T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

YAPAY ZEKA YÖNTEMLERİ İLE BÖLGE TABANLI KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

Hazırlayan
Abdurrahman Yavuz ASLANTAŞ

Danışman
Dr. Öğr. Üyesi Fehim KÖYLÜ

Yüksek Lisans Tezi

Haziran 2022
KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

YAPAY ZEKA YÖNTEMLERİ İLE BÖLGE TABANLI KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

(Yüksek Lisans Tezi)

Hazırlayan
Abdurrahman Yavuz ASLANTAŞ

Danışman
Dr. Öğr. Üyesi Fehim KÖYLÜ

Bu çalışma Erciyes Üniversitesi Bilimsel Araştırma Projeleri Birimi tarafından FYL-2020-10375 kodlu proje ile desteklenmiştir.

Haziran 2022
KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Abdurrahman Yavuz ASLANTAŞ
İmza:

YÖNERGEYE UYGUNLUK

"Yapay Zeka Yöntemleri İle Bölge Tabanlı Kopyala-Yapıştır Sahteciliği Tespiti" adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi'ne uygun olarak hazırlanmıştır.

Tezi Hazırlayan	**Danışman**
Abdurrahman Yavuz ASLANTAŞ	Dr. Öğr. Üyesi Fehim KÖYLÜ

Bilgisayar Mühendisliği ABD Başkanı
Prof. Dr. Veysel ASLANTAŞ

TEŞEKKÜR

Bu tez çalışmasının hazırlanma sürecinde konunun belirlenmesinde, geliştirilmesinde ve deneyler ile sonuçların değerlendirilmesinde maddi-manevi bilgilerini ve tecrubelerini esirgemeyen çok değerli danışman hocam sayın Dr. Öğr. Üyesi Fehim KÖYLÜ'ye teşekkür ederim.

Tez çalışmam sırasında maddi manevi desteğini esirgemeyen, değerli fikir ve görüslerini her zaman benimle paylaşan değerli Dr. Ögr. Üyesi Ahmet Nusret Toprak hocama teşekkür ederim.

Her zaman ve her şartta yanımda olan, bilgisini ve dostluğunu esirgemeyen hem kardeşim hem hocam sayın Arş.Gör. Mehmet ELMACI'ya teşekkürü bir borç bilirim.

Son olarak eğitim hayatım boyunca her zaman destekçim olan aileme sonsuz teşekkür ederim.

YAPAY ZEKA YÖNTEMLERİ İLE BÖLGE TABANLI KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

Abdurrahman Yavuz ASLANTAŞ
Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Haziran 2022
Danışman : Dr. Öğr. Üyesi Fehim KÖYLÜ

ÖZET

Teknolojinin gelişmesi ile beraber sayısal olarak herhangi bir resim üzerinde kolaylıkla değişiklikler yapılabilmektedir. Herhangi bir görüntü üzerinde değiştirilme yapılıp yapılmadığının tespit edilmesi hukuki, askeri, siyasi vb. birçok açıdan büyük bir problem haline gelmiştir. Görüntü üzerinde yapılan sahtecilik türleri içerisinde en yaygın olarak kullanılan biçimi, kopyala yapıştır sahteciliğidir. Literatürde resim içinde tekrar eden bölgelerin belirlenmesi için çeşitli yöntemler ortaya konulmuştur. Bu yöntemler blok temelli, anahtar nokta temelli, bölütleme ve derin öğrenme temelli olmak üzere dört sınıfa ayrılmaktadır.

Görüntü üzerinde anlamlı bölgeleri tespit etme işlemine anlamsal bölütleme denilmektedir. Anlamsal bölütleme askeri, robotik, biyomedikal gibi pek çok alanda kullanılmaktadır. Tez çalışmasında kopyala yapıştır sahteciliği tespiti yöntemleri incelenmiş ve anlamsal bölütlemeye dayalı yeni bir yöntem sunulmuştur. Sahtecilik bölgelerinin daha yüksek doğrulukla tespitini yaparken aynı zamanda hesaplama süresini de azaltacak biçimde ayrık kosinüs dönüşümü ve anlamsal bölütleme tabanlı bir kopyala yapıştır sahteciliği tespit algoritması geliştirilmiştir.

Önerilen yöntem, literatürdeki diğer blok tabanlı çalışmalarla karşılaştırılmıştır. Deney sonuçları ile önerilen yöntemin zaman maliyetini düşürdüğü ve başarı sonucunu artırdığı ispat edilmiştir.

Anahtar Kelimeler: Kopyala Yapıştır Sahteciliği, Görüntü Anlamsal Bölütleme, Derin Öğrenme, Bilgi Güvenliği, Görüntü Sahteciliği

DETECTION OF COPY-PASTE FORGERIES BASED ON REGION USING ARTIFICIAL INTELLIGENCE METHODS

Abdurrahman Yavuz ASLANTAŞ
Erciyes University, Graduate School of Natural and Applied Sciences
M.Sc. Thesis, February 2022
Supervisor: Asst. Prof. Dr. Fehim KÖYLÜ

ABSTRACT

With the advancement of technology, it is simple to modify any digital image. Detecting if a picture has been modified has legal, military, political, and other applications. It has become a significant issue in several ways. Copy-and-paste forgery is the most prevalent sort of picture forgery. Numerous techniques have been presented in the literature for identifying repeating sections in an image. These approaches are categorized as block-based, key-point-based, segmentation-based, and deep learning-based.

The method of identifying meaningful picture sections is known as semantic segmentation. Semantic segmentation is utilized in several disciplines, including the military, robotics, and healthcare. In the thesis, detection approaches for copy-paste fraud were analyzed, and a novel method based on semantic segmentation was developed. A copy-paste forgery detection technique based on discrete cosine transform and semantic segmentation has been developed, which reduces computation time while increasing the accuracy of detecting counterfeit regions.

In the literature, the suggested strategy was compared to existing block-based investigations. The experimental findings demonstrate that the suggested strategy decreases the cost of time and improves the success rate.

Keywords: Copy-Move Forgery Detection, Deep Learning, Semantic Segmentation, İnformation Security, İmage Forensic

İÇİNDEKİLER

YAPAY ZEKA YÖNTEMLERİ İLE BÖLGE TABANLI KOPYALA-YAPIŞTIR SAHTECİLİĞİ TESPİTİ

KISALTMALAR

AKD	Ayrık Kosinüs Dönüşümü
ADD	Ayrık Dalgacık Dönüşümü
DİA	Dijital İmza Algoritması
HOG	Gradyanların Histogramı
YİÖ	Yerel İkili Örüntü
SIFT	Ölçek Bağımsız Özellik Dönüşüm
TDA	Tekil Değer Ayrışımı

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GİRİŞ

Teknolojinin gelişmesi ile günümüzde görüntüleri kaydeden cihazların sayısındaki artış, seri üretimin hızlanması ve maliyetinin düşmesinden kaynaklı olarak sayısal görüntü üzerinde sahtecilik oranı artmıştır. Aynı zamanda internetin aktif kullanılışı, güçlü resim işleme ve düzenleme programlarının artmasından kaynaklı olarak herhangi bir görüntü üzerinde herkes tarafından çok kolay biçimde manipülasyon yapılabilmesini mümkün hale gelmiştir. Bu durum karşılaştığımız görüntülerin sahte mi gerçek mi olup olmadığına güvenilemeyeceği sonucunu çıkartmaktadır. Ancak adli ve tıbbi vakalar olmak üzere birçok durumda görüntünün gerçekliğinin sorgulanması, karar için en temel problemi teşkil etmektedir.

Araştırma Problemi

Sahte görüntü tespiti, kritik önem taşıyan görüntüler üzerinde herhangi bir kurcalama olup olmadığı, görüntü üzerinde bir bilginin üzerine başka bir sahnenin yapıştırılması ile gerçeğin saklanıp saklanmadığı gibi durumları, bilgisayar destekli olarak belirlenmesi problemi olarak ifade edilmektedir.

Güçlü görüntü işleme araçları, her yaş gurubu insan için basit veya profesyonel sahtecilik yapmayı mümkün kılmaktadır. Tıp, gazetecilik, hukuk, istihbarat ve adli olaylarda sıkça delil olarak kullanılan görüntünün doğruluğunun tespiti büyük bir önem arz etmektedir. Sayısal görüntülerin mahkemelerde delil, askeri ve istihbarı alanlarda kritik önem taşıyan bilgilere sahip olması, görüntülerin farklı alanda kullanılır olması, görüntü üzerinde yapılan sahtecilik işlemlerinin artması, eldeki görüntülerin doğruluğunu tespit edebilmeyi zor bir hale getirmiştir. Var olan sahte görüntülerin doğruluğu ispatlanmadan kitleleri yönlendirebilmek, onları istedikleri olaylara kanalize etmek oldukça basit bir durum haline gelmiştir. Görüntü üzerinde yapılan sahtecilik yöntemlerinin artması, görüntü üzerinde elde edilen bilginin sınırlı olması ile, görüntü üzerinde sahtecilik tespiti metotlarını karmaşık bir hale getirebilmektedir.

Kopyala yapıştır sahteciliğini tespit etmek için literatürde kullanılan anahtar nokta tabanlı ve blok temelli olmak üzere iki adet yaklaşım bulunmaktadır. Blok temelli yaklaşımların zaman maliyeti yüksek olduğu için tercihen anahtar nokta tabanlı yaklaşımlara yönelim artmıştır.

Araştırmanın Amacı ve Önemi

Adli bilişim, bir görüntü üzerinde bir bilgiyi gizlemek veya manipüle etmek amacıyla oluşturulan kurcalanmış görüntüleri tespit etmek ve bilgisayar sistemleri yardımıyla analiz edilip bulunmasını temel alan bir mühendislik alanıdır.

Görüntü üzerinde yapılan sahteciliklerde en sık kullanılanı kopyala yapıştır sahteciliği, görüntü üzerinde bir bilgiyi gizlemek için aynı görüntü üzerinde olan bir bölgenin belli bir hedef bölgeye yapıştırılması ile oluşur. Örnek olarak yapılan sahtecilikler ile ülke içerisinde bulunan bir askeri karargâhtan fırlatılan füzenin yerine, aynı görüntü üzerinden yapıştırılan bir gökyüzü parçası ile füze atmadığı ispat edilmeye çalışılabilmektedir. Farklı bir örnek olarak herhangi bir istihbaratı operasyon sonucu cinayete kurban giden kişinin vurulma noktaları, farklı yerlerden alınan deriye ait görüntü parçaları ile kapatılabilmektedir. Bunun için kritik önem taşıyan bir görüntü üzerinde kurcalanmış kaynak ve hedef bölgeleri tespit etmek adli bilişim için önemli bir alandır.
Kaynak ve hedef bölgeyi doğru tespit etmek için blok temelli yaklaşımlar, başarı açısından iyi olsa bile süre maliyeti açısından tercih edilmemektedir. Yapılan çalışma ile bu süre maliyetini minimalize etmek ve tespit başarımını artırmak, blok temelli yaklaşımlara yönelimi artıracaktır.

Tezin Organizasyonu

Tezin ilk bölümün de literatürde olan görüntü sahtecilik türlerinden kısaca bahsedilmiştir. Görüntü sahtecilikleri aktif ve pasif olarak ikiye ayrılmaktadır. Pasif yöntemler içerisinde yaygın olarak kullanılan kopyala-yapıştır sahteciliği hakkında yapılan literatürdeki çalışmalar hakkında bilgi verilmiştir.

Tezin ikinci bölümünde yapılan çalışmanın yöntemi hakkında bilgi verilmiştir. Önerilen yöntemin algoritmik olarak ifade edilmiştir. Aynı zamanda yapılan çalışmada kullanılan modeller ve veri kümeleri hakkında da kısaca bahsedilmiştir.

Tezin üçüncü bölümünde önerilen yöntemin mevcut yöntem ile kıyaslanarak sayısal başarı sonuçları tablolar halinde ifade edilmiştir.

Tezin dördüncü bölümünde yapılan çalışmanın sonucu, gerçekleştirilen yöntemin güçsüz ve eksik kaldığı noktalar ve iyileştirilmesi için ne yapılması gerektiğine dair öneriler verilmektedir.

1. BÖLÜM

GENEL BİLGİLER

Sayısal görüntüler, sayı dizileri ile ifade edilen renk kodları içermektedir. Bu değerler üzerinde belirli sahtecilik yöntemleri ile kolaylıkla oynama yapılabilmektedir. Herhangi bir resim üzerinde olmayan bir nesnenin sonradan eklenmesi, sahnedeki bir cismin kaybedilmesi veya çoğaltılması gibi resim üzerinde yapılan işlemlere görüntü sahteciliği denir. Bu işlemler sayısal resimlerin güvenirliğini azaltan sahtecilik davranışlarının ortaya çıkmasına sebep olmaktadır.

Bu sahtecilik faaliyetleri aynı zamanda suç unsurunu barındırdığı için adli bilişimin ilgi alanı haline gelmiştir. Kurcalanmış görüntüler, kitlelere belli bir fikri dayatma amacı taşıdığı için toplumlar için de tehlikeler taşımaktadır. Örneğin toplumsal olarak kültür farklılığı olan insanlar arası çatışma çıkarabilmek için karşıt tarafların birbirilerinin kutsallarına karşı zarar verici davranışlarının gösterilmiş olduğu sahte fotoğraflar üretmek yeterli olacaktır.

Gözle fark edilemeyecek derecede titiz yapılan rötuşlarla oynanmış bir görüntünün, internetten çok hızlı biçimde yayılmasıyla aynı resmin birçok yerde görülmesi, insanların algısını negatif yönde değiştirip, olayın gerçek zannedilmesine yol açmaktadır. Devletleri, toplumları veya kurumları manipüle edebilecek ve yanlış kararlar alınmasına yol açabilecek diplomatik, siyasi, hukuki, toplumsal, askeri birçok problemin ortaya çıkmasına yol açabilmesi, sahteciliğin var olup olmadığının tespit yöntemlerinin gerçeklerin gün yüzüne çıkabilmesi için ne kadar gerekli olduğunu göstermektedir. Bundan dolayı kaynak görüntünün güvenilirliğini belirlenmesi için otomatik sahtecilik tespiti yöntem ve metotlarına yönelik ilgiyi artırmıştır.

Görüntü sahteciliği tespiti, mevcut bir sayısal görüntünün gerçekliğini veya görüntü

üzerinde kameradan ilk kaydedildiği andaki hali üzerinde herhangi bir kurcalama olup olmadığını doğrulamayı amaçlar. Görüntü sahteciliği, aktif ve pasif yöntemler olmak üzere iki ana başlıkta incelenmektedir. Aktif yöntemlerde mutlaka bir ek bilgi orijinal görüntüye eklenir. Saldırı olup olmadığı eklenen bilginin durumuna göre tespit edilir. Pasif yöntemlerde ise herhangi bir bilgi eklemesi işlemi bulunmamaktadır. Pasif yöntemlerde temel mantık, görüntülerden özellik elde edilmesi ve görüntü sahteciliği tespiti için kullanılmasıdır.

1.1. Görüntü Sahteciliği

Kurcalama kelimesinin edebi anlamı; herhangi bir şeye müdahale etmek için izin verilmeden yapılan değişikliklere veya kasıtlı zarar verme işlemine denir. Görüntü sahteciliği, dijital kameraların ve görüntü üzerinde işlem yapan yazılımların artması ile ciddi bir sorun haline gelmesine rağmen, görüntü sahteciliği yirmi birinci yüzyıla özgü bir sorun değildir. Görüntü sahteciliğinin tarihi 1840'lı yıllara kadar uzanmaktadır. Hippolyte Bayard tarafından intihar ederken çekilmiş olan Şekil 1.1.'de verilen fotoğraf, tarihin kaydetmiş olduğu ilk sahte görüntüdür.

Bilgisayarların ortaya çıkmasından önce fotoğraf manipülasyonu, mürekkep ve boya rötuşlama, çift pozlama, fotoğrafları veya negatifleri karanlık odada bir araya getirme veya negatif resmi çizme yoluyla gerçekleştiriliyordu. Fotoğrafçılığın ilk günlerindeki teknoloji, şimdiki kadar karmaşık ve yüksek performanslı değildi. İlkel yolla yapılan manipülasyonların sonuçları, dijital manipülasyonların sonuçlarıyla karşılaştırılabilir ancak gerçekleştirilmesi çok daha maliyetliydi [1].

Şekil 1.1. Hippolyte Bayard'ın intihar ettiğini gösteren sahte görüntü [2].

Dijital görüntü kurcalama, geleneksel görüntülerin dijital sürümleriyle değiştirilmesi dışında, geleneksel fotoğraf sahteciliğine oldukça benzerdir. Dijital bir görüntünün temel özelliklerinden biri, analog eşdeğerine kıyasla manipülasyon edilebilmesi daha kolaydır. Dijital resim işleme süreci, düşük maliyetli ve gelişmiş resim düzenleme yazılımları sayesinde son yıllarda basitleştirildi ve daha kolay hale getirildi.

Görüntü kurcalama tekniklerinin ilerlemesi birtakım avantajlar ve problemler sunmaktadır. Görüntü düzenleyiciler, görüntüler için bir modelleme olanağı sağlar ve insanları görsel sanatlar alanındaki faaliyetlerini artırmasına yardımcı olurken, aynı zamanda, sahte fikirler ve bu fikirlerin görüntüler üzerinde sunulması ile eldeki görüntünün gerçekliği sorgulanır hale gelmektedir. Bu sahtecilikler fotoğraf üzerinde herhangi bir görünür iz bırakmadan görüntü materyali üretmektedir. Örneğin, resim manipülasyonu siyasi bir kasıtla yapılırsa, ortaya konan sahte görüntüler kamuoyunun dikkatini çekip algı operasyonları yapılmasına neden olmaktadır. Bu bağlamda, Kerry Fonda 2004 seçim fotoğrafı sorunu mükemmel bir örnek teşkil etmektedir. İki ayrı zamanda çekilen iki fotoğraf, kamuoyunu manipüle etmek için birleştirilmiştir. İlerleyen süreçte bu çekimin sahte olduğu ortaya çıktıktan sonra fotoğrafların farklı yıllarda çekilmiş iki ayrı görüntünün birleştirilmesi ile oluşturulduğu tespit edilmiştir. Günümüz teknolojisiyle ileri düzeyde görüntü düzenleme yapmak için gelişmiş görüntü işleme

teknikleri kullanılmıştır. Otomasyon yaklaşımları ile saniyeler içinde sahte görüntüler elde edilebildiği gibi aynı zamanda üretilen sahte resimlerin tespit edilebilmesi de mümkündür.

1.2. Görüntü Sahteciliği Tespit Yöntemleri

Görüntü işleme, dijital cihazlarda yazılım kullanılarak bir görüntü üzerinde gerçekleştirilebilen işlemler bütünüdür. Yaygın olarak kullanılan görüntü işleme teknikleri, sadece bir görüntünün boyutunu değiştirmek için yapılan piksel tabanlı işlemleri değil, aynı zamanda sayısal bir görüntü üzerinde bir nesneyi silme veya ekleme gibi içerik düzeyindeki işlemleri de kapsamaktadır. Fotoğraf üzerinde gerçeği gizlemek veya değiştirmek için kasıtlı olarak yapılan kurcalama işlemine görüntü sahteciliği denir. Genel olarak dijital resim sahteciliği aktif ve pasif yöntemler olmak üzere iki kısma ayrılmaktadır.

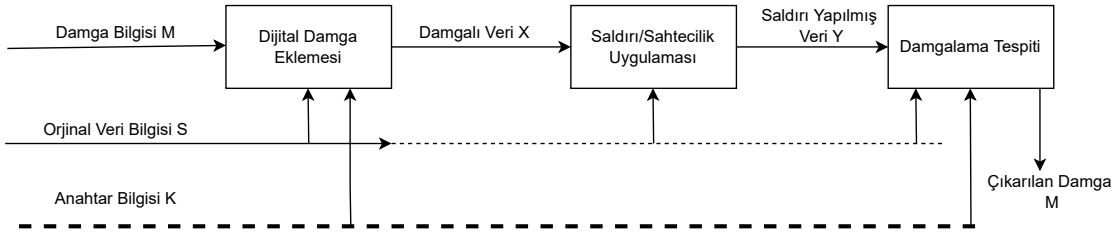
1.2.1. Aktif Yöntemler

Aktif yöntemler görüntü oluşturulurken ya da hazır görüntüye ek bilgi (digital watermark vb.) eklenerek görüntü sahteciliği tespiti yapılmaktadır. Aktif yöntemlerle görüntü sahteciliği temel olarak görüntü damgalama (digital watermark) ve sayısal imza (digital signature) olmak üzere iki farklı yöntem ile yapılmaktadır [2].

1.2.1.1. Görüntü Damgalama

Sayısal damgalama, görsel veri üzerinde herhangi bir saldırı olup olmadığının anlaşılması hususunda yaygın olarak kullanılan bir tekniktir. Sayısal damgalamada temel mantık, bir sayısal verinin damga (filigran) olarak başka bir sayısal veriye gömülmesi işlemidir. Şekil 1.2.'de temel damgalama ve damga çıkarma yöntemi verilmiştir. Burada orijinal veri (S) üzerine dijital damga (M), K anahtarı ile eklenir. Damgalama işlemi sonucunda damgalanmış veri (X) elde edilir. Damgalı X verisine saldırı yapılması ile Y verisi elde edilir. S orijinal verisi ve K anahtar bilgisi kullanılarak Y verisi üzerinde damgalama tespiti yapılır. Bileşenleri gibi orijinal görüntü verilerine veya algısal özelliklerden faydalanacak şekilde tasarlanmıştır. Filigranlamanın temel gereksinimleri saydamlık,

genel sinyal işleme işlemlerine karşı dayanıklılık, kapasite, maliyet ve güvenliktir. Saydamlık görünmez damgalama için oldukça önemlidir.



Şekil 1.2. Dijital damgalama ve damga çıkarma işlemleri.

Normal koşullarda eklenen damga görülmemeli, damga eklenince orijinal görüntünün kalitesi bozulmamalıdır. Ayrıca genel sinyal işleme, resim sıkıştırma (jpeg vb.), ölçekleme, filtreleme ve kırpma işlemleri sonucunda elde edilecek değişimlere karşı damga dayanıklı biçimde kaybedilmemiş olmalıdır. Kapasite, ana görüntüde gizlenebilen ve normal çalışma koşullarında güvenilir bir şekilde algılanabilen bilgi miktarı demektir. Filigran, görüntü üzerinde fark edilebilir bozulmaları en aza indirecek şekilde ölçeklenebilmektedir. Filigranın kendisi filigran bilgisinin, gizli veya genel anahtarın bir işlevi olabilir. Filigranlar seri numarası, kredi kartı numarası, logo, resim ve imza gibi görsel ikili sekans içerebilir. Mevcut tekniklerin birçoğu birçok pikselin üzerine bir bit bilgi ekler veya katsayıları dönüştürür, filigran bilgisini kurtarmak için de klasik algılama şemalarını kullanır. Görüntüler üzerine eklenmiş filigranların tespiti için mevcutsa ana görüntünün sinyalinin kaldırılması ve korelasyon operatörü gereklidir [3] .

Görüntü damgalama, uygulandığı uzay bakımından iki farklı yöntemle gerçekleştirilmektedir. Bunlar görüntü uzayı ve frekans uzayıdır. Görüntü uzayında sayısal damgalama için en eski yöntem, m sekanslarını görüntüden sağlanacak en az önemli bite (Least Significant Bit, LSB) etkili ve şeffaf gömme yöntemidir [3, 4]. M-sekansları iyi korelasyon özelliklerinden dolayı seçilir. Ayrıca bu tekniklerin kullanılması maliyet bakımından avantajlıdır. Bu yöntemlerin kullanılmasının ardından iki boyutlu matris şeklinde filigran ekleme yöntemi önerilmiştir. Bu yöntemde Wolfgang ve arkadaşları m-sekansları iki boyutlu yapıya getirilerek bloklar halinde eklenir. Önerilen yöntemin JPEG sıkıştırmasına karşı sağlam (robust) bir damgalama olduğunu

göstermiştir. Ayrıca görüntü üzerindeki değişiklikleri bloklar bazında tespit edebilen kırılgan bir damgalama yöntemi olduğu görülmüştür [5]. Damgalama tekniklerinin büyük bir kısmı, filigran sinyalinin doğrudan orijinal veriye frekans uzayında eklenmesiyle yapılır. Frekans uzayında damgalama için ayrık dalgacık dönüşümü (Discrete Wavelet Transform,ADD,DWT) başta olmak üzere Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform, AKD, DCT) ve tekil değer ayrışımı (Singular Value Decomposition, TDA, SVD) uzayları kullanılır. Farklı görüntülerin farklı frekans dağılımları mevcuttur. Filigran gömme işlemi yaygın olarak ADD uzayında uygulanır. Çünkü ADD bir görüntüyü farklı bileşenlerine ayırır [6]. Farklı frekans bileşenleri görüntü sıkıştırma işlemlerine karşı farklı hassasiyet gösterir. Bu da filigranın hassasiyetini kontrol edebilmeyi kolaylaştırır [7]. Bir filigranın hassasiyeti başlıca iki faktörden etkilenir: Bunlardan ilki görüntünün her frekans bileşenine gömülü filigran bitlerinin miktarı ve ikincisi de nicelik parametresi ile kontrol edilen filigran gömme gücüdür. Alıcı tarafında görüntüde sahtelik olup olmadığının tespiti, çıkarılan filigranın bozulmuş olup olmaması ile alakalıdır [8]. Görüntü damgalama uygulamalarında optimizasyon algoritmalarının kullanılması, damgalama başarısını artırmaktadır [9, 10]. Görüntü damgalama, damganın dayanıklılık durumuna göre sağlam (robust), kırılgan (fragile) ve yarı kırılgan (semi fragile) olmak üzere üç çeşittir. Sağlam damgalamada görüntüye saldırı yapıldığında bile damga kolaylıkla algılanabilir durumdadır. Sağlam damgalama genellikle telif hakkı korunması gibi işlemlerde kullanılır. Kırılgan damgalama herhangi bir saldırı durumunda bozulmaya uğrar. Kırılgan damgalama genellikle kurcalama tespitinde kullanılır. Yarı kırılgan damgalamada ise uygulanan damga belirtilen, istenen bazı işlemlerden etkilenmez ve istenmeyen her türlü saldırıdan etkilenebilir durumdadır [3, 11].

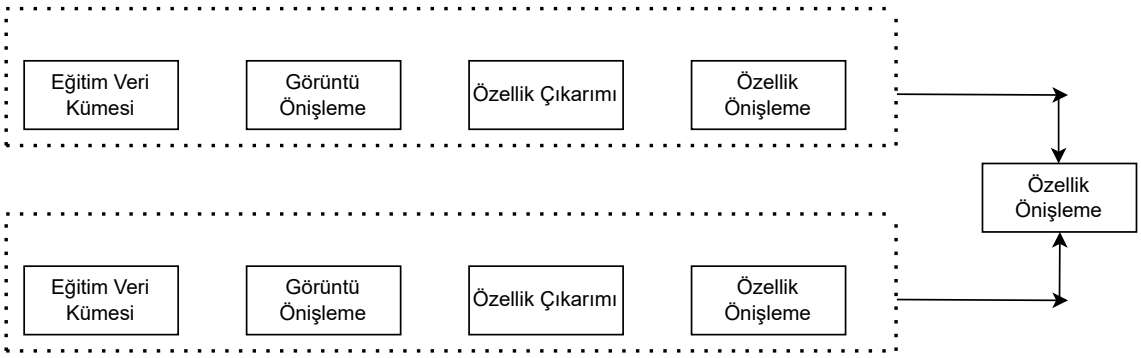
1.2.1.2. Sayısal İmza

Dijital imza, veri doğrulaması için kullanılan bir tür kriptografidir. Burada esas olan, bilgilerin dönüştürülmesinde kullanılan şifreleme ve şifre çözme işlemidir. Erişim anahtarı olmadan kimse bilgilere erişemez. Erişim anahtarı, gizli anahtar (Secret Key, Symmetric Cryptography) ve açık anahtar (Public Key, Assymetric Cryptography) olmak üzere iki farklı şekilde kullanılmaktadır. Gizli anahtar kullanan haberleşmede hem gönderici hem alıcı şifreleme/şifre çözme anahtarını bilmelidir. Açık anahtar yönteminde

ise şifreleme ve şifre çözme için farklı anahtar kullanılır. Şifreleme anahtarı herkes tarafından bilindiği gibi, şifre çözme anahtarını ise yalnız yetkisi olan kişiler tarafından bilinmektedir [12]. Dijital imza yöneticiler tarafından, dijital imza algoritması (Digital Signature Algorithm,DİA, DSA) güvenli bir hash algoritması (Secure Hashing, SHA) kullanılarak kişiye özgü bir şekilde oluşturulur.

1.2.2. Pasif Yöntemler

Pasif yöntemlerle görüntü sahteciliği tespiti, aktif yöntemler gibi herhangi bir ek bilgi veya ön bilgi gerektirmez. Bu yöntemler, düzenleme veya fotoğraf elde edilme türüne dayalı olarak görüntünün kendine özgü özelliklerini çıkararak sahtecilik yapılır. Pasif yöntemlerle yapılmış sahtecilik tespiti, sahtecilik yapılmış görüntü üzerinde hiçbir iz bırakılmadığı varsayımına dayanmaktadır. Bu yöntemler görüntü üzerindeki istatistiksel bilgiler veya görüntü üzerindeki tutarsızlık olarak algılanabilecek bölgeleri tespit etmeye çalışmaktadır. Pasif yöntemlerle sahtecilik tespiti genellikle görüntüden özellik çıkarıp bu özelliklerin bir sınıflandırıcı kullanılarak sınıflandırılmasıyla gerçekleştirilir [13, 14]. Pasif yöntemlerle görüntü sahteciliği tespiti için bazı ara işlemler kullanılabilmektedir. Bunlar; görüntü önizleme (image preprocessing), sınıflandırıcı seçimi (classifier selection), ve sınıflandırma işlemlerinden oluşmaktadır. Şekil 1.3.'te bu işlemler verilmiştir.

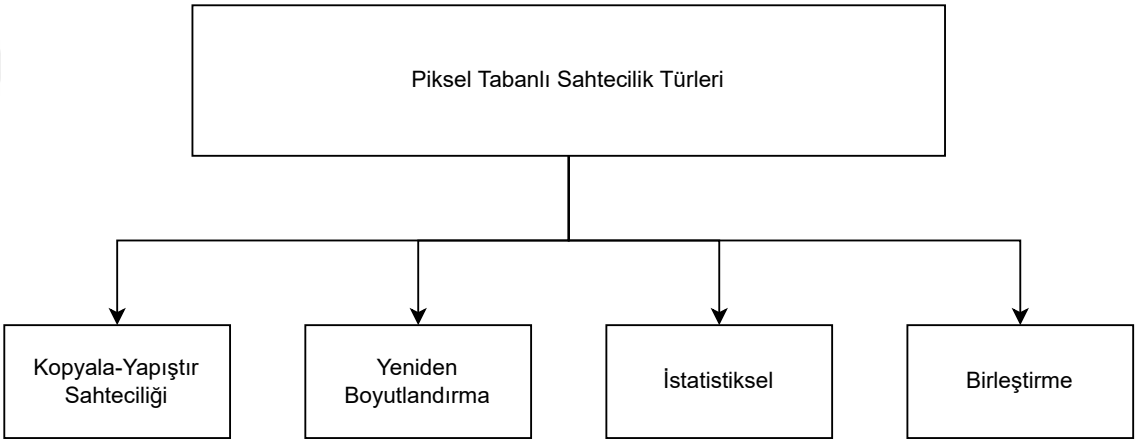


Şekil 1.3. Pasif yöntemlerle sahtecilik tespiti aşamaları.

- **Görüntü rötuşlama:** Diğer görüntü sahteciliği yöntemlerinden daha az tehlikeli bir sayısal görüntü üretme tekniği olarak kabul edilmektedir. Resim rötuşlama işlemi, orijinal görüntü üzerinde tamamen bir değişiklik yapılmamaktadır, ancak orijinal görüntünün belirli özellikleri geliştirilebilmekte veya azaltılabilmektedir. Bu yöntem,

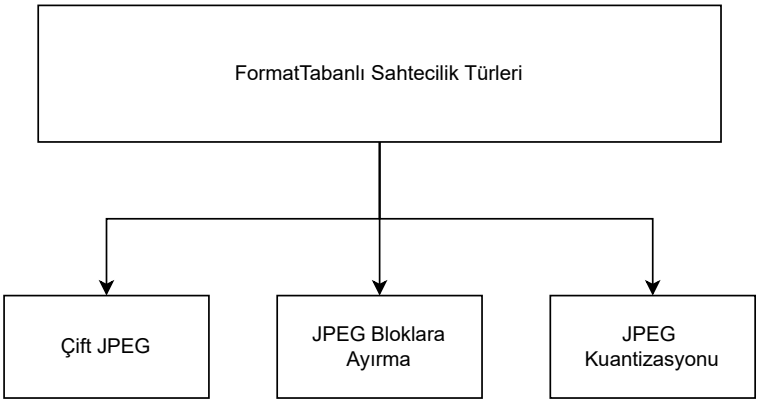
dergi ve gazeteler için resim editörleri tarafından sıklıkla kullanılmaktadır. Bu görüntü sahtekarlığı biçimi, bir görüntünün belirli özelliklerini vurgulamak ve onu daha ilginç hale getirmek için hemen hemen her dergi kapak sayfasında kullanılmaktadır.

- **Piksel Tabanlı Yöntemler:** Şekil 1.4.'te ki gibi, sahtecilik işlemi sırasında piksel düzeyinde ortaya çıkarılan istatistiksel anormallikleri tespit etmeye dayanmaktadır. Bu teknikler ayrıca, doğrudan uzamsal alanda veya bazı dönüştürülmüş bölgelerde belirli bir kurcalama biçiminden kaynaklanan piksel düzeyindeki korelasyonları da analiz etmektedir. Bu teknikler yaygın olarak kullanılmaktadır.



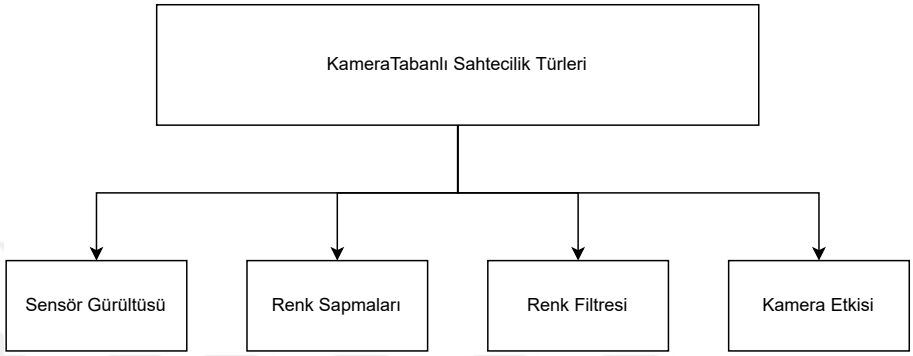
Şekil 1.4. Sayısal görüntü üzerinde piksel tabanlı sahtecilik tespiti yöntemleri.

- **Format Tabanlı Yöntemler:** Mevcut bir görüntünün sıkıştırma veya farklı amaçlarla değiştirilmesi, sahteciliğin tespit edilmesini son derece zorlaştırmaktadır. Örneğin, kaynak resim üzerinde JPEG kullanılarak sıkıştırılma işlemi gerçekleştirilmişse, fotoğraf üzerinde bilgi kaybı olabileceğinden dolayı sahteciliğin olup olmadığının tespiti zorlaşmaktadır. Şekil 1.5.'te format tabanlı yaklaşımlar gösterilmiştir.



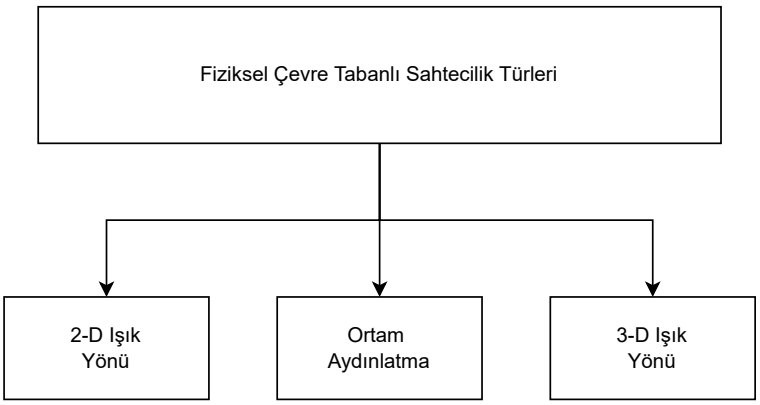
Şekil 1.5. Sayısal görüntü üzerinde format tabanlı sahtecilik tespiti yöntemleri.

- **Kamera Tabanlı Yöntemler:** Görüntü işlemi sırasında oluşturulan sentetik bilgiler kullanılarak, kurcalamayı tespit etmeyi amaçlamaktadır. Ek olarak, bir renk filtresi dizisi, renk sapması, kamera tepkisi ve sensör parazit kusurlarından elde edilen bilgiler kullanılarak, farklı kameralardan oluşan sentetik işlemler tahmin edilebilmektedir. Şekil 1.6.'da kamera tabanlı tespit yöntemleri gösterilmiştir.



Şekil 1.6. Sayısal görüntü üzerinde kamera tabanlı sahtecilik tespiti yöntemleri.

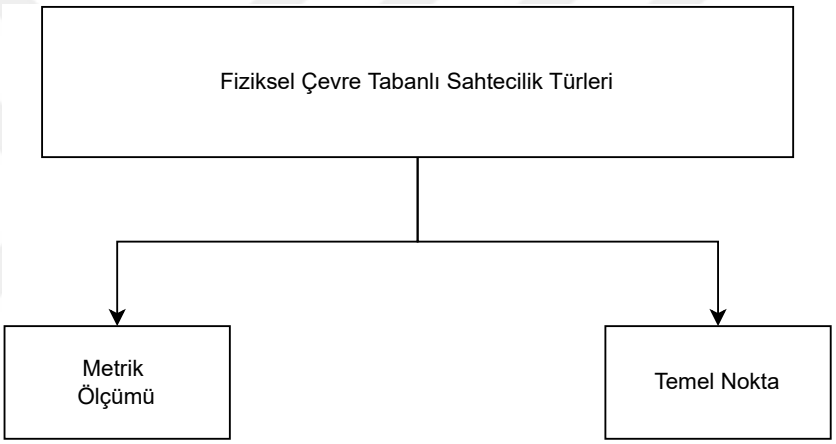
- **Fiziksel Çevre Tabanlı Yöntemler:** Doğal fotoğraflar genellikle farklı ışık koşulları altında çekileceği için çekilen her fotoğrafın parlaklık oranı birbirinden farklı olmak durumundadır. Bu nedenle, iki veya daha fazla resim, kurcalanmış bir görüntü oluşturmak için birleştirilirse, çekilen her farklı fotoğrafın parlaklık düzeyi her zaman değişecektir. Sonuç olarak, kurcalanmış resim üzerindeki manipülasyonu tespit etmek için resimdeki parlaklık düzeyindeki değişiklikleri belirlemek yeterli olacaktır. Şekil 1.7.'de fiziksel çevre tabanlı yaklaşımlar gösterilmiştir.



Şekil 1.7. Sayısal görüntü üzerinde fiziksel çevre tabanlı sahtecilik tespiti yöntemleri.

- **Geometrik Tabanlı Yöntemler:** Kamera merkezinin resim düzlemine izdüşümü olan nokta, gerçek görüntülerde görüntünün merkezine doğru yer almaktadır. Bir kişi

veya nesne kopyalanıp resmin içinde hareket ettirildiğinde (kopyala-yapıştır) veya iki veya daha fazla fotoğraf birleştirildiğinde (görüntü birleştirme), görüntünün merkez noktasını doğru bir perspektifte tutulmasını zorlaştırmaktadır. Böylece görüntünün merkez noktasındaki perspektif özellikleri kullanılarak, sağlam sahtecilik tespit sistemleri oluşturulabilir. Yukarıda özetlenen metodolojilerin tümü, sahteciliği tespit etme zorluğunun karmaşık olduğunu göstermektedir. Bir resme yapılan sahtecilik saldırısının türüne bağlı olarak, bazı tespit yaklaşımları yüksek bir performans sergileyebilirken, diğerleri düşük performans gösterebilmektedir. Şekil 1.8.'de Geometrik tabanlı yaklaşımlar gösterilmiştir.



Şekil 1.8. Sayısal görüntü üzerinde geometrik tabanlı sahtecilik tespiti yöntemleri.

Kopyala yapıştır sahteciliği, tek bir resim üzerinde bulunan bir bilgiyi değiştirmenin en popüler ve sıklıkla kullanılan yöntemlerinden biridir. Bu sahtecilik türünde, bilgi eklemek veya silmek için görüntünün bir kısmı yine aynı görüntü üzerindeki başka bir kısım ile kapatılmaktadır. Klonlama, kopyala-taşı saldırısı için başka bir terimdir. Aynı görüntünün bir bölümü kopyalanır ve aynı görüntünün başka bir bölümüne yapıştırılır. Kopyala-yapıştır saldırısının amacı, aynı görüntünün başka bir parçasını kullanarak orijinal görüntüdeki herhangi bir şeyi gizlemektir. Şekil 1.9. (a) ile verilen örnekte; bir devletin uzun menzilli füzelerinin tatbikatı esnasında çekilmiş gerçek bir görüntümüz mevcuttur. Fotoğraf da görüldüğü üzere 4 adet füze olmasına rağmen 3 adet füzenin ateşlendiği, diğer füzenin ise teknik bir arızadan kaynaklı olarak ateşlenmediği gözükmektedir. Şekil 1.9. (b) ile ateşlenmeyen füzeye, ateşlenen füzelerden bir tanesinin fırlatılmış halinin kopyalanıp yapıştırılması ile elde edilmiş sahte bir görüntü bulunmaktadır.

(a) (b)

Şekil 1.9. Kopyala yapıştır sahteciliği örneği.

Görüntü Birleştirme Sahteciliği, bir sahte görüntü üretme yöntemidir. Görüntü rötuşu tekniğinden çok daha tehlikeli ve etkilidir. Görüntü birleştirme tekniği Şekil 1.10.'da görüldüğü gibi, aynı kaynak görüntüden veya farklı kaynaklardan gelen bölgelerin kırpılıp istenilen bölgeye yapıştırılmasıyla gerçekleştirilmektedir. Sahte bir görüntü oluşturmak için görüntü ekleme tekniğinde iki veya daha fazla fotoğraf üzerinde istenilen bölgelerin kaynak görüntü üzerinden alınıp, hedef görüntü üzerine yapıştırılması ile elde edilmektedir. Yapılan birleştirme işleminden sonra kaynak ve hedef bölgeler arasındaki tutarsızlıkların etkisini azaltmak için yapıştırma işleminin gerçekleştirildiği bölgenin sınırlarına bulanıklaştırma işlemi uygulanmaktadır [15].

a) b)

Şekil 1.10. a) Odak dışı bulanıklığa sahip gerçek bir fotoğraf. (b), (a) verilen görüntünün, bulanıklaştırılmış bir parçasının eklenmesi ile oluşturulan sahte bir görüntü.

Kopyala-yapıştır sahteciliği, pasif temelli yaklaşımlar içerisinde kullanılan doğrulama teknolojilerinin tespit etmeye çalıştığı en yaygın resim sahteciliği tekniğidir. Literatürde Kopyala-yapıştır sahteciliğini tespit etmek için sayısal resimlerin istatistiksel özelliklerine dayalı çok sayıda yaklaşım sunulmuştur. Bu konudaki çalışmanın son yıllarda popülaritesinin artmasına rağmen, sunulan metodolojilerde kusurların olması konunun alaka düzeyini ve güçlü araştırma potansiyelini göstermektedir. Kopyala-yapıştır sahteciliği aynı görüntüde bulunan anlamlı bölgelerin veya bu bölgeler içerisinde bulunan nesnelerin sayısını artırmak ya da gizlemek amacıyla kullanılmaktadır. Şekil 1.11.'de görüntü üzerindeki bir nesnenin gizlenmesine örnek verilmiştir

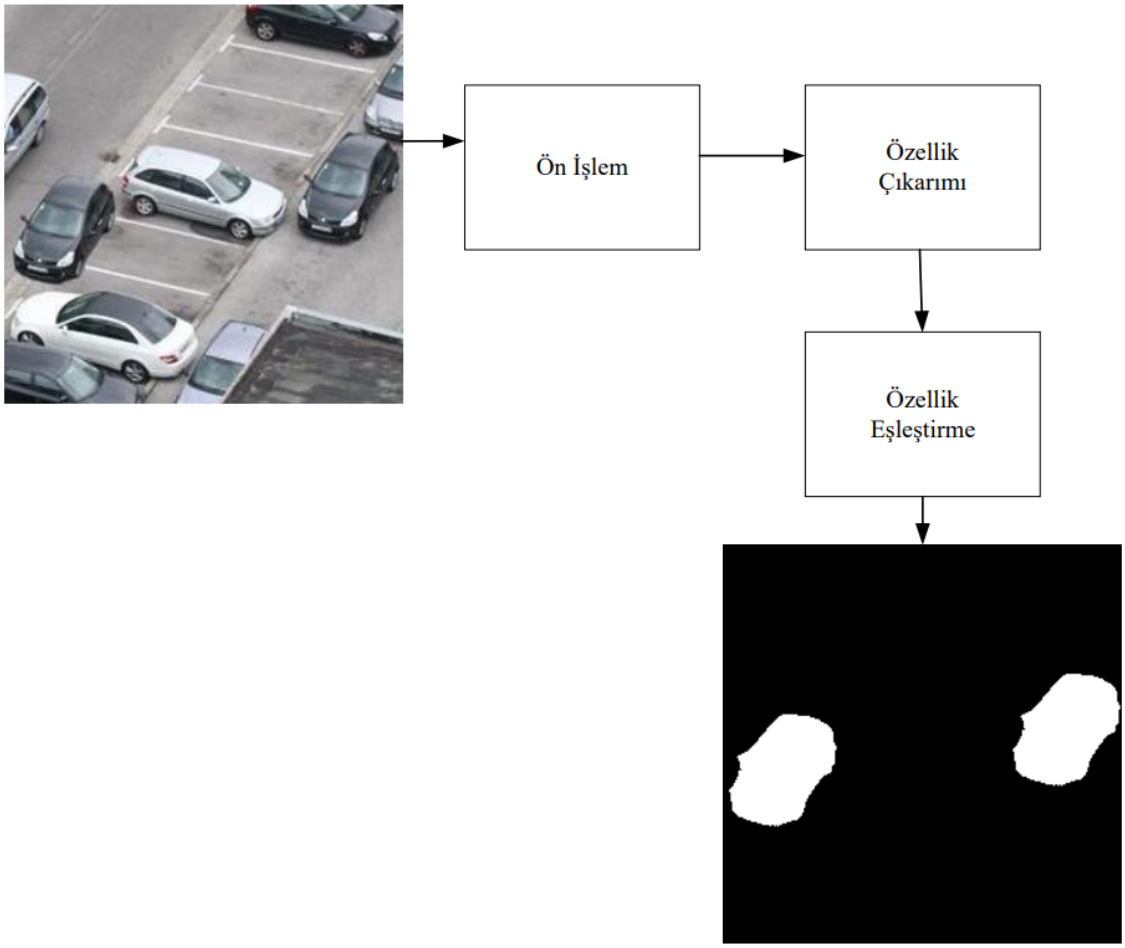
Şekil 1.11. Sayısal görüntü üzerinde kopyala yapıştır sahteciliği örneği.

Görüntü üzerindeki bir bilgiyi gizlemek veya çoğaltmak için yapılan kopyala yapıştır

işleminde, kaynak ve hedef bölgelerin aynı görüntü içerisinde olmasından dolayı parlaklık ve perspektif bilgileri, görüntünün geriye kalan bölgeleri ile benzer olacaktır. İşlem yapılan bölgeler içerisindeki yüksek benzerliklerden ötürü yapılan sahteciliği çıplak göz ile tespit edilebilmesi zordur. Buna ilaveten, yapılan kurcalama işlemlerinin görüntü üzerinde bıraktığı izleri gizlemek maksadıyla görüntü üzerinde birçok teknik uygulanabilmektedir. Bu yöntemler kaynak bölgenin hedef bölgeye yapıştırılmadan önce uygulanan geometrik dönüşüm saldırıları ve yapıştırıldıktan sonra uygulanan son işlem saldırıları olmak üzere kategorize edilmektedir. Geometrik dönüşüm saldırılarının 3 temel işlemi vardır. Bu işlemler aşağıda listelenmiştir.

1. **Ölçekleme:** Kaynak bölgeden alınan görüntü parçasının hedef bölgeye yapıştırılmadan önce boyutunun belirli bir ölçek oranında azaltılması veya artırılması işlemine denir.
2. **Döndürme:** Kaynak bölgeden alınan görüntü parçasının hedef bölgeye yapıştırılmadan önce Belirli bir açıda belirli bir yönde döndürülmesi işlemine denir.
3. **Öteleme:** Kaynak görüntünün belirli bir bilgiyi gizlemek veya görüntü içerisinde olan nesneleri artırmak için yapılan işlemine denir.

Bu işlemler kaynak görüntü parçasının hedef bölgeye taşınmadan önce tek bir sefer yapılabileceği gibi ayni yöntemler hibrit olarak tekrarlı bir şekilde de yapılabilmektedir. Son işlem saldırılarında ise kaynak bölgenin hedef bölgeye taşınma işlemi gerçekleştirildikten sonra oluşabilecek sahtecilik kalıntılarını yok etmek amacı ile uygulanabilecek saldırılar bütünü olarak isimlendirilmektedir. Bu işlemler, sahtecilik yapılan görüntünün genellikle tamamına uygulanmaktadır. Geometrik dönüşüm işlemi yapıldıktan sonra eldeki görüntüyü bulanıklaştırma, jpeg formatına çevirme ve gürültü ekleme gibi saldırı yöntemleri de son işlem saldırıları sınıfında değerlendirilmektedir [16].



Şekil 1.12. Kopyala-taşı sahteciliği tespit yöntemlerinin genel işlem adımları.

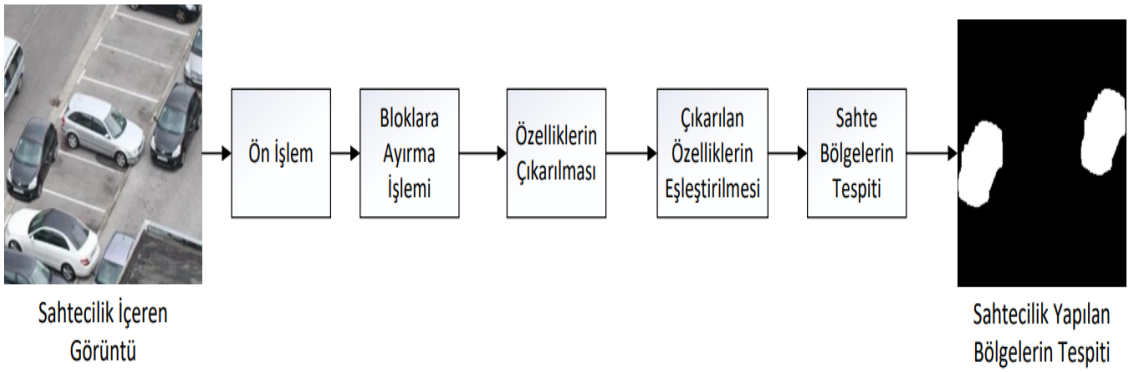
Şekil 1.12.'de kopyala-taşı sahteciliği tespiti alanında yapılan çalışmalarda kullanılan işlem adımlarının, genel olarak bir akış şablonu verilmiştir. Görüntü üzerinde yapılan sahteciliği tespit eden algoritmalar, çoğunlukla giriş görüntüsünün renk uzayını değiştiren bir ön işleme aşamasıyla başlar, ardından hileli alanları tanımlayan özellik çıkarma ve eşleştirme adımları uygulanarak sahtecilik yapılan görüntü parçasının tespiti işlemi gerçekleştirilir. Genel olarak bu ana işlemler bütününden oluşan kopyala-taşı sahteciliği metotları başlangıç olarak blok ve anahtar nokta tabanlı olmak üzere iki grupta kategorize edilirken, günümüzde bölüt ve derin öğrenme temelli yaklaşımlar da önerilmiştir. Hatta bu yöntemlerin hibrit şekilde uygulamaları da mevcuttur.

Blok temelli yöntemler, özellik eşleştirme ve çıkarma işleminden önce görüntü, sabit karesel veya süper piksel olacak şekilde bölünmektedir. Bölme işleminde kullanılan sabit şekle sahip görüntü parçacıklarına blok denilmektedir. Ön işlemde uygulanan

görüntüyü bloklara bölme işlemi, blokların üst üste örtüşen veya örtüşmeyen olacak şekilde iki türlü uygulanmaktadır. Anahtar nokta tabanlı yaklaşımlar, ön işlem olarak herhangi bir bloklara bölme işlemi gerçekleştirmeden, görüntü üzerinde elde edilen anahtar noktalar üzerinden işlem yaparak sahtecilik yapılan bölgeyi tespit etmektedir. Bölütleme temelli yaklaşımlar, sahtecilik yapılmış görüntüyü istenilen bir özelliğe göre mantıksal olarak bölütleme işlemi gerçekleştirdikten sonra, anahtar nokta temelli veya blok temelli yaklaşımlardan gelen bilgilerden yararlanarak sahtecilik yapılan bölgeyi tespit etmektedir. Son zamanlarda, görüntü sahteciliği tespit araştırmalarında derin sinir ağı (DNN) kullanılarak görüntü üzerinden özellik çıkartılıp, özelliklerin uçtan uca eğitilmiş bir ağ üzerinde mantıksal olarak sınıflandırılması ile sahtecilik tespiti gerçekleştirilmektedir [17]. Anahtar nokta temelli, bölütleme temelli, blok temelli ve derin sinir ağı temelli çalışmalar ilerleyen bölümlerde detaylı bir şekilde anlatılacaktır

1.2.2.1. Blok Temelli yaklaşımlar

Blok temelli yaklaşımlar da, ön işlem aşamasını geçen kurcalanmış görüntüyü mantıksal olarak kare veya süper piksel şeklinde yamalara ayırma işlemi gerçekleştirilmektedir. Yapılan bloklara ayırma işlemi sonucunda her bloğa özgü özellik vektörleri literatürde olan ayrık kosinüs dönüşümü veya ayrık dalgacık dönüşümü gibi birçok özellik çıkarma yöntemi ile çıkarılmaktadır [18]. Daha sonra çıkarılan özellik vektörleri, benzer blokları tespit etmek maksadıyla belirli bir eşik değeri üzerinden blokların eşleştirme işlemi gerçekleştirilmektedir. Aynı görüntü üzerinde yapılan bir sahtecilik olan kopyala yapıştır sahteciliğinde, bazı kurcalanmamış görüntü blokları da benzer özellik gösterebileceğinden dolayı, sahte olarak etiketlenebilmektedir. Yanlış tespit edilen bölgeleri temizlemek amacıyla bloklara ait olan konum bilgilerinden yararlanılarak, bir filtreleme işlemi yapılmaktadır. Bu filtreleme işleminde kopyalanan kaynak bölge ile yapıştırılan hedef bölge arasında belirli dönüşüm teknikleri veya vektörler ile kıyaslanan parçalar arasındaki ilişki belirlenerek, sahte olarak etiketlenen bölgenin doğrulama işlemi yapılmaktadır. Şekil 1.13.'te blok temelli yaklaşımların genel işlem adımları gösterilmiştir.



Şekil 1.13. Blok temelli kopyala taşı sahteciliği yaklaşımlarının genel işlem adımları.

Kopyala-taşı sahteciliğinin belirlenmesi için kullanılan blok temelli yaklaşımların genel işlem adımları aşağıdaki gibidir:

1. Adım :Girdi olarak alınan A $\times$ B $\times$ 3 boyutuna sahip sahtecilik gerçekleştirilmiş renkli görüntüyü 2 boyutlu gri seviyeye dönüştürme işlemi gerçekleştirilir. (Renk değerlerini kullanmayan yöntemler için geçerlidir)

2. Adım : Elimizdeki görüntüyü LxL bloklara bölme işlemi gerçekleştirilir. Sonuç olarak toplam blok sayısı N = (A-L+1) $\times$ (B-L+1) formülü ile hesaplanmaktadır.

3. Adım : Çıkarılan her bloğa ait özellik vektörü K olmak kaydıyla, özellik çıkarma yöntemi ile her blok dan 1 $\times$ K şeklinde fi özellik vektörü elde edilir. Daha sonraki işlemlerde bölgeleri tespit etmek amacı ile her bloğun (xi,yi) koordinat bilgisi de fi vektörünün içende tutulur. Vektörün son hali 1 $\times$ (K+2) şeklinde olmaktadır.

4. Adım : Daha sonra her bir bloğa özgü olan fi özellik vektörlerini içerisinde bulunduran N $\times$ (K+2) boyutun sahip F özellik matrisi oluşturulur.

5. Adım : Elde edilen F özellik matrisi içerisinde bulunan her satırı leksikografik olarak sıralama işlemi gerçekleştirilir. Bu sıralama işleminde fi özellik vektörü değerlerine göre birbirine yakın olanlar, sıralama sonucunda da birbirine yakın haline gelecektir. Daha sonra ortalama bir eşik değerine göre en yakın komşuları arasında eşleşen fi özellik vektörleri tespit edilir.

6. Adım : Belirli bir eşik değerinde göre benzer olan vektörler i $\neq$ j olmak kaydıyla fi ve fj olarak iki adet özellik vektörümüz olsun. Benzer bloklar arasında si kaydırma

vektörü hesaplanır. Benzer iki blok arası T1 eşik değerine göre mutlak uzaklığı temsil eden si <T1 olan blokların silinecektir.

7. Adım : Son işlem olarak da yanlış tespit edilen piksel bölgeleri morfolojik işlemler ile yok edilmektedir.

Kopyala yapıştır sahteciliği için Fridrich ve ark. tarafından önerilen yöntemde, girdi olarak alınan sahte görüntü, birbiri üstüne gelen bloklar olacak şekilde parçalara bölünür. Daha sonra elde edilen blokların kendine özgü öznitelik vektörleri çıkarımı işlemi, ayrık kosinüs dönüşümü ile gerçekleştirilir. Her bir blok parçasından alınan özelik vektörlerinden bir özellik matrisi çıkarılır. Daha sonra elde edilen özellik matrisimizin içindeki özellik vektörleri alfabetik olarak sıralama işlemi gerçekleştirilir. Sıralama işlemi sonucunda birbirine yakın değerlere sahip olan blok parçaları yan yana getirildikten sonra sahte bölgelerin tespiti işlemi gerçekleştirilir [19].

Sahtecilik tespiti için Popescu ve ark. Tarafından önerilen yöntemde, giriş görüntüsü üst üste gelmeyecek şekilde sabit boyutlu bloklara bölme işlemi gerçekleştirilir. Elde edilen bloklar üzerinde temel bileşen analizi uygulanarak her bloğun kendine özgü vektörleri çıkartılır. Daha sonra eldeki özellik vektörleri ile blokların ait olduğu konum bilgileri birleştirilerek bir özellik matrisi oluşturulur. Elde edilen özellik matrisi üzerinde alfabetik sıralama işlemi gerçekleştirilir. Benzer vektör değerlerine sahip olan bloklar birbirine yakın olacak şekilde sıralanmıştır. Birbirine yakın olan parçalar belirli bir benzerlik oranı üzerinden sahtecilik yapılan bölgenin tespiti gerçekleştirilir. Aynı zamanda bu yöntem görüntü sıkıştırma ve gürültü ekleme işlemi yapılan görüntüler üzerinde daha dayanaklı olduğu görülmüştür [20].

Huang ve ark. tarafından sunulan yöntemde, renkli giriş görüntüsünü boyutları eşit olacak şekilde bloklara bölünür. Bloklar üzerinde çıkarılan özellik vektörleri 7 parametreli olacak şekilde çıkartılır. Özellik vektörünün başlangıçtaki 3 parametresi, görüntü bloğuna ait olan renk bilgilerini içerir. Geriye kalan dört parametrede ise blok haline getirilmiş görüntü parçasını yatay, dikey ve çaprazlama olarak böldükten sonra elde edilen parçanın piksel değerleri toplamını, bloğun bölünmeden önceki piksel değerlerine oranlanır. Bu şeklide kurcalanmış bölgenin tespiti gerçekleştirilir. Yine bu yöntem de gürültü ekleme ve sıkıştırma saldırılarına karşı dayanıklıdır [13].

Kang ve ark. tarafından ortaya sunulan yöntemde, görüntü üzerinde sahtecilik yapılan bölgelerin tespit edilebilmesi için öncelikle görüntüyü sabit bir boyutta birbiriyle örtüşebilecek şekilde bloklara ayırma işlemi gerçekleştirilir. Bloklardan öznitelik vektörleri elde edebilmek ve resmin boyutunu azaltmak için tekil değişim ayrışımı yaklaşımı uygulanır. Daha sonra elde edilen özellik matrisinde her satırda bulunan özellik vektörleri üzerinde leksikografik olarak sıralama işlemi gerçekleştirilir. İşlem sonrasında birbirine yakın olan blokların vektör değerleri sıralanır ve benzer blokların tespiti için küçültülen bölgeler tekrar büyütülerek kurcalanmış bölgelerin tespiti gerçekleştirilir [21].

Kang ve ark. tarafından ortaya çıkarılan metot da, resim birbirine eş alt bloklara bölünür, daha sonra kopyalanan parçaları bulmak için tekil değer ayrışımı sonucu elde edilen vektörler, alfabetik olarak sıralanmış özellik matrisinde, benzerlik eşleştirmesi yapılır [22].

Huagn ve ark. tarafından yapılan çalışmada, görüntüyü bloklara ayırma işlemi gerçekleştirilmeden, görüntü üzerinde önce ayrık dalgacık dönüşümü uygulanır. İşlem sonrası ortaya çıkan düşük bantlı resmi, birbiri üstüne gelecek şekilde bloklara bölünür. Daha sonra görüntü bloklarına ait özellik vektörleri için ayrık kosinüs dönüşümü ve kuantizasyon ayrışımı yaklaşımı uygulanmaktadır. Elde edilen özellikler bir matris şeklide oluşturulur ve leksikografik olarak sıralanır. Eşleşen benzer bloklarla belli bir eşik değerince kıyaslama işlemi yapılarak kurcalanmış blok parçası tespit edilir [18].

Muhammad ve ark. tarafından yapılan çalışmada, ayrık kosinüs dönüşümü tabanlı yeni bir yaklaşım öne sürülmüştür. Girdi olarak alınan kurcalanmış görüntü, birbiri üzerinde gelecek şekilde eş bloklara ayrılır. Daha sonra her bloğa ait olan özellik vektörleri, ayrık kosinüs dönüşümü gerçekleştirilerek elde edilir. Yalnız özellik çıkarma işlemi gerçekleştirilirken, özellik vektörlerine zigzag teoremi uygulanmıştır. Sonra özellik matrisi leksikografik olarak sıralanır ve benzer bölgeler eşleştirilir. Benzer bloklara ait olan kaydırma vektörü ile kurcalanmış bölgeler tespit edilir [23].

Xingming ve ark. tarafından önerilen yöntemde, kurcalama yapılmış görüntü işleme alınır. Daha sonra kurcalanmış görüntü bloklara bölünür ve her bloğa ait olan renk bilgileri dahil olmak üzere on parametreli özellik vektörleri, özellik matrisi içerisinde tutulur. Özellik değerlerimiz, YUV renk uzayına gönderilen kurcalanmış resimden

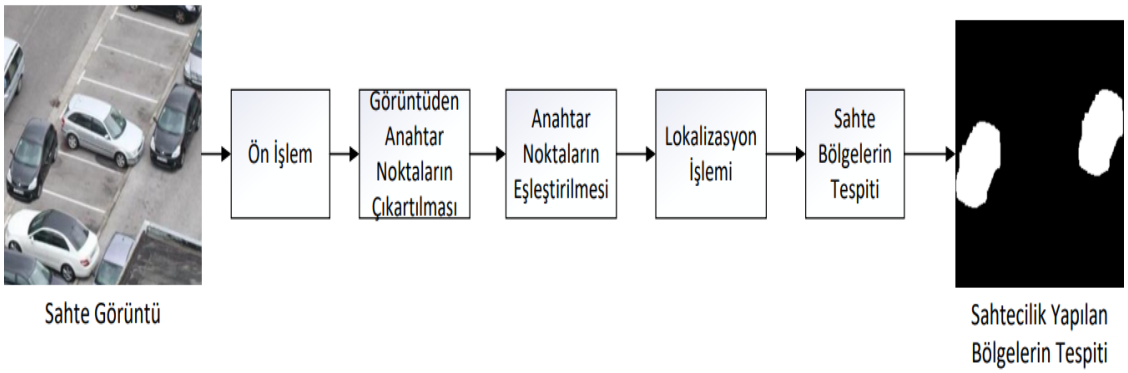
elde edilmiş olan Y değerimizi; geriye kalan kırmızı, mavi ve yeşil gibi dokuz adet parametremizin her biri için, gri düzeydeki ortalamasını ve moment değerlerinin hesaplanması ile elde edilmektedir. Daha sonra özellik matrisi leksikografik şekilde sıralanır ve sıralanmış vektörler belirli bir eşik değerine göre kıyaslanarak kurcalanmış bölgenin tespiti gerçekleştirilir [24].

Kaur tarafından önerilen metot da, kurcalanmış görüntü gri seviyeye dönüştürülür. Daha sonra birbiri üstüne örtecek şekilde eş blok parçalarına bölünür. Mevcut olan her blok parçası yerel ikili örüntü yöntemiyle özellik çıkarımı gerçekleştirilir. Elde edilen vektörlerin toplanmış olduğu özellik matrisi leksikografik sıralamaya tabi tutulur. Birbirine benzer olan blok parçaları öklid yöntemi ile tespit edilmektedir [25].

Desai ve ark tarafından önerilen yaklaşımda, kurcalanmış görüntü gri seviye haline getirilir. İşlem gören resim, birbiri üstüne gelecek şekilde bloklara bölünür. Daha sonra her blok için özellik vektörü ayrık kosinüs dönüşümü ile gerçekleştirilir. Elde edilen özellik vektörleri, iki katsayılı ayrık kosinüs dönüşümü yapılarak, leksikografik sıralama işlemi gerçekleştirilir. Sıralama aşamasında yanlış tespit edilen bölgeler morfolojik işlemler ile filtrelenerek yok edilir. Bu yaklaşım sıkıştırma, bulanıklaştırma ve döndürme ataklarına karşı dayanaklıdır [26].

1.2.2.2. Anahtar Nokta Temelli Yaklaşımlar

Kopyala-taşı sahteciliği tespitinde yaygın olarak kullanılan blok temelli yaklaşımların, geometrik dönüşüm saldırıları gibi sahtecilik operasyonlarına karşı güçsüz oluşu ve yüksek boyutlu görüntülerde özellik çıkarma ve eşleştirme aşamasında uzun zaman alması gibi dezavantajlarından dolayı, anahtar nokta tabanlı yaklaşımlar daha popüler hale gelmiştir. Anahtar noktası tabanlı yaklaşımlarda, kurcalanmış görüntünün tamamından sabit anahtar noktalar çıkartılarak, kopyalanan kaynak bölge ve taşınan hedef bölge tespit edilmeye çalışılmaktadır. Şekil 1.14.'te anahtar nokta tabanlı yaklaşımların genel işlem adımları gösterilmiştir.



Şekil 1.14. Kopyala-taşı sahteciliği anahtar nokta tabanlı tespiti genel işlem adımları.

Ön işlem aşaması olarak işleme alınmış kurcalanmış fotoğrafın renk bilgisi değişimi veya doku bilgilerinin çıkartılması gibi işlemler gerçekleştirilmektedir. Daha sonra görüntünün tamamı üzerinden anahtar noktalar ve anahtar noktalara ait olan vektörlerin çıkarılma işlemi yapılmaktadır. Görüntü üzerinde kurcalanmış bölgelerin tespiti için elde edilmiş olan anahtar noktalarının belirli bir eşik değerine göre kıyaslama işlemi gerçekleştirilmektedir. Daha sonra eşleşen noktaların ait oldukları bölgelerde sahtecilik yapılan bölgenin tam konumunun işaretlenmesi için lokalizasyon işlemi de yapılmaktadır. Genel olarak çalışmalar, görüntüde sahtecilik olup olmadığının tespiti veya sahtecilik olan bölgelerde kaynak ve hedef bölgelerin belirlenmesi olarak yapılmaktadır. Kopyala-taşı sahteciliğinde kullanılan anahtar nokta tabanlı yaklaşımların genel işlem sırası aşağıdaki gibidir.

1. Adım :Kurcanlanmış sahte resime ön işlem uygulanır.
2. Adım : İşleme alınan kurcalanmış reisimin tamamından kilit noktalar ve kilit noktalara ait olan özellik vektörlerinin (fi) çıkartılması
3. Adım : Tespit edilen kilit noktaların, sahtecilik yapılan bölgenin tespitinin yapılabilmesi için koordinat bilgileri fi vektörüne eklenir. Koordinatlar x ve y ekseni üzerinde olduğu için vektörümüze 2 adet bilgi daha ekleme işlemi gerçekleştirilmiştir.
4. Adım : Tespit edilen bütün kilit noktalara ait özellik vektörlerini içerisinde bulunduran özellik matrisi oluşturulur.

5. Adım : Bütün kilit noktaların mutlak uzaklıkları tespit edilerek birbirine en yakın olan kilit noktaların kıyaslama işlemi yapılır.

6. Adım : Kıyaslama işleminde yanlış çıkartılan kilit noktaların belirli bir eşik değerine göre işlem yapılarak sahteciliğin olmadığı bölgeler temizlenmiş olur.

7. Adım : Elimizdeki resimde yeteri kadar kilit noktanın olması durumunda fotoğrafın sahte mi yoksa kurcalanmış mı olduğuna karar verilir.

8. Adım : Kilit noktalara ait konum bilgileri ile kurcalanmış bölgenin sınırları çizilerek lokalize edilme işlemi gerçekleştirilir.

Zhang ve ark. tarafından önerilen yöntemde, kurcalanmış bölgenin tespiti için ilk defa SIFT adlı bir algoritma yöntemi ortaya çıkarıldı. Ölçek Bağımsız Özellik Dönüşümü olan SIFT girdi olarak alınan sahte görüntüden kilit noktalar çıkartma işlemini gerçekleştirmektedir. Daha sonra çıkarılan kilit noktaların kıyaslama işlemi yapılmaktadır. Kullanılan yöntemin döndürme, ölçekleme, sıkıştırma ve gürültü ekleme gibi saldırılara karşı dayanıklıdır [27].

Pan ve ark. tarafından önerilen yöntemde, yeni bir SIFT temelli yaklaşım ortaya koymuşlardır. Önerilen yeni yöntemde SIFT ile çıkarılan kilit noktalardan elde edilen vektörlerin birbiri arasında en yakın olanları tespit etmek için BBF algoritmasını kullanmışlardır. Vektörlerden çıkartılan korelasyon haritası ile kopyalanmış kaynak bölge ile taşınma işlemi gerçekleştirilmiş bölgenin koordinatları tespit edilebilmeyi mümkün kılmaktadır. Eşleşen bölgeler arasında hatalı olanları yok edebilmek için uzaysal dönüşüm bilgileri kullanılmaktadır. Bu yöntemde ortaya sadece eşleşen noktalar belirtilmiyor, aynı zamanda eşleşen benzer noktaların bölgeleri de tespit edilmektedir. Kullanılan yöntemin ölçekleme ve sıkıştırma gibi saldırılara karşı da dayanıklı olduğu ortaya konmuştur [28].

Pan ve ark. tarafından önerilen yeni yöntemde, bir önceki çalışmaları gibi SIFT ile kilit noktaların tespit işlemi yapıldıktan sonra elde edilen öznitelik vektörlerini BBF algoritması yardımıyla kurcalama olabilecek şüpheli bölgelerin tespiti yapılıyordu. Yanlış tespit edilen bölgeleri yok etmek için RANSAC algoritması uygulanmıştır. Kurcalama yapılmış bölge çiftlerinin koordinatlarının tespiti için korelasyon haritası çıkarılmıştır.

Birçok saldırı karşısında bile doğru kopyala-taşı sahteciliği tespiti yapabildiği, deneysel olarak ispatlanmıştır [29].

Amerini ve ark. tarafından sunulan yöntemde, SIFT tarafından elde edilen kilit noktaları hiyerarşik bir şeklide sıralama işlemi yapılmıştır. Yapılan çalışma da yanlış tespit edilmiş bölgelerin elemine işlemi RANSAC algoritması ile gerçekleştirilmiştir. Sonuç olarak bu çalışmanın sıkıştırma ve gürültü ekleme gibi saldırılara karşı dayanıklı olduğu deneysel olarak ispat edilmiştir [30].

Jaberi ve ark. tarafından sunulan yöntemde, ayna yansıması durumuna karşı daha sağlam tespitler yapılabilmesi için, MIFT temelli bir yaklaşım gerçekleştirilmiştir. Önerilen yöntemde ilk olarak kilit noktalar çıkarılmaktadır. Daha sonra Kilit noktalara ait afin dönüşümleri tahmin edilerek kurcalanmış bölgenin tespiti gerçekleştirilmektedir. Hatalı tespit gerçekleştirilen bölgeleri yok etmek için RANSAC algoritması kullanılmıştır. Bu yöntemin dönme ve dönme benzeri ataklar karşısında dayanıklı olduğu gösterilmiştir [31].

Kiruthika ve ark. tarafından önerilen yöntemde, kurcalanmış görüntüyü tespit etmek için SURF temelli bir yaklaşım önerilmiştir. Önerilen yöntem de, ön işlem olarak görüntü gri düzeye çevrilmektedir. Daha sonra SURF yöntemi ile görüntünün tamamından kilit noktalar ve her kilit noktaya ait öznitelik vektörleri çıkarılmaktadır. Benzer kilit noktaları tespit etmek için 2NN algoritması uygulanmıştır. Hiyerarşik bir yaklaşımla yanlış tespit edilen kilit noktaların elemine edilme işlemi gerçekleştirilmiştir [32].

Zhu ve ark. tarafından sunulan yöntemde, kurcalanmış görüntüleri tespit edebilmek için ORB temelli bir yaklaşım tercih edilmiştir. Yazarlar ORB algoritmasını dönme ataklarına karşı dayanıklı olduğu için kullanmışlardır. Uygulama ortamı olarak ölçek den bağımsız bir gauss uzayı tercih edilmiştir. Önerilen yöntemin deneysel olarak SIFT ve SURF yaklaşımlarına göre daha iyi sonuç verdiği ispat edilmiştir. Ayrıca ORB algoritması döndürme ve sıkıştırma gibi ataklara karşı daha dayanıklı olduğu da gösterilmiştir [33].

Wenchang ve ark. tarafından sunulan yöntemde, SIFT tabanlı yeni bir yaklaşım öne sürülmüştür. Bu yöntemde SIFT ile parçacık sürü (PSO) algoritması kullanılmıştır. Önerilen yöntemde, SIFT tarafından çıkarılan anahtar nokta sayısının yetersiz olma durumunda başarılı bir sahtecilik tespiti yapamayacağı deneysel olarak gözlemlenmiştir.

Bu yöntemde genel olarak SIFT tabanlı yaklaşımlardaki işlem adımları uygulanmaktadır. Giriş görüntüsünden kilit noktalar çıkarıldıktan sonra otomatik bir şekilde parametre değerleri üretilmektedir. Yanlış tespit edilen bölgelerin yok edilmesi için RANSAC yöntemi uygulanmıştır. Uygulanan yöntemin döndürme ve sıkıştırma gibi saldırılar karşı güçlü olduğu vurgulanmıştır [34].

1.2.2.3. Bölütleme Tabanlı Yaklaşımlar

Kopyala-taşı sahteciliği tespiti noktasında genel olarak anahtar nokta tabanlı, blok tabanlı ve her ikisinin hibrit bir halde uygulanması ile sahtecilik tespiti gerçekleştirilmektedir. Bu sahada çalışmaların artmasıyla sahtecilik yapılan bölgenin tespitinde görüntü bölütleme tabanlı yaklaşımlarda ortaya çıkarılmıştır. Bu bölümde kopyala yapıştır sahteciliğinde kullanılan bölütleme tabanlı yaklaşımlar incelenecektir. Li ve ark tarafından bölütleme temelli ilk kopyala-taşı sahteciliği tespiti yöntemi önerilmektedir. Girdi olarak alınan kurcalanmış görüntü üzerinde mantıksal olarak bölütleme işlemi gerçekleştirilir. Bölütleme işlemin de birbiri üstüne örtüşmeyen anlamlı bölütler oluşturmak için SLIC algoritması kullanılmıştır. Daha sonra görüntü üzerinden çıkarılan kilit noktalar ve onlara ait olan öznitelik vektörleri eşleştirme işlemi gerçekleştirilir. Daha sonra bölüt parçalarının eşleştirilmesi ile sahtecilik yapılan bölge tespit edilmiş olur [35].

Pun ve ark tarafından kopyala taşı görüntü sahteciliği alanında yeni bir yaklaşım ortaya konmuştur. Giriş olarak sisteme verilen sahte görüntünün bölütleme işlemini gerçekleştirebilmek için SLIC algoritmasından faydalanılmıştır. İki aşamalı olarak görüntü üzerinde bölütleme işlemi gerçekleştirilir. Birinci kısımda bölütleme işlemi gerçekleştirilirken, her bölüt parçasının boyutu aynı olacak şekilde ayarlanmıştır. Birinci aşamadan elde edilen bölüt parçalarına ayrık dalgacık dönüşümü uygulanarak her bölüt parçası için frekans değerleri çıkartılır. Daha sonra eldeki frekans değerlerine göre bölüt parçalarının boyutları tekrardan ayarlanır ve böylece optimum şekilde bölüt boyutları belirlemesi gerçekleştirilmiştir. Daha sonra optimum şekilde hazırlanmış olan bölüt parçalarını, SIFT yöntemi ile kilit noktaların belirlenmesi ve kilit noktalara ait olan öznitelik vektörlerinin oluşturulması işlemi gerçekleştirilmiştir. Elimizdeki bölüt parçalarının vektörel özelliklerine göre korelasyon haritası çıkartılarak sahtecilik yapılmış bölgelerin tespiti gerçekleştirilir. Yanlış tespit edilen bölüt parçaları ise morfolojik ve

yüzey bilgilerinden yararlanılarak elemine edilmiştir. Önerilen yöntemin sıkıştırma ve gürültü ekleme gibi saldırılara karşı dayanıklı olduğu deneysel olarak ispat edilmiştir [36].

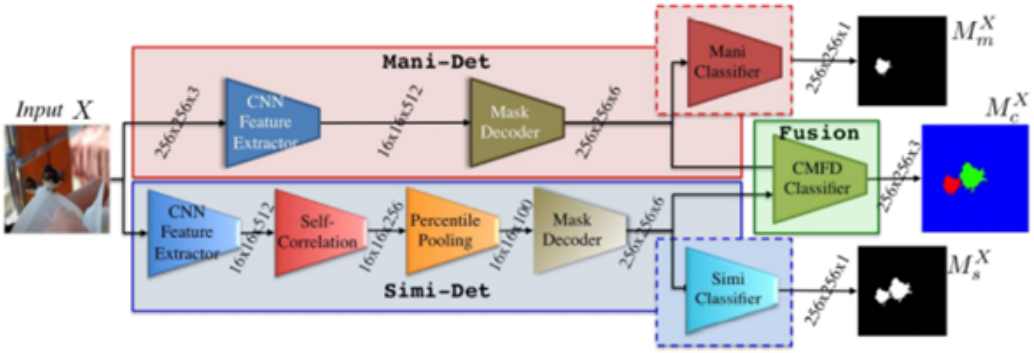
Li ve ark tarafından sunulana yaklaşımda, kilit noktala çıkarımı gerçekleştirilmeden önce SLIC algoritmasından faydalanılarak birbiri üstüne gelmeyen bölüt parçalarına ayrılmaktadır. Giriş olarak alınan görüntünün tamamından, SIFT algoritması yardımıyla çıkartılan kilit noktaların benzer olanlarının bulunduğu bölüt parçalarının kıyaslama işlemi gerçekleştirilir. Kıyaslama sonucu benzer olan bölüt parçaları arasında dönüşüm matrisi tahmini gerçekleştirilir. Dönüşümün gerçekleştirilemediği durumda klasik blok temelli yaklaşımlarda uygulanan işlemler adımları uygulanmaktadır. Yapılan çalışmanın döndürme, gürültü ekleme ve sıkıştırma gibi ataklara karşı güçlü olduğu ispat edilmiştir [37].

Zandi ve ark tarafından önerilen yaklaşımda görüntü üzerinde hatalı olarak tespit edilen bölütlerin elemine edilmesi için bir eşik değeri ortaya konmuştur. Öncelikle resim üzerinden kilit noktaların çıkarma işlemi gerçekleştirilir ve onların benzer olanları tespit edilir. Daha sonra mevcut görüntümüz SLIC algoritması yardımıyla bölütlere ayrılır. Elde edilen bölütlerin kıyaslama işlemi gerçekleştirilir. Benzer bölütler üzerinden minimum üç adet benzer kilit noktaya sahip olamayan bölüt parçalarının yok edilme işlemi gerçekleştirilir [38].

Wang ve ark tarafından sunulan yaklaşımda, bir süper piksel yöntemi olan MBS algoritması ile birbiri üzerine gelmeyen bölüt parçaları oluşturulur. Çıkarılan her bölüt parçasının entropi bilgisi alınır ve ona göre doku bilgisine sahip olan veya olmayan olarak sınıflandırma işlemi gerçekleştirilir. Bu sınıflandırma sonucunda elimizde iki adet sınıf bulunmaktadır. Daha sonra bu bölüt parçalarına ait olan kilit noktalar SURF algoritması yardımıyla elde edilmektedir. Doku bilgisi olmayan bölüt parçalarından daha çok kilit nokta çıkartabilmek için kontrast değeri düşürülmüştür. Öznitelik vektörleri ise PCET yöntemiyle elde edilmiştir. Hatalı olarak tespit edilen bölüt parçalarının elemine işlemi RANSAC yardımıyla çözülmüştür. Tespit edilen kilit noktaların çevresinin sınırları dikdörtgen bir çerçeve içine alınır. Elde edilen çerçeve birbiri üstüne çakışan kare bloklara ayrılır. Her bloğa ait olan öznitelik vektörleri PCET yardımı ile elde edilir [39].

1.2.2.4. Derin Öğrenme Tabanlı Yaklaşımlar

Wu vd. tarafından önerilen BusterNet olarak adlandırılan modelle kopyala taşı sahteciliği tespiti, uçtan uca eğitilebilir bir derin sinir ağı ile gerçekleştirilmiştir. BusterNet modeli iki dallı bir yapıdadır. Birinci dalda görüntü bölütleme ağı gibi düşünülebilir. İlk dalda sahte bölgeleri bölütleyerek maske üreten bir yapı vardır. ˙İkinci dalda ise CNN özellik vektörleri arasında self korelasyon hesaplaması yaparak benzerlik skoru üreten bir yapı mevcuttur. Bu iki dalın çıkışları birleştirilerek bozulmamış, kopyalanmış kaynak ve hedef bölgeler tespit edilmektedir. Şekil 1.15.'te ilgili model verilmiştir [40].



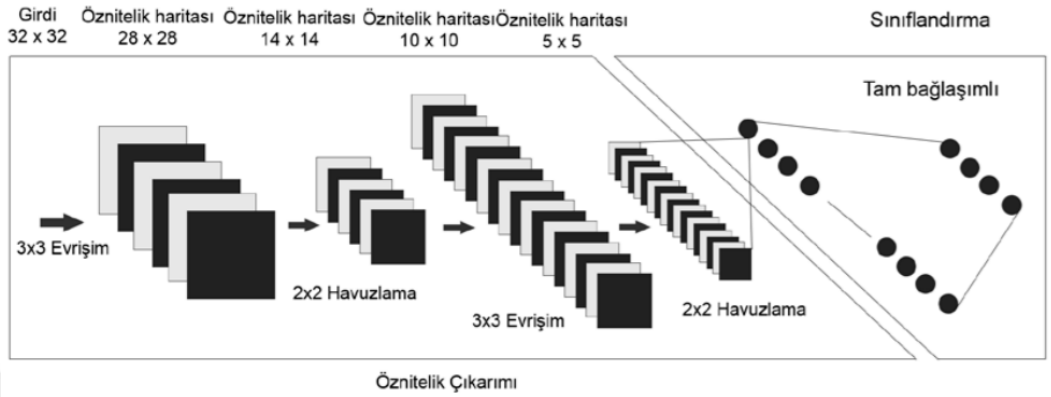
Şekil 1.15. BusterNet genel işlem adımları[41].

Mohamed A. ve arkadaşlaerı tarafından önerilen model, LTSM (CovLSTM) ağlarına ek olarak Evrişimli sinir ağı (CNN) uygulamasına dayanmaktadır. Bu yöntem, görüntü özelliklerini bir dizi Evrişim (CNV) katmanı, ConvLSTM katmanı ve havuzlama katmanları ile çıkarır, ardından özellikleri eşleştirir ve kopya taşıma sahtekarlığını tespit eder [41].

1.3. Evrişimli Sinir Agları

Evrişimli sinir ağları, en az bir evrişimsel işlem katmanı içeren sinir ağlarıdır. Evrişimli sinir ağları, çok boyutlu veri işleme için optimize edilmiştir. Örnek verecek olursak, iki boyutlu matrislerden oluşan renkli resimleri, iki boyutlu verilerde depolanan dil işleme verilerini ve üç boyutlu filmleri hacimsel görüntüleri içerir. Yerel bağlantılar, paylaşılan ağırlıklar, birleştirme ve birkaç katmanın kullanımı, gerçek sinyallerin niteliklerini kullanan evrişimli sinir ağlarının dört kritik öğesidir. Genel olarak, evrişimli sinir ağları

beş farklı yapıdan oluşmaktadır: bir giriş katmanı, bir evrişim katmanı, bir ortak katman, bir tam bağlantılı katman ve bir çıkış katmanı. Şekil 1.16.'da, bir evrişimli sinir ağı mimarisi gösterilmektedir.



Şekil 1.16. Evrişimli sinir ağı modeli.

Şekil 1.16'da gösterilen modelde kullanılan evrişim katmanı üç adet bileşenden oluşmaktadır. İlk olarak girdi olarak alınan veriye evrişim işlemi gerçekleştirilmektedir. İkinci adıma geçildiğinde lineer olmayan bir aktifleştirme fonksiyonu katmana gelen veri üzerinde gerçekleştirilmektedir. Sonuncu adımda ise ortaklama işlemi gerçekleştirilir. Daha sonra gelen veri çıkış katmanına gönderilmektedir [42].

Evrişim katmanı, gelen veriyi ele alan ilk katmandır. Orijinal resim boyutundan daha küçük bir filtre, evrişim katmanındaki görüntünün üzerine gelerek, bu görüntülerden belirli öznitelikleri toplamaya çalışmaktadır. Tek boyutlu veriler için ayrık evrişimin çalışması Denklem 1.1 tarafından sağlanmaktadır. Denklem içerisinde * ile gösterilen işlem evrişim işlemidir [43].

$$s(t) = x(t) * w(t) = \sum_{-\infty}^{\infty} x(a)w(t-a) \tag{1.1}$$

Burada w ifadesi filtreyi (çekirdek), x giris görüntüsünü, s sonuç olarak elde edilen özellik haritasını ve t zaman bilgisini gösterir. Evrişim, resim bilgileri gibi iki boyutlu verilere kullanılan evrişim işleminin matematiksel ifadesi Denklem 1.2.'de ifade edilmiştir.

$$s(i,j) = x(i.j) * w(i,j) = \sum_{m} \sum_{n} x(i,j)w(i-m, j-n) \tag{1.2}$$

Denklem 1.2.'de ki i ve j parametreleri, evrişimli matrisin ait olduğu konumunu belirtir. Şekil, iki boyutlu bir giriş görüntüsüne uygulanan evrişim işlemini göstermektedir. S özellik haritası, x giriş matrisine w filtresi uygulanması sonucu oluşur. 3×4 matris büyüklüğüne sahip olan x girişine w filtreleme işlemi gerçekleştirildiğinde 2×3 büyüklüğünde bir s sonucu üretilir. Bir özellik haritası, elde edilen s sonuçlarının her hücreye yazıldıktan sonra, tüm hücrelerin toplanması sonucu elde edilir. Yapılan çalışmanın türüne göre işlem parametlerinden biri olan aktivasyon fonksiyonunun doğru belirlenmesi gerekmektedir. Literatür de en çok kullanıldığı bilinen aktivasyon fonksiyonları Sigmoid ve ReLU'dür.

Son aşama olarak uygulanan ortaklama işlemi, giriş görüntüsü üzerinde belirli bir boyutta matris gezdirilir ve geçtiği her konumdaki görüntü parçasından bir örnek alarak işlem gerçekleştirmektedir. Giriş matrisini M $\times$ N olarak düşünürsek ve gezen matrisimiz K $\times$ L olursa, çıkış boyutu (M-K) $\times$ (N-L) boyutuna indirgenmektedir. Bu şekilde bir indirgeme işlemi gerçekleştirmesi sayesinde hazırlanan ağ modelinin hesaplama maliyetini düşürmektedir. Bundan dolayı evrişimli sinir ağları için çok büyük bir önem taşımaktadır.

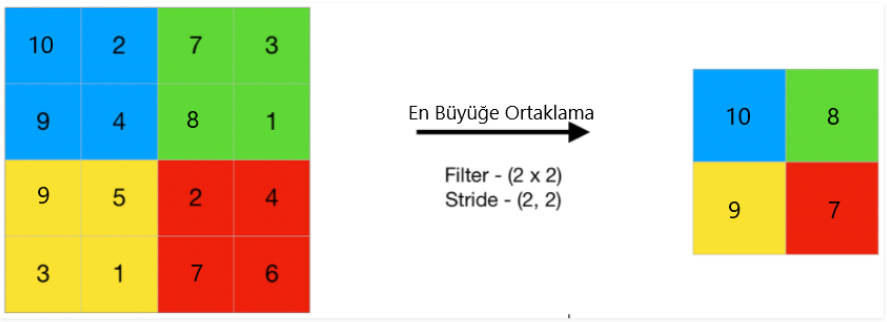
1.3.1. Evrişimli Sinir Ağlarının Temel Bileşenleri

Evrişimli sinir ağları evrişim katmanı, ortaklama katmanı, aktifleştirme fonksiyonları, tam bağlı katman, kayıp katman, yığın normalizasyon katmanı ve birleştirme katmanı olmak üzere 7 temel yapıdan oluşmaktadır. Bu yapılar aşağıda detaylı bir şekilde anlatılmaktadır. Evrişim katmanının birincil işlevi, gerekli özellikleri çıkarmak için seçilen filtreyi giriş matrisine evrişimli olarak uygulamaktır. Evrişim katmanı için kritik parametreler filtre genişliği, filtre sayısı, adım ve ped boyutu olmak üzere dört temel parametresi vardır. Filtre genişliği değeri, giriş matrisi boyunca hareket eden filtre öğesinin hangi boyut ve genişlikte olacağını belirtmektedir. Filtre sayısı değiştirildiğinde, özellik haritasındaki özellik sayısı da aynı şekilde değişmektedir. Adım aralığı, filtre öğesinin giriş matrisini geçtiği aralıkları belirtir. Doldurma boyutu, çıktı boyutunu klasik hale getirmek ve çeşitli şekillerde geri beslemek için kullanılan parametredir.

Havuzlama katmanı (POOL), bir miktar uzamsal değişkenliği olan bir evrişim katmanıyla

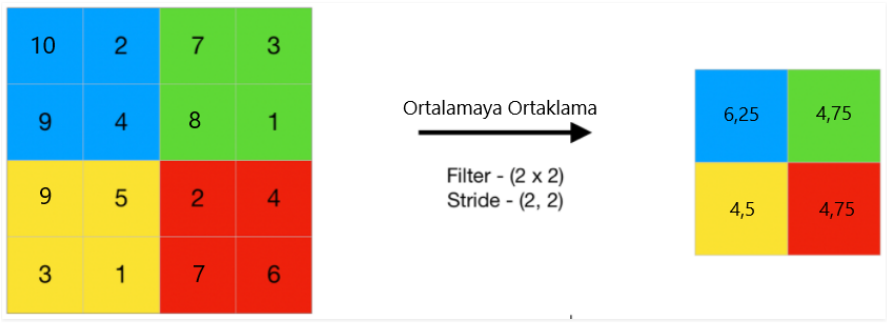
birlikte sıklıkla kullanılan bir örnekleme prosedürüdür. Örneğin, maksimum ve ortalama birleştirme, maksimum ve ortalama değerlerin elde edildiği benzersiz ortaklama türleridir. Ortaklama katmanı genel olarak işlem maliyetini azaltmak için kullanılmaktadır. En fazla kullanılan iki tane ortaklama yöntemi vardır. Aşağı kısımda onlardan bahsedilecektir.

- **En Büyüğe Ortaklama(Max Pooling):** Giriş olarak alınan matriste ortaklama işlemini gerçekleştiren gezen matrisimizin boyutları içerisin de en büyük elemanı çıkışa vermektedir. Girdi olarak alınan bir 4×4 matrise 2×2 en büyüğe ortaklama işleminin gerçekleşmesi Şekil 1.17.'de verilmiştir.



Şekil 1.17. En büyüğe ortaklama işlemi.

- **Ortalama Değere Ortaklama(Pooling):** Giriş olarak alınan matriste ortaklama işlemini gerçekleştiren gezen matrisimizin boyutları içerisin de bulunan elemanların ortalama değerini çıkışa vermektedir. Girdi olarak alınan bir 4×4 matrise 2×2 en ortalama değere ortaklama işleminin gerçekleşmesi Şekil 1.18.'de verilmiştir.



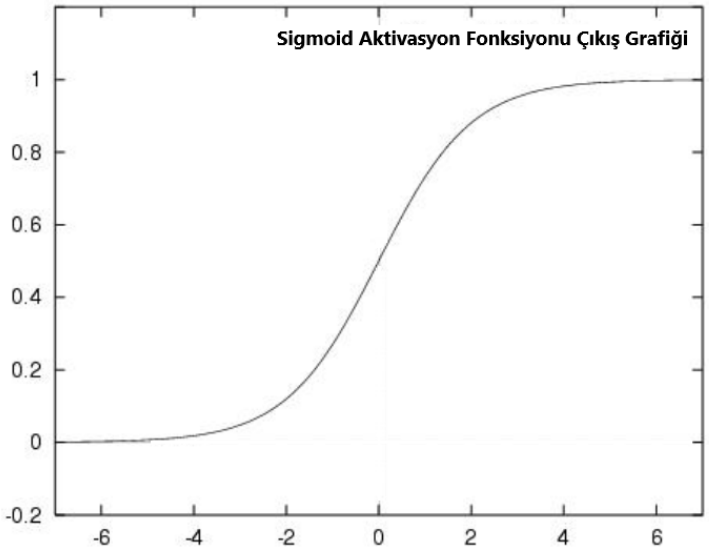
Şekil 1.18. Ortalamaya ortaklama işlemi.

Aktivasyon fonksiyonları, giriş olarak alınan verinin her katmanda işlem gördükten sonra çıkan sonucu, işlem göreceği diğer katmana giriş olarak veren işlem olarak ifade edilmektedir. İşleme alınan verilerin özelliklerine göre uygun aktivasyon fonksiyonu belirlemek, kullanılan ağ için önem arz etmektedir. ReLU ve Sigmoid olarak adlandırılan iki adet yaygın kullanıma sahip aktivasyon fonksiyonu bulunmaktadır.

- **Sigmoid Aktivasyon Fonksiyonu:** Sigmoid işlevi, 0 ile 1 arasındaki sayıları çeviren, sürekli ve türevlenebilir bir matematiksel işlevdir. Kendine özgü "S" şeklinde bir eğriye sahiptir. Sigmoid fonksiyonu, genellikle lojistik fonksiyon veya sigmoidal eğri olarak adlandırılmaktadır. Çok yaygın olarak kullanılan ve doğrusal olmayan bit aktivasyon fonksiyonudur. Sigmoid aktivasyon fonksiyonun matematiksel ifadesi Denklem 1.3.'de verilmiştir.

$$y(t) = \frac{1}{1 - e^{-t}} \tag{1.3}$$

Sigmoid fonksiyonun sınırlı aralıklar da gösterimi Şekil 1.19.'de gösterilmiştir.

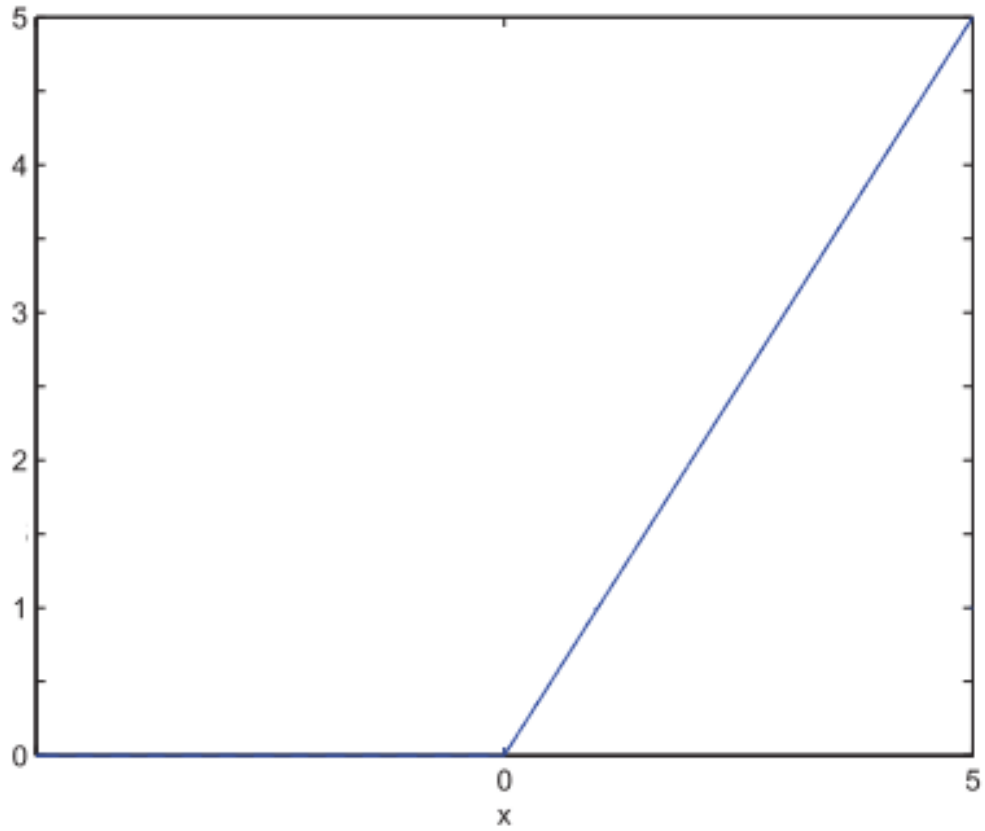


Şekil 1.19. Sigmoid fonksiyonu grafiği.

- **ReLU Aktivasyon Fonksiyonu:** ReLU fonksiyonu, giriş olarak gelen değerin negatif veya pozitif olup olmadığına bakar. Eğer değer negatifse çıkış olarak sıfır sonucu üretmektedir, pozitif ise gelen değeri aynı şekilde çıkış katmanına göndermektedir. Denklem 1.4.'de basit bir şekilde ifade edilmiştir.

$$\mathrm{Re}LU(x) = \begin{pmatrix} x, (egerx \geq 0) \\ 0, (egerx < 0) \end{pmatrix} \tag{1.4}$$

Şekil1.20.'de ReLU aktivasyon fonskiyonun çıkış grafiği gösterilmektedir.



Şekil 1.20. ReLU fonksiyonu çıkış grafiği.

Genel olarak bir sinir ağında evrişim ve ortaklama katmanından sonra tam bağlı katman işlemi gerçekleştirilmektedir. Tam bağlı katman kendisinden önceki katmanlarla birbirine bağlıdır. Tam bağlı katman evrişim ve ortaklama katmanından gelen değerleri kendi içerisinde bulunan değerler içerisinde çarpılıp, elde edilen değerlere bias hesabı yapılmaktadır. Evrişimli sinir ağında evrişim, ortaklama, tam bağ katmanından sonra işlem gören veri son olarak kayıp katmana gelmektedir. Kayıp katmanı veri setimiz ile eğittiğimiz ağın test verisi üzerindeki tahmini ile hedeflenen sonuç arasındaki ilişkiyi bir hata fonksiyonu aracılığıyla hesaplamaktadır. Giriş verisini, olması gerek hedeflerin her biri için bir olasılık değeri çıkartır ve bu değerler içerisinde en büyük değere sahip olan ile ilişkilendirilmesi yapılmaktadır.

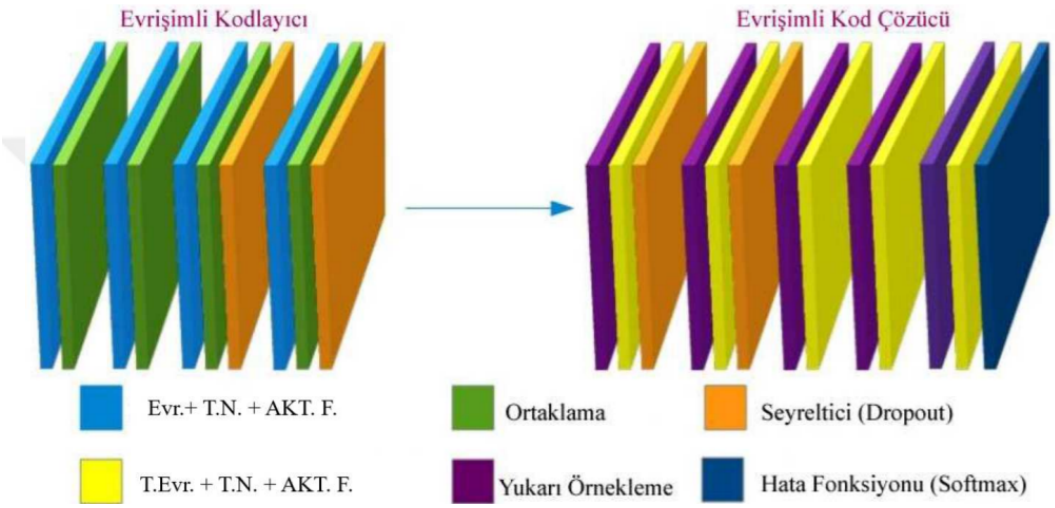
Yığın normalizasyon katmanı, herhangi bir optimizasyon algoritması gerçekleştirilmeden kullanılan evrişim sinir ağının optimize edildiği katmandır. Katman içerisinde optimizasyon işlemi gerçekleştirdiğinden dolayı verilerin eğitim aşaması hızlanmaktadır. Aynı zamanda kullanılan modeli kararlı bir hale getirilmesini sağlayarak test başarımını

artırmaktadır [44].

Birleştirme katmanı, farklı kaynaklardan gelen veriyi uygun bir şekilde birleştiren katmandır. Yani farklı verilerden elde edilen özellik haritalarının birleştirme işlemi gerçekleştirilmektedir.

1.3.2. Kodlayıcı Kod Çözücü Mimarisi

Genellikle görüntüleri anlamsal olarak bölütlemek için evrişim sinir ağının içerisinde bulunan kodlayıcının sonuna, bir kod çözücü eklenmektedir. Daha sonra kod çözücünün sonuna bir sınıflandırıcı koyarak klasik manada bir kodlayıcı-kod çözücü mimarisi oluşturulmaktadır. Şekil 1.21.'de evrişimli sinir ağı içerisinde kullanılan örnek bir kodlayıcı-kod çözücü mimarisi gösterilmektedir [45].



Şekil 1.21. Genel kodlayıcı kod çözücü mimarisi

Evrişimli sinir ağı içerisinde kodlayıcı-kod çözücü mimarisinde kod çözücü içerisinde bulunan yukarı örnekleme işlemi, gelen görüntünün çözünürlük değerlerini artırma işlemi gerçekleştirmektedir. Genellikle ters ortaklama ve ters evrişim işlemleri gerçekleştirilmektedir. Evrişim işleminin trans pozu alınması ile elde edilen işleme, ters evrişim işlemi denilmektedir. Kodlayıcı-kod çözücü mimarisinde kod çözücü içerisinde bulunan ters evrişim katmanı, evrişim işlemi gerçekleştirdikten sonra elde edilen sonuçların, seyreltilme işleminin gerçekleştirildiği işlem aşamasıdır [46].

En büyüğe ortaklama işleminin tersi alınamadığı için ortaklama işlemi yapılırken, elde

edilen en büyük değerlerin bulunduğu konumlardan faydalanılarak ters ortaklama işlemi gerçekleştirilmektedir.

Kodlayıcı-kod çözücü mimarisinde toplu normalizasyon, evrişim ve ortaklama işlemleri kodlayıcı içerisin de yer almaktadır. Ağa giren görüntüyü büyük boyutlu vektörlere çevirerek fazlaca özellik vektörü elde edilmesi sağlanmaktadır. Bu üç temel işlem gerçekleştirildikten sonra çıkışları aktivasyon fonksiyonu ile kod çözücü bölgesine girdi olarak verilmektedir.

Kod çözücü bölgesi içerisinde yuları örnekleme, ters ortaklama, evrişim ve ters evrişim işlemi, normalizasyon ve aktifleştirme fonksiyonu işlemleri gerçekleştirilmektedir. Kodlayıcı kısmında gelen büyük boyutlu vektörleri, kod çözücü kısmında girdi olarak alınan görüntü ile eş boyutta tek bantlı anlamsal bir bölütleme işlemi gerçekleştirilmektedir.

1.4. Öznitelik Çıkarım Yöntemleri

Literatürde birçok blok temelli öznitelik çıkarma metodu olmasına rağmen sıklıkla kullanılan ayrık kosinüs dönüşümü (DCT), yerel ikili örüntü (YİÖ) ve gradyanların histogramı (HOG) yöntemleri kullanımaktadır. Aşağıda YİÖ ve HOG yöntemi açıklanacaktır.

1.4.1. Yerel İkili Örüntü

Gri renkli görüntüler üzerinden farklı türlerdeki doku bilgilerinden özellik çıkaran yöntemdir. Görüntü üzerindeki her piksel üzerinden doku bilgisi elde etmektedir. Görüntü üzerinde 3x3 bir matris aracılığıyla komşulukları kontrol ederek piksel sınıflandırması gerçekleştirmektedir. Referans piksel değerini, 3x3 matris komşuları içerisinde kıyaslamaktadır. Eğer komşuluk değeri referans değerinden büyük ise 1, küçük ise 0 değeri atanmaktadır. (x,y) koordinatlarına sahip olan bir piksel için üretilen yerel ikili örüntü değerini hesaplama formülü Denklem 2.2.'de verilmiştir. Verilen denklem içerisinde bulunan S () fonksiyonunun matematiksel ifadesi Denklem 2.3.'te verilmiştir.

$$LBP_{P,R}(x_C, y_C) = \sum_{P=0}^{P-1} s(i_p - i_c)2^p \tag{1.5}$$

$$s(x) = \begin{pmatrix} 0, (egerx \leq 0) \\ 1, (egerx \geq 0) \end{pmatrix} \tag{1.6}$$

1.4.2. Gradyanların Histogramı (HOG)

Gradyanların histogramı, insanları sınıflandırma problemini çözmek için kullanılmıştır. Karmaşık durumlarda yüksek bir performans göstermektedir. Gradyan histogramı yerel bölgelerde bulunan bir nesneyi histogramlar halinde ifade edebilmek için, hedef bölgelerdeki nesnelerin kenar dağılımları ile alakalı özellikleri çıkarmaktadır. Bu histogramlar, hedef nesnenin belirli bir küçük alanında gradyan yönelimlerinin oluşma sıklığını temsil eder. Histogram özellikleri elde etmek için ilk olarak Denklem 2.4.'te gösterildiği gibi görüntü üzerine [-1,1] gradyan operatürü uygulanmaktadır.

$$G_x = [-1, 0, 1] * I(x, y) \triangleright G_Y = [-1, 0, 1]^T * I(x, y) \tag{1.7}$$

Daha sonra yerel bölgelerde histogram özelliklerinin normalizasyon işlemi gerçekleştirilmektedir.

2. BÖLÜM

YÖNTEM VE MATERYAL

2.1. Kopyala Yapıştır Sahteciliği Veri Seti

Kopyala yapıştır sahteciliğin de kullanılan veri kümeleri, sahteciliğin uygulanma şekline ve görüntülerin boyutlarına göre farklılık göstermektedir. Tablo 2.1.'de hem kullanılan veri kümesi hem de literatürde kullanılan diğer veri kümeleri hakkında bilgi verilmektedir.

Tablo 2.1. Kopyala yapıştır sahteciliğinde kullanılan veri kümeleri [47].

Veri Kümesi	**Görüntü Yapısı**	**Görüntü Boyutları**
MICC-F220	110 adet sahte, 110 adet orjinal fotoğraf bulunmaktadır	722 x 480 den 800 x 600 boyutuna sahip görüntüler bulunmaktadır
MICC-F600	152 adet sahte, 448 adet orjinal fotoğraf bulunmaktadır	800 x 532 den 3888 x 2592 boyutuna sahip görüntüler bulunmaktadır
MICC-F2000	7000 adet sahte, 1300 adet orjinal görüntü bulunmaktadır	2048 x 1536 boyutuna sahip görüntüler bulunmaktadır
SATs-130	48 adet sahte, 48 adet orjinal fotoğraf bulunmaktadır	1024 x 683 den 3264 x 2448 boyutuna sahip görüntüler bulunmaktadır
Kullanılan Veri Kümesi	50 adet sahte, 701 adet orjinal fotoğraf bulunmaktadır	720 x 960 boyutuna sahip görüntüler bulunmaktadır

Bu bölümde yapılan tez çalışması hakkında kullanılan yöntemin ayrıntılı işlem adımları verilecektir. Daha sonra uygulanan yöntemin başarı ve performansı hakkında yapılan değerlendirmeler verilmektedir. Ardından önerilen yöntemde kullanılan anlamsal

bölütleme modelinin eğitim ve test aşamalarında kullanılan veri seti hakkında bilgi verilecektir.

2.2. Önerilen Kopyala Yapıştır Sahteciliği Tespit Yöntemi

Yapılan tez çalışmasında görüntü anlamsal bölütlemesi destekli, blok tabanlı kopyala yapıştır sahteciliği tespit yöntemi geliştirilmektedir.

Önerilen modelde görüntü anlamsal bölütleme yönteminin eğitimi için CamVid veri kümesine ek olarak tez çalışması kapsamında özgün olarak üretilen kopyala yapıştır sahteciliği içeren görüntülerin de eklenmesi ile eğitim işlemi gerçekleştirilmiştir. Daha sonra girdi olarak alınan görüntü üzerindeki bölgeler segmentasyon yardımı ile etiketler halinde sınıflandırılıp, aynı sınıf içerisindeki bölgeler üzerinde kopyala yapıştır sahteciliği olup olmadığı tespit edilmiştir. Önerilen kopyala yapıştır sahteciliği yönteminin başarımı, sahtecilik yapılan görüntüden elde edilen maske ile tespit edilen sahtecilik bölgelerinin kıyaslanması ile elde edilmektedir.

Kopyala-taşı sahteciliğinin tespiti için önerilen yöntemin genel işlem adımları aşağıdaki gibidir:

1. Adım : Girdi olarak alınan sayısal görüntüye anlamsal bölütleme işlemi gerçekleştirilir.
2. Adım: Girdi olarak alınan A $\times$ B $\times$ 3 boyutuna sahip sahtecilik gerçekleştirilmiş renkli görüntüyü 2 boyutlu gri seviyeye dönüştürme işlemi gerçekleştirilir. (Renk değerlerini kullanmayan yöntemler için geçerlidir)
3. Adım: Elimizdeki görüntüyü L $\times$ L üst süte çakışan bloklara bölme işlemi gerçekleştirilir. Sonuç olarak toplam blok sayısı N= (A-L+1) $\times$ (B-L+1) formülü ile hesaplanmaktadır.
4. Adım: Bloklara ayırma işlemi aşamasında, anlamsal bölütleme sonucu elde edilen etiket sınıflarımıza göre blokların kategorize edilme işlemi gerçekleştirilmektedir.
5. Adım: Çıkarılan her bloğa ait özellik vektörü ayrık kosinüs dönüşümü ile çıkarılmaktadır. Dönüşüm gerçekleştirildikten sonra elde edilen dönüşüm matrisine

zigzag uygulanmaktadır [47]. İşlem sonucu her blok dan 1×64 şeklinde fi özellik vektörü elde edilir. Vektörü kıyaslamak için özellik vektörünün ilk 20 elemanı alınır ve son iki elemanlarına konum bilgileri kaydedilir.

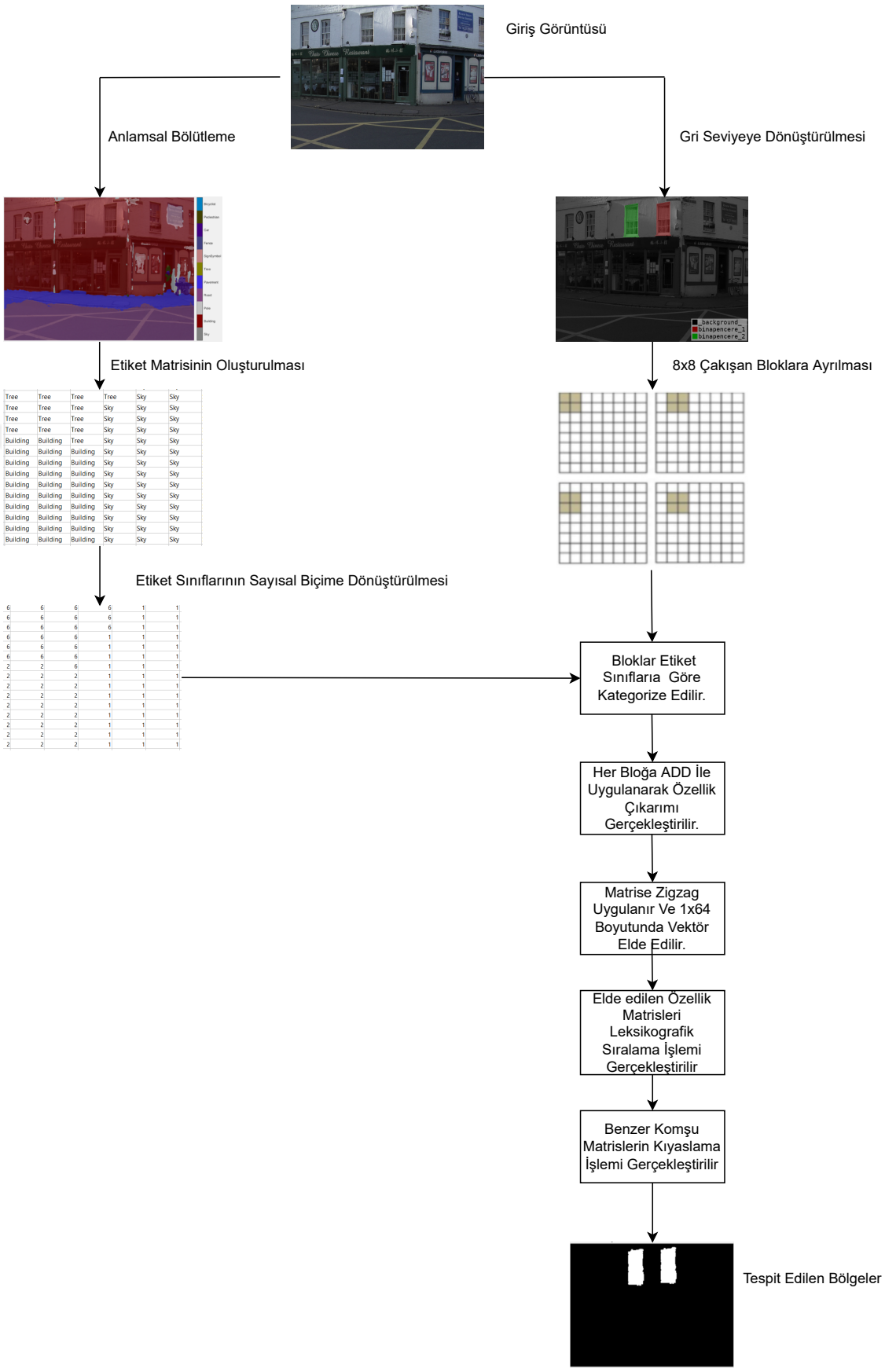
6. Adım: Daha sonra her etiket sınıfı içerisinde bulunan bloklar için F özellik matrisleri oluşturulur.

7. Adım: Elde edilen F özellik matrisleri içerisinde bulunan her satırı leksikografik olarak sıralama işlemi gerçekleştirilir. Bu sıralama işleminde fi özellik vektörü değerlerine göre birbirine yakın olanlar sıralama sonucunda da birbirine yakın haline gelecektir. Daha sonra ortalama bir eşik değerine göre en yakın komşuları arasında eşleşen fi özellik vektörleri tespit edilir.

8. Adım: Belirli bir eşik değerinde göre benzer olan vektörler i $\neq$ j olmak kaydıyla fi ve fj olarak iki adet özellik vektörümüz olsun. Benzer bloklar arasında si kaydırma vektörü hesaplanır. Benzer iki blok arası Öklid bağlantısı sonucu belirli bir eşik değerinin altında ise o blok silinecektir

9. Adım: Son işlem olarak da yanlış tespit edilen bölgeler morfolojik işlemler ile yok edilmektedir.

Şekil 2.1.'de önerilen yöntemin işlem adımları gösterilmiştir.

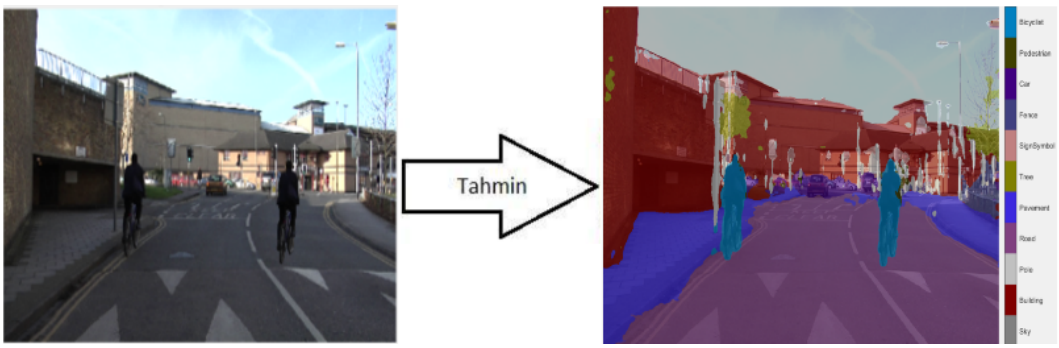


Şekil 2.1. Önerilen yöntemin akış şeması.

2.2.1. Kopyala Yapıştır Sahteciliği Yapılan Görüntülerin Anlamsal Bölütlenmesi

Görüntü üzerinde bulunan her pikselin özellik değerine göre farklı gruplara ayırma işlemine anlamsal bölütleme işlemi olarak ifade edilmektedir. Piksel sınıflandırması gerçekleştiren anlamsal bölütleme işlemi, görüntü içerisinde bulunan benzer bölgeleri kategorize ederek görüntü içeriği noktasında çokça bilgi vermektedir. Benzer özelliklere ait piksellerin kategorize edilme işlemini bölütleme olarak ifade edilirken, resim içerisinde ki bütün piksellerin kategorize edilme işlemi anlamsal bölütleme olarak ifade edilmektedir [48].

Anlamsal bölütleme güncel teknoloji içerisinde tıp ve mühendislik gibi alanlarda fazlaca kullanılmaktadır. Hatta otonom sürüş sistemlerinde kritik bir önem taşımaktadır. Anlamsal bölütleme işlemi iki şekilde yapılmaktadır. Eğer bölütleme işlemi etiketleme işlemi yapılmış pikseller üzerinde gerçekleştirilse buna denetimli bölütleme olarak ifade edilmektedir. Pikseller daha önceden etiketlenmemiş ise buna denetimsiz bölütleme denilmektedir. Şekil 2.2.'de örnek bir görüntü üzerinde on iki farklı sınıfta anlamsal bölütleme işlemi gerçekleştirilen bir örnek verilmiştir [49].



Şekil 2.2. Bir görüntü üzerinde yapılan anlamsal bölütleme işlemi.

Önerilen yöntemde, kullanılmış olan anlamsal bölütleme işlemin de model olarak kodlayıcı ve kod çözücü temelli evrişimli sinir ağı tercih edilmiştir. Tercih edilen deeplabv3+ modeli, deeplabv3 modelinin geliştirilmiş en son versiyonudur. Kullanılan deeplapv3+ modelini, deeplabv3 modeline göre kullanılan görüntüler üzerinde segmentasyon başarısını artırmak için yeni bir kod çözücü modülü geliştirilmiştir. Geliştirilen model, derin evrişimli sinir ağı mimarisine dayanan, atrous uzamsal piramit

havuzlaması ve bir adet kod çözücüden oluşmaktadır. Seçilmiş olan model mimarı olarak bir adet kodlayıcı ve bir adet kod çözücü katman içermektedir.

DeepLab V3+ modeli,mimarı olarak bir adet kodlayıcı ve bir adet kod çözücü katman içermektedir. Model içerisindeki kodlayıcı, girdi olarak alınan yüksek çözünürlüğe sahip bir resimden özellikleri çıkartır ve elde edilen özellikleri daha düşük çözünürlüklü özellik vektörüne dönüştürme işlemi gerçekleştirir. Derin evrişimli sinir ağı temelli deepLab ve deeplabv3 modellerinin kilit parametresi, girdi olarak alınan görüntünün çıkış olarak ifade edilen sonuç çözünürlüğüne oranıdır. DeepLabV3 modelinde olduğu gibi, çıktı çözünürlüğü 16 veya 8 olacak şekilde sonuç almak için, bir atrous konvolüsyon işlemi gerçekleştirip daha sonra son bir veya daha fazla bloktan kademe kademe kaldırılması ile elde edilmektedir.

Bu model, DeepLabV3 algoritmalarının geliştirilmiş bir versiyonudur. Model içerisin de atrous ayrılabilir evrişim ağını oluşturmak için atrous evrişimini, derinlemesine ayrılabilir evrişim ile birleştirilmektedir. Daha sonra atrous uzamsal piramit havuzuna, atrous ayrılabilir evrişim işlemi gerçekleştirilir.

Bu model, literatürdeki başarılı fikirleri kullanarak DeepLabV3 [5] algoritmalarının temelini oluşturmaktadır. Atrous ayrılabilir evrişim oluşturmak için atrous evrişimi derinlemesine ayrılabilir evrişim ile birleştirilmektedir. Daha sonra atrous uzamsal piramit havuzuna, atrous ayrılabilir evrişim uygulanmaktadır [50].

Atrous evrişimli sinir ağı, derin evrişimli sinir ağları tarafından elde edilen özniteliklerin çözünürlüğünü kontrol etmektedir. Aynı zaman da çok ölçekli bilgileri tespit etmek için filtrenin görüş alanını düzenlemeye izin veren, klasik evrişim işlemini genelleştiren güçlü bir araçtır. Giriş olarak alınan iki boyutlu sinyaller durumunda, girdi özellik haritası x üzerinde aşağıdaki gibi atrous konvolüsyon evrişim yapılır: çıkış özellik haritası y üzerindeki her i konumu ve bir evrişim filtresi w için, atrous evrişim aşağıdaki gibi uygulanır:

$$y[i] = \sum_{k} x[i + rk]w[k] \tag{2.1}$$

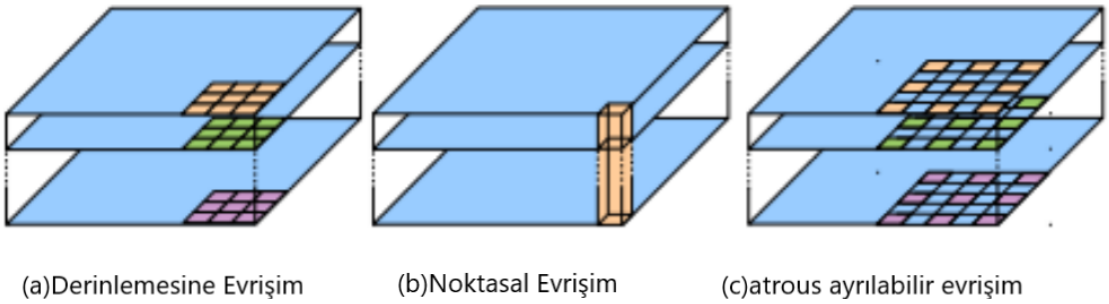
burada r örneklemedir, yani giriş sinyalinin yakalanma hızıdır. Standart evrişim, r

hızının bire eşit olduğu belirli bir örnektir. Hız değeri değiştirilerek filtrenin görüş alanı uyarlanabilir şekilde ayarlanır.

Derinlemesine ayrılabilir evrişim (veya grup evrişim), bazen performansı artırırken hesaplama süresini ve parametre sayısını önemli ölçüde azaltabilen güçlü yöntemlerden biridir. Aynı zaman da konvansiyonel bir evrişimi, derinlemesine ve daha sonra noktasal bir evrişe dönüştürülmesini sağlayan çarpanlara ayırma işlemini gerçekleştirmektedir. Bu, hesaplamanın karmaşıklığını önemli ölçüde azaltmaktadır. Bunun nedeni, her bir giriş kanalının derinlemesine evrişiminin ayrı ayrı yürütme işleminin gerçekleştirilmesidir. Bu işlemi takiben, noktasal evrişim, derinlemesine evrişimin çıktısını birleştirmektedir.

Ayrılabilir derinlemesine evrişim, sıradan evrişimi derinlemesine evrişim (her giriş kanalı için tek bir filtre kullanarak) ve noktasal evrişim (kanallar arasında derinlemesine evrişimden gelen çıktıları birleştirerek) olarak ayrıştırır. Derinlemesine evrişimde atröz evrişimin kullanıldığı DeepLabV3+ modelinde atröz ayrılabilir evrişim tanıtıldı.

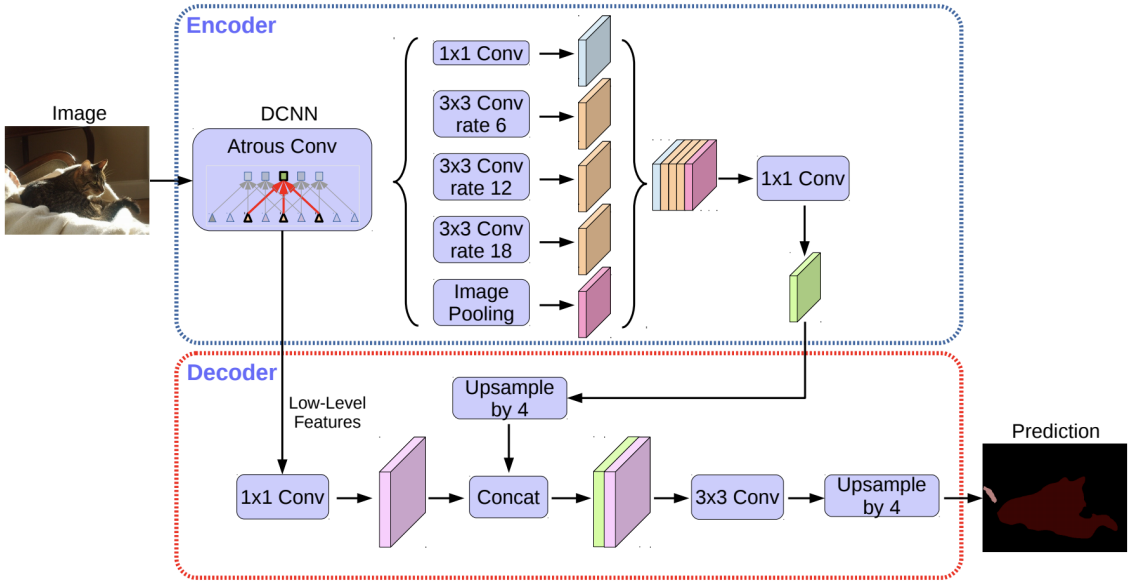
Ayrılabilir derinlemesine evrişim, sıradan evrişimi derinlemesine evrişim (her giriş kanalı için tek bir filtre kullanarak) ve noktasal evrişim (kanallar arasında derinlemesine evrişimden gelen çıktıları birleştirerek) olarak ayrıştırır. Derinlemesine evrişimde atröz evrişimin kullanıldığı DeepLabV3+ modelinde atrous ayrılabilir evrişim Şekil 2.3.'de tanıtıldı [51].



Şekil 2.3. (a) Derin evrişim, (b) noktasal evrişim ve (c) çok ayrılabilir evrişim.

Atrous uzamsal piramitlerin havuzlanması deepLabV3, herhangi bir çözünürlükte derin evrişimli sinir ağları tarafından oluşturulan özellikleri, atrous evrişim yoluyla çıkarmaktadır. Çıkış aşaması, bu bağlamda, girdi olarak alınan görüntünün uzamsal çözünürlüğünün son çıktı çözünürlüğüne oranı olarak ifade edilmektedir (küresel öncesi

havuzlama veya tam bağlantılı katman). Görüntü sınıflandırması için, nihai özellik haritalarının uzamsal çözünürlüğü, giriş resminin uzamsal çözünürlüğünden tipik olarak 32 kat daha düşük olmaktadır, bu da 32'lik bir çıkış adımı ile sonuçlanmaktadır. Anlamsal bölütleme yaparken daha yoğun bir özellik elde etmek için çıktı adımı 16 (veya 8) kullanılması tercih edilmektedir. Ek olarak, DeepLabV3+, atrous uzamsal piramit havuzlaması modülünü görüntü düzeyinde özelliklerle zenginleştirmektedir. Bu modül, değişen oranlarda atrous evrişim gerçekleştirerek çok sayıda ölçekte evrişimsel özellikleri incelemektedir. Orijinal DeepLabV3+'da önerilen kodlayıcı-kod çözücü kombinasyonunda, kodlayıcı çıkışı olarak logitlerden önceki son özellik haritası kullanılmaktadır. Kodlayıcının çıktı özelliği haritasının 256 kanala ve çok sayıda anlamsal veriye sahip olduğu bilinmektedir. Şekil 2.4.'te, önerilen kodlayıcı-kod çözücü yapısı gösterilmektedir ve bu mimari de, kodlayıcıdan çeşitli ölçeklerde özellikleri çıkarmak için kodlayıcı içerisin de uzaysal piramit havuzunu kullanmaktadır [50].

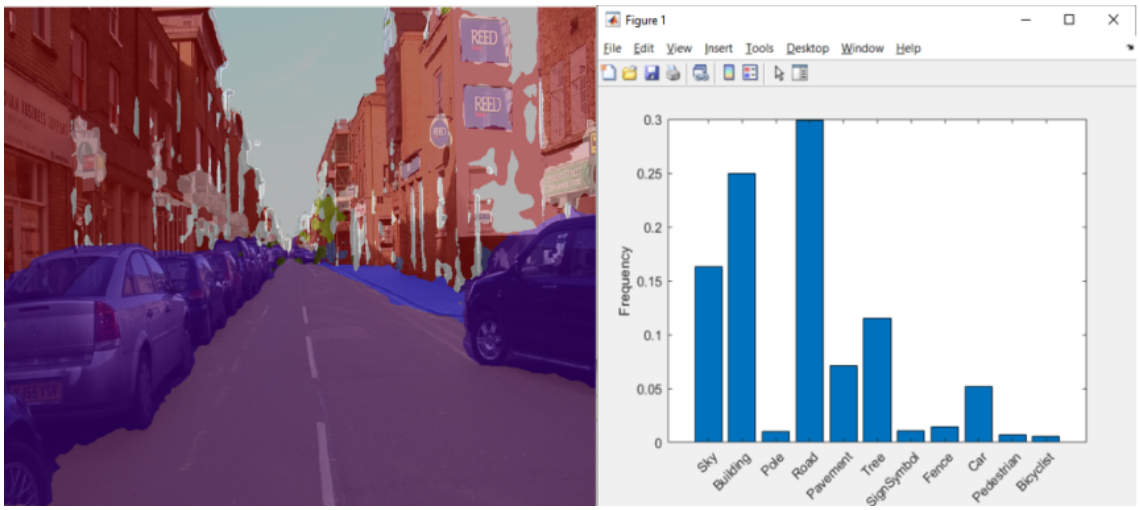


Şekil 2.4. Atrous uzamsal piramit havuzuyla kodlayıcı-kod çözücünün yapısı[43].

Şekil 2.4.'te gösterildiği gibi basit ama etkili bir kod çözücü önerilmektedir. Kodlayıcı özellikleri ilk önce dört faktörü ile çift doğrusal olarak yukarı örneklenmektedir ve daha sonra aynı uzamsal çözünürlüğe sahip eşdeğer düşük seviyeli ağ kodlayıcı özellikleriyle birleştirilmektedir. Daha sonra, kanal sayısını azaltmak için düşük seviyeli özelliklerde 1 x 1 evrişim işlemi daha gerçekleştirilmektedir, çünkü ilişkili düşük seviye özellikler genellikle, zengin kodlayıcı özelliklerinin değerinden daha ağır basabilecek ve

eğitimi karmaşıklaştırabilecek çok sayıda kanal (örneğin, 256 veya 512) içermektedir. Birleştirme aşamasını takiben, özelliklerin netleştirilmesi için 3 x 3 boyutlu bir evrişim kullanılmaktadır, ardından dört faktörlü başka bir standart çift doğrusal yukarı örnekleme yapılmaktadır. Enkoder modülü için çıkış adımı 16 ayarının optimum hız ve doğruluk dengesine ulaştığı gösterilmektedir. Enkoder modülü için çıkış adımı 8 kullanıldığında ise, artan hesaplama karmaşıklığına rağmen performans artmaktadır.

Önerilen yöntem de giriş olarak alınan görüntünün anlamsal olarak bölütlenmesi işlemi gerçekleştirilmektedir. Bu bölütleme işlemi için deeplab modelinin en son ve en güçlü versiyonu olan deeplabv3+ modeli kullanılmıştır [51]. Kopyala yapıştır sahteciliği yapılan görüntüler üzerinde daha başarılı bir anlamsal bölütleme işlemi gerçekleştirmek için, modelin eğitim verisi içerisine kopyala yapıştır sahteciliği yapılan görüntüler de eklenmiştir. Veri kümemiz hem CamVid veri kümesi içerisindeki resimler hemde özgün olarak hazırlanmış kopyala yapıştır sahteciliği görüntülerinden oluşmaktadır. Bu veri kümesi ile yapılan eğitim işlemi, kurcalanmış görüntüler üzerinde anlamsal bölütleme başarısını artırmaktadır. Anlamsal bölütleme işlemi için seçilen model gökyüzü, bina, direk, yol, kaldırım, ağaç,trafik tabelaları, çit, araba, yaya ve bisikletçi olmak üzere sahtecilik yapılmış görüntüyü on bir farklı sınıfta etiketleme işlemi gerçekleştirmektedir. Belirlenen sınıfların dışında kalan bölgeler ise farklı bir etiket ile sınıflandırma işlemi gerçekleştirilmektedir. Şekil 2.5.'te kopyala yapıştır sahteciliği uygulanmış bir görüntü üzerinde, anlamsal bölütleme işleminin gerçekleştirildiği bir örnektir.



Şekil 2.5. Kopyala yapıştır sahteciliği yapılan görüntü üzerinde anlamsal bölütleme işlemi.

Şekil 2.5.'te etiketleme sınıflarımızın görüntü üzerinde ki dağılımlarının oranı verilmektedir.

Anlamsal bölütleme sonrası mevcut etiket haritamız üzerinde 8 $\times$ 8'lik bir matris bloğu gezdirilmektedir. Gezen matris bloğumuz içerisinde en sık tekrar edilen etiket sınıfına göre gruplandırılacağı sınıf tespit edilmektedir. Tespit edilen etiket numarasına göre bloklarımız anlamsal bölütleme de bulunan sınıf sayısı kadar kategorize edilmektedir. Literatürde blok temelli kopyala yapıştır sahteciliği tespiti yöntemleri de genel olarak bir bloğu görüntü içerinde kalan diğer tüm bloklar arasında kıyaslama işlemi gerçekleştirilmektedir. Bu işlem zaman ve performans açısından ciddi bir maliyet oluşturmaktadır. Önerilen yöntem de aynı etiket sınıfları içerisinde kopyala yapıştır sahteciliği yapılabileceği öngörülmüştür. Çünkü çim sınıfı etiketi içerisinde bulunan bir bölgenin, gökyüzü etiketi sınıfında olan bir bölgeye yapıştırılması anlamsız olacaktır. Bu işlem tespiti kolay bir sahtecilik olmasından kaynaklı olarak, yapılan sahtecilik bir amaca hizmet etmeyecektir. Görüntü sahteciliğin de temel kural çıplak göz ile fark edilmeyecek görüntüler üretmektir. Bu yüzden önerilen yöntem de yalnızca kendi sınıfı içerisinde olan benzer bloklar sıralanıp tespit edilmesi önerilmiştir. Önerilen yöntem ile bir blok resmin geriye kalan tüm blokları ile eşleştirmek yerine sadece kendi sınıfı içerisinde kıyaslayarak, zaman açısında yüksek bir performans göstermektedir. Şekil 2.6'te aynı etiket bölgesine dahil olup, yine ayni bölge içerisin de gerçekleştirilen kopyala yapıştır sahteciliği örnekleri gösterilmektedir.

Şekil 2.6. Anlamsal bölütleme işlemi sonucu, aynı etiket bölgesi içerisinde uygulanan kopyala yapıştır sahteciliği görüntü örnekleri.

2.2.2. Ayrık Kosinüs Dönüşümü Öznitelik Çıkarma Yöntemi

Ayrık kosinüs dönüşümü görüntü üzerinde blok temelli yaklaşımlarda sıklıkla kullanılan, öznitelik çıkarımı işlemi gerçekleştiren bir dönüşüm yöntemidir. Giriş olarak alınan bir görüntünün frekans katsayılarını, hedefe uygun bir şekilde dönüşümünü gerçekleştiren işlemdir. Yani farklı frekanslardan elde edilen kosinüs fonksiyonlarının toplamı olarak da ifade edilebilmektedir. Yaygın olarak veri sıkıştırma ve sinyal işleme de frekansları dönüştürmek için kullanılmaktadır [52].

Kopyala yapıştır sahteciliğin de sayısal görüntü üzerin de ki ayırt edici bilgilerin elde edilmesi için ayrık kosinüs dönüşümü kullanılmaktadır.Ayrık kosinüs dönüşümü görüntü işleme gibi sahalar da yaygın kullanıldığı gibi telekomünikasyon alanlarında da kullanılmaktadır. Bu yöntem sayısal olarak alınan bir sinyal üzerine kosinüs fonksiyonu gerçekleştirerek frekansa dönüştürmektedir. Bu yöntemde sadece kosinüs dönüşümü kullanılmaktadır. Bu yüzden sadece aritmetik hesaplama işlemleri gerçekleştirilmektedir. M x N boyutuna sahip sayısal bir görüntü olan I için yapılan dönüşüm işlemi Denklem 2.5.'te gösterilmektedir.

$$C(u,v) = a_u a_v \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m,n) \cos\frac{\pi(2m+1)u}{2M} \cos\frac{\pi(2n+1)v}{2N}, 0 \leq v \leq N-1$$
$$a_u \left\{ \begin{array}{l} \frac{1}{\sqrt{M}}, u = 0 \\ \frac{2}{\sqrt{M}}, 0 < u \leq M-1 \end{array} \right\}, a_v \left\{ \begin{array}{l} \frac{1}{\sqrt{N}}, v = 0 \\ \frac{2}{\sqrt{N}}, 0 < u \leq N-1 \end{array} \right\} \tag{2.2}$$

M x N boyutuna sahip sayılsa görüntüye dönüşüm uyguladıktan sonra yine aynı boyutta ayrık kosinüs dönüşümü katsayıları üretilmektedir. Üretilen katsayılar alçak, orta ve yüksek frekans bileşenleri olarak üç grupta kategorize edilmektedir. Alçak frekans bileşenlerinde orta ve yüksek bileşenlere göre daha fazla bilgi bulundurmaktadır. Yüksek frekans bileşenleri, alçak frekans bileşenlerine göre saldırı altında daha hassastır. Önerilen kopyala yapıştır sahteciliği yöntemin de özellik çıkarma fonksiyonu olarak ayrık kosinüs dönüşümü gerçekleştirilmektedir.

2.2.3. Öznitelik Tanımlayıcıların Eşleştirilmesi

Bölünen bloklar üzerin de ayrık kosinüs dönüşümü işlemi gerçekleştirilerek elde edilen özellikler ile birbirleri arasında en benzer olan blokların belirlenmesi gerekmektedir. Belirlenen benzer bloklar yardımı ile varsayılan kopyala yapıştır sahteciliği bölgelerine ait olan blok çiftleri tespit edilmektedir. Çıkarılan her öznitelik vektörünü geriye kalan tüm vektörler ile kıyaslamak yüksek bir maliyet gerektirmektedir. Bunun için birbirine benzer olan öznitelik vektörlerini tespit etmek ve kıyaslama işlemini belirli bir sayıda vektörle yapmamız gerekmektedir. Bu yöntemi uygulamak için bloklar üzerin de elde edilen tüm öznitelik vektörlerini tek bir matris içerisine depolanması, daha sonra benzer olan aday vektörlerin birbirlerine yakınlaştırma işlemi gerçekleştirilmelidir. Literatür içerisinde en sık kullanılan yöntem leksikografik (sözlük sıralaması) sıralamadır [53]. Leksikografik sırlama işlemi gerçekleştirildikten sonra öznitelik matrisi içerisindeki öznitelik vektörleri söz dizimsel olarak sıralanmış olmaktadır. Leksikografik sıralama dışında radix sıralama [54], hash değerlerinin kıyaslama işlemi [55], k-d ağacı [56] gibi tekniklerde kullanılmaktadır. Benzer öznitelik vektörlerinin birbirine komşu durumuna getirilmesi için öznitelik vektörlerinin kıyaslanmasında kullanılan benzerlik kriterleri vardır. Bunlar Öklid uzaklığı [57], Hausdorf uzaklığı [58], hamming uzaklığı [59] gibi kıyaslamak için gereken benzerlik kriterleridir.

2.2.4. Sahte Bölge Tespitinin Gerçekleştirilmesi

Blok tabanlı yaklaşımlar da daha önceden belirtilen adımların gerçekleştirilmesinden sonra elde edilen sahtecilik bölgeleri tam manada bir doğruluk belirtmemektedir. Kopyala yapıştır sahteciliği uygulanmış bazı görüntüler de görüntünün tabiatından dolayı birbirine benzer gerçek bölge çiftleri de görülmektedir. Bu benzer bölge çiftlerinden elde edilen özelliklerin birbiri ile aynı sonuçları vermesinden dolayı yanlış bölgelerde işaretlenebilmektedir. Bu şekilde sahtecilik olmayan fakat birbirine benzer olan bölgelerin elenebilmesi için uzaklık temelli birçok yaklaşım sunulmaktadır. Bu yaklaşımlardan bazıları kayma vektörü (Shift), alan ve uzaklık kriteri, afin dönüşüm matrisi gibi yaklaşımlardır. Kayma vektöründe, birbirine benzer olan bölgelerin (x,y)

koordinatları arasındaki farkın mutlak değerine bakılmaktadır. Bu tür yaklaşımlarda sahtecilik yapılan bölgelere uygulanan ölçekleme ve döndürme gibi saldıralar dikkate alınmamaktadır.

Geriye kalan diğer yöntemler de ise birbirine yakın olan bölgelerin benzer özellik gösterebilmesinden kaynaklı olarak uzaklık kriteri referans alınarak yanlış tespit edilmiş sahte bölgelerin elenmesi gerçekleştirilmektedir. Bundan dolayı her bloğun birbirine olan mesafeleri hesaplanarak belli bir eşik değeri altındaki yanlış tespit edilmiş blokların elenme işlemi gerçekleştirilmektedir. Bu amaçla kullanılan Öklid uzaklığı [60], maksimum normalize uzaklık [61], en yakın komşu uzaklığı [22] gibi yöntemler kullanılmaktadır.

Öklit Mesafe Ölçümü:İki koordinat arasındaki mutlak ifadenin gösterilmesine denilmektedir. Bir bölgeye ait olan (x,y) koordinatlarının farklarının hipotenüsünün alınması ile elde edilmektedir.

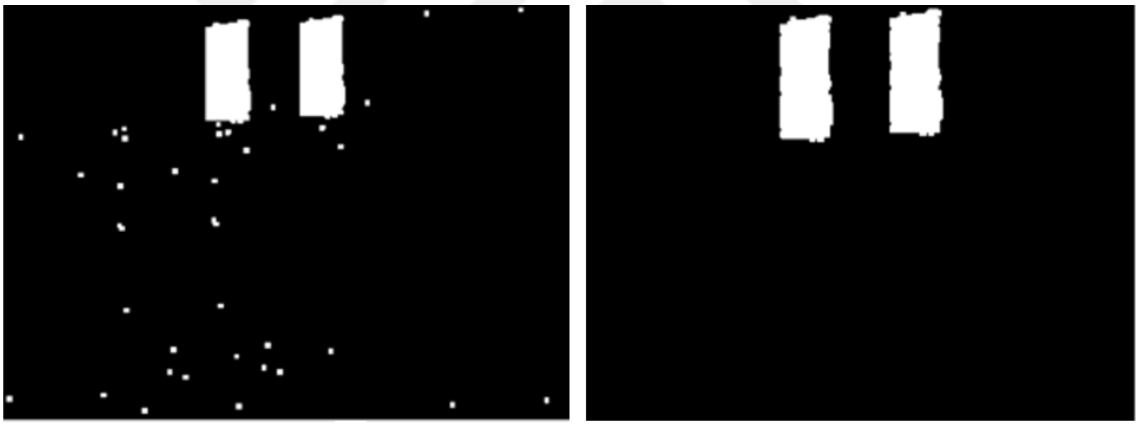
$$d(x,y) = \sqrt{\sum_{n=1}^{n}(x+y)^2} \tag{2.3}$$

Denklem 2.6.'da gösterildiği gibi x ve y bloğa ait olan koordinat bilgisi, d ise bloklar arasındaki mutlak mesafeyi belirtmektedir.

2.2.5. Kopyala Yapıştır Sahteciliği Haritasının İyileştirilmesi

Geleneksel morfolojik operatörler, bir veya daha fazla yapısal faktörün varlığına ihtiyaç duymaktadır. Gerçekte, bu tür operatörler ya bağımsız olmaktadır ya da bir veya daha fazla bağımsız operatörden oluşmaktadır. Bu bağlamda "yerel" kelimesi, belirli bir konumdaki (ayrık durumda piksel) çıktı değerinin küçük (örneğin sonlu) bir komşuluktaki girdi değerleri tarafından referans edildiği gerçeğine atıfta bulunulmaktadır. Geleneksel morfolojik operatörlerin, esasen paralel bir tarzda olmasına rağmen, piksel seviyesinde çalıştığı iddia edilebilmektedir. Bağlı olan morfolojik operatörler temelde farklıdırlar. Tek tek piksellerin değerlerini değiştirmezler, daha çok düz bölgeler olarak adlandırılan sabit gri tonlamalı bitişik alanların değerlerini değiştirme işlemini gerçekleştirmektedir. Bağlı operatörler, operatörün düz bölgelerdeki davranışını düzenleyen parametreler kullanılarak tanımlanmaktadır. Önerilen yöntemi ikili durumla sınırlıyoruz. Bu durumda düz bölgeler, ön planın ve arka planın bağlantılı bileşenlerine (taneler olarak adlandırılır) atıfta

bulunulur. Bu basit durumda bile kriterler oldukça karmaşık olabilir; bunlar bireysel bölgelerin biçim özelliklerine bağlı olabileceği gibi yakın bölgelerin özelliklerine de bağlı olabilmektedir [62]. İşlem görecek görüntü üzerinde bir yapılandırma matrisi gezdirilmektedir. Yapılandırma matrisinin tek boyutlara sahip olması ve orijinin matrisin merkezi olarak belirtilmesi yaygın bir yaklaşımdır. Yapılandırma elemanları, morfolojik görüntü işlemede doğrusal görüntü filtrelemede evrişim çekirdeklerinin yaptığı işlevin aynısını gerçekleştirir. İkili bir resime, bir yapılandırma elemanı eklendiğinde, piksellerinin her biri yapılandırma elemanının altındaki komşuluktaki eşleşen piksele bağlanır. Yapısal elemanın piksellerinin her biri 1'e ayarlanırsa, ilgili görüntü pikseli de aynı şekilde 1'e ayarlanır. Yani yapılandırma matrisinin boyutuna ve istenilen piksel boyutu ve uzaklığına bağlı olarak komşu olan piksellere karar verilerek sınıflandırma işlemi gerçekleştirilmektedir. Şekil 2.7.'da kopyala yapıştır sahteciliği tespit edilmiş bir görüntü üzerinde morfolojik işlem gerçekleştirilmiştir.



Şekil 2.7. a) Sonuç olarak sahtecilik tespiti gerçekleştirilmiş görüntüdür. b) Elde edilen görüntünün morfolojik işlem sonrası çıktısı.

3. BÖLÜM

DENEYLER VE SONUÇLAR

3.1. Deneysel Kurulum

Projenin geliştirilmesinde ve deneylerin yapılmasında kullanılan sistemde 32 GB Bellek,Intel (R) Core (TM) i7 2.67 GHZ işlemci, grafik işleme birimi olarak da GeForce GTX 2070 bulunmaktadır. Anlamsal bölütleme başarısını artırmak için, ürettiğimiz kopyala yapıştır sahteciliği yapımış görüntüleri GIMP programı yardımı ile gerçekleştirdik. Elde edilen sahte görüntüler LABELME programı yardımı ile etiketleme işlemi gerçekleştirilmiştir.

3.2. Deneyler

Kopyala yapıştır sahteciliği yapılan görüntüler üzerin de anlamsal bölütleme işlemi deeplabv3+ modeli ile gerçekleştirilmiştir [51]. Anlamlı bölütleme işlemi için kullanılan veri kümemiz, CamVid veri kümesi içerisine özgün olarak kurcalama işlemi gerçekleştirilmiş görüntüler ile oluşturulmuştur. Oluşturulan veri kümemiz ile eğitim işlemi gerçekleştirilmiştir. Ortaya çıkan model ile kopyala yapıştır sahteciliği yapılan görüntüler üzerinde yapılan deneyler sonucu beş ana kriter değerlerinin dört tanesinde başarım artmaktadır. Sadece bir adet kriter değerinde başarısı düşmüştür. Önerilen yöntem GlobalAccuacy, MeanAccuracy, MeanIoU, WeightedIoU parametrelerinde iyi sonuç verdiği, MeanBFScore da ise başarısız olduğu gözükmektedir. Tablo 3.1.'de önerilen yöntem ve kullanılan modelin sonuçları verilmiştir.

Modelimiz, kullanılan CamVid veri kümesi içerisine 50 adet kopyala yapıştır sahteciliği uygulanmış görüntü ile eğitim işlemi gerçekleştirilmiştir. Tablo 3.1.'de görüldü üzere

Tablo 3.1. Görüntü üzerinde yapılan anlamsal bölütleme başarımı.

Yöntem	**Global Accuracy**	**Mean Accuracy**	**Mean IoU**	**Weighted IoU**	**MeanBF Score**
DeepLabv3+	0.7122	0.54688	0.36852	0.59353	**0.40908**
Önerilen Yöntem	**0.71235**	**0.54789**	**0.36878**	**0.59357**	0.40859

daha başarılı bir sonuç vermiştir. Eğer eğitim işlemi daha çok kopyala yapıştır sahteciliği uygulanmış görüntü üzerinde gerçekleştirilirse başarının daha da artması beklenmektedir. Anlamsal bölütleme başarısı ne kadar iyi olursa tespit edilen sahtecilik bölgeleri o kadar doğru şekilde tespit işlemi gerçekleştirilir.

Anlamsal bölütleme işlemi gerçekleştirildikten sonra önerilen yöntem ile literatürdeki yöntem ile kıyaslamaları aşağıda verilmiştir.

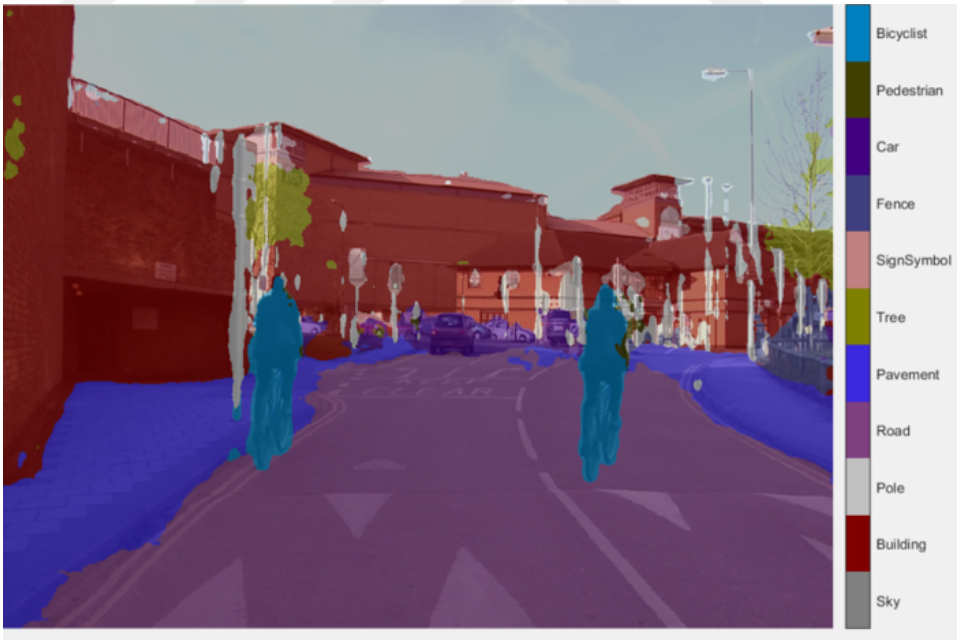
Şekil 3.2. (a) da gösterilen örnek de, bir cadde üzerinde çekilen fotoğrafın bina duvarı üzerinde ki reklam panosunun kopyalanarak yine aynı duvara yapıştırılması ile elde edilmiş bir sahte görüntü vardır. Şekil 3.2. (a) ile gösterilen görüntü üzerinde, sahtecilik yapılmış piksel bölgelerinin tespiti gerçekleştirilip sonucu Şekil 3.2. (b) de gösterilmiştir. Şekil 3.3. (a) da gösterilen örnek de, bir mağaza vitrini üzerinde bulunan camların, kopyala yapıştır sahteciliği uygulanarak üretilmiş sahte bir görüntüsü verilmiştir. Şekil 3.3. (a) ile gösterilen görüntü üzerinde, sahtecilik yapılmış piksel bölgelerinin tespiti gerçekleştirilip sonucu Şekil 3.3. (b) de gösterilmiştir. Şekil 3.4. (a) da gösterilen örnek de, bir sokak üzerinde çekilen fotoğrafın bina duvarı üzerinde ki pencerenin kopyalanarak yine aynı duvara yapıştırılması ile elde edilmiş bir sahte görüntü vardır. Şekil 3.4. (a) ile gösterilen görüntü üzerinde, sahtecilik yapılmış piksel bölgelerinin tespiti gerçekleştirilip sonucu Şekil 3.4. (b) de gösterilmiştir.

Tablo 3.3.'de görüldüğü üzere Şekil 3.4.'de tespit edilen sonuç literatürde kullanılan blok temelli AKD yaklaşımıyla başarı oranı 0.944229 ve maliyet süresi 3197,310495 olarak bulunurken bizim önerdiğimiz yöntemle sonuç 0,94753 ve maliyet zamanı 1205,688449 olduğu görülmektedir.

Tablo 3.3.'de görüldüğü üzere Şekil 3.3.'de tespit edilen sonuç literatürde kullanılan blok temelli AKD yaklaşımıyla başarı oranı 0.955924 ve maliyet süresi 3772,887775 olarak

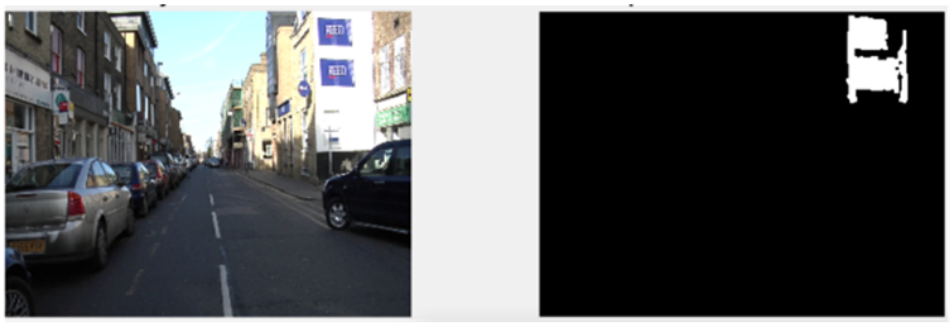
bulunurken bizim önerdiğimiz yöntemle sonuç 0,956333 ve maliyet zamanı 1081,827836 olduğu görülmektedir.

Tablo 3.2.'de anlamsal bölütleme işlemi sonucu etiket sınıflarının başarım oranı verilmiştir. Buna göre yapılan tespit işleminin başarım oranı farklı görüntüler üzerinde farklı doğruluklarda başarı göstermiştir. Bunun nedeni resim üzerindeki kopyalanarak yapıştırılan bölgelerin boyutları ile ilgili olduğu görülmektedir. Şekil 3.1.'de önerilen model ile anlamsal bölütleme işlemi gerçekleştirilmiştir. Tablo 3.2.'de oluşturulan modelimizin Şekil 3.1.'de gösterilen görüntüyü 11 adet (gökyüzü, bina, direk, yol, kaldırım, ağaç, trafik işareti, çit, araba, yaya, bisiklet) sınıfta yapmış olduğu etiketleme başarıları gösterilmiştir. Önerilen model de bölütleme sınıfları içerisinde yol ve gökyüzü tespitinde diğer sınıflara göre daha yüksek bir başarı göstermiştir.



Şekil 3.1. Önerilen model ile anlamsal bölütleme işlemi.

Tablo 3.3.'te önerilen yöntemin literatürdeki diğer blok tabanlı çalışmalara kıyaslan daha iyi sonuç verdiği ve zaman maliyeti olarak yüzde 40 ile 60 arasında düşürdüğü gözükmektedir. Tabloda önerilen yöntemin harcadığı zaman dilimi, anlamsal bölütleme süresi ile sahtecilik yapılan bölgeyi tespit etme süresinin toplamından oluşmaktadır.



a) b)

Şekil 3.2. Duvar üzerindeki mavi renkli logonun aynı şekilde alt kısma yapıştırılmış olduğu kopyala yapıştır sahteciliği tespiti örneği.

a) b)

Şekil 3.3. Önerilen yöntem ile duvar üzerindeki işlemin tespit edilen gerçek ve sahte bölgeler.

a) b)

Şekil 3.4. Üzerinde kurcalama yapılmış bir resim. Orta bölgedeki yan tarafa kopyalanmış ikinci kat penceresi hemen yanına yapıştırılmıştır.

Tablo 3.2. Görüntü üzerinde yapılan anlamsal bölütlemenin etiket sınıfları üzerinde ki sonuçları.

Deney	**Accuracy**	**IoU**	**MeanBFScore**
Gökyüzü	0.78941	0.67027	0.66488
Bina	0.61756	0.52638	0.42678
Direk	0.30011	0.080815	0.27206
Yol	0.86491	0.80428	0.61802
Kaldırım	0.6674	0.44819	0.44892
Ağaç	0.66427	0.48392	0.45867
Trafik İşaretleri	0.38966	0.15917	0.2676
Çit	0.46887	0.19288	0.27869
Araba	0.53425	0.333	0.33077
Yaya	0.36667	0.14916	0.27856
Bisiklet	0.36366	0.20849	0.29122

Tablo 3.3. Görüntü üzerinde yapılan kopyala yapıştır sahteciliği tespit başarımı ve zaman performansı.

Deneyler	**Accuracy**	**ElapsedTime (sn)**
DCT ve Blok Temelli Yaklaşımlar	0.944229	3197.310495
Önerilen Yöntem	0.94753	1205.688449
DCT ve Blok Temelli Yaklaşımlar	0.955924	3772.887775
Önerilen Yöntem	0.956333	1081.827836
DCT ve Blok Temelli Yaklaşımlar	0.970151	3772.887775
Önerilen Yöntem	0.970273	1850.276217

Şekil 3.4. Üzerinde gerçekleştirilmiş olan sonuçlar Tablo 3.4.'te açıklanmıştır. Şekil 3.4 (a) görüntüsüne ait sonuçlardan görüleceği üzere, 8 × 8 seçildiği zaman kurcalanmış pikselleri tespit başarımımız 0,947014 olurken, aynı şekilde 16 × 16 seçildiği zaman başarımımız 0,94153 olarak görülmektedir. Aynı deney Şekil 3.3 (a) üzerinde gerçekleştiğinde 8 × 8 bloklar kullanıldığı zaman tespit başarısı 0,972214 olurken 16 × 16 seçildiği zaman 0,950273 olduğu görülmektedir. Önerilen yöntemin üst üste çakışan blokların 16 × 16 yerine 8 × 8 olmasının deney sonuçları tarafından daha iyi sonuç verdiği Tablo 3.4.'te gözükmektedir.

Tablo 3.4. Görüntü üzerinde yapılan kopyala yapıştır sahteciliği tespiti için belirlenen blok boyutları.

Görüntü	**Blok Boyutu**	**Accuracy**
Şekil 3.4 (a)	8 × 8	0.947014
Şekil 3.4 (a)	16 × 16	0.94153
Şekil 3.3 (a)	8 × 8	0.972214
Şekil 3.3 (a)	16 × 16	0.950273
Şekil 3.2 (a)	8 × 8	0.952214
Şekil 3.2 (a)	16 × 16	0.936346

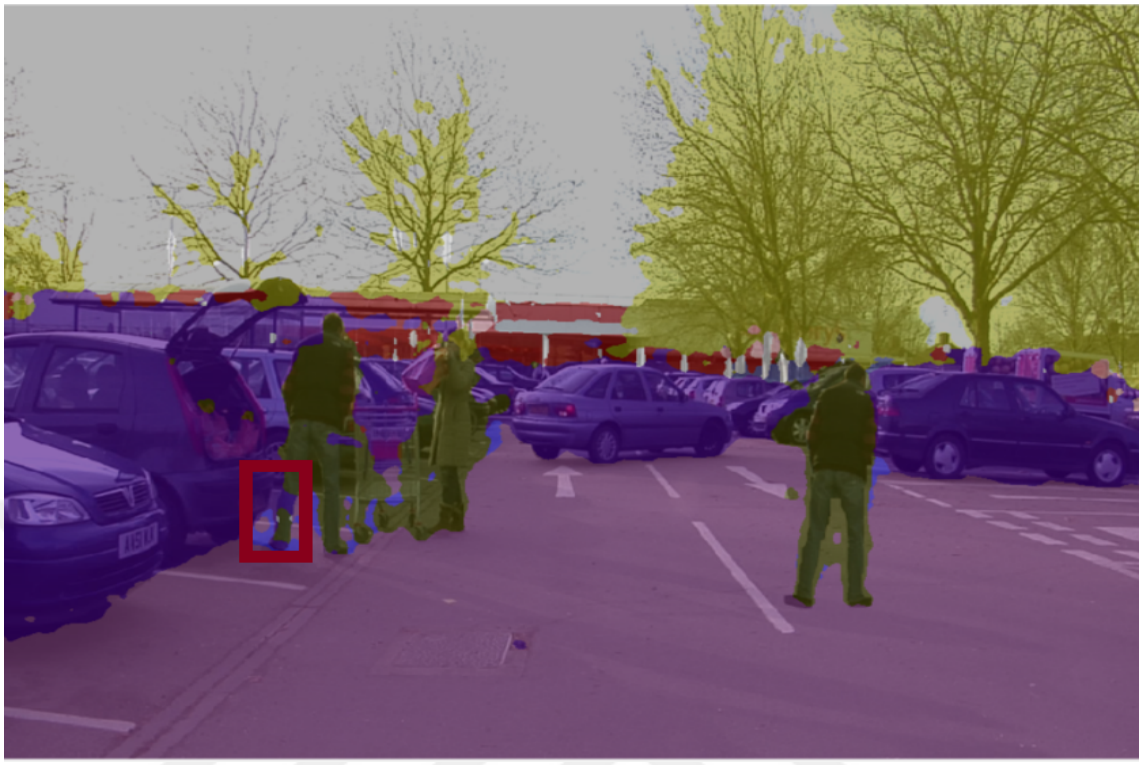
4. BÖLÜM

TARTIŞMA, SONUÇ ve ÖNERİLER

4.1. Tartışma

Önerilen yöntem de başarı temel olarak anlamsal olarak bölütlenmiş etiket bölgelerine bağlıdır. Eğer anlamsal bölütleme işlemi sınıfları doğru bir şekilde ayıramazsa, sahtecilik yapılan görüntü parçası farklı bir sınıf içerisine dahil edilebilmektedir. Bundan dolayı sahtecilik yapılan bölgeyi tespit etmesi imkânsız hale gelecektir. Şekil 4.1.'de görüldüğü üzere sahtecilik yapılmış insan görüntüsünün bacak kısmı yanlış anlamsal bölütleme sonucu araba sınıfı içinde değerlendirilmektedir. Bu da sonucumuzun tespit noktasındaki başarısını azaltacaktır.

Önerilen yöntemin kullanışlı olabilmesi için sahtecilik uygulanmış görüntü üzerinde farklı sınıfların olması gerekmektedir. Kopyala yapıştır sahteciliği uygulanmış Şekil 4.2.'de görüntü üzerinde anlamsal bölütleme yapabileceğimiz tek bir sınıf vardır. Önerilen yöntem de aynı etiket sınıfları içerisinde benzerlikleri araştıracağı için klasik yöntemlerle zaman ve sonuç performansı olarak benzer sonuçlar üretebilmektedir.



Şekil 4.1. Yanlış tespit edilen anlamsal bölütleme bölgesi.

Şekil 4.2. Kopyala yapıştır sahteciliği uygulanmış bir gökyüzü fotoğrafı.

4.2. Sonuç

Önerilen yöntem ile klasik blok temelli yaklaşımların belirli bir blok boyutu ile böldüğü görüntü üzerinde, kendisi dışındaki geriye kalan tüm bloklarla kıyaslama işlemini tamamen bitirmiştir. Anlamsal bölütleme sonucu, modelimiz içerisin de bulunan etiket sayısınca özellik matrisi oluşturup, kıyaslama işlemi her etiket sınıfı içerisinde gerçekleştirilmiştir. Çünkü basit bir şekilde uygulanan kopyala yapıştır sahteciliğinde, sahtecilik yapılan kaynak bölge ile hedef bölgenin aynı etiket sınıfları içerisinde yapıldığı görülmüştür. Yapılan çalışma ile kıyaslanacak bölgelerin, farklı etiket sınıfları içerisinde yapılmasının gereksiz olduğu, boşa yapılan her kıyaslamanın zaman maliyetini artırdığı gözlemlenmiştir. Aynı zaman da benzer değerler gösteren farklı bölgelerin filtreleme işlemi gerçekleştirilerek sonuç performansı artırılmıştır.

Tablo 3.3.'de önerilen yöntemin verdiği sonuçlar ile klasik yöntemlerin verdiği sonuçlar kıyaslanmıştır. Tez çalışması kapsamında deneylerden de anlaşılacağı üzere zaman ve performans açısından kullanışlı bir yöntem sunulmuştur. Alınan sonuçların hepsi 960x720 px boyutundaki görüntüler üzerinden gerçekleştirilmiştir. Önerilen yöntem blok temelli yaklaşımların zaman maliyetini yüzde kırk ile yüzde altmış arasında düşürdüğü ve başarı sonucunu artırdığı için kopyala yapıştır sahteciliği tespiti için kullanışlı bir duruma gelmiştir.

4.3. Gelecek Çalışmalar

Gelecek çalışmalarda anlamsal bölütleme başarısını artırmak için daha fazla kopyala yapıştır sahteciliği uygulanmış görüntüler ile yeni bir model eğitilecektir. Sınıflandırma işlemi için optimizasyon algoritmaları tercih edilebilir. Anlamsal bölütleme başarısı için farklı aktivasyon fonksiyonları ve modeller kullanılabilir. Blok temelli kopyala yapıştır sahteciliği tespiti için farklı öznitelik çıkarma yöntemlerine denenerek başarı artırımı gerçekleştirilebilir.

KAYNAKLAR

1. Farid, H., 2009. Image forgery detection, **IEEE Signal processing magazine**, **26**(2):16–25.

2. Meena, K.B. and Tyagi, V., 2019. Image forgery detection: survey and future directions, Data, Engineering and applications, 163–194, Springer.

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

4. Van Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F., 1994. A digital watermark, *Proceedings of 1st international conference on image processing*, volume 2, 86–90, IEEE.

5. Wolfgang, R.B. and Delp, E.J., 1996. A watermark for digital images, *Proceedings of 3rd IEEE International Conference on Image Processing*, volume 3, 219–222, IEEE.

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

7. Abdel-Aziz, B. and Chouinard, J.Y., 2003. On perceptual quality of watermarked images–an experimental approach, *International Workshop on Digital Watermarking*, 277–288, Springer.

8. Wang, S., Zheng, D., Zhao, J., Tam, W.J., and Speranza, F., 2006. An image quality evaluation method based on digital watermarking, **IEEE transactions on circuits and systems for video technology**, **17**(1):98–105.

9. Aslantas, V., Ozer, S., and Ozturk, S., 2009. Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms, **Optics Communications**, **282**(14):2806–2817.

10. Aslantas, V., 2009. An optimal robust digital image watermarking based on SVD using differential evolution algorithm, **Optics Communications**, **282**(5):769–777.

11. Aslantas, V., Ozer, S., and Ozturk, S., 2008. A novel fragile watermarking based on particle swarm optimization, *2008 IEEE International Conference on Multimedia and Expo*, 269–272, IEEE.

12. Murty, M.S., Veeraiah, D., and Rao, A.S., 2011. Digital signature and watermark methods for image authentication using cryptography analysis, **Signal & Image Processing: An International Journal (SIPIJ)**, **2**(2):170–179.

13. Luo, W., Huang, J., and Qiu, G., 2006. Robust detection of region-duplication forgery in digital image, *18th International Conference on Pattern Recognition (ICPR'06)*, volume 4, 746–749, IEEE.

14. Farid, H., 2009. Exposing digital forgeries from JPEG ghosts, **IEEE transactions on information forensics and security**, **4**(1):154–160.

15. Ramakrishna, M. and Shylaja, S., 2014. Is ORB Efficient Over SURF for Object Recognition?, **International Journal of Advanced Research in Computer Engineering and Technology**, **3**(8):2783–2788.

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

17. Liu, Y., Guan, Q., and Zhao, X., 2018. Copy-move forgery detection based on convolutional kernel network, **Multimedia Tools and Applications**, **77**(14):18269–18293.

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

19. Fridrich, A.J., Soukal, B.D., and Lukáš, A.J., 2003. Detection of copy-move forgery in digital images, *in Proceedings of Digital Forensic Research Workshop*, Citeseer.

20. Popescu, A.C. and Farid, H., 2004. Exposing digital forgeries by detecting duplicated image regions.

21. Kang, X. and Wei, S., 2008. Identifying tampered regions using singular value decomposition in digital image forensics, *2008 International conference on computer science and software engineering*, volume 3, 926–930, IEEE.

22. Ouyang, J., Liu, Y., and Liao, M., 2017. Copy-move forgery detection based on deep learning, *2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI)*, 1–5, IEEE.

23. Huang, Y., Lu, W., Sun, W., and Long, D., 2011. Improved DCT-based detection of copy-move forgery in images, **Forensic science international**, **206**(1-3):178–184.

24. Wandji, N.D. and Xingming, S., 2013. Robust detection of copy-move forgery in color images, *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV)*, 1, The Steering Committee of The World Congress in Computer Science, Computer ....

25. Kaur, R., 2013. Copy-Move Forgery Detection Utilizing Local Binary Patterns.

26. Kumar, S., Desai, J., and Mukherjee, S., 2015. Copy move forgery detection in contrast variant environment using binary DCT vectors, **International Journal of Image, Graphics and Signal Processing**, **7**(6):38.

27. Huang, H., Guo, W., and Zhang, Y., 2008. Detection of copy-move forgery in digital images using SIFT algorithm, *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, volume 2, 272–276, IEEE.

28. Pan, X. and Lyu, S., 2010. Detecting image region duplication using SIFT features, *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 1706–1709, IEEE.

29. Pan, X. and Lyu, S., 2010. Region duplication detection using image feature matching, **IEEE Transactions on Information Forensics and Security**, **5**(4):857–867.

30. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., and Serra, G., 2011. A sift-based forensic method for copy–move attack detection and transformation recovery, **IEEE transactions on information forensics and security**, **6**(3):1099–1110.

31. Jaberi, M., Bebis, G., Hussain, M., and Muhammad, G., 2013. Improving the detection and localization of duplicated regions in copy-move image forgery, *2013 18th international conference on digital signal processing (DSP)*, 1–6, IEEE.

32. Kiruthika, K., Mahalakshmi, S.D., and Vijayalakshmi, K., 2014. Detecting multiple copies of copy-move forgery based on SURF, **International Journal of Innovative Research in Science, Engineering and Technology**, **3**(3):2276–2281.

33. Zhu, Y., Shen, X., and Chen, H., 2016. Copy-move forgery detection based on scaled ORB, **Multimedia Tools and Applications**, **75**(6):3221–3233.

34. Wenchang, S., Fei, Z., Bo, Q., and Bin, L., 2016. Improving image copy-move forgery detection with particle swarm optimization techniques, **China Communications**, **13**(1):139–149.

35. Li, J., Li, X., Yang, B., and Sun, X., 2014. Segmentation-based image copy-move forgery detection scheme, **IEEE transactions on information forensics and security**, **10**(3):507–518.

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

37. Lin, C., Lu, W., Sun, W., Zeng, J., Xu, T., and Lai, J.H., 2018. Region duplication detection based on image segmentation and keypoint contexts, **Multimedia Tools and Applications**, **77**(11):14241–14258.

38. Zandi, M., Mahmoudi-Aznaveh, A., and Talebpour, A., 2016. Iterative copy-move forgery detection based on a new interest point detector, **IEEE Transactions on Information Forensics and Security**, **11**(11):2499–2512.

39. Wang, C., Zhang, Z., Li, Q., and Zhou, X., 2019. An image copy-move forgery detection method based on SURF and PCET, **IEEE Access**, **7**:170032–170047.

40. Wu, Y., Abd-Almageed, W., and Natarajan, P., 2018. Busternet: Detecting copy-move image forgery with source/target localization, *Proceedings of the European Conference on Computer Vision (ECCV)*, 168–184.

41. Elaskily, M.A., Alkinani, M.H., Sedik, A., and Dessouky, M.M., 2021. Deep learning based algorithm (ConvLSTM) for Copy Move Forgery Detection, **J. Intell. Fuzzy Syst.**, **40**:4385–4405.

42. ferhat kurt, 2018. EVRİŞİMLİ SİNİR AĞLARINDA HİPER PARAMETRELERİN ETKİSİNİN İNCELENMES, **Yüksek lisans tezi**.

43. Ian Goodfellow, Y.B. and Courville, A., 2016. Deep Learning, **Deep Learning, MIT press Cambridge.**

44. Zhang, Q., Zhang, M., Chen, T., Sun, Z., Ma, Y., and Yu, B., 2019. Recent advances in convolutional neural network acceleration, **Neurocomputing**, **323**:37–51.

45. Yasrab, R., Gu, N., and Zhang, X., 2016. SCNet: A simplified encoder-decoder CNN for semantic segmentation, *2016 5th International Conference on Computer Science and Network Technology (ICCSNT)*, 785–789, IEEE.

46. Noh, H., Hong, S., and Han, B., 2015. Learning deconvolution network for semantic segmentation, *Proceedings of the IEEE international conference on computer vision*, 1520–1528.

47. Fadl, S.M. and Semary, N.A., 2014. A proposed accelerated image copy-move forgery detection, *2014 IEEE Visual Communications and Image Processing Conference*, 253–257, IEEE.

48. Thoma, M., 2016. A survey of semantic segmentation, **arXiv preprint arXiv:1602.06541**.

49. May, M., 2002. DZUNG L. PHAM.

50. Chen, L.C., Zhu, Y., Papandreou, G., Schroff, F., and Adam, H., 2018. Encoder-decoder with atrous separable convolution for semantic image segmentation, *Proceedings of the European conference on computer vision (ECCV)*, 801–818.

51. Chen, L.C., Papandreou, G., Schroff, F., and Adam, H., 2017. Rethinking atrous convolution for semantic image segmentation, **arXiv preprint arXiv:1706.05587**.

52. Ahmed, N., Natarajan, T., and Rao, K.R., 1974. Discrete cosine transform, **IEEE transactions on Computers**, **100**(1):90–93.

53. Zhao, J. and Guo, J., 2013. Passive forensics for copy-move image forgery using a method based on DCT and SVD, **Forensic science international**, **233**(1-3):158–166.

54. Lin, H.J., Wang, C.W., Kao, Y.T., et al., 2009. Fast copy-move forgery detection, **WSEAS Transactions on Signal Processing**, **5**(5):188–197.

55. Wang, H. and Wang, H., 2018. Perceptual hashing-based image copy-move forgery detection, **Security and Communication Networks**, **2018**.

56. Davarzani, R., Yaghmaie, K., Mozaffari, S., and Tapak, M., 2013. Copy-move forgery detection using multiresolution local binary patterns, **Forensic science international**, **231**(1-3):61–72.

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

58. Chaitawittanun, N., 2012. Detection of copy-move forgery by clustering technique, *International Proceedings of Computer Science & Information Technology*, volume 50.

59. Yao, H., Qiao, T., Tang, Z., Zhao, Y., and Mao, H., 2011. Detecting copy-move forgery using non-negative matrix factorization, *2011 Third International*

Conference on Multimedia Information Networking and Security, 591–594, IEEE.

60. Nguyen, H.C. and Katzenbeisser, S., 2012. Detection of copy-move forgery in digital images using radon transformation and phase correlation, *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 134–137, IEEE.

61. Li, G., Wu, Q., Tu, D., and Sun, S., 2007. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, *2007 IEEE international conference on multimedia and expo*, 1750–1753, IEEE.

62. Heijmans, H.J., 1999. Connected morphological operators for binary images, **Computer Vision and Image Understanding**, **73**(1):99–120.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı, Soyadı	:	Abdurrahman Yavuz ASLANTAŞ
Uyruğu	:	Türkiye (T.C.)

EĞİTİM

Derece	**Kurum**	**Mezuniyet Yılı**
Yüksek Lisans	Erciyes Üniversitesi, KAYSERİ	2022
Lisans	Erciyes Üni. Müh. Fakültesi Bilgisayar Müh., Kayseri	2018

İŞ DENEYİMİ

Yıl	**Kurum**	**Görev**
2021-halen	Ahi Evran Üniversitesi Bilgisayar Mühendisliği, Kırşehir	Araştırma Görevlisi

YABANCI DİL

İngilizce

TEZ AŞAMASINDA YAPILAN YAYINLAR