**TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# ANDROID TELEFONLARDA GÜVENLİ KAMERA UYGULAMASI

**YÜKSEK LİSANS TEZİ**

**Kemal Özgür DUMAN**

**Bilgisayar Mühendisliği Anabilim Dalı**

**Tez Danışmanı: Doç. Dr. Hüsrev Taha SENCAR**

**NİSAN 2019**

Fen Bilimleri Enstitüsü Onayı

……..
**Prof. Dr. Osman EROĞUL**
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksininlerini sağladığını onaylarım.

……
**Prof. Dr. Oğuz ERGİN**
Anabilimdalı Başkanı

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 171111006 numaralı Yüksek Lisans Öğrencisi **Kemal Özgür DUMAN**'ın ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"Android Telefonlarda Güvenli Kamera Uygulaması"** başlıklı tezi **12.04.2019** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

**Tez Danışmanı :** **Doç. Dr. Hüsrev Taha SENCAR** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

**Jüri Üyeleri :** **Doç. Dr. Tansel ÖZYER (Başkan)** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

**Dr. Öğr. Üyesi Murat YILMAZ** .....
Çankaya Üniversitesi

## TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Kemal Özgür DUMAN

# ÖZET

Yüksek Lisans Tezi

ANDROID TELEFONLARDA GÜVENLİ KAMERA UYGULAMASI

Kemal Özgür DUMAN

TOBB Ekonomi ve Teknoloji Üniveritesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Hüsrev Taha SENCAR

Tarih: Nisan 2019

Günümüzde, akıllı telefonlarda bulunan kamera teknolojilerinin gelişmesi ile telefonlar dijital kameraların yerini almaktadır. Bu durum insanların hayatlarının her anında sayısız fotoğraf çekmesine olanak sağlamaktadır. Sosyal medya ve fotoğraf paylaşım teknojilerinin gelişmesi ile insanlar sürekli olarak bu fotoğrafları herkese açık ortamlarda paylaşmaktadır. Kamera sensörlerinin üretimi sırasında oluşan kusurlar sebebiyle bu kameralar ile çekilen fotoğraflarda oluşan gürültü elementleri incelenerek kaynak kamera tespiti yapılabilmektedir. Kaynak kamera tespiti, adli bir vaka durumunda fotoğrafın kaynağının ispatlanması, bir fotoğraf üzerinde yapılan oynamaların tespiti gibi yöntemler için kullanılabilmektedir. Ayrıca bu gürültü elementleri bir saldırgan tarafından bir fotoğraftan diğerine taşınarak aynı kameradan çekilmeyen bir fotoğrafın bu kameradan çekilmiş gibi gösterilebilmesine neden olmaktadır. Herkese açık ortamlara yüklenen bu fotoğraflar belirtilen saldırılar ve illegal kaynak kamera tespiti için bir veri kaynağı oluşturmaktadır. Bu durumlardan korunmak için geliştirilmiş olan fotoğraf anonimleştirme teknikleri için kullanıcılara sunulan bir uygulama olmaması sebebiyle bu işlemler sadece teorik olarak kalmaktadır. Daha güvenli bir anonimleştirme için bu işlemin fotoğrafın çekildiği kaynak üzerinde yapılması gerekmektedir. Ancak böyle bir uygulama olmaması ve bu işlemlerin kısıtlı sistem kaynaklarına sahip akıllı telefonlarda çalıştırılamaması

sebebiyle böyle bir işlev kullanıcılara sunulamamaktadır. Bu çalışmada önerilen parçalı fotoğraf anonimleştirme yöntemi sayesinde kısıtlı sistem kaynaklarına sahip akıllı telefonlarda anonimleştirme işlemi sorunsuz şekilde çalıştırılabilmektedir. Çalışmada, belirtilen yöntem ile geliştirilmiş ve kullanıcılara kaynak kamera imzası bulunmayan fotoğraflar sunabilen Güvenli Kamera Uygulaması geliştirilmiştir. Ayrıca parçalı fotoğraf işlemeye benzer bir yöntem ile HDR fotoğraflarda kaynak kamera tespitinin daha yüksek başarı oranları ile yapılabilmesi için bir yöntem önerilmektedir.

**Anahtar Kelimeler:** Kaynak kamera tespiti, Fotoğraf anonimleştirme, Adli bilişim, Android uygulaması, HDR fotoğraf

## ABSTRACT

Master of Science

SECURE CAMERA APPLICATION ON ANDROID PHONES

Kemal Özgür DUMAN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Computer Engineering Science Programme

Supervisor: Assoc. Prof. Dr. Hüsrev Taha SENCAR

Date: April 2019

Current advances on smartphone's camera technologies leads smartphones to replace digital cameras. This allows people to take images in all aspects of life. In accommodation with social media and data sharing technologies these photographs are uploaded on the internet publicly and continuously. Because of the defects on the camera sensors that are caused by manufacturing process, images taken by those camera sensors carries an hidden noise that allow source camera identification. Source camera identification is not only useful technique for proving the source camera of the image in forensic cases but also identifying forgeries in images. However, the noise element that can be extracted from the image is also allows an attacker to make illegal identity tracking and noise copy attacks to deceive forensic analysis. Publicly available images are easily become the source for these attacks. Image anonymization techniques to prevent such attacks are only theoretically avaible to users as there is no such application to provide it. Since it is more secure for users to apply this anonymization in the source camera that takes the image, it is important to have a such application in smartphones. Because of the absence of such application and impossibility of running these techniques on the smartphones that has limited system resources due to android task killer that kills the processes which are using most system resources when the system lacks of resources, such functionality cannot be provided

to users. In this study we provide a segmented anonymization technique to run the anonymization process on smartphones that has a limited system resources by limiting the resource usage of the process. Also, we provide a fully functional android secure camera application that using this technique to provide a secure images to users. In this process, we also provide a technique for better source camera identification with HDR images.

**Keywords:** Source camera identification, Image anonymization, Digital forensics, Android application, HDR image.

## TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Doç. Dr. Hüsrev Taha SENCAR'a, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, destekleriyle her zaman yanımda olan aileme ve arkadaşlarıma çok teşekkür ederim.

**İÇİNDEKİLER**

# ŞEKİL LİSTESİ

**Sayfa**

# ÇİZELGE LİSTESİ

**Sayfa**

## KISALTMALAR

**PRNU** **:** Photo Response Non-Uniformity
**PNU** **:** Pixel Non-Uniformity
**FPN** **:** Fixed Pattern Noise
**ML** **:** Maximum Likelihood Estimator
**WDF** **:** Dalga Bazlı Gürültü Arındırma Filtresi (Wavelet based Denoising Filter)
**HDR** **:** Yüksek Dinamik Aralığı (High Dynamic Range)
**PCE** **:** Peak to Correlation Energy
**ABO** **:** Anomimleştirme Başarı Oranı

## SEMBOL LİSTESİ

Bu çalışmada kullanılmış olan simgeler açıklamaları ile birlikte aşağıda sunulmuştur.

| Simgeler | Açıklama |
|---|---|
| $\rho$ | PCE oranı |
| α | Normalleştirilmiş çapraz korelasyon |
| γ | Alan matrisi |
| β | FPN bileşeni |
| **Ω** | PRNU bileşeni |
| $\sigma_{pce}$ | PCE alt sınırı |
| $\omega$ | Anonimleştirme faktörü |
| ∀ | Arama sınırı üst limiti |
| $\theta$ | Eşleştirme oranı |

## RESİM LİSTESİ

**Sayfa**

# 1. GİRİŞ

Günümüzde, akıllı telefonlarda bulunan kamera teknolojilerinin gelişmesi ile telefonlar dijital kameraların yerini almaktadır. Bu sayede insanlar hayatlarının her anında kolayca fotoğraf çekebilmeye imkan bulmaktadır. Çekilen sayısız fotoğraflar ile birlikte, sosyal medya kullanımı ve internet üzerinden fotoğraf paylaşımının artması sebebiyle bu fotoğraflar sürekli olarak herkese açık ortamlarda paylaşılmaktadır. Bu fotoğraflar kaynak kamera tespit yöntemleri için kolayca ulaşılabilen bir veri tabanı haline gelmektedir.

Bir fotoğrafın kaynak kamerasının tespit edilebilmesi için daha önce birçok çalışma yapılmıştır [1-4]. [3] çalışmasında gözetimli öğrenme yöntemi ile kaynak kamera analizi yapılması hedeflenmiştir. [4] çalışmasında kamera lensinde bulunan hatalı piksellerin incelenmesi sonucu bir kamera imzası elde edilmesi sağlanmıştır. Bu yöntem sadece hatalı piksele sahip kameralar ile çalıştığından her kamerada verimli olmamaktadır. Kaynak kamera analizinde en başarılı yöntem, kameraların lenslerinin üretimi sırasında oluşan kusurlardan kaynaklı olarak her pikselin ışığa karşı farklı duyarlılık göstermesi sonucunda oluşan gürültüler (PRNU) kullanılarak kamera imzası elde edilmesidir ve eğer bir kameradan çekilmiş yeterli sayıda fotoğraf elde edilirse başka bir fotoğrafın aynı kameradan çekilip çekilmediğini başarılı bir şekilde belirleyebilen bir algoritmada kullanılarak bir kamera imzası çıkartılabilir [5]. Bu teknik Yüksek Dinamik Aralıklı (HDR) fotoğrafların tespitinde yeteri kadar iyi çalışmamaktadır çünkü bu fotoğrafların oluşturulmasında normal fotoğraflara göre ekstra adımlar içeren farklı bir yöntem kullanılmaktadır. Görünen o ki, bu adımlar fotoğrafta bulunan ve kaynak kamera tespiti için kullanılan gürültüyü etkilemektedir. Bu çalışmada, kaynak kamera analizinin HDR fotoğraflar ile daha başarılı bir şekilde çalışması için bir yöntem önerilmektedir.

Kaynak kamera tespiti için kullanılan imzalar başka bir fotoğrafın orijinalliğini tespit etmek için kullanılabilmektedir [6]. Bu yöntem ile suç barındıran bir davada fotoğrafın suçlu kişi tarafından çekildiğini ispat etmek için kullanılsa da illegal kimlik tespiti ve sahte kamera imzası kopyalama saldırılarında da kullanılabilir [7]. Buradan yola

çıkarak fotoğraflarda bu kamera imzasının çıkartılması için kullanılan gürültü elementlerinin fotoğraftan kaldırılabilmesi için de çalışmalar yapılmıştır [8, 9]. Bu yöntem fotoğrafın çekildiği kameranın oluşturduğu gürültünün fotoğraflardan silinmesiyle anonimleştirme sağlamaktadır. Bu gürültü fotoğraflardan silindiğinde kaynak kamerayı tespit etmek için kullanılacak bir bilgi kalmadığı için kaynak kamera tespit tekniklerini başarısız hale getirmektedir. Ancak bu işlemi gerçekleştirecek bir uygulama bulunmadığı için bu teknikler sadece teoride kalmakta ve insanlar tarafından kullanılamamaktadır. Anonimleştirme işleminin güvenli bir şekilde yapılabilmesi için çekilen fotoğrafların telefon dışına çıkartılmadan bu işlemin direkt olarak fotoğrafı çeken kaynak kamera üzerinde uygulanması gerekmektedir. Ancak böyle bir uygulama oluşturulmasındaki problem, bu işlemlerin gerçekleştirilmesi için gereken yüksek miktardaki sistem kaynaklarının akıllı telefonlarda bulunmamasıdır. Android telefonlarda bulunan bir önlem sayesinde, çalışan bir uygulamanın sistem kaynaklarının aşırı kullanasının önüne geçilmektedir. Bu önlem, sistemin sorunsuz çalışabilmesi için çok fazla kaynak tüketen uygulamaların sistem tarafından otomatik olarak kapatılmasıdır. Bu çalışmada, anonimleştirme işleminin kısıtlı sistem gücüne sahip akıllı telefonlarda çalışabilmesi için bir yöntem önerilmektedir. Ayrıca, bu yöntem kullanılarak geliştirilen ve kullanıcılara kamera imzası çıkartılamayan anonim fotoğraflar çekebilen, Güvenli Kamera Uygulaması geliştirilmiştir.

### 1.1 Tezin Amacı

Günümüzde telefonlar tarafından çekilen sayısız fotoğraf, sosyal medyanın ve fotoğraf paylaşım teknolojilerinin gelişmesi ile sürekli olarak herkese açık ortamlara yüklenmektedir. Fotoğrafların sahipleri, yasal olmayan kimlik takibi yapılmasına veya bu fotoğraflar kullanılarak yapılacak saldırılara açık durumda kalmaktadır. Bu sorunu ortadan kaldırmak için geliştirilen fotoğraf anonimleştirme teknikleri kullanıcılara sadece teorik olarak sunulduğundan, herkes tarafından kullanılabilmesi mümkün olmamaktadır. Kullanıcılar için en uygun ve güvenli olacak yöntem, fotoğrafı çekmek için kullanılan kaynak üzerinde aynı zamanda fotoğraf anonimleştirme işleminin yapılması olarak değerlendirebilir. Böyle bir uygulamanın olmamasının temel sebebi olarak fotoğrafın çekildiği kaynak, genellikle kısıtlı sistem özelliklerine sahip akıllı telefonlarda, bu tarz yüksek sistem kaynakları gerektiren bir işlem çalıştırılamaması olarak gösterilebilir. Bu çalışmada, Android telefonlarda fotoğraf anonimleştirme

tekniklerinin sorunsuz çalışabilmesi için bir yöntem önerilmekte ve bu yöntem kullanılarak geliştirilen Güvenli Kamera Uygulaması sunulmaktadır. Aynı zamanda, Yüksek Dinamik Aralığına sahip fotoğraflara var olan kaynak kamera analiz tekniklerinin uygulanabilmesi için daha başarılı bir uygulama yöntemi önerilmektedir.

## 1.2 Tezin İçeriği

Tezin içeriği şu şekildedir; ikinci bölümde tezde yapılan çalışmalar için literatür araştırmasına yer verilmektedir. Bu kapsamda kullanılan kaynak kamera tespitinin amaçları ve yöntemleri ve literatürde bulunan çalışmalar hakkında bilgi verilmektedir. Aynı zamanda fotoğraf anonimleştirme tekniklerine neden ihtiyaç duyulduğu ve fotoğraflar üzerinde nasıl uygulandığını, bu konuda yapılan literatür araştırmasını anlatmaktadır. Üçüncü bölümde bu çalışmada ek olarak sunulan HDR fotoğraflarda kaynak kamera tespitini ve kaynak kamera tespitinde yaşanan sorunlar için önerilen yöntem ve test sonuçları anlatılmaktadır. Çalışma kapsamında geliştirilen güvenli kamera uygulamasının amaçları, böyle bir uygulamanın kısıtlı sistem gücüne sahip telefonlarda çalıştırılabilmesi için önerilen yöntem, uygulama hakkında bilgiler ve sonuç kısmına dördüncü bölümde yer verilmektedir. Son olarak beşinci bölüm çalışmayı özetlemekte ve çalışmanın kısıtlarından bahsetmektedir.

## 2. LİTERATÜR ARAŞTIRMASI

Bu bölümde literatür araştırmasına yer verimektedir ve bu kapsamda iki temel başlık altında kaynak kamera analizi ve fotoğraf anonimleştirme teknikleri için kullanılan yöntemler incelenmektedir.

### 2.1 Kaynak Kamera Tespiti

Kaynak kamera tespiti için ilk aşamada fotoğraflar üzerine kaynak kamera tarafından istenerek bırakılan imzalar kullanılmıştır [10]. Bu yöntemler fotoğraflar üzerinde sadece kaynak kamera modeli ve zaman imzası gibi bilgiler bıraktığı için kullanımı kısıtlı olmakta ve sadece belli bir ortamda alınan fotoğrafların bütünlüğünü korumak için kullanılabilmektedir (Örn. Adli bir vakada inceleme ekibi tarafından çekilen fotoğraflar.). Aynı zamanda öğreticiyle öğrenme, sınıflandırma teknikleri ile kaynak kamera tespiti yapılması hedeflenmiştir [11, 12]. Kaynak kamera tespitinde kamera tarafından özellikle bırakılan imzalar haricinde kamera sensörü üzerinde bulunan tozlar gibi elementlerin incelenmesi ve kamera imzası oluşturulması üzerine de çalışmalar yapılmıştır [4]. Bu yöntemler ile incelenen detaylar kaynak kameranın direkt olarak bir özelliği olmadığı için kaynak kamera tespiti için tek başına yeterli olmamaktadır. Fotoğraflar üzerinde bulunan gürültü desenleri incelenerek yapılan çalışmalardan birisi sadece fotoğraf üzerinde bulunan sabit gürültü desenlerini inceleyerek kaynak kamera tespiti yapmaya çalışmıştır [13]. Kaynak kamera tespitinde daha başarılı sonuçlar elde eden çalışmada fotoğraf üzerinde bulunan ve kamera sensöründeki her pikselin ışığa karşı farklı duyarlılık göstermesinden dolayı oluşan gürültüleri inceleyerek bir fotoğrafın kaynağının tespit edilmesi hedeflenmişir [5]. Bu yöntemler ile yapılan kaynak kamera analizi ile sadece fotoğrafın çekildiği belirli modeli tespit etmek [3, 14, 15] yerine o fotoğrafın çekildiği kaynak kamera direkt olarak tespit edilebilmektedir. Kaynak kameranın tespit edilmesi dışında fotoğraflar üzerinde yapılan değişiklik ve oynamaların tespit için de bir çok yöntem önerilmektedir [16 - 19]. Benzer bir çalışma tarayıcı üzerinden elde edilen fotoğraflar için de uygulanmıştır [20]. Kaynak kamera imzası oluşturmak için kullanılan PRNU

gürültüsü elementleri incelenerek de fotoğraf üzerindeki değişiklik ve oynamaların tespit edilmesi mümkün olmaktadır [6]. Bunlara ek olarak yapılan çalışmaların gösterdiği sonuçlara göre ölçeklendirilen ve kesilen fotoğraflar üzerinde de gürültü elementleri incelenerek kaynak kamera tespiti yapılabilmektedir [21]. Aynı zamanda PRNU gürültüsü kullanılarak sadece dijital olarak olarak değil basılmış fotoğraflar üzerinden de kaynak kamera tespiti yapılabilmektedir [22]. Önceki çalışmalarda gürültü desenleri üzerinden yapılan kaynak kamera tespit tekniği bir milyonun üzerinde fotoğraflar ile test edilmiştir [23].

Bu bölümün devamında kaynak kamera tespiti tekniğinin amaç ve kaynak kamera tespitinin gerçekleştirilebilmesi için gerekli yöntemlerden detayları ile bahsedilmektedir.

### 2.1.1 Amaç

Kaynak kamera tespiti, bir fotoğrafın çekildiği kamerayı tespit etmek için kullanılan bir yöntemdir. Farklı kameralardan toplanan fotoğraflar ile kamera imzaları oluşturulduktan sonra bu imzaların bir fotoğraftan çıkarılan gürültü deseni ile eşleştirilmesi sonucu incelenen sonuçlara göre kaynak kamera tespiti yapılmaktadır. Bu yöntem ile adli bir olayda kanıt niteliği taşıyan bir fotoğrafın ilgili kişi tarafından çekilip çekilmediğinin tespiti yapılabilmekte ve bir fotoğrafın üzerinde değişiklik yapılıp yapılmadığı tespit edilebilmektedir.

### 2.1.2 Yöntem

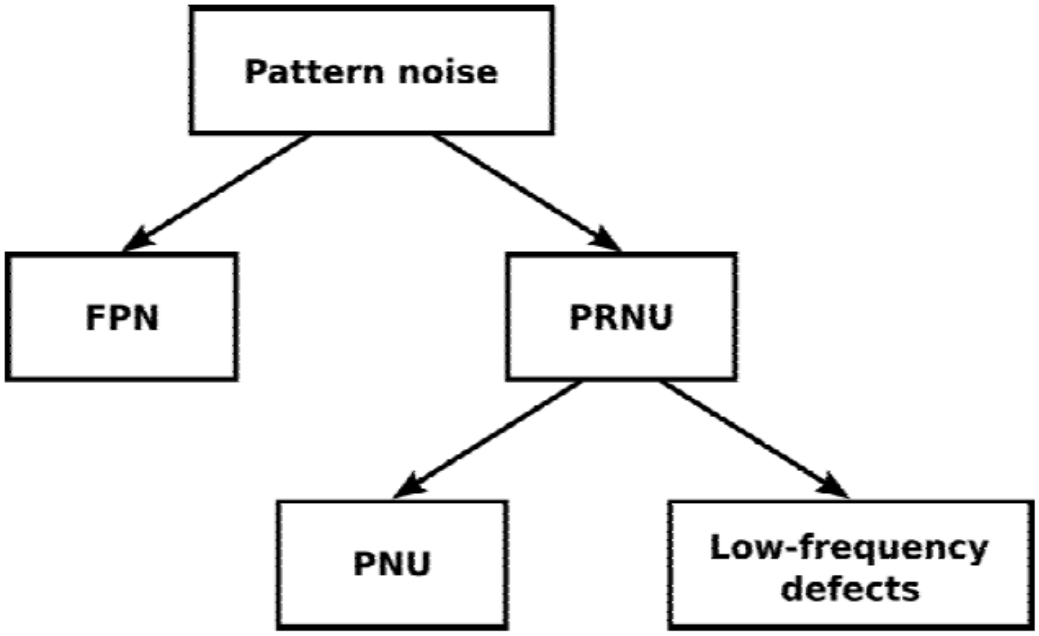
Kaynak kamera tespitinde fotoğraflarda bulunan gürültüler kullanılmaktadır. Bu gürültüler fotoğraflardan gürültü arındırma teknikleri kullanılarak çıkartılmaktadır. Bu verinin her kamerada farklı olmasının sebebi ise kamerada bulunan piksellerin ışığa karşı farklı duyarlılık göstermesinden oluşmaktadır. Kamera modeli aynı olsa bile kameranın üretimi sırasında oluşan kusurlardan kaynaklı olarak bu kamelar fotoğraflar üzerinde farkı gürültü desenleri oluşturmaktadır. Bu desenlerin her fotoğrafta farklı olması durumu göz önüne alınarak her kamera için o kamerayı benzersiz olarak işaret eden kamera imzaları elde edilebilmektedir. Bu imzalar, başka bir fotoğrafdan alınan gürültü desenleri ile eşleştirilerek hangi kameranın hangi fotoğrafı çektiği tespit edilebilmektedir.

Kaynak kamera tespinin yapılabilmesi için 3 yöntem gereklidir. Bu yöntemler şu şekilde sıralanabilir:

- Fotoğraflardan gürültü deseni çıkartılması
- Kaynak kamera imzası oluşturulması
- Kamera imzası ile fotoğrafların eşleştirilmesi

#### 2.1.2.1 Fotoğraflardan gürültü deseni çıkartılması

Kaynak kamera tespitinin temelinde fotoğraflarda bulunan ve kaynak kamera tarafından oluşturulan gürültülerin varlığı yatmaktadır. Doğal fotoğraflarda bulunan gürültü elementleri Şekil 2.1 ile gösterilmektedir. Fotoğraflarda temel olarak iki gürültü elementi bulunmaktadır. Bu elementler Fixed Pattern Noise (FPN) ve Photo Response Non Uniformity (PRNU) olarak isimlendirilmektedir.




Şekil 2.1 : Kamera sensölerinin gürültü deseni [5].

FPN elementi ışığın bulunmadığı ortamlarda çekilen fotoğraflardan toplanabilmektedir. Bu gürültü sadece karanlık çerçevelerden çıkartılmaktadır ve kaynak kamera analiz için yeterli olmamaktadır. Fotoğraflarda bulunan en baskın gürültü elementi PRNU gürültüsüdür. Bu gürültü içerisindeki en etkili element ise PNU (pixel non-uniformity) gürültüsüdür. PNU gürültüsü kamera sensörlerinin üretimi sırasında oluşan kusurlar sebebiyle kamera sensöründeki her pikselin ışığa farklı tepki göstermesinden dolayı oluşmaktadır. PNU gürültüsünün karakteri ve kökeni gereği aynı marka sensörlerden çekilen fotoğraflarda bile farklı gürültü

desenleri oluşması beklenmektedir. PRNU gürültüsüne ayrıca kamera üzerinde bulunan toz parçacıkları ve optik yüzeyde oluşan ışık kırılmaları ve yakınlaştırma ayarlarıda etki etmektedir. Bunlar Şekil 2.1 üzerinde düşük frekanslı hatalar (low-frequency defects) olarak gösterilmekte ve kamera sensörünün bir özelliği olmadığı için kaynak kamera analizinde tek başına kullanılması yeterli değildir [5]. Gürültü desenlerini fotoğraf üzerinden çıkartılabilmesi için fotoğraflarda gürültü arındırma teknikleri kullanılmaktadır. Gürültü arındırma teknikleri fotoğrafın bazı filtrelerden geçirilerek fotoğraf üzerinde bulunan gürültü elementlerinin bastırılması için kullanılmaktadır. Gürültü arındırma tekniklerinin PRNU tabanlı kaynak kamera tespit yöntemleri üzerindeki etkileri [24] çalışmasında da incelenmiştir. Başka bir çalışmadan elde edilen bilgiye göre, gürültü arındırna işlemi için kullanılacak filtre için en iyi sonucu wavelet-base denoising filter (WDF) vermektedir ve bunun sebebi olarakta bu yöntem ile yapılan gürültü arındırma işlemi sonrasında elde edilen gürültü artıkları içerisinde fotoğrafın çekildiği sahne izinin en az seviyede olması olarak gösterilmektedir [5]. Buradan yola çıkarak, kamera *K* ile çekilen fotoğraf *F*'nin *K* ile çekildiğinin tespitinde kullanılacak gürültüyü temizlemek için kullanılacak yöntem *WDF* olduğu varsayılarak, *F* üzerinde bulunan gürültü deseni *G*, formül (2.1) ile elde edilebilir.

$$G = F - WDF(F) \tag{2.1}$$

Formül (2.1) kullanılarak fotoğraf üzerinde uygulanan gürültü arındırma filtresi kullanılarak gürültülerin kaldırıldığı bir temiz bir fotoğraf elde edilmektedir. Temiz fotoğraf orijinal fotoğrafdan çıkartıldığında ise fotoğraf üzerinde bulunan gürültü deseni ortaya çıkartılmaktadır. Bu sayede gürültü arındırma işlemi uygulanan fotoğraf üzerinden temizlenen PRNU gürültü deseninin ortaya çıkartılması ile kaynak kamera analizinde kullanılabilecek bir bilgi ortaya çıkartılmaktadır.

#### 2.1.2.2 Kaynak kamera imzası oluşturulması

Kaynak kamera eşleştirmesi, çekilen bir fotoğraftan alınan PRNU gürültüsünün farklı kameralardan oluşturulmuş kamera imzaları ile karşılaştırılması ile yapılmaktadır. Dolayısıyla, bu yöntem farklı kameraların imzalarından oluşan bir veritabanı gerektirmektedir. PRNU tabanlı kamera imzalarının oluşturulabilmesi için kaynak kameradan çekilen *N* adet fotoğraf gerekmektedir. *N* adet fotoğrafın çekildiği kameranın imzası [25] çalışmasında anlatıldığı gibi Maximum Likelihood Estimator

(ML) kullanarak oluşturulabilir. Bu yöntem ile kamera imzası tahminlemesi $K_I$, Formül (2.2) kullanarak hesaplanabilmektedir.

$$K_I = \frac{\sum_{i=0}^{N} G^{(i)} \quad F^{(i)}}{\sum_{i=0}^{N} (F^{(i)})^2} \tag{2.2}$$

Formül (2.2) de oluşturulan kamera imzası tahminlemesi içinde PRNU gürültüsünün yanı sıra renk enterpolasyonu gibi bileşenler de bulunmaktadır. Bu bileşenler aynı marka kamera sensörüne sahip kaynaklardan oluşturulan PRNU bazlı kamera imzası tahminlemelerinin benzer çıkmasına yol açmakta ve yanlış kaynak kamera tahminlerine yol açmaktadır [25]. Daha başarılı bir kaynak kamera tespiti yapılması için bu bileşenlerin kamera imzası tahminlemesi üzerinden silinmesi gerekmektedir. Bileşenlerin silinmesi için Kaynak kamera imzası tahminlemesi $K_I$ oluşturulduktan sonra, satır ve kolonların ortalaması sıfır'a eşitlenmektedir [26] ve daha sonra Wiener Filter [27] uygulanmaktadır. Böylece aynı marka kamera sensörü kullanan kaynaklardan oluşturulan imzaların birbirine benzemesinin önüne geçilmektedir.

#### 2.1.2.3 Kaynak kamera imzası ile fotoğrafların eşleştirilmesi

Kaynak kamera tespitinin başarılı olabilmesi için Bölüm 2.2.1 de belirtilen gürültü desenlerinin Bölüm 2.2.2 de belirtilen kamera imzaları ile eşleştirilmesi için bir yönteme ihtiyaç duyulmaktadır. Kaynak kamera imzalarının bulunduğu bir veri tabanı olduğu var sayılarak, burada bulunan imzalar ile gelen bir fotoğrafın eşleştirilmesi sonucunda fotoğrafın sahibi olan kameranın tespit edilmesi sağlanmaktadır. Bu eşleştirmenin düzgün şekilde yapılabilmesi için kamera imzası ve PRNU gürültüsü arasında bir korelasyon tekniği kullanılması gerekmektedir. Kamera imzası ve PRNU gürültüsü arasındaki korelasyon işlemi sonucunda oluşan maksimum korelasyon oranının kamera ve fotoğrafın eşleşmediği durumlarda sıfıra yakın olması beklenmektedir. Aynı şekilde eşleşme olduğu durumlarda korelasyon oranının sıfırdan çok daha büyük bir değer olarak gözlemlenmesi beklenmektedir. Dolayısıyla, karar aşamasının gerçekleştirilebilmesi için bir korelasyon oranı alt sınırı belirlenmesi gerekmektedir. Çalışmalar gösteriyor ki, farklı kamera modellerinin ürettiği farklı çözünürlüklerdeki fotoğraflar bulunduğu için bu oranın belirlenmesi mümkün olmamakta ve normal korelasyon teknikleri bu işlem için yetersiz kalmaktadır. Bu sebeple korelasyon yöntemi için Peak to Correlation Energy (PCE) tekniği önerilmektedir [26]. PCE oranı $\rho$, Formül (2.3) kullanılarak hesaplanmaktadır.

$$\rho = \frac{\alpha^2}{\frac{1}{c-|\gamma|} \sum_{n,n\notin\gamma} \alpha_c^2} \tag{2.3}$$

Formül (2.3) de kullanılan $\alpha$, kamera imzası, $K_I$ ile fotoğraftan çıkartılan PRNU gürültüsü $G$'nin normalleştirilmiş çapraz korelasyonunu, c, korelasyonda gözlemlenen supremum değerlerin bulunduğu yerleri, $\gamma$ ise $\alpha$ etrafındaki kare alanı temsil etmektedir.

## 2.2 Fotoğraf Anonimleştirme

PRNU tabanlı kaynak kamera tespiti yöntemlerinin engellenebilmesi için bir çok çalışma yapılmıştır [8, 9, 28, 29, 30]. Fotoğraf anonimleştirme teknikleri sadece kaynak kamera tespitini engellemek için değil aynı zamanda kamera imzası kopyalama saldırılarının [7] önüne geçmek için de kullanılmaktadır. Kaynak kamera tespit işlemlerinin büyük boyutlu kamera imzası veri tabanlarında hızlı bir şekilde yapılabilmesi için çalışmalar yapılmıştır [31]. Çalışmalarda anlatılan yüksek sayıda kamera imzası ile fotoğrafların kısa sürede eşleştirilebilmesi mümkün olduğu için bu yöntemin çok sayıda kamera imzasından oluşan veritabanları kullanılarak gerçek hayatta kullanımı mümkün olmaktadır. Bu sebeple, anonim şekilde fotoğraf paylaşmak isteyen aktivist ve gazeteciler için fotoğraf anonimleştirme tekniklerinin kullanılabilir olması gerekmektedir [32]. Bu anonimleştirme işlemleri arasında kullanılan bazı teknikler fotoğrafın orijinal boyutunu değiştirmektedir [33, 34]. Bu durum fotoğrafın orijinal görüntü oranını değiştirdiği için fotoğrafın orijinal boyutu ve kalitesi korunarak yapılan anonimleştirme teknikleri bu işlem için daha uygun olmaktadır.

Bu bölümün devamında fotoğraf anonimleştirme tekniklerinin amaç ve anonimleştirme işlemi için kullanılan yöntemlerin detayları verilmektedir.

### 2.2.1 Amaç

Günümüzde hemen hemen hayatın her anında sayısız fotoğraf çekilmektedir. Gelişen sosyal medya kullanımı ve fotoğraf paylaşım teknolojileri sayesinde bu fotoğraflar sürekli olarak internete yüklenmektedir. Ancak bir kamera (akıllı telefon) ile çekilen fotoğrafların bir arada olması fotoğraflardan bir kamera imzası oluşturulmasını mümkün hale getirmektedir. Bu durum, aynı kişinin çektiği başka fotoğrafları takip

etmek için bir zemin hazırlamaktadır. Aynı zamanda fotoğrafların sahibi, fotoğraflardan alınan PRNU gürültü verisinin başka bir fotoğrafa aktarılması ile kendisinin çekmediği bir fotoğraftan sorumlu olmasına neden olan saldırılara açık hale gelmektedir. Bu saldırılar [7] çalışmasında PRNU kopyalama saldırıları olarak belirtilmektedir. Buradan yola çıkarak, fotoğraf anonimleştirme tekniğinin temel amacı bir fotoğraftan kaynak kamera bilgisi taşıyan her veriyi kaldırarak, fotoğrafın kaynak kamerasının tespit edilmesini engellemektir.

### 2.2.2 Yöntem

Fotoğraf anonimleştirme işlemi için birçok farklı teknik önerilmiştir. Bunlar şu şekilde listelenebilir:

- Flat fielding
- Seam Carving
- Uyarlamalı PRNU Gürültüsü Arındırma

#### 2.2.2.1 Flat fielding

Bu yöntem fotoğraflarda bulunan iki ana gürültü bileşeni, FPN ve PRNU verisinin hesaplanması ve fotoğrafta bulunan bu gürültülerin bastırılması ile çalışmaktadır [30]. FPN bileşeni $\beta$, tamamen karanlık ortamlarda çekilen *N* adet fotoğrafın ortalaması ile Formül (3.1) ile elde edilmektedir.

$$\beta = \frac{1}{N}\sum_{i=1}^{N} F_i \tag{3.1}$$

PRNU bileşeni **Ω**, homojen olarak ışıklandırılmış ortamlardan alınan *M* adet fotoğrafın FPN bileşeninin çıkartılarak ortalaması alınması ile Formül (3.2) ile elde edilmektedir.

$$\Omega = \frac{1}{M}\sum_{i=1}^{M} F_i - \beta \tag{3.2}$$

Bu iki gürültü bileşeni elde edildikten sonra, aynı kameradan çekilmiş başka bir fotoğrafta flat fielding tekniği Formül (3.3) kullanılarak uygulanabilmekte ve kamera eşleşmesi olmadığı varsayılan fotoğraf $F'$, elde edilmektedir.

$$F' = \frac{F - \beta}{\Omega} \tag{3.3}$$

Ancak bu yöntemde belirtilen tekniğin uygulanması, tekniğin uygulanacağı fotoğraftaki FPN ve PRNU bileşenlerini oluşturan parametreler ile uyumlu olması gerektiği için zordur [30]. Ayrıca bu teknik Formül (3.1) de kullanılan ve bu iş için özel olarak çekilmiş fotoğraflar gerektirmektedir.

#### 2.2.2.2 Seam carving

Seam Carving tekniği PRNU gürültü deseninin fotoğrafdan silinmesi yerine bu desenin hizasının bozulmasını hedeflemektedir. Bu teknik ile fotoğrafda bulunan önemsiz alanların fotoğraflardan silinmesi, önemli görünen alan veya objelerin dokunulmaması ile PRNU deseninin bozulması sağlanmaktadır. Seam Carving tekniği öncelikle fotoğrafı gradyan fotoğraf haline getirerek, piksellerin gradyan enerjileri ölçüldükten sonra en düşük enerjiye sahip piksellerin fotoğrafdan silinmesi ile başarılmaktadır. Silme işlemi gerçekleştirildikten sonra fotoğrafın bütünlüğünün korunması için bir hizalama işlemi gerçekleştirilmektedir [34]. Bu yöntem fotoğraflarda bulunan PRNU gürültü desenini bozarak kaynak kamera tespitini engellesede her fotoğraf için kolayca uygulananamakla birlikte gerçek fotoğrafın görüntü oranını değiştirmektedir.

#### 2.2.2.3 Uyarlamalı PRNU gürültüsü arındırma

Uyarlamalı PRNU gürültüsü arındırma tekniğinin temel amacı, PRNU gürültüsünü fotoğraftan silmektir. Ancak, fotoğraftan çıkarılan PRNU gürültüsünün direkt olarak silinmesi yerine, yinelemeli olarak bu işlemi tekrar etmektedir. Bu tekrar işleminin amacı fotoğraf kamera imzası ile eşlemeyene kadar fotoğraf üzerinde PRNU silme işlemleri gerçekleştirilir. [8] çalışmasında anlatıldığı üzere, Formül (3.4) ile belirtilen orijinal fotoğraf $F$, üzerinden Formül (2.1) ile çıkartılan gürültü $G$, bir sabit $\omega$, ile çarpılıp çıkartıldığında anonimliği henüz belli olmayan fotoğraf $A'$ elde edilmektedir.

$$A' = F - \omega G \tag{3.4}$$

Çalışmaya göre öyle bir sabit değer $\omega$, bulunabilirki Formül (3.4) hesaplaması sonucunda ortaya çıkan fotoğraf, kaynak kamera imzası ile eşleştirildiğinde sonucun sıfır olduğu sonuçlar elde edilebilmektedir. En optimal $\omega$ değerinin bulunabilmesi

Formül (3.5) ile gösterilen fonksiyon ile gerçekleştirilebilse de çalışmada önerilen yöntem, bir PCE alt sınırı değeri belirlenerek, bu değerden düşük veya eşit sonuçlar bulunana kadar anonimleştirme işleminin tekrarlanmasıdır.

$$\omega = \underset{\omega \in [1,\infty)}{argmin}(PCE(\ A', K_I)) \tag{3.5}$$

Anonimleştirme işlemi PCE üst sınır değeri $\sigma_{pce}$, kullanılarak işlemi Formül (3.6) belirtilen koşul gerçekleşene kadar Formül (3.4) işleminin farklı sabit değer ile tekrarlanması ile elde edilmektedir.

$$PCE(\ A', K_I) \leq\ \sigma_{pce} \tag{3.6}$$

Bu yöntem ile daha önce bahsedilen tekniklere göre çok daha yüksek bir başarı elde edilmiş ve fotoğrafların kaynak kameraları ile eşleştirilmeleri engellenmiştir [8].s Ayrıca başka bir çalışmada, kullanılan filtre tekniği değiştirilerek alınan sonuçların daha başarılı hale getirilmesi sağlanmıştır [9].

# 3. HDR FOTOĞRAFLARDA KAYNAK KAMERA TESPİTİ

## 3.1 Ön Bilgiler

Yüksek Dinamik Aralıklı (HDR) fotoğraflar çekebilme işlevi günümüzde hemen hemen her akıllı telefonda ve kamerada bulunan bir özellik haline gelmiştir. HDR fotoğrafların amacı ve oluşturulma tekniği normal fotoğraflardan daha farklı şekildedir. Bu nedenle kaynak kamera analizi teknikleri bu fotoğraflarda normal fotoğraflarda olduğundan farklı şekilde sonuçlar vermektedir.

### 3.1.1 HDR Teknolojisi

Normal fotoğrafların aksine HDR teknolojisi, çok gölgeli ve ışıklı olan alanların insan gözünün gördüğüne daha yakın ve daha gerçekçi hale getirebilmek amacıyla fotoğraf çekimi sırasında ve sonrasında yapılması gereken farklı işlemler gerektirmektedir [35]. Bu işlemler sayesinde, HDR fotoğraflarda bazı alanlarda ışık patlamaları veya çok karanlık kalan detaylar gözlenmemektedir.


Resim 3.1 : HDR ve normal mod ile çekilmiş fotoğraflar [36].

Resim 3.1 de bir sahnenin solda HDR özelliği açıkken ve sağda kapalıyken çekilmiş fotoğrafları gösterilmektedir. Resim 3.1 üzerinde görüldüğü gibi HDR özelliği açıkken çekilmiş olan fotoğrafta detaylar daha net ve farklı alanların ışık seviyesi özellik kapalıyken çekilmiş fotoğrafa göre karanlık alanlar daha belirgin ve daha gerçekçi olarak görülmektedir.

### 3.1.2 HDR Fotoğraf Oluşturulma Yöntemi

HDR fotoğrafların oluşturulması için fotoğrafın çekimi sırasında ve sonrasında farklı işlemler yapılmaktadır. Bu fotoğrafların oluşturulması için farklı ışık seviyelerinde çekilmiş genelde üç adet fotoğraf gerekmektedir. Bu fotoğraflar kullanıcı farkında olmadan kamera tarafından arka arkaya otomatik olarak çekilmektedir. Bu farklı ışık seviyelerine sahip fotoğraflar birleştirilerek yüksek dinamik aralığına sahip tek bir fotoğraf elde edilmektedir [37]. Ancak bu fotoğraflar çok kısa bir süre içerisinde çekilse dahi çekilen sahnedeki objelerin hareket etmesi veya kamera lensinin kullanıcı tarafından titretilmesi sebebiyle bu fotoğraflarda farklılıklar oluşabilmektedir. Bu durum HDR fotoğrafın elde edilmesi için gereken birleştirme işleminde sorun oluşturmaktadır ve bu sorunun çözülebilmesi için bir çok hizalama ve gürültü kaldırma yöntemi önerilmektedir [38 - 41]. Bu yöntemlerin hepsinin temel hedefi aynı kameradan ve aynı sahneden çekilen farklı ışık seviyesine çekilen fotoğrafların birleştirilmesi sırasındaki hizalama sorunlarının çözülmesidir. Hizalama yöntemi fotoğraflarda uygulandıktan sonra birleştirme işlemi sonlanmaktadır ve HDR fotoğraf elde edilmektedir.

## 3.2 Problemin Tanımı

Yüksek Dinamik Araklı fotoğrafların oluşturulması normal fotoğraflara göre farklı işlemler gerektirmektedir. Bölüm 4.1.2 de anlatılan bu işlemler sebebiyle HDR fotoğraflarda kaynak kamera tespit teknikleri tam olarak düzgün çalışamamaktadır. Bunun sebebi fotoğraf üzerinde yapılan hizalama işlemleri kaynak kamera tarafından oluşturulan PRNU gürültü deseninde değişikliklere sebep olmaktadır. Fotoğraf üzerinde hizalama işlemi yapılmayan alanlar olmasının yanı sıra tüm fotoğrafa bakıldığında eşleştirme sonucu için kullanılan PCE değeri çoğu zaman düşük çıkmaktadır. HDR teknolojisinin günümüzde kullanılan çoğu kamerada bulunması

sebebiyle bu eşleştirme işleminin yapılabilmesi, daha başarılı bir kaynak kamera analizi yapılabilmesi için önem arz etmektedir.

### 3.3 Önerilen Yöntem

Fotoğraf üzerinde hizalama yapılmayan alanların bulunması veya kaydırılmış PRNU gürültü desenlerinin saptanması kaynak kamera analizini mümkün hale getirebilir. Bu sebeple kaynak kamera tespiti tekniği HDR fotoğraflar üzerinde daha farklı yöntem ile çalıştırılması gerekmektedir. Bu yöntem öncelikle kaynak kamera imzasıyla parçalı olarak eşleştirilme işlemi yapılabilmesi için HDR bir fotoğrafın bölünmesini gerektirmektedir. Bölünme işlemi bir matrisin, $a\ x\ b$ boyutuna sahip $n$ adet matris haline getirilmesidir. Bu işlem sırasında kullanılan matrisin fotoğraf üzerindeki görüntüsü Resim 3.2 de kırmızı kare olarak gösterilmektedir.

Resim 3.2 : Arama matrisinin HDR fotoğraf üzerindeki görüntüsü.

Bu işlem fotoğraf üzerinde direkt olarak uygulanmaktansa, fotoğraf üzerinden çıkartılan PRNU gürültüsü üzerinden yapılmaktadır. HDR bir fotoğraftan çıkartılan PRNU gürültüsü $G_{HDR}$'nin aynı kameradan çekilen HDR olmayan fotoğraflar kullanılarak oluşturulan kamera imzası $K_I$, ile eşleştirilmesi için kullanılan fonksiyon Formül (4.1) de belirtilmiştir.

$$G_{HDR} = ara(K_I, G_{HDR}) \tag{4.1}$$

Gürültü verisinin bölümlendirilmesi için gerekli veriler, satır büyüklüğü *a* sütun büyüklüğü ise *b* ile gösterilerek, Formül (4.2) kullanılarak elde edilmektedir. Sonuç olarak $G_{HDR}$ üzerinden *n* adet *a x b* boyutunda gürültü matrisi $\overline{G}$, elde edilmektedir.

$$\overline{G} = bol(G_{HDR}, \mathrm{a}, \mathrm{b}) \tag{4.2}$$

Gürültü listesinin kamera imzasıyla eşleştirilebilmesi için her bir gürültü matrisi $G_i$, için kamera imzası arama listesi oluşturulmaktadır. Bu liste Formül (4.3) ile belirtilen fonksiyon ile elde edilmektedir.

$$\overline{K_I}^{(G_i)} = imzaBol(K_I, \mathrm{a}, \mathrm{b}, \forall) \tag{4.3}$$

Formül (4.3) ile belirtilen fonksiyon kamera imzası üzerinde *a x b* boyutundaki bir dikdörtgeni kaydırarak farklı kamera imza parçacıkları oluşturmaktadır. PRNU verisindeki kaymaların mantıklı şekilde ele alınması için kaydırma işleminin sınırlarının belirlenmesi için arama sınırını belirleyen sabit sayı ∀, kullanılmaktadır. Kaydırma işlemi her defasında bir piksel olmak üzere matrisin üst köşesinden başlanarak önce sağa ve aşağı doğru gerçekleştirilmektedir. Daha sonra HDR fotoğraf üzerinden çıkartılan $G_{HDR}$, verisinin kendisi için oluşturulan kamera imzaları $\overline{K_I}^{(G_i)}$ ile eşleştirilerek bir sonuca varılabilmesi için Formül (4.4) de gösterilen eşleştirme fonksiyonu kullanılmaktadır. Karar verme aşamasında $\overline{K_I}^{(G_i)}$ içerisindeki her bir matris $K_{I_j}$ ve gürültü $G_i$, arasında eşleşmenin olup olmadığını belirleyecek PCE alt sınırı $\epsilon_{PCE}$ kullanılmaktadır. Önceki çalışmalardan elde edilen sonuçlara göre bu değer 50 olarak kullanılabilmektedir [8, 42].

$$E(K_{I_j}, G_i) = \begin{cases} 1 & eğer \quad PCE\left(K_{I_j}, G_i\right) \geq \epsilon_{PCE} \\ 0 & aksi\ halde \end{cases} \tag{4.3}$$

Verilen bilgiler kullanılarak eşleştirme algoritmasının sözde kodu Şekil 3.1 ile gösterilmektedir.

```
int eslestir(hdrFoto, kameraImzasi, a, b, kisit, pceEsigi) {
    prnuHdr = prnuCikart();
    gurultuParcalari = bol(prnuHdr, a, b);

    foreach(g in gurultuParcalari) {
        imzaParcalari = imzaBol(kameraImzasi, a, b, kisit);
        foreach(i in imzaParcalari) {
            if(pce(i, g) >= pceEsigi){
                return 1;
            }
        }
    }
    return 0;
}
```

Şekil 3.1 : Eşleştirme algoritması sözde kodu.

### 3.4 Sonuçlar

Önerilen yöntem için test sonuçlarının oluşturulması için, kaynak kameradan toplanan fotoğraflardan kamera imzası oluşturulmuştur. Bu kamera imzası ile aynı kaynak kameradan alınan HDR fotoğraflar için iki farklı senaryosu hazırlanmış ve sonuçlar toplanmıştır. Birinci senaryoda kamera imzası tam fotoğraf eşleştirme yöntemi ile HDR fotoğraflarla eşleştirilmiş, ikinci senaryoda ise aynı fotoğraflar parçalı kamera imzası eşleştirme yöntemi ile eşleştirilmiştir. Testlerde kullanılan kamera imzası 100 adet HDR olmayan fotoğraftan çıkartılmıştır. Parçalı eşleştirme yönteminin çalışması için gerekli olan parametrelerin değerleri Çizelge 3.1 ile verilmiştir.

Çizelge 3.1 : Algoritma parametreleri.

| Parametre | Değer |
|---|---|
| a | 300 |
| b | 300 |
| ∀ | 30 |
| $\epsilon_{PCE}$ | 50 |

Çizelge 3.1 ile verilen değerler kullanılarak 50 fotoğraf ile çalıştırılan testlerde elde edilen eşleştirme oranı $\theta$, her bir fotoğraf için Formül (4.3) ile gösterilen fonksiyondan alınan sonuçların toplamının test için kullanılan HDR fotoğrafların sayısına bölünmesi ile Formül (4.4) kullanılarak hesaplanmaktadır.

$$\theta = \frac{1}{50} \sum_{i=1}^{50} E(K_{I_j}, G_i) \quad (4.4)$$

Çizelge 3.2 de verilen sonuçlar incelendiğinde, HDR fotoğraflarda uygulanan kaynak kamera analizinde parçalı eşleştirme yöntemi tam eşleştirme yöntemine göre %66 daha iyi eşleşme sonucu vermektedir. Testler kapsamında tam fotoğrafın önerilen algoritma ile taranması zamansal olarak uzun bir işlem olduğu için tam fotoğrafın ilk çeyreğinde eşleşme bulunamadığı durumda algoritma sonlandırılmaktadır. Tam fotoğraf üzerinde arama işleminin devam etmesi durumunda tüm fotoğrafların kamera imzası ile eşleştirilmesi mümkün olabilmektedir.

Çizelge 3.2 : HDR fotoğraf eşleştirme sonuçları.

| | Tam Eşleştirme Tekniği | Parçalı Eşleştirme Tekniği |
|---|---|---|
| $\theta$ | 0.24 | 0.9 |

# 4. ANDROID TELEFONLARDA GÜVENLİ KAMERA UYGULAMASI

## 4.1 Amaç

Günümüzde insanların akıllı telefonları ile çekerek internete yüklenen fotoğraf sayısı giderek artmaktadır. Bu fotoğraflar sadece bir anı olmaktan başka PRNU gürültüsü tabanlı kamera imzası olmak için bir kaynak oluşturmaktadır. Bu veri aynı kameradan çekilen başka fotoğrafların tespiti için ve daha önemlisi, adli bir durumda delil olarak kullanılacak bir fotoğraflara kopyalanabilmektedir. Bu durumlardan korunmanın yöntemi herkese açık ortamlara yüklenen fotoğraflardan PRNU gürültüsünün kaldırılmasıyla engellenebilmektedir. Ancak bu işlemi yapacak bir uygulama bulunmadığından bu işlem kullanıcılara sadece teorik olarak sunulmaktadır. Fotoğrafların güvenli kalması ve kullanım kolaylığı açısından bu uygulama, fotoğrafın çekildiği kaynak üzerinde var olması gerekmektedir. Akıllı telefonlarda bulunan kamera teknolojilerinin çok gelişmesi ile bu akıllı telefonları günümüzde birçok insan dijital kameraların yerine kullanmaya başlamıştır. Bu çalışma ile fotoğraf anonimleştirme işlemini kendi içinde sunacak bir güvenli kamera uygulaması geliştirilerek, insanlar, özellikle gazeteciler için bu güvenlik sorununun çözülmesi hedeflenmektedir.

## 4.2 Problemler

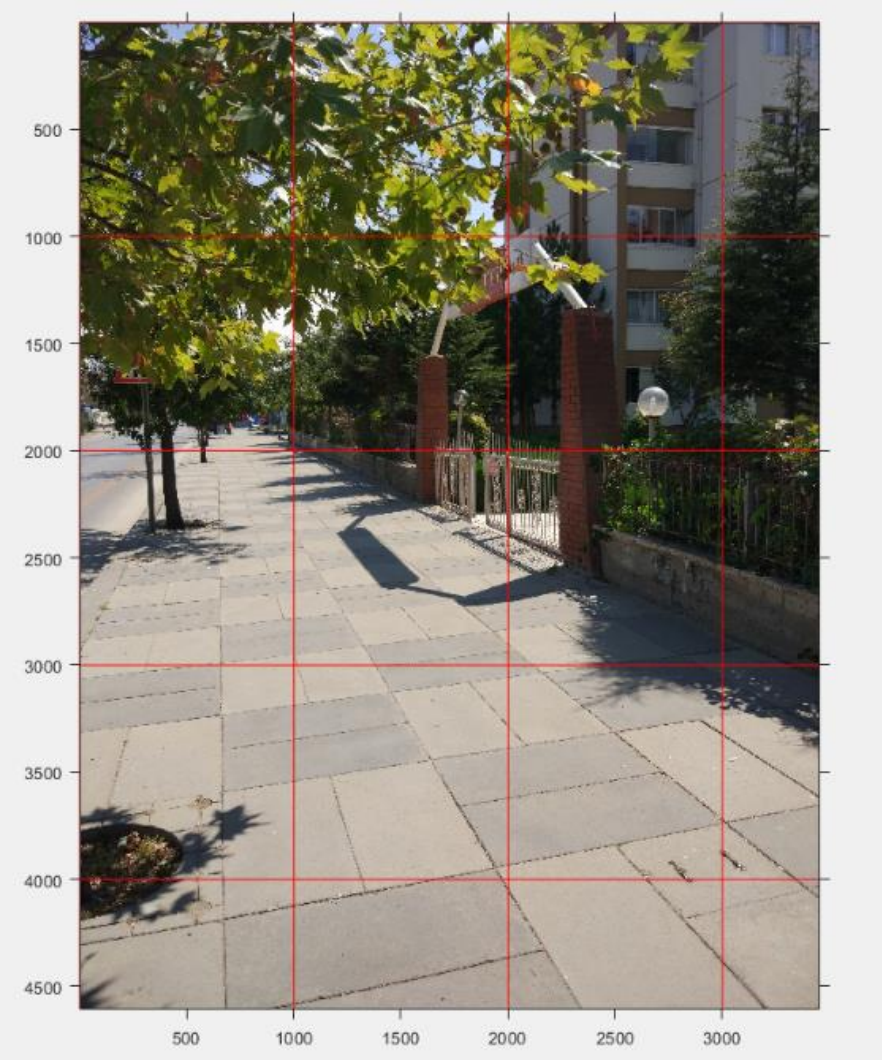
Fotoğraflara anonimleştirme başarısı yüksek olan uyarlamalı PRNU gürültüsü kaldırma yöntemleri [8, 9] uygulanabilmesi için öncelikle kaynak kamera imzası çıkartılması ve anonimleştirme işlemlerinin uygulanması gerekmektedir. Bu işlemler fazla işlem gücü ve bellek gerektirdiği için sistem kaynağı kısıtlı telefonlarda çalıştırılması mümkün olmamaktadır. Bu işlemlerin sistem kaynağı kısıtlı telefonlarda çalıştırılamamasının sebebi olarak Android işletim sisteminde bulunan Android görev öldürücü gösterilebilir. Android görev öldürücünün amacı telefonun stabil olarak çalışmasını sağlamak için fazla sistem kaynağı tüketen uygulamaların sistem tarafından otomatik olarak kapatılmasıdır. Bu sebeple, kamera imzası oluşturma ve

anonimleştirme işlemleri Android telefonlar üzerinde doğrudan çalıştırılamamaktadır. Bu işlemlerin kaynak sistemin işlem gücünü kullanmadan internet üzerine yüklenerek uzak bir sistemde çalıştırılması mümkün olsa bile, bu insanların güvenle kullanmak isteyeceği bir sistem olmayacaktır. Ancak kaynak kullanımı kısıtlayacak şekilde kurgulanmış bir anonimleştirme işlevi içeren bir yöntemin düşünülmemesi sebebiyle bu işlevler doğrudan akıllı telefonlar üzerinde de çalıştırılamamaktadır.

### 4.3 Önerilen Yöntem

Anonimleştirme işlemi için gereken işlemlerin sistem gücü kısıtlı telefonlarda sorunsuz çalışabilmesi oluşturulacak uygulamanın kullanacağı kaynak gücü sınırlanarak ve sistem tarafından kapatılmasının önüne geçilerek gerçekleştirilebilmektedir. Bölüm 2.2.2.3 de belirtilen fotoğraf anonimleştirme işleminin fotoğraflara uygulanabilmesi için öncelikle kamera imzası çıkartılması gerekmektedir. Kamera imzası çıkartılması için gereken fotoğrafların uygulamaya yüklenmesi ve imza oluşturulması sırasında bellek dolmasını engellemek için bu fotoğrafların imzası oluşturulurken boyutlarının azaltılması gerekmektedir. Fotoğrafların çekildiği kalitenin korunması için bu işlemin sıkıştırma teknikleri ile gerçekleştirilmesi uygun olmamaktadır. Uygulamaya fotoğraflar yüklendikten sonra her fotoğrafın üzerinde belirli alanların işaretlenerek bu alanlar ile çevreli fotoğraf parçalarını kullanarak kamera imzaları oluşturulması hem fotoğrafın kalitesini korumakta hem de bellek kullanımı kısıtlamaktadır. Bu yöntem ile kamera imzası oluşturulması için öncellikle $n$ adet fotoğrafın uygulamaya yüklenmesi sağlanmakta ve sonrasında her bir fotoğraf $F$ üzerinde $a$ x $b$ boyutunda alanlar dikdörtgen bir işaretçi ile belirtilmektedir. Resim 4.1 de gösterilen kırmızlı kareler bir fotoğrafta 1000 x 1000 boyutundaki işaretçilerle belirtilmiş alanları göstermektedir. Eğer fotoğraf üzerinde dikdörtgen boyutundan küçük kalan alan var ise (Örn. Resim 4.1 üzerinde gösterilen fotoğrafta en sağ ve en alt tarafta kalan kısımlar.) bu alanlar kendi boyutlarında tutulmaktadır. Bu işaretleme işlemi, kamera imzası oluşturulması için yüklenen her fotoğraf üzerinde gerçekleştirildikten sonra her fotoğrafın aynı indekse sahip parçası için kamera imzası oluşturulması sağlanmaktadır. Böylece her fotoğrafdan elde edilecek parça sayısı $m$, Formül (5.1) ile elde edilebilmektedir. Fotoğrafın uzunluğu $x$, genişliği $y$ ile işaretleyici uzunluğu $a$ ve genişliği $b$ ile belirtilmiştir.

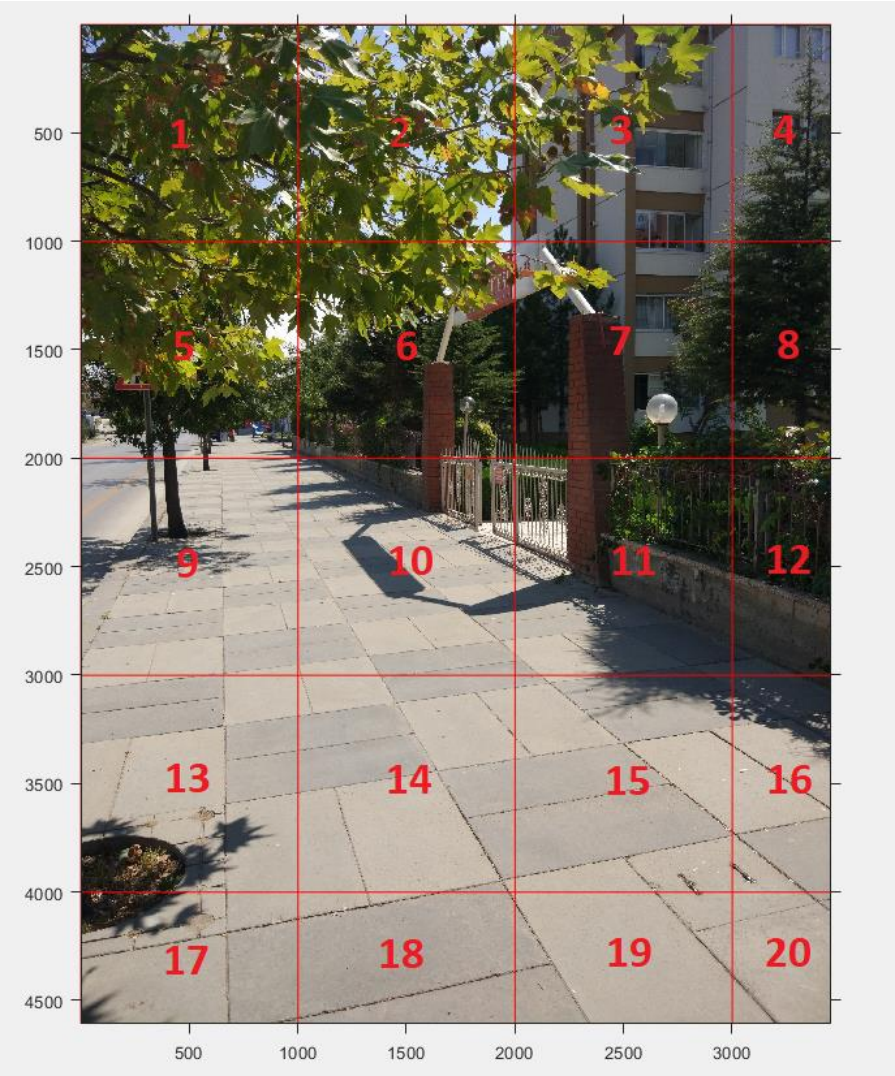
$$m = yukariyuvarla\left(\frac{x}{a}\right) + yukariyuvarla\left(\frac{y}{b}\right) \quad (5.1)$$




Resim 4.1 : 1000 x 1000 boyutunda işaretçiler ile ayrılmış fotoğraf.

Bu işlem sonucunda herbir fotoğrafdan elde edilen toplam *m* adet parçadan oluşan işaretçi listeleri elde edilmektedir. Bu listelerdeki aynı indekse sahip fotoğraf parçaları ile bir kamera imzası toplamda *m* adet imza oluşturulmaktadır. Daha sonra oluşturulan bu imzalar sistem hafızasına kaydedilerek anonimleştirme sürecinde kullanılmak üzere saklanmaktadır. Her anonimleştirme sürecinde aynı kamera imzası kullanılacağı için bu işlemin her kamera için bir kere yapılması yeterlidir. Kamera imzasının tüm fotoğraf yerine fotoğrafdan alınan ve boyutları esas fotoğrafdan çok daha küçük olan parçalar ile oluşturulması sayesinde imzayı oluşturan algoritmanın sadece belirli miktarda bellek ve işlem gücü kullanması sağlanmaktadır.

Kamera imzasının tam boyutlu fotoğraflardan değilde fotoğraf üzerinden alınan küçük parçalar üzerinden çıkartılması sebebiyle anonimleştirme işlemi uygulanacak fotoğrafın da aynı boyutlarla bölümlenmesi ve tek tek anonimleştirilmesi gerekmektedir. Anonimleştirme işlemini için işlemin uygulanacağı fotoğrafın uygulamaya yüklenmesi sağlandıktan sonra kamera imzası oluşturulurken kullanılan aynı boyutlara sahip dikdörtgenler ile bu fotoğrafın işaretlerenerek bölünlenmesi sağlanmaktadır. Daha sonra elde edilen *m* adet parçalanın her biri ile kendisine karşılık gelen kamera imzası kullanılarak Bölüm 2.2.2.3de belirtilen anonimleştirme işlemi gerçekleştirilmektedir.




Resim 4.2 : Fotoğraf işaretçi numaraları.

Anomileştirme işlemi Resim 4.2 ile gösterilen tüm fotoğraf parçaları için 1 numaradan başlayarak 20 numaralı işaretçinin gösterdiği fotoğraf parçasına kadar sıralı şekilde tamamlandıktan sonra her bir parça, fotoğraf üzerinde kendisinin alındığı numaralı

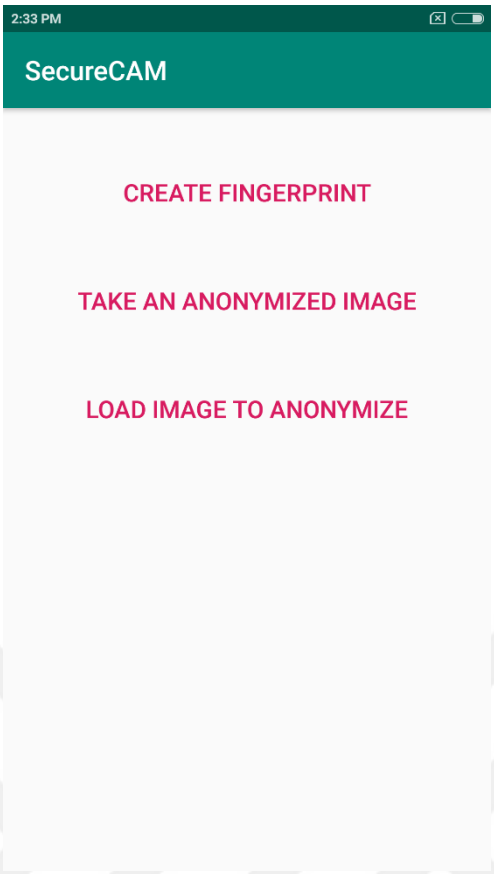
alana yerleştirilerek birleştirme işlemi gerçekleştirilmektedir. Son olarak bu işlem sonucunda elde edilen anonim fotoğraf telefon hafızasına kaydedilmektedir.

### 4.4 Uygulamada Kullanılan Teknolojiler

Güvenli kamera uygulaması Android tabanlı akıllı telefonlar için geliştirildiği için geliştirme işlemi için Android Studio uygulaması kullanılmıştır. Kaynak kamera imzası oluşturulması ve anonimleştirme işlemleri için gerekli algoritmalar C++ dilinde kodlanmıştır ve tüm bu işlemleri sağlayan yerel bir kütüphane oluşturulmuştur. Görüntü işleme işlemleri için OpenCV kütüphanesinden yararlanılmıştır. Android tabanlı cihazlara uygulama geliştirilirken Java dilinin desteklenmesi sebebiyle uygulamanın tüm parçaları Java ile kodlanmıştır. Uygulamanın kamera imzası oluşturma ve anonimleştirme işlemi gerçekleştirebilmesi için C++ ile oluşturulan kütüphane ile haberleşmesini sağlamak için Android tarafından sağlanan Android Native Development Kit (NDK) kullanılmıştır. NDK bir java uygulamasında C/C++ gibi yerel diller ile yazılan kodların çağrılabilmesine olanak sağlayan bir alt yapıdır. Uygulama geliştirilirken uygulamanın çalıştırılması için Android Studio tarafından sağlanan Android Emulator kullanılmıştır. Android Emulator farklı model Android işletim sistemi kullanan telefonların bilgisayar üzerinde simülasyonlarının çalıştırılması için sağlanan bir Android Studio eklentisidir.

### 4.5 Uygulama

Güvenli kamera uygulaması, uygulama üzerinden çekilen veya daha önce çekilmiş bir fotoğrafın uygulama içerisinde yüklenerek fotoğraf üzerinde bulunan PRNU gürültü desenini silmektedir. Uygulama üzerinden çekilen fotoğrafların direkt olarak anonimleştirilerek sisteme kaydedilmesi sayesinde uygulama üzerinden çekilen fotoğraflar güvenli şekilde paylaşılabilir hale gelmektedir. Anonimleştirme işlemi bir kamera imzası gerektirdiği ve bu sebeple anonimleştirme işlemi gerçekleştirilemediği için öncelikle bir kamera imzası oluşturulması istenmektedir.

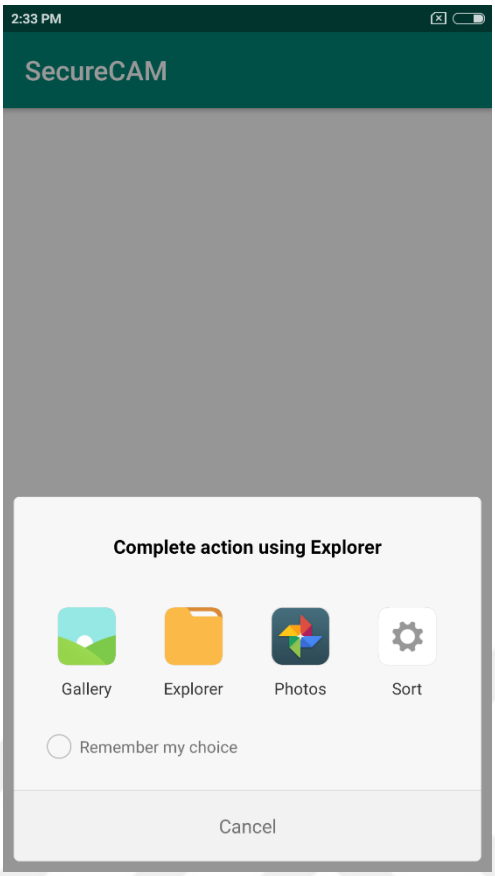



Resim 4.3 : Güvenli kamera uygulaması ana menüsü.

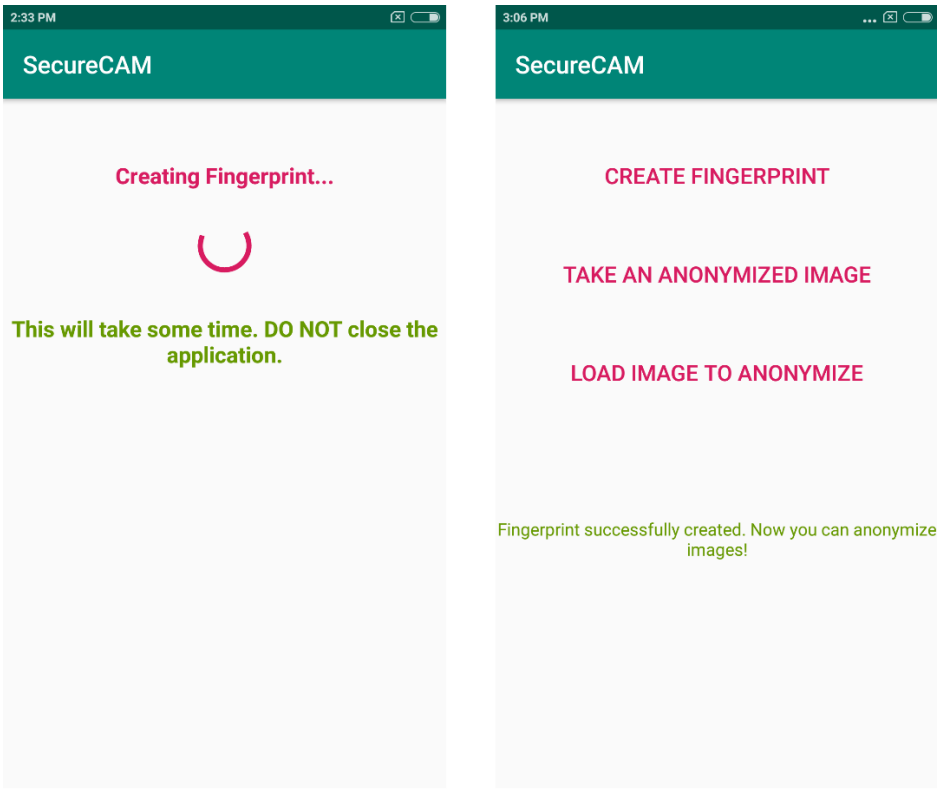
Uygulama üzerinden kullanıcıya sunulan ana menü Resim 4.3 ile gösterilmektedir. Kullanıcıya sunulan üç temel işlev şu şekildedir.

- Kamera imzası oluşturma
- Anonim fotoğraf çekme
- Anonimleştirme için fotoğraf yükleme

Kamera imzası oluşturma işlevinde kullanıcının daha önceden çekmiş olduğu fotoğraflar kullanılarak bir kamera imzası oluşturması beklenmektedir. Bu menüye giriş yapıldığında telefon hafızasından fotoğraf yüklenebilmesi için kullanıcıya Resim 4.4 ile gösterilen ekran ile hafızadan uygulamaya fotoğraf yükleyebilmesi sağlanmaktadır. Belirtilen fotoğraflar seçildikten sonra kamera imzası oluşturma işlemi tamamlanana kadar gösterilen ekran Resim 4.5 üzerinde sol tarafta ve işlem tamamlandığında gösterilen ekran sağ tarafta gösterilmektedir.

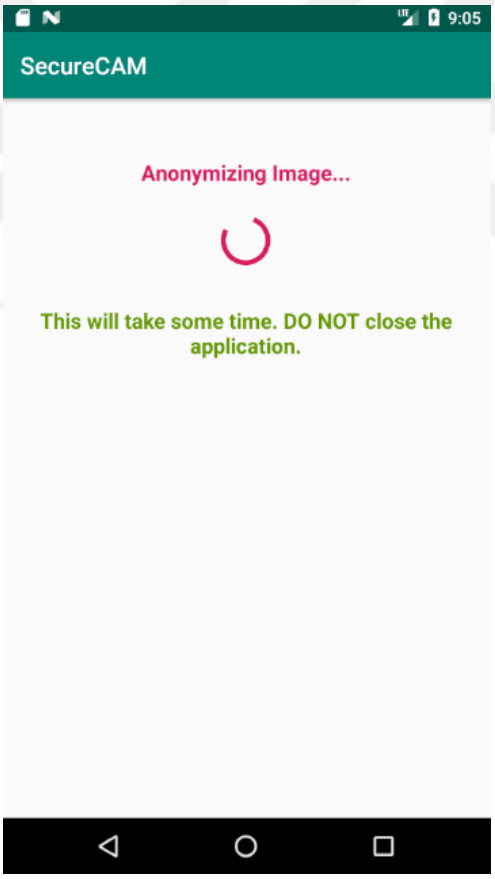



Resim 4.4 : Güvenli kamera uygulaması fotoğraf yükleme ekranı.



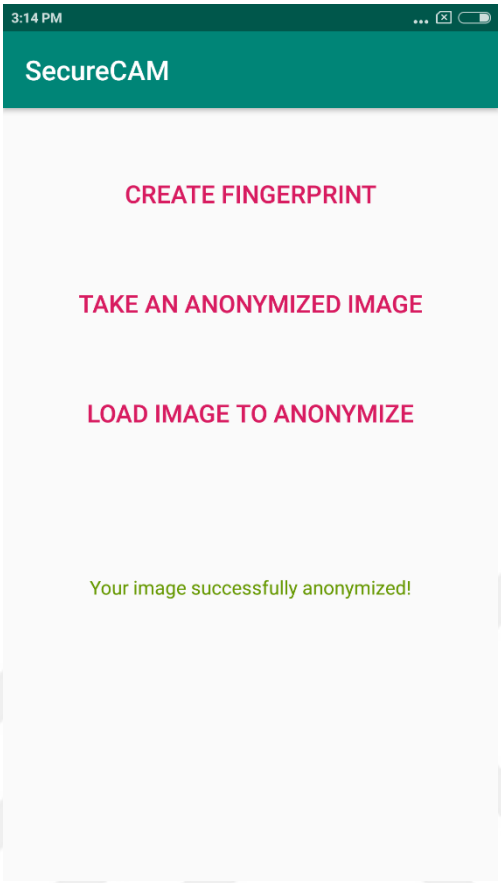

Resim 4.5 : Kamera imzası oluşturulma ve sonrasında gösterilen ekranlar.

Gerekli fotoğraflar telefon hafızasından uygulamaya yüklendikten ve kamera imzası oluşturulduktan sonra kullanıcıya sunulan Anonim Fotoğraf Çekme veya Anonimleştirme için Fotoğraf Yükleme işlevleri kullanılabilir hale gelmektedir. Anonim Fotoğraf Çekme menüsünün seçilmesiyle kullanıcı telefonunun kamera uygulamasına yönlendirilerek fotoğraf çekmesi istenilmektedir ve bu fotoğraf uygulama üzerine aktarılmaktadır. Anonimleştirme için Fotoğraf Yükleme menüsünün seçilmesinde ise Resim 4.4 ile gösterilen fotoğraf yükleme ekranı ile telefon hafızasından fotoğraf yüklenmesi istenmektedir. Bu işlevin amacı daha önce telefon kamera uygulaması veya telefonda bulunan başka bir uygulama tarafından çekilmiş fotoğraflarda anonimleştirme işlemi gerçekleştirilebilmesidir. Anonimleştirme işlemi başlatıldığında kullanıcıya gösterilen ekran Resim 4.6 gösterilmektedir.




Resim 4.6 : Güvenli kamera uygulaması anonimleştirme işlemi ekranı.

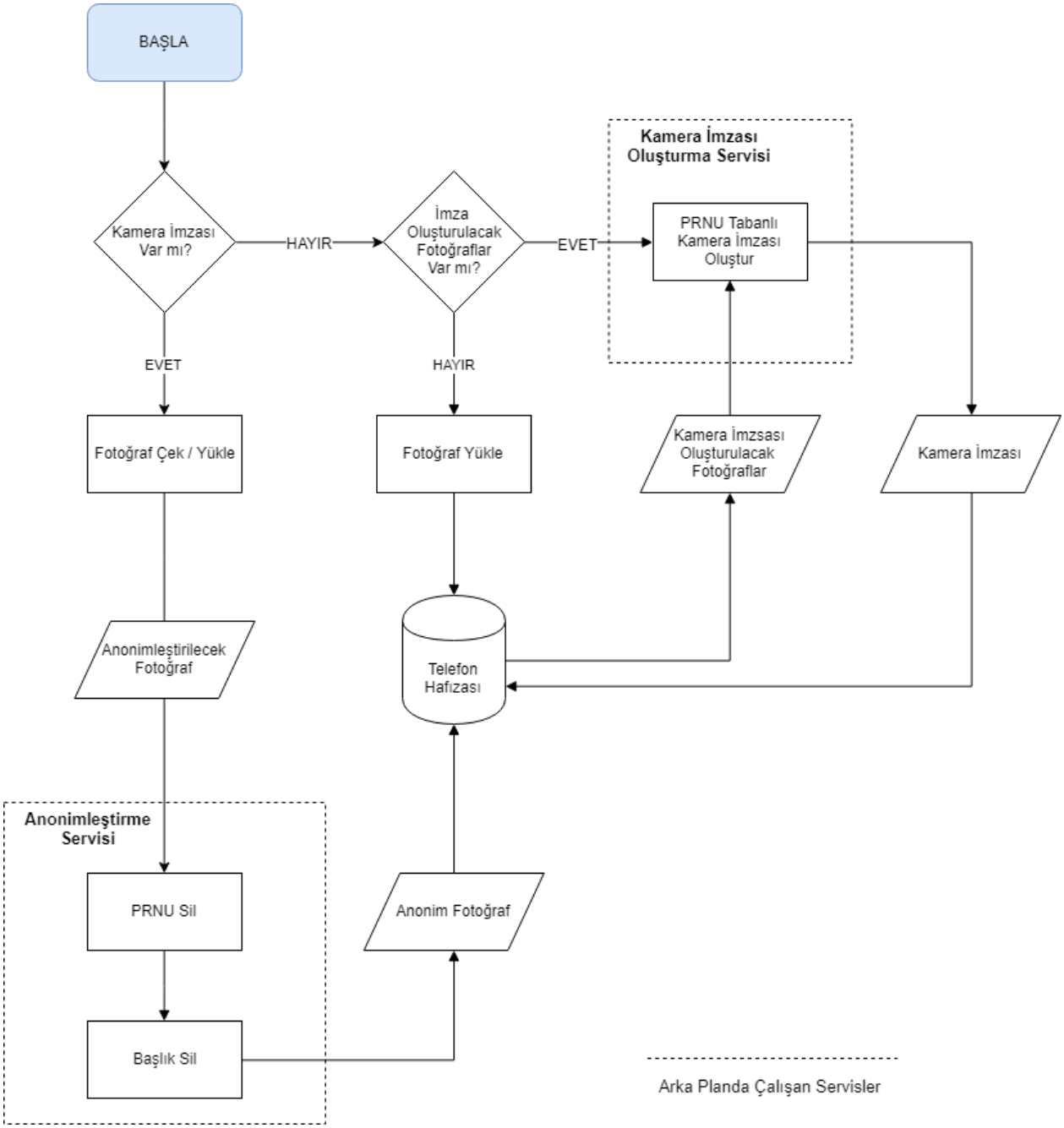
Her iki işlev ile başlatılan anonimleştirme işlemi tamamlandığında kullanıcıya gösterilen ekran Resim 4.7 de gösterilmektedir ve bu işlem sonucunda anonim fotoğraf telefon hafızasına kaydedilmektedir.




Resim 4.7 : Anonimleştirme işlemi sonucunda gösterilen ekran.

Uygulamanın çalışması sırsaında kullanılan iş akışı Şekil 5.1 ile gösterilmektedir. Kullanıcının kamera imzası oluşturulma ve anonimleştirilme işlemleri sırasında telefonda yapabileceği işlemlerin engellenmemesi için bu işlemler (Akış şemasında kesik çizgili olarak gösterilen alanlar.) sistemde arka tarafta çalışan iş parçacıkları üzerinde çalıştırılmaktadır. Uygulamanın kamera imzası oluşturulması ve fotoğraf anonimleştirme süresince açık bırakılması durumunda gösterilen ekranlar Resim 4.5 ve Resim 4.6 de gösterilmektedir. Aynı zamanda çekilen fotoğrafın anonimleştirme sırasında telefonda oluşabilecek bir kapanma sonucunda fotoğrafın kaybedilmemesi için bu fotoğraf uygulama dışından erişilemeyen bir alanda saklanmaktadır. Anonimleştirme işlemi için gereken kamera imzası oluşturulması işleminin sadece bir kere yapılması yeterli olsada kullanıcı Kamera İmzası Oluşturma menüsünü kullanarak bu işlemi tekrar gerçekleştirebilmektedir. Bu işlem sonucunda telefon hafızasında saklanan eski kamera imzasınnın üzerine yenisi yazılmaktadır. Uygulamanın silinip tekrar yüklenmesi sonucu kamera imzasının kaybedilmemesi için

bu imza bilgisi uygulamanın alanında değil dış saklama biriminde (external storage) üzerinde saklanmaktadır.




Şekil 4.1 : Güvenli kamera uygulaması iş akış şeması.

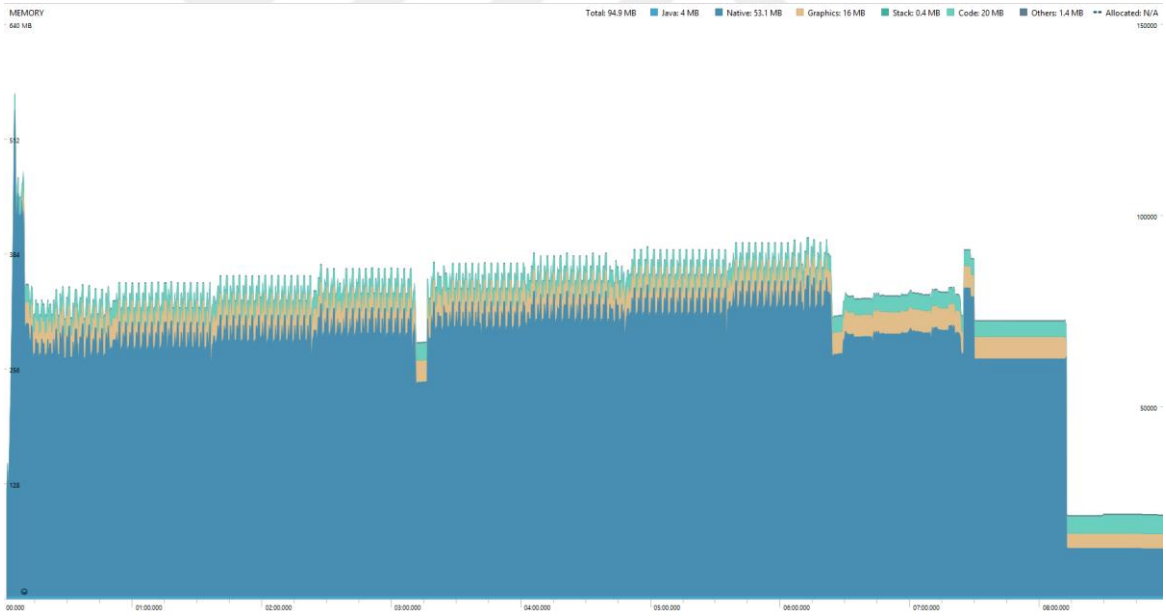
## 4.6 Sonuçlar

Uygulamanın farklı sistem özelliklerine sahip telefonlarda çalışmasının test edilebilmesi için farklı özelliklere sahip telefonlarda üzerinde kamera imzası

oluşturma ve anonimleştirme işlemleri çalıştırılmıştır. Testlerin gerçek durum senaryoları üzerinde gerçekleştirilebilmesi için telefon üzerinde çalışan hiçbir arka plan uygulaması kapatılmadan uygulama çalıştırılmıştır. Kamera imzası oluşturma ve anonimleştirme işlemlerinin kullandığı kaynaklar, Android Studio üzerinde bir eklenti olarak sağlanan Android Profiling Tool ile ölçülmüştür. Android Profilin Tool elde edilen örnek bellek tüketimi grafiği Resim 4.8 de verilmektedir. Uygulama çalıştırılırken kullanılan parametreler, çizelge büyüklüğü ve anonimleştirme sırasında kullanılan ve anonimleştirme işleminin sonucunda ulaşılması gereken maksimum PCE değeri Çizelge 4.1 de verilmektedir.

Çizelge 4.1 : Uygulamada kullanılan parametreler.

| Parametre | Değer |
|---|---|
| a (İşaretçi uzunluğu) | 1000 |
| b (İşaretçi genişliği) | 1000 |
| $\epsilon_{PCE}$ | 10 |




Resim 4.8 : Android Profiling Tool ile elde edilen örnek bellek tüketimi grafiği.

Çizelge 4.1 ile verilen parametrelerle farklı akıllı telefonlarda çalıştırılan kamera imzası oluşturulması işlemi sırasında elde edilen ortalama bellek kullanımı fotoğraf boyutları ve cihaz markaları ile Çizelge 4.2 de verilmektedir. Elde edilen sonuçlara göre ortalama bellek kullanımı en yüksek değeri olarak 680 MB, en küçük değeri olarak ise 480 MB olarak gözlemlenmiştir. Farklı çözünürlükteki fotoğraflar

incelendiğinde Formül (5.1) ile verilen formül kullanıldığında her bir fotoğraf için işlenecek fotoğraf parçası sayısı *m*, hesaplandığında en fazla parça 20 adet ile 3456x4608 çözünürlüğündeki fotoğraflar çeken Xiomi MI 5 ve 4032x3024 çözünürlüğünde fotoğraflar çeken Samsung S8 marka telefonlarda edilmektedir. Aynı hesaplama ile en az parça sayısı 15 adet ile 2322x4128 çözünürlüğünde fotoğraflar çeken Samsung J7 Pro marka telefonda elde edilmektedir.

Çizelge 4.2 : Kamera imzası oluşturma işlemi ortalama bellek kullanımları.

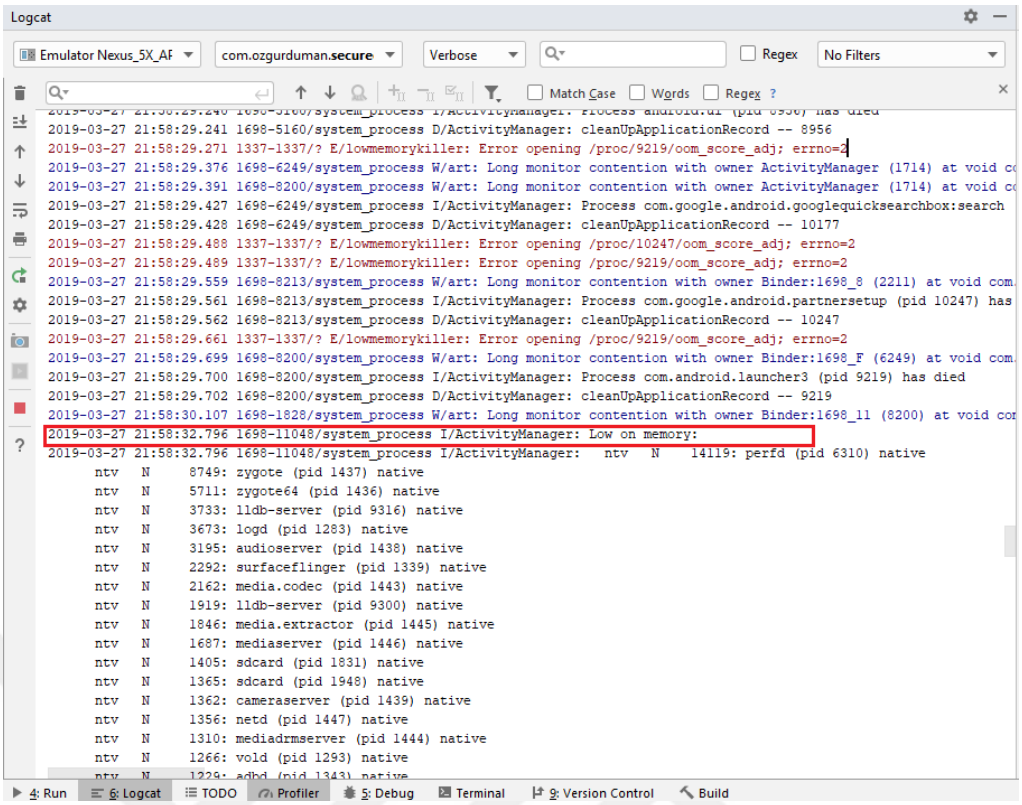
| Cihaz | Çözünürlük | Ortalama Bellek Kullanımı |
|---|---|---|
| Xiomi MI 5 | 3456 x 4608 | 680 MB |
| Samsung Note 4 | 5312 x 2988 | 590 MB |
| Samsung S8 | 4032 x 3024 | 650 MB |
| Samsung Note 5 | 5312 x 2988 | 580 MB |
| Samsung J7 Pro | 2322 x 4128 | 480 MB |

Anonimleştirme işlemi sırasında kullanılan ortalama bellek tüketimleri Çizelge 4.3 de verilmektedir. Farklı çözünürlükteki fotoğrafların bulunduğu sonuçlar incelendiğinde elde edilen en yüksek ortalama bellek tüketimi 490 MB, en küçük değer 285 MB olarak gözlemlenmiştir. Anonimleştirme işlemi sırasında kamera imzasının telefon hafızasından belleğe yüklenmesi gerekmektedir. Anonimleştirme süresi boyunca kamera imzasının bellekte tutulması sebebiyle bu ortalama bellek tüketimine kameranın çektiği fotoğrafların çözünürlüğüne bağlı olarak ek bir yük katmaktadır.

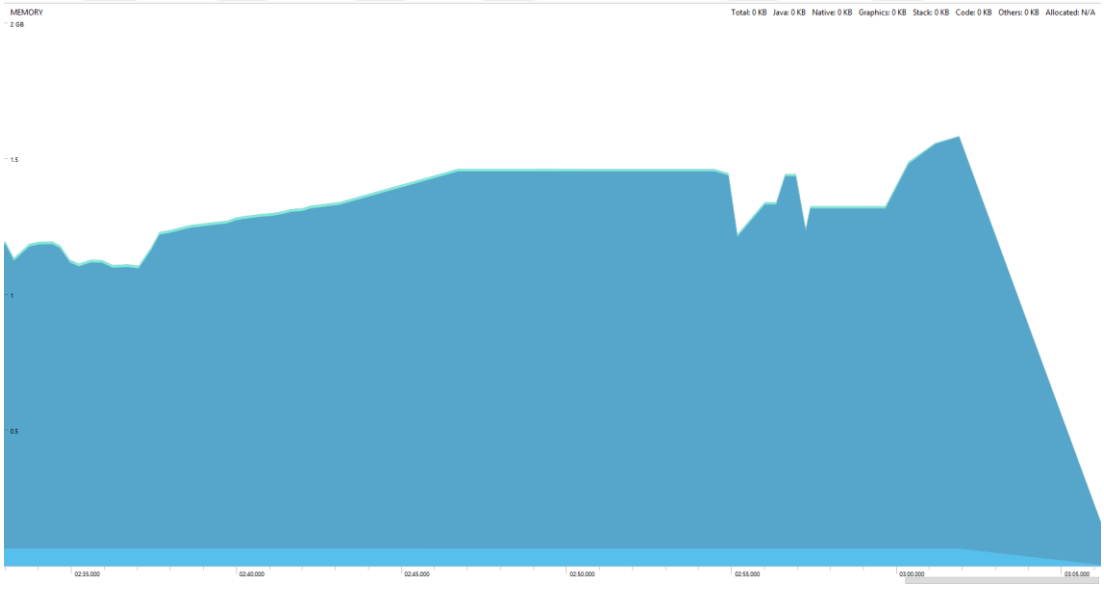
Çizelge 4.3 : Anonimleştirme işlemi ortalama bellek kullanımları.

| Cihaz | Çözünürlük | Ortalama Bellek Tüketimi |
|---|---|---|
| Xiomi MI 5 | 3456 x 4608 | 450 MB |
| Samsung Note 4 | 5312 x 2988 | 490 MB |
| Samsung S8 | 4032 x 3024 | 425 MB |
| Samsung Note 5 | 5312 x 2988 | 485 MB |
| Samsung J7 Pro | 2322 x 4128 | 285 MB |

Ayrıca önerilen yöntem kullanılmadan fotoğrafların tam çözünürlükleri ile uygulama çalıştırdığında, fazla bellek tüketimine dayanarak uygulamanın sistem tarafından kapatıldığı gözlemlenmiştir. Bu durumun sonucunda oluşan ve Android tarafından verilen mesaj Resim 4.9 de gösterilmektedir. Android Profiling Tool ile gözlemlenen bellek kullanımı Resim 4.10 de verilmektedir ve grafik üzerinden gözlemlenen verilere göre bellek kullanımı 1.5 GB'nin üzerinde çıkmaktadır ve sonrasında uygulama kapatılmaktadır.




Resim 4.9 : Tam çözünürlükteki fotoğraflar işlenirken alınan bellek dolu uyarısı.




Resim 4.10 : Tam çözünürlükte fotoğraflar ile elde edilen bellek tüketimi grafiği.

Uygulamanın anonimleştirme başarısının test edilmesi için anonimleştirme başarısı oranı formülü [6] kullanılmıştır. Formül (5.2) ile verilen fonksiyon ile kamera imzası $K_I$, ile listedeki anonimleştirilen i inci fotoğraf $T_i$'nin eşleştirilmesi sonucu ortaya çıkan PCE değeri minimumum PCE değerinden küçük ise 1, değilse 0 sonucu

döndürülmektedir. Anonimleştirme Başarısı Oranı (ABO) Formül (5.3) ile hesaplanmaktadır. Formül (5.3) de kullanılan $T$ değeri çekilen toplam fotoğraf sayısını göstermektedir.

$$F(T_{i,}\epsilon_{PCE}) = \begin{cases} 1 & eğer \quad PCE(T_i, K_I) < \epsilon_{PCE} \\ 0 & aksi\ halde \end{cases} \tag{5.2}$$

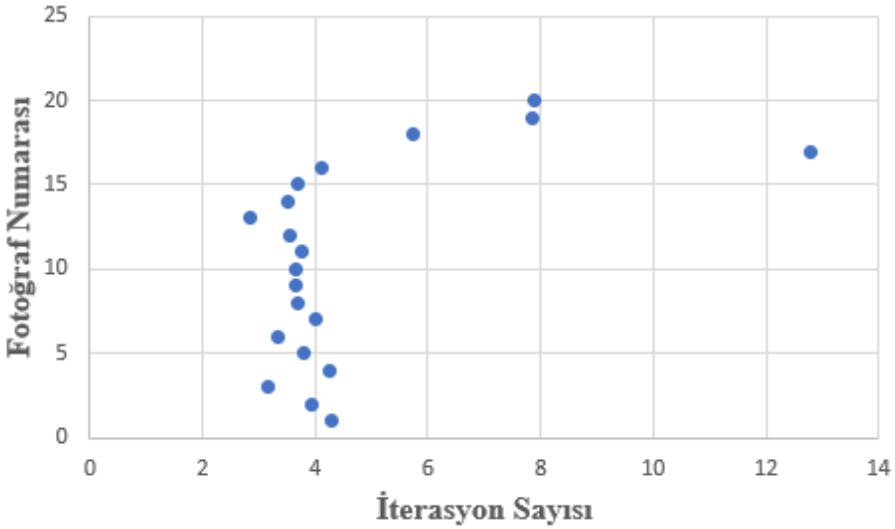
$$ABO = \frac{100}{T} \sum_{i=1}^{T} F(T_{i,}\epsilon_{PCE}) \tag{5.3}$$

Anonimleştirme işlemi gerçekleştirilen fotoğraflardan her bir parça için anonimleştirme faktörü ve anonimleştirme sonucunda elde edilen PCE değerleri toplanmıştır. Sonuçlara göre elde edilen ortalama PCE değeri ve ortalama anonimleştirme faktörü Çizelge 4.4 de gösterilmektedir. Çizelgenin oluşturulmasında kullanılan 20 tane fotoğrafın her bir parçasından elde edilen tüm veriler Çizelge EK 1.1 de verilmiştir.

Çizelge 4.4 : Anonimleştirme işleminde elde edilen değerler.

| Açıklama | Değer |
|---|---|
| Ortalama Anonimleştirme Faktörü | 4.68 |
| Ortalama PCE Değeri | 1.1732 |

Sonuçlara göre her bir parçanın anonimleştirilmesi için kullanılan ortalama anonimleştirme faktörü 4,68 olarak gözlemlenmiştir. Her bir parçanın anonimleştirilmesi için ortalama iterasyon sayısı 4,68 ve elde edilen ortalama PCE değeri 1,1732 olarak gözlemlenmiştir. Gerçekleştirilen anonimleştirme işlemlerinde elde edilen fotoğraf numarası ve iterasyon grafiği Şekil 4.2 de gösterilmektedir. Grafiğe göre elde edilen iterasyon sayıları 3 ile 5 arasında kalmaktadır. Her bir parçanın anonimleştirilmesiyle ve sonrasında birleştirilmesiyle oluşturulan tam boyutlu fotoğrafların anonim başarısının test edilebilmesi için öncelikle aynı kameradan çekilen ve anonimleştirme işlemi için oluşturulan kamera imzasında kullanılmayan 100 adet fotoğraf ile bir kamera imzası oluşturulmuştur. Bu kamera imzası ile aynı fotoğrafların orijinal halleri ve anonimleştirilmiş halleri bu kamera imzası ile eşleştirilerek Çizelge 4.5 ile verilen sonuçlar elde edilmiştir.




Şekil 4.2 : Fotoğraf numarası ve iterasyon grafiği.

Çizelge 4.5 de verilen son kolon Formül (5.2) kullanılarak hesaplanmaktadır ve fotoğrafların 100 adet fotoğraf kullanılarak oluşan kamera imzasına karşı elde edilen anonimleştirme başarısını belirtmektedir.

Çizelge 4.5 : Kaynak kamera tespiti elde edilen PCE değerleri.

| Resim Numarası | PCE Orijinal | PCE Anonim | $F(T_i, \epsilon_{PCE})$ |
|---|---|---|---|
| 1 | 18015.3312 | -6.7300 | 1 |
| 2 | 10989.9426 | -0.5307 | 1 |
| 3 | 14650.2385 | 15.4926 | 1 |
| 4 | 18337.7203 | -5.6575 | 1 |
| 5 | 527.8670 | 5.5611 | 1 |
| 6 | 12488.8922 | -4.2878 | 1 |
| 7 | 13116.4034 | -26.2545 | 1 |
| 8 | 6939.2302 | 17.2456 | 1 |
| 9 | 11393.2204 | 8.4924 | 1 |
| 10 | 20630.7114 | -19.8991 | 1 |
| 11 | 14010.3535 | 25.8898 | 1 |
| 12 | 7214.5747 | 0.0009 | 1 |
| 13 | 9366.9721 | 12.6928 | 1 |
| 14 | 23362.8541 | -336.7857 | 1 |
| 15 | 8514.5246 | 18.9298 | 1 |
| 16 | 12109.9578 | 16.4223 | 1 |
| 17 | 2563.1618 | 18.2552 | 1 |
| 18 | 8050.3612 | 7.7745 | 1 |
| 19 | 24621.7915 | -195.7340 | 1 |
| 20 | 10851.1819 | -27.2870 | 1 |

Anonimleştirme başarısı oranı, Çizelge 4.5 ile verilen sonuçların kullanılması ile Formül (5.3) ile hesaplanmıştır. Elde edilen sonuçlar Çizelge 4.6 ile verilmektedir.

Çizelge 4.6 : Anonimleştirme sonuçları.

| Açıklama | Değer |
|---|---|
| ABO | %100 |

Sonuçlar incelendiğinde elde edilen verilere göre kaynak kameradan toplanan tüm fotoğraflar, 100 adet fotoğraftan oluşturulan kamera imzasına karşı %100 başarı oranı ile anonimleştirilmiştir. Anonimleştirme işlemi için kullanılan bir fotoğrafın orijinal hali Resim 4.11 de anonimleştirme işlemi sonrasındaki hali ise Resim 4.12 de gösterilmektedir. Fotoğraflar incelendiğinde iki fotoğraf arasında gözle görülebilen bir fark gözlemlenmemektedir.

Resim 4.11 : Anonimleştirme işlemi uygulanmamış orjinal fotoğraf.

Resim 4.12 : Anonimleştirme işlemi sonrası elde edilen fotoğraf.

# 5. SONUÇ VE ÖNERİLER

Kaynak kamera imzası tespit yöntemleri, birçok adli vaka için delil niteliği taşıyan fotoğrafların gerçekten ilgili kameradan çekilip çekilmediğinin tespiti için kullanılabilmektedir [5]. Ayrıca bu yöntemin dayandığı PRNU tabanlı gürültüler, fotoğraflardan çıkartılarak başka fotoğraflara kopyalanabildiği saldırılar önceki çalışmalarda işlenmiştir [7]. Günümüzde akıllı telefonlardan çekilen sayısız fotoğrafın internete sürekli olarak yüklenmesi, bu tarz saldırılar ve illegal olarak kaynak kamera tespiti yapılabilmesi için bir kaynak oluşturmaktadır. Bunların önüne geçilebilmesi için fotoğrafın çekildiği kaynakta bulunan bir uygulama ile bu fotoğrafların anonimleştirilmesi gerekmektedir. Anonimleştirme işleminde önerilen yöntemlerin kullanılabilmesi için bir uygulama olamaması ve kısıtlı sistem kaynaklarına sahip telefonlarda bu işlemlerin çalıştırılması mümkün olmadığı için bu yöntemler kullanıcılara teorik olarak sunulmaktadır. Bu bilgilere dayanarak, bu çalışmada anonimleştirme yöntemlerinin sistem kaynakları kısıtlı akıllı telefonlar üzerinde çalıştırılabilmesine olanak sağlayan bir yöntem önerilmektedir ve bu yöntem kullanılarak Android telefonlarda çalışabilen güvenli kamera uygulaması geliştirilmiştir. Yapılan testler sonucunda, önerilen parçalı fotoğraf anonimleştirilmesi yöntemi ile geliştirilen uygulamanın farklı model akıllı telefonlarda sistem kaynaklarını kısıtlı şekilde kullanarak sorunsuz çalışabildiği gözlemlenmiştir. Ayrıca anonimleştirme yöntemlerinin tam boyuttaki fotoğraflar ile uygulandığında kamera uygulamasının telefon üzerinde çalışamadığı ve fazla kaynak tüketimini engellemek için Android sistemi tarafından kapatıldığı gözlemlenmiştir. Sonuçlarda elde edilen verilere göre parçalı fotoğraf anonimleştirme yöntemi ile geliştirilen güvenli kamera uygulaması 100 adet fotoğraftan oluşturulmuş bir kaynak kamera imzasına karşılık %100 oranda anonim fotoğraflar elde etmektedir. Bu çalışmada ek olarak HDR fotoğrafların, kaynak kamera imzası ile eşleştirilebilmesi için bir yöntem önerilmektedir. HDR fotoğrafların çekimi sırasında fotoğraf hizalama işlemleri uygulandığı için fotoğraf içerisindeki PRNU gürültü desenleri değişebilmektedir. Bu durumda kullanılan kaynak kamera analiz yöntemleri ile kamera imzası aynı

kameradan çekilen HDR fotoğraflar ile eşleştirildiğinde düşük eşleşme sonuçları elde edilmektedir. Günümüz akıllı telefonları ve kameralarının çoğunda HDR özelliği bulunması sebebiyle önerilen yöntem ile daha iyi kaynak kamera analizi sonuçları elde edilebilmektedir. Son olarak bu çalışmanın devamında, geliştirilen güvenli kamera uygulamasının ara yüzlerinin daha da geliştirilerek Android Uygulama Marketi üzerinden kullanıcılara sunulması hedeflenmektedir.

### 5.1 Kısıtlar

Güvenli kamera uygulamasında kullanılan parçalı anonimleştirme yöntemi, tek bir fotoğrafın anonimleştirilmesinden farklı olarak fotoğraftan elde edilen bir çok parçanın ayrı ayrı anonimleştirilmesini gerektirmektedir. Bu durum kaynak kamera imzası oluşturma ve fotoğraf anonimleştirme tekniklerinin kısıtlı sistem gücüne sahip telefonlarda çalışmasına olanak sağlamaktadır. Ancak doğal olarak, bu işlem tam bir fotoğrafın anonimleştirilmesinden daha uzun zaman almaktadır. Her iki yöntemde de anlık olarak bir anonimleştirme sağlanması mümkün olmadığı için parçalı anonimleştirme yönteminde işlemin tamamlanma süresinin daha uzun olması işlemler arka planda çalıştırıldığı ve kullanıcının telefon üzerinde yapacağı diğer işlemleri engellemediği sürece kullanım kolaylığı açısından bir sorun yaratmayacağı düşünülmektedir.

HDR fotoğraflarda kaynak kamera tespiti için önerilen yöntemin kısıtları olarak, tam boyutlu fotoğraftan alınan PRNU gürültüsü için kaynak kamera imzası üzerinde arama yapılması gerekmektedir. Dolayısıyla, her bir parça için kamera imzası parçaları ile korelasyon tekniklerinin çalıştırılmasını gerektirmektedir. Tüm parçalar için arama işleminin tamamlanması zamansal olarak uzun bir süre almaktadır. Sürenin kısıtlanması için fotoğrafın ilk çeyreğinde bir eşleştirme yapılamaması durumunda algoritmanın sonlandırılması, HDR fotoğrafın kendisinin çekildiği kaynak kameranın imzası ile eşleştirilememesine yol açabilmektedir.

## KAYNAKLAR


[1] **Dirik, A. E., Sencar, H. T., Memon, N.** (2008). Digital Single Lens Reflex Camera Identification From Traces of Sensor Dust. *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 539–552.

[2] **Bayram, S., Sencar, H. T., Memon, N., Avcibas, I.** (2005). Source camera identification based on CFA interpolation. *Proc. Of the IEEE International Conference on Image Processing (ICIP),* Genova, Italy, September 14.

[3] **Kharrazi, M., Sencar, H. T., Memon, N.** (2004). Blind Source Camera Identification, *IEEE International Conference on Image Processing*, Singapore, October 24-27.

[4] **Geradts, Z., Bijhold, J., Kieft, M., Kurosawa, K., Kuroki, K., and Saitoh, N.** (2001). Methods for Identification of Images Acquired with Digital Cameras, *Proc. Of SPIE, Enabling Technologies for Law Enforcement and Security*, vol. 4232, pp. 505–512.

[5] **Lukáš, J., Fridrich, J., Goljan, M.** (2006). Digital Camera Identification from Sensor Pattern Noise, *IEEE Transactions on Information Security and Forensics*, vol. 1, no. 2, pp. 205–214.

[6] **Chen, M., Fridrich, J., Goljan, M., Lukas, J.** (2008). Determining Image Origin and Integrity Using Sensor Noise, *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90.

[7] **Steinebach, M., Liu, H., Fan, P., Katzenbeisser, S.** (2010). Cell phone camera ballistics: attacks and countermeasures, *Proc. SPIE: Multimedia on Mobile Devices*, vol. 7542, pp. 0B-0C.

[8] **Dirik, A. E., Karaküçük, A.** (2014). Forensic use of photo response non-uniformity of imaging sensors and a counter method, *Optics Express*, vol. 22, no. 1, p. 470.

[9] **Karaküçük, A., Dirik, A. E.** (2015). Adaptive photo-response non-uniformity noise removal against image source attribution, *Digital Investigation*, vol. 12, pp. 66–76.

[10] **Blythe, P. Fridrich, J.** (2004). Secure Digital Camera, *Digital Forensic Research Workshop*, pp. 11–13.

[11] **Lyu, S., Farid, H**. (2002). Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines, *Information Hiding*, pp. 340–354.

[12] **Khanna, N., Mikkilineni, A. K., Chiu, G. T. C., Allebach, J. P., Delp, E. J.** (2007). Forensic classification of imaging sensor types, *Security, Steganography, and Watermarking of Multimedia Contents IX*.

[13] **Kurosawa, K., Kuroki, K., Saitoh, N.** (1999). CCD fingerprint method-identification of a video camera from videotaped images, *Proceedings 1999 International Conference on Image Processing*, vol. 3, pp. 537-540.

[14] **Popescu, A. C., Farid, H**. (2004). Statistical Tools for Digital Forensics, *Information Hiding*, pp. 128–147.

[15] **Swaminathan, A., Min Wu, Liu, K. J. R**. (2007). Nonintrusive component forensics of visual sensors using output images, *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–106.

[16] **Popescu, A. C., Farid, H.** (2005). Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767.

[17] **Popescu, A. C., Farid, H.** (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959.

[18] **Farid, H.** (2006). Exposing digital forgeries in scientific images, *Proceeding of the 8th workshop on Multimedia and security - MM&Sec '06*, pp. 29-36.

[19] **Popescu, A.C., Farid, H.** (2004). Exposing Digital Forgeries by Detecting Duplicated Image Regions, *Technical Report*, TR2004-515. Dartmouth College, Computer Science.

[20] **Gou, H., Swaminathan, A., Wu, M.** (2007). Robust scanner identification based on noise features, *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, pp. 65050S.

[21] **Goljan, M., Fridrich, J.** (2008). Camera identification from cropped and scaled images, *SPIE Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X*, pp. 0E:1 – 0E:13.

[22] **Goljan, M., Fridrich, J., Lukáš, J.** (2008). Camera identification from printed images, *Proc. Of SPIE-IS&T Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, pp. 68190I.

[23] **Goljan, M., Fridrich, J., Filler, T.** (2009). Large scale test of sensor fingerprint camera identification, *Media Forensics and Security. International Society for Optics and Photonics*, vol. 7254, pp. 72540I.

[24] **Amerini, I., Caldelli, R., Cappellini, V., Picchioni, F., Piva, A.** (2009). Analysis of denoising filters for photo-response non-uniformity noise extraction in source camera identification, *Proceedings of the 16th international conference on Digital Signal Processing*, pp 511–517.

[25] **Chen, M., Fridrich, J., Goljan, M.** (2007). Digital imaging sensor identification (further study). *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX*.

[26] **Goljan, M.** (2009). Digital Camera Identification from Images – Estimating False Acceptance Probability, *Digital Watermarking*, Springer Berlin Heidelberg, pp. 454–468.

[27] **Fridrich, J.** *Sensor defects in digital image forensic*, Digital Image Forensics, chap. 5, pp. 179–219, New York, Springer, (2012).

[28] **Goljan, M., Fridrich, J., Chen, M.** (2010). Sensor noise camera identification: countering counter-forensics, *Proc. SPIE 7541, Media Forensics and Security II*, pp. 75410S1 – 75410S12.

[29] **Goljan, M., Fridrich, J., Chen, M.** (2011). Defending against fingerprint-copy attack in sensor-based camera identification, *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 227–236.

[30] **Gloe, T., Kirchner, M., Winkler, A., Bohme, R.** (2007). Can we trust digital image forensics?, *Proc. ACM 15th International Conference on Multimedia*, New York, USA, Sep. 2007. p. 78e86.

[31] **Goljan, M., Fridrich, J., Filler, T.** (2010). Managing a large database of camera fingerprints, *SPIE Conference on Media Forensics and Security*.

[32] **Nagaraja, S., Schaffer, P., Aouada, D.** (2011). Who clicks there: Anonymising the photographer in a camera saturated society, *Proc. 10th Annu. ACM Workshop Privacy Electron. Soc.*, pp. 13-22.

[33] **Avidan, S., Shamir, A.** (2007). Seam carving for content-aware image resizing, *ACM Transactions on graphics*, vol. 26, no. 3.

[34] **Bayram, S., Sencar, H. T., Memon, N. D.** (2013). Seam-carving based anonymization against image & video source attribution. *IEEE 15th International Workshop, Multimedia Signal Processing (MMSP)*, p. 272e7.

[35] **Reinhard, E.** *HDR Image Capture*, High dynamic range imaging. 2nd ed, pp.148-151, Amsterdam, Morgan Kaufmann (2010).

[36] **Dubey, N.** (2017, July 18). What is the HDR mode? and how it works. Retrieved March 29, 2019, from https://viral360.in/hdr-mode-works/

[37] **Debevec, P. E., Malik, J.** (1997). Recovering high dynamic range radiance maps from photographs, *Proc. Of SIGGRAPH 97, Computer Graphics Proc.*, pp. 369–378.

[38] **Granados, M., Kim, K. I., Tompkin, J., Theobalt, C.** (2013). Automatic noise modeling for ghost-free HDR reconstruction, *ACM Transactions on Graphics*, vol. 32, no. 6, pp. 1–10.

[39] **Zimmer, H., Bruhn, A., Weickert, J.** (2011) Freehand HDR Imaging of Moving Scenes with Simultaneous Resolution Enhancement. *Computer Graphics Forum*, vol. 30, no. 2, pp. 405–414.

[40] **Sen, P., Kalantari, N. K., Yaesoubi, M., Darabi, S., Goldman, D. B., Shechtman, E.** (2012). Robust patch-based hdr reconstruction of dynamic scenes. *ACM Transactions on Graphics*, vol. 31, no. 6, art. 203.

[41] **Tomaszewska, A., Mantiuk, R.** (2007). Image Registration for Multi-exposure High Dynamic Range Image Acquisition, *WSCG*. vol. 24, no. 4, pp. 49–56.

[42] **Goljan, M., Fridrich, J., Filler, T.** (2009). Large scale test of sensor fingerprint camera identification, *Media Forensics and Security.* I*nternational Society for Optics and Photonics*, vol. 7254, pp. 72540I.

## EKLER

EK 1: Anonimleştirme işlemi sonrasında fotoğraf parçalarından elde edilen değerler.

**EK 1**

Çizelge EK 1.1 : Fotoğrafların parçalarının ortalama değerleri.

| No | Anonimleştirme Faktörü | PCE Değeri |
|---|---|---|
| 1 | 4.30 | -1.0791 |
| 2 | 3.95 | 1.8434 |
| 3 | 3.15 | -6.0871 |
| 4 | 4.25 | 3.8852 |
| 5 | 3.80 | 3.0254 |
| 6 | 3.35 | 4.1397 |
| 7 | 4.00 | 2.0098 |
| 8 | 3.70 | -4.6315 |
| 9 | 3.65 | -0.2273 |
| 10 | 3.65 | -0.2318 |
| 11 | 3.75 | 1.5342 |
| 12 | 3.55 | -3.6733 |
| 13 | 2.85 | 3.1643 |
| 14 | 3.5 | 1.5784 |
| 15 | 3.7 | -1.3253 |
| 16 | 4.1 | 2.8760 |
| 17 | 12.8 | 7.0750 |
| 18 | 5.75 | -0.1278 |
| 19 | 7.85 | 5.4643 |
| 20 | 7.9 | 6.1735 |

# ÖZGEÇMİŞ


**Ad-Soyad** **:** Kemal Özgür DUMAN

**Uyruğu** **:** T.C.

**Doğum Tarihi ve Yeri** **:** 17.03.1992 Yenimahalle

**E-posta** **:** kemalozgurduman@gmail.com


**ÖĞRENİM DURUMU:**

- **Lisans** **:** 2015, Çankaya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği
- **Yükseklisans** **:** 2019, TOBB Ekonomi ve Teknoloji Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı

**MESLEKİ DENEYİM VE ÖDÜLLER:**

| **Yıl** | **Yer** | **Görev** |
|---|---|---|
| 2016 – Halen | Türkiye Cumhuriyet Merkez Bankası | Bilgisayar Mühendisi |
| 2015 – 2016 | Kale Yazılım A.Ş. | Bilgisayar Mühendisi |

**YABANCI DİL:** İngilizce

## TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER

- **Duman, K. Ö.,** Sencar, H. T., 2019. Android Secure Camera Application, 2nd International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES2019), Apr. 26-28, Alanya, Turkey.