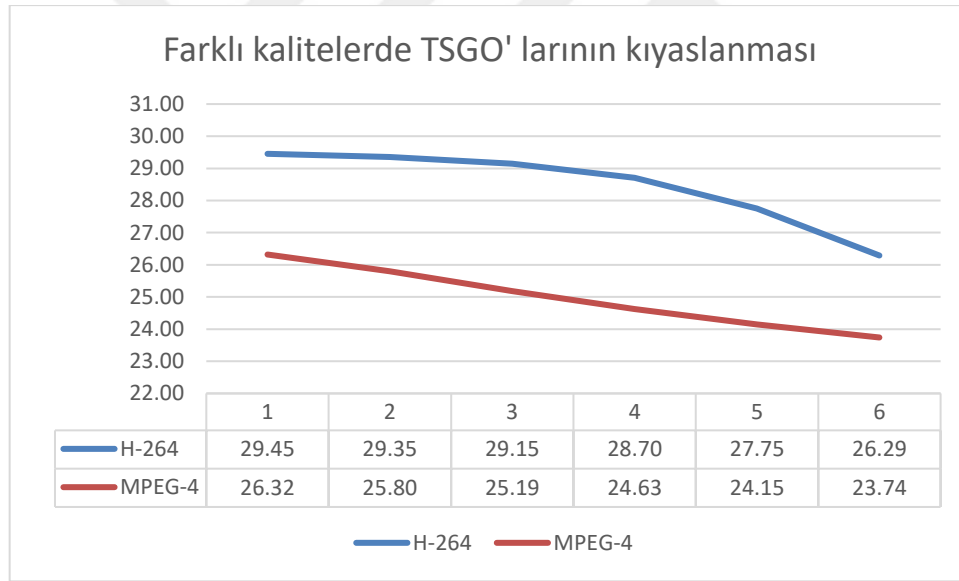
Tez kapsamında deneysel sonuçların alındığı veri setleri seçilirken farklı ve rastgele konumlarda sahtecilik yapan veri setleri seçilmiştir. Bu anlamda Shelke vd., Hongre vd., Fadl vd., Ulutaş vd., SULFA, VTL ve YouTube’ dan alınan videolarla oluşturulan veri tabanı Web-test ile deneysel çalışmalar yapılmıştır. Veri setinin oluşturulması için açık kaynak kodlu VirtualDub ve FFMPEG uygulamaları kullanılmıştır. Oluşturulan yeni veri tabanındaki videolara ait görseller Şekil 3.1.’ de gösterildiği gibidir.



Şekil 3. 1. Web-test oluşturulurken kullanılan orijinal video çerçeve örnekleri

Yapılan sahtecilik işlemleri sonrasında sahtecilik izlerinin kaybedilmesi ve zorluk derecesinin artması için sıkıştırma ve bulanıklaştırma atakları uygulanmıştır. Sıkıştırmanın

etkisi ile mevcut verilerde meydana gelen kayıplar kalitenin düşmesine neden olmaktadır bu yüzden sahtecilik sonrası yapılan izlerin bulunması zorlaştırmaktadır. Bu durum SULFA veri tabanı kullanılarak oluşturulan veri tabanından alınan sahte bir video ile Şekil 3.2.' de gösterildiği gibi örneklendirilmektedir. Video farklı 6 farklı sıkıştırma kalite oranlarında, H-264 ve MPEG-4 kodekler kullanılarak sıkıştırılmıştır. Sıkıştırma işleminde kullanılan kalite faktörleri ile her seferinde bellekte tutulan yer yaklaşık olarak yarısı olacak şekilde seçilmiştir. H.264 için cfr6, crf12, cfr18, cfr24, cfr30, cfr36; MPEG-4 için QS1, QS6, QS11, QS16, QS21, QS26 kalite oranları kullanılmıştır. Sonrasında her sıkıştırılan videonun sıkıştırılmayan video ile TSGO' ları çerçeve düzeyinde tek tek kıyaslanmıştır. Elde edilen çerçeve TSGO oranları sonuçlarının ortalama değerleri alınarak Şekil 3.2. çizdirilmiştir. Şekil üzerindeki grafikler incelendiğinde sıkıştırma kalitesi arttıkça veri kaybı artmakta, görüntü kalitesi düşmektedir.



Şekil 3. 2. Farklı kalitelere sıkıştırılmış sahte can_220_book videosu ile sıkıştırılmamış sahte haldeki video çerçevelerinin ortalama TSGO değerlerinin grafiği

Şekil 3.3.' de de bulanıklaştırma atağı uygulanmış video çerçevesi örneği gösterilmektedir. Bulanıklaştırma atağı da mevcut sahtecilik izlerinin kaybedilmesinde kullanılabilecek bir diğer son işlem uygulamasıdır. Bulanıklaştırma atakları SULFA veri tabanı kullanılarak oluşturulan 20 videoya uygulanarak oluşturulmuştur. Önerilen frekans tabanlı yöntem içerisinde dayanıklılık testleri gerçekleştirilmiştir.



(a)

(b)

Şekil 3. 3. (a) Orijinal ve (b) bulanıklaştırma atağı uygulanmış çerçeve görselleri

Literatürdeki çalışmalarda kullanılan veri tabanları incelendiğinde mevcut veri tabanlarının genellikle SULFA ve VTL veri tabanları kullanılarak elde edilen veri tabanlarından oluştuğu gözlemlenmektedir. Bu veri tabanlarındaki videolara ait çözünürlük boyutlarının ve çerçeve sayılarının az olması yöntemlerin gerçek hayatta kullanılan videolar açısından kıyaslanmasında kısıtlı kalmaktadır. Ayrıca mevcut veri tabanların çoğu erişime kapalı olduğu için kıyaslamalar yapılamamaktadır. Kıyaslaması yapılan çalışmalarda videolar üzerinde yapılan sahtecilik konumları rapor edilmiş ve düzenleme yazılımları ile yeniden sahtecilik yapılarak testler gerçekleştirilmiştir.

Bu eksiklikler göz önünde bulundurulduğunda yapılan yöntemlerin kıyaslanma doğruluklarının günlük hayata uygun videolar üzerinden test edilebilmesi için yeni bir veri tabanı önerilmiştir. Veri tabanındaki videolar durağan ve hareketli arka plan içeren videolardan oluşturulmuştur. Farklı çözünürlükte ve farklı çerçeve sayısı içeren videolar içermektedir.

3.2. Kullanılan Performans Değerlendirme Ölçütleri

Performans değerlendirmesi yapılırken literatürde yapılan diğer yöntemlerin de kullandığı doğruluk oranı (detection accuracy, DO), kesinlik (precision, KE), duyarlılık (recall, DU) ve F_1 skor ile hesaplanması ile kıyaslamalar yapılmaktadır. Çerçevelerin sahte ya da orijinallik bilgisine göre değerlendirme yapılır. Değerlendirmede orijinal videolar negatif,

sahte videolar pozitif kabul edilmiştir. Bu doğrultuda algoritmamızın doğru bulduğu sahte çerçeveler $DP(true - positive/doğru pozitif)$, algoritmamızın sahte olmadığı halde sahte dediği fazladan bulunan çerçevelerde $YP(false-positive/yanlış pozitif)$ olarak hesaplanmıştır. Eşitlik 3.1- Eşitlik 3.4 aralığında bu ölçütlerin hesaplanması verilmektedir. Hibrit çalışma içerisinde tüm sistemin video düzeyinde yapılan sahtecilik türüne göre başarısı ölçülmüştür. Bu şekilde literatüre yeni bir test bir test parametresi kazandırılmıştır. Bu değerlendirme içerisinde örneğin tekrarlama sahteciliği için DP değeri tekrarlama olup, algoritmamızın tekrarlama dediklerini; DN tekrarlama olmayıp, algoritmamızın da tekrarlama demedikleri; YP tekrarlama olmadan kod tarafından tekrarlama denilen videoları; YN ise tekrarlama sahteciliği içeren videolar olup kod tarafından bulunamayan videoları temsil etmektedir.

Doğruluk oranı doğru bulunan çerçevelerin tüm çerçevelere oranını yani sistemin başarısını göstermektedir. Kesinlik, doğru bulunan sahte videoların, yanlış ve doğru bulunan tüm sahte videolara oranını; duyarlılık ise doğru bulunan sahte videoların doğru bulunan sahte ve yanlış bulunan orijinallere oranını göstermektedir. F_1 skor ölçütü de yapılan değerlendirmenin başarısını göstermektedir.

$$DO = (DP + DN)/(DP + DN + YP + YN) \quad (3.1)$$

$$KE = DP/(DP + YP) \quad (3.2)$$

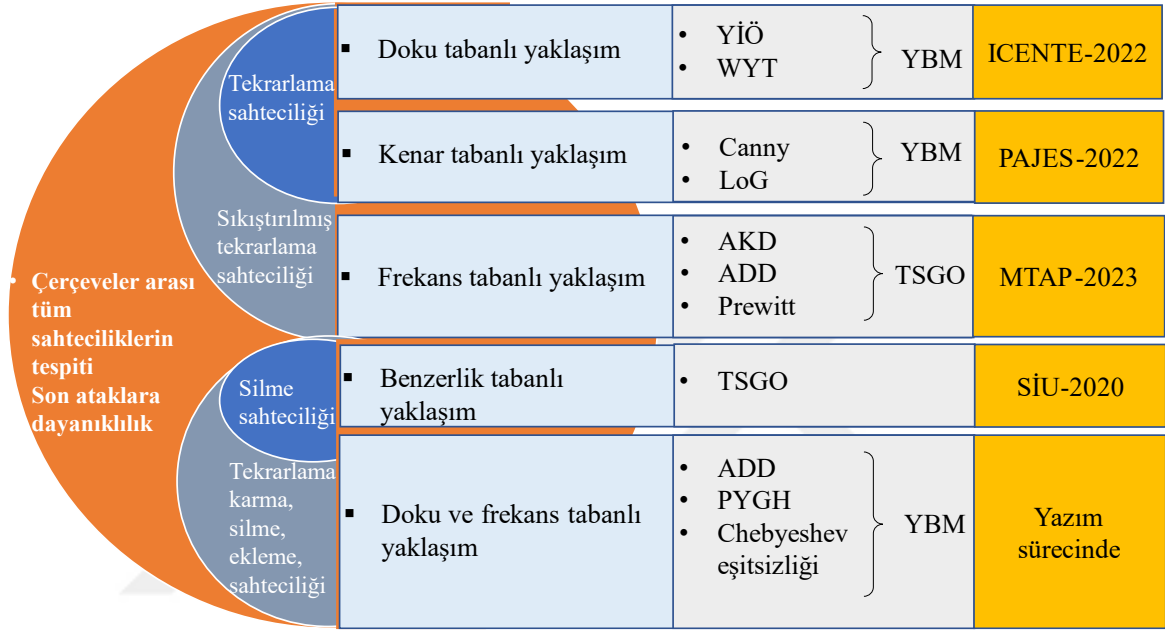
$$DU = DP/(DP + YN) \quad (3.3)$$

$$F_{1skor} = (2 \times KE \times DU)/(KE + DU) \quad (3.4)$$

3.3. Gerçekleştirilen Yöntemlerin Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Tez kapsamında problem odaklı ilerlenmiş ve mevcut çerçeveler arası sahteciliklerin tamamına nasıl efektif bir çözüm sunulabilir, geliştirilen çözümler nasıl son işlem ataklarına dayanıklı olabilir şeklinde çözümler sunulurken ilerlenmiştir. İlk olarak tekrarlama sahteciliğine; doku tabanlı ve kenar tabanlı olmak üzere iki farklı yaklaşım sunulmuş bunların sıkıştırılmaya dayanıklılığını artırmak için frekans tabanlı farklı bir yöntem geliştirilmiştir. Sonrasında silme sahteciliğine çözüm sunulmuş ve iki farklı sahteciliğin tespiti yapıldıktan sonra tüm sahteciliklere çözüm sunabilen hibrit bir çalışma gerçekleştirilmiştir. Son olarak da bu çalışmanın sıkıştırılmaya dayanıklı olabilmesi için ADD ile çıkarılan alçak frekanslı görüntü üzerinden elde edilen öznitelikler ile kıyaslama

yapılmış ve başarılı sonuçlar alınarak tezin amacına ulaşması sağlanmıştır. Yapılan tez çalışmasına ait literatürde bahsi geçen tüm sahtecilik türlerine sunulan çözümler, kullanılan yöntemler ve algoritmalar Şekil 3.4.' de gösterilmektedir. Şekil 3.5.' de de önerilen yöntemlerin kıyaslandığı çalışmalar ve onlara olan üstünlükleri ile kıyaslama işlemi yapılırken kullanılan veri setleri gösterilmektedir.



Şekil 3. 4. Tez kapsamında çözüm sunulan problemler, çözüm yaklaşımları ve kullanılan algoritmalar

3.3.1. Tekrarlama Sahteciliği Tespiti İçin Önerilen Doku Tabanlı Yaklaşım Sonuçları

Tez kapsamında önerilen çalışmaların ilk aşamasında tekrarlar sahteciliğine yönelik doku tabanlı çalışmalar gerçekleştirilmiş kıyaslamalı olarak çeşitli veri tabanları üzerinden sonuçlar elde edilmiştir. İlk olarak algoritmada çerçevelerden elde edilen WYT ve YİÖ özniteliklerinin YBM kıyaslamaları yapılmış ve sonrasında birbirine eşit olan değerler tekrarlar sahteciliğinin yapıldığı değerler olarak belirlenmiştir. Bu çalışma kapsamında Shelke vd., Ren vd., Wei vd., Fadl vd., ve Web-test' deki videolar ile testler gerçekleştirilmiştir. YİÖ algoritması kullanılarak 5 farklı özellikteki veri tabanından alınan sonuçlar incelendiğinde en düşük DO' nun Fadl vd. çalışmasında %96 olduğu görülmektedir. Bu veri tabanı içerisinde doğruluk oranının düşmesine neden olan v29 ve

v30 videolarının sahte çerçevelerinin tamamı bulunmaktadır. Ancak orijinal çerçevelerin sahte olarak bulunması yani yanlış pozitifleri artırmakta, kesinlik değerini düşürmektedir.

	Kıyaslanan çalışmalar	Kullanılan veri tabanları	Önerilen çalışmanın pozitif yönleri
Doku tabanlı yaklaşım	2022 - Shelke vd. [154] 2021 - Ren vd. [124] 2020 - Fadl vd. [126] 2019 - Wei vd. [122] 2016- Yang vd. [119]	- Shelke vd. [154] - Ren vd. [124] - Wei vd. [122] - Fadl vd. [126] - Web-test	- Kıyaslanan çalışmalara göre daha yüksek başarı - Ortalama 0.0863 çerçeve/saniye süre - Hareketli ve sabit arka planlı videolarda çalışabilme
Kenar tabanlı yaklaşım	2020 - Ulutaş vd. [175] 2020 - Fadl vd. [126] 2019 - Bakas vd. [122] 2018 - Zhao vd. [135] 2017 - Liu ve Huang [120] 2014 - Wang vd. [104]	- Fadl vd. [126] - Test veri tabanı [175] - Web-test	- Kıyaslanan çalışmalara göre daha yüksek başarı - İngesel yaklaşım sunulması - Hareketli ve sabit arka planlı videolarda çalışabilme
Frekans tabanlı yaklaşım	2021 - Ren vd. [124] 2020 - Kharat vd. [116] 2019 - Bakas vd. [123] 2019 - Singh vd. [86] 2019 - Wei vd. [122] 2017 - Bozkurt vd. [139] 2014 - Li vd. [136] 2007 - Wang vd. [84]	- Web-test - VTL [158] - SULFA [160] - Ren vd. [124] - Wei vd. [122]	- Kıyaslanan çalışmalara göre daha yüksek başarı - Kaynak ve hedef çerçeve tespiti - Sıkıştırma ve bulanıklaştırma ataklarına dayanıklılık - Hareketli ve sabit arka planlı videolarda çalışabilme
Doku ve frekans tabanlı yaklaşım	2019 - Wei vd. [122] 2012- Lin ve Chang [85]	- Wei vd. [122] - Web-test	- Kıyaslanan çalışmalara göre daha yüksek başarı - Farklı sıkıştırma formatları kalite oranlarına göre değerlendirilme - Farklı sayıda silinen çerçevenin tespit edilebilmesi
Doku ve frekans tabanlı yaklaşım	2022 - Shelke vd. [154] 2021 - Ren vd. [124] 2020 - Fadl vd. [126] 2020 - Kharat vd. [116] 2019 - Bakas vd. [123] 2019 - Singh vd. [86] 2018 - Zhao vd. [135] 2017 - Liu ve Huang [120] 2014- Wang vd. [104] 2014 - Li vd. [136] 2007 - Wang vd. [84]	- Web-test - Ren vd. [124] - Fadl vd. [126] - Shelke vd. [154]	- Kıyaslanan çalışmalara göre daha yüksek başarı - Çerçeveler arası tüm sahtecilikleri tespit edebilme - Sıkıştırma ataklarına dayanıklılık - Hareketli ve sabit arka planlı videolarda çalışabilme

Şekil 3. 5. Tez kapsamında yapılan çalışmaların kıyaslandığı çalışmalar, kullanılan veri tabanları ve pozitif üstünlükleri

Şekil 3.6.’ da Fadl vd.’ nin veri tabanından alınan durağan sahneli videolara ait çerçeve örnekleri gösterilmektedir. YİÖ algoritması doku tabanlı öznitelik çıkarmaktadır ve videonun aynı sahneyi içeren farklı çerçeveleri için yeteri kadar ayırt edici olmamaktadır. Ancak kullanılan veri tabanları göz önünde bulundurulduğunda, kıyaslaması yapılan çalışmalarda kendilerinin önerdiği diğer veri tabanlarındaki çalışmaların tamamından daha yüksek başarı elde edilmiş. Dolayısıyla hem veri tabanları kullanılan çalışmaları hem de onların kıyaslandıkları çalışmalardan daha yüksek başarılar elde edilmiştir.



(a)

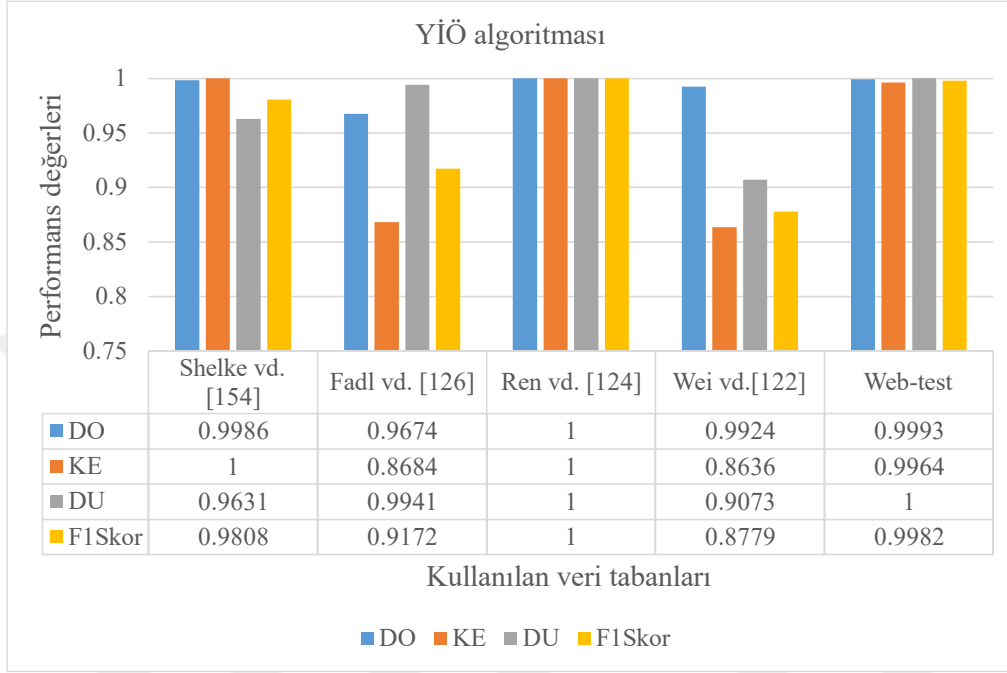


(b)

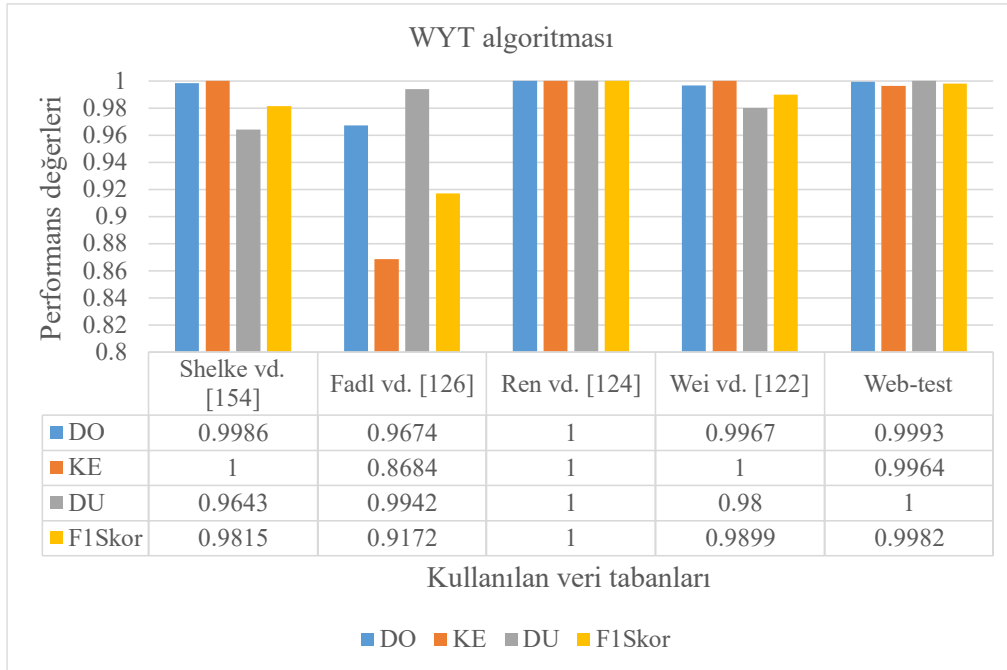
Şekil 3. 6. Fadl vd. önerdiği veri tabanından alınan (a) v29 ve (b) v30 ait görsel örnekler

Her iki algoritma için ayrı ayrı test yapılmıştır. Analiz sonuçları Şekil 3.7.’ de gösterildiği gibidir. Bu iki video için de sabit kamerayla çekilmiş ve sahneye ani şekilde hareketli kişiler girmektedir. Bu videolar için sabit kamera ile kayıt yapılması mevcut videolarda YİÖ ve WYT özniteliklerinin çerçeveler arası yeteri kadar ayırt edici olmadığını göstermektedir. Ancak iki algoritmanın kıyaslamasına bakarsak WYT algoritmasında bulunan, fazladan sahte çerçeve sayısı daha düşük olduğu için performans metrikleri biraz daha yüksek çıkmaktadır. Algoritmaların koşma süreleri incelendiğinde, WYT algoritmasının çerçeve başına düşen koşma süresi yaklaşık olarak 0.08 s/çerçeve iken; YİÖ algoritmasının 0.09 s/çerçeve olmaktadır. Bu nedenle WYT algoritmasının tercih edilebilirliği daha yüksek olacaktır. Bir sonraki aşamada kullanılan WYT ve YİÖ algoritmalarının kıyaslama sonuçları Şekil 3.8.’ de verilmiştir. Kullanılan 5 veri tabanı

üzerinden elde edilen ortalama sonuçlara göre YİÖ' nün WYT algoritmasının performans değerleri bakımından geri kaldığı ve ortalama süre olarak daha yavaş çalıştığı gözlemlenmektedir.

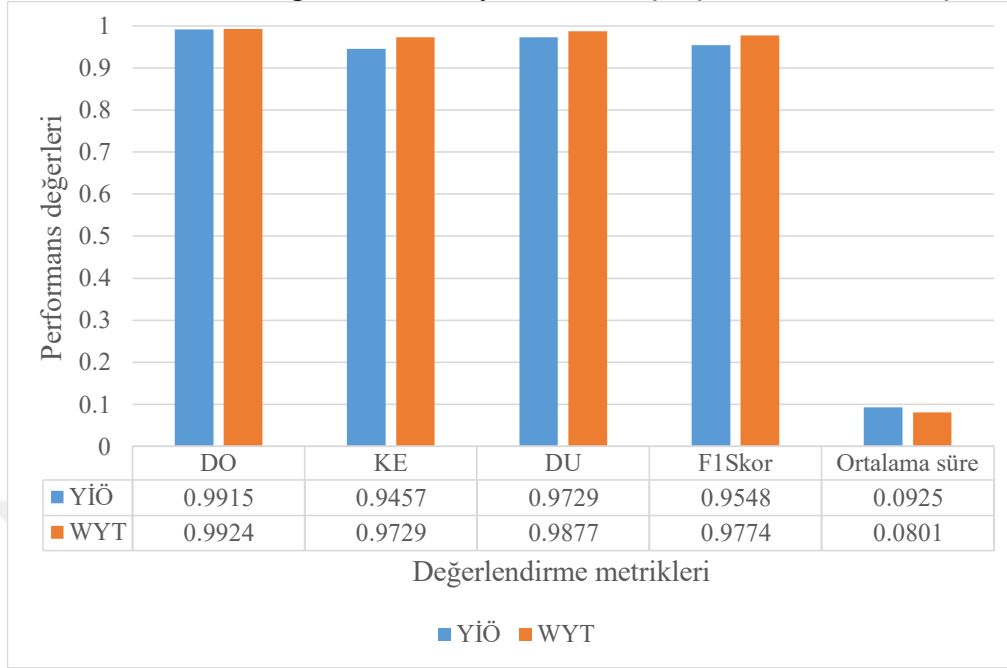


(a)



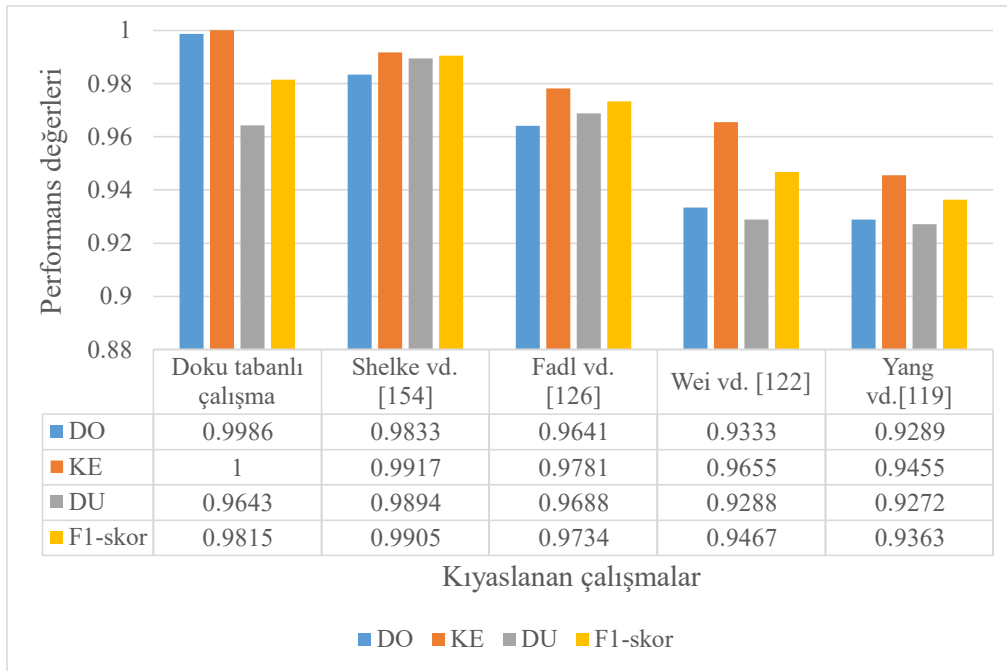
(b)

Şekil 3. 7. (a) YİÖ algoritmasına dayalı önerilen çalışmanın analiz sonuçları (b) WYT algoritmasına dayalı önerilen çalışmanın analiz sonuçları



Şekil 3. 8. YİÖ- WYT kıyaslaması

Shelke vd. çalışmasıyla Şekil 3.9.' da onların önerdiği veri tabanı üzerinden, Shelke vd. [154], Fadl vd. [126], Wei vd. [122] ve Yang vd. [119] çalışmalarıyla kıyaslanmıştır.



Şekil 3. 9. Önerilen yöntem ve doku tabanlı diğer çalışma ile kıyaslanması

Önerilen yöntemin ve Shelke vd. kullandığı iki farklı doku tabanlı algoritmanın ortalamaları alınarak sonuç elde edilmiştir. Şekil 3.9. incelendiğinde önerilen çalışmaya en yakın performans sonuçlarının Shelke vd.’ nin çalışmasında olduğu görülmektedir. Önerilen yöntem Shelke vd.’ nin önermiş olduğu yönteme göre hem farklı boyutlarda ve özniteliklerde veri tabanları üzerinden denenmiş hem de daha efektif çalışmaktadır. Shelke vd. çalışmasında kullanılan doku tabanlı yöntemler yüksek bellek ihtiyacından dolayı sadece 128×128 boyutlu videolar üzerinden denenmiştir. Performans açısından diğer çalışmalardan daha yüksek olduğu gözlemlenmiştir. Ancak yöntemin dezavantajı sıkıştırma gibi son işlem adımları uygulanan videolarda başarı performansı düşmektedir.

Doku tabanlı yaklaşımlar, 5 farklı veri tabanı üzerinden elde ettiğimiz sonuçları gözlemlediğimizde sahtecilik tespitinde yeterli ayırt edici öznitelikleri sağlayabilecek nitelikte olup kullanılabilirler.

3.3.2. Tekrarlama Sahteciliği Tespiti için Önerilen Kenar Algılamaya Dayalı Yaklaşım Sonuçları

Kenar algılama algoritmalarından faydalanılarak öznitelik çıkarılan bu çalışmada çıkarılan özniteliklerin ikili görüntülerinin oluşturularak sahteciliğin tespit edilmesi literatüre bu alanda imgesel bir yaklaşım sunan çalışma kazandırılmasını sağlamaktadır. Yöntem kenarların algılanması, kenar özniteliklerinden fark vektörlerinin çıkarılması ve bunların gruplandırılması, üst üçgensel matris oluşumu ile nihai sonucun elde edildiği sahte çerçevelerin tespiti aşamalarından oluşmaktadır.

Fadl veri tabanından alınan v29 isimli videonun, Şekil 3.10.’ da görsel çıktıları gösterilmektedir. Şekil 3.10. (a)’ da Canny algoritması sonucu elde edilen görüntü, Şekil 3.10. (b)’ de LoG algoritması kullanılarak elde edilen görüntü, Şekil 3.10. (c)’ de ise her iki görüntünün morfolojik işlemler uygulanarak birleştirilmiş görüntüsü verilmektedir. Bu aşamaya kadar öznitelik çıkarımının ilk adımı “kenar algılama” tamamlanmıştır.

Öznitelik matrisinin çıkarılmasında ikinci aşama fark vektörlerinin oluşturulması ve bunların gruplandırılmasıdır. Fark vektörü oluşturulurken ilk olarak tüm çerçeveler 12×16 ölçülerinde bloklara ayrılmaktadır. Sonrasında iki ardışık çerçevenin sırayla tüm blokları arasındaki uzaklık xor ile hesaplanarak iki çerçevenin benzerlik durumu blok bazında kontrol edilmesi amaçlanmaktadır.



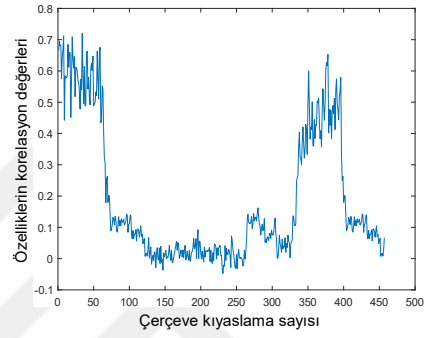
(a)



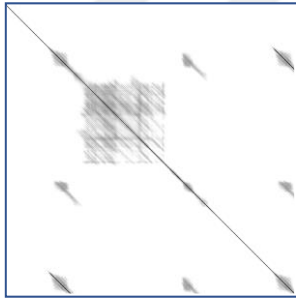
(b)



(c)



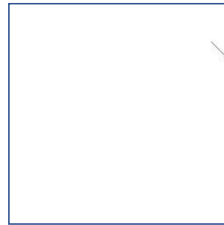
(d)



(e)



(f)



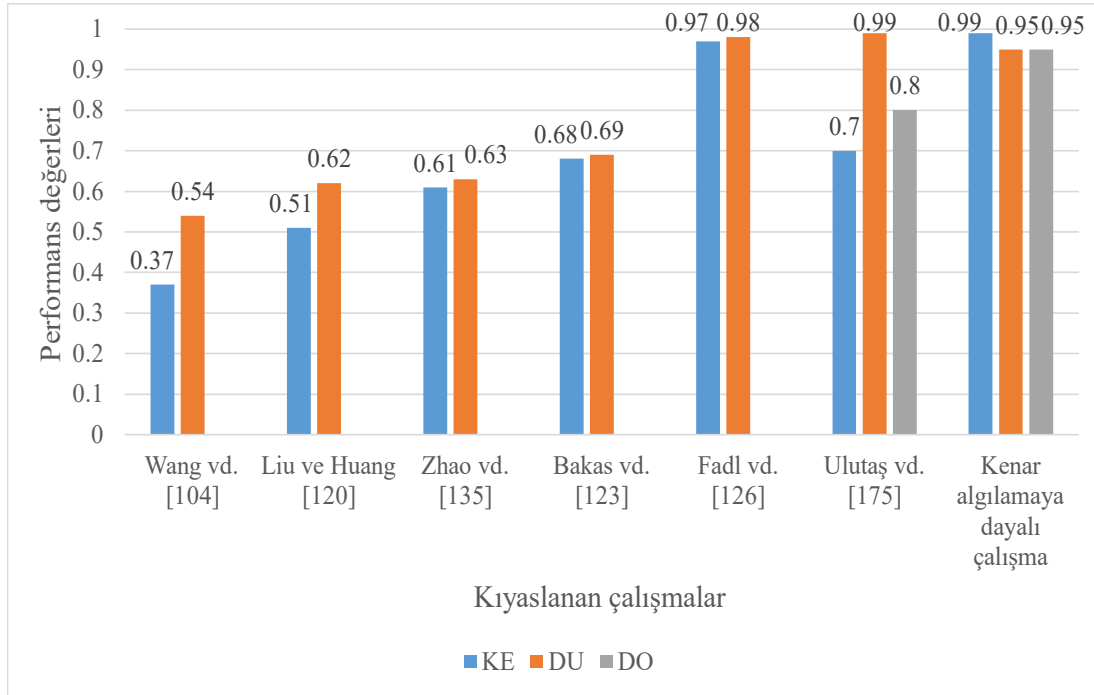
(g)

Şekil 3. 10. Kenar çıkarımına dayalı algoritmanın v29 üzerinden uygulanan görüntü çıktıları (a) Canny görüntüsü (b) LoG görüntüsü (c) Canny ve LoG' un birleştirilmiş görüntüsü (d) Elde edilen özniteliklerin korelasyon grafiği (e) Gruplar arası korelasyon değerlerinin ikili görüntüsü (f) İkili görüntünün üst üçgensel matris imgesi (g) Tekrarlanan sahte çerçeve çiftleri

Her bir blok için elde edilen toplam 1' lerin sayısı ayırt edici öznitelik olarak kullanılmak üzere vektöre dönüştürülmüştür. Bu vektörler arası korelasyon grafiği Şekil 3.10. (d)' de gösterildiği gibidir. Çıkarılan korelasyon bilgine göre inceme yapmak, sabit sahneli videolarda yanlış pozitif oranının artmasına neden olmaktadır. Dolayısıyla çerçeve öznitelikleri sabit uzunluklu alt gruplara ayrılarak bu gruplar arası korelasyonlarda Şekil 3.10. (e)' de gösterildiği gibi olmaktadır. Bu görüntünün alt üçgensel matrisine maksimum değer atanarak, sonraki aşamada eleme yapmak için uygun hale getirilmektedir. Böylece üst üçgensel matris kullanılmaktadır. Bir videodaki çerçevelerin benzerliklerinin normal dağılım göstereceği düşünülmektedir. Buna dayanarak çerçeve benzerliklerinin olasılık dağılımı incelenmiştir. Çerçeveler arası benzerliğin artma olasılığı düşüktür. Tekrarlanan çerçevelerin tespiti için düşük olasılıklı bölgeler araştırılmaktadır. Bu amaçla sadece üst üçgensel matris kullanılarak Otsu algoritması ile bir eşik değeri hesaplanmaktadır ve düşük olasılıklı eşleşme konumlarına 0 değeri, yüksek olasılıklı kısımlara 1 değeri atanmaktadır. Şekil 3.10. (g)' de aday sahte çerçeve konumları gösterilmektedir. Bu aşama ile özniteliklerin kıyaslanması aşaması da bitmiş ve tekrarlama sahteciliğinin tespiti aşamasına geçilmiştir. Son aşamada da sahte çerçevelerin tespiti için diyagonal elemanlar içerisinde en çok sıfır elemanını içeren diyagonal aday doğru olarak belirlenmektedir. Aday doğrunun seçiminden sonra da başlangıç ve bitiş konumlarının tespiti için, bu konumların çevrelerindeki çerçeveler ile YBM' ye dayalı tam konum belirlenmektedir.

Kenar algılama çalışması ile bir önceki çalışmada sabit sahneli videolarda meydana gelen yanlış pozitiflerin elenmesini gerçekleştirmek amacıyla ardışık çerçevelerin öznitelikleri arasında gruplama yapılmıştır. Bu şekilde ardışık çerçevelerin birbirinin kopyası gibi görünmesi durumunun da önüne geçilmiştir. Doku tabanlı yöntemlerin dışında; sahneye ani giriş yapan nesne veya kişilerin daha hassas algılanabilmesi için kenar öznitelikleri kullanılarak öznitelik çıkarımı yapılması amaçlanmıştır. Bu amaçla da tekrarlama sahteciliği tespiti için, kenar algılamaya dayalı yeni bir yaklaşım sunulmaktadır. Üç farklı veri tabanı kullanılıp sıkıştırılmamış videolardan başarılı sonuçların alındığı çalışmada hız bakımından etkinlik sağlanamamakta ancak doğruluk oranları bakımından daha yüksek başarı sağlanmaktadır. Yöntem ilk olarak Fadl vd. önermiş olduğu, tekrarlama sahteciliği yapılan, 9 video kullanılarak test edilmektedir. Bu veri tabanı üzerinden Ulutaş vd. önermiş olduğu LDB' ye dayalı çalışma [175] ve önerilen çalışma koşullarıyla kıyaslama yapılmaktadır. Buna ilişkin sonuçlar Şekil 3.11.' de gösterilmektedir. Bu kıyaslamada Fadl vd.' nin çalışmasında DO sonuçları verilmediği için kıyaslamaya eklenememiştir. Ancak

Ulutaş vd. çalışması ile önerilen çalışma bu veri tabanından test edildiği için bunların DO' su Şekil 3.11. ile gösterilmektedir. Üç çalışmanın kesinlik oranlarına baktığımız zaman %99 ile en yüksek başarı önerilen çalışmadan elde edilmektedir. Ancak sahte çerçevelerin ilk veya son çerçevelerinin eksik bulunmasından ötürü duyarlılık değeri bakımından %95 ile üçüncü sırada yer almaktadır.



Şekil 3. 11. Kenar özniteliklerine dayalı tekrarlama sahteciliği tespit yöntemi Fadl vd.' nin veri tabanında [126] kıyaslanması

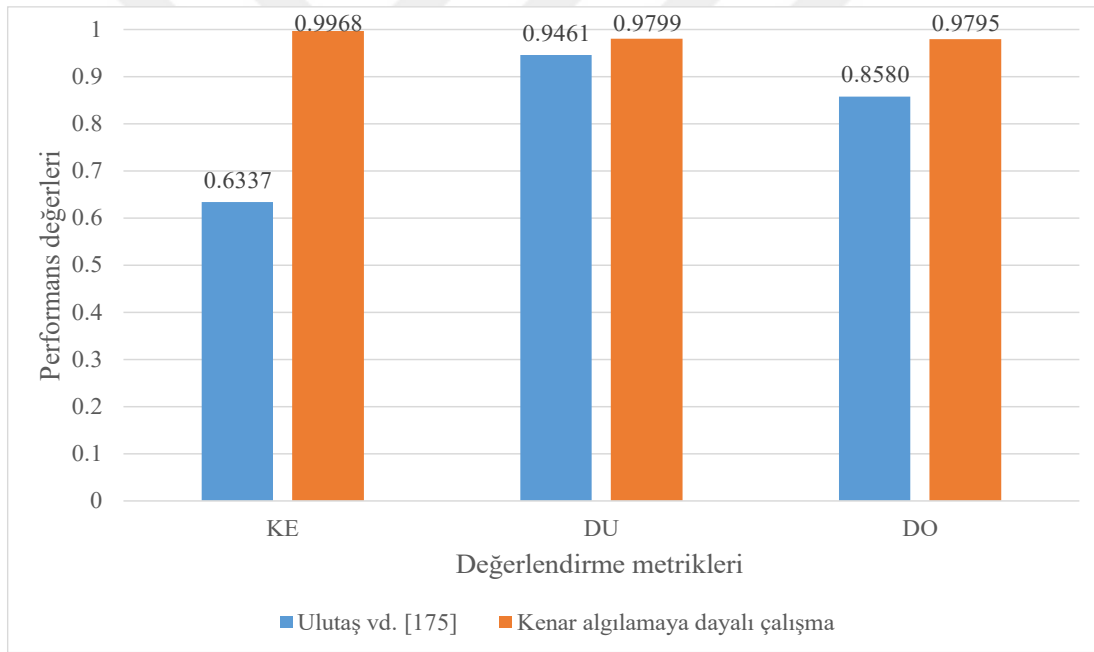
İkinci kıyaslamada veri tabanı genişletilerek üç farklı veri tabanı kullanılmaktadır. Fadl vd.' nin veri tabanı, SULFA ve VTL veri tabanları kullanılarak oluşturulan 30 video üzerinden elde edilen sonuçları göstermektedir. Bu videolar 352×288 , 704×576 , 320×240 , 176×144 , 352×288 olarak 5 farklı çözünürlüğe sahiptir. Kopyalanan çerçeve sayısı ve yapıştırılma konumları rastgele seçilmiştir. Yapıştırılma videonun sonuna yapıldığında da tespit gerçekleştirilebilmektedir. Tüm videolar üzerinden elde edilen doğruluk oranı %98 olarak Tablo 3.1' deki gibi rapor edilmektedir.

Son olarak da [175]' deki çalışma ve önerilen çalışmada SULFA ve VTL veri tabanları kullanılarak oluşturulan 21 video üzerinden test edilmiştir. Bu videoların çözünürlüklerinin ve dosya uzantılarının farklı olması yöntemin farklı video özelliklerine dayanıklılığını göstermektedir.

Tablo 3. 1. Kenar özniteliklerine dayalı tekrarlama sahteciliği tespit yöntemi Web-test ve Fadl vd.' nin veri tabanlarında önerilen çalışmaların kıyaslanması

KE	0.9937
DU	0.9860
DO	0.9825

Ulutaş vd.' nin çalışmasında değişken çözünürlüklü videolar hesaba katılmadığı ve esnek eşik kullanılmadığından yöntemin başarısı önerilen çalışmanın gerisinde kalmaktadır. Bu deneysel sonuçlara ait başarı yüzdeleri de Şekil 3.12.' de verilmektedir.



Şekil 3. 12. Kenar özniteliklerine dayalı tekrarlama sahteciliği tespit yöntemi SULFA ve VTL veri tabanlarında, [175] ve önerilen çalışmaların kıyaslanması

Tekrarlama sahteciliğinin tespitine yönelik önerilen bu iki çalışma da sıkıştırılmamış videolar üzerinden test edilmiştir. Ancak yöntemlerin sıkıştırmaya karşı dayanıklı olması ve daha efektif çalışması gerekmektedir. Dolayısıyla öznitelik çıkarımı için bir sonraki çalışmada frekans düzlemi kullanılmaktadır. Bu şekilde öznitelik vektörleri boyutları azaltılmış olacaktır hem de sıkıştırmaya karşı dayanıklılık sağlanmış olacaktır.

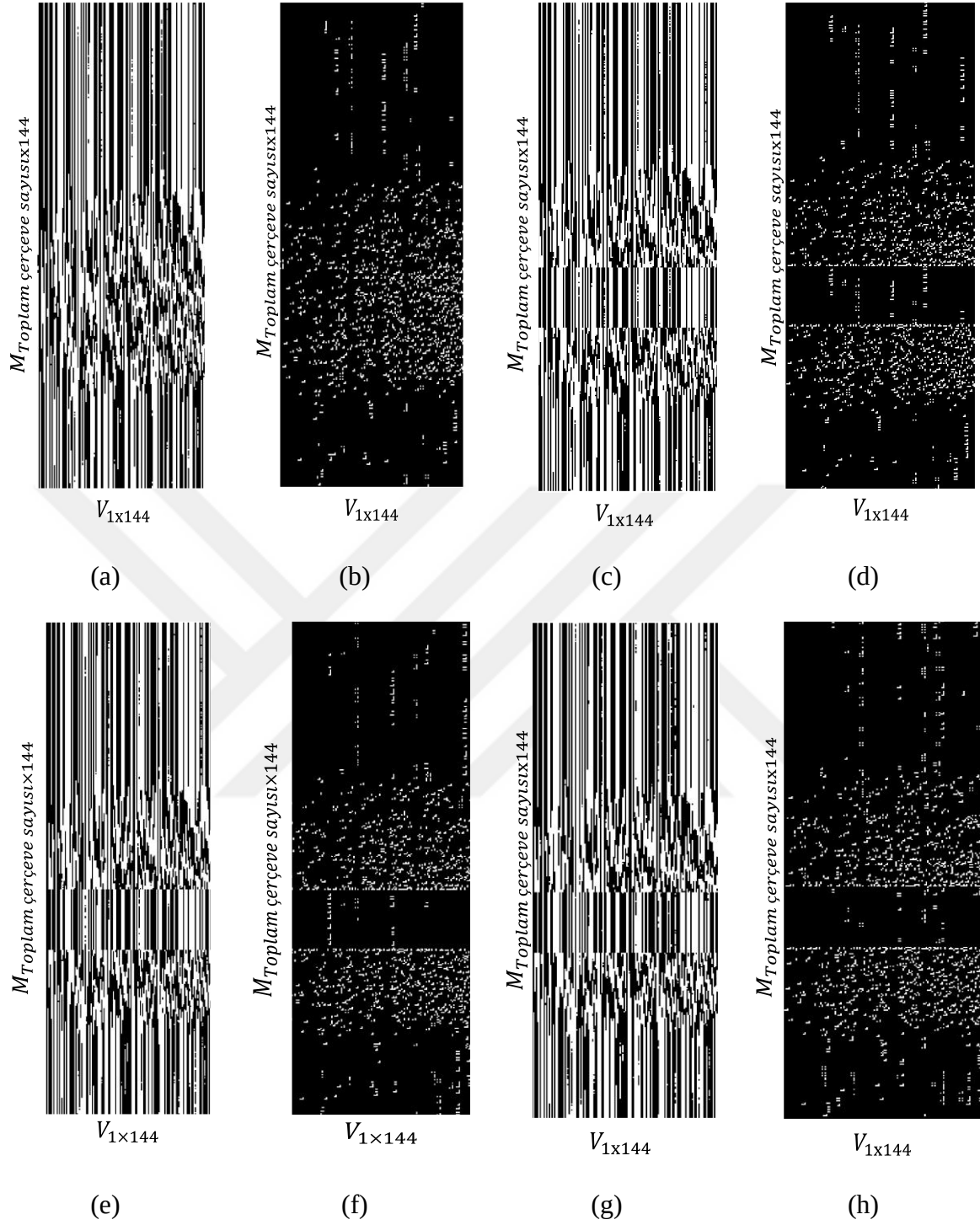
3.3.3. Sıkıştırılmış Videolarda Frekans Düzlemine Dayalı Tekrarlama Sahteciliği Tespit Sonuçları

Bu aşamaya kadar ham videolarda test gerçekleştirilmiştir. Kurcalanan videolarda sıkıştırma ve bulanıklaştırma gibi son işlem atakları videoların istatistiksel özniteliklerinde değişim meydana getirmektedir. Dolayısıyla atakların uygulandığı videolarda sahteciliğin tespit edilmesi zorlaşmaktadır. Bu yöntem ile hem sıkıştırmaya karşı hem de bulanıklaştırma ataklarına karşı testler gerçekleştirilmiş ve elde edilen sonuçlar farklı sıkıştırma formatlarında ve farklı kalite standartlarında tek tek incelenerek rapor edilmiştir. Yöntemin literatürde kıyaslanan diğer çalışmalara göre özgün değerlerinden biri bu ataklara karşı dayanıklı olması, bir diğeri kaynak çerçevelerin tespit edilme doğruluklarının hesaplanması, bir diğeri ise farklı bir yaklaşım ile görselleştirilmiş ikili görüntülerden öznitelik çıkarılmasıdır. Bölüm 2.2.1.3’ de adımları verilen yöntemin ilk aşamasında özniteliklerin çıkarılması için videolar ön işlemeden geçirilmektedir.

Tablo 3. 2. Farklı blok boyutlarına göre değerlendirme sonuçları

Sıkıştırılmamış		4x4	8x8	12x12	16x16
	DO	0.6912	0.9646	0.9947	0.9966
	KE	0.3956	0.7445	0.9733	0.9358
	DU	0.3980	0.7155	0.9664	0.9698
	F1Skor	0.9966	0.9358	0.9315	0.9322

Ön işleme aşamasında öncelikle farklı ölçeklerdeki videolar 240x320 boyutlarına ölçeklenmektedir. Sonrasında video çerçeveleri bloklara bölünmektedir. Blok boyutları hem sıkıştırılmış hem de sıkıştırılmamış videolardan alınan başarı sonuçlarına göre deneysel olarak belirlenmiş olup en ideal sonucun 12x12 boyutlarında bloklar için alınmış olduğu gözlemlenmiştir. Bunun için elde edilen sonuçlar Tablo 3.2.’ de gösterilmektedir. Ön işleme de blokların ortalamaları alınarak, öznitelik görüntülerinin oluşturulmasında ortalamalara AKD ve ADD algoritmaları uygulanmaktadır. Çerçeve sayısı kadar öznitelik vektörünün alt alta sıralanması ile elde edilen öznitelik matrisi M , ikili görüntüye çevrilerek yeni bir yaklaşım ile öznitelik çıkarma aşaması tamamlanmaktadır.



Şekil 3. 13. Orjinal can_220_book videosuna ait (a) Sıkıştırılmamış orijinal videonun, (c) Sıkıştırılmamış sahte videonun, (e) H264 crf30 kalite faktörü ile sıkıştırılmış sahte videonun (g) MPEG-4 QS21 kalite faktörü ile sıkıştırılmış sahte videonun; AKD öznitelikleri alınmış ikili M görüntüsü (b) Sıkıştırılmamış orijinal videonun, (d) Sıkıştırılmamış sahte videonun (f) H264 crf30 kalite faktörü ile sıkıştırılmış sahte videonun, (h) MPEG-4 QS21 kalite faktörü ile sıkıştırılmış sahte videonun; Prewitt algoritması uygulanmış görüntüsü

Web-test/SULFA veri setinden alınan can_220_book videosuna ait sırasıyla orijinal, sıkıştırılmamış sahte ve H.264 crf-30 ile MPEG-4 QS21 kalite faktörlerinde sıkıştırılmış sahte videolardan alınan görsel çıktıları gösterilmektedir. *M* matrisine ait görseller Şekil 3.13. (a), Şekil 3.13. (c), Şekil 3.13. (e) ve Şekil 3.13. (g) ile gösterilmektedir. *M* matrislerinin ikili görüntü görselleri ise orijinal şekliyle Şekil 3.12. (b)' de, sıkıştırılmamış sahte şekliyle Şekil 3.13. (d)' de, H-264 ile sıkıştırılmış haliyle Şekil 3.13. (f)' de ve MPEG-4 ile sıkıştırılmış haliyle Şekil 3.13. (h)' de gösterilmektedir. Şekil 3.13' de gösterilen video önce sabit sonra hareketli arka plana sahip sahnelerden oluşmaktadır. Şekil üzerinde net olarak görünmesi için sabit arka planlı bölümden hareketli bölüme yapıştırma yapılmış ve öznitelik vektöründe de açıkça sahte olan yerlerin anlaşılması sağlanmıştır. Farklı sıkıştırma formatları ve sıkıştırılmamış video arasındaki fark da elde edilen ikili görüntü üzerindeki beyaz piksellerden fark edilmektedir. *M* matrisindeki yatay elemanlar 144 boyutlu olup her bir çerçeveye ait öznitelikleri, düşey elemanlar da videoda bulunan çerçeveleri göstermektedir. Bir sonraki aşamada tekrarlanan sahte çiftlerin bulunmasında, ikili görüntü üzerindeki kenar oluşturan aykırı çerçeve öznitelikleri yapıştırılan konumun yaklaşık olarak tespit edilmesini sağlar. Yapıştırılan çerçevelerin bulunması işleminden sonra ilgili çerçeve ile eş olabilecek kaynak çerçevelerin tespiti gerçekleştirilmektedir. Son aşamada ise bulunan çerçevelerin komşuluk ilişkileri incelenerek yanlış pozitiflerin elenmesi sağlanmaktadır. Böylece sahte çerçevelerin asıl konumları bulunmaktadır.

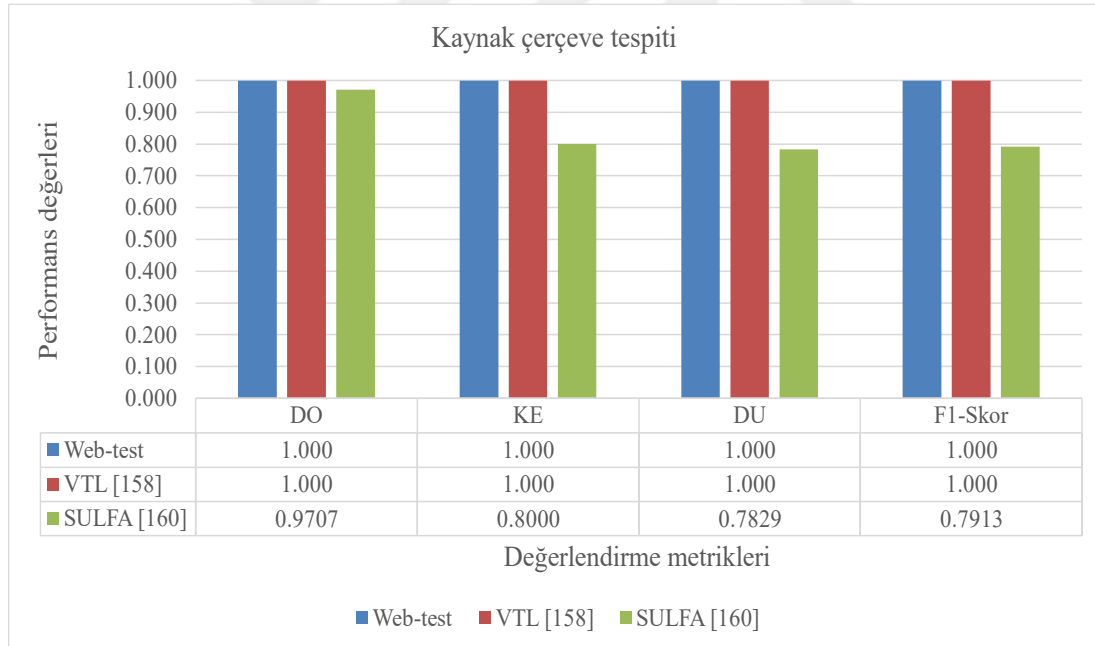
Sıkıştırılmış videolar için farklı sıkıştırma kalite formlarında incelenmiş blok boyutunun belirlenmesinde ideal sonucun 12x12 olduğu gözlemlenmiştir. Tablo 3.3.' de blok boyutu 12 olan farklı kalite oranlarında sıkıştırılmış H264 videoların ortalama doğruluk oranı %97' dir. Blok boyutu 16 olduğunda ortalama doğruluk oranı %96' dır. F1-skor değeri ise 12 bloklu videolarda ortalama %85 iken 16 bloklu videolarda %96 olmaktadır. Dolayısıyla bu sonuçlar dikkate alındığında elde edilen blok boyutu 12 olarak belirlenmiştir.

Bu yöntemin literatürdeki çalışmalara katkı sağlayacak bir diğer özgün değeri, tekrarlama sahteciliğinde kaynak çerçevelerin, algılanma doğruluğunun tespiti gerçekleştirilmektedir. Yapılan çalışmalarda tekrarlama sahteciliğinin tespiti gerçekleştirilirken çiftler halinde algılama doğruluğu hesaplanmaktadır. Bu çalışmada ise sahte olarak bulunan çerçevenin kopyasının alındığı kaynak çerçevenin de tespiti gerçekleştirilmektedir.

Tablo 3. 3. Farklı sıkıştırma kalitelerine göre elde edilen değerlendirme sonuçları

	Blok boyutu 12x12						Blok boyutu 16x16					
	CRF-6	CRF-12	CRF-18	CRF-24	CRF-30	CRF-36	CRF-6	CRF-12	CRF-18	CRF-24	CRF-30	CRF-36
<i>DO</i>	0.9869	0.9887	0.9827	0.9707	0.9477	0.9484	0.9973	0.9904	0.9858	0.9670	0.9553	0.8683
<i>KE</i>	0.9500	0.9488	0.9500	0.9000	0.8000	0.8500	1.0000	1.0000	1.0000	0.9000	0.8421	0.6500
<i>DU</i>	0.9294	0.9296	0.8934	0.8270	0.6936	0.6558	0.9784	0.9290	0.8930	0.7780	0.6877	0.4436
<i>F1-skor</i>	0.9396	0.9391	0.9127	0.8520	0.7220	0.7081	0.9396	0.8911	0.8643	0.8037	0.6876	0.4864

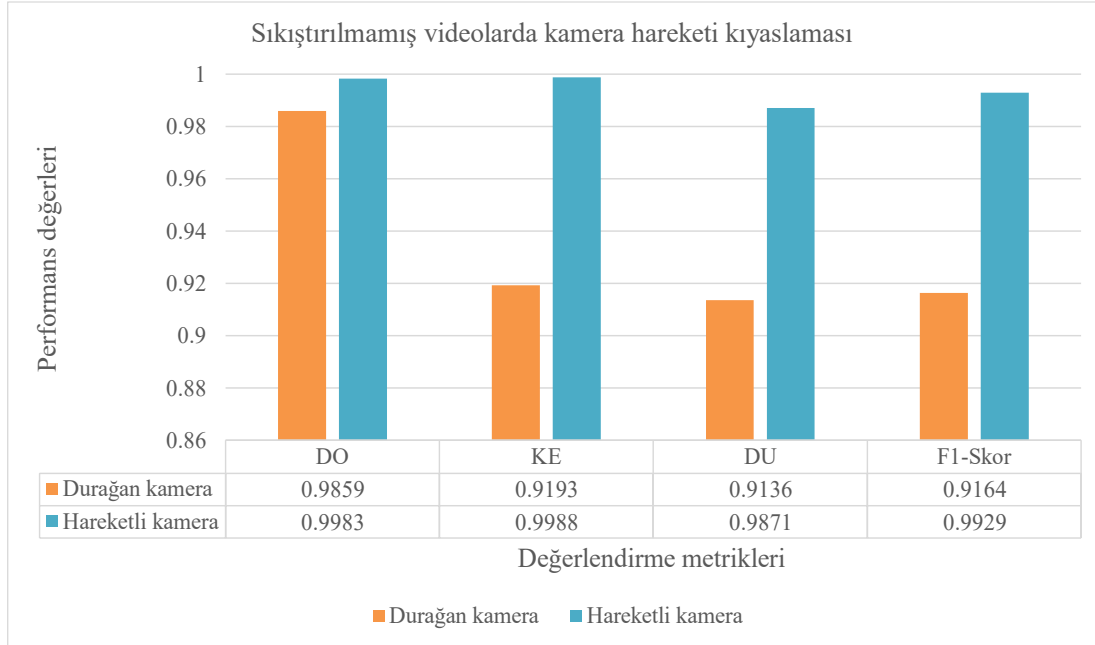
Üç farklı veri tabanında yapılan testlerden alınan kaynak çerçeve tespit sonuçları Şekil 3.14.' de gösterildiği gibidir.



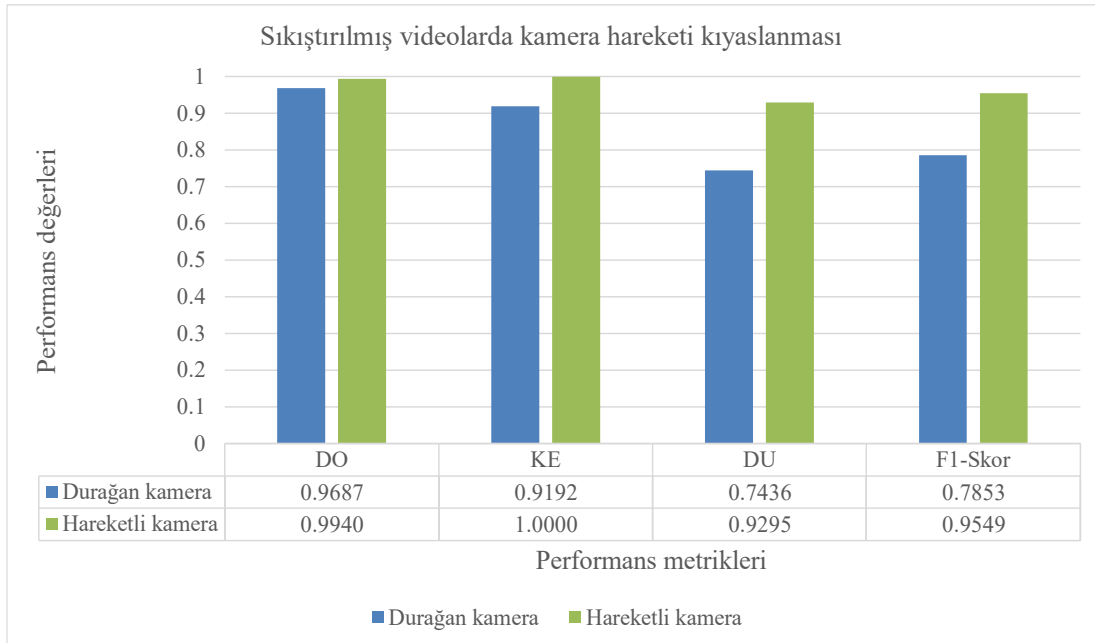
Şekil 3. 14. Kaynak çerçeve tespit sonuçları

Literatürde değerlendirilmesi çok az çalışmada bulunan ve video kayıtlarını yapan cihazlara göre sabit ve hareketli videolar olarak sınıflandırılması sonucunda elde edilen doğruluk oranı grafiği Şekil 3.15. ve Şekil 3.16.' da gösterildiği gibidir. Videoların bu şekilde sınıflandırılması yöntemin farklı bir tespit başarısını göstermektedir. Çünkü

oluşturulan algoritmaların bazısı durağan sahneli videoların, art arda gelen çerçevelerinin birbirlerine çok benzemesi dolayısıyla düşük tespit gerçekleştirmektedir.



Şekil 3. 15. Sıkıştırılmamış sabit ve hareketli kamera ile çekim yapılan videolarda elde edilen tespit sonuçları



Şekil 3. 16. Sıkıştırılmış sabit ve hareketli kamera ile çekim yapılan videolarda elde edilen tespit sonuçları

Bazı videolarda ise içeriğin çok hareketli olması çerçevelerin birbirleriyle hiç ilişkili değilmiş gibi olmasına doğruluk oranlarının düşmesine neden olmaktadır. Şekil 3.15.' de görüldüğü gibi DO değerleri arasında çok fark bulunmaması yöntemin durağan ve hareketli sıkıştırılmamış videoların hepsi için iyi çalıştığını göstermektedir. Bu yöntem içerisinde komşuluk ilişkilerinin tek tek incelenmesi sayesinde elde edilen bir başarıdır.

Kamera hareketine göre sınıflandırma, farklı türden video kayıtlarına karşı algoritmanın dayanıklılığını göstermektedir. Bu çalışma içerisinde kullanılan veri tabanındaki 30 videonun 13'ü sabit kamera ile çekilmiş 17'si ise hareketli kamera ile çekilmiştir.

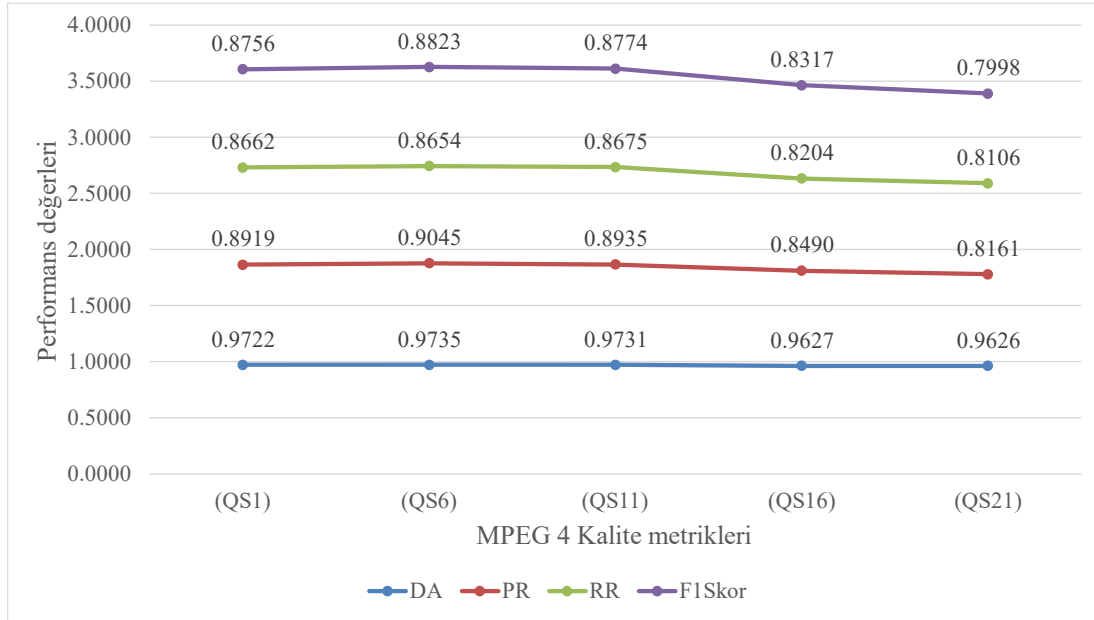
Şekil 3.15. ve Şekil 3.16.' daki sonuçlar incelendiğinde sıkıştırılmamış videolar için sabit kamera ile %98 doğruluk oranı sağlanırken, hareketli kamera için %99 doğruluk oranı sağlanmıştır. Sıkıştırılmış videolar da ise bu oran beklenildiği gibi düşmekte ve özellikle sabit sahneli videolarda daha fazla veri kaybı yaşanacağı için doğruluk oranı daha da düşmektedir. Sahte olan çerçevelerin tamamının bulunamamasından dolayı duyarlılık miktarı durağan sıkıştırılmış videolar için %78' lere kadar gerilemektedir.

MPEG- 4 ve H.264 formatında sıkıştırılmış videolar için elde edilen sonuç değerleri de Şekil 3.17.' de verildiği gibidir. Bir sonraki değerlendirme parametresi olarak farklı sıkıştırma formatlarında farklı sıkıştırma kalite oranları kullanılarak elde edilen kriterlere göre performans değerlendirilmesi yapılmıştır. Elde edilen sonuçlar MPEG-4 formatı için QS1, QS6, QS11, QS16 ve QS21; H.264 formatında da CRF-6, CRF-12, CRF-18, CRF-24 ve CRF-30 sıkıştırma kalite ölçütleri referans olarak belirlenerek sonuçlar test edilmiştir. H.264, MPEG-4'ün daha güncel bir sıkıştırma kodeğidir. H.264 kodeği ile sıkıştırma yapıldığında önceki MPEG-4 kodeklerine göre daha yüksek bir sıkıştırma sağlanmaktadır. Buna karşın video kalitesinde daha az kayıp olmaktadır [137]. Kalite metriklerindeki artış oranları seçilirken yapılan sıkıştırma ile videoların bellekte kapladıkları alanların yaklaşık olarak yarı boyuta indiği düşünülerek seçim yapılmıştır.

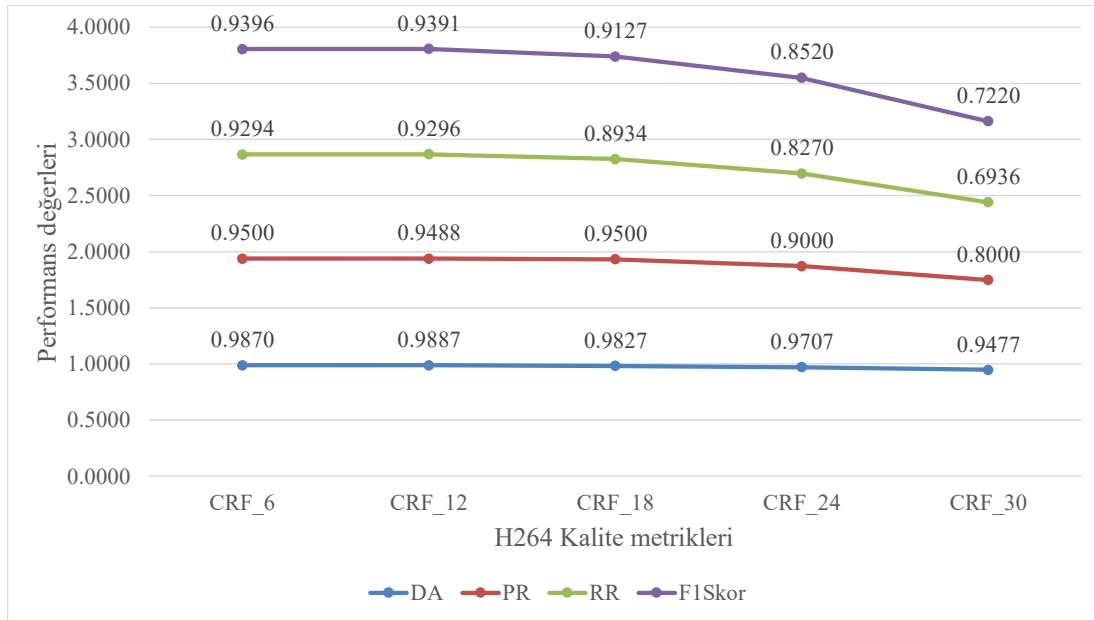
Şekil 3.17. (a) ve (b)' de görüldüğü gibi sıkıştırma kalitesi artıkça veri kaybının artmasıyla birlikte çerçevelerin birbirlerine benzerliği düşmekte; dolayısıyla tekrarlama sahteciliği için yapılan bu testler de tanılama doğruluğu da düşmektedir.

Şekil 3.18. sıkıştırılmamış ve MPEG-4 ile H.264 formatlarında sıkıştırılan videoların ortalama performans ölçütleri verilmektedir. Sıkıştırılmamış videolarda beklenildiği gibi en yüksek doğruluk elde edilmektedir. Sıkıştırılmış video sonuçları değerlendirildiğinde oldukça yakın sonuçlar elde edildiği görülmüştür. MPEG-4 kullanılan videolarda sıkıştırma oranı daha az olsa da nispeten daha düşük görüntü kalitesi oluşmaktadır.

Böylece daha düşük performans değerleri elde edilmesi mümkün olmaktadır. Diğer yandan videoların hareketli içerik içermesinden dolayı, kullanılan video türlerinin etkisi de söz konusu olmaktadır.

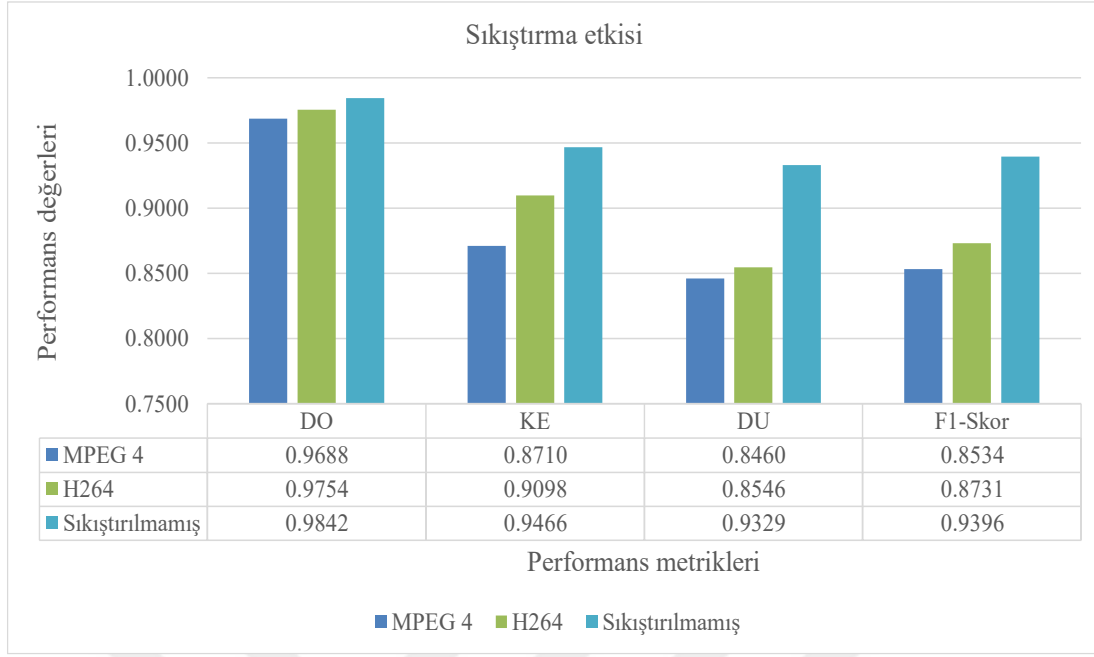


(a)



(b)

Şekil 3. 17. (a) MPEG-4 (b) H.264 ile sıkıştırılmış videolar için farklı kalite oranlarında sıkıştırma etkisinin izlenmesi



Şekil 3. 18. Sıkıştırılmış ve sıkıştırılmamış videolarla olan tespit kıyaslaması sonuçları

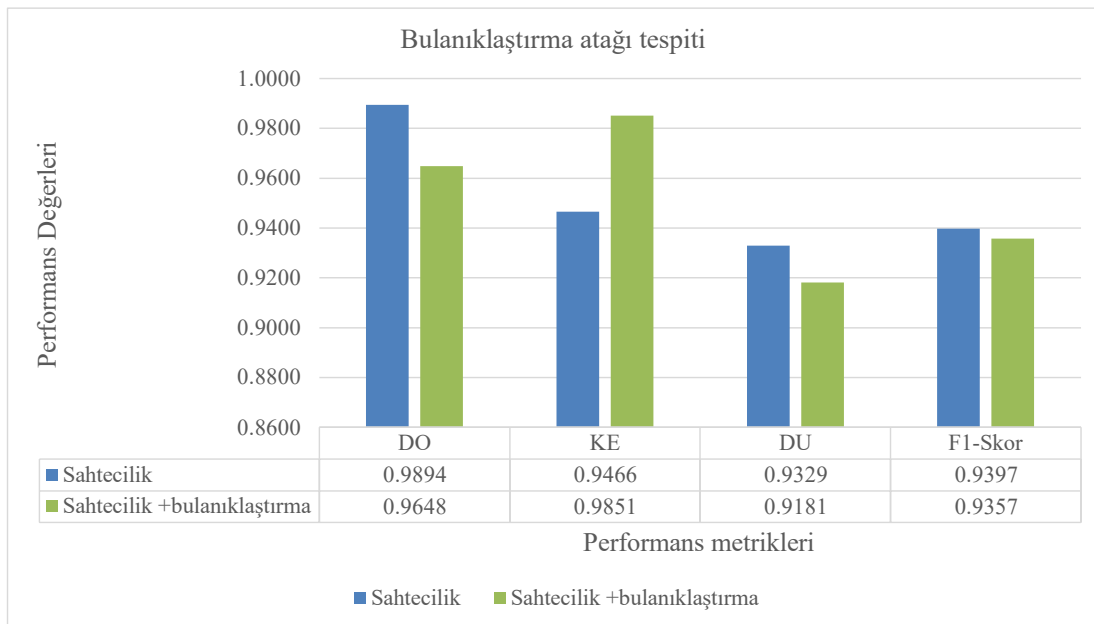
Bu durumun sonuçlara etkisi incelendiğinde, deneylerde farklı kodekler kullanılmasına rağmen, kullanılan veri tabanında sıkıştırılmış video tespit performanslarında çok büyük fark oluşmadığı gözlemlenmiştir.

Süre açısından incelediğimiz de ise genel olarak veri kaybı artmasına rağmen yapılan kıyaslama sayısı aynı olduğu için çok az bir farkla azalma ve artmalar gerçekleşmektedir. Tablo 3.4.' de farklı sıkıştırma formatları için koşma sürelerini göstermektedir.

Tablo 3. 4. MPEG-4 ve H.264' e göre ortalama koşma süreleri

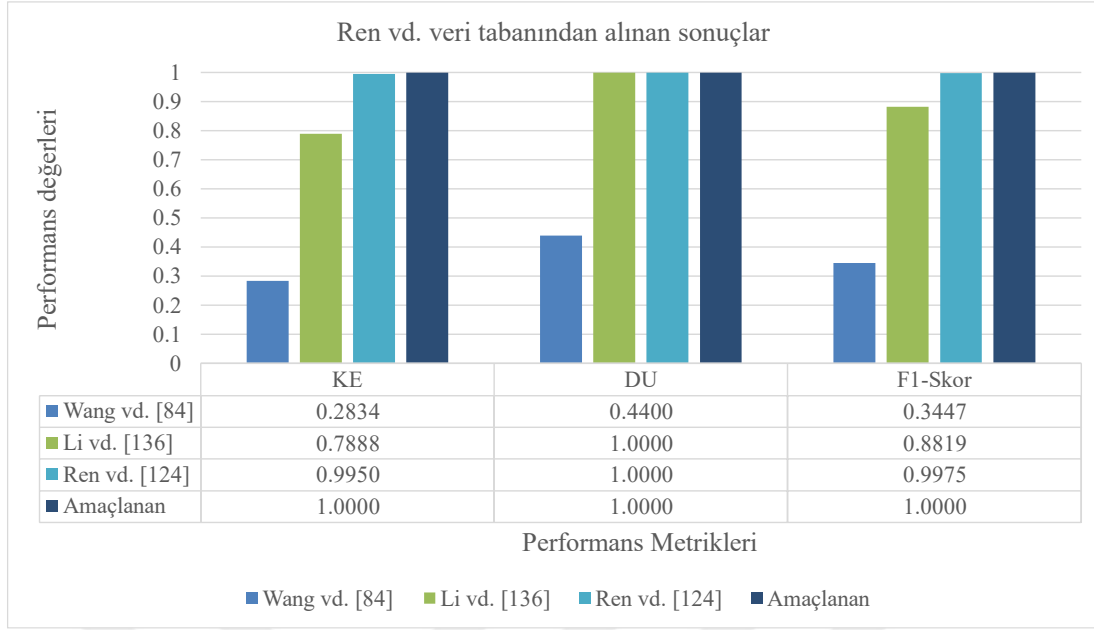
MPEG-4 kalite oranlarına göre çerçeve başına düşen ortalama koşma süreleri (s/çerçeve)				
QS1	QS6	QS11	QS16	QS21
0.0101	0.0104	0.0101	0.0108	0.0108
H.264 kalite oranlarına göre çerçeve başına düşen ortalama koşma süreleri (s/ çerçeve)				
CRF6	CRF12	CRF18	CRF24	CRF30
0.0119	0.0119	0.0119	0.0117	0.0104

Sahtecilik yapan kişiler tarafından yapılan sahtecilik izlerinin kapatılması ve tespit tekniklerinin işe yaramamasını hedefleyen son ataklardan birisi de bulanıklaştırma atağı olup, yöntemin atağa dayanıklılığı test edilmiştir. Sahtecilik yapılan videolarda sonrasında bulanıklaştırma işlemi uygulanmış 20 SULFA veri tabanından alınan video üzerinden test gerçekleştirilmiştir. Elde edilen sonuçlar Şekil 3.19.' da verildiği gibidir. VirtualDub üzerinden uygulanan ataklı videoların algılama doğruluğu %96 olarak bulunmuştur. Atak uygulanmadan önce elde edilen doğruluk oranı ise %98 olup beklenildiği gibi doğruluk oranı küçük de olsa azalma yaşamıştır.

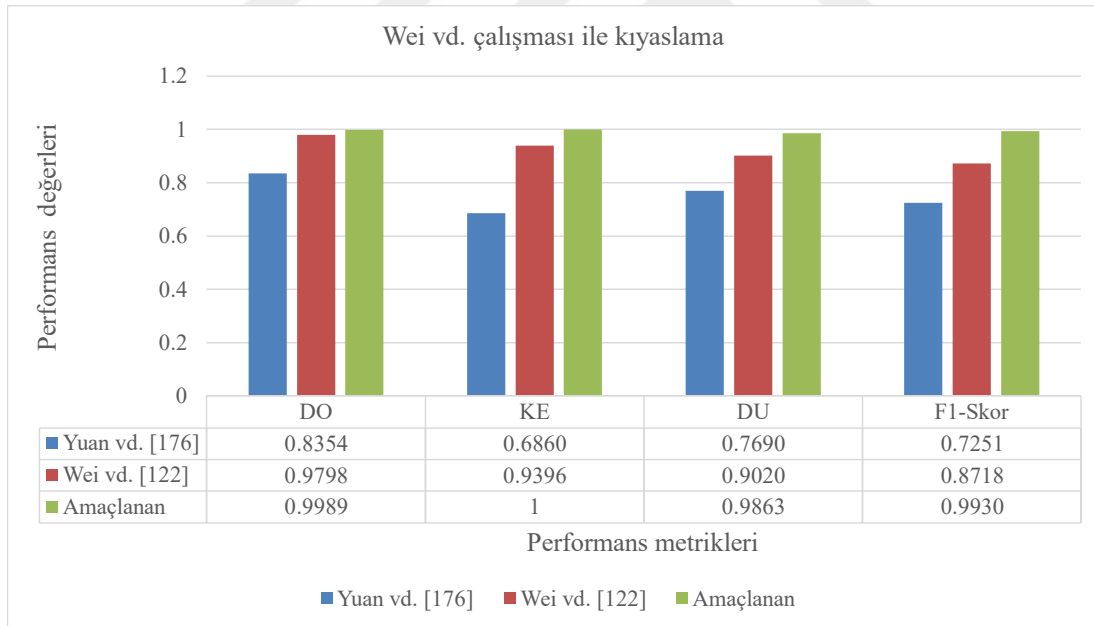


Şekil 3. 19. Bulanıklaştırma ataklarına karşı elde edilen sonuçlar

Kaynak çerçevelerin tespiti, kameraların sabit ve hareketli olmasına göre sahtecilik tespiti, sıkıştırma ve bulanıklaştırma ataklarına karşı dayanıklılığın test edildiği bu çalışma birbirinden farklı özellikleri içeren ve literatürde popüler olan veri setleri üzerinde de test edilmiştir. İlk olarak Ren vd. önerdiği çalışmada kullanılan veri seti üzerinden alınan sonuçlar ile kıyaslama yapılmıştır. Bu veri setinin özelliği VTL veri tabanından alınan videoların başlangıç konumlarından eşit sayıda alınan çerçevelerin tüm videolar için video sonuna tekrar yapıştırılmasıyla veri tabanı oluşturulmuştur. Elde edilen sonuçların ve Ren vd.' nin ortak olarak kullandığı veri setinden alınan sonuçlar Şekil 3.20.' de gösterildiği gibidir. Ren vd.' nin çalışmasında DO rapor edilmediği için tespit sonuçlarında kıyaslamaya yer verilmemiştir.



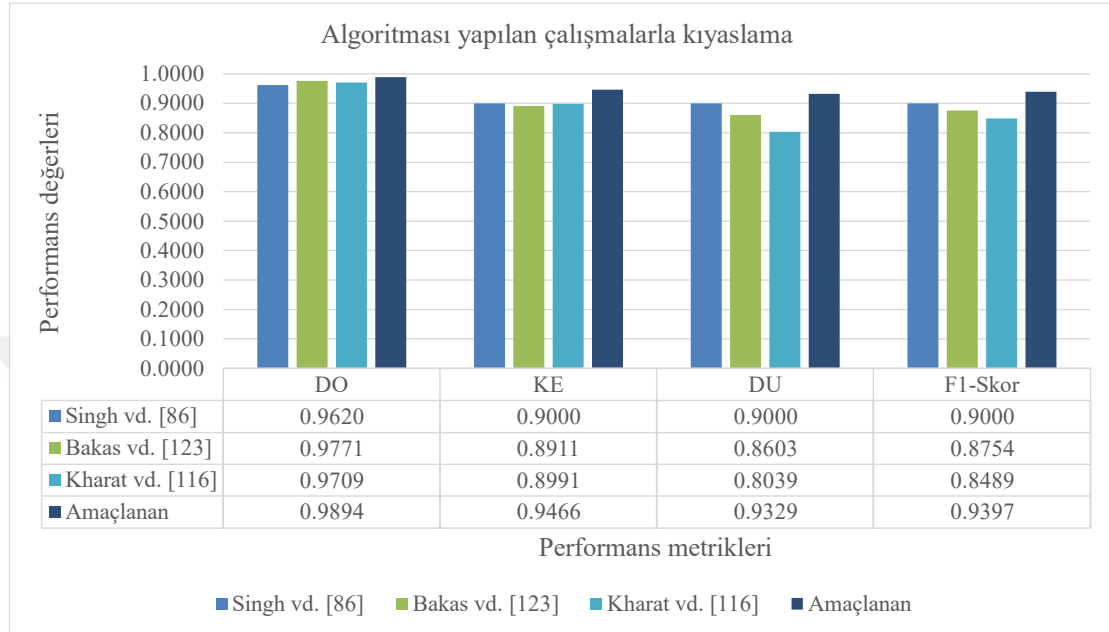
Şekil 3. 20. Ren vd. çalışması ile ortak veri tabanı kullanılarak tekrarlama sahteciliği tespit sonuçları



Şekil 3. 21. Wei vd. çalışması ile ortak veri tabanı kullanılarak tekrarlama sahteciliği tespiti sonuçları

Wei vd. önerildiği çalışma [122] için Yuan vd. [176] oluşturduğu veri tabanı kullanılmış rastgele konumlardan alınan çerçevelerin bir kısmı eklenerek yapıştırılırken, bir kısmı mevcut çerçevelerin üzerine yapıştırılmıştır. Kıyaslama sonuçları Şekil 3.21.' de gösterilmektedir.

Ortak veri tabanı kullanılarak oluşturulan iki farklı tarzdaki veri tabanı ile kıyaslamaların dışında bir de algoritmaları koşularak kıyaslaması yapılan son yılların popüler çalışmaları ile kıyaslamaları da Şekil 3.22.' de verildiği gibidir.



Şekil 3. 22. Algoritması koşulan çalışmalar ile kıyaslama sonuçları

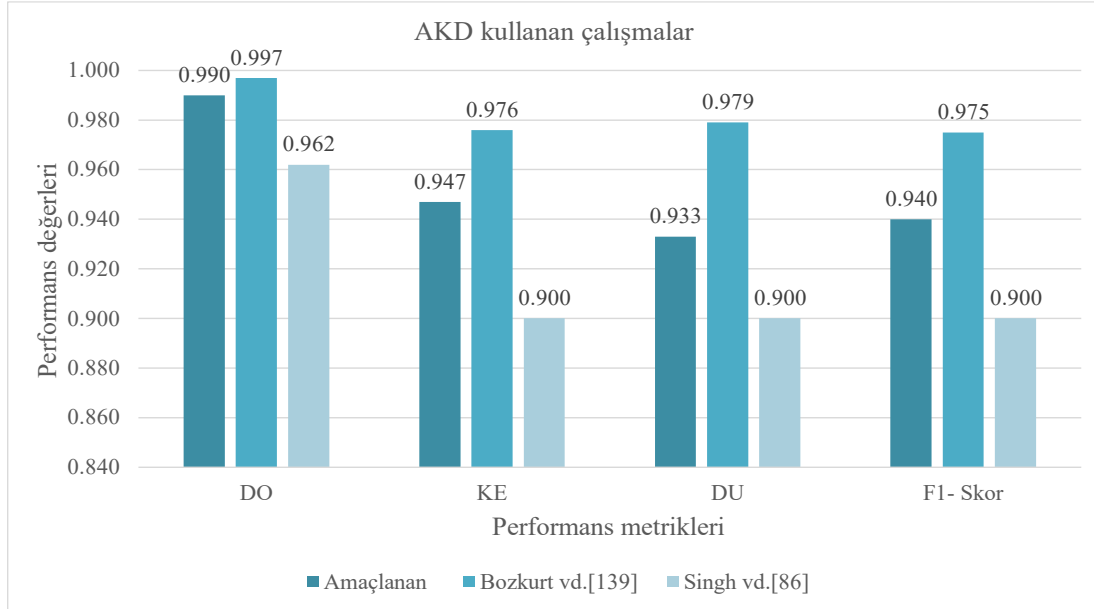
Bu algoritmalar kullandıkları veri tabanlarında koşulurken statik eşik kullanılmıştır. Ancak kullanılan bu eşiklerin bizim oluşturduğumuz veri tabanı için uygun olmaması dolayısıyla yanlış pozitiflerin sayısı artmıştır. Dolayısıyla mevcut algoritmaların eşikleri dinamik olacak şekilde değiştirilmiştir. Bu çalışmaların süre bakımından kıyaslaması da Tablo 3.5' de verildiği gibidir.

Tablo 3. 5. Kıyaslanan çalışmaların ortalama koşma süreleri

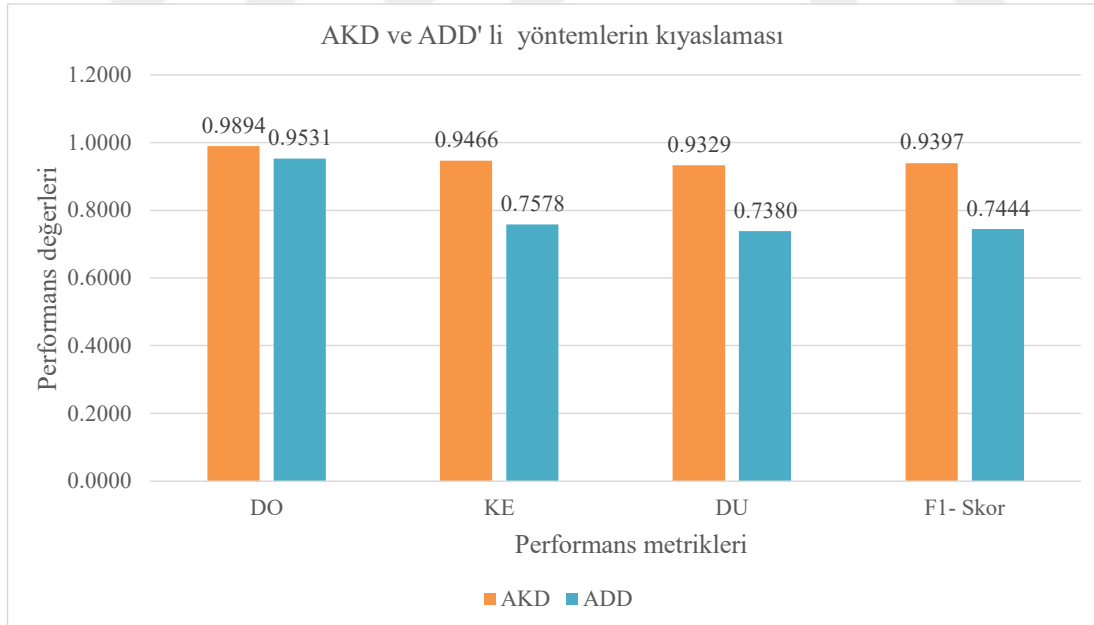
	Kharat vd.	Bakas vd.	Singh vd.	Amaçlanan
<i>s/çerçeve</i>	0.1607	0.0389	0.0109	0.0110

Yöntemin başarısı, istatistiksel özniteliklerden AKD tabanlı öznitelik çıkarım algoritmasını kullanarak yapılan yöntemlerle kıyaslandığında elde edilen sonuçlar Şekil 3.23.' de gösterildiği gibi olmaktadır. Şekil 3.23.' de Bozkurt vd. [139]' nin önerdiği

yöntemin bu çalışmada kullanılan veri tabanında da başarılı sonuçlar ürettiği gözlemlenmiştir.



Şekil 3. 23. AKD tabanlı yöntemlerin kıyaslanması



Şekil 3. 24. AKD ve ADD yöntemlerinin kıyaslamalı sonuçları

Bozkurt vd.' nin çalışmasında çiftler halinde araştırma yapılması yöntemin başlangıç veya bitiminde sahtecilik yapılması durumunda yöntemin başarısının düştüğü

gözlemlenmiştir. Burada kullanılan veri tabanında bu tarz bir çalışma olmadığı için başarı yüksek görünmektedir.

Frekans özniteliklerini kullanabileceğimiz bir diğer yöntem olan dalgacık dönüşümü, AKD yerine kullanılarak ikisinin, SULFA veri tabanında oluşturularak elde edilen tespit sonuçlarının da kıyaslaması gerçekleştirilmiştir. Kıyaslama sonuçlarına ait görsel Şekil 3.24.' de verildiği gibidir. AKD kullanılarak gerçekleştirilen çalışmada ortalama koşma süresi 0.0110 iken dalgacık dönüşümü kullanıldığında 0.0139 sn sürmektedir.

Bu çalışmanın kıyaslamasını yaptığımız diğer çalışmalarla kıyaslamasını yaptığımızda kaynak çerçevelerin tespit sonuçlarının verilmesi, bulanıklaştırma ataklarına karşı test edilmesi farklı sıkıştırma oranlarında farklı kalite metriklerine göre kıyaslamalarının yapılması sonucunda diğer çalışmalardan [84][86][116][122][123][124] [136] [139] daha iyi olduğu gözlemlenmiştir. Ancak yöntem birden fazla sahteciliğe çözüm sunamamaktadır. Özetlemek gerekirse yapılan birinci çalışma ile 6 farklı yönden çalışmaların incelemesi gerçekleştirilmiştir. Bu incelemeler Şekil 3.25.' de verildiği gibidir.



Şekil 3. 25. Önerilen yöntemin hangi açılardan incelendiğinin gösterilmesi

Aynı zamanda yapılan çalışmanın elde edilen sonuçları farklı veri tabanları kullanılarak ve oluşturulan ortak veri tabanı üzerinden farklı çalışmaların algoritması

koşularak kıyaslanmış, aynı öznitelik çıkarım tekniğini kullanan farklı çalışmalarla kıyaslanmış ve son olarak frekans düzlemini kullanan AKD ve ADD yöntemleri ile öznitelik çıkarımı kullanarak kıyaslanmıştır.

Tekrarlama sahteciliği ile yapılan testler sonrasında doku tabanlı yöntemin başarısı kenar tabanlı yaklaşıma göre daha efektif olmakta ancak sıkıştırma atakları başarısını düşürmektedir. Frekans tabanlı çalışmalar ile de sıkıştırma işlemine dayanıklılık sağlanmaktadır.

3.3.4. Çerçeveler Arası Sahteciliklere Çözüm Sunmak İçin Önerilen Çalışma Sonuçları

3.3.4.1. Silme Sahteciliği Tespit Yöntemi Sonuçları

Silme sahteciliğinin tespitinin gerçekleştirildiği bu çalışmada birçok açıdan değerlendirilme yapılmıştır. Silme konumunun tespiti için hareketli ve hareketsiz videolarda çeşitli sıkıştırma formatlarında ve kalite metriklerinde, testler yapılmıştır.

Bu yöntem ile literatürde silme sahteciliği tespitine yönelik, yapılan çalışmalarda kullanılan anomali tespitine dayalı izlenilecek adımların farkına varılması gerçekleştirilmiştir. Bu amaçla SULFA veri tabanı kullanılarak 20 farklı orijinal video ve Trace Library' den 5 orijinal video alınarak Wei vd.' nin [122] çalışmayla karşılaştırılması yapılmıştır. SULFA veri tabanından alınan can_220_garden (1) videosuna ait 1. çerçeve Şekil 3.26. (a)' da, videonun 1. çerçeve ile diğer çerçevelerinin TSGO kıyaslaması Şekil 3.26. (b)' de ve ardışık çerçevelerin TSGO değişim grafiği Şekil 3.26. (c)' de gösterilmektedir.

Tablo 3.6' da Wei vd.' nin kullanmış olduğu veri tabanından alınan sonuçlar gösterilmektedir. Tabloda gösterildiği gibi bu 5 videonun konumu tam olarak tespit edebilirken, kıyaslaması yapılan yöntem 4 videoyu 1'er farkla birini ise tam tespit edebilmiştir. Lin ve Chang' ın çalışması [85] ise bu videolarda gerçekleştirilen silme sahteciliklerinin hiçbirini tespit edememiştir. [85]' deki çalışmanın sonuçları Wei vd.' nin çalışmasında rapor edildiği şekilde ortak veri tabanı üzerinden test yapılarak verilmektedir. Önerilen yöntemin saniyede çerçeve başına koşma süresi beş video üzerinden ortalama 1 ms/çerçeve' dir.

Tablo 3. 6. Wei vd.' nin önerdiği veri tabanına göre kıyaslama sonuçları

No	Silme aralığı	Toplam çerçeve	Hatalı çerçeve			Süre (ms/çerçeve)
			Önerilen yöntem	[122]	[85]	
1	140-190	250	0	1	Tespit edemedi	0.6
2	240-279	261	0	0	Tespit edemedi	0.7
3	221-249	272	0	1	Tespit edemedi	0.7
4	131-150	1046	0	1	Tespit edemedi	0.5
5	100-119	131	0	1	Tespit edemedi	1.2

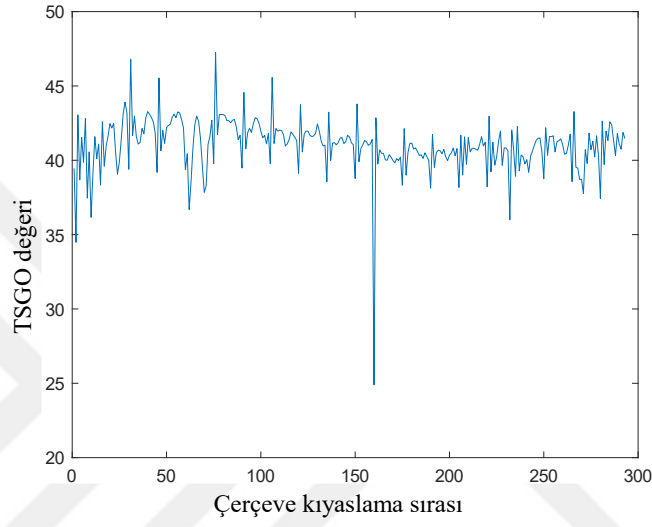
H.264 ve MPEG-4 formatlarında kalite faktörleri 31, 15, 1 olacak şekilde 100 sahte video oluşturulmuştur. Veri tabanı oluşturulurken 4'er tane; 50'den 10 çerçeveye kadar silme işlemi yapılmıştır. Böylece silinen çerçeve sayısının sahtecilik algılama performansını da etkilemediği gözlemlenmiştir. Silme sahteciliğinde durağan sahneye bir nesnenin girmesi TSGO değişiminde ani bir sıçramaya neden olmaktadır. Ancak sahneye giren nesnenin ilerlemesi bir akış meydana getireceği için yani birden fazla çerçeve de değişime neden olacağı için tek çerçeve yerine ardışık çerçeve TSGO' larının incelenmesi daha doğru sonuçların alınmasını sağlamaktadır. Ani değişimin olduğu yerler sadece silme sahteciliğinin yapıldığı yerlerde olmadığından bir eşik değerinin kullanılması kaçınılmaz olmaktadır.

Nesnenin gizlendiği veya sahnelerin tamamen silindiği videolarda TSGO farkında meydana gelen değişim yüksek olmaktadır. Bu çalışma için deneysel olarak belirlenen eşik değeri 2 olarak seçilmiştir.

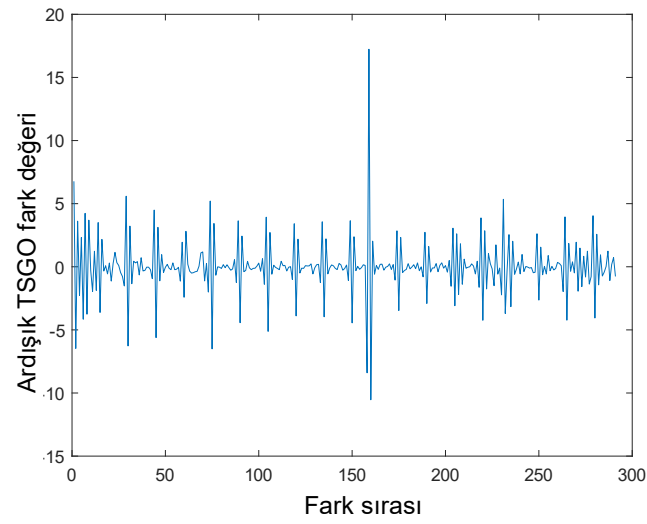
Silme sahteciliğine çözüm bulmak amacıyla ardışık çerçeveler arası fark çerçevelerinin TSGO özniteliklerinin değişimine dayalı önerilen çalışmadan elde edilen sonuçlar Şekil 3.27.' deki gibidir. Bu şekilde de görüldüğü gibi farklı kodek yapılarına bağlı olarak DO değişmektedir. Ayrıca sıkıştırma oranı artıkça başarı düşmektedir. Kullanılan veri tabanındaki sıkıştırılmamış videoların tamamının silme konumu tam olarak tespit edilebilmektedir.



(a)

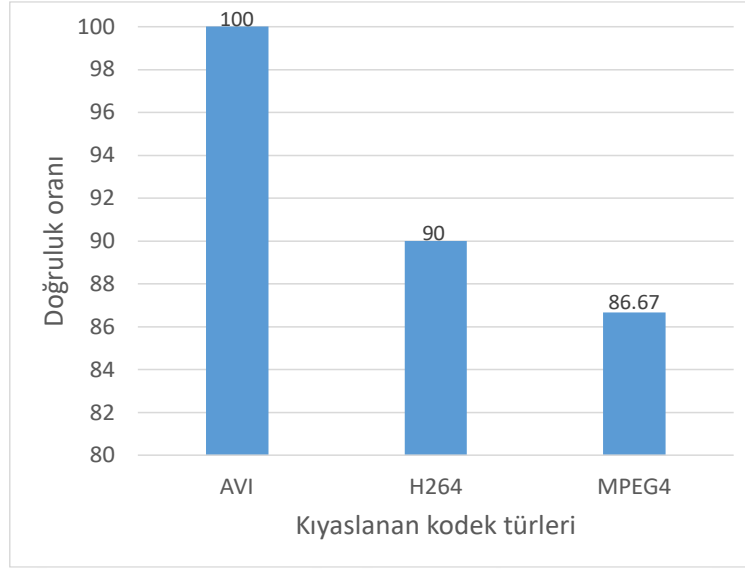


(b)

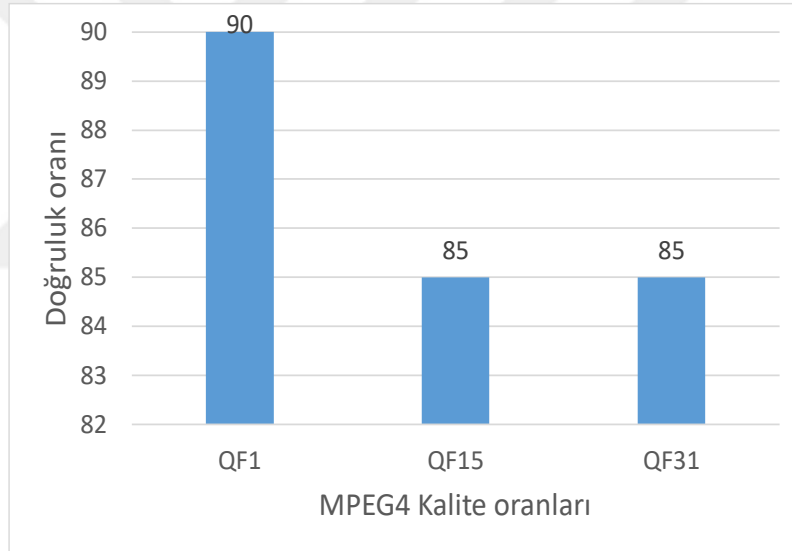


(c)

Şekil 3. 26. (a) 160. çerçevede silme sahteciliği yapılan can_220_garden (1) videosunun çerçeve örneği (b) TSGO grafiği (c) TSGO' ların değişim grafiği



(a)



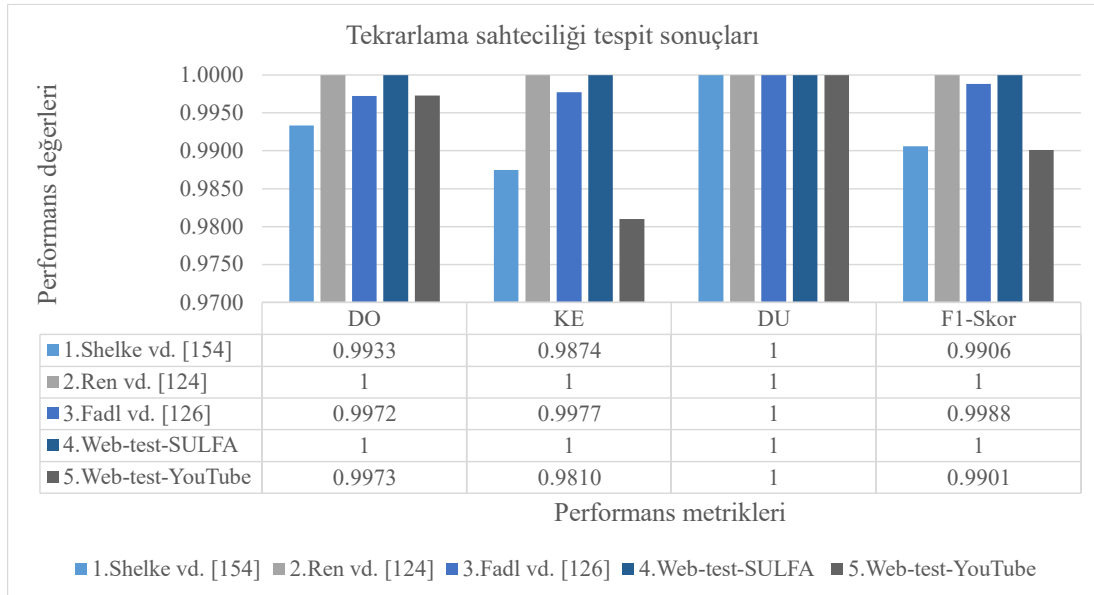
(b)

Şekil 3. 27. Silme sahteciliğinin farklı sıkıştırma metriklerinden elde edilen sonuçları

Yöntemin koşma süreleri sıkıştırılmamış videolar için ortalama 0.0007s, H264 videolar için 0.0005s, MPEG-4 videolar için ise 0.0006s sürmektedir. Sonuçlardan gözlemlendiği gibi silme sahteciliğinin yapıldığı konumun tespiti çıkarılan özniteliklerin komşuluk ilişkileri göz önünde bulundurularak anomali tespitine göre gerçekleştirilebilir.

3.3.4.2. Silme, Tekrarlama, Ekleme ve Karma Olmak Üzere Çerçeveler Arası Sahteciliklerin Tespitine Yönelik Önerilen Çalışma Sonuçları

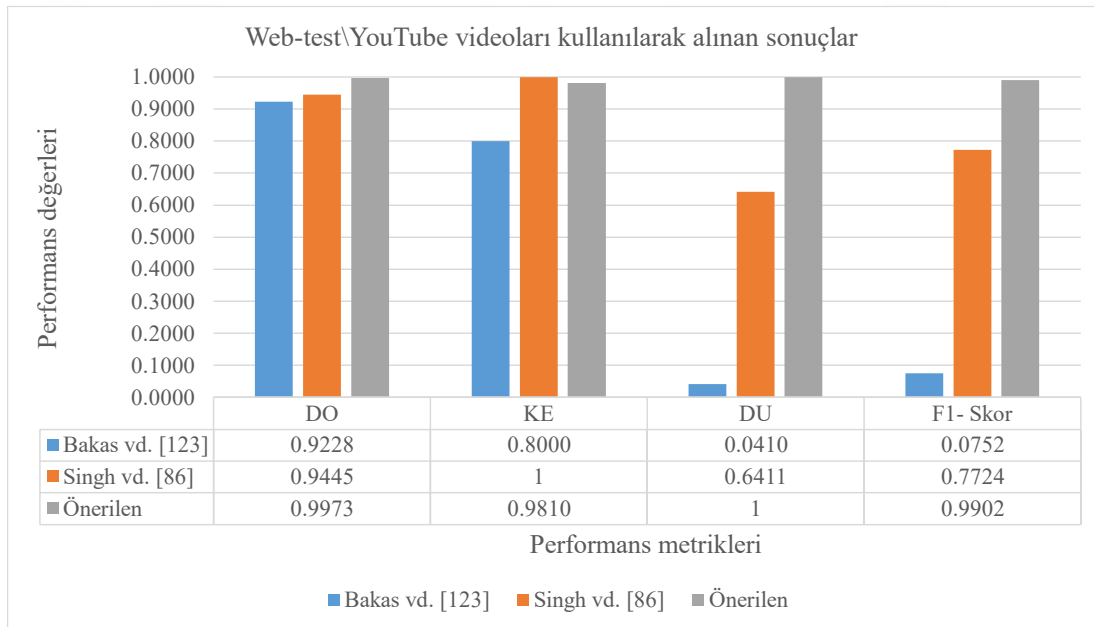
Silme sahteciliği tespitinden elde edilen başarılı sonuçlar neticesinde hem silme hem de tekrarlama sahteciliklerine çözüm bulabilen yeni bir algoritmanın tasarlanabileceği öngörülmüştür. Bu doğrultuda yeni bir çalışma olan PYGH algoritmasına dayalı tüm çerçeveler arası sahteciliklere çözüm sunabilen yeni bir yöntem önerilmiştir. Yöntemin detayları Bölüm 2.3.2.2’ de anlatılmaktadır. Yöntemin literatürdeki çalışmalara göre avantajı literatürde bahsi geçen tüm çerçeveler arası sahteciliklere çözüm sunabilmesi ve bunu yaparken de yapılan sahteciliğin sayısının birden fazla olması durumunda kontrolünün yapılabilmesidir. Aynı zamanda önerilen algoritma çerçevelere ADD dönüşümü uygulandıktan sonra öznitelik çıkarımı yapılarak sıkıştırma ataklarına da dayanıklı hale getirilmiştir. Son yılların popüler 3 farklı veri tabanlarında ve Web-test’ ten alınan videolarda yapılan sahtecilikler üzerinden testler gerçekleştirilmiştir. [124][126][154] veri tabanlarından ve Web-test videolarından elde edilen sonuçlar Şekil 3.28.’ deki gibidir. Bu sonuçlar tekrarlama sahteciliği için oluşturulan videolardan alınan sonuç değerleridir.



Şekil 3. 28. PYGH’ 1ı çalışmanın farklı veri tabanlarından alınan sonuç kıyaslamaları

Şekil 3.28. incelendiğinde tüm veri tabanlarından elde edilen DU’ ların 1 olduğu, yani sahte çerçevelerin hepsinin bulunduğu görülmektedir. KE değerleri ise Ren vd. [124]

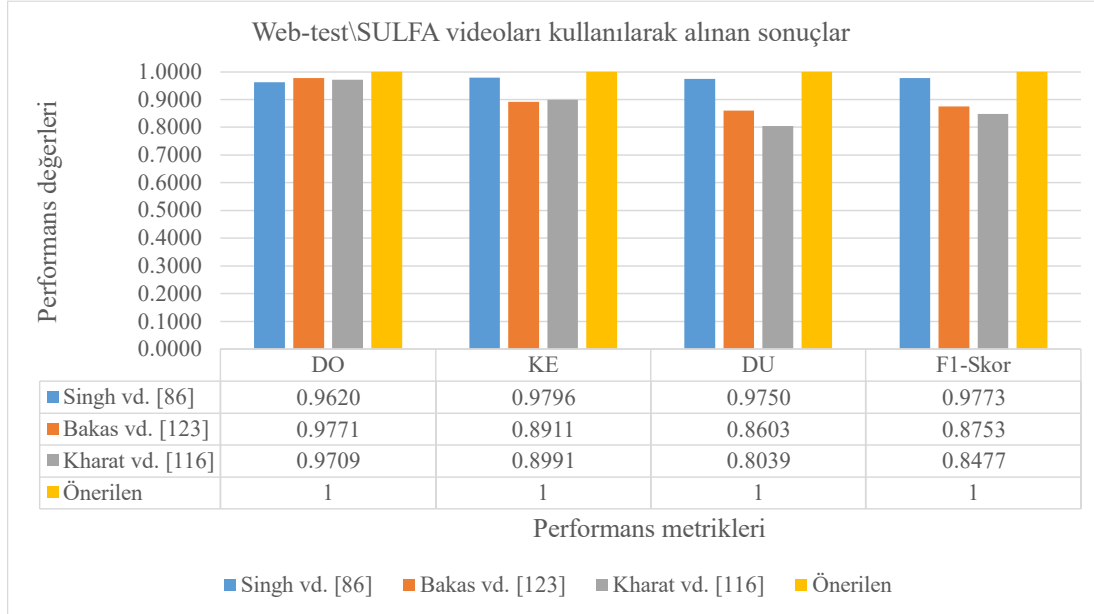
ile Web-test' in kullandıkları veri tabanlarında tüm orijinal çerçevelerin de tam olarak bulunduğu ancak diğerlerinde fazladan sahte çerçevelerin bulunabildiği gözlenmektedir. Yöntem, gelen olarak bakıldığında tekrarlama sahteciliği tespitinde %99 DO ile başarılı sonuçlar elde edilmesini sağlamaktadır. Tekrarlama sahteciliğinin tespitinde her veri tabanında farklı çalışmalarla olan kıyaslamaların da gösterimi yapılmıştır. Kharat vd. [116], Singh vd. [86] ve Bakas vd. [123] kıyaslama yapılan çalışmalardır. Bu çalışmaların algoritması oluşturularak, ilgili veri tabanlarında koşmak suretiyle kıyaslama yapılmaktadır. İlk olarak kendi oluşturduğumuz veri seti olan Web-test üzerinden YouTube'dan alınan videolar ile elde edilen sonuçlar Şekil 3.29.' da gösterilmektedir.



Şekil 3. 29. Web-test veri tabanından alınan sonuçlar

Şekil 3.29.'da yapılan kıyaslamalarda Kharat vd.' nin [116] önermiş olduğu çalışmaya ait sonuçlar verilmemektedir. Çünkü çalışma içerisinde kullanılan algoritmanın çalışma süresi gerçek hayatta kullanılan videolara uygulanmaya elverişli olmamaktadır. Elde edilen sonuçlara bakıldığında Bakas vd.' nin [123] önermiş olduğu çalışma içerisinde statik eşik kullanıldığı için tespit sonuçları diğer çalışmaların gerisinde kalmaktadır. Çalışma içerisinde kullanılan eşik değeri kullanılan veri tabanlarına göre güncellenmiştir. Bu şekilde sahte çerçevelerin çoğu bulunamadığı için DU oranı düşük çıkarken, orijinal çerçevelerin çoğunluğunun doğru bulunması KE ve DO değerlerinin yükselmesini sağlamaktadır.

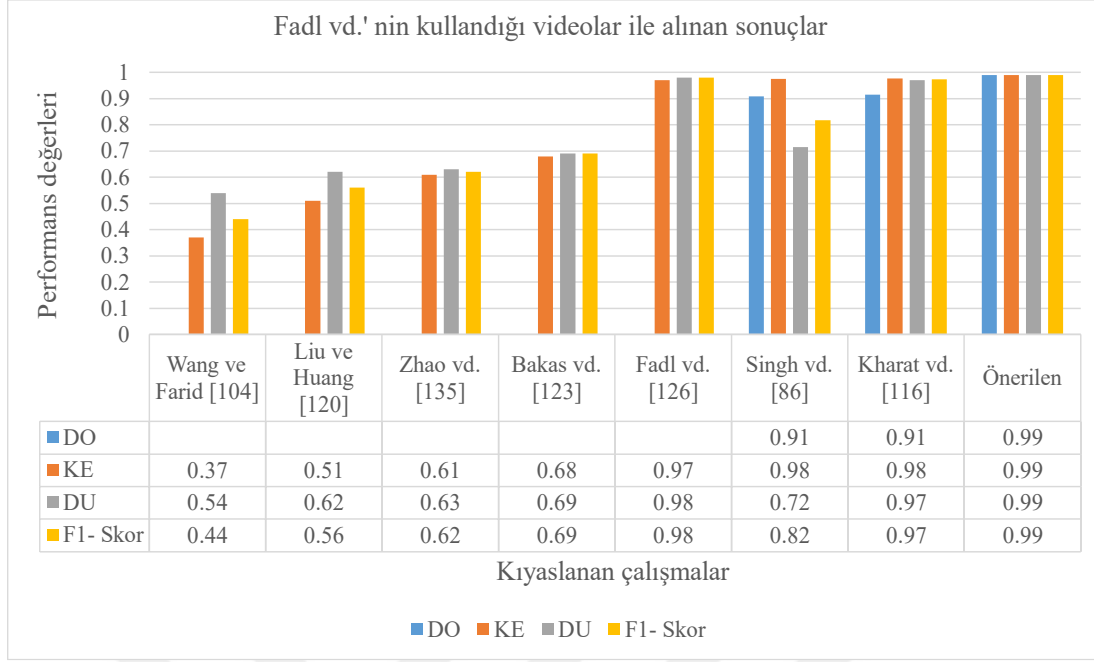
Bir sonraki kullanılan veri tabanı SULFA veri tabanından alınan videolar ile sahtecilik yapılarak oluşturulan Web-test/SULFA veri setidir. Elde edilen sonuçlar Şekil 3.30.' da gösterilmektedir.



Şekil 3. 30. Web-test’ teki SULFA veri tabanından alınan sonuçlar

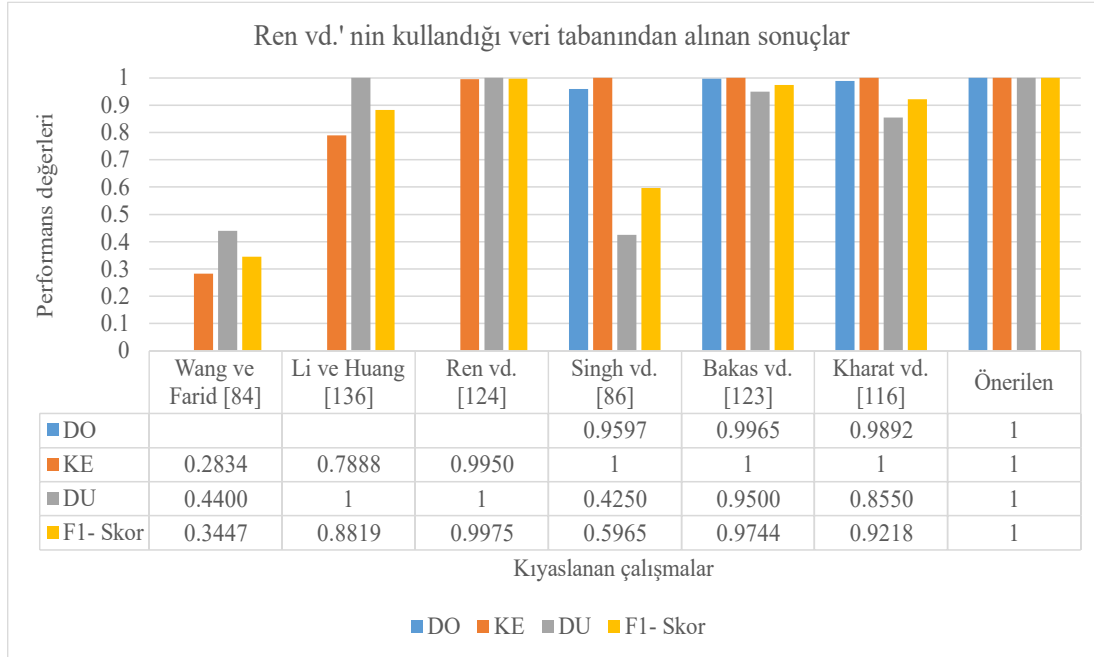
Şekil 3.30.’ da sonuçlar incelendiğinde önerilen çalışmanın tüm sahte ve orijinal videoları tam olarak bulduğu gözlemlenmektedir. Kharat vd.’ nin [116] çalışması düşük çözünürlüklü videolarda çalıştığı için kıyaslama yapılabilmiş ve Bakas’ ın çalışması ile birlikte yaklaşık %97 DO hesaplanmıştır. Bakas vd.’ in [123] kullandığı eşik değeri bu ve bundan sonraki kullanılan tüm çalışmalar için veri tabanına uygun olacak şekilde güncellenmektedir. Algoritmanın dayanıklılığını ölçmek için farklı veri tabanlarında da aynı çalışmalar kıyaslanmaktadır. Şekil 3.31., Şekil 3.32. ve Şekil 3.33.’ de bu sonuçlar gösterilmektedir.

Şekil 3.31.’ de Fadl vd.’ nin [126] önerdiği veri tabanında 10 tane tekrarlama sahteciliği videosu üzerinden testler yapılmıştır. Bu grafikte Singh vd. [86], Bakas vd. [123], Kharat vd.’ nin [116] algoritmaları koşulmuş, diğer çalışmalarında ortak veri tabanından alınan Fadl vd.’ nin [126] çalışmalarında sundukları sonuçlar alınmıştır. Bakas vd.’ nin algoritması [123], veri tabanına göre belirlenen eşik ile koşulduğunda DO %99, KE 1, DU %99 şeklindedir. Önerilen çalışma ise bu veri tabanında %100 başarı elde etmektedir.



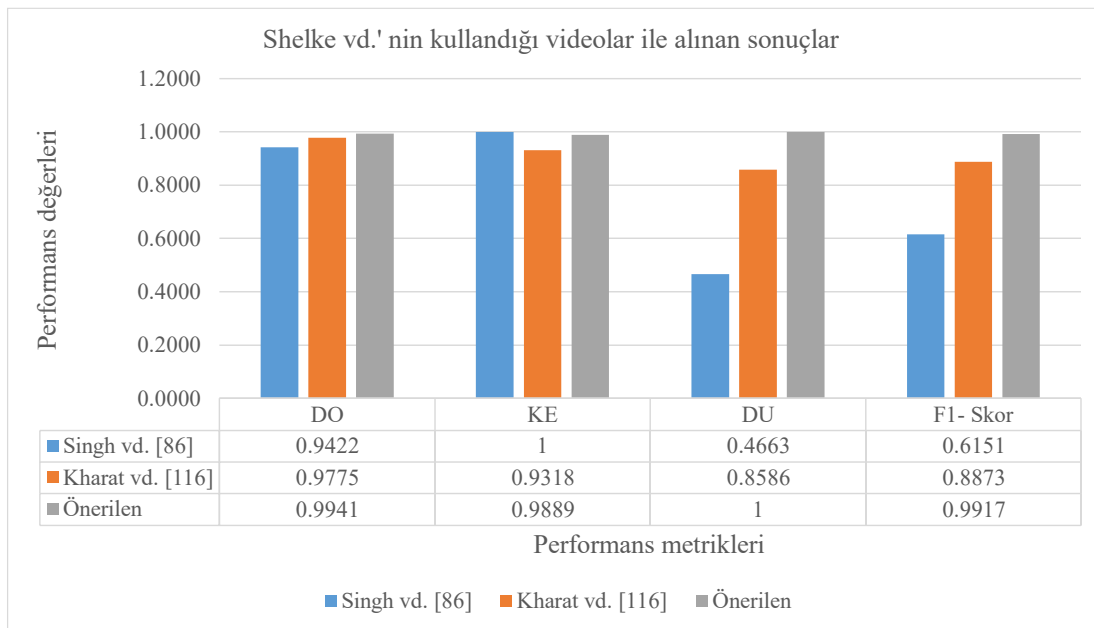
Şekil 3. 31. Fadl vd.' in [126] kullandığı veri tabanından alınan sonuçlar

Ren vd. [124] önerdiği veri tabanı aynı sayıda çerçevenin videonun en başından en sonuna yapıştırılmasıyla sahte videolar elde edilmektedir.



Şekil 3. 32. Ren vd.' nin [124] kullandığı veri tabanından alınan sonuçlar

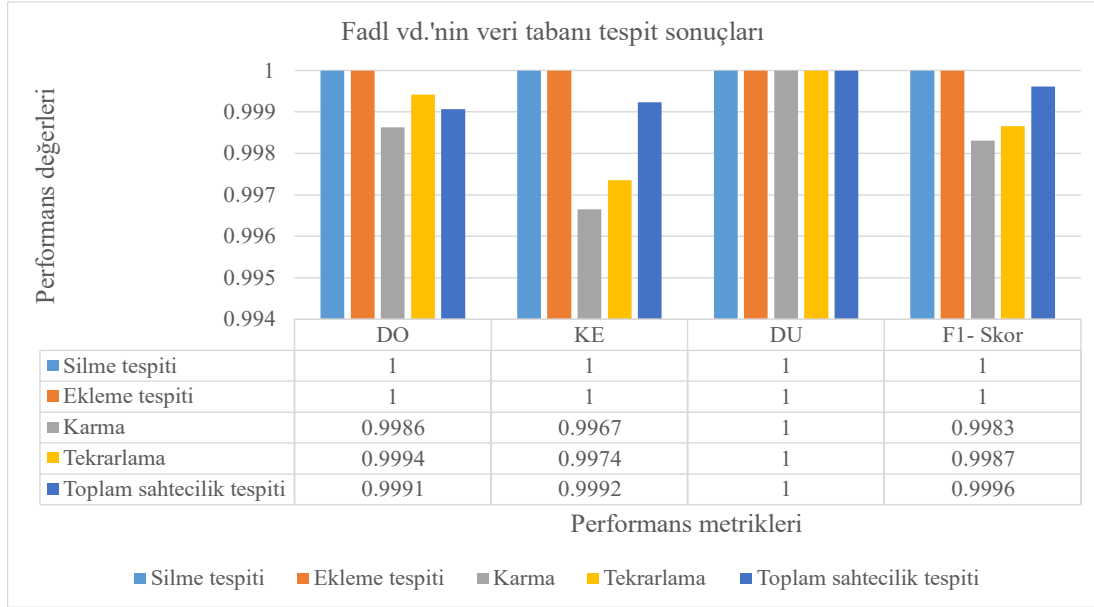
Algoritmanın farklı durumlar için dayanıklılığın test edilmesi açısından Ren vd.’nin [124] kullandıkları bu veri tabanında yapılan test sonuçları da önemlidir. Bu veri tabanından alınan sonuçlar Şekil 3.32.’de gösterilmektedir. Şekil 3.32.’de gösterilen çalışmalardan Wang ve Farid’ın [84] ile Li ve Huang’ın [136] çalışması Ren vd.’nin önermiş olduğu çalışmadan alınan sonuçları göstermektedir. Ancak kıyaslanan diğer çalışmalar, bu veri tabanında koşularak elde edilen sonuçlardır. Önerilen yöntem veri tabanında kullanılan 10 video için de %100 doğruluk vermektedir. Son olarak da Shelke vd. [154] veri tabanında yapılan kıyaslama Şekil 3.33.’de verilmektedir.



Şekil 3. 33. Shelke vd. kullandığı veri tabanından alınan sonuçlar

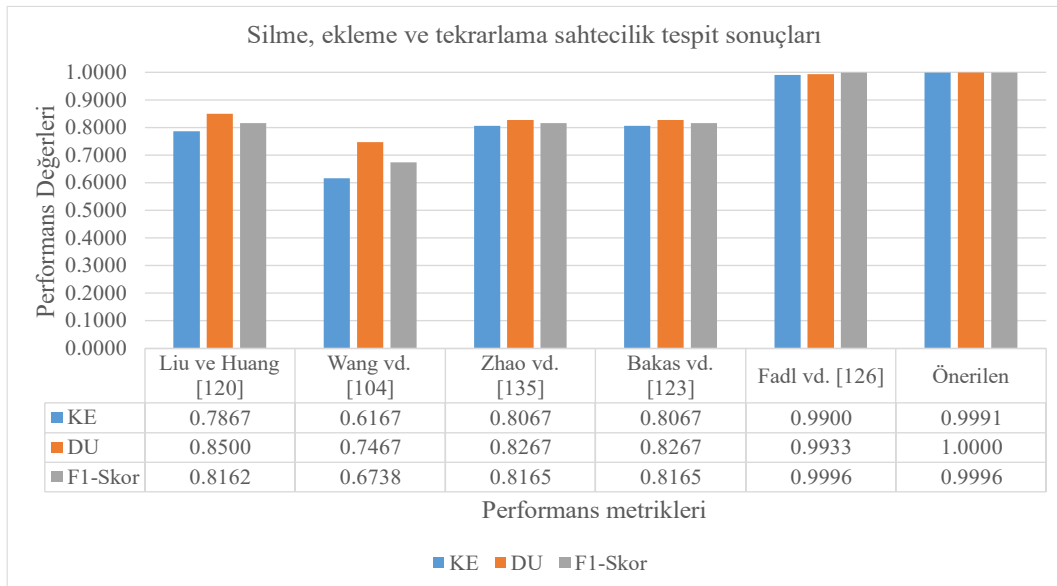
Shelke vd.’nin veri tabanında koşulan üç çalışmanın sonuçları incelendiğinde en yüksek doğruluk oranı ve F1-skorun önerilen yöntemde olduğu gözlemlenmektedir. Buraya kadar tekrarlama sahteciliği için elde edilen sonuçlar verilmektedir. Kullanılan kıyaslanan çalışmalar içerisinde açık veri tabanı olarak sunulan Fadl vd.’nin önerdiği veri tabanı üzerinden ekleme ve silme sahteciliklerinin tespiti için elde edilen sonuçlar Şekil 3.34.’de verilmektedir. Sonuçlar incelendiğinde silme, ekleme ve karma sahtecilikleri ilgili videolar üzerinden testler gerçekleştirilerek alınmıştır. Sadece tekrarlama sahteciliği tespiti sonuçları DO %99.72, KE %99.77, DU 1 ve F1skor %99.88 şeklinde hesaplanmıştır. Veri tabanında aynı video üzerinde karma ve tekrarlama sahteciliklerinin aynı anda yapıldığı videolar bulunmaktadır. Bu yüzden Şekil 3.34.’de verilen tekrarlama

tespiti sonuçları içerisinde bu videolar da bulunmaktadır. Yöntemin Fadl vd.' nin [126] önerdiği veri tabanı üzerinden elde edilen sonuçlarının tamamı %99' un üzerindedir.



Şekil 3. 34. Fadl vd.' nin önerdiği veri tabanından elde edilen sahtecilik tespit sonuçları

Fadl vd.' nin çalışması [126] ile kıyaslama sonuçları da Şekil 3.35.' de gösterilmektedir.



Şekil 3. 35. Fadl vd. çalışması ile üç tür sahteciliğin kıyaslama sonuçları

Kıyaslanan çalışmalarla da incelendiğinde üç tür sahteciliğin tespiti için algoritma başarılı olarak çalışmaktadır. Fadl ve önerilen çalışma dışındaki çalışmalar karma sahteciliğinin tespitini gerçekleştirmedikleri için Şekil 3.35.' de silme, ekleme ve tekrarlama sahtecilik tespit sonuçlarının ortalamaları gösterilmektedir.

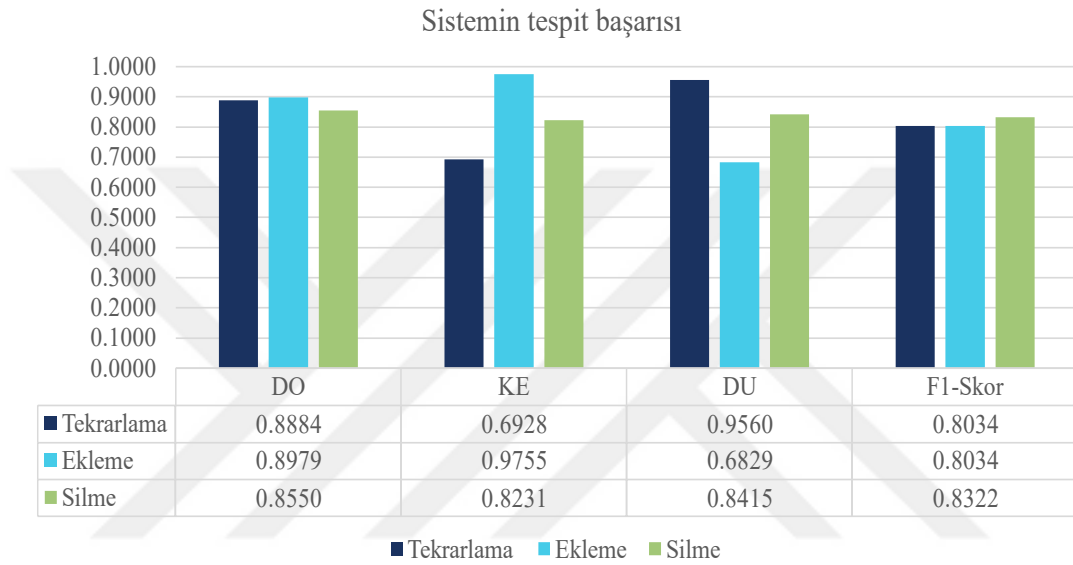
Fadl vd. çalışması ile önerilen çalışmanın karma sahteciliği tespiti yönünden kıyaslaması Tablo 3.7. ile gösterilmektedir. Tablodaki sonuçlar incelendiğinde tüm sahteciliklerin tespitinde önerilen yöntem kıyaslandığı çalışmalardan daha iyi performans sonuçları göstermiştir.

Tablo 3. 7. Önerilen çalışma ile Fadl vd. 'nin çalışmasının karma sahteciliği tespit sonuçları

	<i>KE</i>	<i>DU</i>	<i>F1-Skor</i>
<i>Fadl vd. [126]</i>	0.96	0.94	0.95
<i>Önerilen</i>	0.99	1	0.99

Buraya kadar incelenen sonuçların tamamı sıkıştırılmamış videolar üzerinden elde edilen sonuçları göstermekteydi. Ancak tez kapsamında önerilen hibrit yöntemin sıkıştırma ataklarına karşı güçlendirilmesi gerekmektedir. Bu yüzden öznitelik vektörü çıkarılmadan önce çerçevelere ADD algoritması uygulanarak sadece alçak frekans düzlemi üzerinden PYGH öznitelikleri çıkarılmaktadır. Bu sayede sıkıştırma işlemi ile kayba uğrayan yüksek frekans bileşenlerinden bağımsızlık sağlanarak yöntemin sıkıştırma ataklarına karşı dayanıklılığı artırılmıştır. Ancak sıkıştırma işlemine karşı dayanıklılık sağlanan videolarda tekrarlanan çerçeveler birbirinin aynısı olmayacağı için videolara göre dinamik bir eşik kullanılarak benzerlik ilişkisi, eşiğe göre belirlenmektedir. Bu durumda ilk olarak sıkıştırılmış videolar üzerinden deneysel olarak belirlenen eşiğe göre video içerisinde eşleşen çiftlerin varlığı aranmıştır. Eşleşen çiftlerin varlığı videolarda tekrarlama sahteciliğinin yapıldığını göstermektedir. Eğer eşleşen çift bulunamadıysa bu durumda ekleme ve silme sahteciliklerinin tespiti gerçekleştirilmektedir. Bu çalışma ile literatürde daha önce başarısı test edilmeyen yeni bir test yaklaşımı önerilmiştir. Bu yaklaşım ile video bazında test edilen videolarda hangi sahteciliğin yapıldığının başarısı ölçülmüştür. Bu başarıya ait sonuçlar Şekil 3.36.' da gösterildiği gibidir. Elde edilen sonuçlar toplam 1050 video üzerinden test edilmiştir. Bölüm 3.2.' de kullanılan değerlendirme

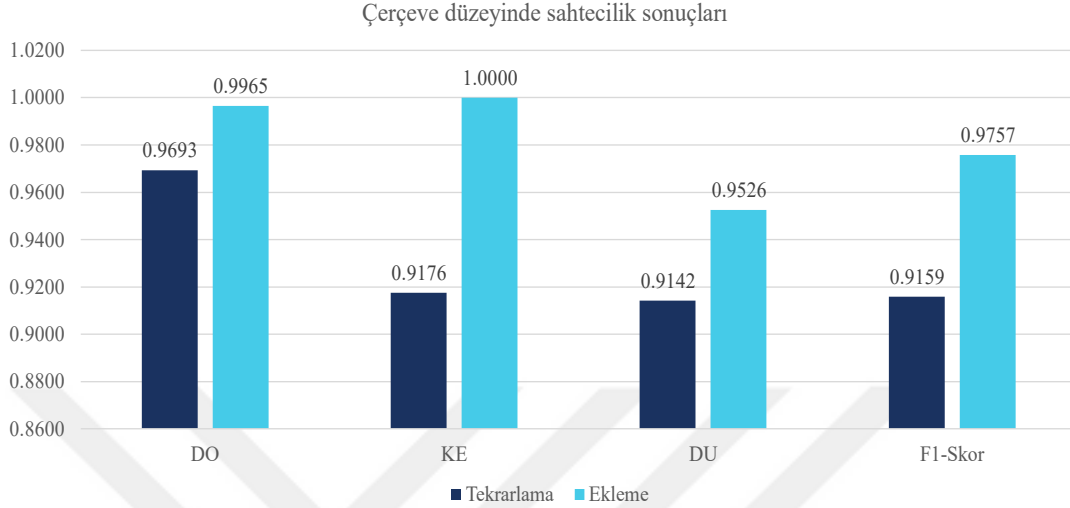
ölçütlerinden bahsedilmiştir. Burada DN değerleri belirlenirken tekrarlama sahteciliği üzerinden örnek verilecek olunursa; tekrarlama olmayan ve algoritmanın da tekrarlama demediği yani içerisinde hem ekleme hem de silme videolarının bulunduğu değerler baz alınmıştır. Sistem yaklaşık olarak tekrarlama sahteciliği olan videoları %89, ekleme sahteciliği olan videoları %90, silme sahteciliği yapılan videoları ise %86 doğruluk oranı ile tespit edebilmektedir.



Şekil 3. 36. Sahtecilik türlerinin tespit başarısı

İkinci olarak da sıkıştırılmış videolarda sahte çerçevelerin bulunduğu, ekleme ve tekrarlama sahteciliklerinin çerçeve düzeyinde elde edilen başarıları Şekil 3.37.' de gösterilmiştir. Sıkıştırılmış videolar üzerinden elde edilen sonuçlar incelendiğinde sıkıştırma işlemi ile kayba uğrayan istatistiksel öznitelikler neticesinde sahtecilik tespit tanılama oranları düşmektedir. Çerçeve düzeyinde ekleme sahteciliğinin tespit başarısının, tekrarlama sahteciliğinin tespit başarısından yüksek olduğu gözlenmektedir. Bu eşleşen çerçeve sayısının tamamının bulunamamasından kaynaklanmaktadır. Dolayısıyla eksik bulunan sahte çerçeveler duyarlılık değerini düşürmektedir. Ekleme sahteciliğinde kullanılan videolar farklı iki videonun birleştirilmesi ile oluşturulduğundan anomali noktaları daha belirgin olmaktadır. Sıkıştırmadan dolayı tekrarlama sahteciliğinde elde edilen anomali noktalarına göre daha az etkilenmektedir. Genel olarak baktığımızda sıkıştırılmış videolar üzerinden yaklaşık olarak %97 DO ile tekrarlama sahteciliği, %99

DO ile ekleme sahteciliği tespiti gerçekleştirilmektedir. Sıkıştırma işlemleri için H-264 formatında, CRF-6, CRF-12, CRF-18, CRF-24, CRF-30 kalite oranları kullanılmıştır.



Şekil 3. 37. Çerçeve düzeyinde elde edilen tekrarlama ve ekleme sonuçları

Ekleme sahteciliği için videoların başına ve videoların arasına olacak şekilde ekleme işlemi gerçekleştirilmiştir. Tekrarlama sahteciliği yapılan 50 video farklı sıkıştırma oranlarında toplam 250 video, ekleme sahteciliği yapılan 70 video farklı sıkıştırma kalitelerinde toplam 350 video, silme sahteciliği yapılan 90 video 5 farklı sıkıştırma kalitesi kullanılarak sıkıştırılmış toplam 450 video ile testler gerçekleştirilmiştir.

3.4. Tez Kapsamında Önerilen Yöntemlerin Karşılaştırılması

Tez kapsamında önerilen çalışmaların kıyaslaması Tablo 3.11.' de gösterilmektedir. Burada “+” ile gösterilen hücreler o özelliğin varlığını, “-” olan yerler ise üst kısımdaki özniteliklerin olmadığını ifade etmektedir. Tez boyunca ilk olarak tekrarlama sahteciliklerinin tespitine yönelik çalışmalar gerçekleştirilmiştir. İlk çalışmada sabit arka planlı videolarda, durağan sahnelerin birbirine çok benzemesi ve bunların doku tabanlı öznitelik çıkarım tekniği ile yeterince ayırt edilememesinden dolayı, çerçeveler arası benzerlik yüksek olmakta ve tespit doğruluğu düşmektedir. Dolayısıyla bu sorunun üstesinden gelmek için ikinci çalışmada kenar tabanlı yöntemler kullanılarak hem ayırt ediciliğin artırılması hem de çerçeveler arası gruplama yaparak ardışık olup durağan

sahnelerin sahte çerçevelerden ayrılması sağlanmıştır. Üçüncü çalışma ile ilk iki çalışmada olmayan ve sahtecilik işlemi yapıldıktan sonra sahteciliğin anlaşılmasını zorlaştıran bulanıklaştırma ve sıkıştırma gibi ataklara karşı dayanıklılığın artırılması amacıyla frekans tabanlı yaklaşım önerilmiştir.

Tablo 3. 8.Tez kapsamında yapılan çalışmaların kıyaslaması

	Tekrarlama sahteciliği tespiti	Karma sahteciliği tespiti	Ekleme sahteciliği tespiti	Silme sahteciliği tespiti	Sabit arka planlı videolarda tespit	Hareketli arka planlı videolarda tespit	Sıkıştırma dayanıklılığı	Bulanıklaştırma ataklarına dayanıklılık	Kaynak çerçeve tespiti
1. Doku tabanlı yaklaşım	+	-	-	-	-	+	-	-	-
2. Kenar tabanlı yaklaşım	+	-	-	-	+	+	-	-	-
3. Frekans tabanlı yaklaşım	+	-	-	-	+	+	+	+	+
4. İstatistiksel tabanlı yaklaşım	-	-	-	+	+	+	+	-	-
5. Doku ve Frekans tabanlı yaklaşım	+	+	+	+	+	+	+	-	-

Tezin bu aşamasına kadar tekrarlama sahteciliğine popüler veri tabanları kullanılarak başarılı bir çözüm sunulmuş bu aşamadan sonra çerçeveler arası diğer sahteciliklerin tespiti araştırılmıştır. İlk olarak silme sahteciliğinin çözümüne yönelik istatistiksel bir yaklaşım sunulmaktadır. Sonrasında tüm sahteciliklere çözüm sunabilecek hibrit bir algoritma geliştirilmiştir. Bu algoritma ile hem çerçeveler arası tekrarlama, karma, ekleme ve silme sahteciliklerine çözüm sunulmuş hem de ataklara karşı dayanıklılık test edilmiştir. Tez kapsamında yapılan çalışmalardan kullanılan veri tabanlarına ve kıyaslanan çalışmalara göre tanılama doğruluğu yüksek çalışmalar oluşturulmuştur.

4. TARTIŞMA VE SONUÇLAR

Veri doğrulanması gelişen teknolojik çalışmalar doğrultusunda günümüzün en önemli güvenlik problemlerinden biridir. Veriler üzerinde yapılan oynamalar iyi amaçlar için kullanılabileceği gibi kötü niyetli kişiler tarafından da kolaylıkla uygulanabilir. Açık kaynak kodlu yazılımlar ile içeriği değiştirilerek günlük hayatımız vazgeçilmez iletişim kaynaklarından biri olan sosyal medya uygulamalarıyla topluma mal edilen video gibi canlı kanıt niteliği taşıyan verilerin doğrulanması önemli bir problem olarak literatürde yer almakta ve gelişmekte olan bir konu olarak popülerliğini sürdürmektedir.

Video verilerinin doğrulanması için kullanılan pasif sahtecilik teknikleri derin sahte videoların tespit edilmesi, konumsal sahtecilik tespit teknikleri ve zamansal sahtecilik tespit teknikleri olarak sınıflandırılabilir. Son yıllarda derin sahte videoların üretimine olan ilginin artması, yapılan videoların tespitinin de gerekliliğini ortaya çıkarmış ve yeni bir alan olarak literatüre girmesini sağlamıştır. Konumsal sahtecilikler tespit teknikleri literatürde genellikle zamansal sahteciliklerle birlikte kullanılan sahtecilik tespit teknikleridir. Çünkü sahte videonun oluşturulması için, kurcalama gerçekleştiren kişinin daha uzman olmasını gerektirir. Videolar çok sayıda görüntüden oluşmaktadır ve yapılan kurcalamanın mevcut sahnedeki tüm çerçevelere uyumlu olmasını gerektirir. Aksi halde yapılan sahtecilik gözle dahi fark edilebilir bu da delil olarak kullanılmasını engeller. Ancak zamansal sahtecilik tespit teknikleri üzerine literatürde çok sayıda çalışma önerilmiştir. Çünkü çerçeveler üzerinde oynamak sahtekârlar tarafından zaman almadan kolaylıkla yapılabilmektedir. Zamansal sahtecilik tespit teknikleri önerilen yöntemlerin uygulama şekillerine göre; öznitelik çıkarımına dayalı öğrenmeye dayalı ve ikisinin bir arada kullanıldığı hibrit yöntemler olarak sınıflandırılabilir. Öznitelik çıkarımına dayalı teknikler ise sıkıştırma kalıntılarına dayalı, gürültü kalıntılarına dayalı, hareket özniteliklerine dayalı ve istatistiksel özniteliklere dayalı olarak sınıflandırılabilir. Sıkıştırma kalıntılarına dayalı tespit tekniklerinin dezavantajı RGY sayısının katları şeklinde sahtecilik yapılması durumunda yetersiz kalması, gürültü kalıntılarına dayalı sahtecilik tespit tekniklerinin dezavantajı değişen kamera lensleri ve cihazlara uyumlu olacak şekilde yeni çalışmalarla sürekli desteklenmesi gerekliliğidir. Hareket özniteliklerine dayalı tespit tekniklerinin problemi ise videoların saniyede görüntülen

çerçeve sayısına veya içindeki nesne hareket hızlarına bağlı olarak performanslarının değişmesidir. İstatistiksel özniteliklere dayalı tespit teknikleri sadece önerilen algoritmanın efektifliğine bağlı olarak koşma zamanı bakımından dezavantaj gösterebilir. Bu anlamda tez kapsamında en avantajlı tespit tekniklerinden olan istatistiksel özniteliklere dayalı tespit teknikleri kullanılarak efektif çalışabilen beş farklı çalışma önerilmiştir. Bu çalışmalardan ilk ikisi tekrarlama sahteciliğinin tespitini sıkıştırılmamış videolar üzerinden gerçekleştirmektedir. Sonraki çalışma ise tekrarlama sahteciliğinin tespitini sıkıştırılmış videolar üzerinden de gerçekleştirebilmektedir. Tez çalışmasında tekrarlama sahteciliğine efektif çözümler bulunduktan sonra diğer bir problem olan silme sahteciliğine benzerlik tabanlı bir yaklaşım ile çözüm sunulmuştur. Son olarak da çerçeveler arası sahteciliklere hem sıkıştırılmış hem de sıkıştırılmamış videolar üzerinden çözüm sunabilen hibrit çalışma gerçekleştirilmiştir. İlk olarak tekrarlama sahteciliğinin çözümü için doku tabanlı ve kenar algılamaya dayalı iki farklı yaklaşım önerilmiştir. Bu çalışmalar sıkıştırılmamış videolarda efektif çalışmaktadır. Bir sonraki çalışmada tekrarlama sahteciliğinin tespit edildiği sıkıştırma ataklarına dayanıklı AKD özelliği kullanılarak yüksek doğruluk alınan yeni bir çalışma önerilmiştir. Çalışma da farklılık olarak çıkarılan özniteliklerin ikili görüntüleri oluşturularak bu görüntüler üzerinde sahtecilik taraması yapılmıştır. Ayrıca yöntem bulanıklaştırma ve sıkıştırma ataklarına karşı test edilmiştir. Literatürdeki popüler sekiz çalışma ile kıyaslamaları yapılmış onlardan daha yüksek başarı oranları ve farklı kıyaslama sonuçları elde edilmiştir. Çerçeveler arası tekrarlama sahteciliğine efektif çözüm sunulduktan sonra, bir sonraki çalışmada TSGO' larına dayalı silme sahteciliği tespiti gerçekleştirilmiştir. Beşinci çalışma zamansal boyutta yapılan literatürde adı geçen tüm sahteciliklere çözüm sunabilen bir çalışma olup kıyaslaması yapılan çalışmalardan sıkıştırılmamış videolarda daha yüksek başarı oranları sağlamaktadır. Yöntem farklı veri tabanlarında test edilen sıkıştırma atağına dayanıklı başarılı bir çalışma olmuştur. Çalışmada özellik çıkarım tekniği olarak ilk olarak sadece PYGH ile öznitelik çıkarılarak sıkıştırılmamış videolar üzerinden elde edilen sonuçlar verilmektedir. Sonrasında ise sıkıştırmaya dayanıklılık sağlamak için PYGH ile ADD' si alınan çerçevelerin alçak frekans bileşenleri üzerinden öznitelik çıkarımı yapılmıştır. Literatürde birden fazla sahteciliğe çözüm sunan çalışmaların sıkıştırma ataklarına karşı dayanıklılık testi gerçekleştirilmemiştir. Bu anlamda literatüre katkı sağlayan ilk çalışma niteliğini sağlamaktadır.

5. ÖNERİLER

Çoklu ortam verilerinin doğrulanması için kullanılan sahtecilik tespit teknikleri verilerin istatistiksel olarak tutarlılığının sağlanmasını teyit etmekte olup bu sayede bu verilerin birer delil olarak kullanılabilmesine olanak tanır. Günümüzde en çok kullanılan iletişim araçlarının başında gelen internet, televizyon ve sosyal medya araçlarının kullanmış olduğu videolar olayların aktarılmasını sağlayabilecek en gerçekçi kanıtlardır.

Literatürde video sahteciliklerinin tespiti alanında yapılan çalışmaların sayısı video kullanım araçlarının artmasına paralel olarak ilerleyememekte olup, gelişim aşamasındadır. Örneğin henüz video içerisinde nesne birleştirme sahteciliklerinin tespiti, derin öğrenme teknikleri ile gerçekleştirilen sahteciliklerin tespiti gibi alanlarda sayılı çalışma bulunmaktadır. Video sahteciliklerinin tespitini zorlaştıracak çeşitli ataklara karşı sayılı sayıda test edilmiş çalışma vardır. Video sahtecilik tespiti alanında yapılan çalışmalar konusunda ölçüt olabilecek geniş bir ortak veri tabanlarına ihtiyaç bulunmaktadır. Mevcut veri tabanları genellikle orijinal videoları içerecek şekilde araştırmacılara hizmet etmektedir. Çalışmalarını yapan araştırmacılar bu videolar üzerinde çeşitli atakları geliştirerek mevcut çalışmalarla ya da sahte videoların verildiği kısıtlı veri tabanlarını içeren çalışmalar ile kıyaslama yapmaktadır. Yapılan çalışmaların kullanılan veri tabanları ile tanılama ve tespit başarıları yüksek çıkmaktadır. Dolayısıyla literatüre kazandırılacak; dönme, ölçekleme, bulanıklaştırma veya gürültü ekleme gibi çeşitli atakları içeren bir veri tabanı oluşturulabilir. Yapılan çalışmalar yeni veri tabanları üzerinden test edilebilir.

Diğer yandan video çerçevelerinde çerçeveler arasında sadece belirli bölümler kopyalanabilir ya da silinebilir. Bu tür sahteciliklerin yapılması zor olduğu için nispeten daha az tercih edilmektedir. Ancak gelecek çalışmalarda bu tür sahteciliklerin de araştırılması önemli olacaktır. Zamanla görüntü seviyesinde uygulanan kopyala yapıştır, görüntü birleştirme ve iç boyama teknikleri ile de video oluşturmak kolay hale geleceği için yeni veri tabanlarında bu tarz videoların bulunması da geliştirilen yöntemlerin gelişimine katkı sağlayacaktır.

Pasif tespit teknikleri gibi aktif tespit teknikleri de videoların bütünlüklerinin tespitinde kullanılan farklı bir araştırma alanıdır. Bu alanda yapılan çalışmalar videoların orijinal

hallerinin olmasını gerektirir. Aynı zamanda ek bir yazılım veya donanım kullanılarak videoların güvenilirliğinin test edilmesini sağlamaktadırlar.



6. KAYNAKLAR

1. Bozkurt, F., Covid-19 Pandemi Sürecindeki Sahte ve Yalan Haberlerin Bir Getirisi: İnfodeminin Türkiye Bağlamında İncelenmesi, *Uluslararası Halkbilimi Araştırmaları Dergisi*, 4,7, (2021) 135-151.
2. Başlar, Y., Elektronik Delilin Toplanması ve Muhafazası, *Hacettepe Hukuk Fakültesi Dergisi*, 10, 1, (2020) 77-107.
3. Özen, M. ve Özocak, G., Adli Bilişim Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), *Ankara Barosu Dergisi*, 0,1, (2015) 41-77.
4. [https://www.bakiokan.av.tr/#!post-106-CEZA%20YARGILAMASI%20A%C3%87ISINDAN%20ELEKTRON%C4%B0K%20\(D%C4%B0J%C4%B0TAL\)%20KANIT](https://www.bakiokan.av.tr/#!post-106-CEZA%20YARGILAMASI%20A%C3%87ISINDAN%20ELEKTRON%C4%B0K%20(D%C4%B0J%C4%B0TAL)%20KANIT) Okan, B., Okan ve Okan Hukuk Bürosu. 21 Haziran 2023.
5. Başlar, Y., Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri, *TBB Dergisi*, 148, (2020) 47-76.
6. Akhtar, N., Saddique, M., Asghar, K., Bajwa, U. I., Hussain, M. ve Habib, Z., Digital Video Tampering Detection and Localization: Review, Representations, Challenges and Algorithm, *Mathematics*, 10, 2, (2022) 168.
7. Yu, J. Y., Kim, Y. ve Kim, Y. G., Intelligent video data security: a survey and open challenges, *IEEE Access*, 9, (2021) 26948-26967.
8. <https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=video+forgery+detection&sid=a7eb1d6cb6cbdf5bba7117ee274597a8&sot=b&sdt=b&sl=38&s=TITLE-ABS-KEY%28video+forgery+detection%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present> 21 Ocak 2023.
9. Al-Sanjary, O. I., Ahmed, A. A. ve Sulong, G., Development of a video tampering dataset for forensic investigation, *Forensic science international*, 266, (2016) 565-572.
10. Kaur, H. ve Jindal, N., Image and video forensics: A critical survey, *Wireless Personal Communications*, 112, 2, (2020) 1281-1302.
11. http://www.100fps.com/how_many_frames_can_humans_see.htm 100fps.com. 21 Ocak 2023.
12. Zhuo, R., Lin, P., Wu, Y., Wu, Z., Ye, D., ve Huangfu, J., Sensorless LED display screen interaction and object recognition. *Journal of the Society for Information Display*, 30,2, (2022) 141-158.

13. Kumar, V., Singh, A., Kansal, V. ve Gaur, M., A comprehensive survey on passive video forgery detection techniques, Recent Studies on Computational Intelligence, Khanna, A., Singh, A.K., Swaroop, A., 921, 39-57, Springer, Singapur, 2021.
14. <https://www.youtube.com/watch?v=DQ1R2YJMPiU&list=RDCMUcRt021aa4HQ1dHROMc6u2-Q&index=3> Örnek video. 21 Ocak 2023.
15. <https://en.teyit.org/does-the-video-show-people-with-the-coronavirus> Ulusal İnfodemi Haberleri. 21 Ocak 2023.
16. <https://www.indiatoday.in/fact-check/story/viral-video-does-not-show-forced-mass-testing-covid-china-1983293-2022-08-03> Uluslararası İnfodemi Haberleri. 21 Ocak 2023.
17. DEMİRCAN, B., Gördüğün Her Şeye İnanma: Derin Sahte Çalışmaları Üzerine Bir Doküman Analizi, TRT Akademi, 613, (2021) 728-747.
18. Ünal, R. ve ÇİÇEKLİOĞLU, A. Ş., Fake News Pandemic: Fake News And False Information About Covid-19 and An Analysis on Fact Checking from Turkey in Sample Teyit. org. Erciyes İletişim Dergisi, 9, 1, (2022) 117-143.
19. Wang, Y., Peng, C., Liu, D., Wang, N. ve Gao, X., ForgeryNIR: Deep Face Forgery and Detection in Near-Infrared Scenario. IEEE Transactions on Information Forensics and Security, 17, (2022) 500-515.
20. ISO, “Information technology- coding of audio-visual objects- part 2: Visual,” ISO/IEC IS 14496-2, Üçüncü Baskı, International Organization for Standardization, Cenevre, İsviçre, 2009.
21. ISO, “Information technology- coding of audio-visual objects- part 10: Advanced video coding (avc),” ISO/IEC IS 14496- 10, International Organization for Standardization, Cenevre, İsviçre, 2010.
22. Singla, N., Nagpal, S. ve Singh, J., A Review on HEVC Video Forensic Investigation under Compressed Domain, International Journal of Image, Graphics and Signal Processing 12, 5, (2022) 44.
23. Wang, W. ve Farid, H., Exposing digital forgeries in video by detecting double MPEG compression, In Proceedings of the 8th workshop on Multimedia and security, 26 Eylül 2006, Cenevre, İsviçre, Bildiriler Kitabı, 37-47.
24. Su, Y., Nie, W. ve Zhang, C., A frame tampering detection algorithm for MPEG videos, In 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Ağustos 2011, Çongçing, Çin, Bildiriler Kitabı, 461-464.
25. Yao, H., Ni, R. ve Zhao, Y., An approach to detect video frame deletion under anti-forensics, Journal of Real-Time Image Processing, 16, 3, (2019) 751-764.
26. Hasanabadi, S. S., Lashkari, A. H. ve Ghorbani, A. A., A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of

- forensic agents behaviour, Forensic Science International: Digital Investigation, 35 (2020) 301024.
27. Sitara, K. ve Mehtre, B. M. Differentiating synthetic and optical zooming for passive video forgery detection: An anti-forensic perspective, Digital Investigation, 30 (2019) 1-11.
 28. Fadl, S., Han, Q. ve Li, Q., CNN spatiotemporal features and fusion for surveillance video forgery detection, Signal Processing: Image Communication, 90 (2021) 116066.
 29. Kingra, S., Aggarwal, N. ve Kaur, N., Emergence of deepfakes and video tampering detection approaches: A survey, Multimedia Tools and Applications, (2022) 1-45.
 30. Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T. T., Pham, Q. ve Nguyen, C. M., Deep learning for deepfakes creation and detection: A survey, Computer Vision and Image Understanding, 223, (2022), 103525.
 31. Verdoliva, L., Media forensics and deepfakes: an overview, IEEE Journal of Selected Topics in Signal Processing, 14, 5, (2020) 910-932.
 32. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. ve Bengio, Y., Generative adversarial networks, Communications of the ACM, 63, 11, (2020) 139-144.
 33. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K. ve Li, H., Protecting World Leaders Against Deep Fakes, In CVPR workshops, Haziran 2019, Long Beach Kaliforniya, Bildiriler Kitabı, 1:38.
 34. Tayseer, M., Mohammad, J., Ababneh, M., Al-Zoube, A. ve Elhassan, A. Digital Forensics and Analysis of Deepfake Videos, In 11th International Conference on Information and Communication Systems (ICICS), Nisan 2020, Ürdün, Bildiriler Kitabı, 053- 058.
 35. Aggarwal, A., Mittal, M. ve Battineni, G., Generative adversarial network: An overview of theory and applications, International Journal of Information Management Data Insights, 1, 1, (2021) 100004.
 36. Mitra, A., Mohanty, S. P., Corcoran, P. ve Kougianos, E., A machine learning based approach for deepfake detection in social media through key video frame extraction, SN Computer Science, 2, 2, (2021) 1-18.
 37. Perov, I., Gao, D., Chervoniy, N., Liu, K., Marangonda, S., Umé, C., Dpfks, M., Facenheim, C. S., RP, L., Jiang, J., Zhang, S., Wu, P., Zhou, B. ve Zhang, W., DeepFaceLab: A simple, flexible and extensible face swapping framework, arXiv:2005.05535, (2020).
 38. Shahzad, H. F., Rustam, F., Flores, E. S., Luís Vidal Mazón, J., de la Torre Diez, I. ve Ashraf, I., A Review of Image Processing Techniques for Deepfakes, Sensors, 22, 12, (2022) 4556.

39. Shelke, N. A. ve Kasana, S. S., A comprehensive survey on passive techniques for digital video forgery detection. Multimedia Tools and Applications, 80, 4, (2021) 6247-6310.
40. Singh, R. D. ve Aggarwal, N., Detection of upscale-crop and splicing for digital video authentication, Digital Investigation, 21, (2017) 31-52.
41. Zhong, J. L., Gan, Y. F., Vong, C. M., Yang, J. X., Zhao, J. H. ve Luo, J. H., Effective and efficient pixel-level detection for diverse video copy-move forgery types. Pattern Recognition, 122, (2022) 108286.
42. Nabi, S. T., Kumar, M., Singh, P., Aggarwal, N. ve Kumar, K., A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. Multimedia Systems, 28, (2022) 1-54.
43. Bagiwa, M. A., Wahab, A. W. A., Idris, M. Y. I., Khan, S. ve Choo, K. K. R., Chroma key background detection for digital video using statistical correlation of blurring artifact. Digital Investigation, 19, (2016) 29-43.
44. Liu, Y., Huang, T. ve Liu, Y., A novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking. Multimedia Tools and Applications, 77, 6, (2018) 7405-7427.
45. Shafii, K., Mohammed, A. U., Bagiwa, M. A. ve Sulaiman, N., Challenges to Blue Screen Composition Detection in Digital Videos, Proceedings of 2nd International Conference of the IEEE, Ekim 2019, Nijerya, Bildiriler Kitabı, 339.
46. Shafii, K., Bagiwa, M. A., Obiniyi, A. A., Sulaiman, N., Usman, A. M., Fatima, C. M. ve Fatima, S., Blue Screen Video Forgery Detection And Localization Using An Enhanced 3-Stage Foreground Algorithm, Fudma Journal Of Sciences, 5, 2, (2021) 133-144.
47. Singh, G. ve Singh, K., Chroma key foreground forgery detection under various attacks in digital video based on frame edge identification, Multimedia Tools and Applications, 81, 1, (2022) 1419-1446.
48. Sharma, H. ve Kanwal, N., Video interframe forgery detection: Classification, technique and new dataset. Journal of Computer Security, 29,5, (2021) 1-20.
49. Singh, R. D. ve Aggarwal, N., Video content authentication techniques: a comprehensive survey, Multimedia Systems, 24, 2, (2018) 211-240.
50. Kumar, V., Singh, A. ve Gaur, M., A Comprehensive Analysis on Video Forgery Detection Techniques. Proceedings of the International Conference on Innovative Computing & Communications (ICICC), Mart 2020, Hindistan Bildiriler Kitabı, 1-5.
51. Sowmya, K. ve Chennamma, H., A survey on video forgery detection, International Journal of Computer Engineering and Applications, 9, 2, (2015) 17-27.
52. Tyagi, S. ve Yadav, D., A detailed analysis of image and video forgery detection techniques, The Visual Computer, 39, 3, (2023) 813-833.

53. Rivest, R. L., Shamir, A. ve Adleman, L. M., A method for obtaining digital signatures and public key cryptosystems. Secure communications and asymmetric cryptosystems, 69, (2019) 217-239.
54. Kaur, R. ve Kaur, A., Digital signature, 2012 International Conference on Computing Sciences, Eylül 2012, Hindistan, Bildiriler Kitabı, 295-301.
55. Khan, S. CLIFD: A novel image forgery detection technique using digital signatures. Journal of Engineering Research, 9, 1, (2021) 168-175.
56. Ramaswamy, N. ve Rao, K. R., Video authentication for H. 264/AVC using digital signature standard and secure hash algorithm, Proceedings of the 2006 international workshop on Network and operating systems support for digital audio and video, Mayıs 2006, New York, Bildiriler Kitabı, 1-6.
57. Langelaar, G. C., Setyawan, I. ve Lagendijk, R. L., Watermarking digital image and video data, A state-of-the-art overview, IEEE Signal processing magazine, 17, 5, (2000) 20-46.
58. Asikuzzaman, M. ve Pickering, M. R., An overview of digital video watermarking, IEEE Transactions on Circuits and Systems for Video Technology, 28, 9, (2017) 2131-2153.
59. Altay, Ş. Y. ve Ulutaş, G., Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain, Multimedia Tools and Applications, 80, 15, (2021) 23457-23484.
60. Altay, Ş. Y. ve Ulutaş, G., DWT-QR based blind image watermarking method using firefly algorithm, 28th Signal Processing and Communications Applications Conference (SIU), Ekim 2020, Gaziantep, Bildiriler Kitabı, 1-4.
61. Javed, A. R., Jalil, Z., Zehra, W., Gadekallu, T. R., Suh, D. Y. ve Piran, M. J., A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions, Engineering Applications of Artificial Intelligence, 106, (2021) 104456.
62. Guefrechi, S., Jabra, M. B. ve Hamam, H., Deepfake video detection using InceptionResnetV2, 6th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Mayıs 2022, Tunus, Bildiriler Kitabı, 1-6.
63. Pan, G., Sun, L., Wu, Z. ve Lao, S. Eyeblink-based anti-spoofing in face recognition from a generic web camera, IEEE 11th international conference on computer vision, Ekim 2007, Brezilya, Bildiriler Kitabı, 1-8.
64. Sun, L., Pan, G., Wu, Z. ve Lao, S. Blinking-based live face detection using conditional random fields, International Conference on Biometrics, Ağustos 2007, Berlin, Bildiriler Kitabı, 252-260.
65. Li, Y., Chang, M. C. ve Lyu, S., In ictu oculi: Exposing ai created fake videos by detecting eye blinking, IEEE International workshop on information forensics and security (WIFS), Aralık 2018, Hong Kong, Bildiriler Kitabı, 1-7.

66. Kollreider, K., Fronthaler, H., Faraj, M. I. ve Bigun, J., Real-time face detection and motion analysis with application in “liveness” assessment, IEEE Transactions on Information Forensics and Security, 2, 3, (2007) 548-558.
67. Atoum, Y., Liu, Y., Jourabloo, A. ve Liu, X., Face anti-spoofing using patch and depth-based CNNs, IEEE International Joint Conference on Biometrics (IJCB), Ekim 2017, Colorado, Bildiriler Kitabı, 319-328.
68. Koopman, M., Rodriguez, A. M. ve Geradts, Z., Detection of deepfake video manipulation, The 20th Irish machine vision and image processing conference (IMVIP), Ağustos 2018, İrlanda, Bildiriler Kitabı, 133-136.
69. Afchar, D., Nozick, V., Yamagishi, J. ve Echizen, I., Mesonet: a compact facial video forgery detection network, IEEE international workshop on information forensics and security (WIFS), Aralık 2018, Hong Kong, Bildiriler Kitabı, 1-7.
70. Suratkar, S. ve Kazi, F., Deep Fake Video Detection Using Transfer Learning Approach, Arabian Journal for Science and Engineering, (2022) 1-11.
71. Güera, D. ve Delp, E. J., Deepfake video detection using recurrent neural networks, 15th IEEE international conference on advanced video and signal based surveillance (AVSS), Kasım 2018, Güney Kore, Bildiriler Kitabı, 1-6.
72. Amerini, I., Galteri, L., Caldelli, R. ve Del Bimbo, A., Deepfake video detection through optical flow based CNN, Proceedings of the IEEE/CVF international conference on computer vision workshops, Ekim 2019, Güney Kore, Bildiriler Kitabı, 0-0.
73. Verde, S., Bondi, L., Bestagini, P., Milani, S., Calvagno, G. ve Tubaro, S., Video codec forensics based on convolutional neural networks, 25th IEEE International Conference on Image Processing (ICIP), Ekim 2018, Yunanistan, Bildiriler Kitabı, 530-534.
74. Pessoa, R., Kokaram, A., Pitie, F. ve Sugrue, M., CNN-Based Video Codec Classifier For Multimedia Forensics, IEEE International Conference on Image Processing (ICIP), Eylül 2021, Arizona, Bildiriler Kitabı, 3033-3037.
75. Vinolin, V. ve Sucharitha, M., Video Forgery Detection Using Distance-based Features and Deep Convolutional Neural Network, 4th International Conference on Computing and Communications Technologies (ICCCT), Aralık 2021, Hindistan, Bildiriler Kitabı, 350-355.
76. Long, C., Smith, E., Basharat, A. ve Hoogs, A., A c3d-based convolutional neural network for frame dropping detection in a single video shot, IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Temmuz 2017, ABD, Bildiriler Kitabı, 1898-1906.
77. Long, C., Basharat, A. ve Hoogs, A., Video Frame Deletion and Duplication, Multimedia Forensics, (2022) 333-362.

78. Bagiwa, M. A., Wahab, A. W. A., Idris, M. Y. I. ve Khan, S., Digital video inpainting detection using correlation of hessian matrix, Malaysian Journal of Computer Science, 29, 3, (2016) 179-195.
79. Chen, S., Tan, S., Li, B. ve Huang, J., Automatic detection of object-based forgery in advanced video, IEEE Transactions on Circuits and Systems for Video Technology, 26, 11, (2015) 2138-2151.
80. Lin, C. S. ve Tsay, J. J., A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis, Digital Investigation, 11, 2, (2014) 120-140.
81. D'Avino, D., Cozzolino, D., Poggi, G. ve Verdoliva, L., Autoencoder with recurrent neural networks for video forgery detection, arXiv preprint arXiv:1708.08754 (2017).
82. Bakas, J. ve Naskar, R., A digital forensic technique for inter-frame video forgery detection based on 3D CNN, In Information Systems Security: 14th International Conference (ICISS), Aralık 2018, Hindistan, Bildiriler Kitabı, 304-317.
83. Sharma, H., Kanwal, N. ve Batth, R. S., An ontology of digital video forensics: Classification, research gaps and datasets, International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Aralık 2019, Dubai, Bildiriler Kitabı, 485-491.
84. Wang, W. ve Farid, H. Exposing digital forgeries in video by detecting duplication. In Proceedings of the 9th workshop on multimedia and security, Eylül 2007, New York, Bildiriler Kitabı, 35-42.
85. Lin, G. S. ve Chang, J. F., Detection of frame duplication forgery in videos based on spatial and temporal analysis, International Journal of Pattern Recognition and Artificial Intelligence, 26, 7, (2012) 1250017.
86. Singh, G. ve Singh, K., Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation, Multimedia Tools and Applications, 78, 9, (2019) 11527-11562.
87. Wang, W., Farid, H., Exposing digital forgeries in video by detecting double MPEG compression, ACM Press, New York, (2006) 37-47.
88. Wang, W. ve Farid, H., Exposing digital forgeries in video by detecting double quantization. In Proceedings of the 11th ACM workshop on Multimedia and security, Eylül 2009, New Jersey, Bildiriler Kitabı, 39-48.
89. Su, Y. ve Xu, J., Detection of double-compression in MPEG-2 videos. 2nd International Workshop on Intelligent Systems and Applications, Mayıs 2010, Wuhan, Bildiriler Kitabı, 1-4.
90. Aghamaleki, J. A. ve Behrad, A., Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding, Signal Processing: Image Communication, 47, (2016) 289-302.

91. Mahfoudi, G., Retraint, F., Morain-Nicolier, F. ve Pic, M. M., Statistical H. 264 Double Compression Detection Method Based on DCT Coefficients, IEEE Access, 10, (2022) 4271-4283.
92. Bayram, S., Sencar, H., Memon, N. ve Avcibas, I., Source camera identification based on CFA interpolation, In IEEE International Conference on Image Processing, Eylül 2005, İtalya, Bildiriler Kitabı, 3-69.
93. De, A., Chadha, H. ve Gupta, S., Detection of forgery in digital video, The 10th World Multi Conference on Systemics Cybernetics and Informatics, Temmuz 2006, Fransa, Bildiriler Kitabı, 229-233.
94. Mondaini, N., Caldelli, R., Piva, A., Barni, M. ve Cappellini, V., Detection of malevolent changes in digital video for forensic applications, In Security, steganography, and watermarking of multimedia contents IX, Şubat 2007, Kaliforniya, Bildiriler Kitabı, 300-311.
95. Bayram, S., Sencar, H. T. ve Memon, N., Video copy detection based on source device characteristics: a complementary approach to content-based methods, In Proceedings of the 1st ACM international conference on Multimedia information retrieval, Ekim 2008, Kanada, Bildiriler Kitabı, 435-442.
96. Kobayashi, M., Okabe, T. ve Sato, Y., Detecting video forgeries based on noise characteristics, In Pacific-Rim Symposium on Image and Video Technology, Ocak 2009, Berlin, Bildiriler Kitabı, 306-317.
97. Kobayashi, M., Okabe, T. ve Sato, Y., Detecting forgery from static-scene video based on inconsistency in noise level functions, IEEE Transactions on Information Forensics and Security, 5, 4, (2010) 883-892.
98. Taspinar, S., Mohanty, M. ve Memon, N., PRNU-based camera attribution from multiple seam-carved images, IEEE Transactions on Information Forensics and Security, 12, 12, (2017) 3065-3080.
99. Verdoliva, D. C. G. P. L., Extracting camera-based fingerprints for video forensics, In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Haziran 2019, Kaliforniya, Bildiriler Kitabı, 130-137.
100. Aslan A., Derin öğrenme tabanlı optik akış ile hareket tespiti, Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elâzığ, 2021.
101. Su, Y., Zhang, J. ve Liu, J., Exposing digital video forgery by detecting motion-compensated edge artifact, International Conference on Computational Intelligence and Software Engineering, Aralık 2009, Çin, Bildiriler Kitabı, 1-4.
102. Dong, Q., Yang, G. ve Zhu, N., A MCEA based passive forensics scheme for detecting frame-based video tampering, Digital Investigation, 9, 2, (2012) 151-159.
103. Chao, J., Jiang, X. ve Sun, T., A novel video inter-frame forgery model detection scheme based on optical flow consistency, In International workshop on digital watermarking, Ekim 2012, Berlin, Bildiriler Kitabı, 267-281.

104. Wang, W., Jiang, X., Wang, S., Wan, M. ve Sun, T., Identifying video forgery process using optical flow, In International Workshop on Digital Watermarking, Ekim 2013, Berlin, 244-257.
105. Singh, R. D. ve Aggarwal, N., Optical flow and prediction residual based hybrid forensic system for inter-frame tampering detection, Journal of Circuits, Systems and Computers, 26, 07, (2017) 1750107.
106. Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A. B., Ali, M. A. ve Zangana, H. M., Detection clone an object movement using an optical flow approach, IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), Nisan 2018, Malezya, Bildiriler Kitabı, 388-394.
107. Ding, X., Li, Y., Xia, M., He, J. ve Yang, G., Detection of motion compensated frame interpolation via motion-aligned temporal difference, Multimedia Tools and Applications, 78, 6, (2019) 7453-7477.
108. Tripathi, P.ve Singh, J., Identifying Video Forgery using Object Trajectory and Optical Flow, In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Aralık 2020, Hindistan, Bildiriler Kitabı, 980-985.
109. Karthikeyan, P., Bhavani, R., Rajiniginirath, D. ve Priya, R., Automatic Forged Scene Detection in Advanced Video Using Combined Mpeg-2 and Optical Flow Features, International Journal of Advanced Research in Engineering and Technology (IJARET), 11, 2, (2020) 246-258.
110. Ding, X., Huang, Y., Li, Y. Ve He, J., Forgery detection of motion compensation interpolated frames based on discontinuity of optical flow, Multimedia Tools and Applications, 79, 39, (2020) 28729-28754.
111. Singh, R. D. ve Aggarwal, N., Optical flow and pattern noise-based copy–paste detection in digital videos. Multimedia Systems, 27, 3, (2021) 449-469.
112. Kancherla, K. ve Mukkamala, S., Novel blind video forgery detection using markov models on motion residue, In Asian Conference on Intelligent Information and Database Systems, Mart 2012, Berlin, Bildiriler Kitabı, 308-315.
113. Zhang, Z., Hou, J., Li, Z. ve Li, D., Inter-frame forgery detection for static-background video based on MVP consistency, In International Workshop on Digital Watermarking, Ekim 2015, Tokyo, Bildiriler Kitabı, 94-106.
114. Yu, L., Wang, H., Han, Q., Niu, X., Yiu, S. M., Fang, J. ve Wang, Z., Exposing frame deletion by detecting abrupt changes in video streams, Neurocomputing, 205, (2016) 84-91.
115. Bakas, J., Naskar, R.ve Bakshi, S., Detection and localization of inter-frame forgeries in videos based on macroblock variation and motion vector analysis, Computers and Electrical Engineering, 89, (2021) 106929.

116. Kharat, J. ve Chougule, S., A passive blind forgery detection technique to identify frame duplication attack, Multimedia Tools and Applications, 79, 11, (2020) 8107-8123.
117. Wu, Y., Jiang, X., Sun, T. ve Wang, W., Exposing video inter-frame forgery based on velocity field consistency, IEEE international conference on acoustics, speech and signal processing (ICASSP), Mayıs 2014, İtalya, Bildiriler Kitabı, 2674-2678.
118. Sitara K., Mehtre B. M., A comprehensive approach for exposing inter-frame video forgeries, IEEE 13th International colloquium on signal processing its applications (CSPA), Ekim 2017, Malezya, Bildiriler Kitabı, 73-78.
119. Yang, J., Huang, T. Ve Su, L., Using similarity analysis to detect frame duplication forgery in videos, Multimedia Tools and Applications, 75, (2016) 1793-1811.
120. Liu, Y. ve Huang, T., Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis, Multimedia Systems, 23, (2017) 223-238.
121. Singh, V. K., Pant, P ve Tripathi, R. C., Detection of frame duplication type of forgery in digital video using sub-block-based features, In International conference on digital forensics and cyber crime, Ekim 2015, Güney Kore, Bildiriler Kitabı, 29-38.
122. Wei, W., Fan, X., Song, H. ve Wang, H., Video tamper detection based on multi-scale mutual information, Multimedia Tools and Applications, 78, 19, (2019) 27109-27126.
123. Bakas, J., Naskar, R. ve Dixit, R., Detection and localization of inter-frame video forgeries based on inconsistency in correlation distribution between Haralick coded frames, Multimedia Tools and Applications, 78, 4, (2019) 4905-4935.
124. Ren, H., Atwa, W., Zhang, H., Muhammad, S. ve Emam, M., Frame duplication forgery detection and localization algorithm based on the improved levenshtein distance, Scientific Programming, (2021) 1-10.
125. Aloraini, M., Sharifzadeh, M., Agarwal, C. ve Schonfeld, D., Statistical sequential analysis for object-based video forgery detection, Electronic Imaging, 5, (2019) 543.
126. Fadl, S., Han, Q. ve Qiong, L., Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image, Multidimensional Systems and Signal Processing, 31, 4, (2020) 1365-1384.
127. Dawood, H., Dawood, H. ve Guo, P., Texture image classification with improved weber local descriptor, In International Conference on Artificial Intelligence and Soft Computing, Haziran 2014, Polonya, Bildiriler Kitabı, 684-692.
128. Liao, S. Y. ve Huang, T. Q., Video copy-move forgery detection and localization based on Tamura texture features, 6th international congress on image and signal processing (CISP), Aralık 2013, Çin, Bildiriler Kitabı, 864-868.

129. Tralic, D., Grgic, S. ve Zovko-Cihlar, B., Video frame copy-move forgery detection based on cellular automata and local binary patterns, X International Symposium on Telecommunications (BIHTEL), Ekim 2014, Bosna Hersek, Bildiriler Kitabı, 1-4.
130. Saddique, M., Asghar, K., Bajwa, U. I., Hussain, M., ve Habib, Z., Spatial video forgery detection and localization using texture analysis of consecutive frames, Advances in Electrical and Computer Engineering, 19, 3, (2019)97-108.
131. Shelke, N. A., ve Kasana, S. S., Multiple forgery detection and localization technique for digital video using PCT and NBAP, Multimedia Tools and Applications, 81, 16, (2022) 22731-22759.
132. Kaur, M., Texture Feature Analysis for Inter-Frame Video Tampering Detection, In Proceedings of International Joint Conference on Advances in Computational Intelligence, Ekim 2022, Singapur, Bildiriler Kitabı, 305-318.
133. Pandey, R. C., Singh, S. K. ve Shukla, K. K., Passive copy-move forgery detection in videos, International conference on computer and communication technology (IC CCT) Eylül 2014, Hindistan, Bildiriler Kitabı, 301-306.
134. Ulutaş, G., Üstübioğlu, B., Ulutaş, M. ve Nabiyeve, V. V., Frame duplication detection based on bow model, Multimedia Systems, 24, 5, (2018) 549-567
135. Zhao, D. N., Wang, R. K. ve Lu, Z. M., Inter-frame passive-blind forgery detection for video shot based on similarity analysis. Multimedia Tools and Applications, 77, 19, (2018) 25389-25408.
136. Li, F. ve Huang, T., Video copy-move forgery detection and localization based on structural similarity, The 3rd International Conference on Multimedia Technology (ICMT 2013), Kasım 2013, Berlin, Bildiriler Kitabı, 63-76.
137. Van der Auwera, G., David, P. T. ve Reisslein, M., Traffic and quality characterization of single-layer video streams encoded with the H. 264/MPEG-4 advanced video coding standard and scalable video coding extension, IEEE Transactions on Broadcasting, 54(3), (2008) 698-718.
138. D'Amiano, L., Cozzolino, D., Poggi, G. ve Verdoliva, L., A patchmatch-based dense-field algorithm for video copy-move detection and localization, IEEE Transactions on Circuits and Systems for Video Technology, 29, 3, (2018) 669-682.
139. Bozkurt, I., Bozkurt, M. H. ve Ulutaş, G., A new video forgery detection approach based on forgery line, Turkish Journal Of Electrical Engineering and Computer Sciences, 25, 6, (2017) 4558-4574.
140. Fadl, S. M., Han, Q. ve Li, Q., Authentication of surveillance videos: detecting frame duplication based on residual frame, Journal of forensic sciences, 63, 4, (2018) 1099-1109.
141. Singh, G. ve Singh, K., Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation, Multimedia Tools and Applications, 78, 9, (2019) 11527-11562.

142. Jin, X., Su, Y. ve Jing, P., Video frame deletion detection based on time–frequency analysis, Journal of Visual Communication and Image Representation, 83, (2022) 103436.
143. Shanableh, T., Detection of frame deletion for digital video forensics, Digital Investigation, 10, 4, (2013) 350-360.
144. Wang, Q., Li, Z., Zhang, Z. ve Ma, Q., Video inter-frame forgery identification based on consistency of correlation coefficients of gray values, Journal of Computer and Communications, 2, 4, (2014) 51.
145. Hong, J. H., Yang, Y. ve Oh, B. T., Detection of frame deletion in HEVC-Coded video in the compressed domain, Digital Investigation, 30, (2019) 23-31.
146. Huang, C. C., Lee, C. E. ve Thing, V. L., A novel video forgery detection model based on triangular polarity feature classification. International Journal of Digital Crime and Forensics (IJDCF), 12, 1, (2020) 14-34.
147. Yao, Y., Shi, Y., Weng, S. ve Guan, B., Deep learning for detection of object-based forgery in advanced video, Symmetry, 10, 1, (2017) 3.
148. Kono, K., Yoshida, T., Ohshiro, S. ve Babaguchi, N., Passive video forgery detection considering spatio-temporal consistency, International Conference on Soft Computing and Pattern Recognition, Aralık 2018, Portekiz, Bildiriler Kitabı, 381-391.
149. Hong, J. H., Yang, Y. ve Oh, B. T., Detection of frame deletion in HEVC-Coded video in the compressed domain, Digital Investigation, 30, (2019) 23-31.
150. Fadl, S., Hosny, K. M. ve Hammad, M., Automatic fake document identification and localization using DE-Net and color-based features of foreign inks, Journal of Visual Communication and Image Representation, 92, (2023) 103801.
151. Yang, P., Baracchi, D., Iuliani, M., Shullani, D., Ni, R., Zhao, Y. ve Piva, A., Efficient video integrity analysis through container characterization, IEEE Journal of Selected Topics in Signal Processing, 14, 5, (2020) 947-954.
152. Xiang, Z., Horváth, J., Baireddy, S., Bestagini, P., Tubaro, S. ve Delp, E. J., Forensic Analysis of Video Files Using Metadata, The IEEE/CVF Conference on Computer Vision and Pattern Recognition, Haziran 2021, ABD, Bildiriler Kitabı, 1042-1051.
153. Altıncık, E., Sencar, H. T. ve Tabaa, D. Video Source Characterization Using Encoding and Encapsulation Characteristics, IEEE Transactions on Information Forensics and Security, 17, (2022) 3211-3224.
154. Shelke, N. A. ve Kasana, S. S. Multiple forgeries identification in digital video based on correlation consistency between entropy coded frames, Multimedia Systems, 28, 1, (2022) 267-280.
155. Sharma, H. ve Kanwal, N., Video interframe forgery detection: Classification, technique and new dataset, Journal of Computer Security, 29, 5, (2021) 531-550.

156. Panchal, H. D. ve Shah, H. B., Video tampering dataset development in temporal domain for video forgery authentication, Multimedia Tools and Applications, 79, 33, (2020) 24553-24577.
157. <https://sites.google.com/site/rewindpolimi/downloads/datasets/video-copy-move-forgeries-dataset> Video Copy-move forgeries dataset- REWIND Project. 15.12.2019.
158. <https://media.xiph.org/video/derf/> Video Test Media. 15.12.2019.
159. Ismael Al-Sanjary O., Ahmed A. A, Sulong G., Development of a video tampering dataset (VTD) for forensic investigation, Forensic Sci Int 266, (2016) 565–572.
160. Qadir G., Yahaya S. ve Ho A. T. S., Surrey University Library for Forensic Analysis (SULFA) of video content, IET Conference on Image Processing (IPR), Temmuz 2012, Londra, Bildiriler Kitabı, 1-6.
161. Soomro, K., Zamir, A. R. ve Shah, M., UCF101: A dataset of 101 human actions classes from videos in the wild, arXiv:1212.0402. (2012).
162. Cuevas, C., Yáñez, E. M. ve García, N., Labeled dataset for integral evaluation of moving object detection algorithms: LASIESTA, Computer Vision and Image Understanding, 152, (2016) 103-117.
163. Oh, S., Hoogs, A., Perera, A., Cuntoor, N., Chen, C. C., Lee, J. T., Mukherjee S., Aggarwal J. K., Lee H., Davis L., Swears E., Wang X., Ji Q., Reddy K., Shah M., Vondrick C., Pirsiavash H., Ramanan D., Yuen J., Torralba A., Song B., Fong A., Roy-Chowdhury A. ve Desai, M., A large-scale benchmark dataset for event recognition in surveillance video, Computer Vision and Pattern Recognition (CVPR) Haziran 2011, Colorado Springs, Bildiriler Kitabı, 3153-3160.
164. Jung, Y. J., Lee, S. I., Sohn, H., Park, H. ve Ro, Y. M., Visual comfort assessment metric based on salient object motion information in stereoscopic video, Journal of Electronic Imaging, 21, 1, (2012) 011008.
165. Ojala, T., Pietikäinen, M. ve Harwood, D., A comparative study of texture measures with classification based on featured distributions. Pattern recognition, 29, 1, (1996) 51-59.
166. Chen, J., Shan, S., He, C., Zhao, G., Pietikäinen, M., Chen, X. ve Gao, W. WLD: A robust local image descriptor, IEEE transactions on pattern analysis and machine intelligence, 32, 9, (2009) 1705-1720.
167. Wang, Z., Bovik, A. C., Sheikh, H. R. ve Simoncelli, E. P., Image quality assessment: from error visibility to structural similarity, IEEE transactions on image processing, 13, 4, (2004) 600-612.
168. Irmak H., Real Time Traffic Sign Recognition System On FPGA, Yüksek Lisans Tezi, M.E.T.U., Fen Bilimleri Enstitüsü, Ankara, 2010.
169. Canny, J., A computational approach to edge detection, IEEE Transactions on pattern analysis and machine intelligence, 6, (1986) 679-698.

170. Marr, D. ve Hildreth, E., Theory of edge detection, Proceedings of the Royal Society of London. Series B. Biological Sciences, 207, 1167, (1980) 187-217.
171. Ahmed, N., Natarajan, T. ve Rao, K. R., Discrete cosine transform, IEEE Trans. Computer, C-32, (1974) 90-93.
172. <https://www.mathworks.com/help/images/discrete-cosine-transform.html/> AKD. 14.04.2023
173. Mallat, S. G., A theory for multiresolution signal decomposition: the wavelet representation, IEEE transactions on pattern analysis and machine intelligence, 11, 7, (1989) 674-693.
174. Rinky, B. P., Mondal, P., Manikantan, K. ve Ramachandran, S., DWT based feature extraction using edge tracked scale normalization for enhanced face recognition. Procedia Technology, 6, (2012) 344-353.
175. Ulutaş, G., Üstübioğlu, B., Ulutaş, M. ve Nabiyeve, V., Video forgery detection method based on local difference binary, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 26, 5, (2020) 983-992.
176. Yuan, X. J., Huang, T. Q., Chen, Z. W., Wu, T. H. ve Su, L. C., Digital video forgeries detection based on textural features, Computer Systems and Applications, 21, 6, (2012) 91-95.

ÖZGEÇMİŞ

Işılray Bozkurt; Konya’ da başladığı eğitim hayatını Ağrı ve İçel illerinde devam ettirdikten sonra Gaziantep’ de lise eğitimini tamamladı. Lisans eğitimini Karadeniz Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü’nde 2012 yılında tamamladı. Ardından mezun olduğu sene Gaziantep’te telekom sektöründe 1 sene çalıştı ve 2014 yılında yüksek lisans eğitimine başlayarak 1 sene İngilizce hazırlık okuduktan sonra 2015 yılında Of Teknoloji Fakültesi Yazılım Mühendisliği bölümünde araştırma görevlisi olarak çalışmaya başladığı görevine halen devam etmektedir. 2017 yılında yüksek lisans eğitimini tamamlayarak doktora eğitimine başladı. Tez kapsamında yayınlanan başlıca yayınları sonraki sayfada verilmiştir.

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

- 1- Bozkurt I., Ulutaş G., Detection and localization of frame duplication using binary image template, Multimedia Tools And Applications, 10.1007/s11042-023-14602-y.

Ulusal hakemli dergilerde yayınlanan makaleler (ESCI)

- 1- Bozkurt I., Ulutaş G., Duplicated frame forgery detection in videos based on edge detection, Pamukkale University Journal Of Engineering Sciences, 10.5505/pajes.2021.88393.

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

- 1- Bozkurt I., Ulutaş G., Exposing inter frame forgery in videos by hybrid system, (Gönderim aşamasında).

Ulusal ve uluslararası konferanslarda sözlü sunumu yapılan bildiriler

- 1- Bozkurt I., Ulutaş G., Duplication forgery detection based on weber algorithm, International Conference on Engineering Technologies, Türkiye, 17 Kasım 2022, Bildiriler Kitabı: 73- 76.
- 2- Bozkurt I., Ulutaş G., Duplication detection in videos using DWT algorithm, International Conference on Engineering Technologies, Türkiye, 17 Kasım 2022, Bildiriler Kitabı: 65- 68.
- 3- Bozkurt I., Ulutaş G., The Localization of Deleted Frames in the Forged Videos, 28th Signal Processing and Communications Applications Conference, SIU 2020, Gaziantep, Türkiye, 05- 07 Ekim 2020, Bildiriler Kitabı: 1- 4.