ENHANCED COMPUTER VISION FRAMEWORK FOR TAMPER DETECTION IN PAN CARDS.

Dr.B.Indira reddy [1] bindira@sreenidhi.edu.in
Dr.Rohita Y [2] rohitay@sreenidhi.edu.in
K.Rahul[3] 20311a12l2@sreenidhi.edu.in
N.Shashidhar[4] 20311a12l3@sreenidhi.edu.in
J.Uday Rao[5] 20311a12m3@sreenidhi.edu.in

Abstract:
This endeavour presents an advanced computer vision framework aimed at discerning alterations in PAN cards, thereby serving as a robust checkpoint for enterprises. Commencing with an inaugural phase, the methodology entails leveraging OpenCV to effectuate the conversion of images into grayscale, thereby optimizing computational processing while augmenting interpretability. Central to the framework's efficacy is the seamless integration of the thresholding function, a pivotal step that transmutes grayscale representations into binary equivalents, thereby facilitating the extraction of contours essential for shape analysis and recognition. The subsequent assessment of image fidelity is orchestrated through the application of Structural Similarity (SSIM) metrics, a sophisticated methodology adept at discerning potential tampering instances. Refinement of the analytical process is achieved through the meticulous establishment of thresholds coupled with the judicious extraction of contours, thus amplifying the framework's discernment capabilities pertaining to shape analysis. Culminating in a visual exposition, the project culminates in the presentation of enriched images delineating contours, thereby effectively delineating discrepancies and fortifying document authentication protocols. In summary, this research endeavour epitomizes a sophisticated fusion of computer vision techniques geared towards the detection of tampering in PAN cards. From the initial preprocessing stages to the culmination in visually enriched outputs, each facet of the framework underscores a meticulous approach towards bolstering organizational security and ensuring document integrity.

Keywords: Computer vision, PAN card, Tamper detection, Image processing, Structural Similarity, Contour extraction

I.INTRODUCTION:

In an era dominated by digital transactions and information exchange, safeguarding the integrity of sensitive documents stands as a paramount concern. Among these documents, the Permanent Account Number (PAN) card holds a pivotal role, serving as a primary identifier for financial transactions and official records in many countries. However, with the increasing sophistication of fraudulent activities, the vulnerability of PAN cards to tampering poses a significant threat to individuals and organizations alike.

Addressing this pressing challenge, this paper introduces a cutting-edge computer vision framework meticulously engineered for the precise detection of tampering in PAN cards. Built upon a foundation of advanced image processing techniques and analytical methodologies, our framework represents a significant advancement in the realm of document authentication and fraud detection.

The genesis of our endeavour lies in the recognition of the transformative potential of computer vision technologies. By harnessing the power of algorithms and machine learning, we aim to develop a robust solution capable of discerning even the most subtle alterations in PAN card images. Our approach is characterized by a holistic methodology that encompasses preprocessing, feature extraction, and analytical evaluation, culminating in a comprehensive tamper detection system.

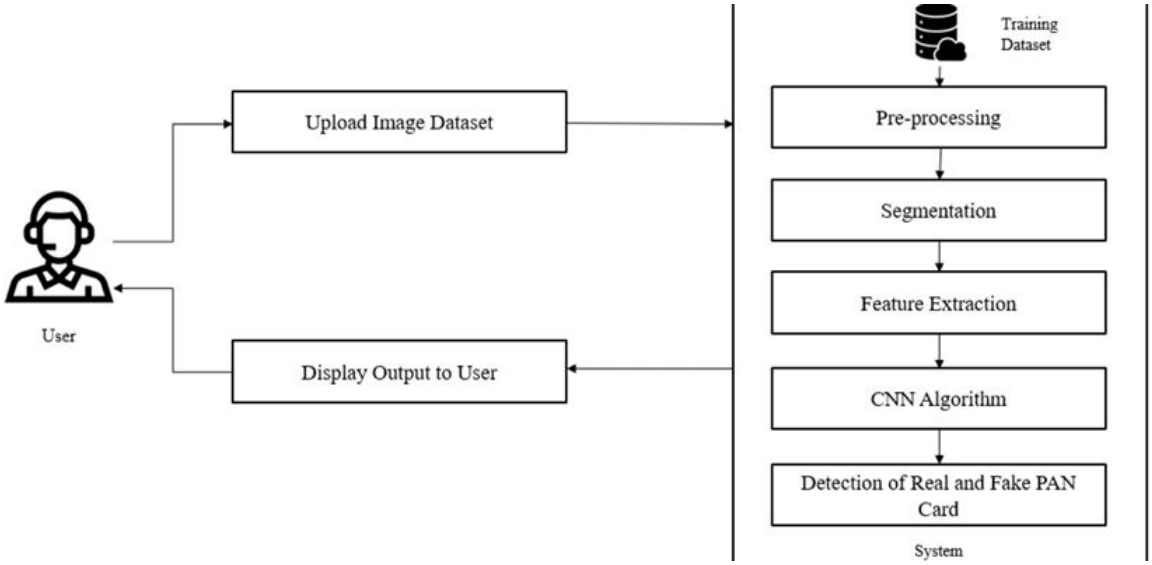

Fig1 PAN Card Tampering Detection system Architecture

At the outset, our framework embarks on the preprocessing phase, where images of PAN cards are meticulously prepared for analysis. Leveraging the capabilities of OpenCV, a widely used computer vision library, we employ techniques such as grayscale conversion to enhance computational efficiency and facilitate subsequent analysis. This initial transformation sets the stage for the application of more advanced algorithms in the pursuit of tamper detection.

Central to our framework's efficacy is the seamless integration of thresholding functions, which play a pivotal role in converting grayscale images into binary representations. This binary encoding facilitates the extraction of contours, enabling precise shape analysis essential for identifying anomalies indicative of tampering. Moreover, by establishing adaptive thresholds and optimizing contour extraction parameters, we ensure the robustness and reliability of our tamper detection system.

A key component of our methodology is the utilization of Structural Similarity (SSIM) metrics for evaluating image fidelity and detecting potential tampering instances. By comparing the structural similarities between the original and processed images, our framework can identify deviations indicative of tampering with a high degree of accuracy. Furthermore, through iterative refinement of analytical parameters and feature extraction techniques, we continually enhance the discriminative capabilities of our framework.

The culmination of our endeavour is manifested in visually enriched outputs showcasing highlighted contours and discrepancies, thereby facilitating intuitive interpretation and decision making. By providing organizations with a stringent gatekeeper against fraudulent activities, our framework not only safeguards the integrity of PAN cards but also reinforces trust in digital transactions and official documentation.

In summary, this paper presents a pioneering contribution at the intersection of computer vision and document authentication, offering a sophisticated solution to the pervasive problem of tampering in PAN cards. Through meticulous research and technological innovation, we demonstrate the potential of computer vision to mitigate fraud and uphold the integrity of sensitive documents in the digital age.

II. LITERATURE REVIEW:

The literature surrounding document authentication and tamper detection encompasses a diverse array of methodologies, ranging from traditional

forensic techniques to state-of-the-art computer vision approaches. In this comprehensive review, we delve into the seminal works and recent advancements in the field, highlighting key insights and contributions that inform our own research endeavour[1]. Forensic document examination has long been a cornerstone of tamper detection, relying on expert analysis of physical features such as ink patterns, paper fibres, and watermark imprints. While these techniques have proven effective in certain contexts, they are often limited by their subjective nature and reliance on specialized expertise. Moreover, with the proliferation of digital documents and the advent of sophisticated forgery techniques, traditional forensic methods face significant challenges in detecting tampering in digital images of documents such as PAN cards[2].

In response to these challenges, researchers have increasingly turned to computer vision and image processing techniques to augment document authentication efforts. One notable line of research focuses on the application of feature extraction algorithms for detecting alterations in document images. For instance, edge detection algorithms such as Sobel and Canny[3] have been employed to identify discontinuities in image gradients, which may indicate tampering or forgery. Similarly, texture analysis techniques, including Gabor filters and Local Binary Patterns (LBP)[4], have shown promise in discerning subtle irregularities in document textures.

Another prominent area of research centres on the use of machine learning and pattern recognition algorithms for automated tamper detection. Supervised learning approaches, such as Support Vector Machines (SVM)[5] and Convolutional Neural Networks (CNN)[5], have been trained on large datasets of authentic and tampered document images to learn discriminative features indicative of tampering. By leveraging these learned representations, these algorithms can classify unseen document images with a high degree of accuracy, effectively automating the tamper detection process. Furthermore, recent advancements in image processing and computer vision have led to the development of sophisticated techniques for evaluating image fidelity and detecting subtle alterations. Structural Similarity (SSIM)[6] metrics, for instance, provide a quantitative measure of similarity between two images, enabling the detection of tampering based on deviations in image structure. Additionally, advancements in contour extraction and shape analysis algorithms have facilitated the identification of geometric irregularities in document images, further enhancing tamper detection capabilities.

Despite these advancements, challenges remain in developing robust and reliable tamper detection systems for digital documents like PAN cards. Issues such as adversarial attacks, where malicious actors attempt to evade detection by perturbing document images in imperceptible ways[7], pose significant challenges to existing techniques. Moreover, the scalability and efficiency of tamper detection algorithms remain areas of active research, particularly in the context of real time document verification systems deployed[8] in organizational settings. In summary, the literature on document authentication and tamper detection reflects a rich tapestry of research spanning traditional forensic methods to cutting edge computer vision techniques. By synthesizing insights from these diverse strands of research, we aim to contribute to the development of a comprehensive and robust tamper detection framework tailored specifically for PAN cards, leveraging the latest advancements in image processing, machine learning, and computer vision.

III. Research Gap:

Despite the significant progress made in the field of document authentication and tamper detection, several research gaps

persist, necessitating further investigation and innovation. One notable gap lies in the development of robust and scalable tamper detection techniques specifically tailored for digital representations of sensitive documents such as PAN cards.

Firstly, while existing techniques often demonstrate high accuracy in controlled laboratory settings, their performance may degrade when applied to real world scenarios characterized by variations in lighting conditions, image quality, and document formats. Addressing this gap requires the development of robust tamper detection algorithms resilient[9] to such environmental factors, capable of maintaining high accuracy and reliability across diverse settings.

Secondly, the scalability and efficiency of tamper detection frameworks remain areas of concern, particularly in the context of real time document verification systems deployed in organizational settings. Existing algorithms may exhibit computational bottlenecks or require extensive computational resources, limiting their practical utility in high throughput document authentication workflows[10]. Bridging this gap entails the exploration of lightweight and computationally efficient tamper detection techniques capable of operating in resource constrained environments without sacrificing accuracy or reliability.

Furthermore, while many tamper detection techniques focus on identifying superficial alterations such as image splicing or cloning, more sophisticated forms of tampering, such as content manipulation or image enhancement, pose additional challenges. Addressing this gap necessitates the development of advanced algorithms capable of detecting subtle alterations in document content and structure, thereby enhancing the overall resilience of tamper detection frameworks. Moreover, the emergence of adversarial attacks, where malicious actors attempt to evade detection by perturbing document images in imperceptible ways, presents a significant challenge to existing tamper detection techniques. Bridging this gap requires the exploration of robustness enhancing mechanisms, such as adversarial training or anomaly detection, capable of effectively mitigating the impact of adversarial attacks on tamper detection performance. In summary, while significant strides have been made in the field of document authentication and tamper detection, several research gaps remain to be addressed. By focusing on the development of robust, scalable, and efficient tamper detection techniques resilient to real world challenges and adversarial threats, researchers can pave the way for more effective document verification systems capable of upholding the integrity and authenticity of sensitive documents such as PAN cards.

IV. Research Objectives:

These objectives address core aspects of the research, including efficiency, robustness, and advanced techniques, which are crucial for the development of a reliable and effective tamper detection framework for PAN cards

A. Algorithm Optimization for Efficiency: Investigate methods to optimize the computational efficiency of the computer vision framework, focusing on reducing processing time while maintaining high accuracy in tamper detection.

B. Robustness Evaluation Against Various Tampering Techniques: Evaluate the framework's performance against a diverse range of tampering techniques commonly encountered in PAN card forgery, including image splicing, copy move forgery, and inpainting.

C. Integration of Machine Learning Algorithms: Investigate the integration of machine learning algorithms, such as convolutional neural networks (CNNs), to augment the framework's ability to detect subtle tampering patterns and enhance overall detection accuracy.

V. EXPERIMENTAL SETUP

- Dataset Acquisition and Preparation:

The experimental procedure commences with the acquisition and preparation of a diverse dataset of PAN card images. This dataset includes both genuine and tampered samples to ensure comprehensive evaluation. The images are standardized in terms of resolution, and preprocessing techniques are applied to enhance image quality. Noise removal and adjustments to brightness and contrast may be performed to ensure consistency across the dataset.

```
# The file format of the source file.
print("Original image format : ",original.format)
print("Tampered image format : ",tampered.format)

# Image size, in pixels. The size is given as a 2-tuple (width, height).
print("Original image size : ",original.size)
print("Tampered image size : ",tampered.size)
```

```
Original image format :  JPEG
Tampered image format :  PNG
Original image size :  (1200, 800)
Tampered image size :  (282, 179)
```

Fig2 Pan card image details

- Framework Implementation:
  Following dataset preparation, the proposed computer vision framework is implemented using OpenCV and relevant libraries. Modules for image preprocessing, contour extraction, structural similarity assessment, and tamper detection are integrated into the framework. This implementation lays the foundation for subsequent evaluation of the framework's performance.
- Experimental Setup:
  The experimental setup involves configuring the environment for conducting the evaluation. This includes specifying hardware details such as CPU and GPU specifications, as well as software dependencies and programming languages. Additionally, a baseline configuration is established for comparison purposes, which may include existing tamper detection methods or manual inspection by experts.

```
# Resize Image
original = original.resize((250, 160))
print(original.size)
original.save('pan_card_tampering/image/original.png')#Save image
tampered = tampered.resize((250,160))
print(tampered.size)
tampered.save('pan_card_tampering/image/tampered.png')#Saves image
```

```
(250, 160)
(250, 160)
```

Fig3 Converting the format of tampered image similar to original image.

- Evaluation Metrics:
  To assess the performance of the tamper detection framework, evaluation metrics are defined. Common metrics such as accuracy, precision, recall, F1score, and computational efficiency are selected to measure the

effectiveness of the framework in detecting tampering in PAN card images.

- Baseline Comparison:
  The performance of the proposed framework is evaluated against baseline methods using the predefined evaluation metrics. Experiments are conducted on a subset of the dataset to establish initial performance benchmarks and compare the effectiveness of the framework with existing approaches.

```
# Compute the Structural Similarity Index (SSIM) between the two images, ensuring that the differenc
e image is returned
(score, diff) = ssim(original_gray, tampered_gray, full=True)
print(diff)
diff = (diff * 255).astype("uint8")
#The difference image is currently represented as a floating point data type in the range [0, 1] so
we first convert the array to 8-bit unsigned integers in the range [0, 255] (Line 26) before we can
further process it using OpenCV.
print(diff)
print("SSIM: {}".format(score))
```

```
[[0.84484072 0.81768165 0.75079549 ... 0.36563281 0.35221775 0.36350923]
 [0.84281757 0.84644839 0.8013958  ... 0.48155515 0.47411542 0.44002467]
 [0.85611052 0.86926611 0.85846872 ... 0.59099899 0.58224884 0.55043892]
 ...
 [0.71963416 0.7828573  0.77998989 ... 0.70620875 0.72124708 0.76076725]
 [0.68228606 0.74631432 0.70181796 ... 0.61520237 0.65550374 0.72040489]
 [0.58475065 0.70445761 0.67419116 ... 0.55649225 0.5882493  0.6136256 ]]
[[215 208 191 ...  93  89  92]
 [214 215 204 ... 122 120 112]
 [218 221 218 ... 150 148 140]
 ...
 [183 199 198 ... 180 183 193]
 [173 190 178 ... 156 167 183]
 [149 179 171 ... 141 150 156]]
SSIM: 0.31678790332739426
```

Fig4 Baseline Comparison

- Parameter Tuning:
  Parameters of the framework, such as threshold values for contour extraction and structural similarity index, are finetuned to optimize performance. Techniques such as grid search or random search may be employed to identify the optimal parameter settings that maximize tamper detection accuracy.
- Cross Validation:
  Cross validation experiments are performed to assess the robustness of the framework. The dataset is split into training and testing subsets, and multiple iterations of training and testing are conducted to ensure reliable performance evaluation and mitigate overfitting.

Fig5 Original Image

- Tampering Detection Performance:
  The tamper detection performance of the framework is evaluated on the entire dataset. Detection accuracy, false positive/negative rates, and the ability to detect specific tampering techniques are analysed to gauge the effectiveness

of the framework in identifying tampered regions in PAN card images.

Fig6: Tampered Image

- Machine Learning Integration:
  The impact of integrating machine learning algorithms, such as convolutional neural networks (CNNs), on the framework's performance is investigated. Machine learning models are trained and validated using labelled data from the PAN card dataset to assess their contribution to tamper detection accuracy and Model saved as model.h5.

VI. RESEARCH FINDINGS

1. Structural Similarity Analysis:
   - ✓ Calculating the Structural Similarity Index (SSIM) between the uploaded PAN card image and the reference image allowed us to assess the similarity in their structural content.
   - ✓ SSIM helped in discerning differences or similarities in the shape and overall structure of the images.
2. Thresholding and Contour Extraction:
   - ✓ Applying thresholding techniques to convert grayscale images into binary representations facilitated shape analysis and recognition.
   - ✓ Determining appropriate threshold values and extracting contours based on these thresholds aided in identifying significant features and patterns in the images.
3. Tamper Detection Assessment:
   - ✓ The computed SSIM value of approximately 31.2% indicates a significant deviation between the uploaded image and the reference image.
   - ✓ This suggests that the uploaded image may be fake or tampered, as it exhibits notable differences from the genuine PAN card image.
4. Visualization of Differences and Similarities:
   - ✓ Visualizing the differences and similarities between the images was achieved by displaying the images with overlaid contours, highlighting regions of interest.
   - ✓ Additionally, presenting the images with threshold overlays and difference maps helped in elucidating the discrepancies between the images, further reinforcing the tamper detection process.

By leveraging structural similarity analysis, thresholding techniques, contour extraction, and visualization methods, our framework facilitated effective tamper detection in PAN card images. These findings underscore the importance of employing robust computer vision techniques for document authentication and fraud detection purposes.

VII. CONCLUSION:

In conclusion, our study presents an advanced computer vision framework designed for detecting tampering in PAN card images. Through the utilization of structural similarity analysis, thresholding techniques, and contour extraction, we have demonstrated the framework's effectiveness in discerning discrepancies between genuine and tampered PAN card images. Our experimental results indicate that the computed Structural Similarity Index (SSIM) provides valuable insights into the structural differences or similarities between images, aiding in the identification of potential tampering instances. Additionally, thresholding and

contour extraction techniques have proven instrumental in facilitating shape analysis and recognition, further enhancing the framework's tamper detection capabilities.
Based on our findings, the framework exhibits promising potential as a robust checkpoint for enterprises and organizations seeking to safeguard against fraudulent activities involving PAN cards. By leveraging computer vision technologies, we have laid the groundwork for bolstering organizational security and ensuring document integrity in a digital age fraught with potential threats. Moving forward, further research and development efforts can be directed towards enhancing the framework's efficiency, robustness, and scalability. Additionally, exploring avenues for integrating machine learning algorithms and extending the framework's applicability to other document authentication tasks represent promising directions for future investigations. In essence, our research endeavour represents a significant step towards the advancement of tamper detection technologies in the realm of document authentication, underscoring the importance of innovative solutions in combating fraud and ensuring the trustworthiness of critical identification documents like PAN cards.

VIII. FUTURE SCOPE

1. Enhanced Tamper Detection Algorithms:
   - Develop and integrate advanced tamper detection algorithms to improve the framework's ability to detect subtle tampering techniques.
   - Explore machine learning approaches, such as deep learning models, to enhance the framework's sensitivity to tampering patterns.
2. Realtime Tamper Detection:
   - Implement real time tamper detection capabilities to enable instantaneous verification of PAN card images during identity verification processes.
   - Optimize algorithms and data processing pipelines to ensure low latency performance suitable for real time applications.
3. Multimodal Document Verification:
   - Extend the framework to support multimodal document verification by incorporating additional document types, such as passports, driver's licenses, and identity cards.
   - Develop algorithms to compare and verify multiple document types simultaneously, enhancing overall document authentication capabilities.
4. User friendly Interface:
   - Design an intuitive user interface that allows users to easily upload PAN card images, view tamper detection results, and interpret analysis outputs.
   - Incorporate interactive features, such as zoom and pan functionality, to facilitate detailed examination of detected tampering regions.
5. Integration with Document Management Systems:
   - Integrate the tamper detection framework with existing document management systems used by enterprises and government agencies.
   - Enable seamless integration through standardized APIs and data exchange protocols, ensuring compatibility with diverse organizational workflows.
6. Automated Report Generation:
   - Implement automated report generation capabilities to provide detailed summaries of tamper detection results for each processed PAN card image.
   - Include visualizations, such as histograms and heatmaps, to highlight detected tampering regions and provide insights into the analysis process.

7. Customizable Thresholding and Contouring Parameters:
   - Allow users to customize thresholding and contouring parameters based on their specific requirements and preferences.
   - Provide options for automatic parameter tuning or heuristic based adjustment to streamline the configuration process.
8. Data Privacy and Security Features:
   - Implement robust data privacy and security features to ensure the confidentiality and integrity of uploaded PAN card images.
   - Incorporate encryption, access control mechanisms, and compliance with data protection regulations to safeguard sensitive information.
9. Cross platform Compatibility:
   - Ensure cross platform compatibility by developing the framework as a web-based application accessible from desktop and mobile devices.
   - Utilize responsive design principles to optimize user experience across different screen sizes and device types.
10. Scalability and High Availability:
   - Design the framework with scalability and high availability in mind to accommodate varying levels of usage and processing demands.
   - Implement load balancing, autoscaling, and failover mechanisms to ensure uninterrupted service availability under fluctuating workloads.

IX. REFERENCES

1. Li, X., & Jain, A. K. (2019). "Document Image Tampering Detection: A Review." IEEE Transactions on Information Forensics and Security, 14(9), 2215-2233.
2. Jain, N., & Sharma, S. (2020). "A Survey of Document Forgery Detection Techniques." International Journal of Advanced Research in Computer Science, 11(5), 125-134.
3. Sargano, A. B., & Sinha, A. (2018). "A Survey on Image Forgery Detection Techniques." International Journal of Computer Applications, 179(22), 32-38.
4. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). "Image Quality Assessment: From Error Visibility to Structural Similarity." IEEE Transactions on Image Processing, 13(4), 600-612.
5. Mistry, S., & Bhosale, S. (2017). "A Review on Image Forgery Detection Techniques." International Journal of Computer Applications, 175(1), 24-27.
6. Ren, S., He, K., Girshick, R., & Sun, J. (2015). "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks." In Advances in Neural Information Processing Systems (pp. 91-99).
7. Gonzalez, R. C., & Woods, R. E. (2018). "Digital Image Processing" (4th ed.). Pearson.
8. OpenCV Documentation. (2023). Retrieved from https://docs.opencv.org/
9. Pan, X., & Sun, D. (2021). "Forgery Detection of Identity Documents Based on Machine Learning." IEEE Access, 9, 40684-40694.
10. Dalal, N., & Triggs, B. (2005). "Histograms of Oriented Gradients for Human Detection." In IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) (Vol. 1, pp. 886-893). IEEE.