



MÜHENDİSLİK FAKÜLTESİ

SİBER GÜVENLİK YÜKSEK LİSANS BÖLÜMÜ

TEZSİZ YÜKSEK LİSANS DÖNEM PROJESİ

FOTOĞRAF ÜZERİNDE YAPILAN
MANİPÜLASYONUN İNCELENEREK TESPİTİNE
YÖNELİK BİR ARAŞTIRMA

AHMET YESEVİ
ÜNİVERSİTESİ

HAZIRLAYAN
Hünkar AKDEMİR

ETİK İLKELERE UYGUNLUK BEYANI

Dönem proje yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.



Hünkar AKDEMİR

FOTOĞRAF ÜZERİNDE YAPILAN MANİPÜLASYONUN İNCELENEREK TESPİTİNE YÖNELİK BİR ARAŞTIRMA

Hünkar AKDEMİR

AHMET YESEVİ ÜNİVERSİTESİ
SİBER GÜVENLİK YÜKSEK LİSANS BÖLÜMÜ

2024

ÖZET

Günümüzde dijital kolayca işlenebilir olması, savcılıkta soruşturma aşamasında, mahkemelerde ise yargılama sırasında güvenilirlik ve görüntünün gerçek olup olmadığı sorunlarını ortaya çıkarmaktadır. Görüntüler üzerinde yapılan manipülasyonların tespiti, adli olayların aydınlatılmasında önemli bir yer almaktadır. Bu sebeple adli süreçlerde, bir görüntünün gerçek olup olmadığının veya manipüle edilip edilmediğinin tespit edilmesi, adli makamların dava ya da soruşturma dosyalarında vereceği kararları doğrudan etkileyebilmektedir. Fotoğraf ve görüntüler üzerinde yapılan manipülasyonlar, genellikle fotoğrafın üzerine nesne eklenerek, mesajlaşma uygulamaları üzerinden gönderilen alınan mesajlar üzerinde düzenleme yapılarak olmayan mesajın gerçek gibi gösterilmesi şeklinde olabilmektedir. Çalışma kapsamında, klonlama ve yapay zeka aracı ile nesne ekleme işlemi gerçekleştirilerek manipüle edilmiş manzara görüntüleri, Fakewhats.com web sayfası üzerinde whatsapp isimli programdan alınmış gibi gösteren sahte bir ekran görüntüsü ve cep telefonundan alınan mesajlaşmaya ait ekran görüntüsü üzerinde yapılan kelime taşıma, değiştirme işlemleri uygulanarak manipüle edilmiş görüntü üzerinde manipülasyonunun tespitine yönelik farklı teknikler incelenmiştir. Bunlar hata düzeyi analizi (ELA), Histogram analizi ve meta veri analizi (EXIF) yöntemlerini içermektedir. Orijinal görüntüler ile üzerinde manipülasyon işlemi gerçekleştirilen görüntüler üzerinde ELA analizi ve EXIF verileri kontrolü gerçekleştirildiğinde, manipülasyon işleminin görüntü üzerinde nerede veya nasıl yapıldığına dair belirgin bir sonuç sağladığı, Histogram analizinin ise yapılan manipülasyonun fotoğraf ya da görüntü üzerinde doğal bir sonuç elde etmesi sebebiyle yetersiz kaldığı sonucuna ulaşılmıştır. Araştırma sonuçlarına göre, ELA analizi ile EXIF verilerine ait incelemelerinin birlikte kullanılmasının, manipülasyonun tespitinde yüksek bir doğruluk sağladığı görülmüştür. Çalışmada kullanılan yöntemlerin, farklı yöntemler ile genişletilmesi ile fotoğraf ya da görüntüler üzerinde manipülasyon yapıp yapılmadığını tespit edeceği öngörülmektedir. Bu çalışmanın, adli süreçlerde delil niteliği taşıyan fotoğraf ve görüntüler üzerinde yapılan manipülasyonların tespitine katkı sağlaması ve ilgili alanlardaki adli bilişim uzmanları için faydalı bir kaynak oluşturması beklenmektedir.

Anahtar Kelimeler: Fotoğraf, Görüntü, Manipülasyon, Metadata Analizi, Hata Seviyesi Analizi, Histogram

Danışman: Prof. Dr. Mutlu Tahsin ÜSTÜNDAĞ

A RESEARCH TO EXAMINATE AND TEST THE MANIPULATION MADE ON PHOTOGRAPHS

Hünkar AKDEMİR

AHMET YESEVI UNIVERSITY

ENGINEERING FACULTY CYBER SECURITY MASTER'S DEPARTMENT

2024

ABSTRACT

The ease of processing images today raises issues of reliability and authenticity during the investigation stage in prosecution and the trial stage in courts. Detecting manipulations on images plays a significant role in clarifying judicial cases. Therefore, determining whether an image is authentic or manipulated directly affects the decisions made by judicial authorities in case or investigation files. Manipulations on photos and images are typically carried out by adding objects to the photo, editing messages received or sent through messaging applications to make non-existent messages appear real. In the scope of this study, various manipulations were applied, including the cloning and addition of objects using artificial intelligence to landscape images, a fake screenshot created using the FakeWhats.com website to appear as if it was taken from a program named WhatsApp, and screenshots of messaging on a mobile phone where words were moved or altered. Different techniques were then examined to detect manipulations in these manipulated images. These techniques included Error Level Analysis (ELA), Histogram Analysis, and Metadata Analysis (EXIF). When performing ELA analysis and checking EXIF data on both original and manipulated images, it was observed that the manipulation's location or method on the image could be clearly identified. However, Histogram Analysis was found to be inadequate because the manipulations often produced natural-looking results on the photo or image. Based on the research findings, combining ELA analysis and EXIF data examinations resulted in high accuracy in detecting manipulations. It is anticipated that expanding the methods used in this study with additional techniques will enhance the ability to detect manipulations on photos or images. This study is expected to contribute to the detection of manipulations on photos and images used as evidence in judicial processes and serve as a valuable resource for forensic experts in related fields.

Keywords: Photo, Image, Manipulation, Metadata Analysis, Error Level Analysis, Histogram

Advisor: Prof. Dr. Mutlu Tahsin ÜSTÜNDAĞ

İÇİNDEKİLER

ETİK İLKELERE UYGUNLUK BEYANI	ii
ÖZET.....	iii
ABSTRACT	iv
İÇİNDEKİLER	v
ŞEKİLLER LİSTESİ.....	vii
TABLolar LİSTESİ	viii
SİMGELER VE KISALTMALAR.....	ix
BÖLÜM I GİRİŞ	1
1.1. Problem	1
1.2. Araştırmanın Amacı.....	2
1.3. Araştırmanın Önemi	3
1.4. Sayıtlar	3
1.5. Sınırlılıklar	4
1.6. Tanımlar	4
BÖLÜM II KAVRAMSAL ÇERÇEVE	5
2.1. Görüntülerde Kullanılan Kavramlar	5
2.1.1. Dijital Görüntü	5
2.1.2. Genişletilmiş Dosya Bilgisi (Exif – Extended File Information).....	5
2.1.3. Görüntü üzerinde Histogram.....	6
2.1.4. ELA Analizi – Error Level Analysis	7
2.2. Görüntü Üzerinde Yapılan Manipülasyon ve Tespit Yöntemleri	8
2.2.1. Aktif Sahtecilik	8
2.2.2. Pasif Sahtecilik.....	8
2.3. Görüntü Üzerinde Yapılan Manipülasyonlar.....	9
2.3.1. Orijinal Görüntü ve Manipüle Edilmiş Görüntü Oluşturulması	9
2.3.2. Sahte WhatsApp Ekran Görüntüsü Oluşturulması	10
2.3.3. Orijinal Mesajlaşmaya ait Ekran Görüntüsü ve Manipüle Edilmiş Mesajlaşma Görüntülerinin oluşturulması.....	12
2.4. Görüntü Üzerinde Yapılan Manipülasyonların Tespiti	13
2.4.1. Görüntüler üzerinde ELA Analizi	13
2.4.2. Görüntüler üzerinde Histogram Analizi	16
2.4.3. Görüntüler üzerinde Exif Verileri Analizi	18
BÖLÜM III YÖNTEM	23

3.1. Araştırmanın Modeli	23
3.2. Evren ve Örneklem.....	23
3.3. Veri Toplama Araçları.....	23
3.4. Verilerin Toplanması.....	24
3.5. Verilerin Analizi.....	24
BÖLÜM IV	26
BULGULAR VE YORUM	26
4.1. Görüntü Üzerinde Yapılan Manipülasyonların ELA Analizi Üzerinde Etkisi	26
4.2. Görüntü Üzerinde Yapılan Manipülasyonların Histogram Verileri Üzerinde Etkisi	26
4.3. Görüntü Üzerinde Yapılan Manipülasyonların Exif Verileri Üzerinde Etkisi	26
BÖLÜM V	28
SONUÇ.....	28
5.1. Sonuç	28
KAYNAKÇA.....	29



ŞEKİLLER LİSTESİ

Şekil 2. 1 Exif verileri kontrolüne ait sonuçlar.....	6
Şekil 2. 2 Histogram örnekleri.....	7
Şekil 2. 3 Manzara görüntüsü ve manipüle edilmiş manzara görüntüleri	9
Şekil 2. 4 Fakewhats.com web sayfası üzerinden oluşturulmuş görüntü.....	11
Şekil 2. 5 Kısa mesajlaşmaya ait görüntü ve manipüle edilmiş mesajlaşma görüntüsü	12
Şekil 2. 6 Manzara görüntüsü ELA analizi.....	13
Şekil 2. 7 Klonlama işlemine maruz kalmış görüntüye ait ELA analizi	14
Şekil 2. 8 Yapay zeka işlemi kullanılarak manipüle edilmiş görüntüye ait ELA analizi....	14
Şekil 2. 9 Mesajlaşma görüntüleri üzerinde ELA analizi.....	15
Şekil 2. 10 Manzara görüntüsü ve manipüle edilen görüntüler üzerinde histogram analizi	16
Şekil 2. 11 Mesajlaşma ve manipüle edilen mesajlaşmaya ait görüntü üzerinde histogram analizi	17
Şekil 2. 12 Manzara görüntüsüne ait EXIF verileri	18
Şekil 2. 13 Manzara görüntüsü üzerinde klonlama işlemi uygulanması sonucu EXIF verileri	19
Şekil 2. 14 Manzara görüntüsüne yapay zeka ile tekne eklenmesi sonucu EXIF verileri ..	20
Şekil 2. 15 Web sayfası üzerinden oluşturulan mesajlaşma ekran görüntüsü üzerinde EXIF verileri	20
Şekil 2. 16 Mesajlaşmaya Ait Orijinal Görüntü Üzerinde Exif Verileri.....	21
Şekil 2. 17 Mesajlaşma ekran görüntüsü üzerinde manipülasyon yapılması sonrası EXIF verileri	22

TABLÖLAR LİSTESİ

Tablo 1 Manzara görüntüsü ve manipüle edilen görüntüler üzerinde histogram analizi verileri	17
Tablo 2 Mesajlaşma görüntüsü ve manipüle edilen mesajlaşma görüntüsü üzerinde histogram analizi verileri.....	18
Tablo 3 Orijinal/manipüle edilmiş görüntülerde ELA, histogram ve EXIF verileri kontrol tablosu	24



SİMGELER VE KISALTMALAR

Kisaltmalar	Açıklamalar
-------------	-------------

AI	: Artificial intelligence – yapay zeka
----	--

ELA	: Error level analysis – hata seviyesi analizi
-----	--

Exif	: Extended file information - genişletilmiş dosya bilgisi
------	---

JPEG	: Joint photographic experts group
------	------------------------------------

PNG	: Portable network graphic – taşınabilir ağ grafiği
-----	---

RGB	: Red green blue - kırmızı yeşil mavi
-----	---------------------------------------

SMS	: Short message service – kısa mesaj servisi
-----	--



BÖLÜM I

GİRİŞ

1.1. Problem

Günümüzde görüntülerin, dijital görüntü düzenleme yazılımları ile kolay ve hızlı bir şekilde değiştirilmesine imkan tanımaktadır. Birtakım fotoğraf düzenleme yazılımları ile kişiler, görüntüler üzerinde kesme, taşıma, yeniden örnekleme, nesne ekleme ya da çıkarma gibi işlemler gerçekleştirebilmektedir. “Manipülasyon, Fransızca kökenli bir kelime olup, bilgilerin seçilmesi, eklenmesi veya çıkarılması yoluyla elde edilen yeni görüntünün sunumu ile gerçekleşir.” (Demirel, 2015). Belirtilen düzenleme işlemlerinin dışında yapay zeka destekli araçlar ile gerçekçi manipülasyonlar yapabilmektedir. Bu durumu “gelişmiş harika görüntü işleme araçları vardır; herkes gerçek bir resmi kolayca değiştirebilir ve sahte bir görüntü oluşturabilir” olarak belirtmiştir (Al-Husseinawi, Jubori, Salim, ve Mohammed, 2015). Yami (2009) çalışmasında “bilgisayar teknolojisinin kullanımı ile dijital fotoğrafçılığın ortaya çıkışı, ve mevcut yazılım programları ile, fotoğraflar üzerinde oynama yapılabilir olması bizi geçtiğimiz yüzyıldan itibaren yepyeni bir sorunla karşı karşıya bırakmıştır” olarak belirtmiştir.

Görüntü üzerinde yapılan manipülasyonlar, özellikle sosyal medya platformları, haber siteleri, adli soruşturma dosyaları ve mahkeme dosyalarında görsellerin doğruluğu ve güvenilirliği konusunda gerçekliğin sorgulanmasına yol açmaktadır. Bu durumu “özellikle yasal fotografik kanıtlar söz konusu olduğunda görsellerin gerçekliğini kesin olarak kabul edilmemektedir. Görüntü adli bilişimi, bu bağlamda, daha önce yapılan manipülasyonların izlerini ve türlerini belirlemek ve dijital bir görüntünün kaynağını ve olası özgünlüğünü tespit etmekle ilgilenir.” olarak belirtmişlerdir (Bayram, Avcıbaş, Sankur ve Memon, 2006). Ayrıca, Samet ve Atılgan (2018) çalışmasında “Mahkemelere sunulan görüntüler üzerinde manipülasyon yapıldığını gösterir bulguların ortaya çıkması ve bu durumun yaygınlaşması, mağdurun mağduriyetini giderecek bulguların delil olarak kabul edilmesini sağlayacak tespitlerin yapılmasını mecbur kılmıştır.” olarak önermişlerdir. Bundan dolayı üzerinde oynama-manipülasyon yapılarak gerçekliği değiştirilmiş görüntülerin yayılması, doğru olmayan bilgilerin yayılmasını arttırarak güvenilir bilgiye erişimi engellemektedir.

Literatür üzerinde yapılan araştırmalarda, Samet ve Atılgan’a (2018) göre, görsel değerlendirmelerin yapılmasını, görüntünün exif bilgilerine başvurulması gerektiğini ve sonuçların hep birlikte değerlendirilmesi gerektiğini, Ahmed, Yoon, Sharma, Singh ve Islam

(2023) ise çalışmalarında, gelecekte manipülasyon tespiti üzerine yapılacak araştırmalarda daha fazla işlem türünün dahil edilmesi gerektiği belirtmişlerdir.

Literatürde yapılan bu çalışmalar, dijital görüntü manipülasyonlarının tespiti alanında önemli ilerlemeler sağlamış olsa da, farklı manipülasyon türlerini tespit etmek için yöntemlerin, birbirinden bağımsız kullanıldığı görülmektedir. Manipülasyon tespitine yönelik mevcut yöntemlerin etkinliğini artırmak ve farklı yöntemlerin bir arada kullanılmasını sağlayacak yaklaşımlar geliştirmek, alan yazında hala çözüm bekleyen önemli bir problem olarak karşımıza çıkmaktadır.

1.2. Araştırmanın Amacı

Araştırmanın temel amacı, dijital manipülasyonların tespitine yönelik mevcut yöntemlerden olan ELA Analizi, Histogram Analizi ve Exif verileri etkinliğini analiz etmek ve sonuçlarını değerlendirmektir. Bu amaç doğrultusunda üç farklı senaryo incelenmiştir:

- Orijinal manzara görüntüleri üzerine klonlama ve yapay zeka ile nesne ekleme işlemleri uygulanmış yeni görüntüler
- Fakewhats.com platformu kullanılarak oluşturulan sahte WhatsApp mesajlarının bulunduğu ekran görüntüsü
- Cep telefonunda, kısa mesajlaşma servisi (SMS) üzerinden gönderilen ve alınan mesajların yer aldığı ekran görüntüleri üzerinde kopyala-yapıştır ve taşıma yapılarak oluşturulan ekran görüntüleri,

Araştırma esnasında, belirlenen senaryolar ile manipüle edilen görüntüler üzerinde aşağıda yer alan sorulara cevap aranmaktadır.

- Üzerinde klonlama yapılmış ve yapay zeka ile nesne ekleme işlemi gerçekleştirilerek manipüle edilmiş yeni manzara görüntüsü üzerinde ELA analizinin, histogram analizinin, EXIF verilerinin etkisi var mıdır ve analiz ile görüntü üzerinde yapılan manipülasyon tespit edilebilir mi?
- Fakewhats.com platformu kullanılarak oluşturulan sahte WhatsApp mesajlarının bulunduğu ekran görüntüsü üzerinde ELA analizinin, histogram analizinin, EXIF verilerinin etkisi var mıdır ve analiz ile görüntü üzerinde yapılan manipülasyon tespit edilebilir mi?
- Cep telefonunda, kısa mesajlaşma servisi (SMS) üzerinden gönderilen ve alınan mesajların yer aldığı manipüle edilmiş ekran görüntüleri üzerinde ELA analizinin,

histogram analizinin, EXIF verilerinin etkisi var mıdır ve analiz ile görüntü üzerinde yapılan manipölasyon tespit edilebilir mi?

1.3. Araştırmanın Önemi

Dijital manipölasyonların yaygınlaşması, sahte görüntülerin güvenlik ve adli bilişim alanlarında ciddi tehditlerin oluşturmalarına neden olmaktadır. Özellikle hukuki süreçlerde manipüle edilmiş görüntülerin kullanılması, sosyal medyada sahte içeriklerin viral hale gelmesi ve yanlış bilgilerin hızla yayılması gibi durumlar, manipölasyon tespitine duyulan ihtiyacı giderek artırmaktadır.

Fotoğraf üzerinde yapılan manipölasyonun incelenerek tespit edilmesi, adli bilişim alanında uzmanların, savcılık veya mahkemelerdeki dava dosyalarında görevlendirilen bilirkişilerin veya alanında araştırma yapacak kişilerin yararlanacağı bir kaynak olarak kullanılabilir. Ayrıca yapılan bu çalışmanın, fotoğraf ve görüntü üzerinde yapılan manipölasyon tespiti alanında yapılacak yeni araştırmalara rehberlik ederek katkıda bulunacaktır.

Bu çalışma, ELA Analizi, Histogram Analizi ve Exif verileri kontrolü gibi mevcut yöntemlerin bir arada kullanılmasının, farklı manipölasyon türlerini tespit etmede etkili olup olmadığını değerlendirmektedir. Uygulanan yöntemlerin bir arada kullanılması ile yöntemlerin geliştirilmesi ve genişletilmesine yönelik bilimsel bir zemin oluşturmaya katkı sağlamaktadır.

1.4. Sayıtlar

Araştırmada kullanılan ELA, Histogram Analizi ve Exif verileri incelemesi esnasında, görüntüler üzerinde yapılan manipölasyonları doğru tespit ettiği ve güvenilir sonuçlar verdiği varsayılmıştır. Görüntü manipölasyonları yapılması esnasında kullanılan yazılımlardan Adobe Photoshop yazılımının görüntü üzerinde kusursuza yakın işlem yaptığı ve Adobe FireFly yapay zeka aracının, gerçeğe yakın sonuçlar sunduğu kabul edilmiştir. Fakewhats.com platformu üzerinden oluşturulan sahte whatsapp mesajlarına ait sahte görüntünün gerçek görüntüye benzemesi sebebiyle araştırmaya dahil edilmiştir. Manipüle edilen görüntüler üzerinde yapılan araştırmada, analiz sürecini etkileyecek başka bir değişkenin bulunmadığı varsayılmıştır. Exif verileri analizinin, görüntü üzerinde yapılan

değişiklikler neticesinde verilerinin değişerek güvenilir bilgiler ortaya çıkardığı varsayılmıştır.

1.5. Sınırlılıklar

Araştırma esnasında sınırlı sayıda manipüle edilmiş görüntü kullanılmıştır. Daha fazla sayıda manipüle edilmiş görüntü üzerinde yapılacak çalışmanın, elde edilecek bulgu ve sonuçlar kısmında verilen bilgileri arttırabildiği gibi araştırma süresini arttırmaktadır. Çalışma esnasında kullanılan ELA, Histogram Analizi ve Exif verilerinin incelenmesi sadece belirli türde manipüle edilmiş görüntüler üzerindeki değişiklikler hakkında araştırmaya katkı sağlamaktadır. Fakewhats.com isimli web sayfası üzerinden oluşturulan sahte ekran görüntüsünün, Exif verileri üzerinde analiz için yeterli olmadığı değerlendirilmiştir. Adobe FireFly Yapay Zeka aracı kullanılarak manipüle edilmiş görüntüler ile belirli türde içerik oluşturulmuş ve görüntüye eklenmiştir.

1.6. Tanımlar

Piksel : Fotoğrafi oluşturan görüntünün en küçük birimidir.

RGB : Fotoğrafın renkli görüntüsünü sağlayan kırmızı, yeşil, mavi renklerdir.

Adli Bilişim : Dijital verilerin incelenerek hukuki ve güvenlik açısından delil sunma süreci.

Genişletilmiş dosya bilgisi (EXIF): Fotoğraflar üzerinde bulunan ve fotoğrafın çekim şartlarını, çekim özelliklerini saklayan verilerin, metadataların bulunduğu kısımdır.

BÖLÜM II

KAVRAMSAL ÇERÇEVE

2.1. Görüntülerde Kullanılan Kavramlar

2.1.1. Dijital Görüntü

Çok sayıda Pikselin birleşmesiyle oluşan görüntüye dijital görüntü denmektedir. Dijital görüntüler, orijinal belgelerden taranma, dijital fotoğraf makineleriyle veya dijital ortamlardan ekran kaydetme (screenshot) metoduyla kaydedilmektedir. Dijital ortamda bulunan Görüntülerin tamamında dosya adı, genişlik, yükseklik, boyut, bit derinliği, oluşturulma tarihi, dosya türü gibi bilgiler bulunmaktadır. Bu kısımda yer alan verilerin tamamı Exif Meta verilerinde yer almaktadır. Dijital görüntü üzerinde yazılımlar ile yapılan değişiklikler ile görüntüye ait özellikler değiştirilebilmektedir.

2.1.2. Genişletilmiş Dosya Bilgisi (Exif – Extended File Information)

Dijital görüntüler üzerinde yer alan özgün verilerin yanısıra Exif verileri daha kapsamlı bilgi sağlamaktadır. Exif verileri ile görüntüler üzerinde değişiklik ya da düzenleme olup olmadığını öğrenmek mümkündür. Exif verileri üzerinde yer alan bilgiler, ‘dosya adı, dosya boyutu, dosya tarihi, Flash Kullanımı, Çözünürlük, Pozlama süresi, Odak uzunluğu, GPS verileri, Lens Bilgileri’ şeklinde olabilmekte ve hatta fotoğraf üzerinde düzenleme yapılması halinde bu kısımda ‘Yazar adı ve değişiklik yapılan uygulamaya ait’ ek bilgiler yer almaktadır. (Alvarez, 2004)

Metadatalarda yer alan veriler, görüntü üzerinde inceleme yapacak olan uzman kişilere fayda sağlamaktadır. EXIF metadata verilerinde çok sayıda etiket türü olmasına rağmen, bu veriler üzerinde değişiklik yapılabilmektedir. (Ghazali, Khan ve Zakaria, 2020)

Amerikan yargı sisteminde mahkemesi görülen ‘Jhonny Depp ve Amber Heard’ davasında, Amber Heard tarafından sunulan görüntünün, orijinal görüntü olup olmadığına dair (şekil 2.1) yapılan tespitler neticesinde, görüntüye ait Exif verileri kontrol edilmiş ve görüntünün “Photos 3.0” programı ile düzenlendiği ortaya çıkarılmıştır. Görüntü üzerinde düzenleme yapıldığına mahkeme tarafından karar verilmiştir.

(<https://www.youtube.com/watch?v=eoQK1iAza9M>, 2022)

Şekil 2. 1

Exif verileri kontrolüne ait sonuçlar

EXIF IFD0 @ Absolute 0x00000026
Dir Length = 0x0009

[Make	] = "Apple"
[Model	] = "iPhone 6"
[Orientation	] = 1 = Row 0: top, Col 0: left
[XResolution	] = 72/1
[YResolution	] = 72/1
[ResolutionUnit	] = 1
[Software	] = "Photos 3.0"
[DateTime	] = "2015:12:16 11:44:00"
[ExifOffset	] = 0x00000000

Offset to Next IFD = 0x00000000

EXIF SubIFD @ Absolute 0x000000D8
Dir Length = 0x001F

[ExposureTime	] = 1/30 s
[FNumber	] = F2.2
[ExposureProgram	] = Normal program
[ISO Speed Ratings	] = 250
[ExifVersion	] = 02.21
[DateTimeOriginal	] = "2016:09:21 21:24:52"
[DateTimeDigitized	] = "2016:09:21 21:24:52"
[ComponentsConfiguration	] = [Y Cb Cr .]
[ShutterSpeedValue	] = 5845/1191
[ApertureValue	] = 7892/3469
[BrightnessValue	] = 3141/2051
[ExposureBiasValue	] = 0.00 eV
[MeteringMode	] = Pattern
[Flash	] = Flash did not fire
[FocalLength	] = 4 mm
[SubjectLocation	] = 833, 1071, 1076, 1077
[MakerNote	] = 8 0x029C
[SubSecTimeOriginal	] = "513"
[SubSecTimeDigitized	] = "513"
[FlashPixVersion	] = 01.00
[ExifImageWidth	] = 0x[00000990] / 2448
[ExifImageHeight	] = 0x[00000990] / 2448
[SensingMethod	] = One-chip color area sensor
[SceneType	] = A directly photographed image
[ExposureMode	] = Auto exposure

LAW & CRIME CHANNEL

FOLLOW LAW&CRIME'S SIDEBAR PODCAST FOR TRIAL RECAPS

LISTEN ON APPLE & SPOTIFY | LINKS IN THE DESCRIPTION

back camera 4.15mm f/2.2

2.1.3. Görüntü üzerinde Histogram

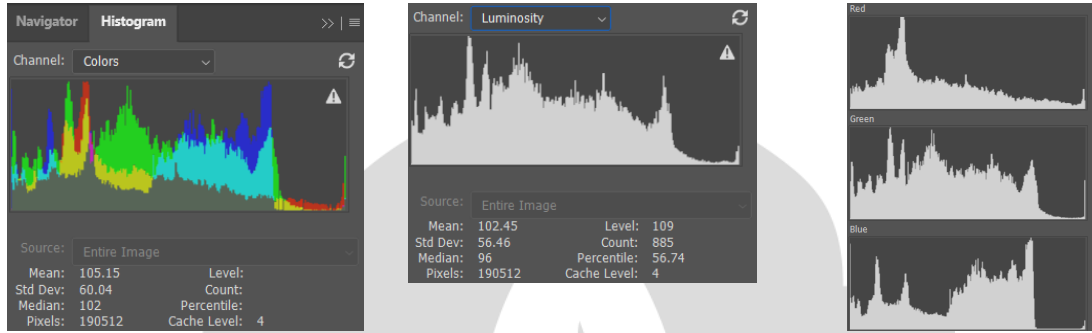
Histogram dijital görüntülerdeki piksellerin dağılımını gösteren önemli bir bilgi temsil yöntemidir. Gri seviyeli görüntülerde tek boyutlu dizi işlenirken, renkli görüntülerde üç boyutlu dizinin analizinin yapılması gereklidir. (Kılıçaslan, Tanyeri ve Demirci, 2018) Histogram, Görüntüde parlaklık ve renk dağılımını grafik halinde sunmaktadır.

Histogramlar, fotoğraf manipülasyonunun tespitinde bir görüntünün ton aralığındaki tutarsızlıklarının incelenebilmesi amacıyla faydalı grafiklerdir. Bir görüntü klonlandığında veya görüntünün başka bir bölümünden kopyalandığında histogram, kopyalanan ton değerlerinde ani bir artış gösterecektir. Fotoğraf üzerinde yapılan manipülasyonların

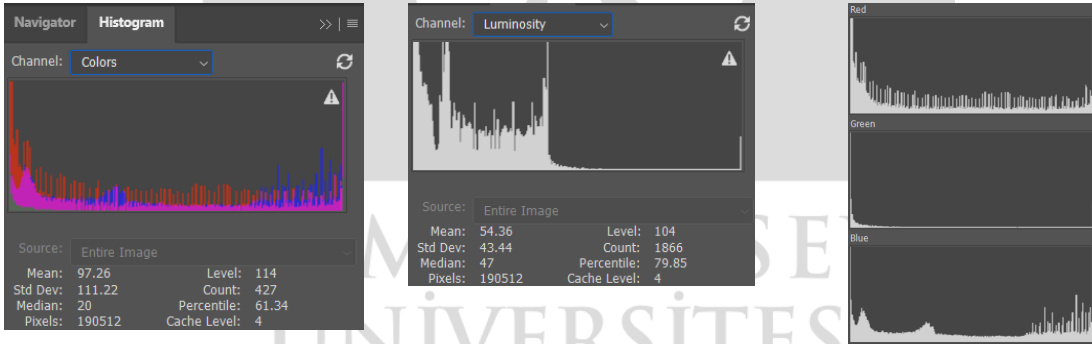
tespitinde Histogram büyük bir öneme sahip olmakta ve ortaya çıkan sonuçlar objektif kanıt olarak değerlendirilmektedir. Orijinal görüntüye ait histogram verileri ile üzerinde düzenleme yapılmış görüntülere ait histogram verileri Şekil 2.2 üzerinde verilmiştir. Yapılan inceleme neticesinde, üzerinde düzenleme yapılan görüntülere ait Histogram verilerinde, Renk Doygunluğunun ve Parlak alanlarına ait verilerin daha daraltılmış şekilde görüntülediği, RGB renk uzayına ait grafiklerde ise çizgilerin belirli aralıklarda ve dağınık yapıda bulundukları gözlemlenmiştir. Görüntüler üzerinde yapılan Kontrast Analizi, Fotoğraf Düzenleme ve Manipülasyonun tespiti için Histogram büyük önem taşımaktadır.

Şekil 2. 2

Histogram örnekleri



(a) Orijinal görüntüye ait histogram verileri



(b) Manipüle edilmiş görüntüye ait histogram örnekleri

2.1.4. ELA Analizi – Error Level Analysis

ELA Analizi tekniği, farklı sıkıştırma seviyelerini tespit ederek görüntünün parçalarının tanımlanması amacıyla kullanılmaktadır. ELA tekniği ile görüntü üzerinde yapılan manipülasyonların tespiti öğrenilebilmekte ve görüntüde manipüle edilmiş alanlar fark edilebilmektedir. ELA, orijinal görüntü ile görüntünün yeniden kaydedilmiş versiyonu arasındaki farkı hesaplar. Yeniden kaydedilen görüntü üzerinde, orijinal görüntüye benzer miktarda sıkıştırma bulunur. (Raković, 2023) çalışmasında, Orijinal görüntü ile yeniden

kaydedilen görüntü arasındaki fark, sıkıştırma işleminin neden olduğu hata miktarını gösterir. Görüntünün değişmeyen alanlarında hata düzeyinin düşük, manipüle edilen alanlarda ise hata düzeyinin yüksek olduğunu belirtmiştir. Bu çalışmada, orijinal görüntüler ile manipüle edilmiş görüntüler <https://fotoforensics.com/> isimli websayfası üzerinden değerlendirmeye alınmıştır.

2.2. Görüntü Üzerinde Yapılan Manipülasyon ve Tespit Yöntemleri

Aktif sahtecilik ve pasif sahtecilik olmak üzere Görüntü sahteciliği için iki tür teknik vardır. Aktif Sahtecilik, Dijital Parmak izi ve Dijital İmza olmak üzere ikiye ayrılırken, Pasif Sahtecilik ise Rütuşlama, Ekleme ve Klonlama olarak üçe ayrılmaktadır (Sridevi, Mala ve Sanyam, 2012). Veri hakkında herhangi bir bilgi bulunmadığı durumlarda ise aktif teknikler güçsüz hale gelip pasif tekniklere odaklanılması gerekir. Bu sebepten aktif ve pasif teknikler kullanılarak manipülasyonun tespit edilmesi oldukça önemli bir durumdur.

2.2.1. Aktif Sahtecilik

Aktif teknikler, dijital filigran ve dijital imzaya ihtiyaç duymaktadır. Dijital Filigran, görüntü üzerine eklenen bir işaret iken, Dijital İmzalar ise Dijital imzalar, bit akışının kimliğini doğrulayan düz şifreleme yöntemleridir. Fakat kullanılan her görüntüde bu bilgilerin bulunması beklenemez. Bu problem aktif tekniklerin en büyük dezavantajı ve güçsüz yönüdür.

2.2.2. Pasif Sahtecilik

Pasif teknikler ise, veri ve verinin özelliklerini kullanarak sahtecilik tespitine odaklanan tekniklerdir. Pasif tekniklerde ise sahteciliğin tespit edilmesi aktif tekniklere kıyasla daha zordur (Akdeniz ve Becerikli, 2023). Rütuşlama, görüntüdeki bir bölgeyi veya deliği doldurmayı içerir. Rütuşlama, genellikle görüntülerdeki hasarlı bölgeleri onarmak için kullanılır. Ekleme – Image Splicing, Bu sahtecilik, yapıştırılan bölgelerin/nesnelerin bir veya daha fazla başka görüntüden kesilmesi arasındaki farkla kopyala-taşı'ya benzer. Bazı içerikleri gizlemek veya sahte bir durumu göstermek amacıyla ekleme sahteciliği yapılabilir. Klonlama, Kopyala-Taşı olarak da bilinen bu yöntemde, görüntünün bir kısmı kopyalanır ve aynı görüntünün başka bir bölümüne enjekte edilir. Bu genellikle bir nesneyi görüntünün

başka bir kısımdan kopyalanan bir bölümle kaplayarak görüntüden kaybolmasını sağlamak amacıyla gerçekleştirilir. Çim, bitki örtüsü, çakıl veya düzensiz desenlere sahip kumaş gibi dokulu alanlar bu amaç için idealdir (Kaur ve Manro, 2019).

2.3. Görüntü Üzerinde Yapılan Manipülasyonlar

Görüntüler, üzerinde manipülasyon yapılmaya uygun nitelikte olan bir manzara görüntüsü (Şekil 2.3), Fakewhats.com web sayfası üzerinden yapay olarak oluşturulan mesajlaşmaya ait görüntü (Şekil 2.5) ve cep telefonu üzerinden kısa mesajlaşma servisi (SMS) üzerinden mesajlaşma esnasında alınan ekran görüntüsü (Şekil 2.6) ait olmak üzere üç farklı orijinal görüntü seçilmiştir.

2.3.1. Orijinal Görüntü ve Manipüle Edilmiş Görüntü Oluşturulması

Orijinal görüntü üzerinde yer alan ‘Martı’ üzerinde klonlama işlemi gerçekleştirilmiş ve Şekil 2.3 (b) elde edilmiştir. Aynı orijinal görüntüye Adobe Photoshop FireFly Yapay Zeka (AI) aracı kullanılarak “deniz üzerinde hareket halinde olan bir tekne” görüntüsü eklenmiş Şekil 2.3. (c)’de görüntülenen sonuca ulaşılmıştır. Orijinal manzara görüntüsü ve bu görüntüye manipülasyon uygulanarak oluşturulan görüntüler, üzerinde Meta Veri Analizi, ELA Analizi ve yapısal kısımdan analiz edilmek üzere incelemeye alınmıştır.

Şekil 2. 3

Manzara görüntüsü ve manipüle edilmiş manzara görüntüleri



(a) Orijinal görüntü



(b) Klonlama ile manipüle edilmiş görüntü



(c) Adobe photoshop firefly yapay zeka işlemi kullanılarak manipüle edilmiş görüntü

2.3.2. Sahte WhatsApp Ekran Görüntüsü Oluşturulması

Dijital manipülasyon tekniklerinin yaygınlaşmasıyla birlikte, sahte ekran görüntüleri oluşturmak için çeşitli çevrimiçi araçlar ve yazılımlar geliştirilmiştir. Bunlardan biri de FakeWhats.com adlı web sitesidir. Bu websayfası üzerinde, kullanıcılara iletişim uygulaması olan Whatsapp isimli mobil uygulama arayüzüne benzeyen sahte ekran görüntüleri oluşturma imkanı sunmaktadır. Kullanıcılar, mesaj içeriklerini, mesajın gönderildiği zaman damgalarını, profil fotoğraflarını, telefonun mobil şebeke sinyalini ve bağlı olduğu mobil ağ operatörünü, telefonun batarya şarj durumunu gösterir yüzdelik dilimini, cihaz saatini, mesaj yazım kısmında yer alan metni ve alıcı isimlerini özelleştirebilmektedir.

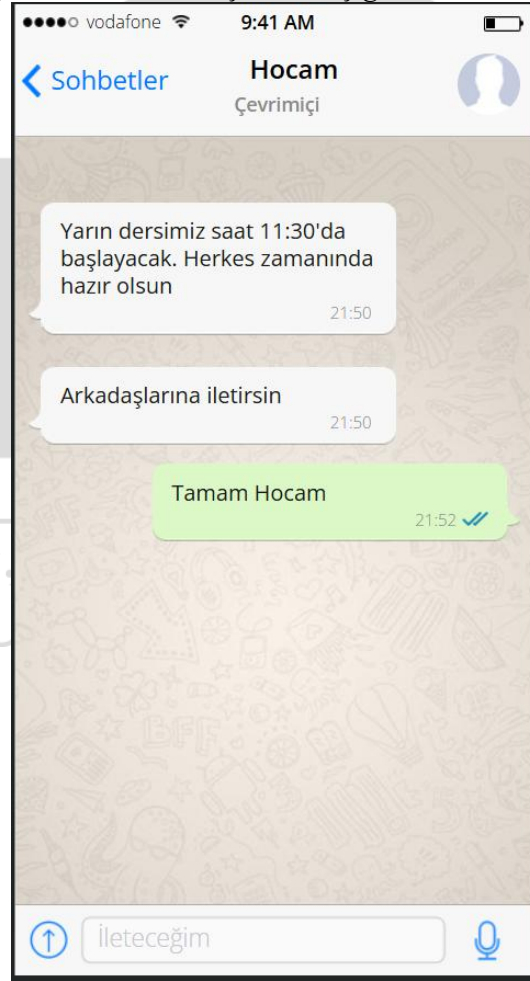
Bu çalışma kapsamında, FakeWhats.com domaini üzerinde kullanılarak bir sahte ekran görüntüsü oluşturulmuştur. Hazırlanan ekran görüntüsünde, alıcı ismi gerçekte var olmayan

kişiyi ait olacak şekilde ‘Hocam’ olarak manipüle edilmiştir. Alınan mesaj içerikleri “Yarın dersimiz saat 11:30’da başlayacak. Herkes zamanında hazır olsun”, “Arkadaşlarına iletirsin” olarak, ‘Hocam’ isimli kişiyi gönderilen mesaj ise “Tamam Hocam” olarak düzenlenmiş ve belirli bir kişi hakkında yanıltıcı bilgi yaymak amacıyla oluşturulmuştur. Mesajın gönderildiği saat bilgileri “21:50 – 21:52” zaman aralığını gösterecek şekilde kronolojik olarak düzenlenmiştir.

Dersin başlayacağı zamana dair ‘Hocam’ isimli kişiden gelen mesajların, zaman damgalarının, mesajlara karşılık olarak gönderilen 1 adet mesaj bulunmaktadır. Manipüle edilmiş png uzantılı mesajlaşma görüntüsü üzerinde (Şekil 2.4) Meta Veri Analizi, ELA Analizi ve yapısal kısımdan analiz edilmek üzere incelemeye alınmıştır.

Şekil 2. 4

Fakewhats.com web sayfası üzerinden oluşturulmuş görüntü

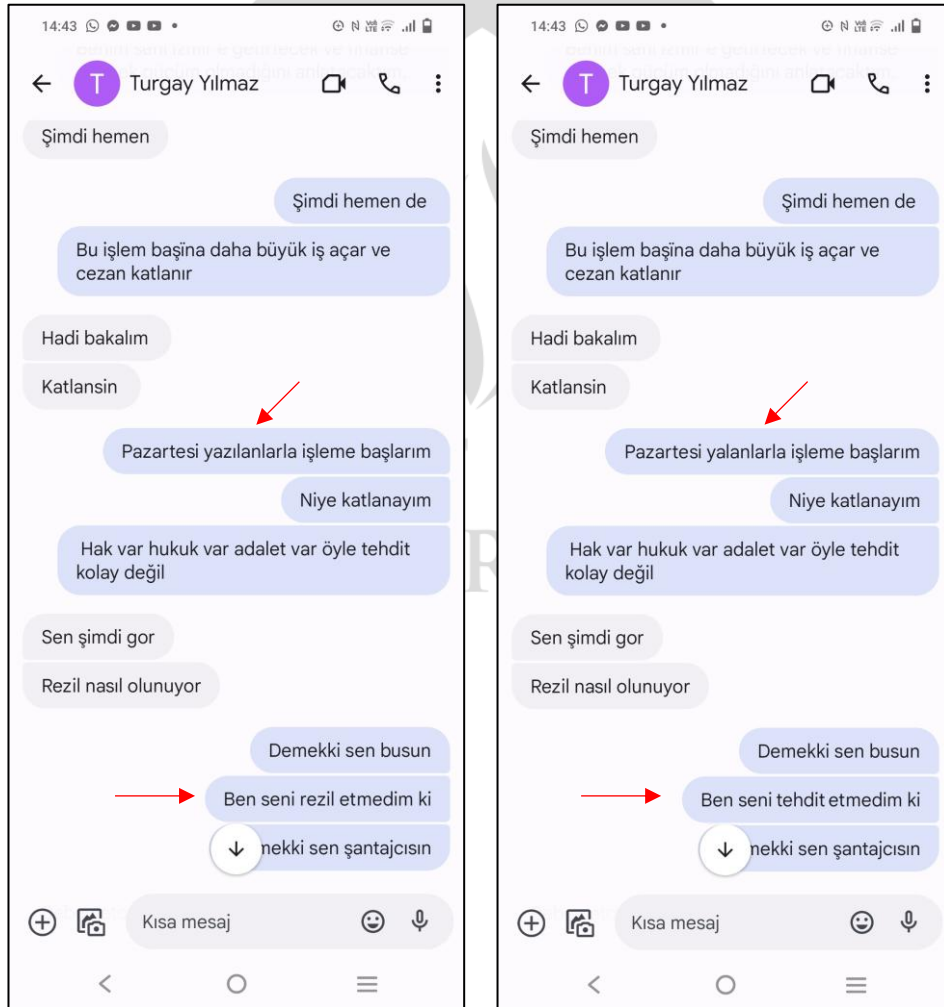


2.3.3. Orijinal Mesajlaşmaya ait Ekran Görüntüsü ve Manipüle Edilmiş Mesajlaşma Görüntülerinin oluşturulması

Günümüz iletişiminin önemli bir parçası olan cep telefonları üzerinden sıklıkla mesajlaşmaların gerçekleştiği bilinmektedir. Kısa Mesajlaşma Servisi üzerinde karşılıklı olarak yapılan mesajlaşmalardan alınan görüntüler üzerinde, bir takım yardımcı programlar ile düzenlemeler yapılması mümkündür. Gönderilen ya da alınan mesajların düzenlenmesi esnasında kopyala-Yapıştır ve taşıma işlemleri gerçekleştirilerek gerçeklikten uzak iletiler oluşturulabilmektedir. Bu çalışmada, Mesajlaşmaya ait ekran görüntüsü üzerinde gönderilen mesajlar üzerinde kelime değişiklikleri yapılarak manipüle edilmiş bir örnek incelemeye alınmıştır.

Şekil 2. 5

Kısa mesajlaşmaya ait görüntü ve manipüle edilmiş mesajlaşma görüntüsü



a) Orijinal Görüntü

b) Manipüle Edilmiş Ekran görüntüsü

Cep Telefonu üzerinden alınan orijinal ekran görüntüsü (Şekil 2.6) üzerinde, metin olarak bulunan “Pazartesi yazılanlarla işleme başlarım” ve “Ben seni rezil etmedim ki” cümleleri üzerinde Kopyala-Yapıştır ve Taşıma yöntemleri kullanılarak manipülasyona uğrayan görüntü (Şekil 5.b) oluşturulmuştur. Görüntünün arka plan, kayıtlı kullanıcı adı gibi genel yapısı orijinal haliyle bırakılmıştır. Görüntüler üzerinde, Pasif Sahteciliğin tespiti amacıyla Histogram, ELA, Gürültü Analizi incelemeleri ile Exif Meta Veri kontrolü yapılarak araştırma sonuçları elde edilmiştir.

2.4. Görüntü Üzerinde Yapılan Manipülasyonların Tespiti

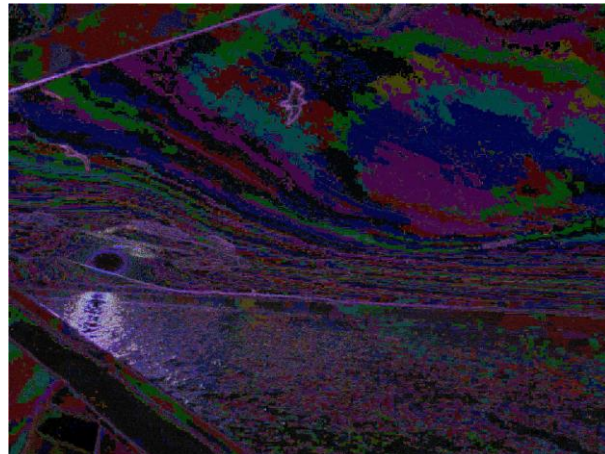
Orijinal Görüntüler ile Manipüle edilen görüntüler arasında karşılaştırma yapılarak, görüntüler üzerinde ELA Analizi, Histogram Analizi ve Exif Verileri değerlendirilmek üzere incelemeye alınmıştır. İnceleme esnasında, <https://fotoforensics.com/> isimli websayfası üzerinde ELA analizi ile Exif veri analiz, Adobe Photoshop isimli program üzerinde Histogram verileri kontrol edilmiştir.

2.4.1. Görüntüler üzerinde ELA Analizi

Çalışmada, ilk olarak orijinal olduğu bilinen manzara görüntüsü üzerindeki ELA analizi sonuçları gösterilmiş, görüntünün üzerine klonlama işlemi ve Adobe Photoshop FireFly yapay zeka işlemi uygulanarak manipüle edilmesi sonucu oluşan ELA analiz sonuçları değerlendirmeye alınmıştır. Uygulama esnasında <https://fotoforensics.com/> isimli websayfası üzerinden yapılan analizi verileri kontrol edilmiştir.

Şekil 2. 6

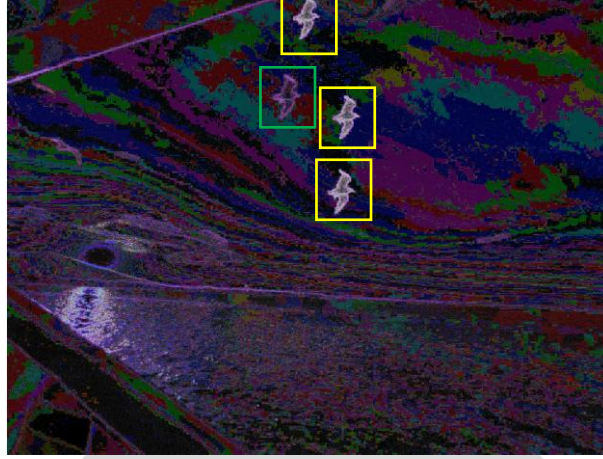
Manzara görüntüsü ELA analizi



Orijinalliği bilinen manzara fotoğrafı üzerinde yapılan ELA analiz işleminde, manzara görüntüsünün, üzerinde yer alan objelerin ve fotoğrafa ait renklerin tutarlı bir dağılımda bulunduğu görülmüştür.

Şekil 2. 7

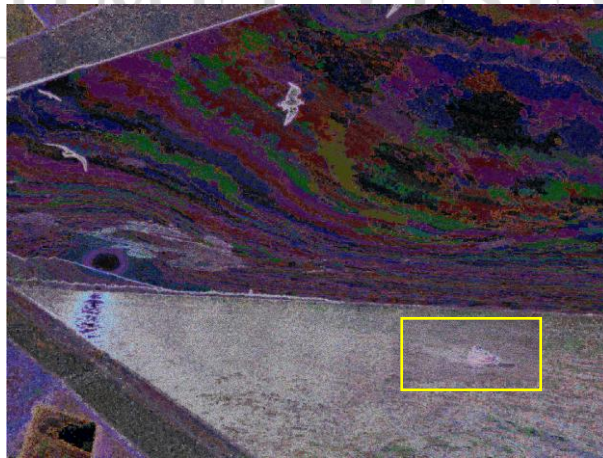
Klonlama işlemine maruz kalmış görüntüye ait ELA analizi



Manzara görüntüsü üzerinde bulunan martı klonlanarak üç adet martı görüntüsü oluşturulmuştur. Manipüle edilen görüntü üzerinde ELA analizi gerçekleştirildiğinde, klonlaması yapılan martıya ait renk değerinin, manzara görüntüsü üzerinde soluk bir şekilde görüntülendiği, manzara görüntüsü üzerinde yer alan renk dağılımı ile uyumlu olduğu, klonlanan üç adet martının ise manzara görüntüsüne ve klonlaması yapılan martıya göre daha açık renkte olduğu görüntülenmiştir.

Şekil 2. 8

Yapay zeka işlemi kullanılarak manipüle edilmiş görüntüye ait ELA analizi



Manzara görüntüsü üzerine, Adobe Photoshop FireFly yapay zeka işlemi uygulanarak tekne görüntüsü eklenmesi sonucu yeni görüntü oluşturulmuştur. Şekil 2.7’de orijinal görüntüye

ve üzerine nesne eklenerek oluşturulan yeni görüntü (Şekil 2.9) üzerinde ve ait ELA analizi karşılaştırıldığında, manipüle edilmiş görüntünün daha parlak olduğu, görüntüye eklenen nesnenin bulunduğu kısımlardaki renk dağılımında dalgalanmaların bulunduğu görüntülenmiştir.

Bu araştırmada görüleceği üzere, üzerinde klonlama yapılan ve yapay zeka ile nesne eklenmesi ile oluşturulan görüntüye ait ELA analiz sonuçlarında, manipülasyonun manzara görüntüsü üzerinde nerede ve nasıl yapıldığı konusunda bilgi sağlamıştır.

Şekil 2. 9

Mesajlaşma görüntüleri üzerinde ELA analizi



FakeWhats.com web sayfası üzerinden indirilen görüntünün karşılaştırılması yapılacak başka bir görüntü bulunmaması sebebiyle üzerinde ELA Analizi yapılmasının araştırmaya katkı sağlamasına imkan bulunmamaktadır. Ancak mesajlaşmaya ait orijinal görüntü ve manipüle edilmiş mesajlaşma görüntüsünde, metinleri gösteren kısımlar ile fon kısımlarında yer alan renklerin orijinal mesajlaşmaya ait görüntüden daha parlak olduğu görülmüştür. Manipüle işlemi sonrası oluşan mesajlaşma görüntüsünde, renklerin daha parlak olması sebebiyle görüntü üzerindeki dairesel şekillerin daha belirginleştiği görülmüştür.

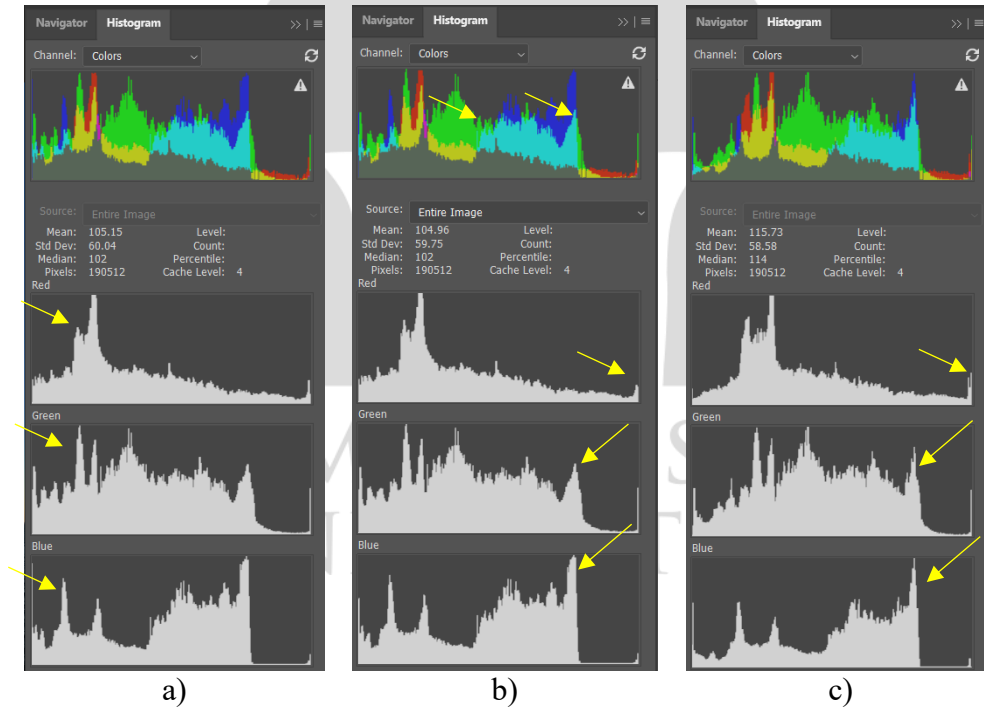
2.4.2. Görüntüler üzerinde Histogram Analizi

Histogram analizi, manzara görüntüsü ve manipüle edilen manzara görüntülerinde, kısa mesajlaşma ve manipüle edilen kısa mesajlaşma görüntüsü üzerinde gerçekleştirilmiştir. FakeWhats.com web sayfası üzerinden indirilen sahte whatsapp uygulamasına ait mesajlaşmayı gösterir tek olması, benzerinin bulunmaması sebebiyle karşılaştırma yapılmak üzere incelemeye dahil edilmemiştir.

Manzara görüntüsüne ve manipüle edilerek oluşturulan yeni görüntülere ait Histogram Grafikleri analiz edildiğinde yapılan analizlerde, manzara görüntüsü üzerinde yer alan mavi ve yeşil renk alanlarının yoğunluğunun, manipüle işlemi sonrası histogram üzerinde farklılaştığı sonucuna ulaşılmıştır.

Şekil 2. 10

Manzara görüntüsü ve manipüle edilen görüntüler üzerinde histogram analizi



Orijinal Manzara Görüntüsüne ait Histogram Grafiği üzerindeki istatistikleri ve üzerinde Klonlama ve Yapay Zeka kullanılarak manipüle edilmiş görüntülerde, Histogram Grafiklerinde Anlam, Standart Sapma, Medyan, Piksel bilgisine ait verilerin değişikliğe uğradığı sonucuna ulaşılmış ve bu değişiklikler tablo olarak (Tablo 1) verilmiştir.

Tablo 1

Manzara görüntüsü ve manipüle edilen görüntüler üzerinde histogram analizi verileri

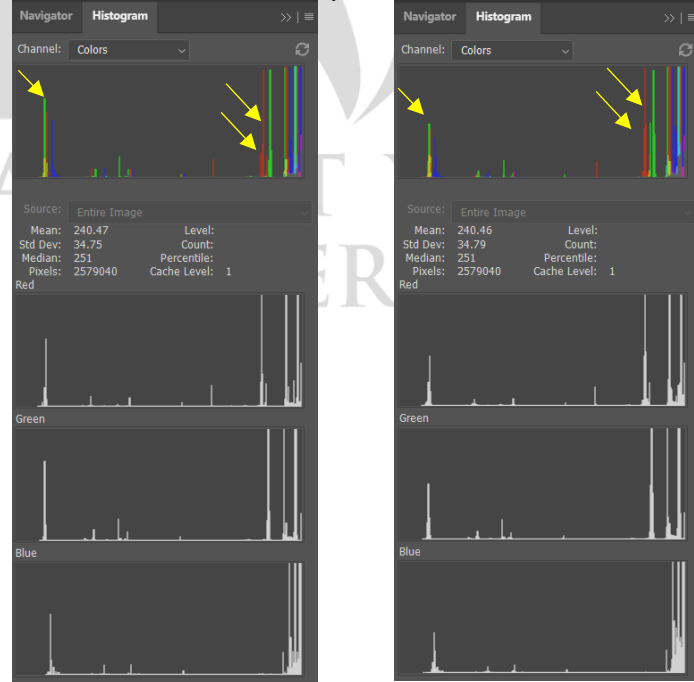
Başlıklar / Görüntüler	Orijinal Görüntü	Klonlama Yapılarak Manipüle Görüntü	Yapay Zeka Kullanılarak Manipüle Edilmiş Görüntü
anlam (mean)	105.15	104.96	115.73
standart sapma	60.04	59.75	58.58
medyan (median)	102	102	114
pikseller (pixels)	190512	190512	190512

Tablo da görüleceği üzere, üzerinde düzenleme yapılan manzara görüntülerinin, Anlam verisinde artma ve azalma gerçekleştiği, Klonlama ve Yapay Zeka uygulanan görüntülerin Standart Sapmasında düşüklük bulunduğu, Medyan Değerinin sadece Yapay Zeka Kullanılarak manipüle edilmiş görüntüde değerlerin arttığı anlaşılmıştır.

Mesajlaşma görüntüsü ve Mesajlaşma görüntüsünün manipüle edilerek oluşturulan yeni görüntüsü üzerinde Histogram Grafikleri analiz edilmiştir. Yapılan analizlerde, manzara görüntüsü üzerinde yer alan Mavi ve Yeşil Renk alanlarının yoğunluğunun, manipüle işlemi sonrası Renk oranlarının Histogram üzerinde farklılaştığı sonucuna ulaşılmıştır.

Şekil 2. 11

Mesajlaşma ve manipüle edilen mesajlaşmaya ait görüntü üzerinde histogram analizi



a)

b)

Tablo 2

Mesajlaşma görüntüsü ve manipüle edilen mesajlaşma görüntüsü üzerinde histogram analizi verileri

Başlıklar / Görüntüler	Orijinal Mesajlaşma Görüntüsü	Manipüle Edilmiş Mesajlaşma Görüntüsü
anlam (mean)	240.47	240.46
standart sapma	34.75	34.79
medyan (median)	251	251
pikseller (pixels)	2579040	2579040

Mesajlaşmadan alınan orijinal görüntü ile üzerinde düzenleme yapılan görüntü karşılaştırıldığında, Tabloda da görüleceği üzere, Orijinal Mesajlaşma Görüntüsü ile Manipüle Edilmiş Mesajlaşma görüntüsü üzerinde yer alan Anlam verisinde azalmanın, Standart Sapma verisinde artma yaşandığı sonucuna varılmıştır.

2.4.3. Görüntüler üzerinde Exif Verileri Analizi

Bu çalışma kapsamında, farklı yöntemlerle manipüle edilmiş beş ayrı görsel üzerinde analiz gerçekleştirilmiş ve dijital manipülasyon süreçleri ile Exif verilerinin önemi ortaya konmuştur.

Manzara görüntüsüne ait Exif Verileri

Orijinalliği değiştirilmemiş olan görüntünün ilk olarak 8 Kasım 2022 tarihinde kaydedilmiştir. Görüntü üzerinde değişiklik yapılmadan önceki Exif verileri araştırma yapılmak üzere incelemeye alınmıştır.

Şekil 2. 12

Manzara görüntüsüne ait EXIF verileri

EXIF	
Make	Apple
Camera Model Name	iPhone 13 Pro
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	16.0
Modify Date	2022:11:08 17:44:14
Host Computer	iPhone 13 Pro
Exposure Time	1/1754
F Number	1.8
Exposure Program	Program AE
ISO	32
Exif Version	0232
Date/Time Original	2022:11:08 17:44:14
Create Date	2022:11:08 17:44:14

Manzara görüntüsünde bulunan Martıların Klonlama işlemi ile çoğaltılması (Şekil 3.b) ile oluşan Exif Verileri

Orijinal olan ilk görüntü (Şekil 3.a), deniz manzarasına ait bir görüntüden oluşmaktadır. Görsel üzerinde yer alan martı dijital araçlar kullanılarak çoğaltılmıştır. Bu tür bir manipülasyon, bir görüntüde mevcut unsurların kopyalanarak çoğaltılması yoluyla sahnenin doğasını değiştirmektedir.

Şekil 2. 13

Manzara görüntüsü üzerinde klonlama işlemi uygulanması sonucu EXIF verileri

EXIF	
Photometric Interpretation	RGB
Make	Apple
Camera Model Name	iPhone 13 Pro
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	Adobe Photoshop 26.0 (Windows)
Modify Date	2024:11:26 10:55:40
Host Computer	iPhone 13 Pro
Exposure Time	1/1754
F Number	1.8
Exposure Program	Program AE
ISO	32
Exif Version	0232
Date/Time Original	2022:11:08 17:44:14
Create Date	2022:11:08 17:44:14

Yapılan araştırmada, 8 Kasım 2022 tarihinde çekilmiş olan deniz manzarasına ait görüntü üzerinde, klonlama yöntemi ile çoğaltılan martıların Exif verilerini değişikliğe uğrattığı ve uğratmadığı incelenmiştir. Yapılan manipüle işlemi sonrası Exif verileri üzerinde yer alan Software -Yazılım ve Modify Date başlıkları kontrol edildiğinde, üzerinde değişiklik yapılan görüntünün Adobe Photoshop 26.0 ile yazılımı ile 26 Kasım 2024 tarihinde değiştirildiği gözlemlenmiştir.

Manzara görüntüsünde Deniz Üzerine Tekne Eklenmesi (Şekil 2.14)

Aynı deniz manzarası, Adobe Photoshop Firefly yapay zeka aracı kullanılarak manipüle edilmiştir. Bu işlem sırasında, orijinal görsel üzerinde bulunmayan bir tekne, yapay zeka algoritmalarının yardımıyla deniz yüzeyine eklenmiştir. Bu manipülasyon, gerçek olmayan unsurların bir sahneye entegre edilmesine örnek teşkil etmektedir.

Şekil 2. 14

Manzara görüntüsüne yapay zeka ile tekne eklenmesi sonucu EXIF verileri

EXIF		JUMBF	
Orientation	Horizontal (normal)	JUMD Type	(c2pa)-0011-0010-800000aa00389b71
X Resolution	72	JUMD Label	c2pa
Y Resolution	72	Actions Action	c2pa.edited
Resolution Unit	inches	Actions Software Agent	Adobe Firefly
Software	Adobe Photoshop 26.0 (Windows)	Actions Digital Source Type	http://cv.ipptc.org/newscode/digitalsourcetype/compositeWithTrainedAlgorithmicMedia
Modify Date	2024:11:23 19:31:30	Exclusions Start	4044
Color Space	Uncalibrated	Exclusions Length	13391
Exif Image Width	4032	Name	jumbf manifest
Exif Image Height	3024	Alg	sha256
Compression	JPEG (old-style)	Hash	(Binary data 32 bytes)
Thumbnail Offset	318	Pad	(Binary data 9 bytes)
Thumbnail Length	3726	Title	Generated image
Thumbnail Image	(Binary data 3726 bytes)	Claim generator	Adobe_Photoshop/26.0.0 adobe_c2pa/0.12.2 c2pa-rs/0.32.5
		Claim Generator Info Name	Adobe Photoshop
		Claim Generator Info Version	26.0.0

Aynı manzara görüntüsü üzerine, manipüle işlemi uygulanarak Exif verileri kontrol edildiğinde, görüntünün yine Adobe Photoshop yazılımı ile düzenlendiği, görüntü üzerinde Adobe FireFly Yapay Zeka işlemi uygulandığı gözlemlenmiştir.

FakeWhats.com ile Oluşturulan Görsel (Şekil 2.15)

FakeWhats.com adlı çevrimiçi araç kullanılarak, WhatsApp arayüzüne benzeyen bir ekran görüntüsü oluşturulmuştur. Bu sahte ekran görüntüsünde, kullanıcı isimleri, mesaj içerikleri ve zaman damgaları özelleştirilmiştir. Görsel, bir manipülasyon örneği olarak incelenmiştir.

Şekil 2. 15

Web sayfası üzerinden oluşturulan mesajlaşma ekran görüntüsü üzerinde EXIF verileri

File	
File Type	PNG
File Type Extension	png
MIME Type	image/png
PNG	
Image Width	483
Image Height	894
Bit Depth	8
Color Type	RGB
Compression	Deflate/Inflate
Filter	Adaptive
Interlace	Noninterlaced
SRGB Rendering	Perceptual
Gamma	2.2
Pixels Per Unit X	4724
Pixels Per Unit Y	4724
Pixel Units	meters
Software	Greenshot
Composite	
Image Size	483x894
Megapixels	0.432

Görüntü üzerinde yer alan Software- Yazılım bilgisinin ‘Greenshot’ isimli ekran kaydetme programı ile kaydedildiği sonucunu göstermektedir.

Orijinal Kısa Mesaj Ekran Görüntüsü (Şekil 2.16)

Cep telefonundan alınmış orijinal bir kısa mesaj ekran görüntüsü incelemeye dahil edilmiştir. Bu görsel, bir referans niteliği taşımakta ve herhangi bir düzenleme içermemektedir.

Şekil 2. 16

Mesajlaşmaya Ait Orijinal Görüntü Üzerinde Exif Verileri

EXIF	
Date/Time Original	2024:01:07 14:43:24
Create Date	2024:01:07 14:43:24
Color Space	Uncalibrated
Light Source	Unknown
Orientation	Unknown (0)
Modify Date	2024:01:07 14:43:24

Kısa Mesajlaşmaya ait görüntü üzerindeki Exif Verileri Kontrol edildiğinde, görüntünün 7 Ocak 2024 tarihinde kaydedildiği, görüntünün üzerinde herhangi bir düzenleme yapılmadığından oluşturulma ve düzenleme tarihlerinin aynı oldukları, bu sebeple Exif verileri üzerinde bir değişikliğin bulunmadığı görülmektedir.

Kısa Mesaj Görseli Üzerinde Kelime Değişiklikleri (Şekil 2.17)

Şekil 5.a’da yer alan kısa mesaja ait ekran görüntüsünde yer alan bazı kelimeler değiştirilmiş ve görüntü manipüle edilmiştir. Bu tür manipülasyonlar, ekran görüntülerinin gerçekliğine dair güveni sarsan örnekler arasında yer almaktadır.

Şekil 2. 17

Mesajlaşma ekran görüntüsü üzerinde manipölasyon yapılması sonrası EXIF verileri

EXIF	
Photometric Interpretation	RGB
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	Adobe Photoshop 26.0 (Windows)
Modify Date	2024:11:26 20:22:38
Exif Version	0231
Date/Time Original	2024:01:07 14:43:24
Create Date	2024:01:07 14:43:24
Light Source	Unknown
Color Space	Uncalibrated
Exif Image Width	1080
Exif Image Height	2388
Compression	JPEG (old-style)
Thumbnail Offset	470
Thumbnail Length	3045
Thumbnail Image	(Binary data 3045 bytes)

Mesajlaşma görüntüleri üzerinde yapılan manipölasyon işlemi sonrası Exif Verileri analiz edildiğinde, 7 Ocak 2024 tarihinde kaydedilen görüntünün, Adobe Photoshop isimli görüntü işleme yazılımı aracılığıyla 26 Kasım 2024 tarihinde manipüle edildiği, yapılan manipölasyon işlemi sonrası yeni bir görüntü oluşturulduğu bilgisi öğrenilmiştir.

AHMET YESEVİ
ÜNİVERSİTESİ

BÖLÜM III

YÖNTEM

3.1. Araştırmanın Modeli

Araştırma esnasında, fotoğraf ve görüntüler üzerinde manipülasyonlar uygulanmış, ortaya çıkan manipüle edilmiş görüntüler üzerinde bilinen yöntemlerden olan ELA Analizi, Histogram Analizi, Exif Verileri İncelemesi ayrı ayrı uygulanmıştır. Orijinalliği bilinen görüntüler ve manipüle edilmiş görüntüler üzerinde yapılan değişikliklerde manipülasyonun tespiti amaçlanmıştır. Bu yöntemler, sistematik olarak uygulanmıştır.

3.2. Evren ve Örneklem

Araştırmanın evreni olarak, orijinal olduğu bilinen bir manzara görüntüsü, bu görüntü üzerinde yer alan martı klonlama tekniği ile çoğaltılarak yeni bir görüntü, aynı manzara görüntüsü üzerinde yapay zeka teknolojisi kullanarak deniz üzerinde hareket eden bir tekneye ait bir görüntüsü seçilmiştir. Manipülasyon işlemlerinin gerçekleştiği başka bir platform olan whatsapp isimli uygulamaya benzer görüntülerin oluşturulabildiği fakewhats.com isimli web sayfası üzerinden sahte bir görüntü oluşturulmak suretiyle araştırmaya dahil edilmiştir. Ayrıca, cep telefonundan alınan mesajlaşmaya dair asıl görüntü üzerinde kelime değişikliği yapılarak manipüle edilen yeni görüntüler oluşturularak araştırmaya dahil edilmiştir. İncelemesi yapılan fotoğraf ve görüntüler, üzerlerinde yapılan manipülasyonun tespit yöntemlerinin çeşitliliğini göstermek amacıyla itinayla belirlenmiştir.

3.3. Veri Toplama Araçları

Araştırmada, görüntüler üzerinde manipülasyon yapmak amacıyla çeşitli yazılımlar ve araçlar kullanılmıştır. Manzara görüntüleri ve mesajlaşmalar üzerinde düzenleme yapmak için Adobe Photoshop yazılımı kullanılmış, yapay zeka destekli içerik oluşturmak amacıyla Adobe Firefly yapay zeka aracı tercih edilmiştir. Histogram verilerinin analizi için yine Adobe Photoshop yazılımından yararlanılmıştır. Sahte WhatsApp mesajına ait görsellerin oluşturulması sürecinde ise FakeWhats.com platformu kullanılmıştır. Manipüle edilen görüntülerin Exif verilerinin analizi ve ELA işlemleri, Fotoforensics isimli web tabanlı analiz aracı ile gerçekleştirilmiştir.

3.4. Verilerin Toplanması

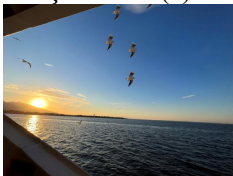
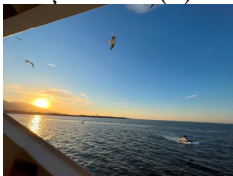
Veriler üç farklı manipülasyon tekniği kullanılarak hazırlanmıştır. Orijinalliği bilinen manzara fotoğrafı üzerinde klonlama tekniği kullanılarak görüntü çoğaltma ve yapay zeka ile oluşturulmuş nesne eklenerek görüntü üzerinde manipülasyon gerçekleştirilmiştir. FakeWhats web uygulaması üzerinden Whatsapp konuşmasına ait görüntü oluşturularak sahte mesajlaşmaya ait içerik oluşturulmuştur. Ekran görüntüsü üzerinde metinlerin kopyalanarak yapıştırılması sonucunda gerçek mesaja ait olmayan veriler elde edilmiştir.

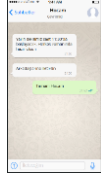
3.5. Verilerin Analizi

Araştırma sonucunda elde edilen veriler, üç farklı analiz yöntemiyle değerlendirmeye alınmıştır. Görüntüler üzerinde yapılan manipülasyonların algılanabilmesi için hata seviyeleri görselleştirilmesi amacıyla ELA yöntemi kullanılmış ve görüntüler üzerinde analiz sağlanmıştır. Görüntülerin renk ve ton dağılımları üzerinde inceleme gerçekleştirilerek orijinal ve manipüle edilmiş alanlar arasındaki farklılıklar Histogram Analizi ile tespit edilmiştir. Fotoğrafların metadata bilgileri incelenmiş, manipülasyon izi olabilecek düzenleme kayıtları, EXIF Verileri üzerinde analiz edilmiştir. Analiz sonuçları, her yöntemin farklı türde manipülasyonları tespit etme kabiliyeti hakkında bilgi sağlayarak araştırmaya katkı sağlamıştır.

Tablo 3

Orijinal/manipüle edilmiş görüntülerde ELA, histogram ve EXIF verileri kontrol tablosu

Görüntüler	ELA	Histogram	Exif Verileri
 Şekil 2.3 (a)	Orijinal Görüntü üzerinde değişiklik görülmemiştir.	Orijinal Görüntü üzerinde değişiklik görülmemiştir.	Orijinalliği Değiştirilmemiştir.
 Şekil 2.3 (b)	Manipüle edilen görüntü üzerinde değişiklik gözlemlenmiştir.	Belirgin bir değişiklik görülmemiştir.	Orijinalliği Adobe Photoshop ile değiştirilmiştir.
 Şekil 2.3 (c)	Manipüle edilen görüntü üzerinde değişiklik gözlemlenmiştir.	Belirgin bir değişiklik görülmemiştir.	Orijinalliği Adobe Photoshop ile değiştirilmiştir.



Şekil 2.4

Orijinal Görüntü
üzerinde değişiklik
görülmemiştir.

Orijinal Görüntü
üzerinde değişiklik
görülmemiştir.

Orijinal Görüntü
üzerinde değişiklik
görülmemiştir.



Şekil 2.5 (a)

Orijinal Görüntü
üzerinde değişiklik
görülmemiştir.

Orijinal Görüntü
üzerinde değişiklik
görülmemiştir.

Orijinalliği
Değiştirilmemiştir.

Manipüle edilen görüntü
üzerinde değişiklik
gözlemlenmiştir.

Belirgin bir
değişiklik
görülmemiştir.

Orijinalliği Adobe
Photoshop ile
değiştirilmiştir.

Şekil 2.5 (b)



BÖLÜM IV

BULGULAR VE YORUM

4.1. Görüntü Üzerinde Yapılan Manipülasyonların ELA Analizi Üzerinde Etkisi

Araştırma üzerinde incelemeye alınan Evren ve Örneklem üzerinde ELA analizi gerçekleştirildiğinde, Adobe Photoshop ile klonlanan nesnelerin ve Adobe FireFly yapay zeka aracı ile manipüle edilen görüntülerde, manipülasyonun görüntü üzerinde nerede ve nasıl ortaya çıktığı gözlemlenmiştir. Klonlama işlemi sonrası ELA Analiz verileri göz önüne alındığında, klonlanan nesnenin görüntü üzerinde daha parlak olduğunu, yapay zeka ile oluşturulan nesnenin ise görüntüdeki parlaklığı düşürerek düzenlenmiş alandaki gren sayısını arttırdığı göstermiştir. Fakewhats.com sayfası üzerinden oluşturularak indirilen sahte içerikli whatsapp mesajına ait görüntünün tek olması sebebiyle üzerinde ELA analizine ait karşılaştırma yapılamamıştır. Cep telefonundan alınan mesajlaşmaya ait ekran görüntüsü ve bu görüntü üzerinde yapılan kelime değişiklikleri ile manipüle edilen haline ilişkin görüntü üzerinde gerçekleştirilen ELA analizinde, manipüle edilmiş görüntünün daha parlak olduğu, görüntü üzerinde yer alan dairesel şekillerin daha belirgin olduğunu göstermiştir.

4.2. Görüntü Üzerinde Yapılan Manipülasyonların Histogram Verileri Üzerinde Etkisi

Görüntüler üzerinde yapılan manipülasyonlar ile oluşturulan yeni görüntülerde genel renk dağılımında çok fazla bir değişiklik yaratmadığı gözlemlenmiştir. Özellikle Photoshop ile görüntü üzerinde gerçekleştirilen manipülasyonların, histogram verilerini değiştirmemesi sebebinin, manipülasyonun gerçekleştiği alanda renk tonlarının korunmasından kaynaklandığı, dolayısıyla renk değerlerinin doğal olabilecek bir sonuç çıkardığını göstermektedir.

4.3. Görüntü Üzerinde Yapılan Manipülasyonların Exif Verileri Üzerinde Etkisi

Evren ve Örneklem üzerinde yapılan manipülasyonların Exif Verileri üzerinde kontrolü sağlandığında, Adobe Photoshop ile manipüle edilen görüntülerde, yapılan düzenlemeye ait meta bilgilerin Exif verilerinde yer aldığı, düzenlemenin yapıldığı programı açık bir şekilde

gösterdiği sonucuna varılmıştır. FakeWhats isimli web sayfası ile oluşturulan sahte mesajlaşma görüntüsü üzerinde exif verilerinin sınırlı olduğu, manipülasyonun bu yöntemle sadece yazılım vasıtasıyla ekran kaydetme metodu ile alındığı bilgisini göstermektedir. Cep telefonundan alınan mesajlaşmalara ait ekran görüntüsü üzerinde gerçekleştirilen manipülasyon işlemi sonrası düzenleme yapılan zamanın ve programın net olarak görüntülenmesi sebebiyle görüntünün Exif verileri etkilediği görülmüştür.



BÖLÜM V

SONUÇ

5.1. Sonuç

Bu çalışmada fotoğraf ve ekran görüntüleri üzerinde yapılan manipülasyonların tespitine yönelik bilinen yöntemlerden olan ELA analizi, Histogram analizi ve Exif verileri değerlendirilmiştir. Görüntü üzerinde yapılan Manipülasyonlarda, Adobe Photoshop yazılımı kullanılarak klonlama, Adobe FireFly isimli yapay zeka destekli içerik ekleme, sahte WhatsApp mesajı oluşturma ve mesajlaşmalar üzerinde metin değişiklikleri yapılmıştır. Bu manipülasyonların tespiti için ELA analizi, histogram analizi ve Exif veri analizi gibi yöntemler kullanılmıştır.

ELA analizinin, Adobe Photoshop programı ile klonlanan ve aynı program ile yapay zeka destekli içerik kullanılarak nesne ekleme işlemi uygulanan görüntülerdeki manipülasyonları ve cep telefonu mesajlaşmalarının yer aldığı ekran görüntüsü üzerinde metin değiştirme işlemlerini etkili bir şekilde tespit edebildiği sonucuna ulaşılmıştır.

Histogram Analizinin renk ve ton dağılımını göstermesi sebebiyle, manipüle edilen görüntülerde, anlamlı bir farklılık tespit edilememiştir. Özellikle doğal tonların korunduğu işlemlerde histogram analizinin sınırlı tespit kabiliyeti sağladığı görülmüştür.

Exif veri analizinin, Adobe Photoshop kullanılarak düzenlenen görseller üzerinde yapılan değişiklikleri ortaya çıkarmıştır. FakeWhats platformundan düzenlenerek kaydedilen sahte ekran görüntülerinde Exif verilerinin yeterli bilgiyi sunmadığı görülmüştür. Exif verilerinin yalnızca belirli programlar ile düzenleme yapılan görüntüler üzerindeki işlemleri tespit etmede etkili olduğu sonucuna ulaşılmıştır.

KAYNAKÇA

- Ahmed, S., Yoon, B., Sharma, S., Singh, S., ve Islam, S. (2023). General Image Manipulation Detection Using Feature. *Mathematics*, 11(4537), 19-22.
- Akdeniz, F. ve Becerikli, Y. (2023). Dijital multimedya verilerinin güvenliği ve sahtecilik tespiti. *Adli Tıp Dergisi*, 37(3), 87-93.
- Al-Husseinawi, M. F., Jubori, H. K., Salim, S. A. ve Mohammed, A. Q. (2015). Image Splicing Forgery Detection Using Local Binary Pattern and Shift Vector. *Index Copernicus Value*, 405.
- Alvarez, P. (2004). Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis. *International Journal of Digital Evidence*, 1.
- Bayram, S., Avcıbaş, İ., Sankur, B. ve Memon, N. (2006). Image manipulation detection. *Journal of Electronic Imaging*, 041102-1.
- Demirel, G. (2015). Fotoğrafın manipülasyon ve gündem saptama gücü. *International Journal of Social Sciences and Education Research*, 1(2), 625.
- Ghazali, J. M., Khan, S. M., & Zakaria, L. Q. (2020). Image Classification using EXIF Metadata,. *International Journal of Engineering Trends and Technology (IJETT)*.
<https://www.youtube.com/watch?v=eoQKliAza9M>. (2022). (Google) Youtube.com. adresinden alındı
- Image Forensics to Detect Image Authenticity using Error Level Analysis and Noise Analysis Methods. (2023). 185.
- Kaur, G. ve Manro, R. (2019). Comparative Study of Copy Move Forgery Techniques. *International Journal of Engineering Trends and Technology (IJETT)*, 67(3), 146.
- Kılıçaslan, M., Tanyeri, U. ve Demirci, R. (2018). Düzce Üniversitesi. (6), 1094.
- Raković, D. N. (2023). Error Level Analysis (ELA). *TEHNIKA – ELEKTROTEHNIKA*, 72, 445.
- Samet, R. ve Atılgan, M. (2018). Güvenlik Kamera Görüntülerindeki Tarih ve Zaman Sayacı. *BİLİŞİM TEKNOLOJİLERİ DERGİSİ*, 333.
- Sridevi, M., Mala, C. ve Sanyam, S. (2012). Comparative Study of Image Forgery and Copy-Move. D. C. Wyld, J. Zizka, & D. Nagamalai (Dü.). içinde (s. 715). India: Conference proceedings.
- Yami, V. Ş. (2009). Dijital Manipülasyon ve Medya Etiği. M. YAĞBASAN (Dü.), *Medya ve Etik Sempozyumu* içinde (s. 60). ELAZIĞ: Karınca Yayınları.