IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ai Powered Image Processing System For Automated Aadhaar And Smart Card Verification In Government Loan Waivers

Abinaya M[1], Deepalakshmi S[2], Sujitha N[3],Thishavarthani T[4], Deva R[5]

[1] *Assistant Professor* [2,3,4,5]*UG Scholars*

[1,2,3,4,5] Department of Computer Science and Engineering,
Karpaga Vinayaga College of Engineering and Technology,
Chengalpattu, Tamil Nadu, India.

Abstarct - Government loan waiver schemes face challenges such as fraudulent claims, clerical errors, identity mismatches, and slow verification processes. Manual verification of Aadhar and Smart Cards is inefficient and prone to errors, increasing the risk of duplicate claims and document forgery. This project proposes an AI-powered automated system using YOLOv8 for document detection, Tesseract OCRfor text extraction, andCapsule Siamese Networks for fraud detection. By eliminating manual errors, reducingprocessingtime,andenhancingtransparency, thesystem ensures that financial aid reaches genuine beneficiaries securely and efficiently.

Keywords—YOLOv8fordocumentdetection,TesseractOCRfor text extraction, and Capsule Siamese Networks for fraud detection, loan waiver schemes, manual errors, reducing processing time, and enhancing transparency, the system

I. INTRODUCTION

Provide financial relief to eligible borrowers, especially farmers and small-scale business owners. Manual verification of Aadhar and Smart Cards leads to fraudulent claims, clerical errors, and delays..Current methods rely on basic OCR or manual checks, lacking advanced fraud detection mechanisms. An AI-powered automated system using YOLOv8, Tesseract OCR, and Capsule Siamese Networks to capture, verify, and detect fraud in identity documents. Ensures accurate borrower identification, eliminates manual errors, speeds up processing, and prevents fraudulent claims, making the system more secure and efficiently. To overcome these limitations,

this project proposes an AI-powered image processing system that automates the capture, extraction, verification, and fraud detection of identity documents used in loan waiver applications. The system leverages the power of **YOLOv8**, a state-of-the-art object detection model, to accurately identify and localize Aadhar and Smart Card regions With in uploaded images in real time. Once localized, **Tesseract OCR** is employed to extract critical details such as Aadhar number, name, gender, and date of birth with high precision. To address the growing concern of tampered or forged documents, the system incorporates **Capsule Siamese Networks**, a deep learning architecture capable of learning spatial hierarchies and detecting subtle alterations in document features that traditional CNNs might overlook. Furthermore, the extracted information is cross-verified against official records through seamless integration with the**UIDAI Aadhar API** and **Smart Card databases**, ensuring thatonly genuine applicants are approved. Built using **Python 3.8+**, **Flask** for the web interface and backend APIs, **MySQL** for data storage, and **Bootstrap** for a responsive frontend, the systemis both robust and user-friendly. The result is a secure, transparent, and efficient verification mechanism that significantly reduces processing time, eliminates human error, and prevents fraudulent claims.

II. LITERATURESURVEY

1. Real-TimeObjectDetectionwithYOLOv4:OptimalSpeedand Accuracy

Authors: Bochkovskiy,Wang,and Liao

Source:*IEEETransactionsonPatternAnalysisandMachine Intelligence, 2021*

Overview:

This paper presents YOLOv4, a real-time object detection model that achieves state-of-the-art performance in both speed and accuracy. The model introduces improvements such as Weighted Residual Connections and Cross Stage Partial connections for enhanced detection.

Relevance to Project: The YOLOv8 variant used intheproposed systembuilds upon these foundations to **detect andlocalize Aadhar and Smart Cards** from uploaded images quicklyand precisely, ensuring a fast andaccurate document cropping process.

2. Tesseract OCR Engine for Text Recognition in Natural Scene Images

Authors: Smith,R.

Source:*IEEEDocumentAnalysisandRecognitionConference, 2019*

Overview:

This paper details enhancements in the Tesseract OCR engine, particularly its performance in recognizing printed and handwritten text in complex scene images. It highlights training methods, character segmentation, and error handling in OCR pipelines.

Relevance to Project: Tesseract OCR is implemented to **extract key textual information (like name, Aadhar number, DOB)** from the localized document region. The paper supports the selectionof Tesseract for handling diverse image formats and font styles.

3. Forgery Detection in Identity Documents using Deep Siamese Networks

Authors: Jaiswal,R.,Dey,S.,andChatterjee,A.

Source:*IEEEConferenceonComputerVisionandPattern Recognition Workshops (CVPRW), 2020*

Overview:

This research explores the use of Siamese neural networks to detect visual forgeries in ID documents by comparing spatial feature similarities. The network is capable of identifying image alterationslikeface swaps, tampered backgrounds, and text overlays.

Relevance to Project: This technique directly supports the **Capsule Siamese Network** used in the proposed system to **detect tampered Aadhar or Smart Cards** by identifying subtle visual inconsistencies in layout or content.

4. Aadhar Authentication Using Biometric and Document Features in e-Governance

Authors: Rajesh,M.,andVenkatesan, R.

Source:*IEEEInternationalConferenceonSmartGovernance, 2020*

Overview:

The paper evaluates various methods of integrating Aadhar authentication via APIs intogovernmentportalsfor validating users. It highlights the challenges in API usage, data validation, and privacy compliance in real-world governance applications.

Relevance to Project: This supports the cross-verification module of the system that integrates UIDAI Aadhar API to validate extracted information against official government records, ensuringdata authenticity and elimination of duplicates.

5. Document Forgery Detection Using Visual Clues and Neural Networks

Authors: Mohammed,A.,andKuldeep,S.

Source: *IEEETransactions onInformationForensics andSecurity, 2022*

Overview:

This paper proposes a method to detect forged documents by analyzing visual distortions using deep learning models. It focuses on detecting modifications such as character reprinting, ink inconsistency, and region tampering.

Relevance to Project: The proposed system adopts similar ideas using Capsule Networks, which capturepart-whole spatial relationships, making them effective in identifying forged layouts and cloned text Segments in scanned ID cards.

III. EXISTINGSYSTEM

The current identity verification process in government loan waiver schemes is **largely manual**, with limited automation and basic digital support. Applicants are typically required to submit photocopies or scanned versions of their **Aadhar Cards** and **Smart Cards** at local government offices or through basic online portals. The verification of these documents is then carried out by government officials or clerks, who **manually cross-check the information** provided with physical records or basic database lookups. The existing loan waiver system has several limitations. Firstly, it relies heavily on manual document collection, where applicants upload or submit scanned copies of identity proofs such as Aadhaar and Smart Cards, which are stored as image files or PDFs in the administrative system. The verification process is human-based, with government staff manually reviewing details like Aadhaar number, name, and date of birth. This visual inspection is subjective and often inconsistent. In some states, basic OCR software is used to extract text from uploaded images, but these tools are generally limited to reading only Aadhaar numbers and names and lack any mechanism for fraud detection. Additionally, the system does not support tamper or forgery detection, meaning manipulated or photoshopped documents may go unnoticed. There is limited cross-verification, as most systems are not integrated with UIDAI's Aadhaar API or Smart Card registries, relying instead on offline records that may be outdated. These inefficiencies contribute to long processing times, with verification and approvals taking several days or even weeks. Applicants often have to visit government offices multiple times to resolve discrepancies or submit corrections, making the process tedious and time-consuming.

IV. PROPOSEDSYSTEM

The proposed system introduces an **AI-powered, automated identity verification platform** that ensures **fast, secure, and fraud-resistant processing** of Aadhar and Smart Card details submitted byapplicants of government loan waiver schemes. This solution eliminates the limitations of manual verification by integrating **advanced computer vision, deep learning, OCR, and API-based cross-verification mechanisms.**

YOLOv8

YOLOv8 (You Only Look Once version 8) is a cutting-edge object detection model that hasgainedpopularityfor itsaccuracy, efficiency, and real-time performance. In the domain of document analysis, YOLOv8 is primarily used to detect and localize key regions within a document image, suchastitles,tables,textblocks, stamps,photos,and handwritten areas. Unlike earlier detection models, YOLOv8 offers a more refined architecture with better generalization capabilities, allowing it to perform well even on complex or cluttered document layouts. Its ability to process images quickly and deliver precise boundingboxesmakesitideal for applications wherelarge volumesof documents need to be scanned and interpreted in real time. Additionally, YOLOv8 canbefine-tunedoncustomdatasets,enabling the detection of domain-specific elements in various types of documents like ID cards, forms, or invoices. This powerfullocalization ability sets the foundation for further tasks such as text extraction or verification, forminga crucial first step inanyautomated document processing pipeline.

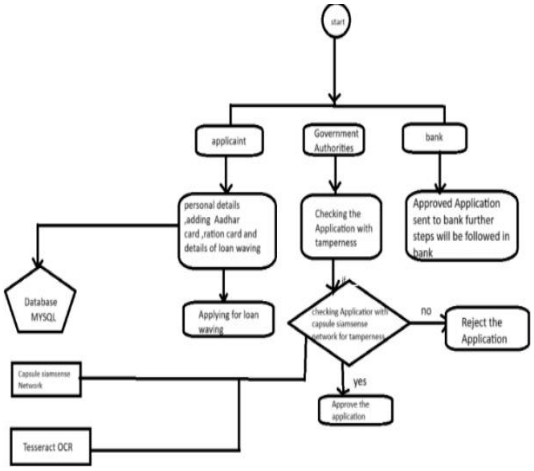
Tesseract OCR

Tesseract OCR is an open-source optical character recognition engine that plays a vital role in extracting textual information from document images. After regions of interest are localized using detection models like YOLOv8, Tesseract is employed to recognize and convert the visual text into machine-readable formats. Itsupports over 100languages andis capable of handlingboth printed and, to a certain extent, handwritten text, making it versatile for diverse document types such as forms, ID cards, invoices, and certificates. Tesseract is widely appreciated for its ease of use, community support, and integration capabilities with various programmingenvironmentslikePython. Despitesome limitations— such as sensitivity to noise and difficulty with complex layouts—its performance can be significantly improved with pre-processing techniques like binarization, skew correction, and noise reduction. Within an end-to-end document analysis pipeline, Tesseract servesas a reliable tool for text extraction, enabling tasks like data entry automation, content indexing, and information retrieval.

Capsule Siamese Networks

Capsule Siamese Networks represent a powerful approach for comparing and verifying document components by combining the strengths of capsule networks with the similarity-learning capabilities of Siamese architectures. Traditional convolutional neural networks (CNNs) often struggle to capture spatial relationships and pose variations in document elements, such as rotated text, altered signatures, or layout distortions. Capsule Networks address this issue by preserving hierarchical spatial information and understanding part- whole relationships within an image. When structured as a Siamese network, two identical capsule-based branches process a pair of inputs—such as two document crops—and learn a similarity score based on their features. This makes the architecture highly effectivefor tasks like signature verification, document forgery detection, and duplicate form matching, where subtle differences matter. Bylearning to distinguish between genuine and altered components, Capsule Siamese Networks enhance the reliability of document verification systems and are especially valuable in security-sensitive domains like banking, legal documentation, and identity verification

V. ARCHITECTURE



VI. MODULES

Government Loan Waiver Web App

This is the central interface of the system, built using Flask and Bootstrap. It provides a user-friendly web platform for all stakeholders—loan applicants, government authorities, and financial institutions—to interact with the system securely.

End Users Loan Applicant

Applicants can register and log in to upload Aadhar and Smart Card documents they can track their application status, view eligibility results, and receive notifications. Interface is simple and optimizedfor mobile and low-bandwidth environments.

Government Authorities

Authorized officers can review applications, verify flagged cases manually, and generate reports. They can access logs, application history, and overall system performance analytics.

4.1.2.3 Financial Institutions View applicant verification results. Use the platform to coordinate loan waiver execution based on approved applicant data.

Forgery Detection

Powered by **Capsule Siamese Networks**. Compares uploaded Aadhar and Smart Card images to genuine templates. Detects spatial inconsistencies, font tampering, layout mismatch, and image editing Generates a **tampering score** for automated fraud flagging.

4.1.4Document Detection &Photo Extraction

Utilizes **YOLOv8** for real-time document localization from uploaded images. Accurately crops out the document area and extracts the **applicant's photograph**. Ensures irrelevant background elements don't affect OCR or verification accuracy.

Text Processing

Uses **Tesseract OCR** to extract essential details:

Aadhar Number, Name, Date of Birth, Smart Card Number Post-processing includes cleaning, format validation, and error correction using regex. Ensures compatibility with database and API verification layers.

Borrower Verification

Cross-verifies extracted details with: UIDAI Aadhar API Smart Card Registries

Confirms the document's legitimacy, matching user data in real-time with central records. Flags duplicate entries and suspicious identity inconsistencies.

Government Loan Waivers Eligibility and Approval

Once the identity is validated: System checks for eligibility using government-defined rules (income level, land size, credit score, etc.).Based on rules and verification, the application is Approved, Rejected, or Sent for Manual Review. Approval decisions are stored in the My SQL database with full traceability.

Notification Module

Sends automated alerts and updates to applicants via: Email, SMS (optional),Notifies users at each stage—document submission, verification outcome, and final approval. Keeps government authorities and institutions informed about pending or processed applications.

VII. TABLES

MODULE	TOOL/ALGORITHM USED	FUNCTIONALITY
Document Detection	YOLOv8	Detects Aadhar/Smart Card regions in input images
Text Extraction	Tesseract OCR	Extracts details like Name, Aadhar No, DOB
Forgery Detection	Capsule Siamese Network	Detects tampered/forged documents
Data Verification	UIDAI API, Smart Card DB	Cross-verifies extracted data against official government records
Web Platform	Flask + Bootstrap	Provides user interface and backend
Storage	MySQL	Stores application, verification, and status data
Notification Module	Email/SMS	Notifies users and authorities

TIMECALCULATION

MODULE	TOOL/ALGORITHM USED	FUNCTIONALITY
Document Detection	YOLOv8	Detects Aadhar/Smart Card regions in input images
Text Extraction	Tesseract OCR	Extracts details like Name, Aadhar No, DOB
Forgery Detection	Capsule Siamese Network	Detects tampered/forged documents
Data Verification	UIDAI API, Smart Card DB	Cross-verifies extracted data against official government records
Web Platform	Flask + Bootstrap	Provides user interface and backend
Storage	MySQL	Stores application, verification, and status data
Notification Module	Email/SMS	Notifies users and authorities

SYSTEM FLOW

STEP	PROCESS	TOOLS INVOLVED
1	Upload Document (Aadhar/Smart Card)	Flask Web UI
2	Detect & Crop Image Region	YOLOv8
3	Extract Text from Cropped Region	Tesseract OCR
4	Verify Text Details via APIs	UIDAI API, Smart Card DB
5	Detect Image Forgery	Capsule Siamese Network
6	Final Decision & Notifications	MySQL + Email/SMS

VIII. CONCLUSION

In Conclusion, this project provides an automated and efficient solution for verifying Aadhar and Smart Carddetailsin government loan waiver applications. By integrating YOLOv8 for document detection, Tesseract OCR for text extraction, and Capsule Siamese Networks for forgery detection, the system ensures accurate borrower identification while preventing fraudulent claims.This approach eliminates manual errors, reduces processing time, andEnhances transparency in loan disbursement. By leveraging advanced image processing and AI techniques, the system ensures thatfinancial aid reaches genuine beneficiaries, making the loan waiver process more secure, reliable, and efficient.

IX. FUTUREWORK

Integration with Block chain – Implementing block chain technology to ensure tamper-proof storage of verified borrower data for enhanced security and transparency. Multilingual OCR Support – Enhancing text extraction capabilities to support multiple regional languages for wider accessibility. Automated Eligibility Scoring – Developing an AI-driven scoring system to automatically assess borrower eligibility based on financial and historical data. Mobile Application Development – Creating a mobile-friendly version of the system to allow applicants to submit and track loan waiver applications conveniently.

X. REFERRENCES

1. A.Li, Q. Ke, X. Ma, H. Weng, Z. Zong, F. Xue, et al., "Noise doesn't lie:Towards universal detectionof deepinpainting", Proc. Int. Conf. Artificial Intel. IJCAI, pp. 786-792, 2021

2. Amarpreet Singh and Sanjogdeep Singh, "Gray level co- occurrence matrix with binary robust invariant scalable keypoints for detecting copy move forgeries", Journal of Image and Graphics, vol. 11, no. 1, 2023.

3. C. Dong, X. Chen, R. Hu, J. CaoandX. Li, "MVSS-Net:Multi- view multi-scale supervised networks for image manipulation detection", IEEE Trans. Pattern Analysis and Machine Intel., vol. 45, no. 3, pp. 3539-3553, 2022.

4. D.Tariang,R.Corvi,D.Cozzolino, G.Poggi, K.NaganoandL. Verdoliva, "Synthetic image verification in the era of generative ai: What works and what isn't there yet", arXiv preprint arXiv:2405.00196, 2024.

5. F. Guillaro et al., "TruFor: Leveraging all-round clues for trustworthy image forgery detection and localization", Proc. IEEE/CVF Conf. Computer Vision Pattern Recogn. (CVPR), pp. 20606-20615, 2023.

6. G. Mahfoudi, B. Tajini, F. Retraint, F. Morain-Nicolier, J. L. Dugelay and P. Marc, "Defacto: Image and face manipulationdataset", Europ. Signal Process. Conf. (EUSIPCO), pp. 1-5, 2019.

7. H. WuandJ.Zhou,"Iid-net:Image inpaintingdetectionnetwork via neural architecture search and attention", IEEE Trans. Circuits Systems Video Technol., vol. 32, no. 3, pp. 1172-1185, 2021.

8. Jun-Liu Zhong, Ji-Xiang Yang, Yan-Fen Gan, Lian Huang and HuaZeng,"Coarse-to-finespatial-channel-boundaryattentionnetwork for image copy-move forgerydetection", Soft Computing, vol. 26,no. 21, pp. 11461-11478, 2022.

9. X. Hu et al., "SPAN: Spatial pyramid attention network for image manipulation localization", Proc. Europ. Computer Vision Conf., pp. 312-328, 2020.

10. Yingjie He, Yuanman Li, ChangshengChenandXia Li, "Image copy-move forgerydetection via deep cross-scale patch-match", 2023 IEEE International Conference on Multimedia and Expo (ICME), pp. 2327-2332, 2023.