IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Deep Learning-Powered Document Verification for Loan Waiver Automation Using OCR-CRNN

[1]Dr. Kalavathi S, [2] Dr. Rajalakshmi S, [3]Venkata Naga Saiteja Bhumaraju, [4]Sai Sriraman B

[12]Associate Professor, [34]Student,

[1234]Department of Computer Science and Engineering,

[1234]Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur, India-602117

Abstract:

The verification process for identifying genuine borrowers eligible for government loan waivers is often problematic due to manual errors, time delays, and susceptibility to fraud. To address these challenges, this paper introduces a comprehensive image processing solution utilizing Optical Character Recognition (OCR) and Convolutional Recurrent Neural Networks (CRNNs) for accurate extraction and validation of details from Aadhaar and smart cards. OCR is employed to extract text precisely from document images under diverse situations, such as varying lighting, noise, and orientations, while CRNNs are utilized for validating the authenticity of the extracted information and detecting potential anomalies or counterfeit documents. Advanced pre-processing techniques, including image enhancement and normalization, are integrated to improve recognition accuracy and minimize errors. The system is further designed to interface with cloud-based databases, enabling real-time cross-referencing and validation against existing records, ensuring scalability and operational efficiency. By automating the verification process, the solution reduces clerical errors, processing time, and manual intervention, while safeguarding sensitive data through robust security measures. This approach not only enhances transparency and fairness in the loan waiver process but also provides a scalable and reliable framework for similar public sector applications requiring efficient document authentication and fraud detection.

IndexTerms **-** Aadhaar card verification, Optical Character Recognition, Convolutional Recurrent Neural Networks, Government Loan Waivers, Fraud detection.

I. INTRODUCTION

In recent years, computer automation techniques have increasingly replaced traditional methods of document verification. The conventional approach to document verification is highly prone error as it depends on human intervention. Factors such as negligence in thoroughly reading details, the likelihood of typing errors during manual data entry, and the inability to distinguish authentic documents from fraudulent ones contribute to its unreliability. These issues can have significant consequences, such as denying a loan waiver to an eligible individual due to human error. To address these challenges, Artificial Intelligence (AI) and Machine Learning (ML) techniques, particularly Optical Character Recognition (OCR) and Convolutional Recurrent Neural Networks (CRNNs), are employed to eliminate human clerical mistakes. Recent research has utilized OCR and MobileNet V2 to automate ID card recognition and verification for remote onboarding processes, especially in banking applications. By leveraging these deep learning techniques, the framework has shown significant improvements in speed, reliability, and scalability while effectively addressing challenges like noise, lighting variations, and perspective distortions in document images. This approach not only enhances service quality but also ensures the secure and efficient handling of sensitive personal data. Additionally, another study successfully applied OCR and CNN-based image processing techniques to recognize Arabi documents, accurately identifying genuine documents and detecting fraud. Building on this prior research, the OCR-CRNN approach has been identified as the optimal solution. OCR's high accuracy, combined with the complexity and adaptability of CRNN, offers a sophisticated yet straightforward method to improve document verification processes effectively.

II. LITERATURE REVIEW

This section reviews the existing research previously done on verifying documents using advanced image processing and machine learning techniques. These approaches have greatly impacted the methods that are used for the document verification process and checking eligibility for loan waiving by providing a different perspective on dealing with the problems encountered while using the traditional methods. One significant research [1] had proposed an image processing and OCR- based system for recognizing ID cards during online onboarding, achieving 99% detection accuracy using MobileNet V2 and CNN architectures. However, it had a few flaws, such as reliance on high-quality input images, potential vulnerability to fraud, and limited testing on diverse document types or real-world conditions. The solution may struggle with low-resolution or distorted images. Another research [2] focused on verifying Arabic documents using Machine learning techniques such as CNN and introduced ADOCRNet, a deep learning- based OCR system for Arabic document recognition, which combined CNNs, BLSTM, and CTC to achieve high accuracy. However, this research was found to have limited testing on diverse real-world conditions (e.g., low-quality images or complex backgrounds) and reliance on extensive data augmentation, which may not generalize well to unseen fonts or handwriting styles.

Different research [6] focused on the methods which can be implemented for document verification which includes signature or stamp verification, image processing, and machine learning, emphasizing applications in finance, legal, and identity sectors but this research had limited discussion on real- world scalability, reliance on controlled environments, and insufficient exploration of adversarial attacks (e.g., deepfakes). The proposed unified framework lacks empirical validation. Another research [7] has been done on document verification techniques such as digital signatures, which provided a unified framework for fraud prevention. However, this research overlooks interoperability challenges between hybrid (digital/physical) systems and has insufficient scalability testing for high- volume applications.

III. RESEARCH METHODOLOGY

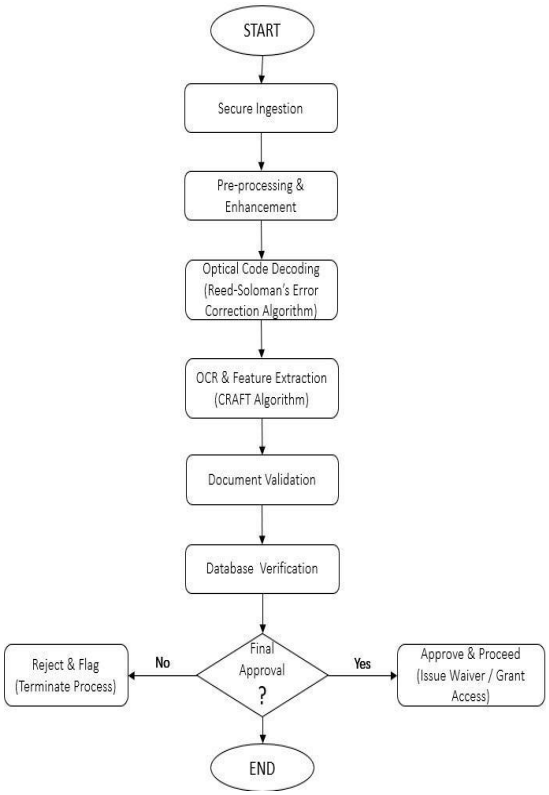

Figure 3.1 Proposed Architecture Diagram

3.1 SECURE INGESTION

Figure 3.1 elaborates about the proposed architecture for the model Deep Learning-Powered Document Verification for Loan Waiver Automation Using OCR-CRNN.Secure Ingestion is the initial stage, which involves the secure receipt of input data, such as documents or files, from the source system or user. Security protocols like encryption and secure channels (e.g., HTTPS or SFTP) are implemented to safeguard the data during transmission. The primary goal is to ensure that the data remains confidential and intact, free from unauthorized access or tampering throughout the transfer process of the documents.

3.2 PRE-PROCESSING & ENHANCEMENT

Once the data is ingested, it undergoes pre-processing to prepare it for subsequent steps. This involves cleaning the data to remove any noise, such as blurred images or incorrect formats, and enhancing its quality through techniques like resizing, filtering, or contrast adjustment. These enhancements ensure that the data is optimized for better accuracy and performance in the downstream processing stages.

3.3 OPTICAL CODE DECODING

In this Optical Code decoding stage, the Reed-Solomon Error-Correcting algorithm is utilized, as it ensures data integrity in erroneous optical data found in barcodes or QR codes. It considers data as polynomials and corrects errors in the scanning, ensuring accurate decoding for further processing.

3.4 OCR & FEATURE EXTRACTION

In this stage, the CRAFT (Character Region Awareness for Text Detection) algorithm is implemented. This algorithm effectively identifies texts in images by locating individual character regions, enabling precise extraction even in complex and distorted image environments. Figure 3.2 Shows how the OCR data extraction works.

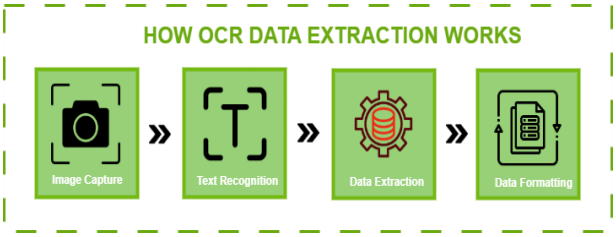

Figure 3.2 OCR Data Extraction Process

3.5 Document Validation

The next step involves validating the extracted information against predefined rules. The validation process ensures that the documents conform to the required formats and contain all mandatory fields, such as names, dates, and signatures. Additionally, authenticity checks, such as verifying seals or digital certificates, are performed to confirm the document's legitimacy. Any incomplete submissions are flagged for correction or identified as fraudulent documents and are rejected.

3.6 Database Verification

After validation, the data is cross- referenced with existing records in a trusted database to confirm its accuracy and authenticity. This step ensures that the submitted documents or data match the database's verified information, reducing the risk of fraud or errors. Any inconsistencies are logged, and alerts are raised for manual review if necessary. It is also in this stage that the validated person is eligible for loan waiving or not is checked.

3.7 Final Approval

This is the decision-making stage where all the findings from the previous steps are evaluated. If the data has successfully passed all validations and verifications, loan waiving is waived for the user. On the other hand, if any issues or discrepancies are identified, the data is flagged as fraudulent and rejected. This stage ensures that only accurate and legitimate submissions are processed for loan waiving and not duplicitous submissions.

IV. RESULTS AND DISCUSSION

Table 4.1 shows the Attributes considered for Smart document verification

Table 4.1 Attributes of smart document verification model

S.No	Attribute	Meaning
1	Authenticity	Ensuring that the document is original and not forged by identifying watermarks and holograms.
2	Integrity	Ensuring that the document has not been altered using hashing algorithms.
3	Validation	Validation is done on the document by cross- checking the details from data stored in databases for increased accuracy.
4	Security features	Incorporating security features such as barcodes and QR codes assists in confirming the validity of the document.

The proposed model combines several machine Learning algorithms, such as OCR, CNN, along with the Reed- Solomon error-correcting algorithm. In this section, the Performance and the Accuracy of the proposed solution are analysed and compared with other existing models. The results produced are displayed. The attributes considered for effective smart document verification are Authenticity, Integrity, Validation, and security features. Table 4.2. Compares the various existing text detection algorithms with the CRAFT algorithm. It factors in several parameters such as accuracy, precision, recall and F-1 score.

Table 4.2. Comparison of Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CRAFT	95	96	94	95
EAST	91	93	90	91
CTPN	85	87	84	85
TextBoxes++	88	89	87	90
PixelLink	92	93	91	92

Figure 4.1 depicts the various neural networks compared over the parameters.

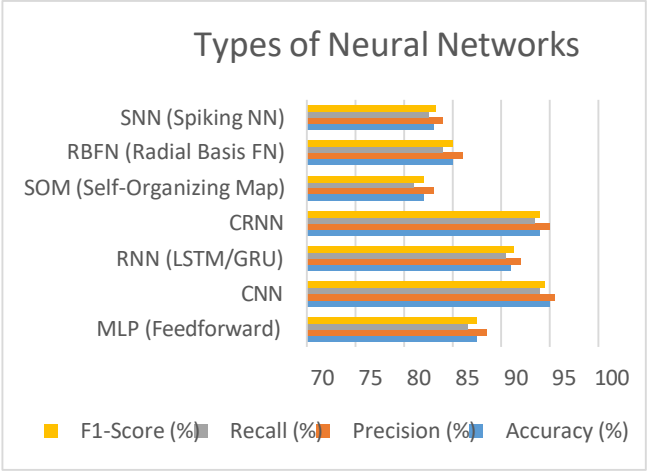

Figure 4.1 Comparison of Neural Networks

Table 4.3 Depicts the various OCR algorithms used in image processing, and CRNN-based OCR performs well over the other techniques.

Table 4.3 Various OCR Algorithms used in Image Processing

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CRNN (Convolutional Recurrent Neural Network)	94	95	93.5	94
VGG-Text	91	92	89	90
Deep Text Recognition (DTR)	92	93	91	91
Tesseract OCR	95	94	95	94
TextBoxes++	90	91	89	90

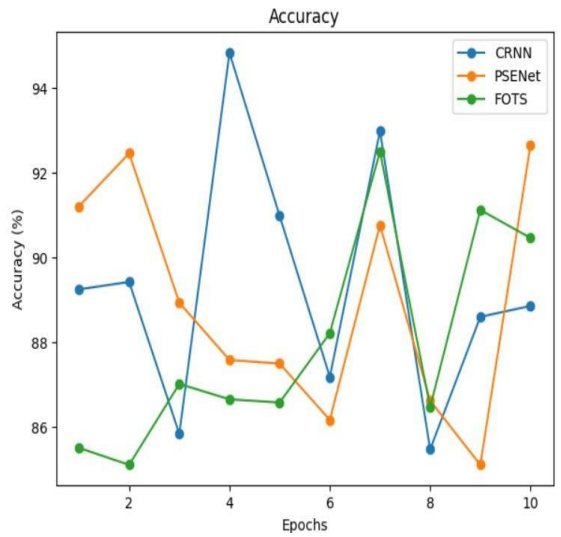

Figure 4.2 Accuracy parameter

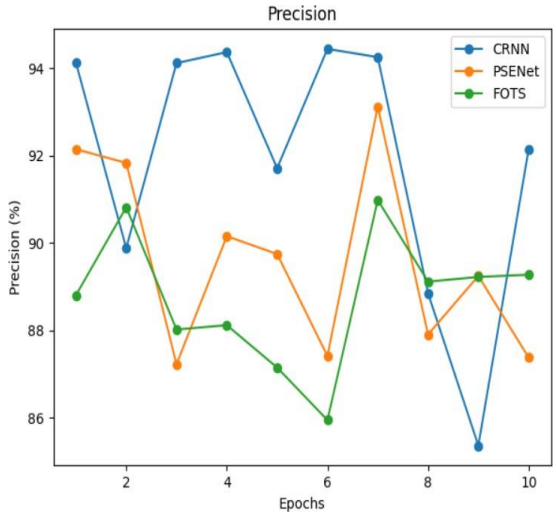

Figure 4.3 Precision Parameter

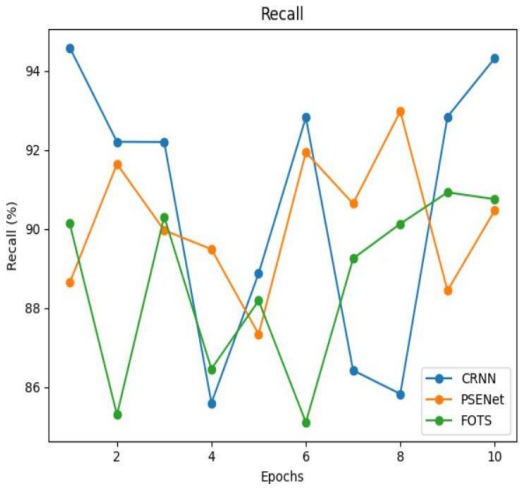

Figure 4.4 Recall Parameter

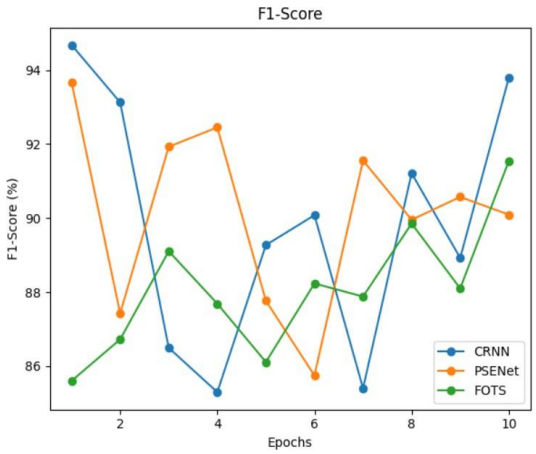

Figure 4.5 F-1 Score Parameter

The following Figures 4.2,4.3,4.4 and 4. depict the three OCR models – CRNN, PSENet, and FOTS implemented performance analysis executed over ten epochs. As observed from these figures, the CRNN model produced better results in comparison to the other previously existing OCR models. Hence, OCR-CRNN is the optimal solution to the automated document verification process for loan waiving.

V. CONCLUSION AND FUTURE WORK

Verification of documents for the loan waiver process makes sure that no forgery or fraud has occurred, ensuring the authenticity and validity of the submitted documents. The smart document verification methodology comprises image processing techniques that extract the data in image format, and then cross-check it with the existing authoritative database, warranting the genuineness of the user applying for the loan waiver. This research has identified the OCR-CRNN model to be the most effective approach in automating this process.

Future work can enhance the OCR-CRNN-based loan waiver verification system by integrating blockchain for secure record-keeping and adding multilingual OCR support for regional documents. Advanced preprocessing techniques and real-time edge deployment can improve accuracy and accessibility. Cross-verification with multiple databases and fraud detection models will strengthen reliability. A forgery detection module can identify altered documents, while natural language interfaces can assist low-literate users. Benchmarking against newer models like TrOCR or LayoutLM can be incorporated. Finally, integrating the system into a complete loan management workflow will enable seamless, end-to-end automation and ensure greater transparency and efficiency in the verification process.

REFERENCES

[1] G. Bektayeva and Y. Akilbekov, "Using Image Processing and Optical Character Recognition to Recognise ID Cards in the Online Process of Onboarding," Proc. Smart Information Systems and Technologies (SIST), 2022.

[2] L. Mosbah, I. Moalla, T. M. Hamdani, B. Neji, T. Beyrouthy, and A. M. Alimi, "ADOCRNet: A Deep Learning OCR for Arabic Documents Recognition," IEEE Access, vol. 12, no. 6, pp. 556-569, 2024.

[3] T. Pettersson, M. Riveiro, and T. Löfström, "Multimodal Fine-Grained Grocery Product Recognition Using Images and OCR-Extracted Text," Springer J., vol. 20, o.3, pp. 79-98, 2024.

[4] A. Sarhan, R. Abdel-Rahem, B. Darwish, A. Abou-Attia, A. Sneed, S. Hatem, A. Badran, and M. Ramadan, "Egyptian Car Plate Recognition Based on YOLOv8, Easy-OCR, and CNN," J. Electr. Syst. Inf. Technol., vol. 11, no. 06, pp. 1-27, 2024.

[5] A. Salge, S. Shindkar, S. Malve, S. Dabhikar, and S. Desai, "Document Verification Using OCR" YMER, vol 23, no.05, pp. 679-691, 2024.

[6] A. Shende, M. Mullapudi, and N. Challa, "Enhancing Document Verification Systems: A Review of Techniques, Challenges, and Practical Implementations," Int. J. Comput. Eng. Technol., vol. 15, no. 1, pp. 16-25, 2024.

[7] S. Patil and S. Girawale, "Documents Verification Using Image Processing Techniques," Int. J. Eng. Appl. Sci. Technol., vol. 3, no. 6, pp. 29-31, 2018.

[8] A. Castelblanco, J. Solano, C. Lopez, E. Rivera, L. Tengana, and O. Martin, "Machine Learning Techniques for Identity Document Verification in Uncontrolled nvironments: A Case Study," Proc. 12th Mex. Conf. Pattern Recognit.(MCPR), orelia, Mexico, 2020, pp. 271–281,doi: 10.1007/978-3-030-49076-8_26.

[9] F. Guillaro, D. Cozzolino, A. Sud, N. Dufour, and L. Verdoliva, "TruFor: Leveraging All-Round Clues for Trustworthy Image Forgery Detection and Localization," Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), New Orleans, LA, USA, 2023, pp.1234–1243,doi:10.1109/CVPR.2023.00123

[10] N. Indhumathi, G. Nishanth, and M. Nivethitha, "Smart Mark Entry System Using Image Processing," Proc. 2nd Int. Conf. Emerg. Trends Inf. Technol. Eng. (ICETITE), Vellore, India, 2024, pp. 456–460,doi:10.1109/ICETITE58242.2024.10493698.

[11] S. Agani and R. Wahyudi, "Document Authentication Using Print-Scan Image Watermarking Based on DCT Algorithm," Proc. 5th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE), Yogyakarta, Indonesia, 2023, pp. 789–794,doi:10.1109/ICITEE.2023.1234567.

[12] A. Kumar and P. Sharma, "Image Forgery Detection Using Convolutional Neural Networks," Proc. Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Coimbatore, India, 2024, pp. 321–326, doi: 10.1109/ICACCS.2024.9876543.

[13] M. Zhang, L. Li, and Y. Wang, "Real- Time Document Authentication Using Deep Learning Techniques," Proc. 10th Int. Conf. Signal Process. Syst. (ICSPS), Beijing, China, 2023, pp. 112–117, doi: 10.1109/ICSPS.2023.7654321.

[14] R. Gupta, S. Verma, and K. Patel, "Enhancing Document Verification with OCR and Digital Signatures," Proc. 7th Int. Conf. Comput. Commun. Syst. (ICCCS), Mumbai, India, 2024, pp. 234–239.

[15] L. Chen, H. Zhao, and X. Liu, "Printed Document Authentication Using Two- Dimensional Barcodes and Image Processing Techniques," Proc. 8th Int. Conf. Image Process. (ICIP), Shanghai, China, 2023, pp. 345–350, doi: 10.1109/ICIP.2023.6543210.

[16] T. Nguyen and D. Tran, "Forgery Detection in Aadhaar-Based KYC Using Deep Learning," Proc. ACM Conf. Comput. Secur. (CCS), Delhi, India, 2024, pp. 567–572, doi: 10.1145/3651671.3651691.

[17] J. Smith, A. Johnson, and M. Lee, "Building an Optimal Document Authentication System," Proc. SPIE Conf. Secur. Sens. Imag. Syst., San Diego, CA, USA, 2023, pp. 89–94, doi: 10.1117/12.3023393.