

## SAYISAL İMGELER İÇİN PRNU VE CNN TABANLI BÖLGESEL MÜDAHALE TESPİTİ

*Ahmet Gökhan POYRAZ\**

Alınma:22.01.2019; düzeltme: 23.05.2019; kabul: 30.05.2019

**Öz:** Sayısal resimler üzerinde yapılan çeşitli oynamaları tespit edebilmek, gelişen yazılımların karmaşıklığından ötürü oldukça zorlaşmaktadır. Bu karmaşıklığa çözüm olarak klasik müdahale tespiti yöntemlerine ek olarak son yıllarda evrimsel sinir ağı tabanlı yöntemler geliştirilmiştir. Böylelikle çok karmaşık müdahaleleri bile tespit edebilen ağlar eğitilebilmiştir. Bu makalede, küçük boyutlarda pencere kullanarak bölgesel müdahale tespiti yapabilen klasik yöntemlerden olan, kameranın kendisine ait olan sensörlerinden elde edilen parmakizini kullanan sensör tabanlı PRNU(Photo Response Non Uniformity) yöntemi ile yeni bir yaklaşım olan evrimsel sinir ağı(CNN) tabanlı kamera model sınıflandırıcısı yöntemi karşılaştırılmıştır. Böylelikle hangi yöntemin daha başarılı olduğu detaylıca ortaya koyulmuştur. Toplamda 26 adet kamera modeli ve bu kamera modellerinden seçilen 96 x 96'lık piksel blokları ile eğitilen CNN modeli, hem 96 hem de 128'lik pencere boyutu kullanılarak çalışan PRNU yöntemi ile kıyaslanmıştır. Bu kıyaslama sonucunda bölgesel müdahale tespiti probleminde CNN tabanlı kamera model sınıflandırıcısının PRNU yöntemine göre daha başarılı olduğu gösterilmiştir.

**Anahtar Kelimeler:** Lokal müdahale tespiti, evrimsel sinir ağı, PRNU, oynanmış bölge tespiti, kamera model sınıflandırıcısı, derin öğrenme

### PRNU and CNN Based Local Tamper Detection For Digital Images

**Abstract:** Detecting various forgeries on digital images is becoming more difficult due to the complexity of developing software. As a solution to this complexity, in addition to conventional detection methods, convolutional neural network (CNN) based methods have been developed in recent years. Thus, networks capable of detecting even very complex interventions could be trained. In this paper, a new approach to the convolutional neural network (CNN) based camera model classifier method is compared with the sensor-based PRNU (Photo Response Non Uniformity) method, which is one of the classical methods that can detect local detection using small-scale windows. Thus, which method is more successful is revealed in detail. A total of 26 camera models and the CNN model, which was trained with 96 x 96 pixel blocks selected from these camera models, was compared with the PRNU method using both the 96 and 128 window size. As a result of this comparison, CNN based camera model classifier has been shown to be more successful than PRNU method in the local tamper detection problem.

**Keywords:** Local tamper detection, convolutional neural network, PRNU, image forgery, camera model classifier, deep learning

\* Uludağ Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Mühendisliği, Görükle-Bursa TÜRKİYE

İletişim Yazarı: Ahmet Gökhan POYRAZ (agpoyraz@gmail.com)

## 1. GİRİŞ

Sosyal medyanın kullanımının artması ve sosyal medya mecralarının çoğalmasıyla birlikte bilgi paylaşımı, özellikle bu sayısal ortamda resim ve video paylaşımını oldukça arttırmıştır. Ancak bu durum internet üzerinde paylaşılan bilgilerin güvenilirliği konusunu tartışmaya açmıştır. Güncel yazılımlar kullanılarak artık bir sayısal resmi manipüle etmek oldukça basit bir işlem haline geldi. Hatta cep telefonlarında artık kolaylıkla manipüle işlemi gerçekleştirilebiliyor. Bu oynamalarda, manipüle ya da filtreleme işlemleri yapılırken kötü niyet taşınmasa bile, başkaları tarafından yanlış işler için kullanılıp kullanılmayacağından emin olamayız. Örneğin bir haber kanalına oynanmış bir resmi gerçekmiş gibi gönderip insanları kandırmak mümkündür. Bu gelişmelerle birlikte adli bilişim alanında resimlerdeki bütünsel veya bölgesel müdahale tespiti oldukça önem kazanmıştır.

Adli bilişim konusunda çalışan araştırmacılar bu probleme çözüm olarak çeşitli yöntemler sunmuştur. Bu yöntemler arasında PRNU tabanlı kaynak cihaz tanıma (Miroslav Goljan ve diğ. 2009 ) yöntemi en önde gelen yöntemlerden biridir. Temel olarak kamera cihazının değişmeyen sensör özelliklerini kullanarak bir sayısal resmin test edilen kamera cihazına ait olup olmadığı basit bir korelasyon formülüyle saptanabilmektedir. Z. Lin ve diğ. (2009) çifte sıralı kuantalama tespitini önermişlerdir. Bu yöntemde 8 x 8 piksel blokları kullanılarak çifte JPEG sıkıştırması yapılan resimlerdeki izler tespit edilerek kameraya ait olmayan bölgeler tespit edilmeye çalışılmıştır. Ferrara, P. ve diğ. (2012) resmin çekilmesi işlemi sırasında renkli filtreden geçirilme işleminin baz almıştır. Renk filtresinden kaynaklanan örüntü istatistiğini inceleyerek resim üzerindeki farklı olabilecek olan kısmı bulmayı hedeflemiştir. Krawetz ve diğ. (2007) bir resmin belirli bölgelerinin diğer bölgelerine göre daha az seviyede JPEG sıkıştırması yapıldığında, bu bölgeyi hata analiz yöntemiyle bulmayı hedeflemişlerdir. Farid (2009), resim üzerindeki düşük JPEG kalitesinde kaydedilen bölgeyi bularak oynanmış bölgeyi tespit etmeyi hedeflemiştir. Temel olarak irdelenen resim ile, resmin farklı seviyede sıkıştırılmış versiyonlarıyla arasındaki karesel farka bakarak bölgesel minimum noktayı bulmayı hedeflemektedir. Dirik, A. E. ve Memon, N. (2009) Bayer örüntüsü içindeki renk filtesini tahmin ederek oynanmış bölge tespiti yapabilen bir yöntem sunmuşlardır. Ye, S. ve diğ. (2007) resim içerisindeki güvenilir bloklardan kuantalama matrisini tahmin ederek JPEG ayrık kosinüs dönüşümü dağılımdaki tutarsız bölgeleri bulabilmektedir.

Son yıllarda derin öğrenme tabanlı yöntemler de adli bilişim alanında kullanılmaya başlandı. Özellikle CNN tabanlı kamera model tanıma çalışmaları Luca Bondi ve diğ. (2017) ve Amel Tuama ve diğ. (2016) ekipleri tarafından yapılmıştır. Bu çalışmalarda derin öğrenme yaklaşımı kullanılarak kamera modellerinde ait özelliklerin evrimsel sinir ağları tarafından çıkarılması sağlanmış, elde edilen özellikler sınıflandırılarak kamera modelleri arasında sınıflandırma yapabilen derin bir sinir ağı modeli oluşturulmuştur. Böylelikle bir resmin hangi marka ve model kameradan çekildiği tespit edilebilmektedir. Bu yöntemler küçük boyutlu pencereler kullanarak karar verdikleri için(Örn. 64x64 piksel) resmin geneli taranarak oynanmış bölgelerin tespiti mümkündür( Luca Bondi ve diğ. 2017a). Derin öğrenme tabanlı lokal müdahale tespiti uygulamaları da bulunmaktadır. Bayar ve diğ. (2016) genel olarak çalışabilen derin öğrenme tabanlı bir yöntem sunmuştur. Sunduğu yöntem ile belirlenen oynama çeşitlerini öğrenen derin öğrenme tabanlı bir makine eğitmiştir. Luca Bondi ve diğ.(2017-b) elinde bulunan bütün kamera modelleriyle CNN tabanlı bir kamera model sınıflandırıcısı eğitmiştir. Sunmuş olduğu algoritma ile kamera model bilgisine ihtiyaç duyulmadan genel çalışabilen bir lokal müdahale tespit edici geliştirmeyi hedeflemiştir. Benzer şekilde Yaqi Liu ve diğ.(2017) CNN tabanlı oynanmış bölge tespit edici sunmuşlardır. Ancak bu yöntemlerde kamera modeli eğeri bilinmiyorsa çok daha etkili çalıştığı gösterilmiştir.

Bu makalede kamera model tanıma kullanarak bölgesel müdahale tespit etme problemine çözüm olarak sunulan önde gelen yöntemlerden olan PRNU yöntemi ile CNN tabanlı kamera model tanıma kullanılarak yapılan lokal oynama tespiti yöntemi karşılaştırılacaktır. İki yöntemin de kamera model bilgisine ihtiyaç duyması bu karşılaştırmayı yapabilmemize olanak

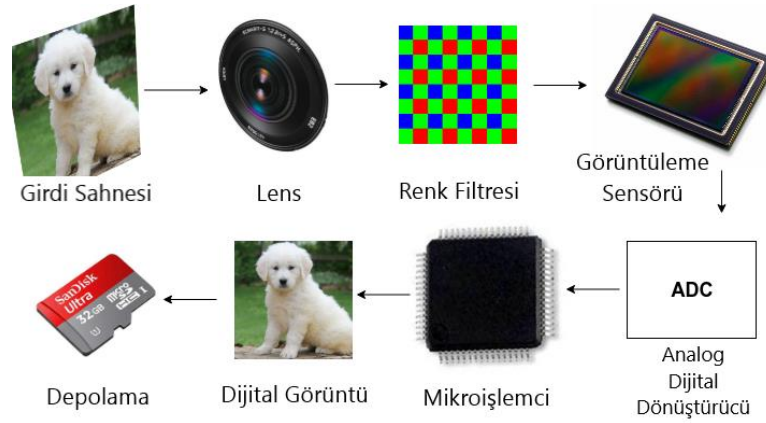
sağlamaktadır. Özellikle küçük boyutta pencereler seçilerek bu iki farklı temel yöntemin bölgesel müdahaleleri tespit etmedeki başarısı incelenmiştir. PRNU yönteminin kameranın değişmeyen sensör özelliğini kullanmasına karşın, CNN tabanlı yöntem kameranın renk filtresini baz almaktadır. Hangi özelliğin daha başarılı sonuç ürettiğinin literatürde incelenmemiş olması açısından ve PRNU yönteminden daha iyi çalışabilen bir yöntemin gösterilmesi açısından makale bu alanda yenilik taşımaktadır.

Makalenin gidişatı şu şekildedir: 2. Karşılaştırılacak olan yöntemlerin anlatılması, 3. Kullanılan veri seti ve formatının anlatılması, 4. Deney sonuçlarının sunulması, 5. Sonuç.

## 2. KARŞILASTIRILAN YÖNTEMLER VE TEORİK ALTYAPILARI

### 2.1 PRNU Tabanlı Kamera Model Tanıma

Dijital kameralarda, resmi etkileyen bir takım gürültüler mevcuttur. Bu gürültülerden bazıları kameranın donanımından, bazıları ise harici olarak dışarıdan kaynaklanabilir. Bir resmin temel olarak çekilme aşaması adım adım Şekil 1’de gösterilmiştir.



**Şekil 1:**  
*Sayısal resmin çekilme aşamaları*

Kameranın içerisinde bulunan sensörler kendi yapısından kaynaklanan (materyal özelliği gibi) sebeplerden ötürü gelen ışığı ölçerken çok küçük miktarda sabit bir gürültü eklemektedir. Bu sensörler her kamerada farklı olduğu için bu değişmeyen gürültüler kameranın parmakizini oluşturuyor diyebiliriz. Miroslav Goljan ve diğ. (2009) bu değişmeyen parmakizini tahmin ederek kamera kaynak cihaz tanıma probleminde oldukça etkili çalışan bir çözüm sunmuşlardır. Ölçülen ışık miktarı  $I$  olmak üzere ışığı şu şekilde ifade etmek mümkündür:

$$I = I_0 + I_0 * F + \emptyset \quad (1)$$

Burada  $I_0$  gelen ışık miktarı,  $F$  sensörden kaynaklanan değişmeyen gürültü miktarı,  $\emptyset$  ise harici kaynaklardan gelen değişken gürültüdür. Buradaki değişmeyen  $F$  değerinin bulunabilmesi için ölçülen ışık gürültüden temizlenir. Bu işlem için genellikle Dalgacık (Wavelet) gürültü çıkarıcı (Lukas J. ve diğ. 2006) kullanılmaktadır.

$$\hat{I} = \text{gürültü\_çıkarıcı}(I) \quad (2)$$

Denklem 2’den yola çıkarak gürültü  $= I - \hat{I}$  yapılarak bulunabilir.  $\hat{G}$  gürültü olmak üzere

$$\hat{G} \cong I_0 * F + \emptyset \quad (3)$$

olarak yazılabilir. Denklem 3'teki  $\emptyset$ , değişken değerinde olduğu için aynı cihazdan çekilmiş birden fazla resim kullanılarak varyans değeri sifıra yaklaştırılabilir. Bu sebepten ötürü parmakizi tahmini yapılırken birden fazla resim(ideal sayı 50 ya da yukarısı olarak kabul edilmektedir) kullanılmaktadır. Bu adımdan sonra parmakizi Goljan M. ve diğ. (2009, Şubat) 'da verilen MLE'ye göre tahmini olarak hesaplanır. Hesaplanan tahmini parmakizi kullanılarak bir resmin test edilen cihaza ait olup olmadığı,  $\hat{F}$  tahmini parmakizi,  $I_t$  test edilen görüntünün parlaklık değeri,  $G$  test edilen resmin gürültüsü olmak üzere korelasyon

$$\rho = \text{corr}(G, I_t * \hat{F}) \quad (4)$$

denkleminde ya da PCE değeri Goljan M. ve diğ. (2009, Şubat) makalesindeki formülden hesaplanır.

Bu çalışmada PRNU yöntemi için öncelikle parmakizi tahmini gerçekleştirildi. Tahmini parmakizi oluşturulurken her bir hedef kamera için daha sonraki aşamalarda test ve eğitim kısmında kullanılmayan 50'şer adet görüntü seçilmiştir. Seçilen 50'şer adet görüntü kullanılarak hedef kameralar için parmakizi elde edilmiştir. Test edilecek olan her bir bloktan denklem (4)'teki korelasyon formülü kullanılarak  $\rho$  korelasyon değeri üretilmiştir. Ancak gürültü matrisi resim içerisinde seçilen her bir bloktan elde edilmek yerine, bloğun çıkarıldığı büyük resimden elde edilmiştir. Bu sayede gürültü daha doğru olacak şekilde çıkarılabilmektedir.

## 2.2 Evrişimsel Sinir Ağı Tabanlı Kamera Model Tanıma

Evrişimsel sinir ağı, yapay sinir ağlarının(YSA) bir alt kolu olarak insan beyninin sinir sistemi yapısından ilham alınarak oluşturulmuş bir yöntemdir. Özellikle obje tanıma, yüz tanıma ve segmente etme problemlerindeki başarısıyla son yıllarda popülerliğini arttırmıştır. Ayrıca adli bilişim alanında da kullanılmaya başlanmıştır. YSA ile CNN mantık olarak aynıdır. YSA'da her bir girdi, kendisi içindeki her bir düğüme ait olan ağırlık değeriyle çarpıldıktan sonra çıktı olarak bir diğer düğüm'e girdi olarak verilir. CNN'nın YSA'dan tek farklı yanı ise bu çarpım işleminde tek bir düğüm yerine filtre şeklinde çarpım olabilmektedir. Yani YSA'da her bir düğüm birbiriyle noktasal olarak çarpılırken, CNN'da belirli bir filtre (Örn.  $3 \times 3$ ,  $5 \times 5$  gibi) boyutuyla çarpım işlemi gerçekleştirilir. CNN, yapısında belirli katmanları bulundurmaktadır. Her bir katman kendisinden bir önceki katmandan gelen çıktıyı girdi olarak almaktadır. Bu girdiyi  $E \times B \times D$  (En, Boy, Derinlik) şeklinde gösterecek olursak  $g$  girdi,  $f$  filtre ve  $\chi$  çıktı olmak üzere girdi matrisi  $E_g \times B_g \times D_g$  ile filtre matrisi  $F_g \times F_g \times D_g$  çarpılarak çıktı matrisini  $E_\chi \times B_\chi \times D_\chi$  oluşturmaktadır. Sadece bütün-bağlı katmana gelindiğinde matris formundan vektör formuna dönüşmektedir( $D=1$ ). Bu çalışmada kullanılan CNN yapısını ve katmanlarını şu şekilde açıklayabiliriz:

**-Evrişim Katmanı:** Bu katmanda girdi olarak alınan  $E_g \times B_g \times D_g$  girdi matrisi ile filtre  $F_g \times F_g \times D_g$  matrisi belirlenen kaydırma miktarı  $A_t$ 'ye göre evrişim çarpımı ile çarpılır. Kaydırma miktarına bağlı olarak çıktının boyutu  $(E_g - F_g + 1) / A_t$  formülüne göre değişmektedir. Aynı formülde  $E$  yerine  $B$  yazılarak  $B_\chi$  de hesaplanır.

**-Bölütleme katmanı:** Hem yapılan çarpım sayısının azaltılabilmesi hem de girdi boyutunu istenen düzeye indirebilmek için bölütleme katmanı kullanılır. Bu çalışmada maksimum bölütleme kullanılmıştır. Şöyle ki; belirlenen  $A_t$ 'ye göre filtredeki en büyük sayı alınarak çıktı matrisine ya da vektörüne yazılır. Bu katman ile bazen elde edilen özellik matrislerindeki istenmeyen küçük değerler de ortadan kaldırılabilir.

**-Bütün-bağlı katman:** Girdinin matris boyutundan vektör boyutuna indikten sonraki kısımdır. Girdi vektörünün noktasal çarpım ile filtre vektörüyle çarpılması işlemi bu katmanda gerçekleştirilir. Burada kaydırma miktarı bulunmamaktadır.

**-ReLU katmanı:** Doğrusallığı ortadan kaldırabilmek için ReLU (rectifier linear unit) katmanı kullanılır. Bu çalışmada  $x$  düğüm girdisi olmak üzere  $\max(0, x)$  fonksiyonu kullanıldı. Oldukça

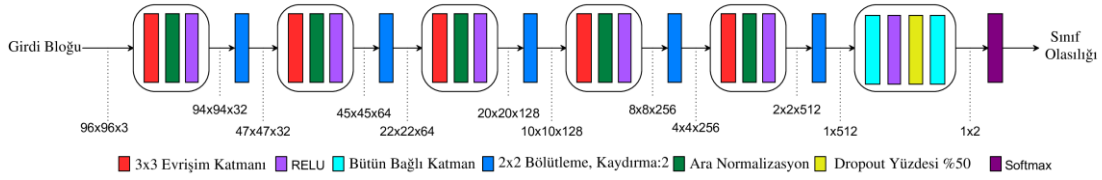
basit bir işlem olmasına rağmen modelin doğrusallığını değiştirdiği için eğitim başarısını arttırmaktadır.

**-Softmax katmanı:** Bütün bağlı katmandan elde edilen çıktı vektörünü toplamı 1 olacak şekilde olasılık değerlerine normalize eden katmandır.

**-Ara Normalizasyon katmanı:** Eğitim esnasında yapılan güncelleme işlemleri neticesinde veri dağılımı değişebilmektedir. Ara normalizasyon katmanı kullanılarak katmanlar arasındaki geçiş esnasında veriler normalize edilir.

**-Eksiltme (Dropout) katmanı:** Bütün-bağlı katmanda bazı bağlantıların koparılmasıyla modelin eğitim setini aşırı öğrenmesine engel olunur. Bu koparma işlemi rastgele olarak yapılır.

Öğrenme adımında YSA'dakine benzer şekilde düğümlerdeki her bir ağırlığın belirlenen güncelleme algoritmasına göre hatayı en aza indirecek değere getirilmesi amaçlanır. Bu çalışmada hata fonksiyonu olarak softmax loss fonksiyonu, güncelleme algoritması olarak da dereceli azalma algoritması kullanılmıştır.



**Şekil 2:**  
*Evrimsel Sinir Ağı Modeli*

CNN eğitimi yapılırken birçok farklı yapı denenmiştir. Deneysel olarak en iyi sonucu veren model Şekil 2'de gösterilmiştir. Farklı modeller denenirken küçük boyutta filtre kullanıldığında daha başarılı sonuçlar elde edildiği gözlemlenmiştir. CNN modelinde girdi olarak 96 x 96 piksel bloklar kullanılarak eğitim yapılmıştır. Her evrişim katmanından sonra ara normalizasyon katmanı hemen sonrasında da bölütleme katmanı kullanılmıştır. Ek olarak aşırı öğrenmeyi önlemek amacıyla eksiltme katmanı bütün-bağlı katmanda %50 olacak şekilde eklenmiştir.

PRNU yöntemi kullanılırken kamera cihazına ya da cihazdan elde edilmiş olan parmakzine ihtiyaç duyulmaktadır. Karşılaştırmanın daha adil olabilmesi açısından CNN eğitimi yapılırken kullanılan kamera modelleri hedef kamera ve diğerleri olmak üzere iki sınıftan oluşmaktadır. CNN eğitimi her bir hedef kamera için ayrıca yapılmıştır. Yani eğitilen her bir CNN ağı eğitildiği kamera modelini test etmektedir. Örneğin, Canon IXUS 70 modeli için eğitilen ağ'a 96 x 96 piksel boyutunda bir girdi verildiği zaman, eğitilmiş ağ verilen girdinin Canon IXUS 70'e ait olup olmadığını yüzdesel olarak üretmektedir. Bu sayede her bir kamera modelinden seçilen cihaz adil bir şekilde karşılaştırılmıştır.

### 3. KULLANILAN VERİ SETİ VE EĞİTİM PARAMETRELERİ

Bu çalışmada literatürdeki en çok kullanılan veri seti olan Dresden veri seti (Gloe, T., & Böhme, R. (2010, March)) tercih edilmiştir. Bu set içerisinde 26 adet kamera modelinden 74 tane cihaz bulunmaktadır. Eğitimde ve testlerde kullanılmak üzere 26 adet kamera modelinin her birinden 1'er adet cihaz seçilmiştir. Eğitim aşamasında kullanılan hedef(koyu renkli olanlar) ve hedef olmayan kamera modelleri Tablo 1'de gösterilmiştir.

**Tablo 1. Hedef olmayan kamera modelleri**

Marka	Model	Çözünürlük [Piksel]	Sensör Boyutu (inch ya da mm)	Odak Uzaklığı (mm)
AgfaPhoto	DC-504	4032×3024	-	7,1
AgfaPhoto	DC-733s	3072×2304	-	6,2–18,6
AgfaPhoto	DC-830i	3264×2448	-	6,2–18,6
AgfaPhoto	Sensor 505-X	2592×1944	-	7,5
AgfaPhoto	Sensor 530s	4032×3024	-	6,1–18,3
Canon	Ixus 55	2592×1944	1/2,5”	5,8–17,4
Casio	EX-Z150	3264×2448	1/2,5”	4,65–18,6
Kodak	M1063	3664×2748	1/2,33”	5,7–17,1
Nikon	Coolpix S710	4352×3264	1/1,72”	6,0–21,6
Nikon	D70/D70s	3008×2000	23,7×15,6 mm	18–200
Nikon	D70	3008×2000	23,7×15,6 mm	18–200
Nikon	D200 Lens A/B	3872×2592	23,6×15,8 mm	18–135/17–55
Olympus	μ1050SW	3648×2736	1/2,33”	6,7–20,1
Panasonic	DMC-FZ50	3648×2736	1/1,8”	7,4–88,8
Pentax	Optio A40	4000×3000	1/1,7”	7,9–23,7
Pentax	Optio W60	3648×2736	1/2,3”	5,0–25,0
Praktica	DCZ 5,9	2560×1920	1/2,5”	5,4–16,2
Rollei	RCP-7325XS	3072×2304	1/2,5”	5,8–17,4
Samsung	L74wide	3072×2304	1/2,5”	4,7–16,7
Samsung	NV15	3648×2736	1/1,8”	7,3–21,9
Sony	DSC-H50	3456×2592	1/2,3”	5,2–78,0
Sony	DSC-T77	3648×2736	1/2,3”	6,18–24,7
Sony	DSC-W170	3648×2736	1/2,3”	5,0–25,0

**Tablo 2. Hedef kamera modelleri**

Marka	Model	Çözünürlük [Piksel]	Sensör Boyutu (inch ya da mm)	Odak Uzaklığı (mm)
Canon	Ixus 70	3072×2304	1/2,5”	5,8–17,4
Fujifilm	FinePix J50	3264×2448	1/2,5”	6,2–31,0
Ricoh	Capilo GX100	3648×2736	1/1,75”	5,1–15,3

Her bir kameraya ait CNN eğitiminin yapılması oldukça çok işlem maliyeti gerektirdiğinden ötürü 3 adet kamera için eğitim yapılmıştır. Hedef ve hedef olmayan kamera modelleri için PRNU parmakizi çıkarma işlemi her bir cihaz için yaklaşık olarak 5-6 dakika sürmüştür. Ancak asıl işlem maliyeti gerektiren kısım CNN eğitimidir. Yapılan CNN eğitimi her bir cihaz için yaklaşık olarak 2,5 gün sürmüştür. Seçilen bu 3 adet kamera modeli rastgele olarak belirlenmiştir. Diğer kameralar ise CNN eğitiminde diğer sınıfına ait olmak üzere kullanılmıştır. Her bir cihazdan toplamda 50’şer adet resim seçilmiştir. Kamera modellerinin çözünürlük bilgisi modelden modele göre farklılık gösterdiğinden ötürü her bir resmin ortasından 1080 x 1440 piksellik bölge kesilmiştir. Böylelikle çözünürlük bilgisi sabitlenmiş olmuştur. Ek olarak eğitilen CNN modeli resmin sadece ortasından bloklar alınarak eğitilmesine rağmen, resmin eğitimde kullanılmayan kısımlarında da çalıştığı gösterilmek istendi. Kırpılmış olan her bir resmin rastgele bir bölgesinden CNN eğitiminde kullanılmak üzere 96 × 96 boyutunda resim blokları çıkarılmıştır. İki sınıfa ait çıkarılan blok sayıları şu şekildedir: yapılacak olan tek bir eğitim için, hedef sınıfındaki kamera modeli için 50 adet resimden toplamda 10 bin blok, hedef olmayan sınıf için her bir kamera modelinden 1 bin blok çıkarılmıştır. Hedef olmayan sınıfa ait toplamda 25 adet kamera bulunduğundan toplam 25 bin blok hedef olmayan sınıf için

çkarılmıştır. Böylelikle eğitim yapılırken sınıflara ait veri dağılımı dengesi 10/25 olacak şekilde belirlenmiştir. Yapılan eğitimlerde çıkarılan blokların %80'i eğitim için %20'si test için ayrılmıştır. Kullanılan blok sayılarının test/eğitim ve hedef/diğer sınıflarına göre dağılımı Tablo 2'de gösterilmiştir.

**Tablo 2. CNN eğitiminde ve testlerde kullanılan toplam blok ve resim sayıları**

	Resim Sayıları		Blok Sayıları	
	Hedef Sınıf	Diğer Sınıf	Hedef Sınıf	Diğer Sınıf
Eğitim	40	1000	400 bin	1000 bin
Test	10	250	100 bin	250 bin
Toplam	50	1250	500 bin	1250 bin

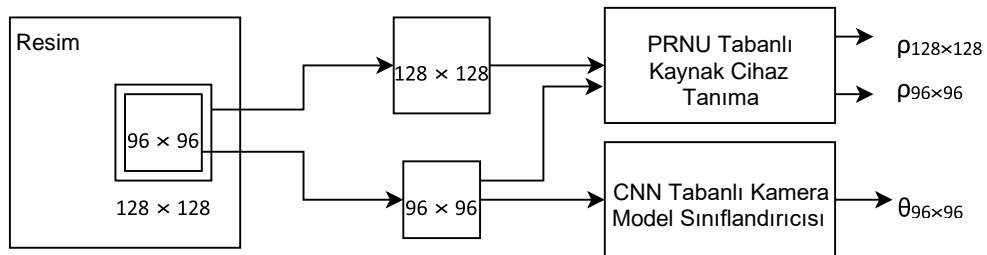
Hem resimlerin kırılması esnasında hem de blok çıkarma işlemi sırasından herhangi bir veri kaybı yaşanmaması açısından bütün kayıt işlemleri kayıpsız mod olan .PNG formatında yapılmıştır. CNN eğitimi yapılırken MatConvNet (Vedaldi, A. ve diğ 2017) kütüphanesi kullanıldı. Momentum olarak 0.9 değeri ve ağırlık zayıflatma değeri  $5 \times 10^{-4}$  şeklinde sabitlendi. Toplamda 50 tur döngü ile eğitim gerçekleştirildi.

Eğitimde ve test kısmında kullanılan 50 adet resim seçilirken, içeriği aşırı karanlık ya da aşırı parlak olan resimler hariç tutuldu. Bu işlemin yapılmasındaki amaç resim içerisinde yeterli istatistik bilgi olmayan resimlerin eğitime dahil edilmeyerek daha kaliteli bir ağ eğitilebilmesidir. Ek olarak benzer sahne içeren içeren resimlerden sadece 1 adet seçildi. Böylelikle eğitilen ağ yalnızca verilen sahneleri öğrenmesi engellenmeye çalışıldı. Yapılan CNN eğitimleri başarılı bir şekilde gerçekleştirilmiştir. Hedef kameralar için eğitilen CNN'ların eğitim başarıları Canon IXUS 70, Ricoh GX100 ve FujiFilm FinePixJ50 için sırasıyla %85, %99 ve %95'tir.

#### 4. KARŞILAŞTIRMA SONUÇLARI VE TARTIŞMA

Bölüm 2'de detayları anlatılan PRNU tabanlı kamera kaynak tanıma yöntemi ile CNN tabanlı kamera model sınıflandırıcısı belirlenen blok boyutları kullanılarak karşılaştırılmıştır. Bu çalışmada eğitilen CNN modelinin girdisinin  $96 \times 96$  olması sebebiyle karşılaştırma boyutu ilk olarak  $96 \times 96$  piksel olarak belirlenmiştir. Her bir blok karşılaştırılan bu iki yöntem ile test edilmiştir. Test neticesinde her bir blok için PRNU yönteminden gelen  $\rho$  korelasyon değeri ve  $\theta$  CNN ağının ürettiği olasılık değeri olmak üzere toplam 2 adet sonuç üretilmiştir. Test işlemine ait süreç Şekil 3'de gösterilmiştir.

Test edilen görüntü bloklarına ait resim ve blok sayıları Tablo 2'de verilmiştir. Elimizde hem hedef kameralara ait hem de diğer sınıfa ait bloklardan elde edilen  $\rho$  ve  $\theta$  değeri bulunmaktadır. Bu iki değeri karşılaştırabilmek için elde edilen sonuçları ve gerçek değerlerini baz alarak TP, FP, TN, FN değerleri kullanılarak TPR, FPR ve Doğruluk değerleri hesaplanmıştır.



**Şekil 3:**  
Test İşlemi Süreci

Pozitif hedef sınıfını, negatif de diğer sınıfı temsil etmek üzere burada

TP: Üretilen değer pozitif ve gerçek değer pozitif ise

FP: Üretilen değer pozitif ve gerçek değer negatif ise

TN: Üretilen değer negatif ve gerçek değer negatif ise

FN: Üretilen değer negatif ve gerçek değer negatif ise değerlerini göstermektedir.

Bu değerler kullanılarak TPR, FPR ve Doğruluk değerleri sırasıyla Denklem 5, 6 ve 7’de ki formüller kullanılarak hesaplanmıştır.

$$TPR = \frac{TP}{TP + FN} \quad (5)$$

$$FPR = \frac{FP}{FP + TN} \quad (6)$$

$$\text{Doğruluk} = \frac{TP + TN}{TP + FN + FP + TN} \quad (7)$$

Yapılan deneyin ikinci aşamasında  $96 \times 96$  boyutundaki CNN modelinin daha büyük boyuttaki PRNU korelasyon değerine göre karşılaştırılması yapılmak istenmiştir. Bu kısım yapılırken sadece PRNU penceresi  $96 \times 96$ ’dan  $128 \times 128$  piksel boyutuna çıkarılmıştır. Yani  $128 \times 128$ ’lik bloklardan elde edilen  $\rho$  değerleri  $96 \times 96$  piksellik bloklardan elde edilen  $\theta$  değerleriyle karşılaştırılmıştır. Burada karşılaştırmanın adil olabilmesi açısından Çıkarılan  $128 \times 128$  piksellik blokların tam orta kısmındaki  $96 \times 96$  piksellik bölge CNN ağına  $\theta$  değerlerini üretmesi için verilmiştir. Toplamda 350 bin bloktan hem  $\rho$  hem de  $\theta$  değeri üretilmiştir.

**Tablo 3. Şekil 4,5 ve 6’daki ROC eğrilerinin alt kısmında kalan alan değerleri**

Kamera Adı	PRNU		CNN
	$96 \times 96$	$128 \times 128$	$96 \times 96$
Canon IXUS 70	0,920	0,958	0,890
FujiFilm FinePixJ50	0,856	0,908	0,992
Ricoh GX100	0,722	0,779	0,963

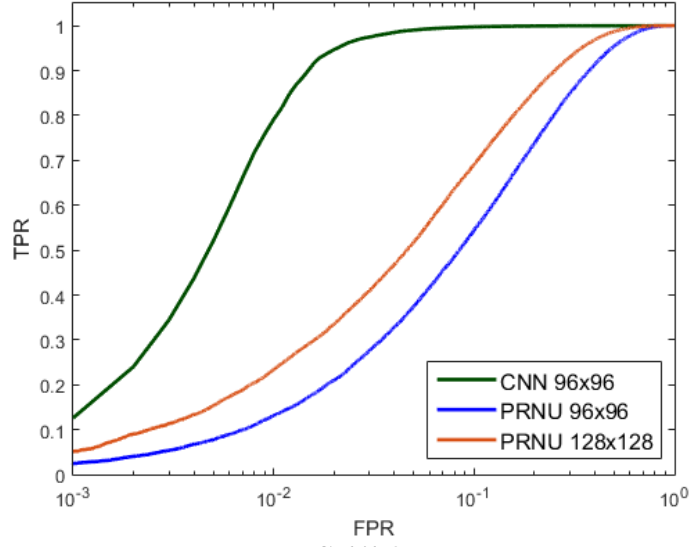
**Tablo 4. En yüksek Doğruluk değerini veren eşikleme değeri için hesaplanan TPR, FPR ve Doğruluk değerleri**

	TPR			FPR			Doğruluk		
	CNN 96	PRNU 96	PRNU 128	CNN 96	PRNU 96	PRNU 128	CNN 96	PRNU 96	PRNU 128
Canon IXUS 70	0,95	0,95	<b>0,96</b>	0,31	0,30	<b>0,20</b>	0,87	0,87	<b>0,91</b>
FujiFilm FinePixJ50	<b>0,97</b>	0,94	0,93	<b>0,11</b>	0,73	0,61	<b>0,95</b>	0,74	0,77
Ricoh GX100	<b>0,98</b>	0,93	0,95	<b>0,04</b>	0,44	0,34	<b>0,97</b>	0,82	0,86

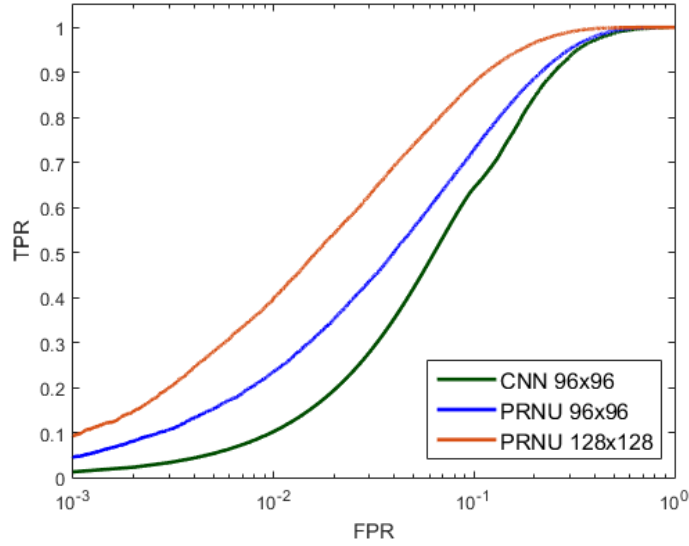
Test kümesinin oldukça geniş olması yapılan testin başarısını daha iyi ortaya koymaktadır. Her bir cihazın testinde kullanılan 350 bin adet  $96 \times 96$  piksel boyutundaki bloklar ile Çalışma Karakteristikleri elde edilmiştir. Elde edilen Çalışma Karakteristiği eğrileri Şekil 4, 5 ve 6’da ve bu eğriler altında kalan alan bilgisi Tablo 3’de verilmiştir. Ayrıca Tablo 4’te, Şekil 4, 5 ve



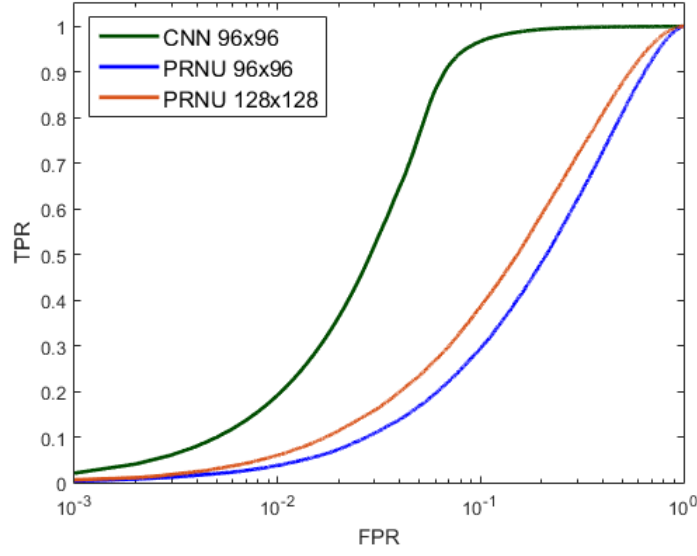
6'daki Çalışma Karakteristiği eğrilerinden en iyi eşikleme değeri seçilerek hesaplanan TPR, FPR ve Doğruluk değerleri verilmiştir. Tablo 3'deki çalışma karakteristiği eğrilerinin altında kalan alan ve Tablo 4'teki doğruluk yüzdelere göre 2 kamera cihazında CNN tabanlı yöntem, geriye kalan 1 adet cihazda ise PRNU tabanlı yöntemden daha iyi çalışmaktadır. PRNU yönteminin daha iyi çalıştığı cihazda bile PRNU yöntemi, CNN tabanlı yöntemle göre çok az bir farkla üstünlük sağlamaktadır. Ek olarak CNN tabanlı yöntemin iyi olduğu kamera cihazlarında CNN tabanlı yöntem PRNU yönteminin  $128 \times 128$  'lik pencere boyutunda elde ettiği sonuçlardan bile daha iyi performans göstermiştir.



**Şekil 4:**  
*Ricoh'a ait ROC*



**Şekil 5:**  
*Canon'a ait ROC*



**Şekil 6:**  
Fuji'ye ait ROC

Kamera cihazlarının hepsinden bazen iyi bir parmakizi tahmin edilememektedir. Bu durumlarda CNN tabanlı yöntem kullanmak daha doğru sonuçlar üretecektir. Oynanmış resimlerin olduğu bir görüntü kümesinde test yapmak karşılaştırma açısından daha iyi olacak olsa da işlem maliyeti açısından çok fazla zaman alacağı için blok bazlı karşılaştırma yapılmıştır. Ancak yöntemlerin nasıl çalıştığını görsel olarak gösterebilmek için  $400 \times 400$ ,  $200 \times 200$  ve  $100 \times 100$  boyutlarında sırasıyla ağır, orta ve hafif olacak şekilde oynamalar için yöntemlerin sonuçları Şekil 7, 8 ve 9'da gösterilmiştir. Şekil 7, 8 ve 9'da sırasıyla  $400 \times 400$ ,  $200 \times 200$  ve  $100 \times 100$  boyutunda bir bölge diğer sınıfına ait olan kameralardan kesilip hedef kamera resimleri üzerinde rastgele bir kısma yapıştırılmıştır.

	Oynanmış Resim	Oynanan Bölge	CNN Çıktısı 96x96	PRNU Çıktısı 96x96	PRNU Çıktısı 128x128	Sonuç CNN 96x96	Sonuç PRNU 96x96	Sonuç PRNU 128x128
Canon								
Fuji								
Ricoh								

**Şekil 7**

Test edilen yöntemlerin  $400 \times 400$  oynama boyutu için sonuç çıktıları. Sonuç kısmında uygulanan eşikleme değeri çalışma karakteristiği eğrilerinden yüzde 1 FP olacak şekilde belirlenmiştir.

	Oynanmış Resim	Oynanan Bölge	CNN Çıktısı 96×96	PRNU Çıktısı 96×96	PRNU Çıktısı 128×128	Sonuç CNN 96×96	Sonuç PRNU 96×96	Sonuç PRNU 128×128
Canon								
Fuji								
Ricoh								

**Şekil 8:**

Test edilen yöntemlerin  $200 \times 200$  oynama boyutu için sonuç çıktıları. Sonuç kısmında uygulanan eşikleme değeri çalışma karakteristiği eğrilerinden yüzde 1 FP olacak şekilde belirlenmiştir.

	Oynanmış Resim	Oynanan Bölge	CNN Çıktısı 96×96	PRNU Çıktısı 96×96	PRNU Çıktısı 128×128	Sonuç CNN 96×96	Sonuç PRNU 96×96	Sonuç PRNU 128×128
Canon								
Fuji								
Ricoh								

**Şekil 9:**

Test edilen yöntemlerin  $100 \times 100$  oynama boyutu için sonuç çıktıları. Sonuç kısmında uygulanan eşikleme değeri çalışma karakteristiği eğrilerinden yüzde 1 FP olacak şekilde belirlenmiştir.

## 5. SONUÇ

Bu çalışmada bölgesel müdahale tespiti yapan temel yöntemlerden PRNU tabanlı kamera kaynak tanıma yöntemi ile evrişimsel sinir ağı tabanlı kamera model tanıma yöntemi karşılaştırılmıştır. Literatürde ayrı ayrı olarak iki yöntem de karşılaştırılmıştır. İki yöntem de kendi alanlarında öncü olmaktadır. Ancak bu iki yöntemin birbiriyle olan karşılaştırılması bulunmamaktadır. PRNU yöntemi kamera cihazının değişmeyen sensör özelliklerine dayanırken, CNN tabanlı yöntem kamera cihazının renk filtresini temel almaktadır. PRNU yöntemi kullanılarak yapılan oynanmış bölge tespiti seçilen pencere boyutuna göre farklılık göstermektedir. Seçilen pencere boyutu büyüdükçe tespit doğruluğu artarken, tespit edilebilen bölge büyüklüğü hassasiyetini kaybetmektedir. CNN tabanlı yöntemde ise pencere boyutunun büyümesinin daha iyi sonuç üreteceği yargısı CNN modeline, parametrelerine ve eğitim verisine bağlı olduğundan net bir şekilde söylenemez. Yapılan karşılaştırma neticesinde 3 kamera cihazından 2 tanesinde oldukça büyük bir farkla CNN tabanlı kamera model sınıflandırıcısı klasik PRNU yöntemine göre daha başarılı çalışmıştır. Geriye kalan bir adet kamera cihazında ise hemen hemen aynı performansı göstermiştir. Seçilen pencere boyutunun küçük olmasının PRNU yönteminin başarısı aşağıya çekmesinden ötürü CNN tabanlı yöntem küçük pencere boyutunda daha iyi bir performans göstermektedir. Ancak Canon marka cihazın parmakizi  $96 \times 96$  kadar küçük seçilen bir pencere boyutunda dahi kuvvetli çıkmaktadır. Bu durum tamamen cihazın sensörlerinin bırakmış olduğu izler ile alakalıdır. Bu sebepten ötürü Canon

marka cihazda PRNU yöntemi, CNN tabanlı yöntemden daha düşük ancak hemen hemen yakın bir performans göstermektedir. Bu sonuçlara göre CNN tabanlı yöntemin  $96 \times 96$  gibi küçük boyuttaki pencerelerde daha başarılı bir yöntem olduğu söylenebilir. Karşılaştırılan bu iki yöntemin kameranın farklı özelliklerinden faydalanarak sonuç ürettiğini baz alarak gelecek çalışmamızda bu iki yöntemin birleştirilerek daha iyi bir tespit edici yapılması planlanmaktadır.

## KAYNAKLAR

1. Bayar, B., & Stamm, M. C. (2016, June). A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security (pp. 5-10). ACM. DOI:10.1145/2909827.2930786
2. Bondi, L., Baroffio, L., Güera, D., Bestagini, P., Delp, E. J., & Tubaro, S. (2017). First steps toward camera model identification with convolutional neural networks. *IEEE Signal Processing Letters*, 24(3), 259-263. DOI: 10.1109/LSP.2016.2641006
3. Bondi, L., Güera, D., Baroffio, L., Bestagini, P., Delp, E. J., & Tubaro, S. (2017). A preliminary study on convolutional neural networks for camera model identification. *Electronic Imaging*, 2017(7), 67-76. DOI: <https://doi.org/10.2352/ISSN.2470-1173.2017.7.MWSF-327>
4. Bondi, L., Lameri, S., Güera, D., Bestagini, P., Delp, E. J., & Tubaro, S. (2017, July). Tampering detection and localization through clustering of camera-based CNN features. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1855-1864). IEEE. DOI: 10.1109/CVPRW.2017.232
5. Dirik, A. E., & Memon, N. (2009, November). Image tamper detection based on demosaicing artifacts. In Image Processing (ICIP), 2009 16th IEEE International Conference on (pp. 1497-1500). IEEE. DOI: 10.1109/ICIP.2009.5414611
6. Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. *IEEE transactions on information forensics and security*, 4(1), 154-160. DOI: 10.1109/TIFS.2008.2012215
7. Ferrara, P., Bianchi, T., De Rosa, A., & Piva, A. (2012). Image forgery localization via fine-grained analysis of CFA artifacts. *IEEE Transactions on Information Forensics and Security*, 7(5), 1566-1577. DOI: 10.1109/TIFS.2012.2202227
8. Gloe, T., & Böhme, R. (2010, March). The'Dresden Image Database'for benchmarking digital image forensics. In Proceedings of the 2010 ACM Symposium on Applied Computing (pp. 1584-1590). ACM. Doi:10.1145/1774088.1774427
9. Goljan, M., Fridrich, J., & Filler, T. (2009, February). Large scale test of sensor fingerprint camera identification. In Media Forensics and Security (Vol. 7254, p. 72540I). International Society for Optics and Photonics. Doi: 10.1117/12.805701
10. Krawetz, N., & Solutions, H. F. (2007). A Picture's Worth... Hacker Factor Solutions, 6.
11. Lin, Z., He, J., Tang, X., & Tang, C. K. (2009). Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. *Pattern Recognition*, 42(11), 2492-2501. Doi:<https://doi.org/10.1016/j.patcog.2009.03.019>
12. Liu, Y., Guan, Q., Zhao, X., & Cao, Y. (2018, June). Image forgery localization based on multi-scale convolutional neural networks. In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (pp. 85-90). ACM. Doi:10.1145/3206004.3206010

- 13.** Lukas, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2), 205-214. DOI: 10.1109/TIFS.2006.873602
- 14.** Tuama, A., Comby, F., & Chaumont, M. (2016, December). Camera model identification with the use of deep convolutional neural networks. In *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on* (pp. 1-6). IEEE. DOI: 10.1109/WIFS.2016.7823908
- 15.** Vedaldi, A., & Lenc, K. (2015, October). Matconvnet: Convolutional neural networks for matlab. In *Proceedings of the 23rd ACM international conference on Multimedia* (pp. 689-692). ACM. Doi:10.1145/2733373.2807412
- 16.** Ye, S., Sun, Q., & Chang, E. C. (2007, July). Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In *Multimedia and Expo, 2007 IEEE International Conference on* (pp. 12-15). IEEE. DOI: 10.1109/ICME.2007.4284574

