International Journal of Scientific Research in Engineering & Technology
Volume4, Issue2 (March-April 2024), PP: 114-115.
https://www.doi.org/10.59256/ijsreat.20240402017
www.ijsreat.com ISSN No: 2583-1240

Technological Advancements in Pan Card Security: A Robust Tampering Detection Framework

Pratik Mukherjee[1], Papia Bhowmik[2], Subhojit Samanta[3], Gokul Sarkar[4], Aparajita Mukherjee[5], Kaustuv Bhattacharjee[6], Anirban Das[7]

[1,2,3,4,5,6,7] *Department of Computer Application, University of Engineering and Management, Kolkata, West Bengal, India.*

To Cite this Article: *Pratik Mukherjee[1], Papia Bhowmik[2], Subhojit Samanta[3], Gokul Sarkar[4], Aparajita Mukherjee[5], Kaustuv Bhattacharjee[6], Anirban Das[7], "Technological Advancements in Pan Card Security: A Robust Tampering Detection Framework", International Journal of Scientific Research in Engineering & Technology Volume 04, Issue 02, March-April 2024, PP: 114-115.*

Abstract*:* *This research uses cutting-edge machine learning techniques to combat the rising problem of Pan card tampering. Our technology examines the PAN card picture and looks for any irregularities or evidence of possible manipulation. With the use of cutting-edge techniques like machine learning, identifying any questionable document may be done quickly. The present study is highly committed to the establishment of a safe digital financial environment. It allays consumers' worries about interacting with real people.*

Key Word: *Pan Card, Tampering detection, Machine Learning, Financial Security.*

I.INTRODUCTION

Pan card frauds are a growing concern of our digital society. People use fraudulent/fake pan cards for tax evasions, loans, transaction frauds and also for fake IDs. This project mainly focuses on detecting and separating of those fake PAN cards from genuine ones. We used various machine learning algorithms to distinguish them.

The implementation of this research is made with an user friendly web application where the user can sustain their doubts with some simple steps. This gives the assurance to the user that our system can definitely detect and show where the anomaly is detected.

Also users can contact us through the website to give their feedback and ask us if they are facing any problems during usage.

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.

II.BACKGROUND STUDY

The ever-increasing instances of tampering or use of counterfeit and forged IDs, also the association of these things with PAN cards underlined a need of robust and efficient detection system. A comprehensive study of existing historical literatures reveals the requirement of these kinds of research dedicated to document security.

1. "A comprehensive study of document security system, open issues and challenges" (Riaz Khan and Sajjad Lone, 2021): This research emphasizes on how privacy and security of identity documents like Passports, PAN cards, Driving License as well as other important personal documents like academic degree certificates are now at an all-time high, given how easy and cheap the new technologies make it to produce forged documents.
2. "Machine Learning Applications in Document Authentication" (Jones and Patel, 2020): This paper dives into the applications of machine learning algorithms in the realm of document authentication. It surveys the landscape of document fraud detection and discusses the potential of machine learning models to adapt and evolve in response to emerging threats.
3. "Image forgery detection: a survey of recent deep-learning approaches"(MarcelloZanardelli, Fabrizio Guerrini, Riccardo Leonardi & Nicola Adami, 2023): Mainly focusing on a survey of some of the most recent image forgery detection methods that are specifically designed upon Deep Learning (DL) techniques, focusing on commonly found copy-move and splicing attacks. Deepfake generated content is also addressed in it.

III.METHODOLOGY

To provide the solution we need to understand the problem a bit more. It says that detecting of tampering of PAN image, so to detect that we need to use various measures like different ML modules, contouring of those images, using gray scaling and comparing the image with original image in black or white.

First, we need to install the necessary libraries and packages like skimage, imutils, cv2 and requests, these are required to the project and our primary dependencies. Next, we need the image provided by the user and our original image to be of same size and format, by size here we mean the specifications of the images. Meanwhile if we need to do some re-sizing and re-formatting, those need to be done with immediate priority. Now that our images are in the favorable condition, we start the process to detect any kind of anomaly.

First, we read the images (both uploaded and original) as an image array, then we convert those into grayscale images. Next job is to calculate structural similarity, contours and threshold to detect the parts where the tampering might has happened.

We also provide the images of comparison with the contours drew on it for better understanding for the end users. Lastly, we calculate confidence score that is to what extent the image seems to be legitimate. So we are giving the image legitimate or Real status if the confidence score becomes greater than 95%.

At the end we fetch a Pan card Image object from the database based on the provided id, extracts the URLs of three images from this object, and then render the 'show.html' template with these image URLs in the web application. The user will get the confidence score and our depiction of that score and also the images as the result. They can access their previous image and it’s history by simply logging in to the application.

IV.RESULTS AND DISCUSSION

The main target of this was to find a solution to mitigate the threats of tampering and forging of PAN cards. This project is quite successful in doing that. We developed a relatively easy solution to detect any tampering in PAN cards.

We are using advanced Machine Learning algorithm to find out these things quite efficiently with minimum human involvement. As human involvement is minimized so the human errors which could be fatal to any organization is tackled with ease.

1. Performance and Accuracy: Our ML model has achieved a high degree of accuracy and has been a decent performer. It’s strength is in detection of anomally and help users in understanding flagged areas.

2. User friendly Interface: The application is easy to use and there is scope to provide useful insights regarding any difficulty in using.

3. Limitation and Future: As the technology is ever evolving so we have be on our toes to implement better techniques.We need more trustful datasets. We look forward to future enhancements.

4. Collaborative Works: We are always open to collaboration with organizations to understand more about their problems and with brainstorming it will a nice challenge to find solution for those.

V.CONCLUSION

In the culmination of the "Pan Card Tampering Detection System" project, the integration of machine learning proves to be a vital step, enhancing the security landscape surrounding PAN cards. Through a comprehensive analysis of historical tampering instances and leveraging advanced algorithms, this system demonstrates efficacy in identifying and mitigating potential security threats.

The robustness of the machine learning models fortifies the system against evolving tampering techniques. As evidenced by the project outcomes, the implementation of this system holds promise in minimizing security concerns associated with PAN cards.

Our project highlights that how can machine learning algorithms proves to be crucial for identification of an individual. This promising aspect has a broad degree of usage in various fields.

This is an ML based project and there is always scope of fine tuning and upgradation. As technology evolves, so too must our strategies for safeguarding sensitive information, and this project represents a meaningful step in that ongoing journey.

REFERENCES

[1] MachineLearningFundamentals,Medium,JavaidNabi,https://towardsdatascience.com/machine-learning-basics-part-1-a36d38c7916

[2] Machine Learning by Amit Kumar Das,Saikat Dutt,Subramanian Chandramouli, Pearson

[3] Fundamentals of Machine Learning for Predictive Data Analytics by John D. Kelleher, Brian Mac Namee, and Aoife D’Arcy

[4] A comprehensive study of document security system, open issues and challenges,Riaz Khan and Sajjad Lone, 2021

[5] Machine Learning Applications in Document Authentication,Jones and Patel, 2020

[6] Image forgery detection: a survey of recent deep-learning approaches,MarcelloZanardelli, Fabrizio Guerrini, Riccardo Leonardi & Nicola Adami, 2023