

**ORIGINAL ARTICLE****THE ROLE OF ARTIFICIAL INTELLIGENCE SUPPORTED IMAGE ANALYSIS IN INSURANCE FRAUD AND RAPID DECISION MAKING PROCESSES: REALITYCHECKER**

Sefer DARICI

**Abstract**

Insurance fraud represents a pervasive issue that results in substantial financial losses, particularly for insurance providers. The advent of digital technology has facilitated the utilisation of an array of techniques by fraudsters, enabling them to achieve their objectives with greater ease and security, whilst simultaneously facilitating the detection of such activities. The digital forensic analysis of documents and images necessitates a high degree of expertise, is a laborious process, and is susceptible to human error. Such occurrences can result in financial, temporal, and labour losses, in addition to delays in decision-making processes. This article examines the potential of an artificial intelligence-powered document and image analysis system, designated “RealityChecker,” for the detection of insurance fraud and the facilitation of rapid decision-making processes for insurers. The software developed by the author of this article for the authentication of diverse content offers considerable potential for applications not only in the insurance sector but also in the media and journalism. The RealityChecker software, which has also been released in a GPT version with limited features for rapid access, employs a range of techniques, including forensic image analysis and optical flow, to detect forgery and fraud in the insurance sector. It also facilitates the integration of multiple analysis methods and data types, enabling insurers to make accurate and rapid decisions. This article examines the RealityChecker software, discusses its effectiveness and usefulness in detecting fraud and forgery, and demonstrates its technical approaches by providing sample codes.

**Keywords**

Insurance fraud, artificial intelligence, Reality Checker, image analysis, fake accident detection, forensic analysis.

**JEL Classification**

K14, G22

**Authors Notes:**

Assoc. Prof. Dr. Faculty of  
Communication, Department of New  
Media and Communication,  
Sivas Cumhuriyet University Digital  
Economic Research Center,  
Azerbaijan State University of Economics,  
UNEC (University of Economy)  
ORCID: 0000-0002-3630-4511  
sdarici@cumhuriyet.edu.tr

## 1. INTRODUCTION

The financial losses incurred by insurance companies as a result of insurance fraud are estimated to reach billions of dollars on an annual basis. In the United States, the estimated annual cost is approximately 308.6 billion dollars. These losses, which encompass a range of areas including health, property, and casualty insurance, illustrate the considerable financial burden borne by the industry (Insurance Information Institute, 2023; CAS Actuarial Society, 2024). In the past, insurance adjusters and a variety of manual techniques have been employed to detect fraudulent accident claims. However, these methods are both time-consuming and often inadequate. Those engaged in fraudulent activities are employing increasingly sophisticated methods to produce fake images and fake evidence, thereby rendering detection an increasingly complex process. The methods employed by fraudsters are becoming increasingly diverse, with the use of staged accidents and digitally manipulated evidence representing two notable developments. These developments have the effect of rendering fraud more difficult to detect and of placing greater pressure on insurers to adapt their existing methods (Insurance Information Institute, 2023). The need for insurers to deploy effective and innovative tools capable of detecting such fraud quickly and accurately is therefore becoming increasingly pressing. In order to prevent fraud, insurers are turning to innovative technologies such as data analytics and predictive models (CAS Actuarial Society, 2024).

The forthcoming RealityChecker software is set to become a leading solution for document and image analysis, offering comprehensive capabilities that are currently unparalleled in the industry. RealityChecker employs sophisticated analytical techniques based on advanced artificial intelligence algorithms and image processing methodologies, thereby facilitating the early identification of fraudulent and fabricated content. A version with limited features is also published as RealityChecker GPT in ChatGPT to facilitate faster and more accessible utilisation by all parties. This system, which can be employed by journalists, televangelists and citizens alike, also assists in accelerating the process and reducing costs by alleviating the workload of insurance adjusters and decision makers. RealityChecker's artificial intelligence-based approach enables higher accuracy rates in fraud detection and allows insurance companies to operate more efficiently.

The prevention of fraud is of paramount importance to the insurance industry, not only in terms of the reduction of financial losses but also in the maintenance of customer confidence. It is essential that insurance companies are able to detect fraud in a timely and effective manner in order to ensure the accurate and fair payment of claims. In this context, the technological advantages provided by RealityChecker offer significant gains for both the insurance industry and the insured.

## 2. REALITYCHECKER AND INSURANCE FRAUD DETECTION

RealityChecker employs a range of sophisticated technical analysis techniques to ascertain the veracity of an image. This bespoke artificial intelligence model is adept at detecting both artificially generated content and manual manipulations. In the context of insurance fraud detection, in particular, the analysis of fake accident images entails the utilisation of methodologies such as optical flow analysis, axis irregularities, artificial production traces, manual manipulation detection and advanced deepfake analysis. The extensive analytical capabilities of RealityChecker facilitate more efficacious combating of insurance fraud.

RealityChecker is not only capable of detecting fraud; it also provides guidance to insurance adjusters in the evaluation of complex cases. By integrating a variety of analytical techniques, this system enables a more comprehensive examination of fraud cases. A diverse range of methodologies, including optical flow analysis and artificial production traces, minimise the probability of fraud and facilitate its detection. For insurance companies, the utilisation of such a system offers significant advan-

tages in terms of both time and cost. Furthermore, the analysis provided by RealityChecker enables insurance loss adjusters to make accurate assessments by basing their decisions on more reliable data.

### 3. TECHNOLOGICAL APPROACHES

RealityChecker employs a variety of techniques to identify fraudulent activity. The subsequent analysis and methodologies presented here represent a partial overview. The code is provided as an illustrative example.

#### 3.1. Optical Flow Analysis

Optical flow analysis is a technique used to examine the movement of objects in a video sequence. Optical flow is a technique used to analyse the change of movements in a video over time. RealityChecker employs optical flow analysis to ascertain the authenticity of movements depicted in an accident scene. This analysis can be utilized to discern whether the movements in the scene are incongruous or contrived (Keçeli and Kaya, 2018). For instance, abrupt alterations in velocity or the manifestation of superhuman movements during the motion of a vehicle may indicate the fabrication of an accident. Optical flow analysis serves as a pivotal instrument in the detection of manipulated accident footage, facilitating the assessment of the veracity of accident claims by insurance adjusters.

#### Code Example (Python):

```
import cv2
import numpy as np

def analyze_optical_flow(video_path):
    cap = cv2.VideoCapture(video_path)
    ret, frame1 = cap.read()
    prvs = cv2.cvtColor(frame1, cv2.COLOR_BGR2GRAY)
    hsv = np.zeros_like(frame1)
    hsv[... , 1] = 255

    while True:
        ret, frame2 = cap.read()
        if not ret:
            break
        next_frame = cv2.cvtColor(frame2, cv2.COLOR_BGR2GRAY)
        flow = cv2.calcOpticalFlowFarneback(prvs, next_frame, None, 0.5, 3, 15, 3, 5, 1.2, 0)
        mag, ang = cv2.cartToPolar(flow[... , 0], flow[... , 1])
        hsv[... , 0] = ang * 180 / np.pi / 2
        hsv[... , 2] = cv2.normalize(mag, None, 0, 255, cv2.NORM_MINMAX)
        bgr = cv2.cvtColor(hsv, cv2.COLOR_HSV2BGR)
        cv2.imshow('Optical Flow', bgr)
        prvs = next_frame
        if cv2.waitKey(30) & 0xFF == ord('q'):
            break
    cap.release()
    cv2.destroyAllWindows()
```

#### 3.2. Axis Irregularities and Manipulation Analysis

RealityChecker identifies anomalies and discrepancies by examining multiple elements of an image. Discrepancies in the positioning of light sources can indicate the presence of artificial manipulation. For instance, if the shadows cast by different objects fall in disparate directions or the light sources are inconsistent in an accident scene, it may be indicative of forgery. Such inconsistencies may result from manual edits or the rendering of images with inaccurate lighting (Kee et al., 2014)

**Code Example (Python - Light Mismatch Detection):**

```

import cv2
import numpy as np

def detect_light_inconsistencies(image_path):
    # Görüntüyü yükle
    image = cv2.imread(image_path)

    # Gri tonlamalı görüntüye dönüştür
    gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)

    # Kenarları tespit et (Canny algoritması kullanarak)
    edges = cv2.Canny(gray, threshold1=100, threshold2=200)

    # Kenar tespitini görüntüle
    cv2.imshow('Detected Edges', edges)

    # Kullanıcı pencereyi kapatana kadar bekle
    cv2.waitKey(0)
    cv2.destroyAllWindows()

# Kullanım örneği
detect_light_inconsistencies('kaza_goruntusu.jpg')

```

**3.3. Forensic Image Analysis**

RealityChecker employs Error Level Analysis (ELA) and EXIF data analysis to ascertain whether an image has undergone digital manipulation. This method is employed to identify alterations made to the image. For instance, if the error level is higher in certain regions of a photograph taken after an incident, this may suggest that these regions have been digitally modified. Error Level Analysis (ELA) and EXIF data analysis are forensic techniques commonly used to detect manipulation of digital images. ELA reveals possible edits by analysing compression errors in different regions of an image. EXIF data analysis analyses the metadata of the image, evaluating information such as the time of capture, the device used and the settings. These methods are particularly effective in cases where forgery is suspected (Krawetz, 2007). ELA and EXIF analysis are effective techniques for detecting suspected forgeries, and RealityChecker significantly reduces the probability of fraud through this type of analysis.

**Code Example (Python - ELA):**

```

from PIL import Image, ImageChops, ImageEnhance

def analyze_ela(image_path):
    original = Image.open(image_path)
    ela_path = 'ela_image.jpg'
    original.save(ela_path, 'JPEG', quality=90)
    ela_image = Image.open(ela_path)
    ela_diff = ImageChops.difference(original, ela_image)
    extrema = ela_diff.getextrema()
    max_diff = max([e[1] for e in extrema])
    scale = 255.0 / max_diff if max_diff != 0 else 1
    ela_diff = ImageEnhance.Brightness(ela_diff).enhance(scale)
    ela_diff.show()

```

**3.4 Manual Manipulation Detection**

Manual manipulation detection in imagery involves analysing inconsistencies introduced during digital editing processes. Techniques such as detecting lighting inconsistencies, colour tone changes and object substitutions are crucial in identifying tampered regions (Farid, 2009). RealityChecker is a software tool that analyses changes made to images using digital editing software such as Photoshop and GIMP, as well as inconsistencies in the objects and lighting in images, in order to detect instances of manual manipulation. It is capable of identifying instances of face or object substitution, as well as discrepancies in lighting and colour tone manipulation. As an example, it can be used to detect the addition of an object to an image after an accident, by analysing the light sources and shadows present.

### Code Example (Python - Object Replacement Detection):

```

import cv2
import numpy as np

def detect_object_replacement(image_path):
    image = cv2.imread(image_path)
    gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
    orb = cv2.ORB_create()
    keypoints, descriptors = orb.detectAndCompute(gray, None)
    image_with_keypoints = cv2.drawKeypoints(image, keypoints, None, color=(0, 255, 0))
    cv2.imshow('Keypoints', image_with_keypoints)
    cv2.waitKey(0)
    cv2.destroyAllWindows()

```

### 3.5. Deepfake Detection

The advent of deepfake technology has led to a notable rise in the prevalence of fake content. The detection of deepfake videos is of critical importance in the identification of such content. Optical flow and motion analysis represent effective methods for detecting deepfakes, particularly through the examination of elements such as facial manipulations, unnatural movements and audio synchronisation. RealityChecker employs optical flow and motion analysis to identify instances of deepfake content. The examination of specific characteristics, such as facial manipulations, unnatural movements, and audio synchronisation, is a crucial aspect of detecting deepfakes (Amerini et al., 2019). For instance, minor delays in a person's facial expression or anomalous facial movements may be indicative of a forgery created using deepfake technology.

### Code Example (Python - Deepfake Optical Flow Detection):

```

import cv2
import numpy as np

def detect_deepfake_optical_flow(video_path):
    cap = cv2.VideoCapture(video_path)
    ret, frame1 = cap.read()
    prvs = cv2.cvtColor(frame1, cv2.COLOR_BGR2GRAY)
    hsv = np.zeros_like(frame1)
    hsv[... , 1] = 255

    while True:
        ret, frame2 = cap.read()
        if not ret:
            break
        next_frame = cv2.cvtColor(frame2, cv2.COLOR_BGR2GRAY)
        flow = cv2.calcOpticalFlowFarneback(prvs, next_frame, None, 0.5, 3, 15, 3, 5, 1.2, 0)
        mag, ang = cv2.cartToPolar(flow[... , 0], flow[... , 1])
        hsv[... , 0] = ang * 180 / np.pi / 2
        hsv[... , 2] = cv2.normalize(mag, None, 0, 255, cv2.NORM_MINMAX)
        bgr = cv2.cvtColor(hsv, cv2.COLOR_HSV2BGR)
        cv2.imshow('Deepfake Optical Flow', bgr)
        prvs = next_frame
        if cv2.waitKey(30) & 0xFF == ord('q'):
            break
    cap.release()
    cv2.destroyAllWindows()

```

### 3.6. Advanced Manipulation Detection

RealityChecker employs a sophisticated algorithmic approach to analyse the visual inconsistencies present in an image, with the objective of detecting instances of advanced manipulation, including the creation of fake accident scenes. Furthermore, it is capable of identifying the artificial intelligence techniques employed in the fabrication of fictitious events. To illustrate, if an accident scene was indeed generated through the use of computer-generated imagery (CGI), RealityChecker is able to discern this through its ability to assess the physical behaviour of objects within the scene and ascertain whether it aligns with the laws of physics. In order to detect the presence of deepfakes and other forms of facial manipulation, it is essential to undertake a detailed analysis of the visual artefacts present in the images in question. In particular, it is of great importance to identify any physical inconsistencies

that may be present in the images, as these can provide valuable clues as to their authenticity (Matern et.al., 2019). The capacity to detect advanced manipulation is particularly beneficial in instances of more intricate fraud, and RealityChecker’s proficiency in this regard represents a significant advantage for insurance companies.

### Code Example (Python - Advanced Manipulation Detection):

```

import cv2
import numpy as np

def detect_advanced_manipulation(image_path):
    image = cv2.imread(image_path)
    lab = cv2.cvtColor(image, cv2.COLOR_BGR2LAB)
    l, a, b = cv2.split(lab)
    clahe = cv2.createCLAHE(clipLimit=3.0, tileGridSize=(8, 8))
    cl = clahe.apply(l)
    limg = cv2.merge((cl, a, b))
    final = cv2.cvtColor(limg, cv2.COLOR_LAB2BGR)
    cv2.imshow('Advanced Manipulation Detection', final)
    cv2.waitKey(0)
    cv2.destroyAllWindows()

```

### 3.7. Machine Learning Model Prediction

The detection of fake images produced by Generative Adversarial Networks (GAN) and the determination of the specific GAN model used to create them is possible through the analysis of the distinctive “fingerprints” associated with different GAN models. This approach enables the identification of the source of the fake images (Yu et. al., 2019). RealityChecker employs deep learning-based classifiers to ascertain the provenance of an image, specifically identifying the AI model (e.g., DALL-E, MidJourney, Stable Diffusion) responsible for its generation. Such tools are of particular utility in the context of insurance fraud detection, where they can be employed to identify instances of artificially generated content. To illustrate, if an AI-generated image of an accident is presented as evidence of a real accident, a RealityChecker-like system can recognise this and alert the insurance company. In light of the growing prevalence of AI-based fake content, the importance of such model prediction tools is increasing.

### Code Example (Python - Model Prediction):

```

import tensorflow as tf
from tensorflow.keras.models import load_model
import numpy as np
from PIL import Image

def predict_ai_model(image_path, model_path):
    model = load_model(model_path)
    image = Image.open(image_path).resize((224, 224))
    image_array = np.array(image) / 255.0
    image_array = np.expand_dims(image_array, axis=0)
    prediction = model.predict(image_array)
    model_names = ['DALL-E', 'MidJourney', 'Stable Diffusion']
    predicted_model = model_names[np.argmax(prediction)]
    print(f'The image was likely generated by: {predicted_model}')

# Kullanicim
# predict_ai_model('image.jpg', 'ai_model_classifier.h5')

```

## 4. USING REALITYCHECKER IN DIFFERENT FRAUD TYPES

RealityChecker has the potential to be utilised in the detection of a multitude of fraudulent and forged transactions within the insurance sector. The following section will present a selection of areas in which it can be employed, accompanied by illustrative scenarios.

#### **4.1. Health Insurance Fraud**

In a scenario where hospitals submit fraudulent or exaggerated invoices to claim payment from insurance, RealityChecker identifies digital manipulations by subjecting patient records and invoices to ELA analysis. This is achieved through the utilisation of OCR technology, which enables the automatic analysis of reports and the detection of anomalous patterns.

#### **4.2. Life Insurance Fraud**

In the event of fraudulent death certificates or identity theft, RealityChecker is capable of detecting any alterations made to the content of the documents in question. Furthermore, it is able to verify the authenticity of digital documents through the use of EXIF analysis.

#### **4.3. Car Insurance Fraud**

In a scenario where fictitious traffic accidents are staged with the intention of obtaining insurance benefits through deception, RealityChecker is capable of identifying inconsistencies in movement, perspective, and the use of computer-generated imagery through the application of optical flow and deep learning-based analytical techniques.

#### **4.4. Property Insurance Fraud**

In circumstances where damage to a residence or business premises is exaggerated, RealityChecker is able to identify inconsistencies in the reported damage through a comparative analysis of images captured before and after the incident. Additionally, it can detect unusual angles of objects and the extent of deliberate damage.

#### **4.5. Transportation Insurance Fraud**

In the context of insurance claims pertaining to the theft or damage of goods, RealityChecker is capable of discerning any instances of digital manipulation through the examination of photographic documentation of the transported items, video footage, and pre- and post-incident digital data.

#### **4.6. Cyber Attack Insurance Fraud**

In the event of insurance claims based on false accusations of cyberattacks, RealityChecker is capable of detecting and verifying the accuracy of any subsequent edits to digital evidence.

### **5. BENEFITS OF REALITYCHECKER FOR THE INSURANCE INDUSTRY**

RealityChecker has the potential to confer a number of advantages upon insurers, operating in a variety of contexts. These include:

#### **Fast Decision Making**

The capacity for rapid decision-making is a further advantage. The detection of fraudulent activity can be accomplished with greater alacrity than is possible with traditional methods. It is widely acknowledged within the insurance industry that the timely detection of fraud is of paramount importance. To illustrate, the necessity for manual forensic examinations in the detection of fake accidents can result in delays due to the extended processing time required. RealityChecker is capable of comple-

ting this process in a matter of minutes, due to the integration of advanced optical flow analysis and forensic image analysis. The utilisation of optical flow analysis to ascertain the consistency of movements within an accident image enables the immediate detection of potential fraud. Furthermore, the utilisation of automated deep learning models facilitates the attainment of more expeditious results. For instance, the identification of anomalous vehicular movements in a fabricated accident enables insurance specialists to expeditiously reach accurate conclusions. Time is a pivotal element for insurance enterprises. RealityChecker is capable of scrutinizing purported accident claims in a brief interval through techniques such as optical flow analysis and sophisticated manipulation detection. The optical flow approach, which assesses the velocity of an incident and the plausibility of the associated movements, facilitates the expeditious detection of fictitious claims.

### **Higher Accuracy Rates**

The application of sophisticated image analysis techniques has led to a notable enhancement in the accuracy of claim detection. While manual methods are susceptible to human error, the use of advanced techniques such as ELA (Error Level Analysis) and deep learning-based model predictions in RealityChecker has resulted in more precise outcomes by reducing the likelihood of human error. The combination of EXIF data and ELA, for instance, has enabled the effective identification of manipulated images. This approach has led to the attainment of remarkably high accuracy rates in the detection of fake accident images.

### **Cost Savings**

The prevention of fraudulent accident claims has the dual benefit of reducing insurance companies' costs and increasing their profitability. The RealityChecker system is designed to work faster and more efficiently than manual reviews, thereby saving insurance companies time and labour. The use of deepfake detection and advanced manipulation analysis to identify fake images is an effective method of preventing false payments, which in turn reduces companies' annual losses and increases cost efficiency.

### **Improved Customer Experience**

The RealityChecker is capable of detecting both manual and AI-based manipulations. In the case of manual manipulations, which may be carried out using tools such as Photoshop or GIMP, the software analyses object replacement and lighting mismatches in order to identify such alterations. Conversely, AI-based manipulations, which may take the form of deepfakes, are determined by means of optical flow analysis and model estimation methods. This versatility provides insurance companies with a robust defence against all types of fraud attempts.

### **Versatile Manipulation Analysis**

RealityChecker is capable of detecting both manual and AI-based manipulations. For example, manual manipulations (changes made with tools such as Photoshop, GIMP) are detected by analysing object replacements and lighting mismatches, while AI-based manipulations (e.g. deepfakes) are identified by optical flow analysis and model estimation. This versatility provides insurance companies with a robust defence against all types of fraud attempts.

### **Automatic Improvement with Machine Learning**

The RealityChecker system is equipped with machine learning capabilities that enable it to self-

improve based on user feedback. The incorporation of user feedback into the machine learning model prediction and improvement processes ensures that the system is consistently updated and optimized to combat emerging fraud methods.

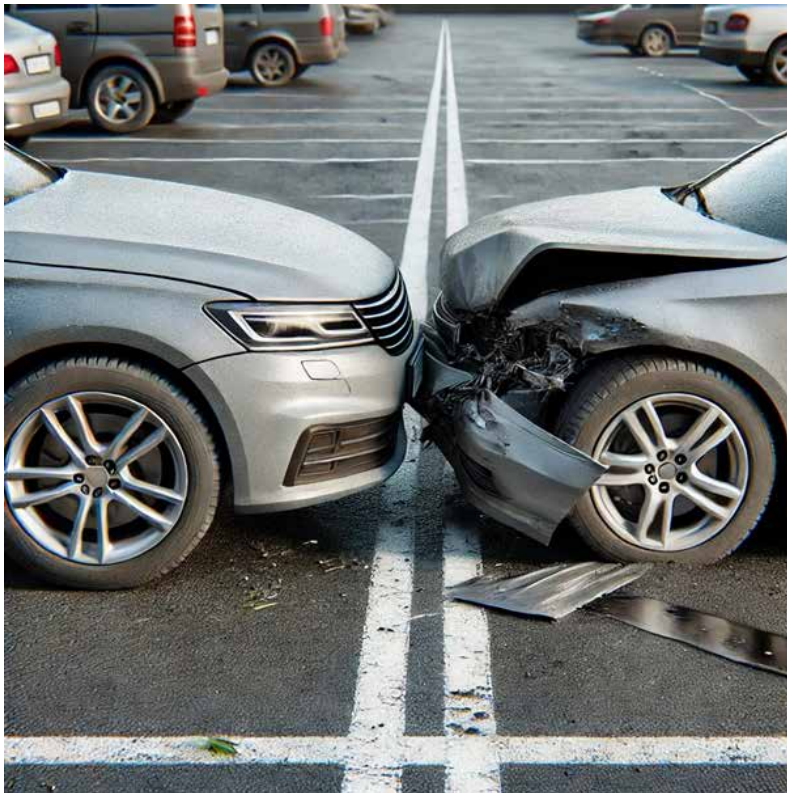
## 6. SAMPLE REVIEW

In order to demonstrate the efficacy of RealityChecker's analysis of accident photos, two photos were analysed using the GPT version. Two additional accident photos were created using the ChatGPT 4 model. RealityChecker GPT was then tasked with examining these images for insurance fraud. The photos and their analysis are provided below for reference.

### ACCIDENT SCENE 1

#### Image 1

Car accident scene photo produced by ChatGPT.



#### 1- Detection of GAN (Generative Adversarial Network) Traces:

**Method:** The methodology employed is as follows: The image was subjected to a grayscale transformation and a Gaussian blurring operation in order to reveal any anomalies present in the pixels. This process was undertaken to identify typical GAN traces (Generative Adversarial Network) in images generated by artificial intelligence. In GAN-based image productions, certain smooth areas and symmetrical errors can be observed.

**Findings:** As a result of this analysis, smoothness and disproportionate transitions were detected in the collision area. These transitions draw attention as unexpected flat and excessively smooth areas in a natural photo. In particular, the pixel structure at the collision point of the vehicles does not show the expected irregularity; this is a feature frequently seen in an artificially generated image.

## GAN Artifacts Detection



### 2- Structural Anomaly Detection (Consistency of Object Boundaries):

**Method:** A Canny Edge Detection Algorithm was employed for the purpose of verifying the structural consistency of the image. The algorithm in question is designed to analyse the boundary regions and edge density. In artificial intelligence-generated scenes, the boundaries between objects frequently fail to reflect the natural transitions observed in real-world scenes. These boundaries may be artificially sharp or irregular.

**Findings:** The analysis revealed the presence of unnaturally sharp boundaries and irregularities in the collision area and in the vicinity of the vehicles. Such irregularities are a common feature of AI-generated or processed images. The anomalies observed at the boundaries of the vehicles suggest that the scene is not real.

### Boundary Consistency Check for Structural Anomalies



### **3- Object Consistency and Semantic Segmentation**

This analysis employed a type of “simulated segmentation” to evaluate object boundaries and consistency in the image. In this method, the boundaries of the objects were analysed with edge detection and expansion techniques. The resulting data are as follows:

#### **3-1. Simulated Object Boundaries**

The edge detection algorithm serves to highlight the boundaries of objects in the image, particularly in the case of colliding vehicles. These boundaries demonstrate the manner in which the objects in question interact with one another physically. It is worthy of note that in the collision zone, the boundaries of the vehicles display a sharpness and regularity that is unexpected. In a real collision scene, the boundaries should manifest greater irregularity and incompatibility with deformation.

#### **3-2. Logical Object Placement**

The physical interaction between the two colliding vehicles does not align with the deformation expectations typically observed in natural collisions. The smooth and regular boundaries at the collision point indicate that the two objects (vehicles) are structurally incompatible. This is a characteristic commonly observed in AI-generated or manipulated scenes, reflecting a lack of realistic physical deformation and interaction.

#### **3-3. Boundary Conformity and Object Consistency**

The clear and artificial separation of the boundaries in the image lends further support to the hypothesis that the scene is an artificial production rather than a real collision. In a real scene, the expected fractures and irregularities in the boundaries of the vehicles after a collision are not visible here.

### **Technical Evaluation and Conclusion**

The results of the simulated semantic segmentation and object consistency analysis yielded findings that lend support to the hypothesis that the image was generated by artificial intelligence. Nesnelerin sınırları pürüzsüz ve doğal olmayan bir şekilde belirgin.

- The object boundaries are observed to be smooth and unnaturally distinct.
- In contrast to the anticipated physical deformations following the collision, the boundaries are observed to be artificially separated.

The data presented here provides scientific evidence that the image is not a natural scene, but rather the result of artificial generation or editing.

## Simulated Segmentation Boundaries (Object Consistency)

### Simulated Segmentation Boundaries (Nesne Tutar)



## 4- Shadow and Reflection Discrepancies

### 4-1. Detection of Shadow Areas

**Method:** The image was binarised using a specific threshold value in order to identify areas of darker intensity, namely shadows. This process enabled the separation and analysis of shadow regions.

**Findings:** The distribution of shadows in the collision area does not fully align with the anticipated natural shadow distribution in a real-world scenario, given the physical interactions between the vehicles. The shadows cast by the vehicles at the bottom are not sufficiently distinct, and the impression of a natural light source is weak. In the case of a close collision between vehicles, the shadows should exhibit greater complexity and irregularity. This indicates that the distribution of shadows may be artificial or inconsistent.

### Shadow Detection (Potential Shadow Regions)



## 4-2. Reflection Analysis

**Method:** The image contrast was increased in order to facilitate an examination of the metal reflections on the surface of the vehicles. The high-contrast analysis facilitated the comprehension of any unnatural brightness or light intensities present on the surfaces of the vehicles.

**Findings:** In the reflection analysis, the light distribution on the metal surfaces of the vehicles appeared unnaturally dense and scattered. Particularly in the collision area, the reflection was not as expected, indicating that the light source was not modelled in a natural manner. This is a common occurrence in AI-generated scenes, as AI models can experience difficulty in realistically simulating light and reflection transitions.

Reflection Analysis (Increased Contrast)



## Technical Evaluation and Conclusion

The analysis of shadow and reflection inconsistencies yielded several key findings that suggest the light distribution and shadow locations in the scene are unnatural:

- The shadows cast on the undersides of vehicles are either absent or irregular, which is an unusual occurrence in natural lighting conditions.
- Furthermore, the distribution of reflections on metal surfaces is deemed to be implausible and does not appear to correlate with the light source.

These findings lend further support to the hypothesis that the image is an AI-generated scene.

## 5- Physical Deformation and Damage Consistency Analysis

This analysis evaluated the deformation and damage regions in the image through the examination of high-frequency components. The analysis of the damage and high-frequency components of the moment of impact (i.e., significant deformation and fractures) yielded the following findings:

### 5-1. The Damage Area Should Be Smooth and Regular

The high-frequency components in the collision region exhibit a smooth and regular structure, which contrasts with the irregular and fragmented deformation that would be expected in a real collision.

This suggests that the fracture and bending density of the metal resulting from the collision differs from that observed in a real accident.

### 5-2. Unnatural Edge Sharpness

The collision areas exhibit an unnatural sharpness of edge. In a genuine collision, these areas would manifest less definition and irregularity due to fracture, bending, and intricate deformations. However, in this image, the lines and edges within the collision area appear unexpectedly sharp and regular.

### 5-3. Inconsistency of High Frequency Components

It can be observed that there is no discernible structural deformation pattern at the impact point. This may be indicative of the hypothesis that the image was created as a result of an artificial impact scenario or manipulation.

### Technical Evaluation and Conclusion

The analysis of physical deformation based on high-frequency analysis indicates that the deformations at the collision point do not align with the principles of physical reality. This finding lends support to the hypothesis that the image in question has been generated or manipulated artificially, rather than representing a genuine collision. Such smooth and regular deformations are not anticipated in a genuine collision.

#### Physical Deformation and Damage Consistency (High-Frequency Analysis)



### 6- Noise Analysis Around the Collision Area

The objective of this analysis was to ascertain whether the damage area was the result of natural causes. To this end, the noise levels in the crash area were compared with those in another area. It was hypothesised that noise levels may reflect irregularities in the pixels, indicating the presence of fake or artificial arrangements.

#### 6-1. Noise Level at Collision Site

The standard deviation of the noise level at the collision site was found to be 67.45. The elevated noise value may be indicative of anomalous noise levels and anticipated irregularities in the pixels. This

may indicate that the damage area may have been fabricated or artificially created.

## 6-2. Noise Level in Collision-Free Zone

The standard deviation of the noise level in another reference region (the area outside the collision) is 58.82. The lower noise level indicates that the pixelation structure in this region of the image is more natural.

### Technical Evaluation and Conclusion

A comparison of the noise levels reveals that the noise level in the area of the crash is higher than in other areas. This type of discrepancy is particularly prevalent in instances of artificial damage created by artificial intelligence or manual editing. Consequently, the divergence in noise levels observed in the area of the crash provides compelling evidence that this region may have been subjected to editing or artificial creation.

Collision Area (Noise STD: 67.45)



Non-Collision Area (Noise STD: 67.45)



## ACCIDENT SCENE 2

### Image 2

Car accident scene photo produced by ChatGPT



## 1- Physical Deformation and Damage Consistency Analysis

The objective of this analysis is to ascertain whether the deformations are attributable to a genuine physical phenomenon by examining the high-frequency components in the region of damage. The investigation of the high-frequency components in the damage and deformation area yielded the following findings:

### 1-1. Smooth and Regular Structure of the Damage Area

In the area of the vehicle exhibiting damage at the rear, the high-frequency components display a greater degree of regularity and smoothness than might be anticipated. In a genuine impact, it is to be expected that the metal will undergo complex deformations in the direction of bending and breaking. In this instance, however, the edges of the scratches and breaks appear quite regular and sharp, which may indicate that the damage is not genuine.

### 1-2. Unnatural Edge Sharpness

The edge sharpness of the scratches and fracture marks in the impact zone exhibits a pattern that is not consistent with the expected characteristics of physical deformations resulting from a real impact. In contrast to this, surface irregularities and more complex fractures are expected in the case of real damage.

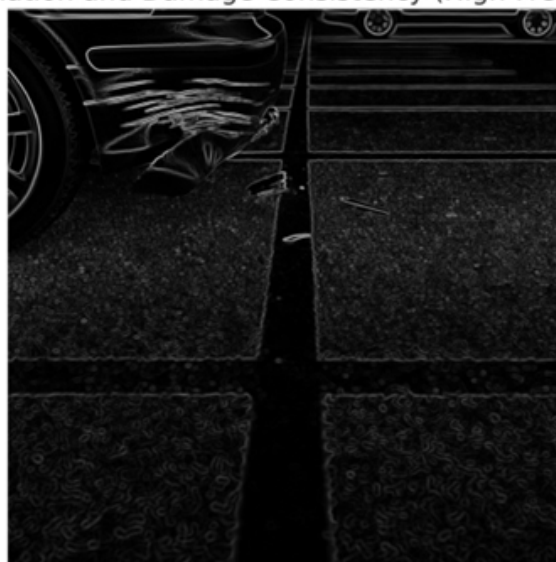
### 1-3. Incompatibility of High Frequency Components

The absence of expected irregularities and the presence of sharp lines in the damage area indicate that the image may have been created or edited in a manner that is not consistent with the known characteristics of the phenomenon under observation.

## Technical Evaluation and Conclusion

This high-frequency analysis shows that the deformations in the damage area do not follow natural physical rules. The damage traces appear to be the result of a digital manipulation rather than a real collision. This strengthens the possibility that the image contains fake accident damage.

### Physical Deformation and Damage Consistency (High-Frequency Analysis)



## 2- Shadow and Reflection Consistency Analysis

The objective of this analysis was to ascertain whether the shadows and surface reflections observed in the vicinity of the vehicle were consistent with the light and shadow conditions that would be expected in a real-world setting.

### 2-1. Shadow Consistency Analysis

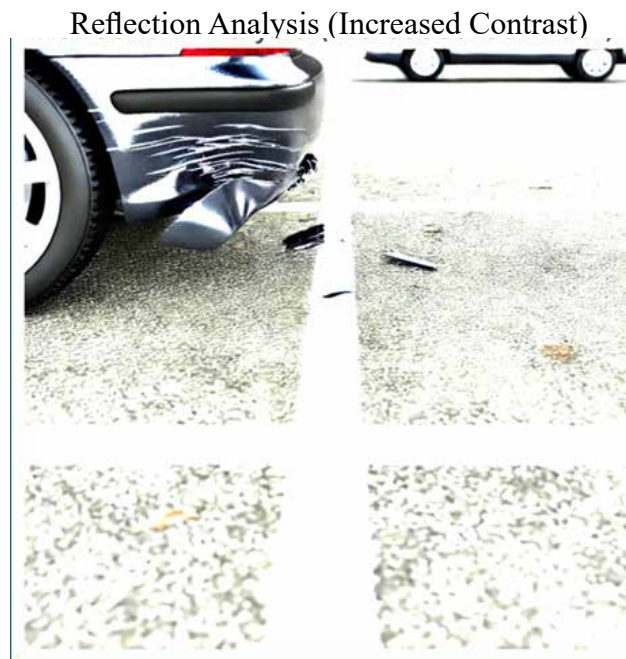
The threshold value was applied to determine the presence of dark areas in the image, which were then subjected to shadow detection. Upon examination of the shadow areas in the image, it was observed that the damage area of the vehicle exhibited less distinct shadow reflections than would be expected. Additionally, the distribution of shadows did not align with the intensity and direction that would be anticipated based on the physical interaction caused by a real collision. This observation may suggest that shadows are not formed under a natural light source or are arranged in a manner that is not representative of real-world conditions..

Shadow Detection (Potential Shadow Regions)



### 2-2. Reflection Consistency Analysis

The contrast has been increased in order to make the reflections more noticeable. The reflections on the metal surface of the vehicle show a discordant glare and scattering, depending on the light source. The metal reflections in the impact area are more homogeneously distributed than would be expected in a natural environment. There is an unnatural brightness, especially around the impact marks, which gives rise to the suspicion that the image may have been generated by AI or digitally edited.



### Technical Evaluation and Conclusion

The analysis of shadow and reflection consistency in the image indicates that the distribution of shadows and surface reflections in the area of impact do not align with the characteristics of a natural light source. These discrepancies reinforce the hypothesis that the image is not an authentic representation of a collision event, but rather a digitally created or manipulated image.

### 7. Conclusion and Recommendations

It is imperative that the ever-changing technologies and innovations of the digital world in the insurance sector are closely monitored. While digital transformation offers significant opportunities for the insurance sector, it also gives rise to an increase in fraud and forgery attempts. It is therefore imperative that the sector monitors these developments closely and deploys the relevant technologies in an effective manner to combat fraud. The structure of the digital world, which requires a high level of technical and complex knowledge, can make it challenging to achieve rapid results in the application of specific analyses and methods. Nevertheless, sophisticated software such as RealityChecker and AI-powered GPT models have the potential to enhance the efficacy and expediency of these processes. Such technologies significantly streamline the decision-making processes of insurance companies by conducting intricate data analyses in a relatively short time. In addition to mitigating the risk of human error, this increases the competitive advantage of insurance companies by enabling the formulation of more precise data-driven decisions.

The insurance sector requires innovative solutions to combat fraud, which offer significant advantages in terms of both time and cost. Conventional methodologies are often both time-consuming and costly in terms of fraud detection. Consequently, the implementation of artificial intelligence and data analytics-based approaches represents a pivotal step for the sector. Advanced systems such as RealityChecker confer a number of advantages upon insurance companies, most notably in the efficiency with which fraud detection and prevention processes may be conducted. These advantages extend beyond mere cost reduction, with a concomitant increase in customer satisfaction.

Further studies should concentrate on the advancement of RealityChecker and the enhancement of fraud detection rates through the incorporation of machine learning models. Furthermore, the integration of additional data sources utilised within the sector into such artificial intelligence systems will facilitate the early detection of fraud. Models developed through the application of machine learning

and deep learning techniques can be significantly more effective in predicting fraudulent activities and taking preventive measures in advance.

It is also crucial for insurance companies to enhance awareness and provide training to their employees and business partners regarding these technological advancements. Having a workforce capable of utilising technology proficiently will optimise the advantages offered by software and artificial intelligence solutions in the fight against fraud. In this regard, enhancing employees' capacity to adapt to technology and fostering their ongoing awareness of evolving fraud techniques will contribute to the long-term prosperity of the sector.

Consequently, the adoption of digital transformation and the utilisation of AI-powered solutions to effectively combat fraud in the insurance industry has become imperative, rather than merely optional. The integration of technological innovations and AI-based solutions into the operational framework of insurance companies will not only enhance the efficacy of fraud prevention measures, but also optimise operational efficiency and enhance customer satisfaction.

## REFERENCES

- Amerini, I., Galteri, L., Caldelli, R., & Del Bimbo, A. (2019). Deepfake video detection through optical flow based cnn. In Proceedings of the IEEE/CVF international conference on computer vision workshops (pp. 0-0).
- CAS Actuarial Society. (2024). The economics of insurance fraud investigation: Balancing costs and savings. *Variance: Advancing the Science of Risk*, 4(2), 173–174. Erişim Tarihi: 10.10.2024. [www.casact.org](http://www.casact.org)
- Farid, H. (2009). Image forgery detection. *IEEE Signal processing magazine*, 26(2), 16-25.
- Insurance Information Institute. (2023). Background on insurance fraud. Insurance Information Institute. Access Date: 7.10.2024. <https://www.iii.org>
- Keçeli, A. S., & Kaya, A. (2018). Optik Akış Görüntüsü ve Bi-Lstm ile Şiddet İçeren Hareketlerin Sınıflandırılması. *Avrupa Bilim ve Teknoloji Dergisi*, (14), 204-208.
- Kee, E., O'brien, J. F., & Farid, H. (2014). Exposing Photo Manipulation from Shading and Shadows. *ACM Trans. Graph.*, 33(5), 165-1.
- Krawetz, N., & Solutions, H. F. (2007). A picture's worth. *Hacker Factor Solutions*, 6(2), 2.
- Matern, F., Riess, C., & Stamminger, M. (2019, January). Exploiting visual artifacts to expose deepfakes and face manipulations. In 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW) (pp. 83-92). IEEE.
- RealityChecker GPT. (2024). <https://chatgpt.com/g/g-X4g0cyDSm-realitychecker>
- Yu, N., Davis, L. S., & Fritz, M. (2019). Attributing fake images to gans: Learning and analyzing gan fingerprints. In Proceedings of the IEEE/CVF international conference on computer vision (pp. 7556-7566).