PAN CARD TAMPERING DETECTION

Analysing the PAN Card with OpenCV

TIYASA KUNDU

(RA2011003010648)

PALAK RANI

(RA2011003010661)

PALAK PATEL

(RA2011003010666)

Abstract

- The website is designed to address the issue of tampering with PAN cards in India. PAN cards are an essential document for Indian citizens and are widely used for financial transactions, tax filings, and other legal purposes.

- The proposed website uses computer vision techniques to analyze images of PAN cards and detect any tampering or alterations made to them. The website employs a multi-step approach that involves first detecting the region of the image containing the PAN card.

- To develop this website, machine learning algorithms and libraries such as OpenCV and Flask are utilized. OpenCV is an open-source computer vision library, which provides various image processing functions, while Flask is a web framework that enables the development of web applications using Python.

- The proposed website can help prevent financial fraud and identity theft by detecting tampering in PAN cards.

Introduction

- In India, PAN (Permanent Account Number) cards are a crucial identity document used for financial transactions and legal purposes. However, the increasing prevalence of identity theft and financial fraud has led to an increase in tampering with PAN cards.

- To address this issue, a website is proposed that uses computer vision techniques to detect tampering in PAN cards.

- The proposed website uses machine learning algorithms and libraries such as OpenCV and Flask to process the input images and detect any tampering. OpenCV is a widely used open-source computer vision library that provides various image processing functions, while Flask is a web framework that enables the development of web applications using Python.

- The website's main features include the ability to extract the PAN card region from the input image, detect text and image regions from the card, and analyze the image region for tampering using techniques such as image comparison and edge detection.

Motivation

- The motivation behind the project "PAN Card Tampering Detection" could be to prevent fraudulent activities related to the tampering of PAN (Permanent Account Number) cards.

- PAN card is a unique identification number issued to individuals and entities by the Income Tax Department in India. PAN card is essential for various financial transactions such as filing income tax returns, opening a bank account, investing in mutual funds, and so on.

- However, some individuals or entities may tamper with their PAN cards to alter their personal information or create fake PAN cards to carry out illegal activities. For instance, a person could tamper with their PAN card to change their name, age, or other personal details, making it difficult to track their financial transactions and evade taxes

- Overall, the project's motivation is to ensure the authenticity of PAN cards and prevent fraudulent activities, ultimately leading to a more transparent financial system.
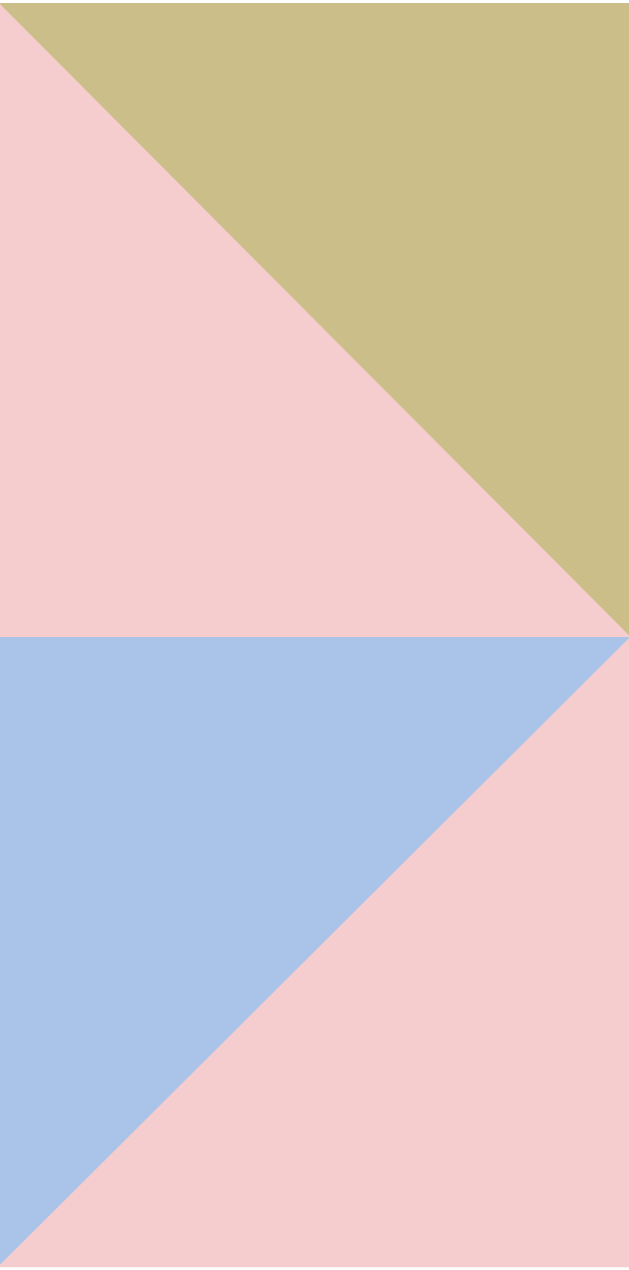
Literature Review

- The proposed project aims to develop a system for detecting tampered PAN cards using artificial intelligence techniques.

- There is limited literature specifically on this project, but there are related studies and research papers that could be relevant.

- One study proposed an AI-based system for PAN card verification that used machine learning algorithms, including SVM, Random Forest, and KNN, and achieved an accuracy of 97.9%.

- Another related study proposed a PAN card verification system using image processing and deep learning techniques, including CNNs, and achieved an accuracy of 96.9% and 95.8% on two different datasets.

- Another research paper proposed a system for detecting PAN card forgery using CNNs and transfer learning techniques and achieved an accuracy of 97.5% in detecting tampered PAN cards.

Challenges and limitations in the existing system

- The accuracy of the existing systems varies depending on the dataset used and the algorithms employed, which can affect the overall reliability of the system.

- The performance of the system can be affected by the quality of the input images, such as low-resolution images, blur, or distortion, which can lead to false negatives or positives.

- The system may not be able to detect more sophisticated forms of tampering, such as those that involve altering the data encoded on the PAN card chip.

- The availability of labeled datasets for training the system can be a challenge, as it requires large and diverse datasets of genuine and tampered PAN card images.

- The system may have limited generalizability across different types of ID cards or across different countries, as the design and security features of ID cards can vary significantly.

- The cost and resources required for implementing the system can be a limiting factor, as it may require significant computing power and expertise to develop and maintain the system.

Objectives

- To develop an AI-based system for detecting tampered PAN cards using machine learning and image processing techniques.

- To improve the accuracy and reliability of PAN card verification by detecting tampered PAN cards.

- To reduce the risk of identity fraud and financial crimes associated with tampered PAN cards.

- To provide a cost-effective and efficient solution for PAN card verification, which can be easily integrated into existing systems.

- To enhance the security and trustworthiness of the PAN card system, which is essential for government and financial institutions to provide reliable and secure services to citizens and customers.

Innovative idea of the project

- The project proposes an innovative solution for detecting tampered PAN cards using AI-based techniques, which has the potential to improve the accuracy and reliability of PAN card verification.

- The project combines machine learning and image processing techniques to develop a robust system for tampered PAN card detection.

- The project uses a dataset of genuine and tampered PAN card images to train the system, which can improve the generalizability of the system across different types of tampering.

- The project proposes the use of deep learning techniques such as CNNs and transfer learning to improve the accuracy of the system in detecting tampered PAN cards.

- The project can contribute to the development of AI-based solutions for identity verification, which has broader applications in various domains, including healthcare, banking, and security.

Scope and application of the project

- The project has the potential to improve the accuracy and reliability of PAN card verification by detecting tampered PAN cards using AI-based techniques.

- The project can be applied in various domains, including government and financial institutions that rely on PAN card verification for providing services to citizens and customers.

- The project can potentially reduce the risk of identity fraud and financial crimes associated with tampered PAN cards, which can have significant social and economic impacts.

- The project can be integrated into existing systems for PAN card verification, which can improve the efficiency and speed of the verification process.
.

Architecture

SYSTEM ARCHITECTURE
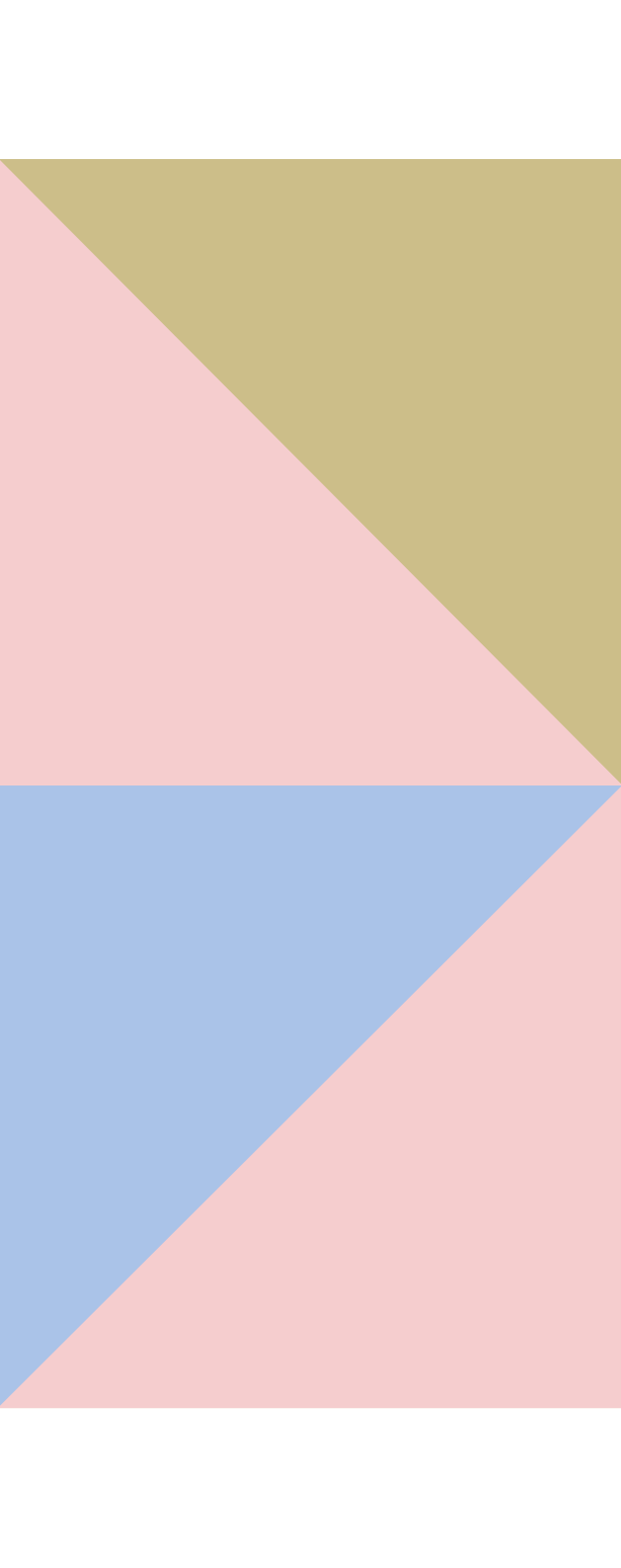
- The user interface component is responsible for allowing users to input the scanned image of their PAN card
- Which is then processed by the image processing component.
- The feature extraction component then extracts relevant features from the image, which are used by the tampering detection component to determine whether the PAN card has been tampered with or not.
- The results of the tampering detection process are stored in the database component.
- A report is generated for the user through the reporting component.

SYSTEM DESIGN


```
+-------------------------------------------------+
|                User Interface                   |
+-------------------------------------------------+
        |                       |
        |                       |
  +------------------+   +------------------+
  |  Upload          |   |  Results         |
  |  Image Form      |   |  Display         |
  +------------------+   +------------------+
        |                       |
        |                       |
+-------------------------------------------------+
|              Image Processing                   |
+-------------------------------------------------+
        |                       |
        |                       |
  +------------------+   +------------------+
  |  Image           |   |  Feature         |
  |  Pre-processing  |   |  Extraction      |
  +------------------+   +------------------+
        |                       |
        |                       |
+-------------------------------------------------+
|              Tampering Detection                |
+-------------------------------------------------+
        |                       |
        |                       |
  +------------------+   +------------------+
  |  Model           |   |  Detection       |
  |  Architecture    |   |  Algorithms      |
  +------------------+   +------------------+
        |                       |
        |                       |
+-------------------------------------------------+
|                 Database                        |
+-------------------------------------------------+
        |                       |
        |                       |
  +------------------+   +------------------+
  |  Data Entry      |   |  Reports         |
  |  & Storage       |   |  Generation      |
  +------------------+   +------------------+
```
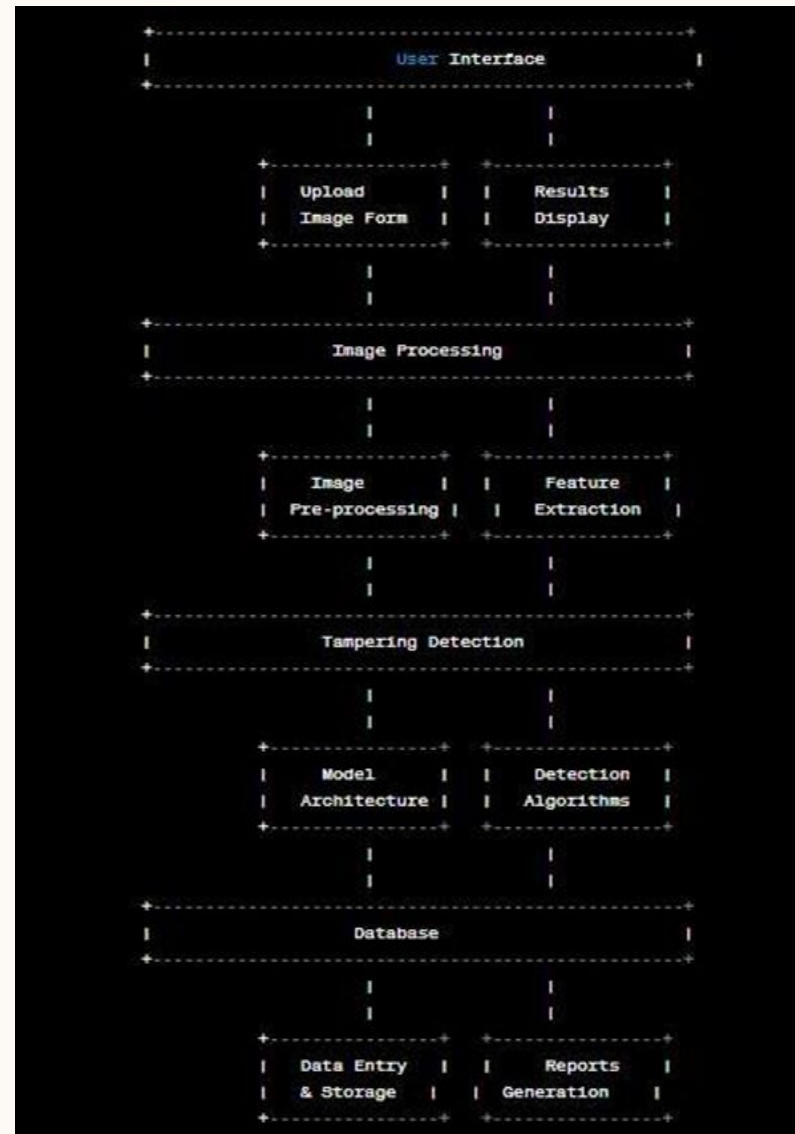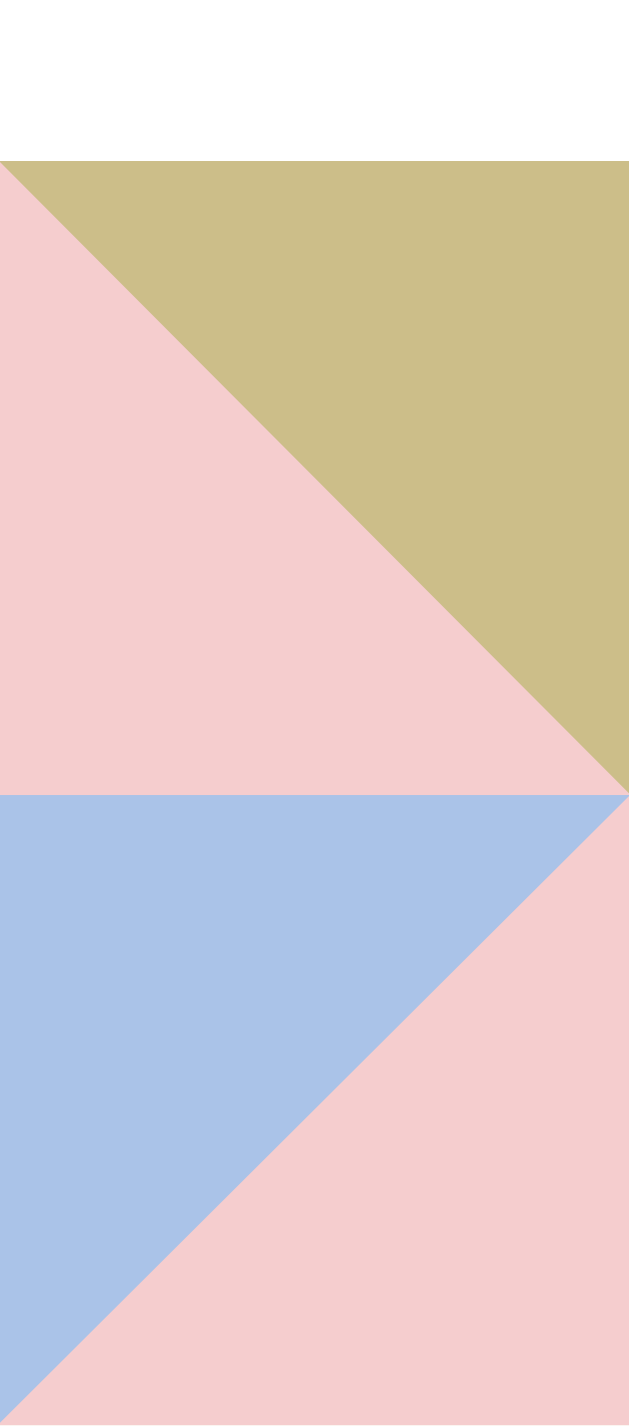
- The user interface component allows users to upload their PAN card images, which are then processed by the image processing component.
- The image processing component is responsible for pre-processing the image and extracting relevant features that are used by the tampering detection component.
- The tampering detection component consists of a machine learning model and detection algorithms that use the extracted features to detect any tampering in the PAN card image.
- The results of the tampering detection process are stored in a database, and reports are generated for the user based on the stored data.

Proposed Modules and their algorithm description

- **Image Acquisition:** This module involves acquiring the PAN card image using a scanner or a camera. The acquired image is then preprocessed to remove any noise or artifacts.

- **Image Preprocessing:** This module involves applying image processing techniques such as thresholding, smoothing, and morphological operations to remove any noise, enhance image contrast, and prepare the image for feature extraction.

- **Feature Extraction:** This module involves extracting relevant features from the preprocessed image using techniques such as scale-invariant feature transform (SIFT) or histogram of oriented gradients (HOG). The extracted features are then used to train the machine learning model.

- **Machine Learning Model:** This module involves training a machine learning model, such as a convolutional neural network (CNN), using the extracted features to classify the PAN card image as genuine or tampered. The machine learning model can also use transfer learning to improve the accuracy of the classification task.

- **Tampering Detection:** This module involves using the trained machine learning model to detect tampered PAN cards by comparing the extracted features of the input PAN card image with the features of the genuine PAN card images. If the input PAN card image is classified as tampered, an alert is generated.

- **User Interface:** This module involves providing a user interface for interacting with the system, which can display the result of the tampering detection and provide an option for the user to reacquire or retake the PAN card image.

Algorithm Description:

- The Image Preprocessing module involves applying various algorithms such as thresholding, smoothing, and morphological operations to remove any noise, enhance image contrast, and prepare the image for feature extraction.
- The Feature Extraction module can use various algorithms such as SIFT or HOG to extract relevant features from the preprocessed image, which are then used to train the machine learning model.
- The Machine Learning Model module involves training a machine learning model, such as a CNN, using the extracted features to classify the PAN card image as genuine or tampered.
- The Tampering Detection module uses the trained machine learning model to detect tampered PAN cards by comparing the extracted features of the input PAN card image with the features of the genuine PAN card images.
- The User Interface module provides a user interface for interacting with the system and displaying the result of the tampering detection.

Result

Original vs Tampered

Original Image

Differentiating Image

Threshold Image

Tampered Image

Original Image

Conclusion

- The project aims to improve the accuracy and reliability of PAN card verification by detecting tampered PAN cards using AI-based techniques.

- The proposed system involves various modules, such as image acquisition, image preprocessing, feature extraction, machine learning model, tampering detection, and user interface, which work together to achieve the objective of tampering detection.

- The project uses advanced artificial intelligence techniques, such as machine learning and deep learning, to achieve high accuracy in tampering detection.

- The project has potential applications in various domains, including government and financial institutions that rely on PAN card verification for providing services to citizens and customers.

- The project can contribute to the development of AI-based solutions for identity verification, which is a rapidly growing field with significant potential for innovation and impact.

References

1. Choudhary, A. K., & Jha, A. (2020). Tampering Detection of PAN Card using Deep Learning. International Journal of Advanced Research in Computer Science, 11(1), 78-82. (https://ijarcs.info/index.php/Ijarcs/article/view/9126)

1. Roy, S., & Saha, S. (2019, September). Detecting Pan Card Tampering Using Convolutional Neural Network. In 2019 International Conference on Data Science, Artificial Intelligence, and Business Analytics (ICDABAX) (pp. 1-6). IEEE. (https://ieeexplore.ieee.org/document/8966814)

1. Rathod, H. R., & Dabhi, V. (2018). Tamper detection of PAN card using image processing techniques. International Journal of Advance Engineering and Research (https://ijaerd.com/papers/finished_papers/Tamper%20Detection%20of%20PAN%20Card%20using%20Image%20Processing%20Techniques1220190903.pdf)

1. Nandhini, A., & Lekshmi, M. (2018). An efficient method for tamper detection of PAN. International Journal of Engineering & Technology, 7(3.21), 202-206. (https://www.sciencepubco.com/index.php/ijet/article/view/20687/9762)

1. Patil, S. S., & Raut, P. M. (2021). Tampering detection of PAN card using deep learning. International Journal of Electrical and Computer Engineering (IJECE), 11(2), 1841-1850. (https://www.iaescore.com/journals/index.php/IJECE/article/view/26788)

THANKYOU!