



DİJİTAL GÖRÜNTÜLERDE KOPYALA TAŞI SAHTECİLİĞİ TESPİTİ

Ahmet BOZ

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

**GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

HAZİRAN 2016

Ahmet BOZ tarafından hazırlanan “DİJİTAL GÖRÜNTÜLERDE KOPYALA TAŞI SAHTECİLİĞİ TESPİTİ” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Hasan Şakir BİLGE

Elektrik Elektronik Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

Başkan: Doç. Dr. M. Fatih DEMİRCİ

Bilgisayar Mühendisliği, TOBB Ekonomi ve Teknoloji Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

Üye: Doç. Dr. Suat ÖZDEMİR

Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

Tez Savunma Tarihi: 08/06/2016

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....
Prof. Dr. Metin GÜRÜ
Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ahmet BOZ

08/06/2016

DİJİTAL GÖRÜNTÜLERDE KOPYALA TAŞI SAHTECİLİĞİ TESPİTİ
(Yüksek Lisans Tezi)

Ahmet BOZ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2016

ÖZET

Dijital görüntü işleme ve düzenleme yazılımlarındaki ilerlemeyle birlikte, dijital görüntülerin orijinalliğini bozarak sahtecilik yapmak kolay hale gelmiştir. Görüntülerin adli araştırmalarda veya diğer bazı alanlarda yasal bir kanıt olarak kullanılabileceği düşünüldüğünde, görüntü sahteciliğinin tespiti ve dijital görüntülerin bütünlüğünü ve özgünlüğünü doğrulamak için tekniklerin geliştirilmesi çok önemlidir. Kopyala taşı görüntü sahteciliği en çok kullanılan sahtecilik yöntemlerinden biridir. Bu çalışmada kopyala taşı sahteciliği tespiti için YİÖ (Yerel İkili Örüntü) ve AKD (Ayrık Kosinüs Dönüşümü) yöntemlerinin birlikte kullanımına dayalı bir yöntem önerilmiştir. Önerimizde öncelikle gri seviyeli görüntü sabit uzunluklu, birbiriyle örtüşen görüntü bloklarına ayrılmakta ve görüntü blokları YİÖ alanına dönüştürülmektedir. YİÖ alanına dönüştürülmüş görüntü bloklarına AKD uygulanarak görüntünün öznitelik matrisi elde edilmektedir. Elde edilen öznitelik matrisi leksikografik sıralanarak benzer görüntü bloklarının ardışık sıralanması sağlanır. YİÖ alanına dönüştürülmüş görüntü bloklarına AKD uygulanarak, değişen aydınlatma koşullarına daha az duyarlı yerel öznitelikler elde edilmesi ve yanlış pozitiflerin azaltılması amaçlanmıştır. Deneysel sonuçlar, YİÖ ve AKD birlikte kullanıldığında, ayrı ayrı kullanılmalarına göre, kopyala taşı görüntü sahteciliği tespitinde daha az yanlış pozitif değeri ile daha başarılı sonuç verdiğini göstermektedir.

Bilim Kodu : 92418
Anahtar Kelimeler : Görüntü Sahtecilik Tespiti, Kopyala Taşı Sahteciliği, AKD, YİÖ
Sayfa Adedi : 55
Danışman : Doç. Dr. Hasan Şakir BİLGE

COPY MOVE DIGITAL IMAGE FORGERY DETECTION

(M. Sc. Thesis)

Ahmet BOZ

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2016

ABSTRACT

With the advances in image processing and editing softwares, it has become easier to commit a forgery by damaging the originality of an image. Since images can be used as legal evidence in legal researches or some other areas, it is very important to develop some techniques to verify the integrity and authenticity of digital images and detect image forgery. Copy move image forgery is one of the most widely used method of image forgery. In this study, a copy move image forgery detection technique which uses LBP (Local Binary Pattern) and DCT (Discrete Cosine Transform) together is proposed. Firstly, the gray level image is divided into fixed-length overlapping blocks and each image block is converted into LBP domain in our proposal. We have derived the feature matrix of the image by applying DCT to the image blocks which are converted into LBP domain. We lexicographically sorted the feature matrix and after this step, similar image blocks are sequentially sorted. It is aimed to minimise the false positives and derive local features which are less sensitive to varying lighting conditions, by applying DCT to the image blocks which are converted into LBP domain. Experimental results show that when LBP and DCT are used together, better results are obtained in fewer false positives in comparison to individual usages of LBP and DCT in copy move image forgery detection.

Science Code : 92418

Key Words : Image Forgery Detection, Copy Move Forgery, DCT, LBP

Page Number : 55

Supervisor : Doç. Dr. Hasan Şakir BİLGE

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
İÇİNDEKİLER	vi
ÇİZELGELERİN LİSTESİ.....	viii
ŞEKİLLERİN LİSTESİ.....	ix
RESİMLERİN LİSTESİ	x
SİMGELER VE KISALTMALAR.....	xii
1. GİRİŞ.....	1
2. PASİF GÖRÜNTÜ SAHTECİLİK TESPİTİ TEKNİKLERİ	5
2.1. Piksel Tabanlı Teknikler	5
2.2. Format Tabanlı Teknikler	5
2.3. Kamera Tabanlı Teknikler	6
2.4. Fiziksel Çevre Tabanlı Teknikler	6
2.5. Geometri Tabanlı Teknikler.....	7
3. PİKSEL TABANLI GÖRÜNTÜ SAHTECİLİK TESPİTİ.....	9
3.1. Kopyala Taşı Sahtecilik Tespiti	9
3.2. Yeniden Örnekleme (Boyutlandırma, Döndürme vs.) Sahtecilik Tespiti.....	10
3.3. Birleştirme (Ekleme) Sahtecilik Tespiti.....	10
3.4. İstatistiksel Görüntü Sahtecilik Tespiti	10
4. KOPYALA TAŞI SAHTECİLİK TESPİTİ TEKNİKLERİ	13
4.1. Kopyala Taşı Görüntü Sahtecilik Tespiti Genel İş Akışı.....	13
4.2. Mevcut Blok Tabanlı Kopyala Taşı Görüntü Sahtecilik Tespiti Yöntemleri.....	17

	Sayfa
5. ÖZNİTELİK ÇIKARIM YÖNTEMLERİ	25
5.1. Ayrık Kosinüs Dönüşümü (AKD).....	25
5.2. Yerel İkili Örüntü (YİÖ).....	25
5.3. Gradyanların Histogramı (HOG)	26
6. ÖNERİLEN YÖNTEM	29
6.1. CoMoFoD – Kopyala Taşı Sahteciliği Tespiti İçin Görüntü Veri Tabanı	31
6.2. Parametre Ayarlama ve Algoritma Çıktısı.....	32
7. SONUÇ VE ÖNERİLER.....	49
KAYNAKLAR	51
ÖZGEÇMİŞ	55

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 4.1. Kopyala taşı görüntü sahtecilik tespiti genel algoritması	16
Çizelge 4.2. Kopyala taşı sahteciliği tespiti için önerilen blok tabanlı yöntemlerin karşılaştırmalı listesi	21
Çizelge 6.1. Önerilen yöneme ilişkin algoritma adımları	30
Çizelge 6.2. Önerilen yöntemin HOG, YİÖ ve AKD'nin ayrı ayrı kullanıldığı yöntemlerle karşılaştırmalı başarı sonuçları	33



ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 1.1. Pasif dijital görüntü sahtecilik tespiti tekniklerinin sınıflandırılması.....	2
Şekil 2.1. Piksel tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması	5
Şekil 2.2. Format tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması.....	6
Şekil 2.3. Kamera tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması.....	6
Şekil 2.4. Fiziksel çevre tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması	7
Şekil 2.5. Geometri tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması	7
Şekil 4.1. Kopyala taşı görüntü sahtecilik tespiti tekniklerinin genel iş akış şeması.....	14
Şekil 5.1. Farklı P ve R değerleri ile dairesel simetrik komşuluklar ($P=8$, $R=1$), ($P=16$, $R=2$), ($P=8$, $R=1$)	26
Şekil 6.1. Kopyala taşı sahteciliği tespiti için önerilen yöntemin blok diyagramı	29
Şekil 6.2. Blok büyüklüğüne bağlı doğruluk karşılaştırması	45
Şekil 6.3. Blok büyüklüğüne bağlı YPO karşılaştırması	46
Şekil 6.4. Blok büyüklüğüne bağlı YNO karşılaştırması.....	47
Şekil 6.5. Hesaplama zamanına göre karşılaştırma grafiği	48

RESİMLERİN LİSTESİ

Resim	Sayfa
Resim 3.1. Kopyala taşı sahteciliği örnek görüntü, (a) orijinal görüntü, (b) kopyala taşı sahteciliği uygulanmış görüntü	9
Resim 3.2. Birleştirme sahteciliği örnek görüntü, (a) birinci orijinal görüntü, (b) ikinci orijinal görüntü, (c) birleştirme sahteciliği ile oluşturulmuş görüntü	10
Resim 6.1. CoMoFoD veri tabanı örnek görüntü, (a) orijinal görüntü, (b) renkli maskeleme, (c) siyah-beyaz ikili maskeleme, (d) sahte görüntü	31
Resim 6.2. Algoritma çıktıları ($b = 8 \times 8$, $T_1 = 150$ ve $T_2 = 8$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi	35
Resim 6.3. Algoritma çıktıları ($b = 12 \times 12$, $T_1 = 50$ ve $T_2 = 12$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi	36
Resim 6.4. Algoritma çıktıları ($b = 16 \times 16$, $T_1 = 30$ ve $T_2 = 16$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi	38
Resim 6.5. Yanlış negatif oranı karşılaştırması için algoritma çıktıları ($b = 8 \times 8$, $T_1 = 150$ ve $T_2 = 8$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) yanlış negatiflerin gösterimi	40

- Resim 6.6. Önerilen yöntemin farklı blok büyüklükleri ile algoritma çıktıları, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) 4×4 blok büyüklüğü ile algoritma çıktısı, (g, h, i) 12×12 blok büyüklüğü ile algoritma çıktısı, (j, k, l) 20×20 blok büyüklüğü ile algoritma çıktısı, (d, g, j) algoritmanın tespit ettiği bölgeler, (e, h, k) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i, l) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri 42
- Resim 6.7. Önerilen yöntemin farklı blok büyüklükleri ile çıktıları, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) 8×8 blok büyüklüğü ile algoritma çıktısı, (g, h, i) 12×12 blok büyüklüğü ile algoritma çıktısı, (j, k, l) 16×16 blok büyüklüğü ile algoritma çıktısı, (d, g, j) algoritmanın tespit ettiği bölgeler, (e, h, k) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i, l) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri 43
- Resim 6.8. Önerilen yöntemin 8×8 blok büyüklüğü ve farklı T_1 parametre değeri ile algoritma çıktıları, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) $T_1 = 150$ ayarlanarak elde edilmiş algoritma çıktısı, (g, h, i) $T_1 = 30$ ayarlanarak elde edilmiş algoritma çıktısı, (d, g) algoritmanın tespit ettiği bölgeler, (e, h) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri 44

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

Açıklamalar

GHz

Giga Hertz

Kısaltmalar

Açıklamalar

ADD

Ayrık Dalgacık Dönüşümü

AKD

Ayrık Kosinüs Dönüşümü

CMFD

Copy Move Forgery Detection

CPU

Central Processing Unit

DCT

Discrete Cosine Transform

DN

Doğru Negatif

DP

Doğru Pozitif

HOG

Histogram of Gradient

İDD

İkili Dalgacık Dönüşümü

KKA

Kuantizasyon Katsayı Ayırışımı

LBP

Local Binary Pattern

PHD

Polar Harmonik Dönüşümü

PTD

Pozitif Tahmin Değeri

TBA

Temel Bileşen Analizi

TDA

Tekil Değer Ayırışımı

YİÖ

Yerel İkili Örüntü

YN

Yanlış Negatif

YNO

Yanlış Negatif Oranı

YP

Yanlış Pozitif

YPO

Yanlış Pozitif Oranı

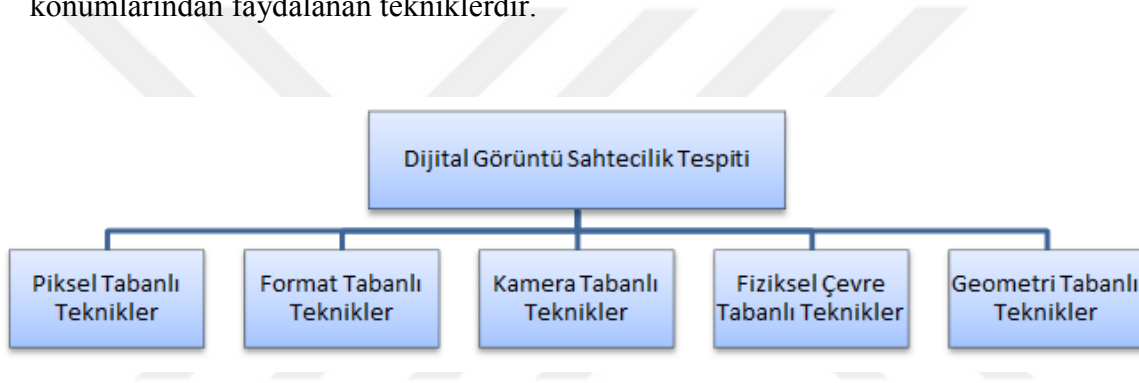
1. GİRİŞ

Sahtecilik insanoğlu için yeni değil, çok eski bir sorundur. Geçmişte sanat ve edebiyat ile sınırlıydı ve kamuoyunu etkilemezdi. Şu günlerde, güçlü görüntü işleme yazılımlarının kolay erişilebilirliği ve hızlı gelişimi ile görüntü işleme alanında çok bilgisi olmayan insanlar için bile görüntüler üzerinde oynamalar yapmak kolay hale gelmiştir. Bir görüntünün sahte olup olmadığını görsel olarak ayırmak insanoğlu için çok zordur. Özellikle görüntüler üzerinde yapılan bu oynamaların profesyonel kişilerce yapıldığı düşünüldüğünde, verilen bir görüntünün gerçekliğini çıplak gözle anlamak zor hatta çoğu zaman imkânsız olacaktır. İnternette ve yaygın olarak kullanılan medyada dijital sahtecilikte hızlı bir artış vardır. Bu eğilim, ciddi güvenlik açıkları gösterir ve dijital görüntülerin güvenilirliğini azaltır. Görüntülerin adli araştırmalarda veya diğer bazı alanlarda yasal bir kanıt olarak kullanılabileceği düşünüldüğünde görüntü sahteciliğinin tespiti ve dijital görüntülerin bütünlüğünü ve özgünlüğünü doğrulamak için teknikler geliştirilmesi çok önemlidir. Son yıllarda, dijital adli bilişim kavramı, dijital görüntülere olan güveni yeniden sağlamak için daha sık gündeme gelmiştir. Bu sebeple görüntü sahtecilik tespitinin birinci öncelikli hedefi görüntünün adli vakalarda kullanımınıdır [1].

Görüntülerin bütünlüğünü ve özgünlüğünü doğrulamak için birçok farklı yöntem olmasına rağmen genel olarak dijital görüntü sahtecilik tespiti teknikleri, aktif ve pasif teknikler olmak üzere sınıflandırılır. Aktif tekniklerde, dijital damgalama görüntüyü doğrulayabilecek bir araç olarak sunulmuştur [2, 3]. Bu yaklaşımda bir tür imza (damga, harici parmak izi) dijital bir görüntü içine gömülür ve gerçek imza test görüntüsünden alınan imza ile eşleştirilir. Eşleşme sağlanırsa özgünlüğü doğrulanır. Bu yaklaşımın bir dezavantajı, pratikte uygulanmasını sınırlayan, dijital görüntülere görüntü oluşum sırasında damga yerleştirme veya imza oluşturma gibi ön işlemleri gerektirmesidir [5]. Ne yazık ki bu donanımına sahip kameralar ve görüntü yakalama araçları çok azdır. Dijital görüntülerin özgünlüğünü doğrulamak için aktif yöntemlerin yetersizliği pasif tekniklere olan ihtiyacı doğurmuştur. Pasif yaklaşımda, aktif yaklaşımın aksine bunlara ihtiyaç yoktur.

Pasif teknikler, dijital görüntü sahteciliklerinin arkasında görüntünün değiştirildiğini gösteren hiçbir görsel ipucu bırakmamasına rağmen, bir görüntünün altında yatan istatistikleri değiştirdiği varsayımı ile çalışırlar. Pasif görüntü sahtecilik tespiti teknikleri Şekil 1.1’de gösterildiği gibi kabaca beş kategoriye ayrılabilir [4]. Bunlar;

- Pksel tabanlı teknikler: Pksel seviyesinde anormalliklerin tespitinden faydalanan tekniklerdir.
- Format tabanlı teknikler: Belirli bir kayıplı sıkıştırma şemasını kullanarak istatistiksel korelasyondan faydalanan görüntü formatı tabanlı tekniklerdir.
- Kamera tabanlı teknikler: Kamera lensi, algılayıcısı veya ön işlem çipi olarak bilinen kamera bileşenlerinden faydalanan kamera tabanlı tekniklerdir.
- Fiziksel tabanlı teknikler: Fiziksel nesneler, ışık ve kamera arasındaki üç boyutlu etkileşimden faydalanan anormallikleri tespit etmeye çalışan fiziksel tabanlı tekniklerdir.
- Geometrik tabanlı teknikler: Gerçek nesnelerin ölçümleri ve onların kameraya göre konumlarından faydalanan tekniklerdir.



Şekil 1.1. Pasif dijital görüntü sahtecilik tespiti tekniklerinin sınıflandırması

Kapsam

Bu çalışmada görüntü sahteciliği tespiti tekniklerinin her birini ayrı ayrı detaylı ele almak mümkün olmayacağından, çalışmanın kapsamında dijital görüntü sahteciliği tespiti pasif tekniklerine yer verilmektedir. Bu tekniklerin çalışma yöntem ve temelleri kısaca özetlenmektedir. Bu tekniklerden piksel tabanlı teknikler ayrıca detaylı ele alınarak bu yöntemlerle yapılabilecek sahteciliklere örnekler verilmektedir. Ayrıca piksel tabanlı tekniklerden olan kopyala taşı sahteciliği tespiti alanında önerilmiş yöntemler karşılaştırılarak ele alınmaktadır. Kopyala taşı görüntü sahteciliği alanında önerilmiş yöntemlerin genel iş akışı ve algoritma şemaları çıkarılarak işlem adımları özetlenmiştir. İncelenen yöntemlerin ışığında, kopyala taşı sahteciliği tespiti için ilk kez YİÖ ve AKD öznitelik çıkarım metotları birlikte kullanarak bir yöntem önerilmiştir. Önerilen yöntem CoMoFoD kopyala taşı sahteciliği veri tabanı üzerinde denenerek algoritma çıktıları verilmiş ve YİÖ, AKD ve HOG yöntemleri ile önerilen yöntemin başarı sonuçları

karşılaştırmalı olarak paylaşılmıştır.

Amaç

Literatürde kopyala taşı sahteciliği tespiti için önerilmiş yöntemler incelendiğinde çalışmalar arasındaki en temel farkın öznitelik çıkarım adımı yapıldığı görülmektedir. Bu adımda görüntüyü temsil eden güçlü özniteliklerin elde edilmesi yöntemlerin başarısını doğrudan etkileyecektir. YİÖ, yüz tanıma uygulamalarında sıklıkla kullanılan öznitelik çıkarım yöntemlerindendir. Bu yöntemle elde edilen yerel öznitelikler görüntünün dokusunu temsilinde güçlü ancak aydınlatma koşullarına karşı hassas olmasıyla bilinir. Biz de çalışmamızda kopyala taşı sahteciliği tespiti için önerdiğimiz yöntemde, YİÖ alanına çevrilmiş görüntü bloklarına AKD yöntemini uygulayarak aydınlatma koşullarına karşı daha az duyarlı yerel öznitelikler elde etmeyi ve güçlü öznitelikler ile görüntü temsilinde YİÖ ve AKD'nin ayrı ayrı kullanıldığı yöntemlere göre yanlış pozitif oranını azaltmayı amaçladık.

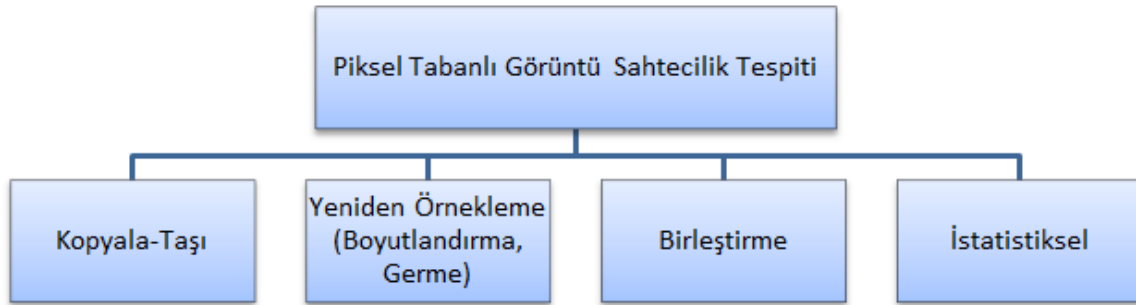
Çalışmanın devamı olarak Bölüm 2'de pasif görüntü sahtecilik tespiti tekniklerinin her birinden kısaca bahsedilmektedir. Bölüm 3'te piksel tabanlı görüntü sahtecilik tespitlerinden, Bölüm 4'te kopyala taşı sahteciliği tespitinde yapılmış çalışmalardan ve mevcut bazı yöntemlerden, Bölüm 5'te öznitelik çıkarım yöntemlerinden, Bölüm 6'da kopyala taşı sahteciliği tespiti için önerdiğimiz yöntemden ve deneysel çalışmalardan bahsedilmektedir. Son olarak Bölüm 7'de önerilen yöntemin sonuçları ve çalışmanın devamı için öneriler verilmiştir.

2. PASİF GÖRÜNTÜ SAHTECİLİK TESPİTİ TEKNİKLERİ

Bu teknikler sahtecilik tespiti için görüntü yakalama cihazlarının algılayıcı gürültüsü veya özel saptanabilir değişiklikler gibi çeşitli gerçek parmak izlerinden yararlanırlar. Bu tekniklerde yanlış pozitiflerin (gerçek bir resmin sahte olarak algılanması gibi) azaltılması, sistemin tam olarak otomatikleştirilmesi, sahteciliğin yer tespiti, farklı görüntü formatlarında sahtecilik tespiti ve sistemin güvenilirliğini ve güçlülüğünü artırma gibi birçok zorlukları vardır. Bu zorlukları aşmak için bu alanda yapılan çalışmalar belirli dallarda özeleşmişlerdir.

2.1. Piksel Tabanlı Teknikler

Dijital etki alanında, bir dijital görüntünün altında yatan yapı taşı piksellerdir. Piksel tabanlı teknikler dijital görüntünün pikselleri üzerinde detaylı çalışır. Bu teknikler kabaca dört tip olarak kategorize edilir. Bu yöntem çok sık kullanılan sahtecilik tespiti tekniklerindendir. Şekil 2.1’de piksel tabanlı sahtecilik tespiti teknikleri sınıflandırılmıştır.

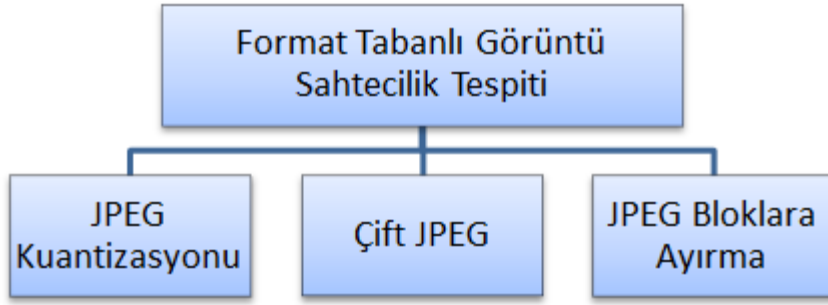


Şekil 2.1 Piksel tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırılması

2.2. Format Tabanlı Teknikler

Herhangi bir adli analizin ilk kuralı mutlaka "kanıt korumak" olmalıdır. Bu bağlamda, JPEG gibi kayıplı görüntü sıkıştırma programları adli analizin en büyük düşmanı olarak kabul edilebilir. Bu teknik görüntü formatlarına dayalıdır ve çoğunlukla JPEG formatında çalışır [1]. Şekil 2.2’de verildiği üzere bu teknik üç ayrı kategoriye ayrılabilir. Sıkıştırılmış bir görüntüde sahtecilik tespiti yapılması çok zordur ancak bu teknik sıkıştırılmış

görüntülerde bile çalışır.



Şekil 2.2. Format tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırması

2.3. Kamera Tabanlı Teknikler

Dijital bir kamerada görüntü aldığımızda, görüntü kamera algılayıcısından hafızaya taşınır ve sayısallaştırma, renk ilişkilendirmesi, zıtlık düzenlemesi, beyaz dengelemesi ve JPEG sıkıştırması gibi bir dizi işlem adımından geçer. Bu işlem adımları kamera modeli ve bileşenlerine bağlı olarak değişebilir. Bu teknik bu ilkeler üzerinde çalışır. Bu teknik Şekil 2.3'te gösterildiği üzere dört kategoriye ayrılabilir.



Şekil 2.3 Kamera tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırması

2.4. Fiziksel Çevre Tabanlı Teknikler

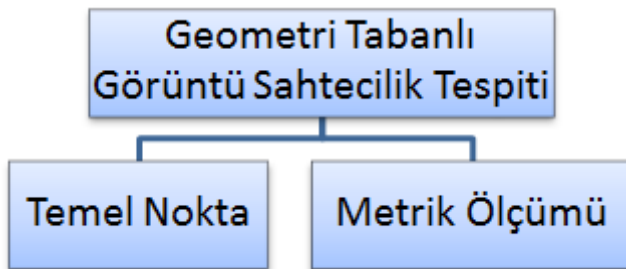
Aydınlatma bir görüntünün fotoğraflanabilmesi için çok önemlidir. İki farklı resmin birleştirilerek bir görüntü sahteciliği oluşturulurken her iki fotoğraftaki ışık efektlerini tam olarak eşleştirmek genellikle zordur. Dolayısıyla görüntüler arasındaki aydınlatma efektleri arasındaki farklar sahtecilik tespiti kanıtı için kullanılabilir [4]. Bu teknikler fotoğraflanmış görüntü veya nesnenin altındaki çevresel aydınlatma efektleri temeli üzerinde çalışır. Bu teknik Şekil 2.4'te görüldüğü üzere üç kategoriye ayrılabilir.



Şekil 2.4. Fiziksel çevre tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırması

2.5. Geometri Tabanlı Teknikler

Silahın namlusuna yapılan yivler, merminin dönme etkisi vererek daha uzun menzilli gitmesini ve hedefe daha doğru ilerlemesini sağlar. Ancak bu işaretler merminin üzerinde izler bırakır ve bu sebeple herhangi bir merminin hangi silahtan çıktığı bağlantısı kurulabilir. Aynı mantıkla, özellikle görüntüleme sürecinin çeşitli aşamalarında kullanılan modellerdeki yapay bozuklukların görüntü üzerinde bırakacakları izler temel alınarak çeşitli görüntü adli analiz teknikleri geliştirilmiştir [1]. Geometri tabanlı teknikler dünyadaki nesnelerin ölçümünü yapar ve kameraya göre konumlarını belirler. Bu teknikler Şekil 2.5'te görüleceği üzere iki kategoriye ayrılabilir.



Şekil 2.5. Geometri tabanlı görüntü sahtecilik tespiti tekniklerinin sınıflandırması



3. PİKSEL TABANLI GÖRÜNTÜ SAHTECİLİK TESPİTİ

Bir önceki bölümde de bahsedildiği gibi piksel tabanlı görüntü sahtecilik tespiti tekniklerinin kabaca dört kategoride incelenebileceğini söylemiştik. Bu teknikler görüntü değiştirmenin belirli bir formundan ortaya çıkan ve her biri doğrudan veya dolaylı olarak piksel seviyesinde korelasyon analizinden faydalanan yöntemlerdendir.

3.1. Kopyala Taşı Sahtecilik Tespiti

Görüntüde yer alan bir kişi veya nesneyi gizlemek için görüntünün bir bölümünden kopyalanarak gizlenecek nesnenin üzerine yapıştırılmasıyla veya görüntüdeki bazı nesneleri çoğaltmak için uygulanan, görüntü sahteciliğinde yaygın olarak kullanılan yöntemlerdendir. Resim 3.1’de kopyala taşı sahteciliğine örnek bir resim vardır.

Kopyalanmış parçanın renk ve dokusuyla bu parçanın yapıştırılacağı bölgenin renk ve dokusunun uyumlu olması durumunda bu iki parça arasında ayırım yapmak çok zordur. Aynı zamanda, aynı orijinal görüntüdeki iki veya daha fazla özdeş nesnelerin varlığı sahteciliğin tespitindeki zorluk seviyesine katkı sağlar. Çoğaltılmış bölge herhangi bir şekil, boyut ve konumda olabileceği için, görüntüde bütün olası yer ve boyutları aramak hesaplama açısından imkânsızdır. Bu yüzden mevcut kopyala-taşı sahtecilik tespiti yöntemlerinin çoğu, ya görüntünün blokları arasındaki benzerlik ölçümlerine ya da gürültü sapma ölçümlerine dayanmaktadır. Bu alanda yapılmış çalışmalardan sonraki bölümlerde detaylı anlatılacaktır.



Resim 3.1. Kopyala taşı sahteciliği örnek görüntü, (a) orijinal görüntü, (b) kopyala taşı sahteciliği uygulanmış görüntü [1]

3.2. Yeniden Örneklem (Boyutlandırma, Döndürme vs.) Sahtecilik Tespiti

İnandırıcı bir bileşik görüntü elde etmek için, genellikle yeniden boyutlandırma, döndürme, ya da bir görüntünün bazı kısımlarını genişletmek ya da uzatmak gibi işlemler yapılır. Örneğin, iki farklı görüntüden iki kişiyi birleştirirken, bir kişinin diğerine göre yüksekliğini eşleştirecek şekilde yeniden boyutlandırılması gerekebilir. Bu süreç komşu pikseller arasındaki belirli periyodik korelasyonu tanımlayan, yeni bir örnek düzlem üzerinde orijinal görüntüyü yeniden yapılandırmayı gerektirir. Çünkü bu korelasyonun doğal olarak ortaya çıkması muhtemel olmadığından, onların varlığı bu özel manipülasyonu tespit etmek için kullanılabilir [7-11].

3.3. Birleştirme (Ekleme) Sahtecilik Tespiti

Görüntü sahteciliğinin diğer bir yaygın kullanım formu olan birleştirme, iki veya daha fazla görüntünün dijital ortamda tek bir resimde birleştirilmiş olmasıdır [12]. Resim 3.2’de bu yöntemle yapılmış örnek bir görüntü mevcuttur. Özenle yapıldığında, birleştirilmiş bölgeler arasındaki sınırlar görsel olarak algılanamazlar. Buna rağmen, [13, 14] çalışmalarında yazarlar, iki farklı görüntüyü birleştirmenin, daha sonra birleştirmenin tespitinde kullanılacak, yüksek mertebeden Fourier istatistiklerini bozduğunu göstermektedir.



Resim 3.2. Birleştirme sahteciliği örnek görüntü, (a) birinci orijinal görüntü, (b) ikinci orijinal görüntü, (c) birleştirme sahteciliği ile oluşturulmuş görüntü [1]

3.4. İstatistiksel Görüntü Sahtecilik Tespiti

$n \times n$ ’lik boyutlarda toplamda 256^{n^2} olası 8 bitlik gri seviyeli görüntüler vardır. $n = 10$ olarak düşündüğümüzde 256^{100} gibi büyük bir rakam karşımıza çıkar. Eğer olası

görüntülerin bu büyük görüntü uzayından rastgele bir çizim yapsaydık, anlamlı bir görüntü elde etmek pek de mümkün olmazdı [4]. Bu gözlemler görüntülerin belirli istatistiksel özellikler içerdiğini göstermektedir. [15, 16, 17] numaralı kaynaklardaki çalışmalarında araştırmacılar, çeşitli görüntü sahteciliklerini tespit etmek için doğal görüntülerdeki istatistiksel düzenliliklerden istifade etmektedirler.





4. KOPYALA TAŞI SAHTECİLİK TESPİTİ TEKNİKLERİ

Kopyala taşı görüntü sahteciliği tespiti algoritmalarının birincil görevi, verilen bir resmin konum ve şekil ön bilgisi olmadan kopyalanmış bölgeleri içerip içermediğinin belirlenmesidir. Kopyala taşı sahteciliğinde kopyalanan kaynak bölge ve kopyalanan kısmın yapıştırıldığı hedef bölge aynı resim içerisindeydir. Bu yüzden çoğaltılmış bölgeler arasında renk sıcaklığı, aydınlatma koşulları ve gürültü değerleri gibi bazı özelliklerin iyi uyum sağlaması beklenir. Birçok kopyala taşı sahtecilik tespiti algoritması bu çıkarımdan faydalanır [6].

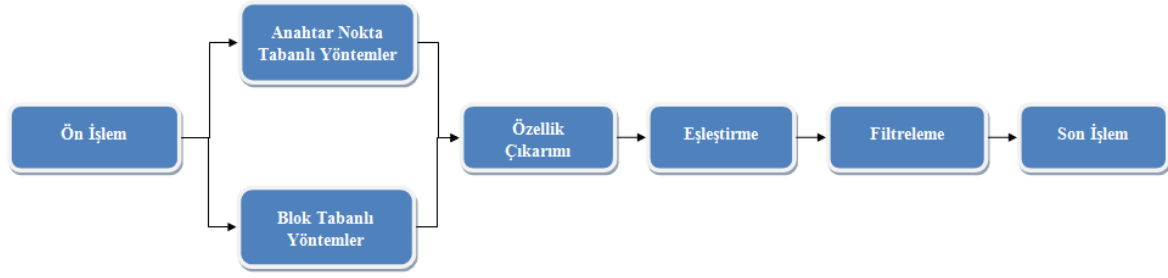
4.1. Kopyala Taşı Görüntü Sahtecilik Tespiti Genel İş Akışı

Görüntüde yer alan benzer bölgelerin tespiti için basit bir yaklaşım, olası her bölge çiftinin ayrıntılı karşılaştırılmasıdır. Ancak çoğaltılmış bölgelere ilişkin şekil, boyut ve konum bilgisi bilinmediğinden böyle bir yaklaşım oldukça karmaşıktır. Bu yüzden bu konuda daha etkin yaklaşımlara ihtiyaç vardır.

Önerilmiş çok sayıda kopyala-taşı sahtecilik tespiti yöntemi olmasına rağmen, bir çok yöntem Şekil 4.1’de verilen genel süreç akışını uygulamaktadır. Akışta da görüldüğü gibi, kopyala taşı sahteciliği tespiti için ön işlemden sonra iki ayrı alternatif mevcuttur: ya anahtar nokta tabanlı yöntemler ya da blok tabanlı yöntemler. Her iki yöntemde de ön işlem adımları uygulanır. Örneğin; birçok yöntem gri seviyeli görüntüler üzerinde çalışmakta ve bu yüzden renk kanalları birleştirilmelidir.

Öznitelik çıkarımı için blok tabanlı yöntemde, görüntü dikdörtgen biçiminde alt bloklara ayrılır [22-27, 29-35]. Her alt blok için öznitelik vektörleri hesaplanır. Benzer öznitelik vektörleri sonradan eşleştirilir. Buna karşılık anahtar nokta tabanlı yöntemlerde herhangi bir görüntü alt bölümü olmadan, sadece yüksek entropi değerine sahip görüntü bölgeleri belirlenir [18-20]. Bu bölgeler “anahtar nokta” olarak adlandırılır ve bu bölgelerin öznitelik vektörleri çıkarılır. Görüntüdeki benzer öznitelikler sonradan eşleştirilir. Hem anahtar nokta hem de blok tabanlı yöntemler sahte eşleşmeleri silmek için bir takım filtreleme uygularlar. Tespit edilen bölgelerdeki eşleşmeleri gruplamak amacıyla isteğe bağlı olarak ortak bir dönüşüm modelini takip eden bir son işlem adımı da

gerçekleştirilebilir.



Şekil 4.1. Kopyala taşı görüntü sahtecilik tespiti tekniklerinin genel iş akış şeması

Eşleştirme

İki öznitelik tanımlayıcısı arasındaki yüksek benzerlik bir çoğaltılmış bölge olabileceği ihtimali olarak yorumlanır. Blok tabanlı yöntemlerde, birçok araştırmacı benzer öznitelik vektörlerinin belirlenmesinde *leksikografik* sıralama kullanımı önerilmektedir [22-27]. *Leksikografik* sıralamada her öznitelik vektörü matris içinde bir satır olacak şekilde, öznitelik matrisi oluşturulur. Sonrasında bu matris satır bazlı sıralanır. Bu işlem çok benzer satır vektörlerinin ardışık sıralanmasını sağlar.

Diğer bazı araştırmacılar yaklaşık yakın komşuları belirlemek için kd-tree algoritmasıyla türetilen Best-Bin-First arama yöntemini kullanır [19, 20]. Özellikle anahtar nokta tabanlı yöntemler genellikle bu yaklaşımı kullanır. Kd-tree ile eşleme işlemi, nispeten verimli en yakın komşu aramayı sağlar. Tipik olarak, Öklid uzaklığı benzerlik ölçüsü olarak kullanılır. Yapılan bir çalışmada kd-tree eşleme kullanımının leksikografik sıralamadan daha iyi sonuçlar verdiği gösterilmiştir [28]. Ancak bu yaklaşımın bellek gereksinimi önemli ölçüde büyüktür.

Filtreleme

Filtreleme şemaları yanlış eşlemelerin olasılığını azaltmak için önerilmiştir. Örneğin, ortak bir gürültü azaltma ölçüsü, mekânsal yakın bölgeler arasındaki eşleşmeleri ortadan kaldırılmasını gerektirir. Açık mavi gökyüzünü içeren bir görüntüde gökyüzünün yer aldığı bölgeler yumuşak geçişlere sahiptir ve birbirine benzer bölgelerdir. Böyle bir görüntüde komşu pikseller genellikle yanlış sahtecilik tespitine yol açabilen benzer yoğunluklara sahiptir. Böylesi durumlarda yanlış eşlemeleri filtrelemek için farklı mesafe ölçütleri

önerilmiştir. Örneğin, birçok araştırmacı eşleştirilmiş öznitelik vektörleri arasındaki Öklid mesafesini önermişlerdir [25, 26]. Buna karşılık, benzerlik ölçütü olarak iki öznitelik vektörü arasındaki korelasyon katsayısını önerenler de olmuştur [21].

Son işlem

Bu son adımın amacı sadece ortak davranış gösteren eşleşmeleri korumaktır. Kopyalanan bölgeye ait eşleşmelerin bir kümesini düşünüldüğünde bu eşleşmelerin kaynak ve hedef blokların (veya anahtar noktaların) birbirine mekânsal yakın olması beklenir. Ayrıca, aynı kopyala-taşı eyleminden kaynaklanan eşleşmelerin, benzer miktarda çevirme, döndürme ve ölçeklendirme göstermesi beklenir. En yaygın kullanılan son işlem çeşidi, eşleşmeler arasında benzer kaydırma vektörlerinin sayısını en aza indirgeyerek aykırı değerleri ele alır [6]. Kaydırma vektörü, eşleştirilmiş iki öznitelik vektörü değerinin ait olduğu blokların başlangıç koordinatları farkını içerir. Döndürülmeden ve ölçeklendirilmeden kopyalanmış bölgelerin blokları düşünüldüğünde, eşleştirilmiş bloklara ait kaydırma vektörü frekanslarının diğer blok çiftlerinin kaydırma vektör frekanslarına göre yüksek olması beklenir [29, 30]. Diğer bazı araştırmacılar eşleştirilmiş çiftleri bağlamak ve uç değerleri çıkarmak için morfolojik işlemleri kullanmışlardır [20, 26, 27].

Önerilen yöntemlerin genelinde blok tabanlı ve anahtar nokta tabanlı yöntemlerin ikisinde de temel bahsedilen konulardan bir tanesi çıkarılan öznitelik vektör boyutu indirgeme işlemidir. Belirlenen blok sayısı (veya anahtar nokta sayısı) ve bunlara ait öznitelik vektör boyutu hesaplama karmaşıklığını ve önerilen yöntemin etkinliğini yüksek oranda etkilemektedir. Kopyala taşı sahteciliği tespiti için önerilmiş yöntemlerin ve genel iş akışının özeti olarak Çizelge 4.1’de ki algoritma adımları verilmiştir.

Çizelge 4.1. Kopyala taşı görüntü sahtecilik tespiti genel algoritması

-
- 1) Verilen görüntü gri seviyesine dönüştürülür (İstisna: [21, 31, 32] öznitelik çıkarımı için bütün renk kanalları kullanılmıştır).
 - 1) Blok tabanlı yöntemler için;
 - a. Görüntüyü $b \times b$ boyutlarında, $0 \leq i < ((M - b + 1) \cdot (N - b + 1))$ olacak şekilde birbiri ile örtüşen B_i bloklarına böl.
 - b. Her B_i bloğu için $\vec{f}_i$ öznitelik vektörü hesaplanır.
 Anahtar tabanlı yöntemler için;
 - a. Anahtar noktalar için görüntüyü tara (yüksek entropi değerine sahip merkezi noktalar).
 - b. Her anahtar nokta için $\vec{f}_i$ öznitelik vektörünü hesapla. Bu iki adım SIFT ve SURF gibi anahtar nokta çıkarma algoritmalarında birleştirilmiştir.
 - 2) Her öznitelik vektörü için benzer en yakın komşularını arayarak eşleştir.
 - a. i ve j öznitelik vektör indislerini gösterecek ve $i \neq j$ olacak şekilde, her $\vec{f}_i$ ve $\vec{f}_j$ öznitelik vektörü için F_{ij} öznitelik vektör çiftlerini belirle.
 - b. $c(\vec{f}_i)$, $\vec{f}_i$ öznitelik vektörünün çıkarıldığı blok ya da anahtar noktanın başlangıç koordinat değerlerini gösterecek. Belirlenen her öznitelik vektör çifti için $c(\vec{f}_i)$ ve $c(\vec{f}_j)$ koordinat çiftleri arasında $\vec{v}_{ij}$ “kaydırma vektörü” hesapla.
 - 3) $\|\cdot\|_2$ Öklid uzaklığını ifade edecek ve T_1 belirli bir eşik değer olacak şekilde, $\|\vec{v}_{ij}\|_2 < T_1$ koşulunu sağlayan F_{ij} çiftleri sil.
 - 2) Kaydırma vektör frekansları hesaplanır ve T_2 eşik değerinden daha az frekansa sahip çiftleri sil.
 - 4) Ortak bir desene bağlı kalan eşleşmeleri kümele.
 - a. Eğer görüntü T_3 eşik değerinden fazla bağlı bölge içeriyor ise kopyala taşı sahteciliği uygulanmıştır ve 5. adıma geç.
 - b. Eğer görüntü T_3 eşik değerinden daha az bağlı bölge içeriyor veya hiç içermiyor ise kopyala taşı sahteciliği uygulanmamıştır, algoritmayı sonlandır.
 - 5) Geriye kalan kaydırma vektör listesi ilişkili blokları görüntüde çoğaltılmış bölgeleri gösterecek şekilde işaretlenir.
-

4.2. Mevcut Blok Tabanlı Kopyala Taşı Görüntü Sahtecilik Tespiti Yöntemleri

Fridrich, Soukal ve Lukas [22], kopyala taşı görüntü sahteciliği tespiti için 2003'te bir yöntem önermişlerdir. Bu yöntemde, görüntü öznitelik vektör çıkarımı için üst üste örtüşen (16×16) bloklara ayrılmıştır. Öneride öznitelik vektörü çıkarımı için AKD katsayıları kullanılmıştır. Her blok için elde edilen öznitelik vektörlerinden öznitelik matrisi elde edilir. Daha sonra öznitelik matrisi satır temelli alfabetik olarak sıralanır. Sıralama sonrası benzer bloklar ardışık dizilirler ve kopyala taşı yöntemiyle değiştirilmiş bölgeler bulunur.

Popescu ve Farid [9], 2004'te görüntüde kopyala taşı ile çoğaltılmış bölgelerin tespiti için bir yöntem önermişlerdir. Araştırmacılar bu yöntemde, görüntüyü böldükleri küçük sabit boyutlu görüntü alt bloklarına $(16 \times 16, 32 \times 32)$ TBA (Temel Bileşen Analizi)'yı uygulayarak öznitelik matrislerini elde etmişlerdir. Her bloğa ait elde ettikleri öznitelik vektörlerinden ve her bloğun başlangıç indislerini tutan değerlerle bir matris elde etmişlerdir ve bu matrisi alfabetik olarak sıralamışlardır. Sıralama sonrası benzer bloklar ardışık sıralanmış ve çoğaltılmış bölgeler otomatik olarak belirlenmiştir. Bu algoritmanın avantajı görüntü sıkıştırılmış veya gürültülü bile olsa çoğaltılmış bölgeleri bulma yeteneğidir.

Luo, Huang ve Qiu [31], 2006 yılında kopyala taşı görüntü sahteciliğine karşı blok tabanlı güçlü bir yöntem önermişlerdir. Araştırmacılar renkli görüntüyü $b \times b$ 'lik sabit boyutlu alt bloklara bölmüşlerdir ve her blok için yedi karakteristik öznitelik çıkarmışlardır. Çıkarılan ilk üç öznitelik sırasıyla kırmızı, yeşil ve mavi renk bileşenleri ortalamasıdır. Diğer dört öznitelik ise Y ($Y = 0.299R + 0.587G + 0.114B$) kanalında görüntü bloklarını yatay, dikey ve iki çapraz köşeden eşit parçalara bölerek elde edilen birinci parçanın piksel değerleri toplamının, bloktaki toplam piksel değerlerine oranı ile elde edilen değerler olarak belirlenmiştir. Önerilen algoritma hesaplama karmaşıklığı açısından etkin ve JPEG sıkıştırmaları ve gürültülü görüntülere karşı güçlüdür.

Li, Wu, Tu ve Sun [24], 2007 yılında sıralı komşu yöntemi ile görüntülerde çoğaltılmış bölgelerin tespiti için blok tabanlı bir yöntem önermişlerdir. Araştırmacılar gri seviyeli görüntü üzerinde öncelikle ADD (Ayrık Dalgacık Dönüşümü) uygulayarak elde ettikleri düşük frekanslı alt bant görüntüyü $b \times a$ boyutlu birbiriyle örtüşen bloklara bölmüşlerdir. Elde edilen bloklarda öznitelik vektör çıkarımı için TDA (Tekil Değer Ayırımı)

kullanılmıştır. Her blok için elde edilen $\min(a, b)$ uzunluklu vektörler ile öznitelik matrisi oluşturulmuş ve satır bazlı leksikografik olarak sıralanmıştır. Sıralama sonrası birbirine benzeyen görüntü blokları ardışık sıralanmışlardır. Araştırmacılar yanlış tespit oranını azaltmak için sıralı komşu bloklar arasında belirli sayıda komşuluk oranına bakarak kaydırma vektörü hesaplarlar. Belirli bir eşik değerinden büyük frekansa sahip kaydırma vektörü ilişkili bloklar sahtecilik tespiti için işaretlenir.

Kang ve Wei [23], 2008 yılında dijital görüntüde çoğaltılmış bölgeleri tanımlamak için TDA kullanımını önermişlerdir. Bu çalışmada araştırmacılar, birbiriyle örtüşen bloklara ayrılmış görüntüde öznitelik vektörü çıkarımı için ve görüntü boyut azaltma işlemi için TDA kullanmışlardır. Leksikografik sıralama satır vektörleri üzerinde uygulanır ve benzer blokların ardışık sıralanması sağlanır. Sonrasında bölge büyütme algoritması ile çoğaltılmış bölgeleri içeren blokların ilişkilendirilmesi sağlanmıştır.

Lin, Wang ve Kao [38], 2009 yılında hızlı bir kopyala taşı sahteciliği tespiti tekniği önermişlerdir. Bu çalışmada araştırmacılar, birbiriyle örtüşen görüntü blokları üzerinde öznitelik vektörü çıkarımı ve görüntü boyutu indirgeme işlemleri için TBA kullanmışlardır. Elde ettikleri öznitelik matrisi Radix sıralaması ile sıralanmıştır. Sıralanmış ardışık satır vektörleri için kaydırma vektörü hesaplanmıştır ve yüksek frekansa sahip kaydırma vektörü ilişkili blokları sahtecilik için işaretlenmiştir. Bu algoritma gürültülü ve sıkıştırılmış görüntüler üzerinde iyi çalışır.

Zhang, Feng ve Su [27], 2008 yılında görüntülerde kopyala taşı sahteciliği tespiti için yeni bir yaklaşım önermişlerdir. Araştırmacılar ADD kullanarak görüntüyü düşük frekanslı dört alt banda bölerler ve faz bağıntısını kopyala taşı bölgeleri arasındaki uzaysal karşılıklarını hesaplamak için kullanırlar. Daha sonra çoğaltılmış bölgelerin tespiti için piksel eşleştirme kullanılır. Yüksek sıkıştırılmış görüntüler üzerinde iyi çalışan ve düşük hesaplama karmaşıklığına sahip güçlü bir yöntemdir.

Kang ve Cheng [39] kopyala taşı sahteciliği için 2010 yılında TDA kullandıkları bir yöntem önerdiler. Görüntü alt bloklara ayrılır ve alfabetik olarak sıralanmış öznitelik matrisi üzerinde benzerlik eşleştirmesi uygulanır ve çoğaltılmış bölgeler tespit edilir.

Ghorbani, Firouzmand ve Faraahi [30], 2011 yılında ADD-AKD tabanlı bir kopyala taşı

sahteciliği tespiti yöntemi önermişlerdir. Araştırmacılar görüntüyü alt bantlara ayırmak için ADD kullanırlar. Elde ettikleri düşük frekanslı alt bant görüntüyü birbiriyle örtüşen bloklara ayırırlar. Her blok için öznitelik vektör boyutunu indirgemek için AKD-KKA (Kuantizasyon Katsayı Ayırımı) kullanırlar. Satır vektörleri leksikografik sıralanır ve ardışık satır vektörleri arasında kaydırma vektörü hesaplanır. Son olarak kaydırma vektörü eşik değeri ile karşılaştırılarak çoğaltılmış bölge bulunur.

Huagn, Lu, Sun ve Long [40], 2011 yılında gelişmiş AKD tabanlı kopyala taşı görüntü sahteciliği tespiti yöntemi önermişlerdir. Araştırmacılar görüntüyü sabit boyutlu birbiriyle örtüşen alt bloklara böldükten sonra öznitelik vektörünü bulmak için AKD kullanmışlardır. Ancak AKD için zig-zag yöntemini uygulayarak öznitelik vektörü boyutunu indirgemişlerdir. Sonra öznitelik matrisi leksikografik sıralanmış ve benzer bloklar ardışık dizilmişlerdir. Ardışık satır vektörleri için kaydırma vektörü hesaplanarak çoğaltılmış bölgeler tespit edilir.

Muhammad, Hussain, Khawaji ve Bebis [33], 2011 yılında İDD (İkili Dalgacık Dönüşümü) kullanılarak kopyala taşı görüntü sahteciliği tespiti yöntemi önermişlerdir. İlk olarak girdi görüntüsünü birinci seviye düşük frekanslı (LL1) ve yüksek frekanslı (HH1) alt bantlara ayrılmıştır. Sonra LL1 ve HH1 alt bantlarını üst üste örtüşen bloklara ayrılarak bloklar arasındaki benzerlik ölçülmüştür. Ana fikir, taşınan bölgedeki gürültüdeki tutarsızlıktan dolayı HH1 alt bandında kopyalanıp taşınan bölgeler arasındaki benzerlik düşük olması gerekirken, LL1 bandından kopyalanıp taşınan bölgeler arasındaki benzerlik yüksek olmalı fikrini benimsemişlerdir. Blok çiftlerini LL1 alt bandında yüksek benzerlik oranına göre, HH1 alt bandında düşük benzerlik oranına göre sıralamışlardır. Kopyalanıp taşınmış bölgelerin sıralanmış listesinden eşik değeri kullanılarak eşleşmiş çiftler elde edilmiştir.

Cao, Gao ve Yang [41], 2012 yılında kopyala taşı sahteciliği tespiti için güçlü bir algoritma önermişlerdir. Araştırmacılar görüntüyü örtüşen bloklara böldükten sonra öznitelik çıkarımı için AKD kullanmışlardır. Çıkarılan öznitelik vektörü boyutunu indirgemek için hesaplanmış AKD katsayıları dairesel bloklar şeklinde gösterimle ifade edilmiş ve dört öznitelik çıkarılmıştır. Elde edilen öznitelik matrisi leksikografik sıralandıktan sonra ardışık satır vektörleri arasında kaydırma vektörü hesaplanmış ve benzer blok çiftleri aranarak sahte bölgeler tespit edilmiştir.

Ketenci ve Ulutas [34], 2013 yılında kopyala taşı sahteciliği tespiti için blok tabanlı bir yöntem önermişlerdir. Araştırmacılar görüntüyü birbiriyle örtüşen bloklara ayırmadan önce 5x5 pencere ile ortalama filtre yöntemini kullanarak görüntüyü düzgünleştirmişlerdir. Bu işlemde sonra görüntü bloklara ayrılarak 2D-Fourier Dönüşümü uygulanarak öznitelik vektörleri çıkarılmıştır. Sonrasında leksikografik sıralanan öznitelik matrisinde ardışık satır vektörlerindeki benzer bloklar eşleştirilmiştir.

Wandji ve Xingming [32], 2013 yılında renkli görüntüler için kopyala taşı görüntü sahteciliği tespiti yöntemi önermişlerdir. Araştırmacılar çalışmalarında görüntüyü bloklara böldükten sonra her blok için öznitelik vektörü hesaplamaktadırlar. Her satır vektörü on öznitelik içermektedir. İlk öznitelik değeri YUV renk uzayına dönüştürülen görüntüden elde edilen ortalama Y bileşeni, diğer dokuz öznitelik ise her R, G ve B renk kanalları için gri seviye ortalaması, ortalama zıtlık ve moment değerleri hesaplanarak elde edilmiştir. Öznitelik matrisi elde edildikten sonra leksikografik sıralanan matrisin satır vektörleri karşılaştırılarak benzer bloklar çıkarılmıştır.

L. Li , S. Li, Zhu ve Wu [35], 2014 yılında kopyala taşı görüntü sahteciliği tespiti yöntemi önermişlerdir. Araştırmacılar ilk olarak görüntüyü gri seviyesine dönüştürdükten sonra, dairesel birbiriyle örtüşen bloklara ayırmışlardır. Sonra her bloğa PHD (Polar Harmonik Dönüşümü) uygulanarak öznitelik vektörleri çıkarılmıştır. Elde edilen öznitelik matrisi leksikografik sıralanarak ardışık satır vektörlerinden birbiriyle benzer olanlar eşleştirilmiştir.

Kaur [36], 2014 yılında kopyala taşı sahteciliği için bir yöntem önermiştir. Önerilen yöntemde görüntü renk kanalları birleştirilerek gri seviyeli görüntü birbiriyle örtüşen bloklara bölünür. Her blok için YİÖ (Yerel İkili Örüntü) yöntemi kullanılarak öznitelik vektörleri çıkarılır. Öznitelik vektörlerinden oluşturulan öznitelik matrisi satır bazlı leksikografik olarak sıralanır ve Öklid uzaklığı yöntemi kullanılarak benzer bloklar eşleştirilir.

Kumar, Desai ve Mukherjee [37], 2015 yılında önerilen kopyala taşı sahteciliği tespiti yönteminde görüntü renk kanalları birleştirilerek gri seviyeli görüntü elde edilir. Gri seviyeli görüntü örtüşen bloklara bölündükten sonra her blok için AKD kullanılarak öznitelik vektörleri çıkarılır. Çıkarılan öznitelik vektör katsayıları ikili AKD katsayılarına

dönüştürülür. Elde edilen öznitelik matrisi satır bazlı leksikografik olarak sıralanır ve benzer bloklar eşleştirilir. Yanlış eşleştirmeleri azaltmak için belirli morfolojik işlemler uygulanır. Önerilen yöntemin JPEG sıkıştırmaları, bulanıklaştırma ve küçük ölçekli döndürmelere karşı dayanıklı olduğu söylenmektedir.

Lee, Chang ve Chen [45], 2015 yılında önerdikleri yöntemde, gri seviyeli görüntüyü birbiriyle örtüşen bloklara ayırdıktan sonra her görüntü bloğuna HOG (Gradyanların Histogramı) uygulayarak öznitelik vektörünü elde etmişlerdir. Elde ettikleri öznitelik vektörlerinden oluşan öznitelik matrisini leksikografik sırladıktan sonra benzer bloklar ardışık sıralanır. Yanlış eşleşmeleri elemek için son işlem adımında 16x16 blok büyüklüklü bir pencere ile görüntü üzerinde gezerek pencere içerisinde belirli bir eşikten az sayıda eşleşen noktalar yanlış pozitif olarak varsayılır ve silinir.

İncelenen blok tabanlı kopyala taşı sahteciliği tespiti önerileri tablo halinde aşağıda Çizelge 4.2’de verilmiştir.

Çizelge 4.2. Kopyala taşı sahteciliği tespiti için önerilen blok tabanlı yöntemlerin karşılaştırmalı listesi

Yazarlar	Kullanılan Yöntem	Artıları	Eksileri	Yayın Yılı
Fridrich, Soukal, ve Lukas [22]	AKD	Alanında yapılmış ilk çalışmalardan olması açısından önemli bir başlangıç noktası	Gürültülü ve sıkıştırılmış görüntülerde başarısı düşüktür	2003
Popescu ve Farid [9]	TBA	Sıkıştırılmış görüntülerde başarısı düşük olsa da çalışabilmektedir	Zaman karmaşıklığı yüksek	2004
Luo, Huang ve Qiu [31]	Benzer Blok Eşleştirme	JPEG sıkıştırmaları ve gürültülü görüntülere karşı güçlüdür	-	2006

Çizelge 4.2. (devam) Kopyala taşı sahteciliği tespiti için önerilen blok tabanlı yöntemlerin karşılaştırmalı listesi

Li, Wu, Tu ve Sun [24]	ADD-TDA	Çoğaltılmış bölgelerin tespitinde etkin ve hesaplama zamanı açısından önceki diğer çalışmalar [9] ve [22]'ye göre daha iyi, ayrıca hem renkli hem de gri seviyeli görüntüler üzerinde çalışır	Yüksek sıkıştırılmış görüntüler üzerinde etkin olduğu söylene de başarı sonuçları verilmemiştir	2007
Kang ve Wei [23]	TDA	Renkli, sıkıştırılmış ve gürültülü görüntülerde çalışır, hesaplama karmaşıklığı iyi	Yüksek gürültülü ve yüksek sıkıştırma oranına sahip görüntülerde çalışmaz	2008
Zhang, Feng ve Su [27]	ADD ve faz bağıntısı	Yüksek sıkıştırılmış görüntüler üzerinde iyi çalışan etkin bir yöntem	Yanlış eşleşmeleri morfolojik işlemler ile siler ve bu işlem karmaşıklığı artırır	2008
Lin, Wang ve Kao [38]	İyileştirilmiş TBA, Radix sıralama	Gürültü ekleme, JPEG sıkıştırması ve döndürme ataklarına karşı başarılı	Küçük kopyala taşı görüntü bloklarında çalışmaz	2009
Kang ve Cheng [39]	TDA	Gürültülü görüntülerde başarısı düşük olsa da çalışabilir	JPEG sıkıştırma, döndürme gibi bazı ataklara karşı düşük başarı	2010
Ghorbani, Firouzmand ve Faraahi [30]	ADD-AKD	Fridrich [22], Li [24] ve Zimba [29]'nın çalışmalarında göre öznelitektör boyutu daha küçük veya aynı	Yüksek sıkıştırma oranına sahip görüntülerde çalışmaz	2011

Çizelge 4.2. (devam) Kopyala taşı sahteciliği tespiti için önerilen blok tabanlı yöntemlerin karşılaştırmalı listesi

Huagn, Lu, Sun ve Long [40]	AKD	Sıkıştırılmış, bulanıklaştırılmış ve gürültü eklenmiş görüntüler üzerinde başarılı	Düzgün çoğaltılmamış görüntü bloklarının olduğu sahte görüntülerde, kopyala taşı sahteciliği uygulanmış alanın tamamını bulmada başarısı düşük	2011
Muhammad, Hussain, Khawaji ve Bebis [33]	İDD	Li ve arkadaşlarının [24] önerdiği yönteme göre daha yüksek başarı oranı elde edilmiştir	Hesaplama maliyeti yüksek ve JPEG sıkıştırması ve gürültü ekleme gibi bazı ataklara karşı zayıf	2011
Cao, Gao ve Yang [41]	AKD	Fridrich [22], Popescu [9] ve Huang [40]'ın çalışmalarına göre daha küçük öznitelik vektör uzunluğuna sahip ve gürültülü ve bulanıklaştırılmış görüntüler üzerinde başarılı sonuç verir	Gökyüzü gibi yumuşak renk geçişlerine sahip görüntülerde yanlış pozitif oranı yüksek	2012
Ketenci ve Ulutas [34]	2D-Fourier Dönüşümü	Görüntü bulanıklaştırılmış ve sıkıştırılmış bile olsa çalışmaktadır, ayrıca önceki birçok çalışmaya göre etkinliği yüksektir	Birden fazla kopyala taşı sahteciliği ile çoğaltılmış görüntü bloklarında başarısı düşüktür	2013

Çizelge 4.2. (devam) Kopyala taşı sahteciliği tespiti için önerilen blok tabanlı yöntemlerin karşılaştırmalı listesi

Wandji ve Xingming [32]	YUV renk uzayı, Benzer blok eşleştirme	Renkli görüntüler üzerinde ve düşük JPEG sıkıştırılmalarında, bulanıklaştırma ve gürültülü görüntülerde çalışabilir	Her renk kanalı için işlemleri tekrar ettiği için hesaplama maliyeti yüksek, düzgün çoğaltılmamış görüntü bloklarında yanlış negatif oranı yüksek	2013
L. Li, S. Li, Zhu ve Wu [35]	PHD	Ölçeklendirilmiş ve döndürülmüş kopyala taşı sahteciliği için güçlü yöntem	Morfolojik işlemlerle yanlış eşleşmeler silinmiştir	2014
Kaur [36]	YİÖ	Çoğaltılmış bölgelerin tam olarak algılanmasına karşı güçlü	Döndürme ve ölçeklendirme gibi ataklara karşı zayıf	2014
Kumar, Desai ve Mukherjee [37]	İkili AKD	Kontrast değişimi atağına karşı güçlü aynı zamanda gürültü eklenmiş ve JPEG sıkıştırması uygulanmış görüntülerde de çalışmakta	Ölçeklendirme ve döndürme gibi ataklara karşı zayıf	2015
Lee, Chang ve Chen [45]	HOG	Küçük ölçekli döndürme, renk indirgeme ve zıtlık değiştirme gibi ataklara karşı güçlü ve yüksek doğruluk oranına sahip, ayrıca önceki birçok çalışmaya göre küçük öznitelik vektör boyutu ile hesaplama maliyeti açısından daha etkin	Büyük ölçekli döndürme, JPEG sıkıştırma ve ölçeklendirme gibi ataklara karşı geliştirilmesi ve iyileştirilmesi gerekli	2015

5. ÖZİNİTELİK ÇIKARIM YÖNTEMLERİ

Literatürde sunulan birçok özinitelik çıkarım yöntemi olmasına rağmen, incelenen çalışmalarda öne çıkan ve önerilen yöntemde kullanılan özinitelik çıkarım yöntemleri bu bölümde anlatılmıştır.

5.1. Ayrık Kosinüs Dönüşümü (AKD)

AKD görüntü işleme uygulamalarında, özinitelik çıkarımı için yaygın kullanılan dönüşüm tekniğidir. Yaklaşım görüntünün bir bütün olarak alınarak amaca uygun frekans katsayılarına dönüşümünü içerir. Bununla birlikte enerji sıkıştırması gerçekleştirerek, görüntüyü daha az veriyle ifade etmeyi amaçlar. Bir görüntünün AKD katsayıları, her biri görüntünün bazı detay ve bilgilerini içeren orta, düşük ve yüksek frekans değerlerinden oluşur. Düşük frekans, genel olarak bir görüntünün ortalama yoğunluğunu içerir. Görüntüyü ifade eden AKD katsayılarının hesaplanması için matematiksel ifade Eş. 5.1, 5.2 ve 5.3'te verilmiştir.

$$F(u, v) = a(u)a(v) \quad (5.1)$$

$$\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \cos \left[\frac{\pi u}{2N} (2x + 1) \right] \cos \left[\frac{\pi v}{2M} (2y + 1) \right] f(x, y) \quad (5.2)$$

$$a(u)a(v) = \begin{cases} \sqrt{\frac{1}{N}}, v \neq 0 \\ \sqrt{\frac{2}{N}}, v = 0 \end{cases} \quad (5.3)$$

N ve M girdi olarak kullanılan görüntünün en ve boyunu, $f(x, y)$ x ve y kordinatlarındaki pikselin yoğunluğunu, $F(u, v)$ AKD katsayısını ifade eder. u , 0 ile $N - 1$ ve v , 0 ile $M - 1$ aralığında değişir.

5.2. Yerel İkili Örüntü (YİÖ)

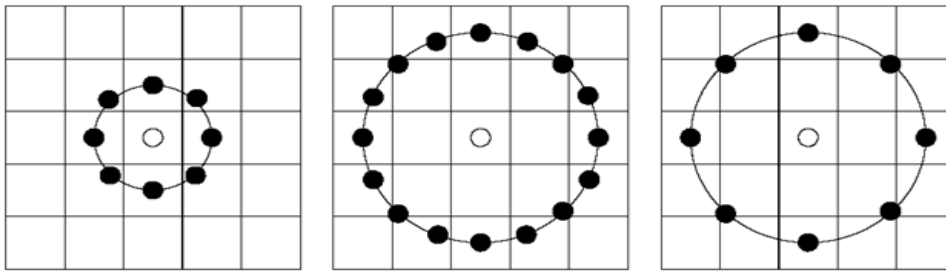
YİÖ farklı tiplerdeki doku yapısının tanımlanmasında kullanılan gri seviyeli bir doku operatörüdür. Orijinal YİÖ operatörü, görüntüdeki her piksel için bir YİÖ kodu üretir.

Operatör, görüntüdeki pikselleri etiketlemek için 3×3 'lük komşulukları kullanır. Merkez pikselin değeri, komşu pikseller ile kıyaslanarak, merkez piksel değerinden büyük olan komşu pikseller için 1 ve küçük olan pikseller için 0 ikili değeri üretilir ve üretilen değerlerin onluk karşılığı ise bölgenin temsilinde kullanılır [10, 13, 46]. YİÖ operatörünün $[0,255]$ aralığında üretmiş olduğu değerler, YİÖ kodları olarak adlandırılır. (x_c, y_c) koordinatlarında yer alan piksel için üretilen YİÖ kod değerinin hesaplanmasında kullanılan matematiksel Eş. 5.4'te verilmiştir. Merkez pikselin parlaklık değeri olan i_c , P adet komşu pikselin parlaklık değeri olan i_p ile kıyaslanarak kod değeri üretilir [46]. R komşulukları belirlemede kullanılan yarıçapı ifade etmektedir. Operatör içerisinde kullanılan $s(x)$ fonksiyonunun tanımı Eş. 5.5'te verilmiştir.

$$LBP_{P,R}(x_c, y_c) = \sum_{p=0}^{P-1} s(i_p - i_c) 2^p \quad (5.4)$$

$$s(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \quad (5.5)$$

Farklı komşuluk sayıları (P) ve komşulukları belirlemek için kullanılan R değerleri ile temsili gösterim Şekil 5.1'de verilmiştir. YİÖ yüz tanıma uygulamalarında sıklıkla kullanılır ve yüz imgesinin temsilinde, değişen aydınlanma koşullarına duyarlı olmasıyla bilinir. Buna karşın AKD, YİÖ yöntemine göre aydınlatma koşullarının değişimine karşı daha güçlüdür [13].



Şekil 5.1. Farklı P ve R değerleri ile dairesel simetrik komşuluklar (P=8, R=1), (P=16, R=2), (P=8, R=1)

5.3. Gradyanların Histogramı (HOG)

HOG, ilk olarak Dalal ve Triggs [42] tarafından insan tanıma problemlerinde kullanılmıştır. Karmaşık ortamlarda yüksek başarı sağlamasından dolayı, öznetelik çıkarımı

yöntemi olarak büyük ilgi görmüş ve literatürde sık kullanılmaya başlanmıştır. HOG hedef şekli temsil eden bir araç olarak, yerel bölgelerdeki hedef kenarların dağılımına ilişkin bilgilerini çıkarır. Amaç, nesneyi bir grup yerel histogramlar olarak tanımlamaktır. Bu histogramlar, nesnenin yerel bir bölgesindeki gradyanların oryantasyonlarının oluşma sayılarından oluşur. HOG öznitelik tanımlayıcılarının gerçekleştirim işlem basamakları aşağıdaki sırada verilebilir;

1. Görüntüye, görüntünün her noktasının iki yöndeki gradyan değerini hesaplamak için basit bir gradyan operatörü $[-1, 0, 1]$ uygulanır. Uygulanan matematiksel ifade Eş. 5.6’te verilmiştir.

$$G_X = [-1, 0, 1] * I(x, y) \text{ ve } G_Y = [-1, 0, 1]^T * I(x, y) \quad (5.6)$$

2. Gradyan büyüklükleri Eş. 5.7 ve (x, y) noktasındaki görüntü kenarlarının oryantasyon değeri de Eş. 5.8 kullanılarak hesaplanır.

$$G(x, y) = \sqrt{G_X(x, y)^2 + G_Y(x, y)^2} \quad (5.7)$$

$$\theta(x, y) = \tan^{-1} G_X(x, y) / G_Y(x, y) \quad (5.8)$$

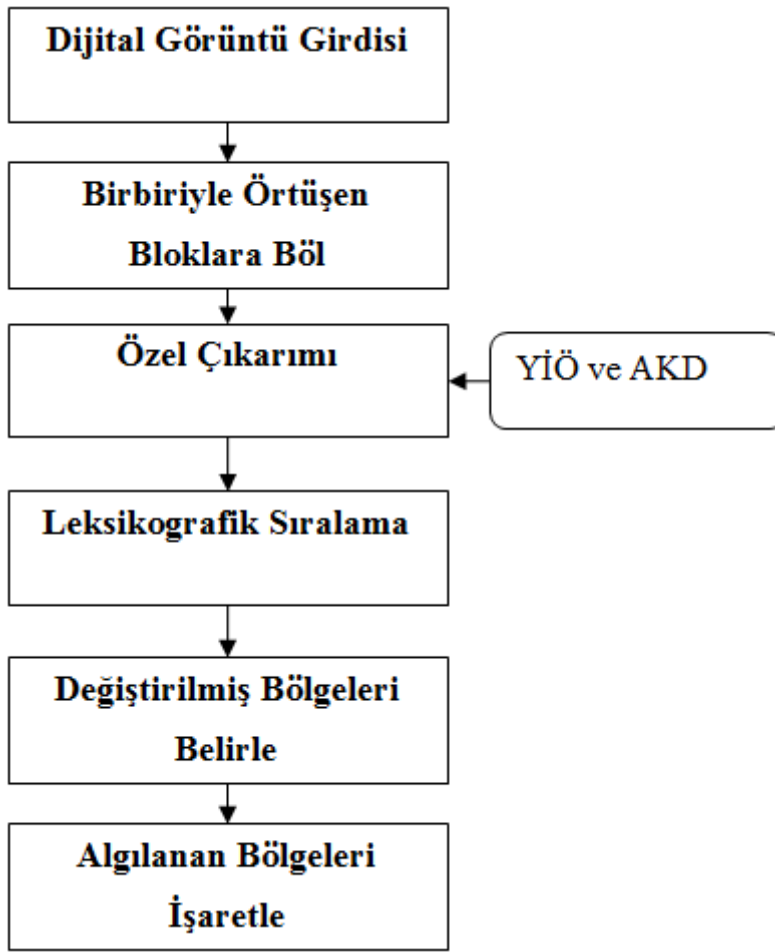
3. Oluşturulan yerel gruplar içindeki histogramların normalize edilmesi.

Gri seviyeli görüntüler üzerinde işlem yapılır. Görüntüdeki her nokta için hesaplanan gradyan büyüklüğü ve yön bilgileri kullanılarak yerel histogramlar elde edilir. Yerel gruptaki her piksel gradyan hesaplamada yön tabanlı histogram kanalında bulunan değer için bir ağırlık bildirir. Histogram kanalları gradyanın işaretli veya işaretsiz olmasına göre 0-180 derece veya 0-360 derece aralıklarında eşit olarak dağılım gösterir.



6. ÖNERİLEN YÖNTEM

Çalışmamızda blok tabanlı kopyala taşı görüntü sahteciliği tespiti ile alakalı, literatürdeki çalışmalarda kullanılan YİÖ ve AKD öznitelik çıkarım yöntemleri birlikte kullanılarak yeni bir yöntem önerilmiştir. Öznitelik çıkarımında YİÖ ve AKD'yi birlikte kullanarak değişen aydınlatma koşullarına daha az duyarlı yerel öznitelikler elde edilmesi ve böylece yanlış pozitiflerin azaltılması amaçlanmıştır. Geliştirilen uygulamaya ilişkin blok diyagramı Şekil 6.1'de verildiği gibidir.



Şekil 6.1. Kopyala taşı sahteciliği tespiti için önerilen yöntemin blok diyagramı

Önerdiğimiz yöntemde gri seviyeli görüntüler üzerinde çalıştık. Öznitelik çıkarımı adımında gri seviyeli görüntü, bxb'lik sabit büyüklüklerde birbiriyle örtüşen alt bloklara bölünmektedir. Her blok için önce YİÖ uygulanarak görüntü blokları YİÖ alanına dönüştürülmekte ve sonrada AKD uygulanarak öznitelik vektörleri çıkarılmaktadır. Her blok için hesaplanan öznitelik vektörleri satır vektörlerini oluşturacak şekilde öznitelik

matrisi elde edilmektedir. Öznitelik matrisi leksikografik sıralanarak benzer bloklar ardışık sıralanmaktadır. Yumuşak renk geçişlerinin olduğu görüntü bloklarında yanlış negatif oranını azalmak için belirli filtrelemeler uygulanmaktadır. Bunun için sıralanmış öznitelik matrisinde, ardışık satır vektörlerinin ilgili bloklarının başlangıç koordinatları farkını içeren kaydırma vektörleri hesaplandıktan sonra her kaydırma vektörünün frekansı hesaplanmaktadır. Kopyala taşı sahteciliği ile çoğaltılmış görüntü bloğu büyüklüğüne bağlı olarak değişen eşik değeri uygulayarak, kaydırma vektör frekansı bu eşik değerin üzerinde kalan blokları kopyala taşı sahteciliği uygulanmış olan bloklar olarak işaretledik. Önerilen yöntemin algoritması Çizelge 6.1’de verilmiştir.

Çizelge 6.1. Önerilen yönteme ilişkin algoritma adımları

-
- 1) $M \times N$ ’lik verilen görüntü gri seviyesine dönüştür.
 - 2) Görüntüyü $b \times b$ boyutlarında, $0 \leq i < k = ((M - b + 1) \times (N - b + 1))$ olacak şekilde birbiri ile örtüşen B_i bloklarına böl.
 - 3) Her $b \times b$ boyutlu B_i bloğuna önce YİÖ uygula ve YİÖ domainine dönüştürülmüş görüntü bloğuna AKD uygulayarak $(b - 2)^2$ uzunluklu $\vec{f}_i$ öznitelik vektörünü oluştur.
 - 4) Her $\vec{f}_i$ öznitelik vektörü, satır vektörlerini oluşturacak şekilde $k \times (b - 2)^2$ boyutlu A öznitelik matrisini oluştur.
 - 5) A matrisini satır bazlı alfabetik sırala ve S matrisini oluştur.
 - 6) s_i ve s_j S matrisinin ardışık satır vektörlerini, (x_i, y_i) ve (x_j, y_j) , s_i ve s_j satır vektörlerinin ilişkili blok lokasyonlarını gösterecek şekilde $s_i = (x_i = (x_i - x_j), y_i = (y_i - y_j))$ kaydırma vektörlerini hesapla.

$$(x_i - x_j, y_i - y_j) \text{ eğer } x_i - x_j > 0$$

$$(x_j - x_i, y_i - y_j) \text{ eğer } x_i - x_j < 0$$

$$(0, |y_i - y_j|) \text{ eğer } x_i = x_j$$

- 7) Hesaplanan kaydırma vektörleri frekanslarını (her bir kaydırma vektörünün listede rastlanma sayısı) hesapla ve frekansı T_1 eşliğinden küçük olanları ele.
- 8) Kalan listede blokların birbirlerine olan Öklid uzaklığı d ’yi hesapla. d uzaklığı T_2 eşliğinden küçük olanları ele.

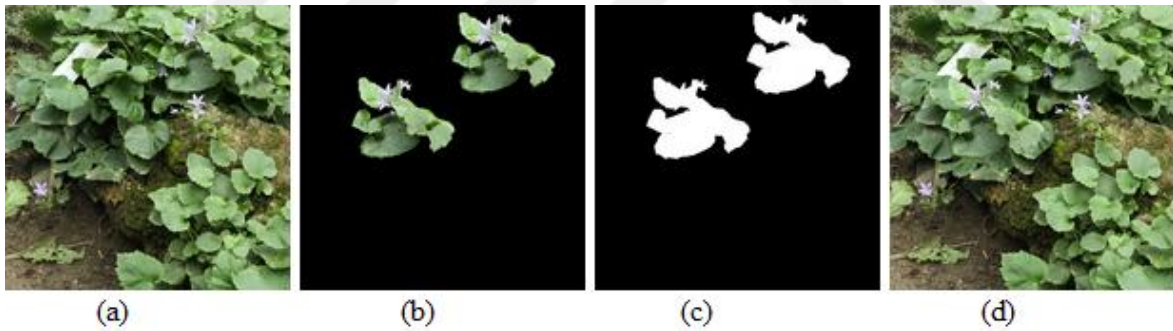
$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

- 9) Listede kalan blok çiftlerini görüntüde çoğaltılmış bölge olarak işaretle.
-

6.1. CoMoFoD – Kopyala Taşı Sahteciliği Tespiti İçin Görüntü Veri Tabanı

Kopyala-taşı sahteciliği için önerilmiş birçok yöntem olmasına karşın, 2013 yılına kadar önerilen yöntemlerde kullanılmak için oluşturulmuş bir veri tabanı yoktu. 2013 yılında VCL (Video Communication Laboratory) tarafından CoMoFoD kopyala taşı sahtecilik tespiti için veri tabanı oluşturulmuştur [44].

Bu görüntü veri tabanı 512×512 boyutlarında 200 ve 3000×2000 boyutlarında 60 adet görüntü barındıran iki ayrı görüntü kümesi içermektedir. Her grupta çevirme, döndürme, ölçeklendirme, birleştirme ve çeşitli işlemlerle bozma gibi beş ayrı manipülasyon ile gerçekliğini yitirmiş görüntüler vardır. Her görüntü kümesinde Resim 6.1’de örneği görüleceği üzere orijinal görüntü, renkli maskeleme, ikili maskeleme ve sahte görüntüler yer almaktadır. Ayrıca her görüntü için JPEG sıkıştırması, bulanıklaştırma, gürültü ekleme, parlaklık değiştirme, zıtlık ayarlama ve renk azaltma gibi çeşitli son işlem teknikleri ile bozulmuş orijinal ve sahte görüntü formları yer almaktadır [44].



Resim 6.1. CoMoFoD veri tabanı örnek görüntü (a) orijinal görüntü, (b) renkli maskeleme, (c) siyah-beyaz ikili maskeleme, (d) sahte görüntü [43]

İsimlendirme

Görüntü kümelerinde yer alan görüntüler N1_M1 şeklinde isimlendirilmektedir. N1 küçük görüntü kümesi için üç, büyük görüntü kümesi için iki rakam içeren ve görüntünün küme içerisindeki sırasını belirten rakamlardır. M1 ise dört farklı değer almaktadır. Bunlar;

- “F” – sahte görüntü
- “B” – ikili maske (siyah ve beyaz maske) uygulanmış görüntü
- “M” – renkli maske (değiştirilmiş bölgeleri gösteren) uygulanmış görüntü

- "O" – orijinal görüntü

Ayrıca görüntüye uygulanan son işlem yöntemlerini belirtecek şekilde (N1_M1_M2) isimlendirilen görüntüler yer almaktadır. M2 görüntüye uygulanan son işlem türünü belirtir ve aşağıdaki değerleri alır.

- "JC" - JPEG sıkıştırması, kalite faktörü = [20, 30, 40, 50, 60, 70, 80, 90, 100]
- "IB" – görüntü bulanıklaştırma, $\mu = 0$, $\sigma^2 = [0.009, 0.005, 0.0005]$
- "NA" – gürültü ekleme, ortalama filtre = [3x3, 5x5, 7x7]
- "BC" – parlaklık değiştirme, (alt sınır, üst sınır) = [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
- "CR" – renk azaltma, her renk kanalı başına yoğunluk seviyeleri = [32, 64, 128]
- "CA" – zıtlık ayarlama, (alt sınır, üst sınır) = [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]

6.2. Parametre Ayarlama ve Algoritma Çıktısı

Önerilen yöntem CoMoFoD veri tabanından sağlanan 512x512 piksellik 40 görüntü üzerinde uygulanmış ve sonuçları verilmiştir. Denenen 40 görüntüden 12 adet görüntüde, kopyalanan alan birden fazla bölgeye yapıştırılarak ve 7 adet görüntüde ise birden fazla farklı bölge kopyala taşı sahteciliği ile çoğaltılmıştır. Ayrıca deneme görüntülerinin çoğunda Resim 6.1’de gösterildiği gibi kopyala taşı sahteciliği uygulanan alan düzgün kopyalanarak çoğaltılmış değildir. Kopyala taşı sahteciliğinin tespitinde, kopyalanan bölgenin düzenli veya düzensiz olmasına göre iki farklı değerlendirme yapılmaktadır. Kare veya dikdörtgen biçiminde düzgün kopyalanarak çoğaltılmış alanlarda, blok tabanlı kopyala taşı sahteciliği tespiti algoritmalarının DP (Doğru Pozitif) oranları yüksek ve YP (Yanlış Pozitif) oranları düşük olabilir.

Blok tabanlı kopyala taşı sahteciliği tespiti algoritmaları uygulanan blok büyüklüğünden küçük çoğaltılmış alanları tespit edemezler. Deneme görüntülerinde en küçük çoğaltılmış bölge 360 piksel [44], yani yaklaşık olarak 20x20 blok büyüklüğü olduğu için yöntemimizi bu blok büyüklüğünden daha küçük ölçülerdeki bloklarla test etmemiz gerekir. Biz 8x8’lik, 10x10’luk, 12x12’lik, 16x16’lık ve 20x20’lik blok büyüklükleri ile test ettik. Kaydırma vektör frekansı için kullanılan T_1 eşliğimizin ideal değeri çoğaltılan bölgenin büyüklüğü ve algoritmada kullanılan blok büyüklüğüne bağlı olarak, 8x8’lik blok büyüklüğü için $(20 - 8 + 1)^2 = 169$, 10x10’lük blok büyüklüğü için $(20 - 10 + 1)^2 = 121$, 12x12 blok büyüklüğü $(20 - 12 + 1)^2 = 81$, 16x16 blok büyüklüğü

$(20 - 16 + 1)^2 = 25$ ve 20×20 blok büyüklüğü $(20 - 20 + 1)^2 = 1$ olarak hesapladık. Ancak T_1 eşiklerini 8×8 , 10×10 , 12×12 , 16×16 ve 20×20 blok büyüklükleri için sırasıyla 150, 100, 50, 30 ve 20 değerlerini kullandık ve bu eşiklerden büyük kaydırma vektörü frekansına sahip blok çiftini sahtecilik yapılmış bölgeler olarak işaretledik. T_2 eşik değerini benzer blokların birbirlerine olan Öklid uzaklıkları için uyguladık. Mavi gökyüzü gibi yumuşak geçişlerin olduğu görüntülerde birbirine bitişik bölgelerde benzer bloklar olabilir. Bu görüntülerde yanlış pozitif oranını azaltmak için blokların sol üst köşe koordinatlarının birbirine olan Öklid uzaklık değeri en az bir blok uzunluğundan büyük olmalıdır. Bu yüzden T_2 eşik değerini yine algoritmada kullanılan 8×8 , 10×10 , 12×12 , 16×16 ve 20×20 blok büyüklükleri için sırasıyla 8, 10, 12, 16 ve 20 olarak ayarladık.

Görüntü bloklarına YİÖ'yü $R=1$ ve $P=8$ parametre değerleriyle uyguladık. Amacımız öznelitekt vektörlerinin çıkarılmasında YİÖ ve AKD'nin birlikte kullanımı olduğu için YİÖ'yü uygularken kullanılan parametrelerin yöntemin başarı oranını etkilemesine bakılmadı.

Çizelge 6.2. Önerilen yöntemin HOG, YİÖ ve AKD'nin ayrı ayrı kullanıldığı yöntemlerle karşılaştırmalı başarı sonuçları

Kullanılan blok büyüklüğü ve parametreler	AKD			YİÖ			HOG			Önerilen Yöntem		
	Doğruluk (%)	PTD (%)	YPO (%)	Doğruluk (%)	PTD (%)	YPO (%)	Doğruluk (%)	PTD (%)	YPO (%)	Doğruluk (%)	PTD (%)	YPO (%)
8×8 , $T_1 = 150$, $T_2 = 8$	98,16	75,65	1,62	99,30	81,97	0,67	99,29	81,99	0,63	99,55	89,79	0,30
10×10 , $T_1 = 100$, $T_2 = 10$	96,99	73,31	2,82	99,11	77,73	0,88	98,67	72,13	1,32	99,53	89,65	0,30
12×12 , $T_1 = 50$, $T_2 = 12$	92,23	65,44	7,69	98,20	67,36	1,87	98,04	67,53	1,96	99,16	84,56	0,68
16×16 , $T_1 = 30$, $T_2 = 16$	77,87	48,79	22,68	96,89	61,56	3,29	96,84	57,41	3,23	98,75	75,14	0,99
20×20 , $T_1 = 20$, $T_2 = 20$	65,83	42,92	35,30	94,78	53,24	5,58	95,39	50,31	4,75	97,97	66,54	1,70

Çizelge 6.2 de önerilen yöntemin başarı sonuçları, YİÖ ve AKD'nin ayrı ayrı kullanımları ve HOG ile PTD (Pozitif Tahmin Değeri), YPO (Yanlış Pozitif Oranı) ve doğruluk ölçütleri kullanılarak karşılaştırmalı olarak verilmiştir. Sonuçlar algoritmaların doğru

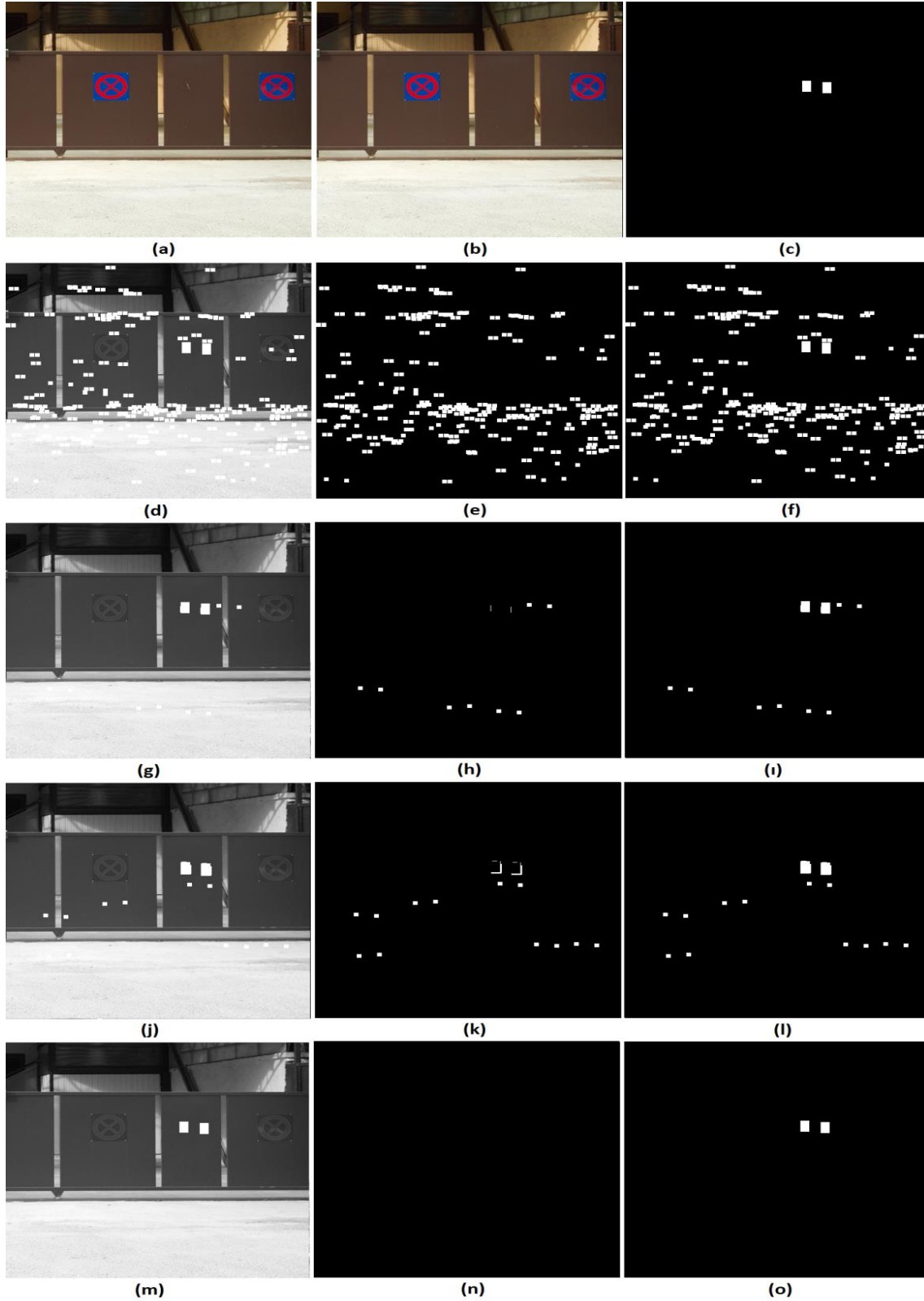
tespit ettiği ve yanlış pozitif olarak işaretledikleri alanlar dikkate alınarak piksel tabanlı hesaplanmıştır. PTD, YPO ve doğruluk değerleri hesaplanması sırasıyla Eş. 6.1, 6.2 ve 6.3'te verilmiştir.

$$PTD = \frac{DP \text{ (Doğru Pozitif)}}{DP+YP \text{ (Yanlış Pozitif)}} \quad (6.1)$$

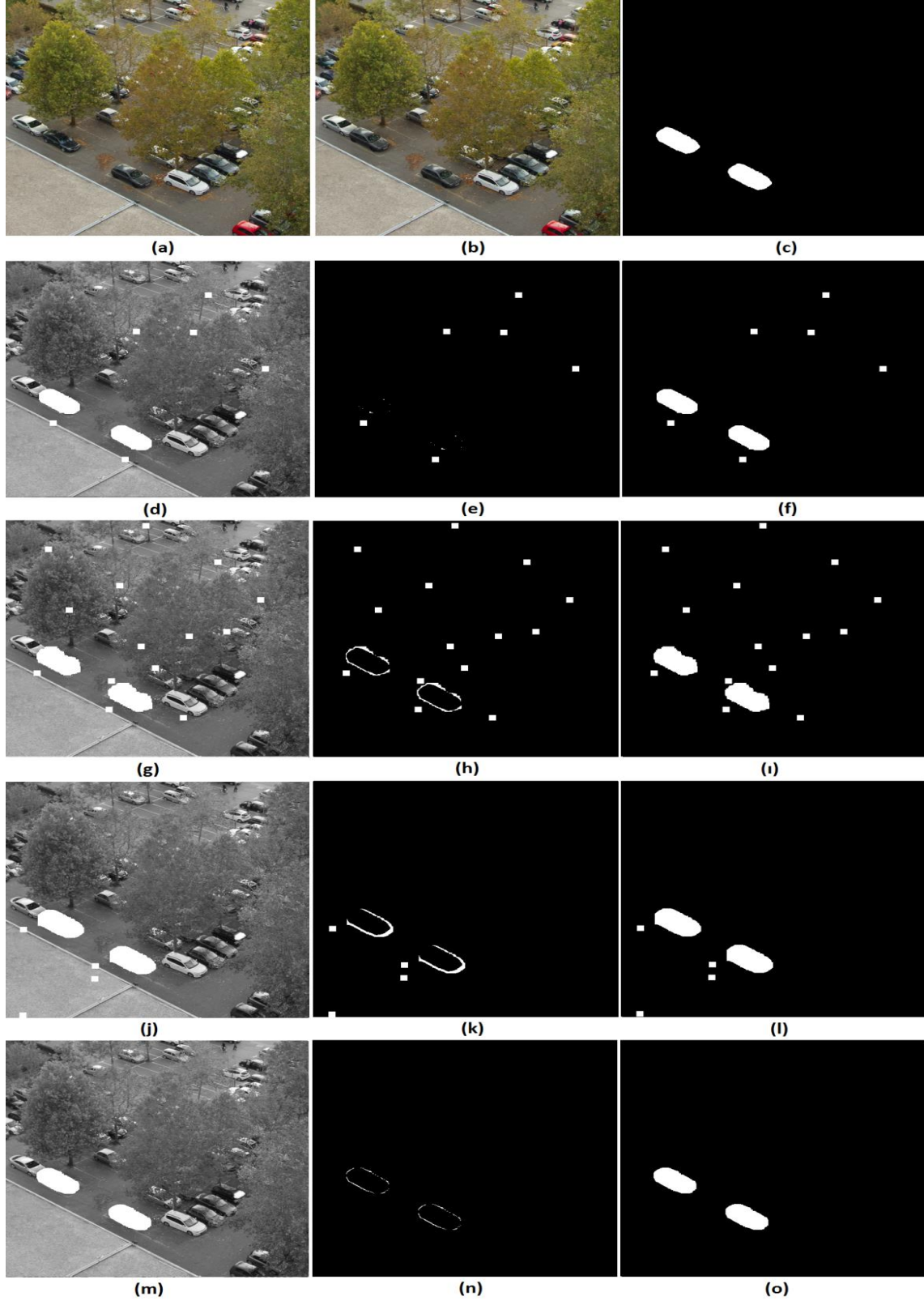
$$YPO = \frac{YP}{YP+DN \text{ (Doğru Negatif)}} \quad (6.2)$$

$$\text{Doğruluk} = \frac{DP + DN}{DP + DN + YP + YN \text{ (Yanlış Negatif)}} \quad (6.3)$$

Resim 6.2'de 8x8'lik blok büyüklüğü ve $T_1 = 150$ ve $T_2 = 8$ ayarlanarak, Resim 6.3'te de 12x12 blok büyüklüğü ve $T_1 = 50$ ve $T_2 = 12$ ayarlanarak önerilen yöntemin, YİÖ ve AKD'nin ayrı ayrı kullanıldığı yöntemlerin ve HOG yönteminin denenilen görüntü üzerindeki çıktıları verilmiştir. Algoritmaların tespit ettiği bölgeler beyaz ile işaretlenmiştir. Resimlerde en üst satırda yer alan (a) orijinal görüntüyü, (b) sahte görüntüyü ve (c) sahtecilik uygulanmış bölgelerin ikili maskelenmiş gösterimini içermektedir. Yine görüntüde ilk satırdan sonraki satırlarda yer alan sol sütundaki görüntülerde (d, g, j, m) sırasıyla AKD, YİÖ, HOG ve önerilen yöntemlerin sahtecilik uygulanmış bölgeler olarak tespit ettiği görüntü bloklarının orijinal görüntü üstünde işaretlenmiş algoritma çıktıları yer almaktadır. Orta sütunda yer alan görüntüler (e, h, k, n) sahtecilik uygulanmamış ancak algoritmaların sahtecilik olarak işaretlediği yanlış pozitifleri göstermektedir ve sağ sütunda yer alan görüntülerde (f, i, l, o) algoritma çıktılarının ikili maskelenmiş gösterimi verilmiştir. Resim 6.2'de algoritmaların çıktılarından önerilen yöntemin yanlış pozitif tespitinin olmadığı ve sahtecilik uygulanmış bölgeleri eksiksiz tespit ettiği görülmektedir. Yine Resim 6.3'te verilmiş sonuç görüntülerde önerilen yöntemin diğer yöntemlere göre yanlış pozitif değerinin az ve başarısının daha yüksek olduğunu söyleyebiliriz. Ayrıca önerilen yöntemin yanlış pozitif olarak işaretlediği görüntü blokları karşılaştırılan AKD, YİÖ ve HOG yöntemlerinin sahtecilik olarak işaretlediği yanlış pozitif değerleri gibi sahtecilik uygulanmış görüntü bloklarından tamamen bağımsız bölgelerde değildir.

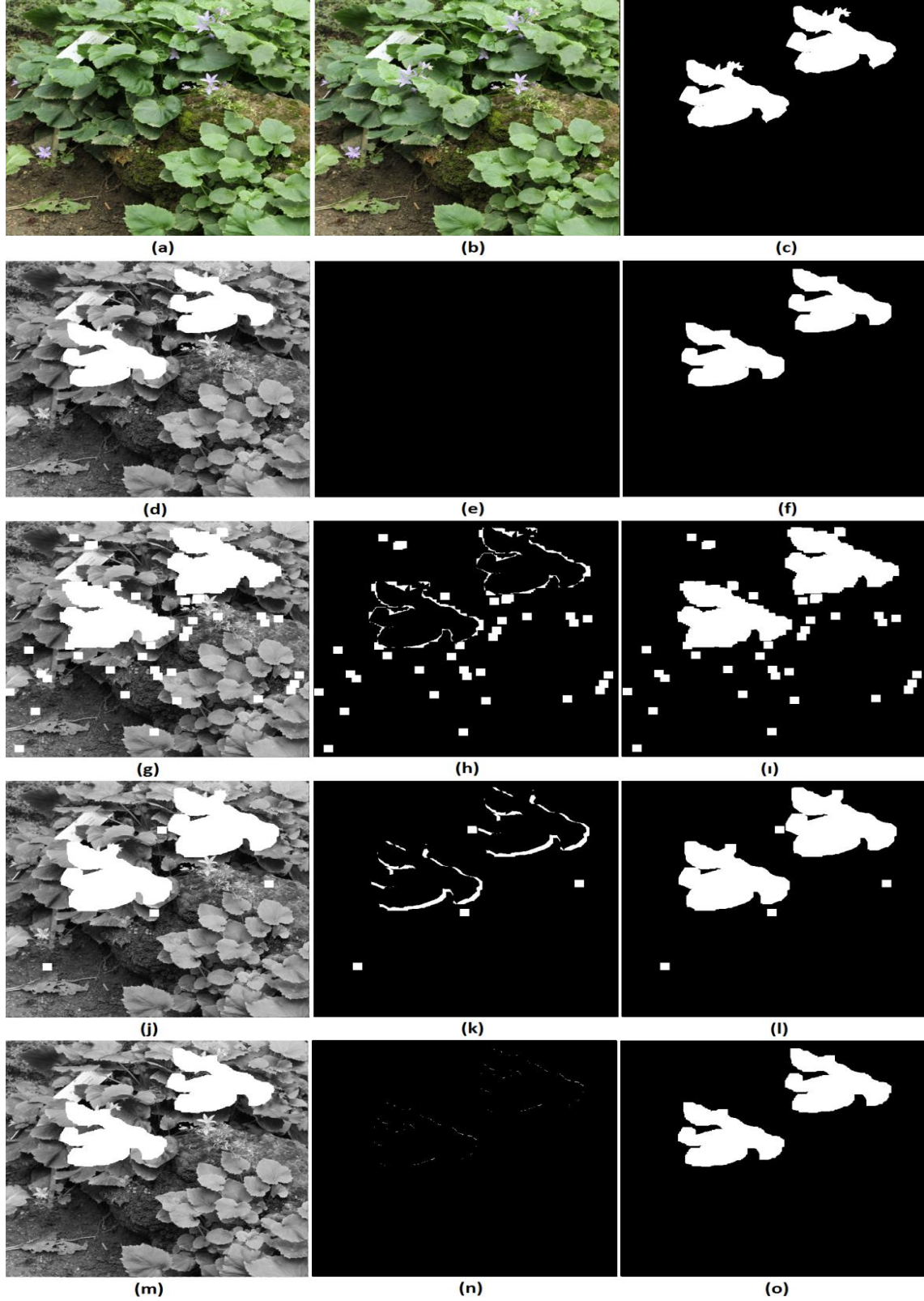


Resim 6.2. Algoritma çıktıları ($b = 8 \times 8$, $T_1 = 150$ ve $T_2 = 8$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi



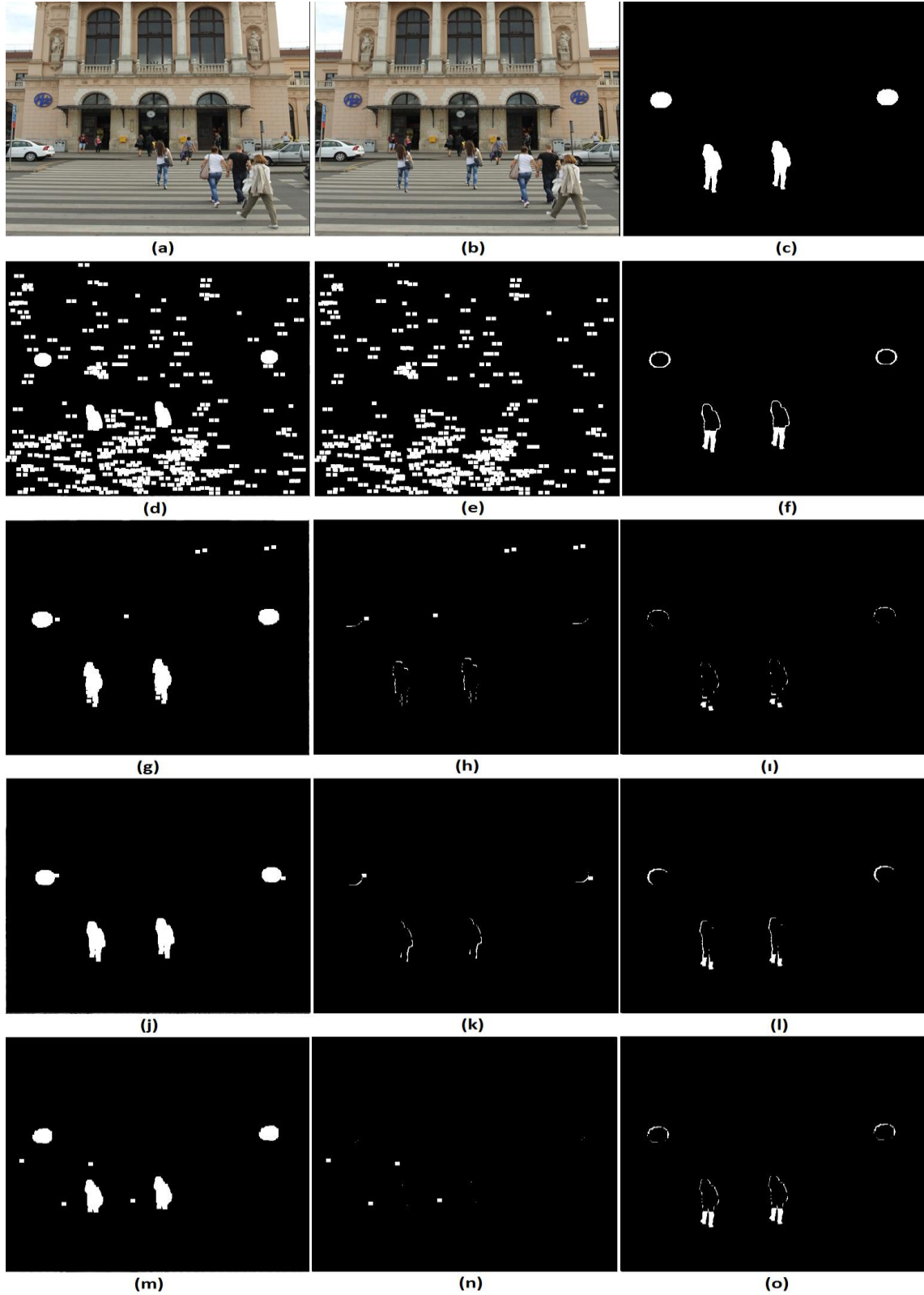
Resim 6.3. Algoritma çıktıları ($b = 12 \times 12$, $T_1 = 50$ ve $T_2 = 12$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi

Resim 6.4'te 16×16 'lık blok büyüklüğü ve $T_1 = 30$ ve $T_2 = 16$ olarak ayarlanarak elde edilmiş algoritma çıktıları verilmiştir. Görüntüde ilk satırda sırasıyla (a)'da orijinal, (b)'de kopyala taşı sahteciliği uygulanmış görüntü ve (c)'de kopyala taşı sahteciliği ile çoğaltılmış görüntü bloğunun ikili maskelenmiş görüntüsü yer almaktadır. (c) de yer alan maskelenmiş görüntü blokları aynı zamanda algoritma çıktılarını değerlendirdiğimiz görüntü olarak referans aldığımız için kesin referans olarak ta adlandırılabilir. Görüntüde ilk satırdan sonraki satırlarda sırasıyla (d, e, f) AKD yöntemi ile, (g, h, i) YİÖ yöntemi ile, (j, k, l) HOG yöntemi ile ve (m, n, o) önerilen yöntem ile elde edilmiş algoritma çıktıları göstermektedir. Ayrıca sol sütundaki (d, g, j, m) görüntüler, algoritmaların sahtecilik olarak bulduğu bölgelerin gerçek görüntü üzerinde işaretlenmiş çıktıları, sağ sütunda yer alan (f, i, l, o) görüntüler algoritmaların sahtecilik olarak işaretlediği bölgelerin ikili maskelenmiş gösterimini ve orta sütundaki (e, h, k, n) görüntüler de algoritmaların yanlış pozitif olarak işaretlediği görüntü bloklarını ifade etmektedir. Sonuçlar incelendiğinde önerilen yöntemin YİÖ ve HOG yöntemine göre yanlış pozitif oranının düşük ve başarısının daha iyi olduğu görülebilir. Ancak AKD ile elde edilen çıktılarda yanlış pozitif olarak işaretlenmiş görüntü bloğu yer almamakla birlikte önerilen yöntem kopyala taşı sahteciliği uygulanmış görüntü bloğunun çevresindeki bazı bölgeleri sahtecilik uygulanmış bloklar olarak işaretlemiş durumdadır. Algoritmanın işaretlediği bu görüntü blokları sahtecilik uygulanmış görüntü bloğundan bağımsız bölgeler değildir. Ancak algoritmaların başarıları piksel bazında hesaplandığı için bu görüntü üzerinde AKD ile elde edilen algoritma çıktıları için YPO önerilen yönteminkinden daha küçüktür. Ancak denenen 40 görüntü üzerinden elde edilen sonuçlara göre önerilen yöntemin AKD'ye ve diğer iki yöntemine göre YPO çok daha düşük ve başarısı çok daha yüksektir.



Resim 6.4. Algoritma çıktıları ($b = 16 \times 16$, $T_1 = 30$ ve $T_2 = 16$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgeler, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi

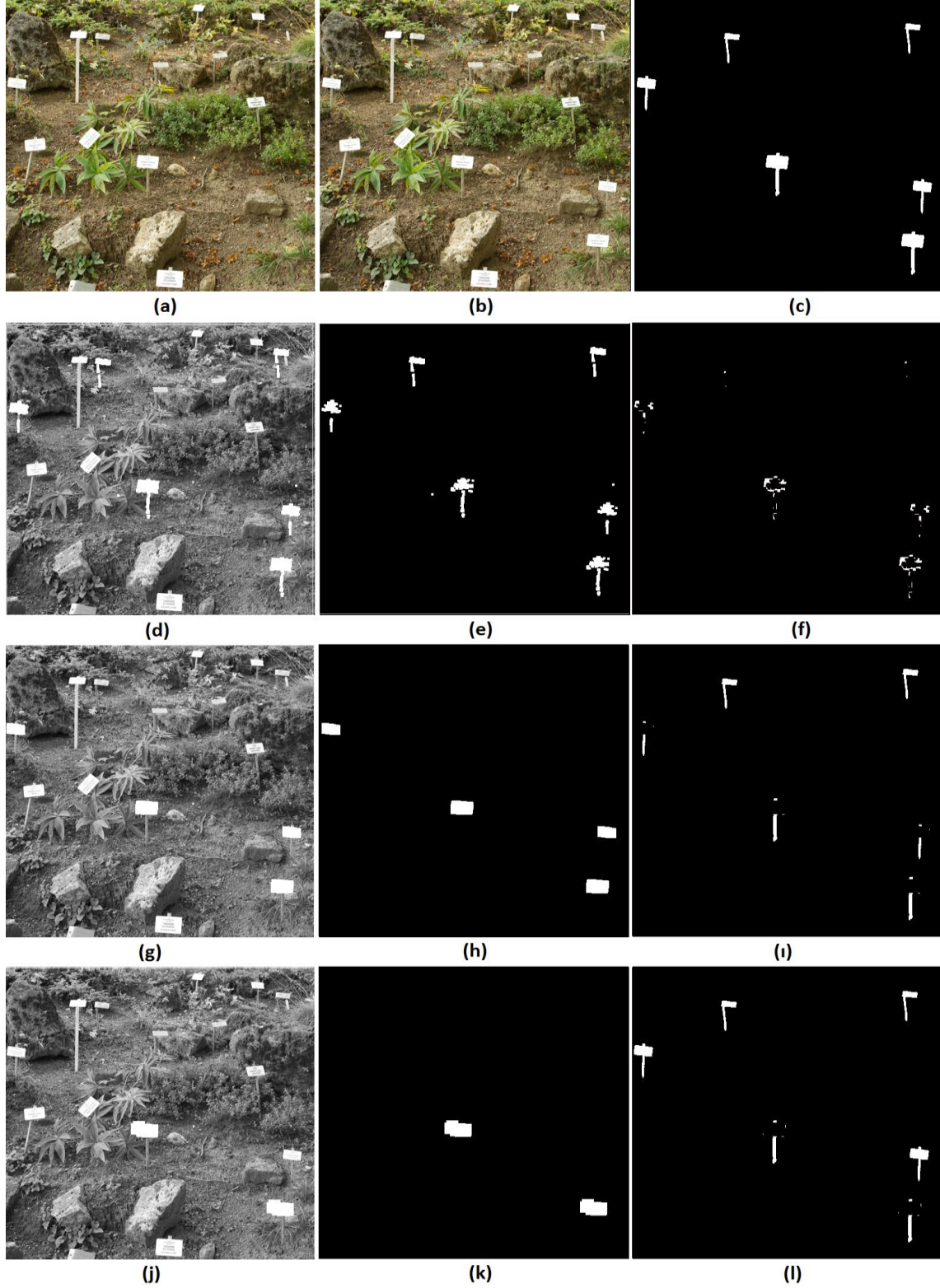
Önerilen yöntemin YİÖ ve AKD'nin ayrı ayrı kullanıldığı yöntemlere göre her ne kadar YPO düşük olsa da, bazı deneme görüntülerinde YİÖ'nün tek başına kullanıldığı yönteme göre YNO (Yanlış Negatif Oranı) yüksek olabilmektedir. Resim 6.5'te 8x8'lik blok büyüklüğü ve $T_1 = 150$ ve $T_2 = 8$ ayarlanarak sırasıyla AKD, YİÖ, HOG ve önerilen yöntemin denenilen bir görüntü üzerindeki algoritma çıktıları verilmiştir. Görüntüde ilk satırda sırasıyla (a)'da orijinal, (b)'de kopyala taşı sahteciliği uygulanmış görüntü ve (c)'de kopyala taşı sahteciliği ile çoğaltılmış görüntü bloğunun ikili maskelenmiş görüntüsü yer almaktadır. (d, e f) öznitelik çıkarımında yalnızca AKD kullanıldığı durumdaki yöntemin algoritma çıktıları, (g, h, i) YİÖ'nün öznitelik çıkarımında tek başına kullanıldığı durumdaki yöntemin algoritma çıktıları, (j, k, l) öznitelik çıkarımında HOG kullanılan yöntemin ve (m, n, o) önerilen yöntemin algoritma çıktıları göstermektedir. İlk sütunda yer alan (d, g, j, m) görüntüler algoritmaların doğru pozitif olarak işaretlediği blokları, orta sütunda yer alan (e, h, k, n) görüntüler algoritmaların yanlış pozitif olarak işaretledikleri blokları ve son sütunda yer alan (f, i, l, o) görüntüleri de sahtecilik uygulanmış ancak algoritmaların sahtecilik olarak işaretlemedikleri bölgeler olan yanlış negatifleri ifade etmektedir. Görüntülerden de anlaşıldığı üzere, önerilen yöntemin yanlış pozitif oranı diğer yöntemlerin yanlış pozitif oranına göre düşüktür. Ancak önerilen yöntemin yanlış negatif oranı, AKD'nin yalnız kullanıldığı yöntemin yanlış negatif oranından daha düşük olmasına karşın, YİÖ ve HOG yöntemlerine göre daha yüksektir. Bu görüntüde olduğu gibi, düzensiz kopyala taşı sahteciliği uygulanmış ve çoğaltılmış bölgelerin içerdiği bazı görüntü bloklarının, algoritmanın denendiği blok büyüklüğünden daha küçük olması durumunda sahtecilik uygulanmış bölgeler eksiksiz tespit edilememektedir. Bu durumlarda, öznitelik çıkarım yöntemi olarak YİÖ'nün veya HOG'un kullanıldığı sahtecilik tespiti yöntemlerinin YNO önerilen yönteme göre daha düşük olabilmektedir. Sahtecilik uygulanmış görüntü bloğunun, algoritmaların kullandığı blok büyüklüğünden küçük olması durumunda tespit edilememesi durumu yalnızca önerilen yöntemin bir eksiği değil, blok tabanlı kopyala taşı sahteciliği tespiti yöntemlerinin bir eksiğidir. Ancak blok büyüklüğüne bağlı olarak sahtecilik uygulanmış bazı görüntü bloklarının tespit edilememesi hassasiyetinin önerilen yöntemde, karşılaştırılan diğer yöntemlere göre daha yüksek olduğu söylenebilir.



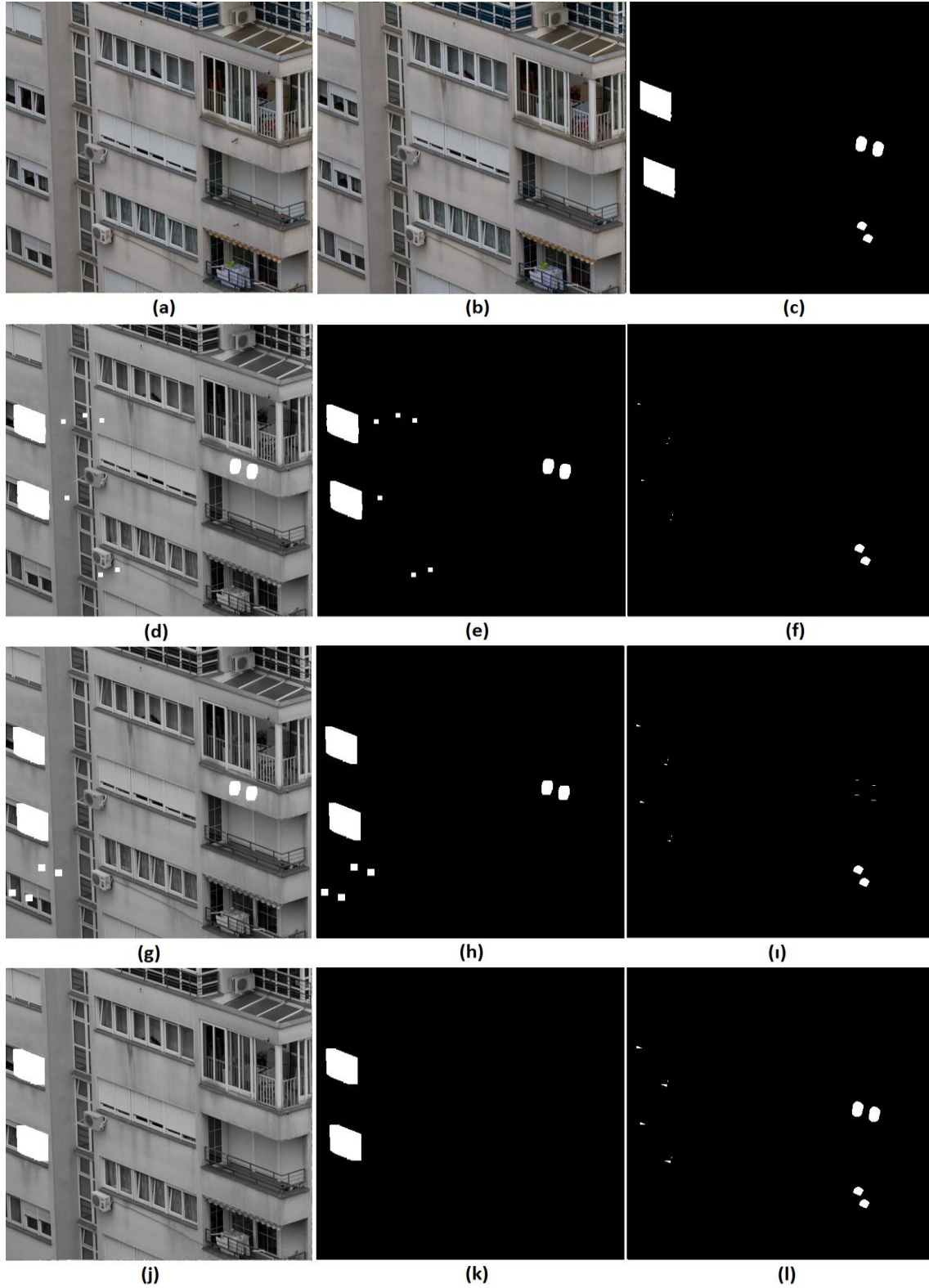
Resim 6.5. Yanlış negatif oranı karşılaştırması için algoritma çıktıları ($b = 8 \times 8$, $T_1 = 150$ ve $T_2 = 8$), (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) AKD yöntemi çıktısı, (g, h, i) YİÖ yöntemi çıktısı, (j, k, l) HOG yöntemi çıktısı, (m, n, o) önerilen yöntemin çıktısı, (d, g, j, m) algoritmaların tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (e, h, k, n) yanlış pozitiflerin gösterimi, (f, i, l, o) yanlış negatiflerin gösterimi

Blok büyüklüğünün çoğaltılmış bölgeleri algılamada deneme sonuçlarını nasıl etkilediğini gözlemlemek için Resim 6.6'da 4×4 blok büyüklüğü ve $T_1 = 150$ ve $T_2 = 4$ parametre değerleri ile, 12×12 blok büyüklüğü ve $T_1 = 50$ ve $T_2 = 12$ parametre değerleri ile ve 20×20 blok büyüklüğü ve $T_1 = 20$ ve $T_2 = 20$ parametre değerleri ile, Resim 6.7'de 8×8 blok büyüklüğü ve $T_1 = 150$ ve $T_2 = 8$ parametre değerleri ile, 12×12 blok büyüklüğü ve $T_1 = 50$ ve $T_2 = 12$ parametre değerleri ile ve 16×16 blok büyüklüğü ve $T_1 = 30$ ve $T_2 = 16$ parametre değerleri ile denenen görüntüler üzerinde algoritma çıktıları verilmiştir. Görüntülerde ilk satırda, (a) orijinal görüntü, (b) kopyala taşı sahteciliği uygulanmış görüntü ve (c) kopyala taşı uygulanmış görüntü bölümlerinin ikili maskelenmiş görüntüsü yer almaktadır. İkinci satırdan itibaren sol sütunda yer alan görüntüler, önerilen yöntemin farklı blok büyüklükleri ile sahtecilik olarak algılanan blokların görüntü üzerinde işaretlenmesi ile elde edilen görüntüleri, orta sütunda yer alan görüntüler, algoritmanın sahtecilik olarak tespit ettiği görüntü bloklarının ikili maskelenmiş gösterimini ve sağ sütunda yer alan görüntüler de algoritmanın sahtecilik olup tespit edemediği piksellerin gösterildiği görüntüleri içermektedir. Farklı blok büyüklükleri ile elde edilmiş her iki deneme görüntüsünde de görüldüğü gibi blok büyüklüğü arttıkça önerilen yöntem, kopyala taşı sahteciliği uygulanmış küçük görüntü bloklarını tespit edememektedir. Buna bağlı olarak blok büyüklüğü arttıkça yöntemin YNO artmakta ve başarı oranı düşmektedir.

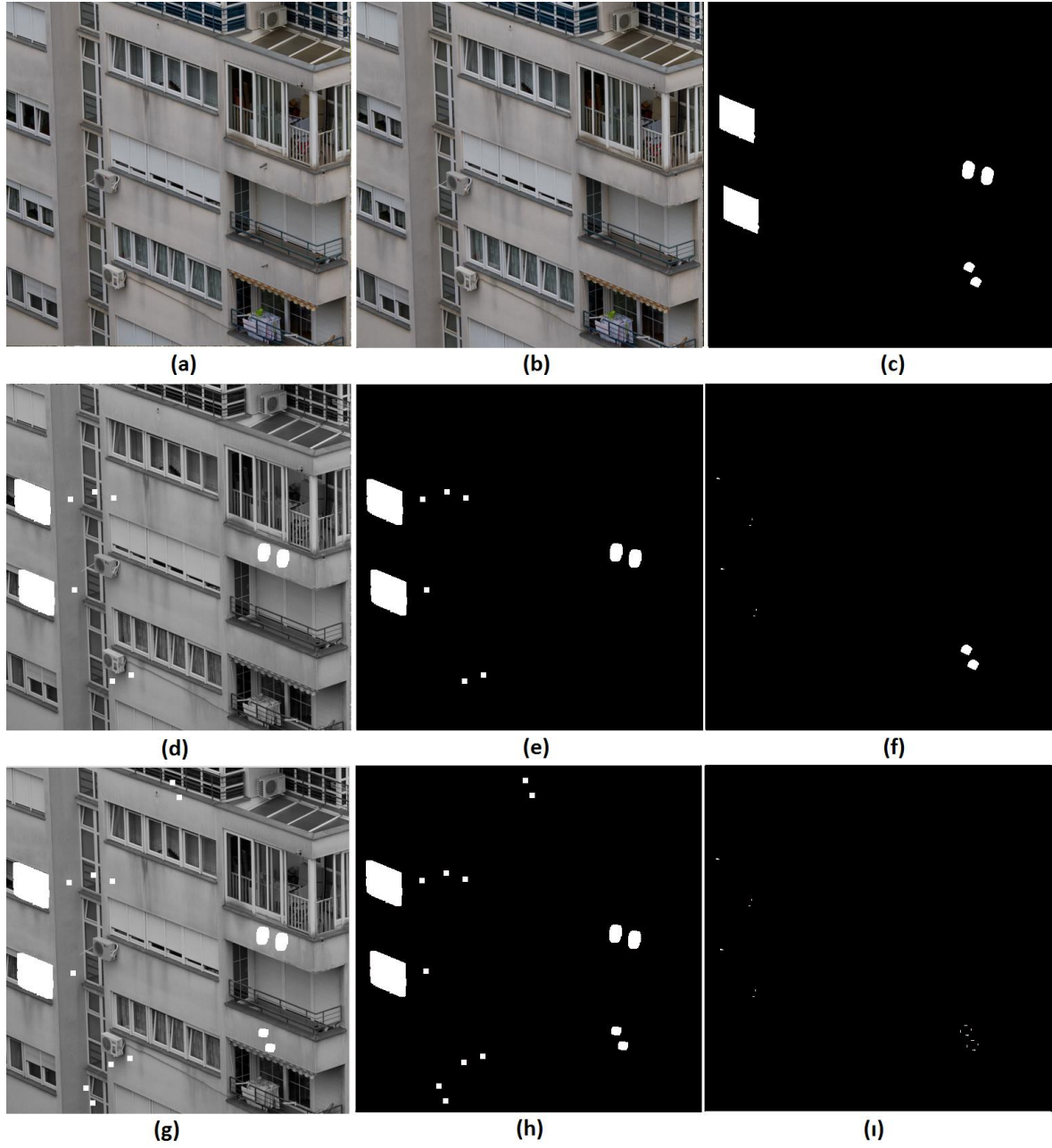
Bazı görüntüler için T_1 parametre değerini küçülterek algoritmanın sahtecilik uygulanmış küçük görüntü bloklarını tespit etmesini sağlamamız mümkün. Ancak bu durumda da yanlış pozitif oranı artabilmektedir. Resim 6.8'de Resim 6.7'de verilen görüntünün 8×8 blok büyüklüğü için T_1 parametre değeri sırasıyla 150 ve 30 olarak ve $T_2 = 8$ ayarlanarak deneme sonuçları paylaşılmıştır. Resimde (d, e, f) görüntüleri $T_1 = 150$ ve (g, h, i) görüntüleri de $T_1 = 30$ ayarlanarak elde edilmiş algoritma çıktılarıdır. (d, g) görüntüleri algoritmanın sahtecilik olarak tespit ettiği görüntü bloklarının gerçek görüntü üzerinde işaretlenmiş gösterimini, (e, h) görüntüleri algoritmanın sahtecilik olarak bulduğu görüntü bloklarının ikili maskelenmiş gösterimini ve (f, i) görüntüleri de sahtecilik uygulanmış ancak algoritmanın tespit edemediği görüntü bloklarını içermektedir. Görüntülerden de anlaşılacağı gibi $T_1 = 30$ olarak ayarlandığında, $T_1 = 150$ iken tespit edilemeyen küçük görüntü blokları tespit edilirken yanlış pozitiflerin arttığı görülebilir.



Resim 6.6. Önerilen yöntemin farklı blok büyüklükleri ile çıktısı, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) 4x4 blok büyüklüğü ile algoritma çıktısı, (g, h, i) 12x12 blok büyüklüğü ile algoritma çıktısı, (j, k, l) 20x20 blok büyüklüğü ile algoritma çıktısı, (d, g, j) algoritmanın tespit ettiği bölgeler, (e, h, k) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i, l) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri

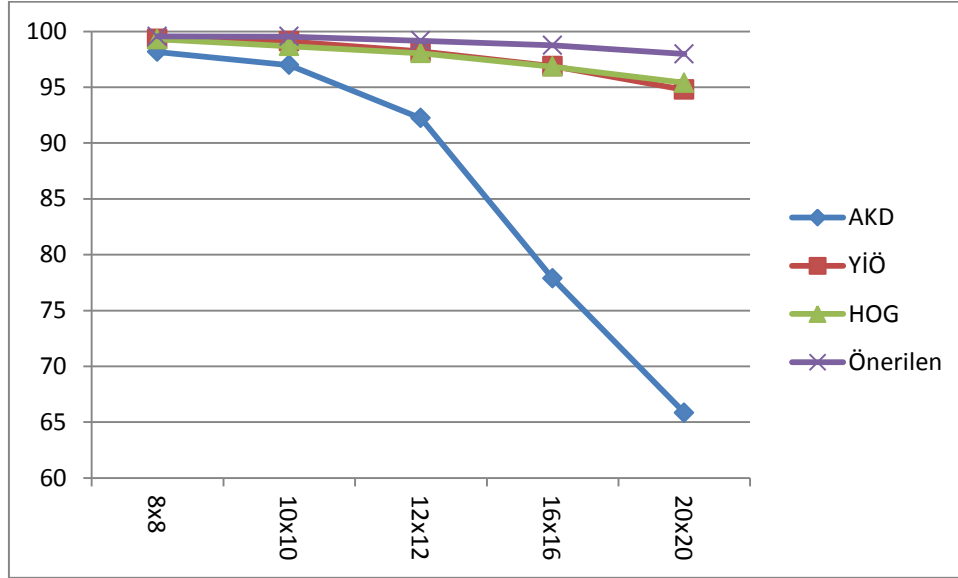


Resim 6.7. Önerilen yöntemin farklı blok büyüklükleri ile çıktıları, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) 8x8 blok büyüklüğü ile algoritma çıktısı, (g, h, i) 12x12 blok büyüklüğü ile algoritma çıktısı, (j, k, l) 16x16 blok büyüklüğü ile algoritma çıktısı, (d, g, j) algoritmanın tespit ettiği bölgeler, (e, h, k) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i, l) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri



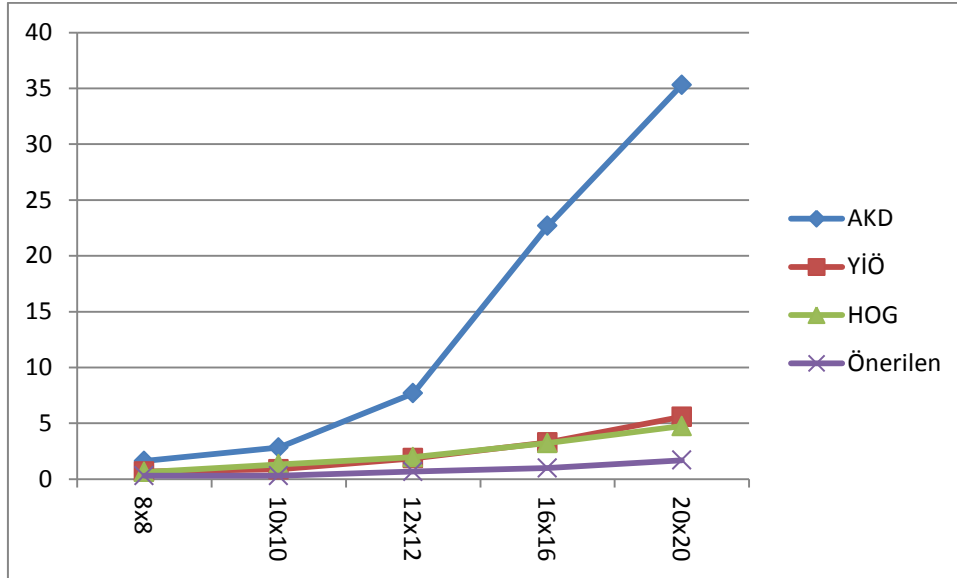
Resim 6.8. Önerilen yöntemin 8×8 blok büyüklüğü ve farklı T_1 parametre değeri ile algoritma çıktıları, (a) orijinal görüntü, (b) sahte görüntü, (c) kesin referans, (d, e, f) $T_1 = 150$ ayarlanarak elde edilmiş algoritma çıktısı, (g, h, i) $T_1 = 30$ ayarlanarak elde edilmiş algoritma çıktısı, (d, g) algoritmanın tespit ettiği bölgeler, (e, h) algoritmanın tespit ettiği bölgelerin ikili maskelenmiş gösterimi, (f, i) algoritmanın tespit edemediği bölgeleri ifade eden yanlış negatif gösterimleri

Ayrıca önerilen yöntemin, AKD, YİÖ ve HOG yöntemleri ile denenen 40 farklı görüntü üzerindeki blok büyüklüğüne bağlı olarak D, YPO ve YNO değişimleri karşılaştırmalı grafikleri sırasıyla Şekil 6.2, 6.3 ve 6.4'te verilmiştir.



Şekil 6.2. Blok büyüklüğüne bağlı doğruluk karşılaştırması

Şekil 6.2’de verilen grafikte yöntemlerin blok büyüklüğüne bağlı doğru tahmin değeri karşılaştırması verilmiştir. YİÖ ve HOG yöntemleri 8x8 ve 20x20 blok büyüklükleri arasında yakın başarı oranı göstermektedir ve blok büyüklüğü arttıkça başarıları %95 seviyelerine inmektedir. Grafikte görüleceği üzere önerilen yöntem dâhil bütün yöntemlerin doğru tahmin değeri blok büyüklüğü artması ile düşmektedir. Özellikle, öznitelik çıkarımı olarak yalnızca AKD kullanılan yöntemin başarısı 12x12’lik blok büyüklüğünden sonra keskin bir düşüş yaşamaktadır. Yöntemler küçük blok büyüklüklerinde daha yüksek başarı sağlamaktadır. Özellikle önerdiğimiz yöntemde 8x8 blok büyüklüğünde %99,55 oranında yüksek başarı elde ettik. Ancak blok büyüklüğünü azaltmak hesaplama maliyetini artırmaktadır. Bu yüzden üzerinde çalışılan görüntünün boyutuna göre deneyerek uygun blok büyüklüğü ayarlanarak çalışılmalıdır. Bütün yöntemlerin başarısı blok büyüklüğü arttıkça düşüş gösterse de önerilen yöntemin başarısının diğer yöntemlere göre en az düşüş gösterdiği ve %95 seviyeleri altına düşmediği görülebilir.

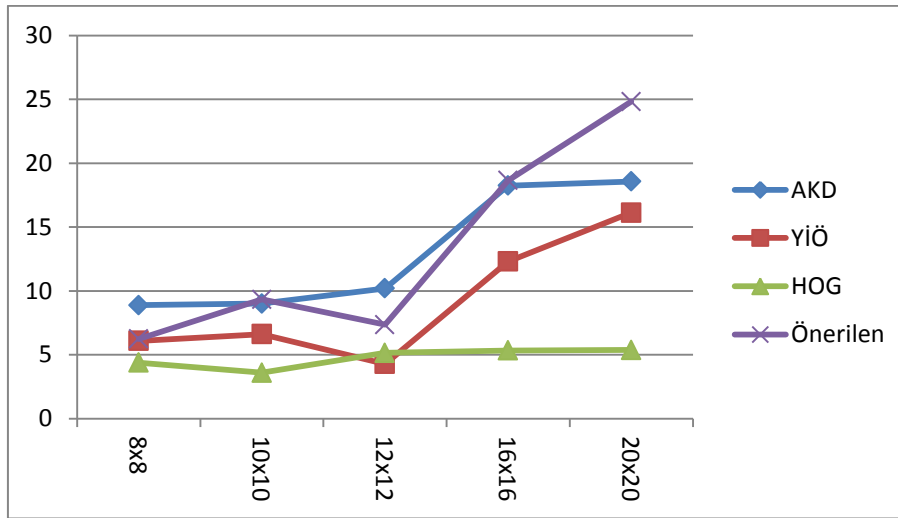


Şekil 6.3. Blok büyüklüğüne bağlı YPO karşılaştırması

Şekil 6.3'teki grafikte yöntemlerin blok büyüklüğüne bağlı YPO değişimi karşılaştırmalı olarak verilmiştir. Grafik incelendiğinde yöntemlerin YPO blok büyüklüğü arttıkça artmaktadır. Ancak önerilen yöntemin YPO diğer yöntemlere göre daha az artış göstermektedir. Şekil 6.2 ve 6.3'teki grafikler birlikte ve doğru değerlendirildiğinde yöntemlerin doğru tahmin değeri ile YPO arasında ters orantı olduğu anlaşılabılır. Blok büyüklüğü arttıkça YİÖ ve HOG yöntemlerinin yanlış pozitif oranı 8x8 ve 20x20 blok büyüklükleri arasında benzer artış gösterir ve %5 oranlarına kadar çıkmaktadır. Bu oran bu iki yöntem için makul bir değer sayılsa da AKD'nin YPO artışı 12x12 blok büyüklüğünden sonra hızlı bir artış göstererek %35 seviyelerine çıkmaktadır. Önerilen yöntemin YPO blok büyüklüğü artması ile artış gösterse de 8x8 ve 20x20 blok büyüklükleri arasında %1,70 değerini geçmemiş ve diğer yöntemlere göre yüksek başarı sağlamıştır.

Bazı görüntüler için T_1 ve T_2 parametre değerlerini artırarak yöntemlerin YPO'sunda bir düşüş sağlanması mümkün olsa da, bu durum daha önceki algoritma çıktıların verildiği deneme görüntülerinde gözlemlenebileceği gibi, görüntüde yer alan kopyala taşı sahteciliği uygulanmış küçük görüntü bloklarının tespit edilmesine engel olabilmektedir. Bu tür sahtecilik uygulanmış küçük görüntü bloklarının tespit edilememesini etkileyen diğer bir parametrede algoritmada kullanılan blok büyüklüğüdür. Blok büyüklüğünün, görüntüde sahtecilik uygulanmış ancak algoritmanın sahtecilik olarak işaretlenmediği

görüntü bloklarını ifade eden YNO'yu nasıl etkilediğini Şekil 6.4'te verilen grafikte inceleyebiliriz. Grafik incelendiğinde, yöntemlerde kullanılan blok büyüklüğü arttıkça kopyala taşı sahteciliği uygulanmış küçük görüntü bölgelerin tamamı bulunamamaktadır ve buna bağlı olarak önerilen ve karşılaştırılan yöntemlerde YNO arttığı görülmektedir. Ancak blok büyüklüğüne bağlı olarak sahtecilik uygulanan küçük görüntü bloklarının tespit edilememesine bağlı YNO en çok artış gösteren yöntem önerilen yöntemdir. Hesaplama piksel bazlı yapıldığı için önerilen yöntem, kopyala taşı sahteciliği ile çoğaltılmış görüntü bloklarının genel olarak yerlerini bulsa da, sahtecilik uygulanmış blokların tamamını tespit edemediği için YNO yüksek çıkmaktadır. Bu durumu incelemek için Resim 6.8'deki görüntü ele alınabilir. Resimde (h)'de yer alan görüntüde önerdiğimiz yöntemin sahtecilik uygulanmış bölgeler olarak tespit ettiği görüntü blokları ikili maskelenmiştir. Bu görüntü (c)'de yer alan kesin referans ile yanlış pozitif olarak işaretlenmiş beyaz noktacıklar dışında benzerlik göstermektedir. Yine aynı resimde (i)'de algoritmanın YN görüntüsü yer almakta. Bu görüntüde anlaşılacağı gibi, algoritma sahtecilik uygulanmış görüntü bloklarının yerlerini eksiksiz tespit etmesine rağmen, sahtecilik uygulanmış görüntü bloğu çevresinde kalan bazı küçük blokları tespit edememiştir. Bu yüzden önerilen yöntemin YNO diğer yöntemlere göre daha fazla çıkabilmektedir.

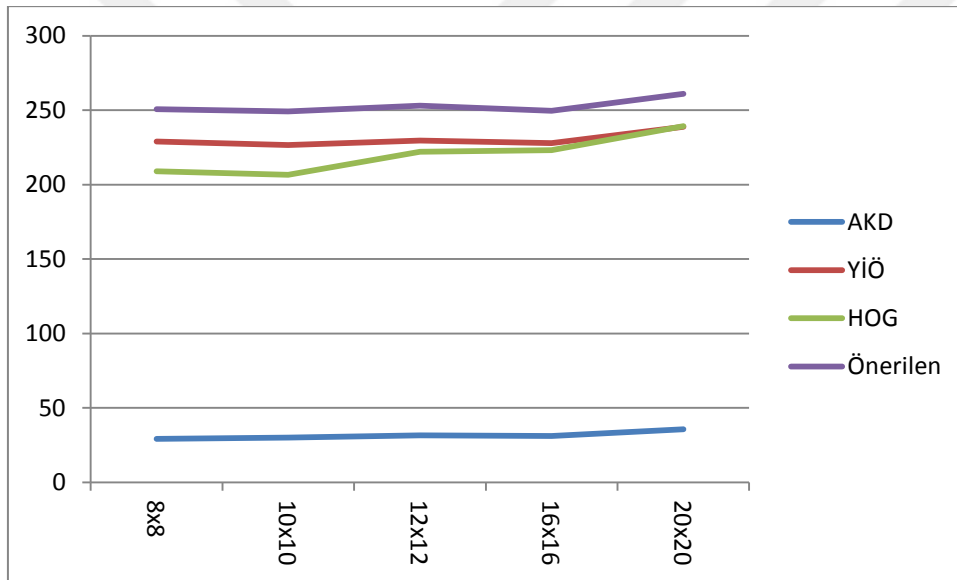


Şekil 6.4. Blok büyüklüğüne bağlı YNO karşılaştırması

Geliştirilen uygulama ayrıca görüntüde çoğaltılmış birden fazla görüntü bölgesi olması durumunda da bölgeleri başarıyla tespit edebilmiştir. Ancak buna karşın deneme sonuçlarından da görüleceği gibi yanlış algılanmış bölgeler de yer almaktadır. Deneme

sonuçları Resim 6.5 ve 6.6 ve 6.7’de incelenebilir.

Yöntemimizde YİÖ ve AKD’yi arka arkaya her blok için uyguladığımızdan, hesaplama zamanı açısından bu iki yöntemin ayrı ayrı kullanıldığı yöntemlere göre yüksek maliyete sahiptir. Deneme görüntüleri üzerindeki algoritma çıktılarını Intel Core i5 CPU’ya ve 2.5 GHz işlemci hızına sahip ve Windows 8 64 bit işletim sistemi kurulu HP dizüstü bilgisayar üzerinde elde ettik. Yöntemlerin hesaplama zamanı açısından karşılaştırması Şekil 6.5’te verilen grafikte görülebilir. Hesaplamalar denenen 40 farklı görüntü için farklı blok büyüklüklerine bağlı olarak ortalama hesaplama zamanları alınarak saniye bazında verilmiştir.



Şekil 6.5. Hesaplama zamanına göre karşılaştırma grafiği

7. SONUÇ VE ÖNERİLER

Kopyala taşı sahteciliğinin tespitinde ilk kez YİÖ ve AKD'yi birlikte kullanarak blok tabanlı bir yöntem önerdik. YİÖ ile görüntünün doku farklılıklarını tanımlama yeteneğini kullanmayı ve öznelik çıkarımında YİÖ'nün değişen aydınlatma koşullarına karşı duyarlılığını, AKD ile aşmayı amaçladık. Böylece aydınlatma koşullarına karşı daha az duyarlı öznelikler ile yanlış pozitif oranını düşürdük. Görüntüyü birbiriyle örtüşen bxb'lik bloklara böldükten sonra her bloğa önce YİÖ uyguladık ve YİÖ alanına dönüştürdüğümüz görüntü bloğuna AKD uygulayarak öznelik vektörlerini elde ettik. Önerdiğimiz yöntemi, HOG, YİÖ ve AKD öznelik çıkarımı yöntemlerini ayrı ayrı kullanan kopyala taşı sahteciliği tespiti yöntemleriyle karşılaştırdık. Önerdiğimiz yöntemi ve karşılaştırdığımız yöntemleri CoMoFoD veri tabanından aldığımız 40 farklı sahte görüntü üzerinde denedik. Denenen görüntülerden 12 adet görüntü, kopyalanan alan birden fazla bölgeye yapıştırılarak ve 7 adet görüntüde ise birden fazla farklı bölge kopyala taşı sahteciliği ile çoğaltılarak elde edilmiştir. Ayrıca sahtecilik uygulanmış görüntü blokları düzgün çoğaltılmış değildir. Veri tabanında görüntülere ait, sahtecilik uygulanmış görüntü blokların ikili maskelenmiş gösterimi yer almaktadır ve biz bu görüntüyü kesin referans olarak kullandık. Algoritma çıktılarımızı kesin referans ile karşılaştırdık ve yöntemlerin doğruluğunu ve başarı sonuçlarını piksel bazında hesaplanan DP, YP, DN ve YN oranlarını dikkate alarak hesapladık. Denemelerimizi 8x8, 10x10, 12x12, 16x16 ve 20x20 farklı blok büyüklüklerinde tekrarladık. Kullanılan blok büyüklüğü arttıkça önerilen yöntem dahil bütün yöntemlerin başarısı düşmekte ve YPO artmaktadır. Ancak denenen bütün blok büyüklüklerinde önerilen yöntemin doğruluğu ve başarısı diğer yöntemlere göre daha yüksek ve YPO daha düşüktür. Denediğimiz blok büyüklüklerinde en yüksek başarıyı 8x8 blok büyüklüğünde elde ettik ve %99,55 doğruluk ile %0,30 YPO elde ederek diğer yöntemlere göre yüksek başarı sağladık.

Blok tabanlı kopyala taşı görüntü sahteciliği tespiti yöntemlerinde, kullanılan blok büyüklüğünden daha küçük sahtecilik uygulanmış görüntü blokları tespit edilemezler. Bu yüzden algoritmalarda kullanılan blok büyüklüğünü ve blok büyüklüğüne bağlı ayarlanan parametreleri iyi belirlemek gerekmektedir. Blok büyüklüğünü artırdıkça yöntemin hem doğruluğu düşmekte, hem de YPO ve YNO artmaktadır. Ancak blok büyüklüğünü küçültmekte yöntemin hesaplama maliyetini artırmaktadır. O yüzden kullanılan blok

büyükülüğü üzerinde çalışılacak görüntülerin büyüklüğüne bağlı olarak optimum blok büyüklüğü ile çalışılmalıdır. Önerdiğimiz yöntemin blok büyüklüğüne bağlı olarak YNO'daki artışı diğer yöntemlere göre daha fazla olmaktadır. Bu yüzden görüntüde yer alan kopyala taşı sahteciliği uygulanmış görüntü bölgelerinin tamamının önerilen yöntem tarafından tespit edilemediği bazı görüntülerde, öznitelik çıkarımı için YİÖ'nün tek başına kullanıldığı ve HOG öznitelik çıkarımı yönteminin kullanıldığı yöntemlerin yanlış negatif oranı önerilen yöntemle göre daha düşük olabilmektedir. Bu görüntüler için algoritmada kullandığımız T_1 ve T_2 parametrelerini azaltarak önerdiğimiz yöntemin YNO'sunu azaltabilmek mümkün oluyor ancak bu durumda YPO artabilmektedir. Ayrıca bahsettiğimiz görüntüler için bile önerdiğimiz yöntemin YNO, karşılaştırdığımız diğer görüntülere göre yüksek olsa da YPO daha düşük ve doğruluğu daha yüksek olabilmektedir. Önerdiğimiz yöntemin YNO'nun yüksek olmasının bir sebebi de hesaplamalarımızı piksel bazında yapmamızdır. Çünkü önerilen yöntem görüntüde yer alan çoğaltılmış bölgelerin yerlerini tespit edip büyük kısmını işaretlese bile sahtecilik uygulanmış görüntü parçasının tamamını işaretleyemediği için bu bölgenin çevresinde kalan görüntü blokları YNO'nun artmasına sebep olmaktadır.

Önerdiğimiz yöntem aynı görüntü içerisinde yer alan birden fazla görüntü bloğunun çoğaltıldığı görüntüler üzerinde de karşılaştırılan diğer yöntemlere göre daha yüksek doğruluk ile görüntü bölgelerini tespit edebilmektedir.

Önerilen yöntem YİÖ ve AKD'yi blok tabanlı kopyala taşı sahteciliği tespitinde kullanmasıyla bir ilk olmasıyla birlikte, gri seviyeli görüntüler üzerinde çalışmaktadır. İlerleyen çalışmalarda, önerilen yöntemin renkli görüntüler üzerinde çalışması ve döndürme, ölçeklendirme, JPEG sıkıştırması ve gürültü ekleme gibi bazı son işlem adımları uygulanmış sahteciliklerin tespiti için uyarlanması planlanmaktadır. Ayrıca önerilen yöntem YİÖ ve AKD öznitelik çıkarım yöntemlerini arka arkaya uyguladığı için hesaplama maliyeti yüksektir. Bu iki yöntemin tek işlem adımıyla birleştirilmesi ile algoritmanın performansı optimize edilebilir. Ayrıca daha büyük blok büyüklükleri için YNO'nun azaltılması ve yöntemin başarısının artırılması için iyileştirmeler yapılacaktır.

KAYNAKLAR

1. Ansari, M. D., Ghrera, S. P. ve Tyagi, V. (2014). Pixel-Based Image Forgery Detection A Review. *IETE Journal of Education*, 55(1), 40-46.
2. Cox, I. J., Miller, M. L. and Bloom, J. A. (2002). *Digital Watermarking*. Multimedia Information and Systems, San Francisco: Academic Press, 41-83.
3. Katzenbeisser, S. ve Petitcolas, F. A. P. (2000). *Information Techniques for Steganography and Digital Watermarking*. Norwood, MA: Artec House, 95-119.
4. Farid, H. (2009). A survey of image forgery detection. *IEEE Signal Processing Magazine*, 26(2), 16-25.
5. Tyagi, V. (2010). *Detection of forgery in images stored in digital form*. International Journal of Computer Applications, 5(12), 9-12.
6. Christlein, V., Riess, C. ve Jordan, J. (2012). An Evaluation of Popular Copy-Move Forgery Detection Approaches. *IEEE Information Forensics and Security*, 7(6), 1841 - 1854.
7. Kirchner, M. (2008). *Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue*. 10th ACM Multimedia and Security Workshop, New York.
8. Mahdian, B. ve Saic, S. (2008). Blind authentication using periodic properties of interpolation. *IEEE Trans. Inform. Forensics Security*, 3(3), 529–538.
9. Popescu, A. C. ve Farid, H. (2004). *Exposing Digital Forgeries by Detecting Duplicated Image Regions*, Yüksek Lisans Tezi, Dartmouth College Department of Computer Science, Dartmouth.
10. Prasad, S. ve Ramakrishnan, K. R. (2006, 9-12 Haziran). *On resampling detection and its application to image tampering*. IEEE International Conference on Multimedia and Expo, Toronto, Canada.
11. Gallagher, A. C. (2005, 9-11 Mayıs). *Detection of linear and cubic interpolation in jpeg compressed images*. The 2nd Canadian Conference on Computer and Robot Vision (CRV'05), British Columbia, Canada.
12. Qu, Z., Qiu, G. ve Huang, J. (2009). Detect digital image splicing with visual cues. *Springer Link, Information Hiding*, 5806(1), 247-261.
13. Farid, H. (1999). *Detecting digital forgeries using bispectral analysis*. Massachusetts Institute of Technology, Perceptual Science Group, MIT, Cambridge.
14. Ng, T. T. ve Chang, S. F. (2004, 24-27 Ekim). *A model for image splicing*. IEEE Int. Conference Image Processing, Singapore, 1169–1172.

15. Bayram, S., Avcibas, I., Sankur, B. ve Memon, N. (2005, 4-8 Eylül) *Image manipulation detection with binary similarity measures*. 13th European Signal Processing Conference, Türkiye, Antalya.
16. Bayram, S., Avcibas, I., Sankur, B. ve Memon, N. (2006). Image manipulation detection. *Journal of Electronic Imaging by SPIE*, 15(4), 41102, 1-17.
17. Farid, H. ve Lyu, S. (2003, 16-22 Haziran). *Higher-order wavelet statistics and their application to digital forensics*. 3th Computer Vision and Pattern Recognition Workshop, Madison, Wisconsin, USA.
18. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. D. ve 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.
19. Huang, H., Guo, W. ve Zhang, Y. (2008, 19-20 Aralık). *Detection of copy-move forgery in digital images using SIFT algorithm*. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan.
20. Pan, X. ve Lyu, S. (2010). Region duplication detection using image feature matching. *IEEE Transactions On Information Forensics And Security*, 5(4), 857–867.
21. Bravo-Solorio, S. ve Nandi, A. K. (2011, 22-27 Mayıs). *Exposing duplicated regions affected by reflection, rotation and scaling*. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague.
22. Fridrich, A. J., Soukal, B. D. ve Lukas, A. J. (2003, 6-8 Ağustos). *Detection of copy-move forgery in digital images*. Proceedings of Digital Forensic Research Workshop, Trumansburg.
23. Kang, X. ve Wei, S. (2008, 12-14 Aralık). *Identifying tampered regions using singular value decomposition in digital image forensics*. International Conference on Computer Science and Software Engineering, Wuhan, Hubei.
24. Li, G., Wu, Q., Tu, D. ve Sun, S. (2007, 2-5 Temmuz). *A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD*. IEEE International Conference on Multimedia and Expo, Beijing.
25. Ryu, S. J., Lee, M. J. ve Lee, H. K. (2010, 28-30 Haziran). *Detection of Copy-Rotate-Move Forgery Using Zernike Moments*. 12th International Information Hiding Conference, Canada.
26. Wang, J., Liu, G., Li, H., Dai, Y. ve Wang, Z. (2009, 18-20 Kasım). *Detection of image region duplication forgery using model with circle block*. International Conference on Multimedia Information Networking and Security Hubei.
27. Zhang, J., Feng, Z. ve Su, Y. (2008, 19-21 Kasım). *A new approach for detecting Copy-Move forgery in digital images*. 11th IEEE Singapore International Conference on Communication Systems, Guangzhou.
28. Christlein, V., Riess, C. ve Angelopoulou, E. (2010, 5-7 Ekim). *A study on features for the detection of copy-move forgeries*. SICHERHEIT, Berlin, Germany.

29. Zimba, M. ve Xingming, S. (2011). DWT-PCA (EVD) Based Copy-move Image Forgery Detection. *International Journal of Digital Content Technology and its Applications*, 5(1), 251-258.
30. Ghorbani, M., Firouzmand, M. ve Faraahi, A. (2011, 16-18 Haziran). *DWT-DCT (QCD) based copy-move image forgery detection*. 18th Systems, Signals and Image Processing (IWSSIP), Sarajevo.
31. Luo, W., Huang, J. ve Qiu, G. (2006, 20-24 Ağustos). *Robust detection of region-duplication forgery in digital images*. 18th International Conference on Pattern Recognition (ICPR'06), Hong Kong.
32. Wandji, N. D. ve 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), China.
33. Muhammad, G., Hussain, M., Khawaji, K. ve Bebis, G. (2011, 6-8 Temmuz). *Blind copy move image forgery detection using dyadic undecimated wavelet transform*. 17th International Conference on Digital Signal Processing (DSP).
34. Kestenci, S. ve Ulutas, G. (2013, 2-4 Temmuz). *Copy-Move Forgery Detection in Images via 2D-Fourier Transform*. 36th International Conference on Telecommunications and Signal Processing (TSP), Rome.
35. Li, L., Li, S., Zhu, H. ve Wu, X. (2014). Detecting copy-move forgery under affine transforms for image forensics. *Computers & Electrical Engineering on Elsevier*, 40(6), 1951–1962.
36. Kaur, R. (2014). Copy-Move Forgery Detection Utilizing Local Binary Patterns. *International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*, 164(14), 290-294.
37. Kumar, S., Desai, J. V. ve Mukherjee, S. (2015). Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 7(6), 38-44.
38. Lin, H. J., Wang, C. W. ve Kao, Y. T. (2009). Fast copy-move forgery detection. *WSEAS Transaction on Signal Processing*, 5(5), 188-197.
39. Kang, L. ve Cheng, X. P. (2010, 16-18 Ekim). *Copy-move forgery detection in digital image*. 3rd International Congress on Image and Signal Processing (CISP 2010), Yantai.
40. Huang, Y., Lu, W., Sun, W. ve Long, D. (2011). Improved DCT-based detection of copy-move forgery in images. *Forensic Science International*, 206(1-3), 178-184.
41. Cao, Y., Gao, T. ve Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. *Forensic Science International*, 2014(1-3), 33-43.
42. N. Dalal ve B. Triggs. (2005, 25 Haziran). *Histograms of oriented gradients for human detection*. IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA.

43. İnternet: Tralic D. Zupancic I. Grgic S. ve Grgic M. (5, 2013). CoMoFoD - Image Database for Copy-Move Forgery Detection. *University of Zagreb, Faculty of Electrical Engineering and Computing Department of Wireless Communications Video Communications Laboratory (VCL)*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.vcl.fer.hr%2Fcomofod%2F&date=2016-06-14>, Son Eriřim Tarihi: 30.05.2016.
44. Tralic D. Zupancic I. Grgic S. ve Grgic M. (2013, 25-27 Eylül). *CoMoFoD - New Database for Copy-Move Forgery Detection*. 55th International Symposium ELMAR-2013, Zadar.
45. Lee, J.C., Chang, C.P. ve Chen, W.K. (2015). Detection of copy-move image forgery using histogram of orientated gradients. *Information Sciences, Informatics and Computer Science Intelligent Systems Applications*, 3(21), 250-262.
46. Ulutas, G., Ulutas, M. ve Nabiyeve, V. (2013, 24-26 Nisan). *Copy move forgery detection based on LBP*. 21. IEEE Sinyal İřleme ve İletiřim Uygulamaları Kurultayı, Kuzey Kıbrıs Türk Cumhuriyeti.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : BOZ, Ahmet
 Uyruğu : T.C.
 Doğum tarihi ve yeri : 01.09.1989, Yozgat
 Medeni hali : Evli
 Telefon : 0 (541) 2688260
 Faks : BOZ
 E-Posta : ahmetboz0508@gmail.com



Eğitim

Derece	Okul/Program	Mezuniyet tarihi
Yüksek Lisans	Gazi Üniversitesi/Bilgisayar Mühendisliği	2016
Lisans	Ege Üniversitesi/Bilgisayar Mühendisliği	2012
Lise	Sorgun Anadolu Lisesi	2007

İş Deneyimi

Yıl	Çalıştığı Yer	Görev
2012-2013	İnnova Bilişim Çözümleri A.Ş.	Yazılım Uzmanı
2013-Halen	TÜBİTAK	Yazılım Uzmanı

Yabancı Dil

İngilizce

Yayınlar

Boz, A., Bilge, H. S. (2016, 16-19 Mayıs). *Görüntülerde Kopyala Taşı Sahteciliğinin YİÖ ve AKD Tabanlı Tespiti*. 24. IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı, Zonguldak, Türkiye.

Hobiler

Yeni Teknolojileri Araştırmak



GAZİ GELECEKTİR...