

A
PROJECT REPORT
ON
PAN CARD TAMPERING DETECTION SYSTEM

Submitted in partial fulfillment of the requirement for

the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

BY

R.Gopichand (20P61A1284)

K.Rajesh (21P65A1209)

N.Dhanush (20P61A1268)

Under the esteemed guidance of

Ms. P.Sony

Associate Professor, Dept of IT



Department of Information Technology

VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Accredited by NBA, NAAC, Permanently Affiliated to JNTUH)

Aushapur (v), Ghatkesar (m), Medchal.dist, TELANGANA-501301

Academic Year 2023-24



VIGNANA BHARATHI
Institute of Technology



AUSHAPUR (V), GHATKESAR (M), MEDCHAL.DIST-501301

Department of Information Technology

CERTIFICATE

This is to certify that the project entitled **“PAN CARD TAMPERING DETECTION SYSTEM”** is being submitted by **R.GOPICHAND (20P61A1284), K.RAJESH (20P65A1209), N.DHANUSH (20P61A1268)** in partial fulfillment of the requirement for the award of the degree of **Bachelor of Technology in Information Technology** is a record of bonafide work carried out by them under the guidance and supervision during the academic year 2023-2024.

The results embodied in this project report have not been submitted to any other University for the award of any degree or diploma.

Internal Guide

Ms.P.Sony

(Asst Professor)

Department of IT

Head of the Department

Dr.K.Kalaivani

Department of IT

Project Coordinator

Mr.K.Venkat Reddy

(Asst Professor)

Department of IT

External Examiner

Name:

College:



VIGNANA BHARATHI
Institute of Technology



AUSHAPUR (V), GHATKESAR (M), MEDCHAL.DIST-501301

Department of Information Technology

DECLARATION

We, **R.GOPICHAND** bearing hall ticket number **20P61A1284**, **K.RAJESH** bearing hall ticket number **21P65A1209** and **N.DHANUSH** bearing hall ticket number **20P61A1268**, hereby declare that the project report entitled “**PAN CARD TAMPERING DETECTION SYSTEM**” under the guidance of **Ms.P.Sony**, Department of Information Technology, **VBIT**, Hyderabad, is submitted in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Information Technology.

This is a record of bonafide work carried out by us and the results embodied in this project have not been reproduced or copied from any source. The results embodied in this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

R.GOPICHAND (20P61A1284)

K.RAJESH (21P65A1209)

N.DHANUSH (20P61A1268)

ACKNOWLEDGEMENT

First and foremost, we wish to express our gratitude towards the institution “**Vignana Bharathi Institute of Technology**” for fulfilling the most cherished goal of our life to do Bachelor of Technology.

It is great pleasure in expressing deep sense of gratitude to our **Internal guide, Ms.P.Sony**, Asst. Professor, Department of Information Technology for her valuable guidance and freedom she gave to us.

We also express our sincere thanks to **Mr.K.Venkat Reddy, B.Tech Coordinator** for his encouragement and support throughout the project.

It is great pleasure in expressing deep sense of gratitude **Dr.K.Kalaivani**, Head of Department, Department of Information Technology for her valuable guidance.

We take immense pleasure in thanking **Dr. P. V. S. Srinivas Principal, Vignana Bharathi Institute of Technology, Ghatkesar** for having permitted us to carry out this project work.

Our outmost thanks also go to all the **FACULTY MEMBERS** and **NON-TEACHING STAFF** of the Department of Information Technology for their support throughout our project work

R.GOPICHAND (20P61A1284)

K.RAJESH (21P65A1209)

N.DHANUSH (20P61A1268)

ABSTRACT

The Permanent Account Number (PAN) Card is an important document that serves as an identification tool for many more purposes like tax payment, verification medium in banks, companies and in other government services in India. However, with the increasing demand for PAN Cards, fraudulent activities involving fake PAN Cards have also increased. For this project we will calculate the structural similarity of the original PAN card and the PAN card uploaded by the user. This is the soul of this project. Similarly in this project with the help of image processing involving the techniques of computer vision we are going to detect that whether the given image of the PAN card is original or tampered (fake) PAN card.

INDEX

CONTENT	PAGE NUMBER
Certification	
Acknowledgement	
Abstract	
List of Figures	
1. INTRODUCTION	1
1.1 Motivation	2
1.1.1 Overview of Existing System	2
1.1.2 Overview of Proposed System	2
1.1.3 System Features	3
1.2 Problem definition	3
1.3 Objective of Project	3
1.4 Scope of Project	3
2 LITERATURE SURVEY	4
3. SYSTEM ANALYSIS	7
3.1 System architecture	8
3.1.1 Architecture Diagram	8
3.1.1.2 Structural Similarity Index (SSIM):	9
3.1.1.3 Computer Vision:	11
3.1.1.4 Working:	11
3.2 Operating Requirements	13
4. SYSTEM DESIGN	14
4.1 UML diagrams	15
5. IMPLEMENTATION	21
5.1 Sample code	17
6. OUTPUT SCREENS	27
6.1 Home Screen	28
6.2 Image Uploading	29
6.3 Image is uploaded & it is real	30
7. TESTING & DEBUGGING	31
7.1 Types of tests	32
7.1.1 Unit Testing	32
7.1.2 Integration Testing	32
7.1.3 Functional Testing	33
7.1.4 White box Testing	33

7.1.5 Black Box Testing	33
7.1.5.1 Test Strategy and Approach	33
7.1.5.2 Test Objectives	34
7.1.5.3 Features to be Tested	34
7.1.6 Integration Testing	34
7.1.7 Acceptance Testing	34
7.2 Test cases	35
8. CONCLUSIONS	37
9. FUTURE ENHANCEMENTS	39
10. REFERENCES	41

LIST OF FIGURES

Fig 3.1.1:Architecture Diagram	8
Fig 4.1 Use case diagram	16
Fig.4.2 Class diagram	17
Fig. 4.3 Sequence diagram	18
Fig. 4.4 Deployment diagram	19
Fig. 4.5 Activity diagram	20

CHAPTER 01

INTRODUCTION

01.INTRODUCTION

The Permanent Account Number (PAN) Card is a very important document for taxpayers in India, as it provides a unique identification number for various financial transactions. However, the increasing demand for PAN Cards has led to an increase in fraudulent activities involving fake PAN Cards, which can be used for tax fraud and other financial crimes. As such, it is essential to have a system in place to detect fake and real PAN Cards. For this project we will calculate the structural similarity of the original PAN card and the PAN card uploaded by the user. This is the soul of this project. Similarly in this project with the help of image processing involving the techniques of computer vision we are going to detect that whether the given image of the PAN card is original or tampered (fake) PAN card.

The PAN card is a vital identification document issued by the Income Tax Department of India and is primarily used for tax-related purposes. It contains important personal and financial information, including the individual's name, date of birth, photograph, and a unique alphanumeric PAN number.

The act of tampering with a PAN card can involve various forms of forgery, alteration, or unauthorized changes to the card's details. Pan card tampering is illegal and unethical, and those who engage in such activities may face severe legal consequences.

Common forms of pan card tampering may include:

1.Forged PAN Cards: Criminals may create counterfeit PAN cards with fictitious or altered information to evade taxes, engage in fraudulent financial transactions, or impersonate someone else.

2.Altered Personal Details: Tampering with the cardholder's name, date of birth, photograph, or other personal details to create a false identity.

3.Falsified Financial Information: Changing the financial details, such as income or investments, to fraudulently obtain benefits or tax concessions.

4.Duplicate PAN Cards: Illegally obtaining multiple PAN cards under different identities to manipulate financial records.

5.Use of Stolen PAN Cards: Stealing someone else's PAN card and using it for illegal activities or identity theft.

To combat pan card tampering and fraud, the Income Tax Department has implemented various security features and verification processes. These measures aim to ensure the authenticity and integrity of PAN cards issued to individuals.

It is essential for individuals to safeguard their PAN cards and report any suspected tampering or loss to the authorities promptly. Additionally, individuals should exercise caution when providing their PAN card details for financial transactions and verification purposes to prevent misuse and identity theft.

Engaging in pan card tampering or using fraudulent PAN cards can lead to legal repercussions, including fines and imprisonment. Therefore, it is crucial to maintain the integrity of this important identification document and report any suspicious activities to the appropriate authorities.

1.1MOTIVATION

1.1.1 OVERVIEW OF EXISTING SYSTEM

Detecting tampered PAN card by extracting Permanent Account Number from User uploaded image and checking with official department. Highly Time consuming processes , Limited to larger organizations only.

Detecting tampered PAN card using computer vision by only checking Structural Similarity between them of original PAN card and the PAN card uploaded by user. Finely tampered Image can't give accurate output as Structural Similarity will be high.

Drawbacks of existing system

- Limited Coverage
- Maintenance and Updates
- Regulatory Compliance
- Accuracy and Reliability
- False Positives and Negatives
- Data Privacy Concerns

1.1.2 OVERVIEW OF PROPOSED SYSTEM

Nowadays frauds are everywhere. From cyber technology to legal documents, everywhere is fraud. So here, we're going to build a pan card tampering detection project using Computer Vision with OpenCV – Python, SSIM(Structural Similarity Index) and Computer vision .This will make organizations easy to find that the id(Pan card) provided by the employees are original or fake.

Advantages of proposed system

- The system helps in detecting fake or tampered PAN cards, preventing identity theft and fraudulent transactions.
- It automates the verification process, making it faster and more efficient than manual verification.
- The system can scale to handle a large number of verification requests efficiently.
- Automation reduces the time it takes to verify PAN cards, improving operational efficiency.

1.1.3 SYSTEM FEATURES

- The ability to verify the authenticity and validity of PAN cards provided by users.
- Secure methods for user authentication to ensure authorized access to the system.
- Tools for managing user accounts, permissions, and access control.
-

1.2 PROBLEM DEFINITION

The problem is to develop an automated system that can accurately and efficiently detect tampering or alterations in PAN (Permanent Account Number) cards, a critical identification document issued by the Indian government and used for various financial and official transactions..

1.3 OBJECTIVE OF PROJECT

The objective of the PAN card tampering detection project is to create an accurate, automated, and secure system for verifying PAN cards. It aims to detect tampering, ensure data accuracy, provide real-time verification (if needed), scale efficiently, integrate with external services, allow customization, comply with regulations, offer a user-friendly experience, maintain an audit trail, continuously improve, ensure usability and accessibility, be cost-effective, provide user education and support, and deploy and maintain the system reliably. The project seeks to enhance identity verification, reduce fraud, and build user trust.

1.4 SCOPE OF PROJECT

The project's scope includes developing an accurate and secure PAN card verification system. It covers tampering detection, automation, accuracy, security, real-time verification (optional), scalability, integration, customization, regulatory compliance, user experience, audit trail, continuous improvement, usability, cost-effectiveness, user education and support, and reliable deployment and maintenance. The project aims to enhance identity verification, reduce fraud, and ensure a seamless user experience.

CHAPTER 02

LITERATURE SURVEY

02.LITERATURE SURVEY

Paper Name: Credit card fraud detection using artificial neural network.

Credit card usage has increased due to technological advancements, leading to an increase in credit card fraud. This problem affects every industry, including banks, automobile manufacturers, and appliance companies. Various techniques, including data mining, machine learning, and algorithmic methods, have been utilized to detect fraud in credit card transactions, but the results have been unsatisfactory. Therefore, it is essential to create algorithms that are effective and efficient. We aim to prevent credit card fraud by utilizing artificial neural network methods and comparing them to other machine learning techniques. Fraud is an offensive act that deceives innocent individuals. When someone fraudulently uses a credit card, they steal the necessary login information from the cardholder and use it unlawfully, often through phone calls or SMS messages. Fraudsters may also use software programs to commit credit card fraud. To detect credit card fraud, the process begins when the customer submits the required information for a credit card transaction. The transaction must be screened for fraud activity before being approved.

Paper Name: Credit Card Fraud Detection Using Random Forest Algorithm.

Credit card fraud is increasing daily, both online and offline. For offline transactions, fraudsters need real cards, while virtual cards suffice for online transactions. These fraudulent activities can result in numerous unauthorized transactions without the actual user's knowledge. Fraudsters seek sensitive data like credit card numbers, bank account information, and other personal details to carry out transactions. They steal the user's credit card for offline transactions, while online purchases require them to steal the user's identity and login credentials. Credit card fraud has become a significant issue for banks and financial institutions in today's technology-driven society. Several fraudulent transactions lead to the loss of sensitive data that is challenging for both users and banking authorities to detect. Different models are utilized to detect fraudulent transactions based on transaction behavior. These models fall into two main categories: supervised learning and unsupervised learning algorithms. Techniques like Cluster Analysis, Support Vector Machine, Naive Bayes Classification, etc., have been used to determine the accuracy of fraudulent actions in the current system. This study employs the Random Forest Algorithm to identify the accuracy of fraudulent transactions.

Paper Name: Fraud Detection using Machine Learning and Deep Learning.

Machine learning is a popular topic this decade and a subset of artificial intelligence. Many businesses are investing in machine learning to improve their services. Machine learning uses a combination of computer algorithms and statistical modelling to enable computers to perform tasks without being explicitly programmed. It uses training data to learn and acquire models that can be used for predictions or actions based on past experiences. Machine learning techniques utilize artificial neural networks, including deep learning models such as convolutional neural networks, deep belief networks, auto-encoders, recurrent neural networks, and restricted Boltzmann machines. Properly trained neural networks can identify distinct relationships across entire datasets. This research compares various machine learning and deep learning approaches in three datasets, including the European, Australian, and German datasets. The study uses an ensemble of the top three models in all three datasets. Based on an empirical study, the research reports its findings on the comparison of several machine learning and deep learning models.

CHAPTER 03
SYSTEM ANALYSIS

03.SYSTEM ANALYSIS

3.1 SYSTEM ARCHITECTURE:

3.1.1.1 ARCHITECTURE DIAGRAM

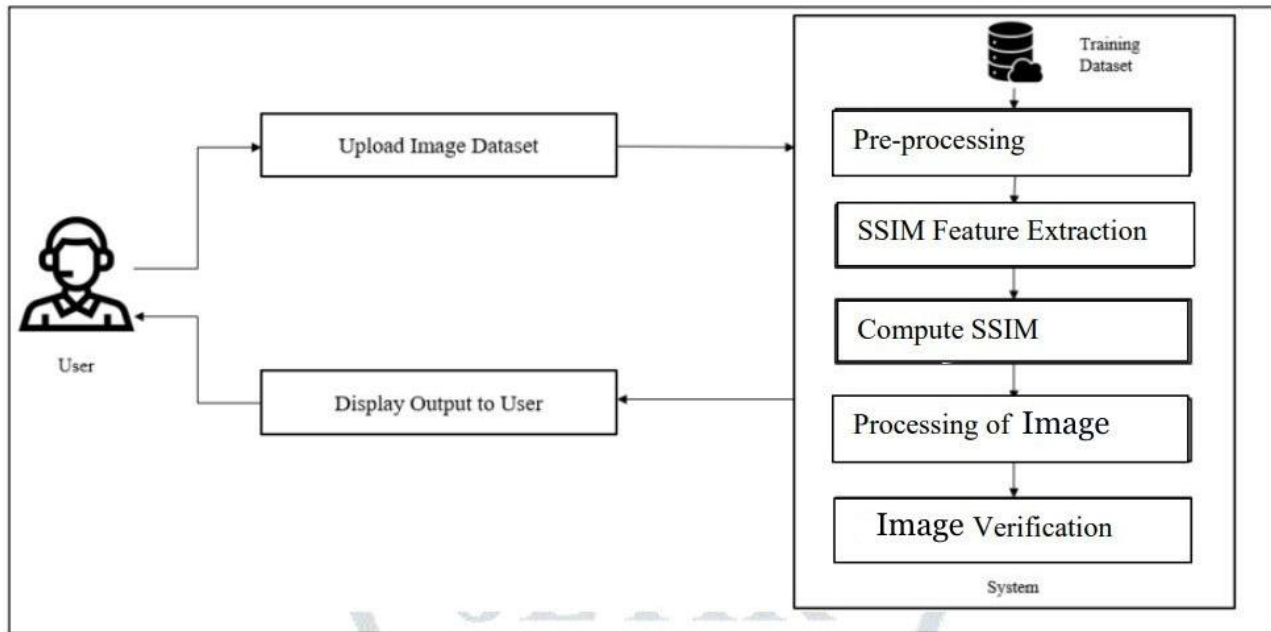


Fig 3.1.1:Architecture Diagram

Implementing a PAN card tampering detection system involves several technical components and steps. Below, I'll provide a high-level explanation of the key aspects of implementation. Begin by understanding the specific requirements of the system, including the desired features, user needs, and regulatory compliance. Choose the appropriate technologies and tools for different system components, including web development frameworks, databases, and machine learning libraries. Create a user-friendly web or mobile interface where users can upload PAN card images for verification. Design the UI to guide users through the verification process, provide feedback, and handle error cases gracefully. Implement user authentication and authorization mechanisms to ensure secure access to the system. Develop user management features, allowing users to create accounts, reset passwords, and manage their profiles. Develop image processing algorithms to preprocess PAN card images, such as re-sizing and format Top of Form conversion. Implement image analysis algorithms, including computer vision and machine learning models, to detect tampering or alterations. Pan card tampering detection using Structural Similarity Index (SSIM) is a technique employed to identify alterations or tampering in Permanent Account Number (PAN) cards by comparing the similarity between the original and scanned/taken PAN card images. The SSIM method is a popular image processing and computer vision technique used for image quality assessment and comparison.

The steps involved in this project are as follows :

1. Import necessary libraries
2. Scraping the tampered and original pan card from the website
3. Scaling down the shape of the tampered image as the original image
4. Read original and tampered image
5. Converting an image into a grayscale image
6. Applying Structural Similarity Index (SSIM) technique between the two images
7. Calculate Threshold and contours and
8. Experience real-time contours and threshold on images

Importing the necessary packages:

```
from skimage.metrics import structural_similarity
import imutils
import cv2
from PIL import Image
import requests
```

Skimage: Scikit-image, or ski-mage, is an open-source Python package, in this project most of the image processing techniques will be used via scikit-image

imutils: Imutils are a series of convenience functions to make basic image processing functions such as translation, rotation, resizing, and displaying images easier with OpenCV.

cv2: OpenCV (Open Source Computer Vision Library) is a library of programming functions. Here in this project major reading and writing of the image are done via cv2.

PIL: PIL (Python Imaging Library) is a free and open-source additional library for the Python programming language that adds support for opening, manipulating, and saving many different image file formats.

3.1.1.2 Structural Similarity Index (SSIM):

The Structural Similarity Index (SSIM) is a widely used metric in the field of image processing and computer vision. It serves as a measure of the similarity or likeness between two images, providing a quantitative assessment of how closely they resemble each other. SSIM is designed to mimic the human perception of image quality and similarity.

1. Objective Assessment:

- SSIM is an objective method for comparing two images. It evaluates their structural similarity based on various visual factors.

2. Components of SSIM:

- **Luminance Comparison:** SSIM takes into account the luminance (brightness) of the images. It assesses how well the contrast and brightness of corresponding pixels match in the two images.
- **Contrast Comparison:** SSIM evaluates the contrast or variations in pixel intensity within local image regions. It checks if the patterns of pixel intensity changes are similar.
- **Structure Comparison:** This component assesses the structural information in the images, examining the patterns and textures. It measures how well corresponding structures are preserved.

3. Scoring:

- The result of the SSIM calculation is a single score between -1 and 1.
- A score of 1 indicates that the two images are identical in terms of luminance, contrast, and structure.
- A score of 0 means there is no similarity between the images.
- A negative score suggests that the images are dissimilar, with some structural differences.

4. Use Cases:

- SSIM is commonly used for image quality assessment, including tasks like image compression, denoising, and restoration.
- It is also used in image and video codecs to evaluate the quality of compressed media.
- In the context of the Pan Card Tampering Detection System, SSIM is applied to compare the original and scanned/taken PAN card images to detect potential alterations or tampering.

5. Advantages:

- SSIM is particularly useful when assessing the quality of images that have undergone compression or other transformations.
- It offers a more comprehensive evaluation of image similarity compared to simple pixel-wise comparisons.

In summary, SSIM is a valuable tool for quantifying the similarity between images, taking into account luminance, contrast, and structure. It provides an objective and quantitative measure of image quality and similarity, making it widely applicable in various image processing and computer vision tasks, including the detection of potential tampering or alterations in identity documents like PAN cards.

3.1.1.3 Computer Vision:

Computer Vision is a multidisciplinary field that empowers computers to perceive and comprehend visual information from the world, mirroring the capabilities of human vision. It encompasses the development of algorithms and techniques to extract meaningful insights from images and videos, enabling computers to recognize objects, analyze scenes, and make decisions based on visual data. Computer Vision plays a pivotal role in a wide range of applications, including facial recognition for security, autonomous vehicles for navigation, medical image analysis for disease diagnosis, augmented reality for immersive experiences, and quality control in manufacturing processes. It involves tasks such as object detection, image segmentation, feature extraction, and 3D reconstruction. With the advent of deep learning and the application of neural networks like Convolutional Neural Networks (CNNs), Computer Vision has witnessed significant advancements in image recognition and understanding, revolutionizing industries and opening doors to innovative solutions across various domains.

3.1.1.4 Working:

The Pan Card Tampering Detection System using the Structural Similarity Index (SSIM) operates by employing advanced image processing techniques to objectively assess the authenticity of Permanent Account Number (PAN) cards and detect any alterations or tampering attempts. Here is a detailed explanation of how this system works:

1. Input Data Acquisition:

- The system begins by acquiring two images: the original PAN card image, typically obtained from a reliable source, and the scanned or captured image of the PAN card that needs to be verified.

2. Image Preprocessing:

- Both images may undergo preprocessing to ensure they are in a consistent format for analysis. This preprocessing may include resizing, cropping, and converting them to grayscale. These steps aim to standardize the images for accurate comparison.

3. SSIM Calculation:

- The heart of the system lies in the calculation of the Structural Similarity Index (SSIM) between the two images.
- SSIM is a mathematical metric that quantifies the structural similarity or likeness between two images. It takes into account luminance, contrast, and structure.
- SSIM produces a score that represents the degree of similarity between the images. A high SSIM score indicates a high degree of similarity, suggesting that the PAN card hasn't been tampered with. Conversely, a low SSIM score implies significant differences between the images, raising suspicion of tampering.

4. Thresholding:

- After obtaining the SSIM score, the system applies a predefined threshold value to classify the result.
- If the SSIM score is above the threshold, the PAN card is considered genuine, and no tampering is detected.
- If the SSIM score falls below the threshold, it indicates a potential discrepancy between the original and scanned images, suggesting tampering or alterations.

5. Additional Analysis (Optional):

- Depending on the SSIM score and the organization's policies, further analysis or human verification may be required.
- This could involve a manual review of the PAN card or additional checks to confirm its authenticity.

6. Decision and Reporting:

- Based on the SSIM score and any additional analysis, the system makes a decision regarding the authenticity of the PAN card.
- Suspicious or tampered PAN cards may be flagged for further investigation, and the results are reported to the relevant authorities or organizations.

7. Logging and Records:

- The system maintains a log of all verification attempts and results, which can be useful for auditing and tracking purposes.

8. Integration with Verification Workflow:

- The PAN Card Tampering Detection System can be seamlessly integrated into the identity verification workflow of organizations, financial institutions, or government agencies to ensure the integrity of PAN cards.

It's important to emphasize that while SSIM is a valuable tool for tampering detection, it is typically used as part of a broader identity verification and fraud prevention strategy. The system may include additional security measures, document validation checks, and human oversight to ensure comprehensive identity verification and the prevention of fraudulent activities. The use of SSIM for PAN card tampering detection provides an objective and quantitative way to assess the similarity between the original and scanned/taken images. It helps organizations and authorities identify potentially altered PAN cards efficiently and accurately.

3.2 OPERATING REQUIREMENTS

HARDWARE REQUIREMENTS

- Processor : Any processor above 500MHz
- Input Device: Standard Keyboard and Mouse
- Output Device : VGA and High Resolution Monitor
- Ram : 4 GB
- Hard Disk : 256 GB

SOFTWARE REQUIREMENTS

- Operating system : Windows
- Coding Language : Python

CHAPTER 04

SYSTEM DESIGN

04.SYSTEM DESIGN

4.1 UML DIAGRAMS

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta- model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modelling and other non software systems.

The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extensibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.

6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

TYPES OF UML DIAGRAM

Each UML diagram is designed to let developers and customers view a software system from a different perspective and in varying degrees of abstraction. UML diagrams commonly created in visual modelling tools include:

A. USECASE DIAGRAM

Display the relationship among actors and Use Cases. A use case is a set of scenarios that describing an interaction between a user and a system. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors

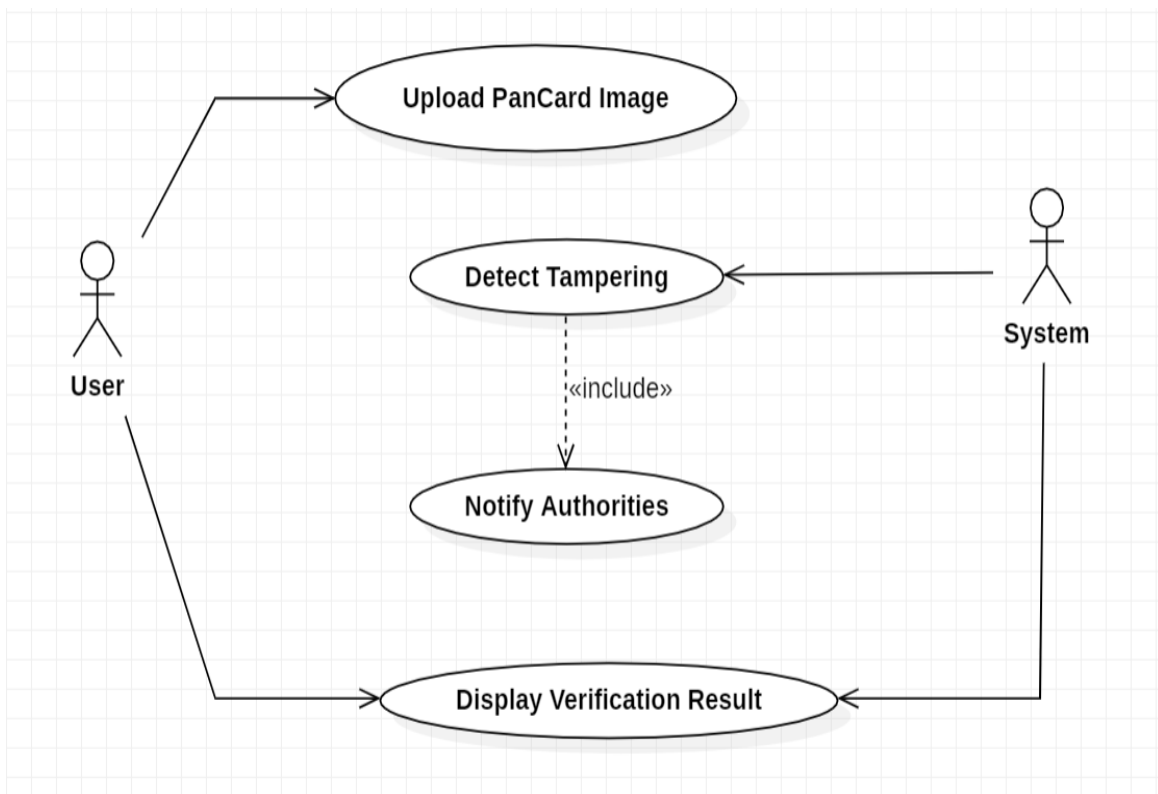


Fig 4.1 use case diagram

B.CLASS DIAGRAM

Class diagrams are widely used to describe the types of objects in a system and their relationships. Class diagrams model class structure and contents using design elements such as classes, packages and objects. Class diagrams describe three different perspectives when designing a system, conceptual, specification, and implementation. These perspectives become evident as the diagrams are created and help solidify the design.

Classes are composed of three things: a name, attributes, and operations.

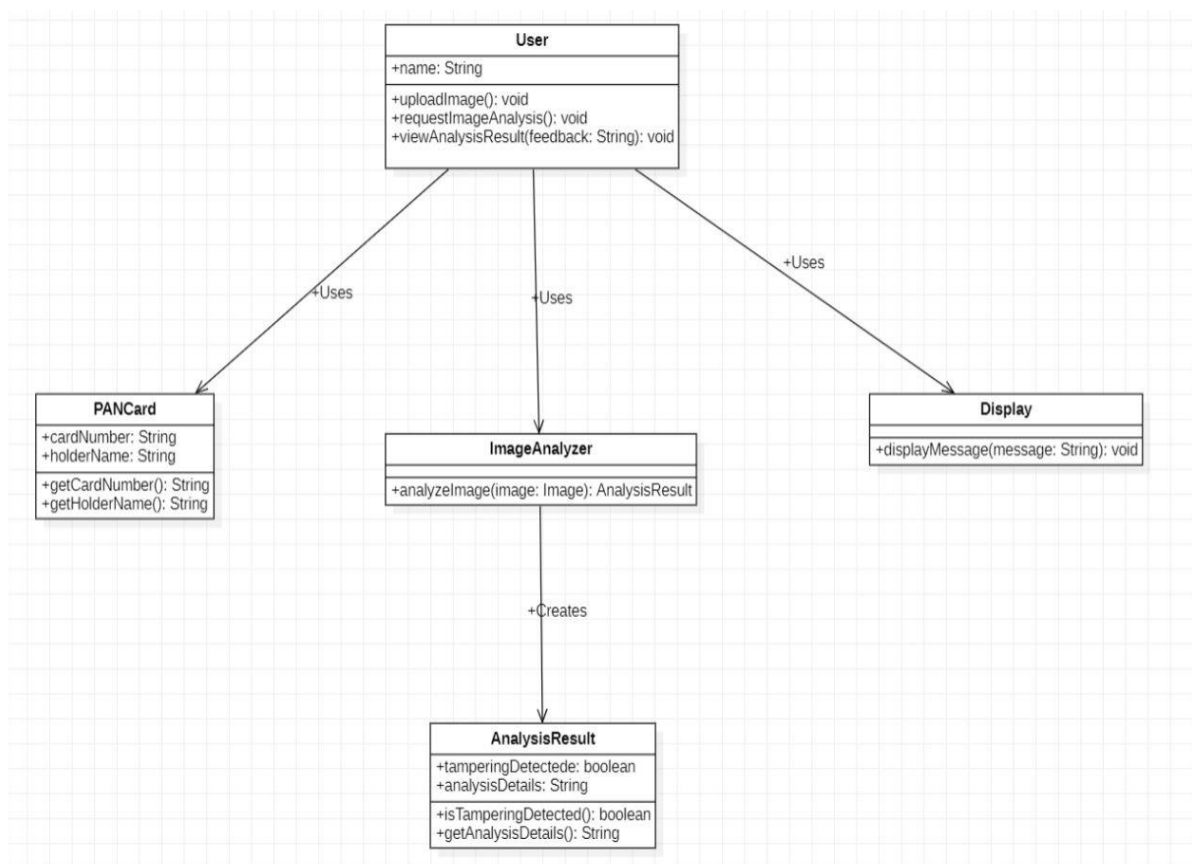


Fig.4.2 class diagram

C.SEQUENCE DIAGRAM

Display the time sequence of the objects participating in the interaction. This consists of the vertical dimension (time) and horizontal dimension (different objects).

Sequence diagrams demonstrate the behavior of objects in a use case by describing the objects and the messages they pass. The diagrams are read left to right and descending. The example below shows an object of class 1 start the behavior by sending a message to an object of class 2. Messages pass between the different objects until the object of class 1 receives the final message.

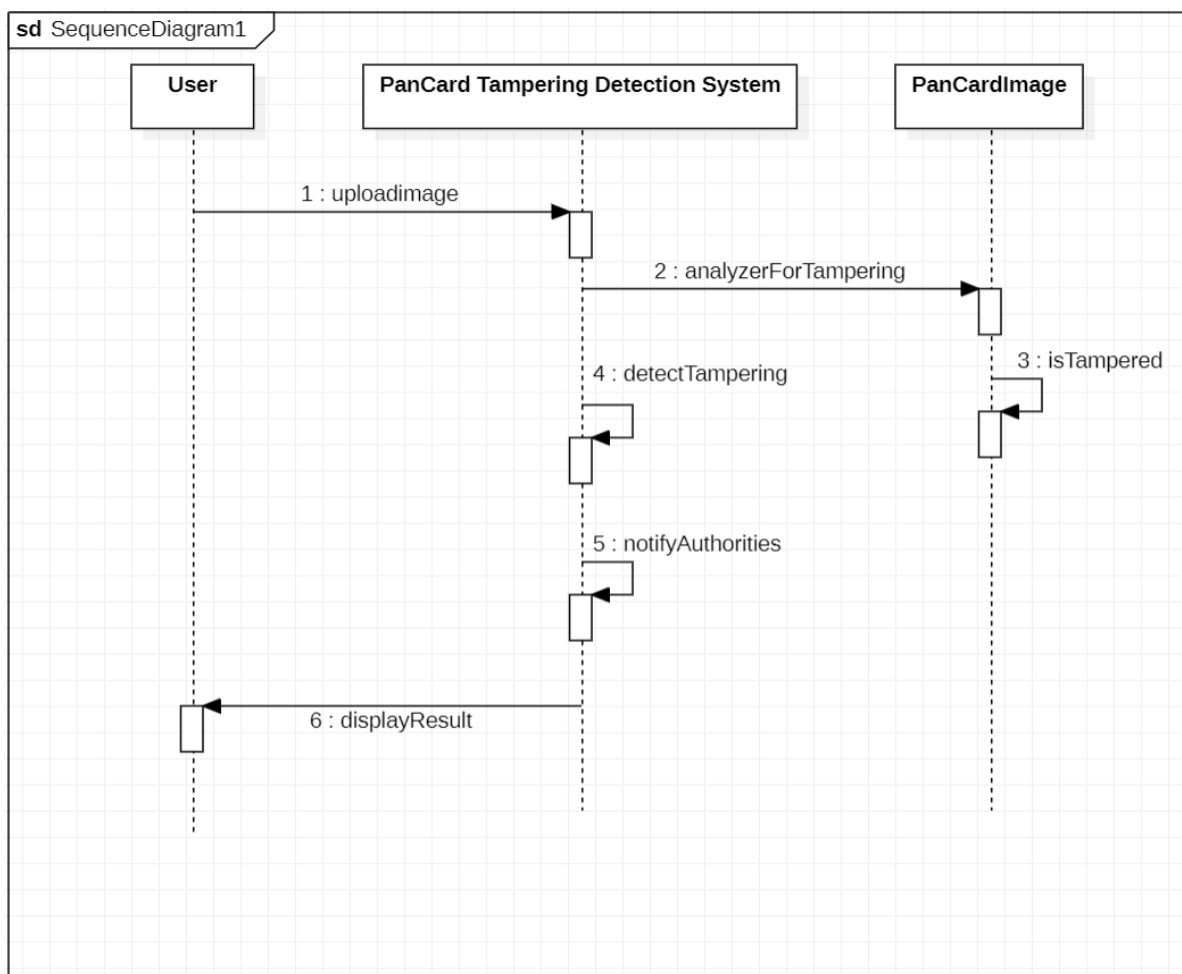


Fig. 4.3 Sequence diagram

D. DEPLOYMENT DIAGRAM

The deployment diagram visualizes the physical hardware on which the software will be deployed. It portrays the static deployment view of a system. It involves the nodes and their relationships.

It ascertains how software is deployed on the hardware. It maps the software architecture created in design to the physical system architecture, where the software will be executed as a node. Since it involves many nodes, the relationship is shown by utilizing communication paths.

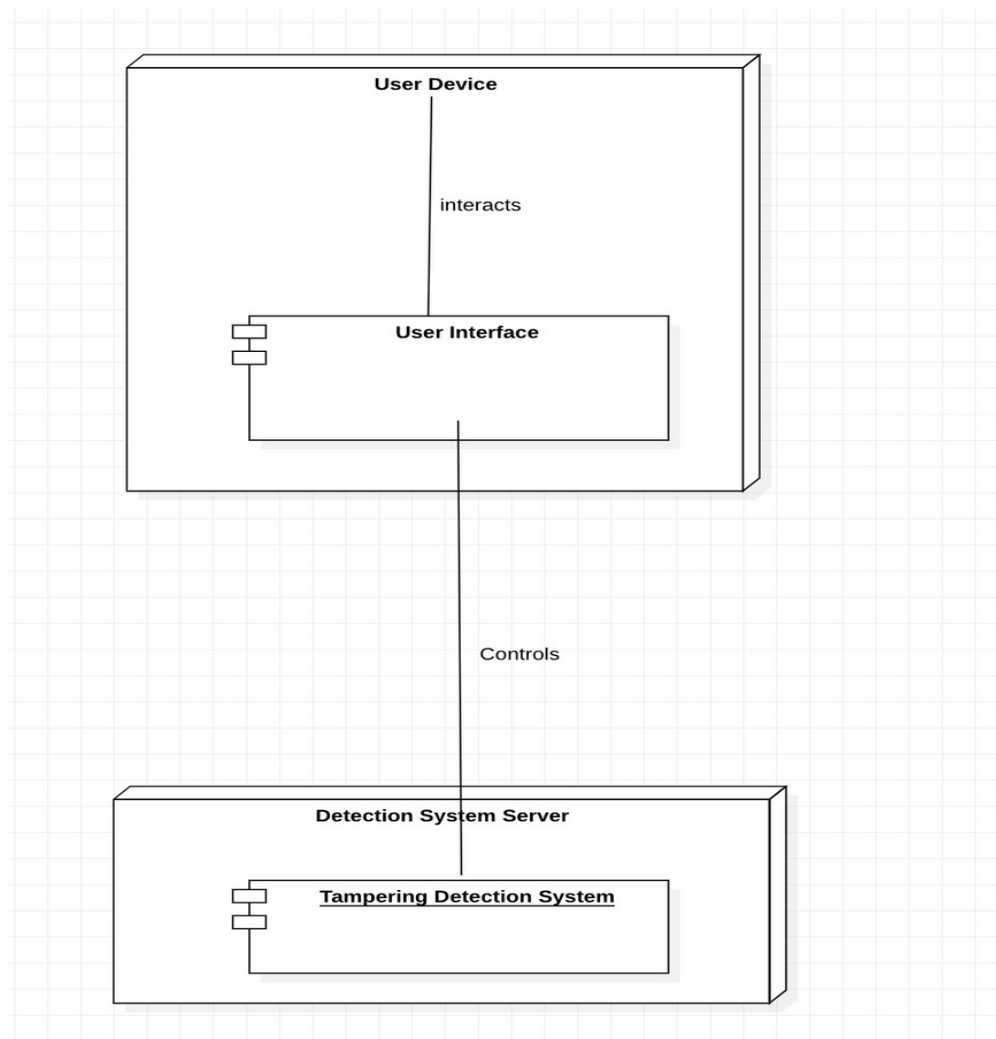


Fig. 4.4 Deployment Diagram

E.ACTIVITY DIAGRAM

An activity diagram is a behavioral diagram i.e. it depicts the behavior of a system. An activity diagram portrays the control flow from a start point to a finish point showing the various decision paths that exist while the activity is being executed.

Activity Diagrams describe how activities are coordinated to provide a service which can be at different levels of abstraction. Typically, an event needs to be achieved by some operations, particularly where the operation is intended to achieve a number of different things that require coordination, or how the events in a single use case relate to one another, in particular, use cases where activities may overlap and require coordination.

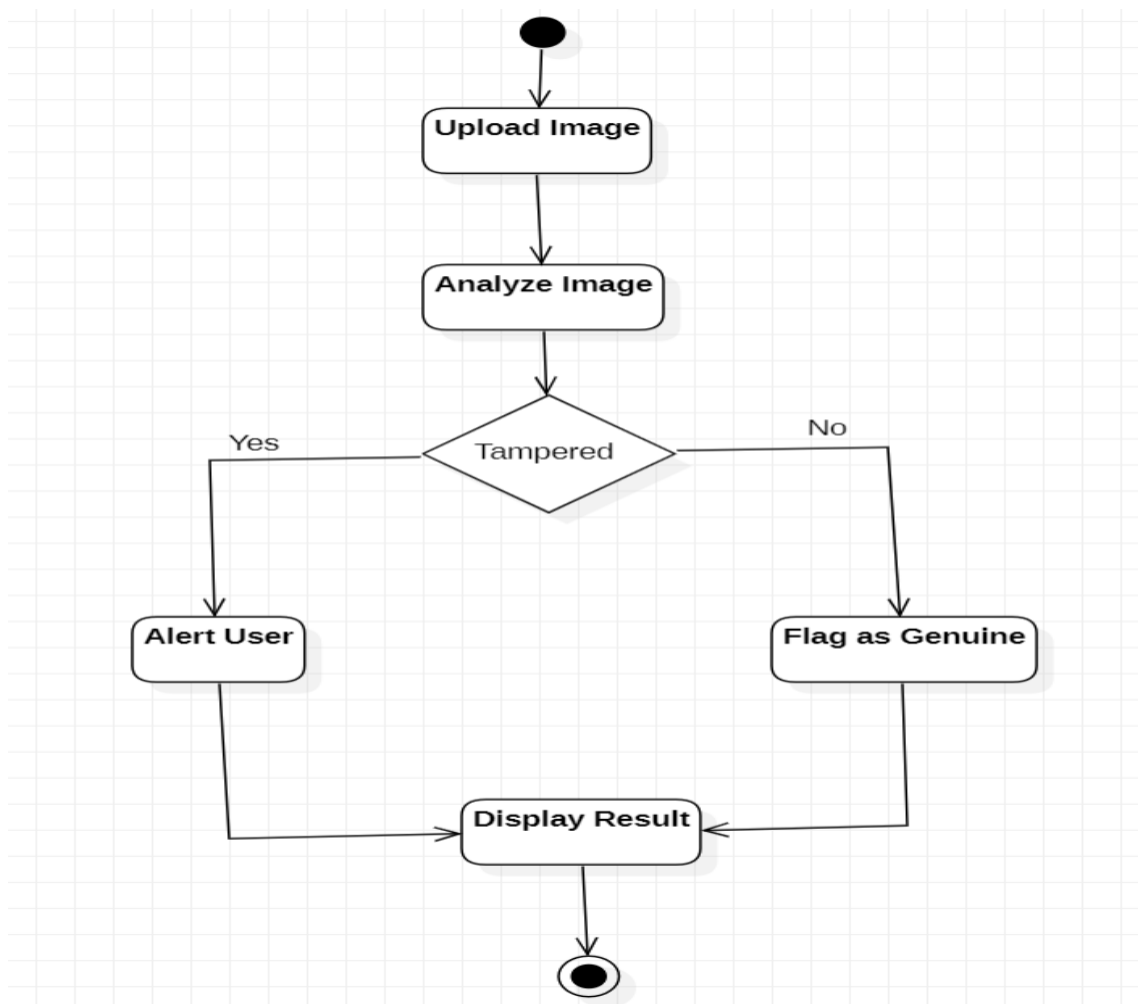


Fig. 4.5 Activity diagram

CHAPTER 05

IMPLEMENTATION

05.IMPLEMENTATION

5.1 SAMPLE CODE

views.py

```
# Important imports

from app import app
from flask import request, render_template
import os
from skimage.metrics import structural_similarity
import imutils
import cv2
from PIL import Image

# Adding path to config
app.config['INITIAL_FILE_UPLOADS'] = 'app/static/uploads'
app.config['EXISTNG_FILE'] = 'app/static/original'
app.config['GENERATED_FILE'] = 'app/static/generated'

# Route to home page
@app.route("/", methods=["GET", "POST"])
def index():

    # Execute if request is get
    if request.method == "GET":
        return render_template("index.html")

    # Execute if request is post
    if request.method == "POST":
        # Get uploaded image
        file_upload = request.files['file_upload']
        filename = file_upload.filename

        # Resize and save the uploaded image
        uploaded_image = Image.open(file_upload).resize((250,160))
        uploaded_image.save(os.path.join(app.config['INITIAL_FILE_UPLOADS'], 'image.jpg'))
```

```

# Resize and save the original image to ensure both uploaded and original matches in size
original_image =
    Image.open(os.path.join(app.config['EXISTNG_FILE'], 'image.jpg')).resize((250,160))
original_image.save(os.path.join(app.config['EXISTNG_FILE'], 'image.jpg'))

# Read uploaded and original image as array
original_image = cv2.imread(os.path.join(app.config['EXISTNG_FILE'], 'image.jpg'))
uploaded_image =
    cv2.imread(os.path.join(app.config['INITIAL_FILE_UPLOADS'], 'image.jpg'))

# Convert image into grayscale
original_gray = cv2.cvtColor(original_image, cv2.COLOR_BGR2GRAY)
uploaded_gray = cv2.cvtColor(uploaded_image, cv2.COLOR_BGR2GRAY)

# Calculate structural similarity
(score, diff) = structural_similarity(original_gray, uploaded_gray, full=True)
diff = (diff * 255).astype("uint8")

# Calculate threshold and contours
thresh =
    cv2.threshold(diff, 0, 255, cv2.THRESH_BINARY_INV | cv2.THRESH_OTSU)[1]
cnts =
    cv2.findContours(thresh.copy(), cv2.RETR_EXTERNAL, cv2.CHAIN_APPROX_SIMPLE)
cnts = imutils.grab_contours(cnts)

# Draw contours on image
for c in cnts:
    (x, y, w, h) = cv2.boundingRect(c)
    cv2.rectangle(original_image, (x, y), (x + w, y + h), (0, 0, 255), 2)
    cv2.rectangle(uploaded_image, (x, y), (x + w, y + h), (0, 0, 255), 2)

# Save all output images (if required)
cv2.imwrite(os.path.join(app.config['GENERATED_FILE'], 'image_original.jpg'),
original_image)

```

```

cv2.imwrite(os.path.join(app.config['GENERATED_FILE'], 'image_uploaded.jpg'),
            uploaded_image)
cv2.imwrite(os.path.join(app.config['GENERATED_FILE'], 'image_diff.jpg'), diff)
cv2.imwrite(os.path.join(app.config['GENERATED_FILE'], 'image_thresh.jpg'), thresh)
return render_template('index.html', pred=str(round(score*100,2)) + '%' + ' correct')

# Main function
if __name__ == '__main__':
    app.run(debug=True)

```

config.py

```

import os

from os import environ

class Config(object):
    DEBUG = False
    TESTING = False
    basedir = os.path.abspath(os.path.dirname(__file__))
    SECRET_KEY = 'pianalytix'
    UPLOADS = "/home/username/app/app/static/uploads"
    SESSION_COOKIE_SECURE = True
    DEFAULT_THEME = None

class DevelopmentConfig(Config):
    DEBUG = True
    SESSION_COOKIE_SECURE = False

class DebugConfig(Config):
    DEBUG = False

from app import app

if __name__ == '__main__':
    app.run()

```

init.py

```

from flask import Flask

app = Flask(__name__)

app.config.from_object("config.DevelopmentConfig")

from app import views

```


index.html

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1.0"/>
  <title>Pan Card Tampering</title>
  <!-- CSS -->
  <link href="/static/css/materialize.css" type="text/css" rel="stylesheet"
media="screen,projection"/>
</head>

<body>
  <nav style="background-color: #5e72e4" class="lighten-1" role="navigation" style="height:
100px">
    <div class="nav-wrapper container">
      <a id="logo-container" class="brand-logo center"><h5>Pan Card Tampering</h5></a>
    </div>
  </nav>
  <div class="section no-pad-bot" id="index-banner">
    <div class="container">
      <div class="row">
        <form action="/" method="post" class="col s12" enctype="multipart/form-data">
          <div class="row">
            <div class="input-field col s3">
            </div>

            <div class="input-field col s5" style="margin-left: 20px; margin-top: 100px">
              <div class="row">
                <label for="first_name"><b>Upload Pan Card Image</b></label><br>
                <div class="file-field input-field">
                  <div class="btn" style="background-color: #5e72e4">
                    <span>Browse</span>
                    <input type="file" name="file_upload" id="file_upload" />
                  </div>
```

```

        <div class = "file-path-wrapper">
            <input class = "file-path validate" type = "text" placeholder = "Upload file"
name="file_name"      id="file_name" />
        </div>
    </div>
</div>
</div>
</div>
</div>

<div class="row center">
    <button type="submit" class="btn-large" style="background-color:
#5e72e4">Check</button>
</div>
</form>
    <div style="text-align: center; padding-top: 50px">
        <h5>{{ pred }}</h5>
    </div>

</div>
<br><br>
</div>
</div>

</div>
</div>

<!-- Scripts-->
<script src="./static/js/materialize.js"></script>
<script type="text/javascript">
    document.getElementById('file_upload').onchange = function () {
        document.getElementById('file_name').value = this.value.slice(12,100);
    };
</script>

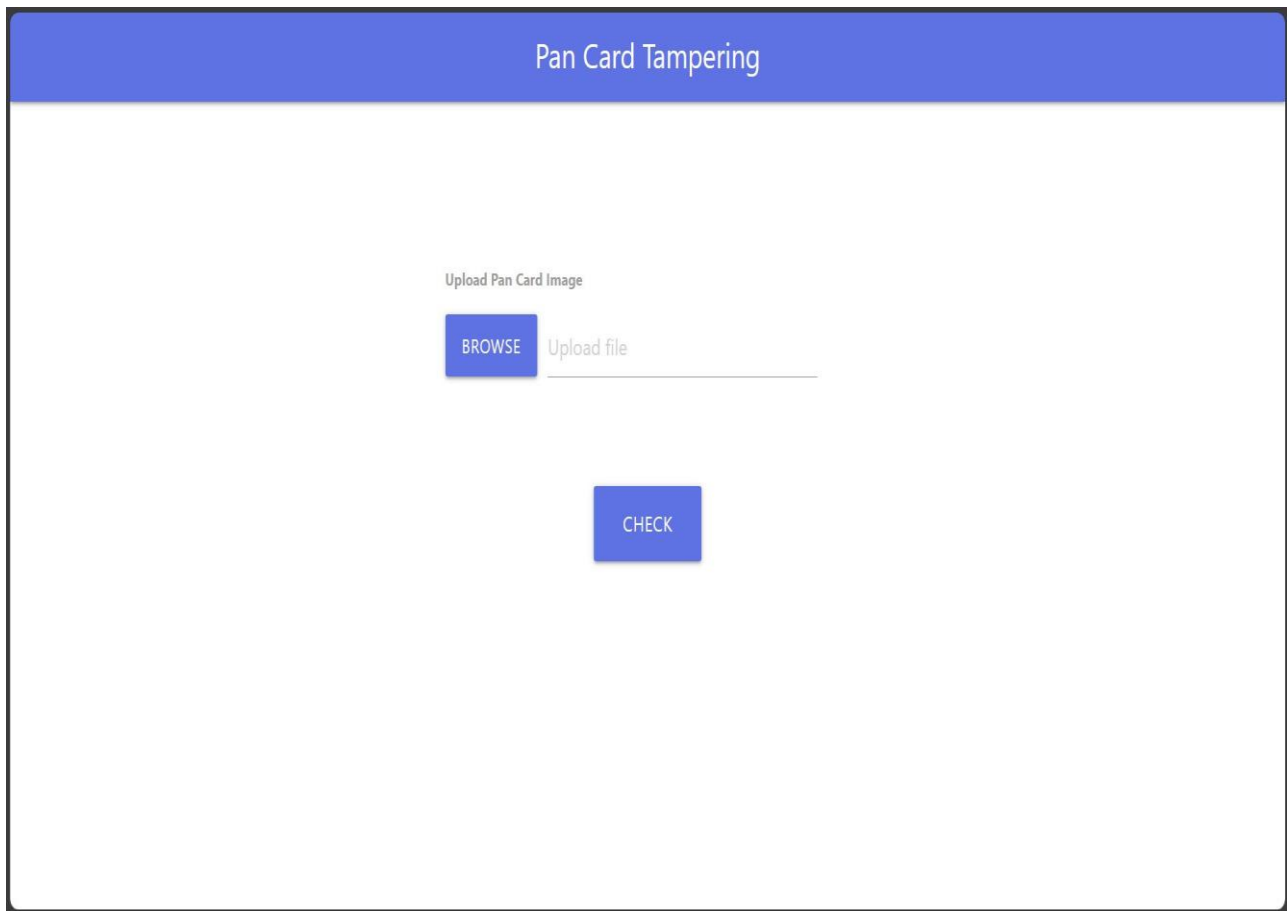
</body>
</html>

```

CHAPTER 06

OUTPUT SCREENS

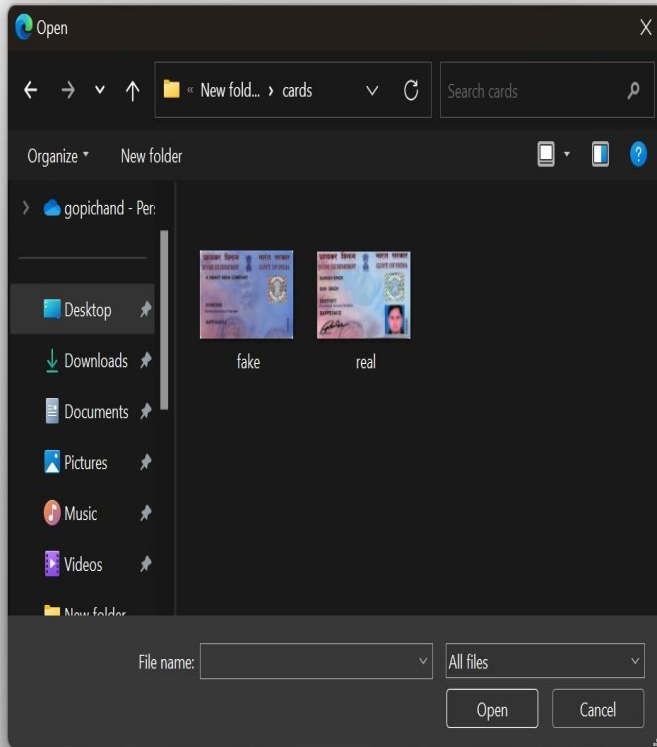
06.OUTPUT SCREENS



The screenshot displays the 'Pan Card Tampering' application interface. It features a blue header bar with the title 'Pan Card Tampering'. Below the header, the text 'Upload Pan Card Image' is centered. Underneath this text, there is a blue button labeled 'BROWSE' and a text input field with the placeholder 'Upload file'. A blue button labeled 'CHECK' is positioned below the input field.

6.1 Home Screen

Pan Card Tampering



6.2 Image Uploading

Pan Card Tampering

Upload Pan Card Image

BROWSE

Upload file

CHECK

99.73% correct

6.3 Image is uploaded and it is real

CHAPTER 07

TESTING AND DEBUGGING

07.TESTING AND DEBUGGING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

7.1 TYPES OF TESTS

7.1.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

7.1.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfactory, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

7.1.2.1 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.1.3 SYSTEM TESTING

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

7.1.4 WHITE BOX TESTING

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is used to test areas that cannot be reached from a black box level.

7.1.5 BLACK BOX TESTING

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box. You cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

7.1.5.1 TEST STRATEGY AND APPROACH

Field testing will be performed manually and functional tests will be written in detail

7.1.5.2 TEST OBJECTIVES

All field entries must work properly.

- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

7.1.5.3 FEATURES TO BE TESTED

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

7.1.6 INTEGRATION TESTING

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or one step up software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.1.7 ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.2 TEST CASES

TEST ID	TEST DESCRIPTION	TEST DESIGN	EXPECTED OUTPUT	ACTUAL OUTPUT	STATUS
1	Check the PAN card is fake or real	Inserting the pan card	Pan card is real	Pan card is real	Pass
2	Check the PAN card is fake or real	Inserting the pan card	Pan card is fake	Pan card is fake	Pass
3	Check whether the website is opening or not	Click on the link	Website is opened	Website is opened	Pass
4	Valid PAN Card - Resized	Resized Original PAN Card Image	Genuine	Genuine	Pass
5	Valid PAN Card - Slight Color Variation	Original PAN Card with Slight Color Variation	Genuine	Genuine	Pass
6	Valid PAN Card - Added Noise	Original PAN Card with Added Noise	Genuine	Genuine	Pass
7	Valid PAN Card - Slight Rotation	Slightly Rotated Original PAN Card	Genuine	Genuine	Pass
8	Suspicious PAN Card - Major Tampering	PAN Card with Major Tampering	Suspicious	Suspicious	Pass
9	Suspicious PAN Card - Blurring	PAN Card with Blurred Text	Suspicious	Suspicious	Pass
10	Suspicious PAN Card - Reversed Colors	PAN Card with Reversed Color Channels	Suspicious	Suspicious	Pass

11	Suspicious PAN Card - Different Font	PAN Card with Different Font	Suspicious	Suspicious	Pass
12	Suspicious PAN Card - Altered Signature	PAN Card with Altered Signature	Suspicious	Suspicious	Pass
13	Suspicious PAN Card - Added Objects	PAN Card with Added Objects (Stickers/Seals)	Suspicious	Suspicious	Pass
14	Invalid PAN Card - No Image	No Image Uploaded	Invalid (No Image)	Invalid (No Image)	Pass
15	Invalid PAN Card - Unsupported Format	Unsupported Image Format (e.g., BMP)	Invalid (Format)	Invalid (Format)	Pass
16	Invalid PAN Card - Empty Image	Empty/Blank Image	Invalid (Empty)	Invalid (Empty)	Pass
17	Invalid PAN Card - Low Quality Image	Low-Quality Image (Blurry/Unreadable)	Invalid (Quality)	Invalid (Quality)	Pass

Table :7.2.1 Test cases for system

CHAPTER 08

CONCLUSION

08.CONCLUSION

PAN card fraud is a growing concern, and it has become increasingly important to develop effective fraud detection methods. This project can be used in different organizations where customers or users need to provide any kind of id in order to get themselves verified. The organization can use this project to find out whether the ID is original or fake. Similarly, this can be used for any type of ID like Aadhaar, voter id, etc.

In conclusion, the development and implementation of a Pan Card Tampering Detection system represent a significant stride towards safeguarding the integrity of Permanent Account Number (PAN) cards and the vital information they hold. This innovative system leverages advanced technologies, including image processing and the Structural Similarity Index (SSIM), to provide a robust and efficient solution for detecting alterations and tampering attempts in PAN cards.

One of the notable strengths of this system is its ability to objectively assess the authenticity of PAN cards. By employing SSIM, it quantifies the structural similarity between the original and scanned/taken images, offering an unbiased and quantitative measure of potential tampering. This objectivity enhances the reliability of the verification process.

Efficiency is another hallmark of this system. With its automated SSIM calculations, it streamlines the verification process, enabling swift and accurate assessments of PAN cards. This efficiency makes it a valuable tool for both individual identity verification and large-scale processes conducted by financial institutions and government agencies.

The system's early detection capabilities are of paramount importance. When PAN cards exhibit SSIM scores below a predefined threshold, the system triggers alerts, allowing authorities and organizations to promptly investigate and take necessary actions. This proactive approach adds an essential layer of security to identity verification processes.

However, it's crucial to recognize that while this system is a powerful tool for tampering detection, it should be integrated into a comprehensive identity verification and fraud prevention strategy. Additional security measures, human oversight, and thorough document validation remain vital components of a comprehensive approach to identity verification.

In summary, the Pan Card Tampering Detection system represents a significant advancement in the realm of identity verification and fraud prevention. Its adoption contributes to heightened security, reduced instances of fraud, and increased confidence in the authenticity of PAN cards. It underscores the commitment to protecting individuals' financial and personal information, aligning with the broader mission of ensuring the integrity and security of financial documents in today's digital age.

FUTURE ENHANCEMENTS

Further enhancements can be providing the new futures of the pan card so that a peoples can find the card is real or fake through it and also converting our application into a mobile app. This makes it even much better and easier to access from anyplace and anytime. Also some extra features can be added such as credit/debit card detection, fake id detection etc.

Certainly, here are potential future enhancements for the Pan Card Tampering Detection Project using SSIM:

In the future, the project can be extended to offer real-time PAN card verification, allowing users to capture PAN card images using their device's camera for immediate analysis. This real-time capability can be particularly valuable for online identity verification services and applications where quick and accurate authentication is essential.

Developing a dedicated mobile application is another promising enhancement. Such an app could provide users with an intuitive interface for verifying their PAN cards using the SSIM-based detection system. Integration with the device's camera and easy image upload capabilities can enhance user convenience and accessibility.

To scale the project's capabilities and handle high volumes of verification requests efficiently, cloud-based verification services can be introduced. Users can securely upload their PAN card images to a cloud server for analysis, ensuring both speed and accuracy in the verification process.

Incorporating machine learning models represents another avenue for improvement. These models can enhance the system's ability to identify sophisticated tampering techniques by learning from a wide range of examples. Deep learning models, in particular, can be trained to recognize various types of alterations and forgeries.

Expanding the project to support verification of other identity documents such as passports, driver's licenses, and Aadhar cards can make it a versatile tool for different use cases and regions. Multi-language support can further broaden its applicability, ensuring accurate text recognition for documents in diverse languages.

Enhanced reporting features can provide users with detailed verification reports, including information about specific discrepancies detected in their PAN cards. This added transparency can assist users in understanding and rectifying issues, enhancing trust in the verification process.

Considering blockchain technology for secure storage and verification of PAN card information is another

avenue. Blockchain's decentralized and immutable nature can bolster data security and prevent unauthorized alterations to PAN card records.

Continuous improvement in image processing techniques is crucial. Staying current with state-of-the-art algorithms ensures that the system maintains its accuracy in detecting tampering and alterations in PAN cards.

A focus on user authentication is vital to ensure that only authorized individuals can access and use the verification system, protecting the integrity of the process. Additionally, compliance with any evolving government regulations related to PAN cards and identity verification is essential to ensure that the system remains legally compliant.

Enhancements in the user interface and overall user experience should not be overlooked. A user-friendly interface that is intuitive and accessible to individuals of all technical backgrounds can improve the project's adoption and usability.

Scalability is a key consideration to accommodate a growing user base and increased verification requests. The system should be designed to handle increased traffic without compromising performance or accuracy.

To enhance security, stringent measures should be implemented to protect user data and ensure the confidentiality of PAN card information. Additionally, the introduction of a feedback mechanism can empower users to report issues or false positives/negatives, contributing to ongoing system refinement and improvement.

Continuous monitoring and auditing of the verification process can help detect and prevent fraudulent activities, ensuring the project's effectiveness in safeguarding the authenticity of PAN cards. These future enhancements collectively aim to make the Pan Card Tampering Detection Project more robust, versatile, and user-friendly, addressing evolving challenges in identity verification and fraud prevention.

REFERENCES

- Asha RB, Suresh Kumar KR,” Credit card fraud detection using artificial neural network. 35– 41, 2021, Doi: <https://doi.org/10.1016/j.gltp.2021.01.006>
- M.Suresh Kumar, V.Soundarya, S.Kavitha, E.S. Keerthika, E.Aswini, ”Credit Card Fraud Detection Using Random Forest Algorithm,” 2019, Doi: <https://doi.org/10.1109/ICCCT2.2019.8824930>
- Pradeepan Raghavan, Neamat El Gayar,” Fraud Detection using Machine Learning and Deep Learning,” December 2019, Doi: <https://doi.org/10.1109/ICCIKE47802.2019.9004231>
- Badal Soni, Pradip K. Das, Dalton Meitei Thounaojam. CMFD: a detailed review of block based and key feature-based techniques in image copy-move forgery detection, 2018. IET Image Processing 12:2, pages 167-178
- Francisco Cruz, Nicolas Sidere, Mickael Coustaty, Vincent Poulain “ D’Andecy, and Jean-Marc Ogier. Local binary patterns for document forgery detection. In Document Analysis and Recognition (ICDAR), 2017 14th IAPR International Conference on, volume 1, pages 1223–1228. IEEE, 2017
- Y. Sahin, E. Duman,” Detecting Credit Card Fraud by ANN and Logistic Regression”, 2011, Doi: <https://doi.org/10.1109/INISTA.2011.5946108>
- He, Zhiwei, et al. "A new automatic extraction method of container identity codes." IEEE Transactions on intelligent transportation systems 6.1 (2005): 72-78
- S. Shang, N. Memon, and X. Kong, “Detecting documents forged by printing and copying,” EURASIP Journal on Advances in Signal Processing, vol. 2014, no. 1, p. 140, 2014.
- Ulutas, G., Muzaffer, G.: ‘A new copy move forgery detection method resistant to object removal with uniform background forgery’, Math. Probl. Eng., 2016, 2016, pp. 1–19
- Bashar, M., Noda, K., Ohnishi, N., et al.: ‘Exploring duplicated regions in natural images’, IEEE Trans. Image Process., 2016, 99, pp. 1–40