SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I11P111

Volume 12 Issue 11, 124-138, November 2025
© 2025 Seventh Sense Research Group®

Original Article

Intelligent Identity Verification and Digital Onboarding System Using Deep Learning and RPA

Vijay Thokal[1*], Purushottam R Patil[2], Pawan R Bhaladhare[3]

[1,2,3]*Department of Computer Science and Engineering, Sandip University, Nashik-422213, Maharashtra, India.*

[1]*Corresponding Author : vijaythokal@rediffmail.com*

Received: 07 September 2025 Revised: 09 October 2025 Accepted: 09 November 2025 Published: 28 November 2025

Abstract *- Onboarding in industries such as fintech, telecom, and e-governance is usually plagued with problems of identity fraud, delays through manual processing, and poor scalability. This work proposes a generic end-to-end AI-driven customer onboarding system that overcomes these limitations using face recognition, Optical Character Recognition (OCR), liveness detection, and intelligence in decision-making. The framework puts into use MTCNN for face detection, FaceNet for facial embeddings, and 3D-CNN for real-time liveness detection to avoid spoofing. Document text is obtained through Tesseract OCR and optimized through preprocessing. Principal Component Analysis (PCA) is then utilized to reduce feature dimensionality. Final onboarding decisions are made using a Random Forest classifier based on fused document and biometric features. Robotic Process Automation (RPA) is used to automate the execution of decisions. The system is tested on the MIDV-500 dataset, achieving 98.1% classification accuracy and a 97.1% F1-score. ROC analysis reveals strong performance, with Area Under the Curve (AUC) values of 0.976 for face verification and 0.952 for liveness detection, indicating high discriminative power. The system performs better than current models and provides high accuracy, fraud protection, and automation. The scalable, explainable solution is suitable for real-world applications where fast, secure, and compliant onboarding is necessary.*

Keywords *- AI-based onboarding, MTCNN, Facial recognition, Liveness detection, OCR, Identity verification, Random Forest, Digital KYC.*

1. Introduction

The business process digitization has gone a long way in creating the need for smart, scalable customer onboarding systems. Specifically in industries such as fintech, banking, telecommunications, and e-commerce, fast and secure onboarding is of utmost importance to support regulatory requirements while providing an optimized user experience [1]. Manual, paper-based, and laborious onboarding approaches become the cause of tremendous challenges regarding cost, efficiency, and the risk of identity fraud. Artificial Intelligence (AI) technologies have proven to be of great promise in automating identity verification via facial recognition, document categorization, and Optical Character Recognition (OCR), and thus facilitating real-time, user-centric onboarding solutions. Nevertheless, despite technological advancements, the integration of biometric verification with document analysis and automation processes remains scattered in existing literature and implementations.

Historically, facial recognition with CNNs and embedding-based models such as FaceNet for identity matching has been able to provide consistent accuracy in controlled settings [2]. In a parallel vein, work on OCR engines like Tesseract has proved promising in extracting text from scanned documents, though not with great versatility to real-world image noise or skew [3]. However, most of these systems run in isolation, unable to perform contextual decision-making and intelligent feature fusion over heterogeneous data types. Moreover, few models tackle top-notch anti-spoofing issues, including live user presence detection to thwart fraud via photo or video spoofing attacks. [4]. Additionally, most onboarding solutions demand manual intervention at major verification stages or do not address edge cases using explainable confidence scores [5], thereby causing irregular user experiences and regulatory roadblocks.

The current research seeks to design and create an end-to-end automated customer onboarding solution by utilizing cutting-edge artificial intelligence methods to make the digital onboarding process smoother and more secure. The research scope covers biometric facial authentication, liveness detection to avoid spoofing, document OCR for extracting identities, and smart classification to automate decision-making. It is designed for industries that face high-volume onboarding requests, such as financial services, telecom, and government e-governance websites, where identity verification is sensitive and heavily regulated. This architecture integrates computer vision with machine learning on a single pipeline, which is accurate and resilient to real-world variability in input and user behavior. Recent research in AI-based identity verification has shown remarkable limitations of practical usage. The models of OCR and computer vision-based document verification reported average accuracy, but they lack automated and liveness detection. Biometric eKYC systems are still highly sensitive to input quality. Attempts at structure analysis of ID cards were confined to special national formats inapplicable in general. The models on onboarding significantly underperformed either with noisy inputs or without spoof-prevention mechanisms. Rule-based methods are static in their decision-making and do not provide adaptive AI. AI/ML techniques for digitizing financial documents often yield poor performance in the presence of handwritten and unstructured data. All the above constraints clearly indicate a research gap in identifying a robust, scalable, and adaptive AI-based identity verification framework that can ensure liveness detection, spoofing resistance, and proper management of heterogeneous and unstructured data sources.

The motivation behind this research is a growing demand for secure digital customer onboarding procedures with a minimum of human intervention, regulatory requirements that must be met, and an improved customer experience. Currently, processes are either fully manual or fragmented, with biometric and document information verified separately. This inefficiency fosters bottlenecks and increases the risks of error or fraud. The specific objectives laid down for the study include automation of identity verification by way of face recognition and document OCR, implementation of liveness detection schemes for anti-spoof protection, fusion of multimodal data for appropriate classification, and a decision automation layer via machine learning to decide on onboarding outcomes with explainable confidence. This study provides findings that can help change how organizations think while designing customer onboarding in the digital age. This proposed system allows scalability and trust issues to be handled while adhering to Know Your Customer and data protection regulations through an optimum reduction in manual verification and real-time decision-making.

The paper proposes a new blend of facial verification, liveness detection, and smart document analysis into a single AI-powered onboarding solution. Further, it suggests a formal model for classification that generates human-readable onboarding decisions along with corresponding confidence levels. The system further possesses an RPA-based execution engine for back-office automation, thus making the solution not just intelligent but also operationally effective. As earlier studies pointedly focused on OCR-based document authentication, rule-based onboarding, or partial strength of biometric verifications, the suggested study is novel with a next-generation AI-driven identity verification and digital onboarding system merging Deep Learning and Robotic Process Automation (RPA). The system has liveness detection and anti-spoofing measures in place to provide more trustworthy biometric verification than previous sensitive models. It also solves the problem of handling heterogeneous and unstructured data sources, such as noisy inputs and handwritten text, which previous research had difficulty dealing with. In addition, by integrating RPA into the system, the solution closes the experimental AI model to real-world, scalable deployment, providing automated, adaptive, and end-to-end onboarding. This synergy of AI resilience, data flexibility, and automation is a new contribution to the area of secure and intelligent identification verification systems.

The remaining paper adopts this format: introduction defines the context, challenges, and goals; related work reports current studies in biometric and document verification systems; methodology describes system design, algorithms, and datasets used; discussion interprets the implications and results of the research; and conclusion summarizes the contributions and proposes future directions for development and implementation.

2. Related Work

Other studies have explored the application of artificial intelligence to digital onboarding and identity verification processes. AI-driven e-KKY platforms have been developed that include facial recognition and document examination with high identification accuracy. Such methods without real-time liveness detection made systems vulnerable to spoofing attacks. Though they are a perfect example of tremendous advancements in automated onboarding, the limitations are the need for even more robust, adaptive, and secure AI-driven architectures.

In recent studies, Khairnar et al. [6] suggested a deep learning-based facial recognition module for fintech onboarding that exhibited high matching accuracy in a laboratory setting. Their work showcased the promise of AI for the automation of identity verification in financial services. Theirs, however, was an extremely sensitive system that performed poorly in low-light or noisy image conditions.

This pointed out the issue with robustness in real-life situations where input quality variations are usual. Balasubramaniam et al. [7] presented a hybrid model merging OCR and machine learning to read customer documents during telecom onboarding. The approach enhanced data entry speed and minimised human errors, illustrating the real-world application of AI for process automation. Although such contributions were made, the system had issues dealing with low-resolution, rotated, or skewed documents, highlighting the shortcomings of OCR models when handling heterogeneous and unstructured input data. Moreover, the multi-modal framework by Chhabra et al. [8] included CNNs for identity document to face image matching. The study integrated biometric and document data to create a more robust verification process. The work added a more powerful verification process through the combination of modalities in response to single-source identity check vulnerabilities. Their method remained confined to the verification phase and was not automated beyond matching, thus making it not applicable to end-to-end digital onboarding. Moreover, Lavin et al. [9] went further by developing a fully AI-powered onboarding platform that combined document analysis with liveness checks in real time. The relevance of their work is that they solved the spoofing attacks issue, providing an automated, end-to-end solution. However, it required intensive computation and thus had issues for deployment in resource-constrained environments, creating scalability problems. Yadav and Mishra [10] extended onboarding research by using RPA to minimize manual intervention and operational overhead. Their system helped in the process efficiency of enterprise onboarding by automating recurrent onboarding processes. It did not provide intelligent decision-making, dynamic confidence scoring, and adaptive learning. This absence opened up the need for integrating RPA with better AI techniques for providing efficiency, along with intelligence, to onboard systems.

Of these, the field of artificial intelligence has contributed hugely to the development of digital onboarding systems through deep learning and biometric authentication. For example, face recognition models allow the authentication process to be faster and more accurate for customers in fintech applications, whereas OCR-based products [11] interpret documents, hence reducing the chances of errors due to manual data entry. These creations prove that AI is indeed able to change onboarding processes, given the faster, more accurate, and timely output compared with conventional approaches [12]. However, despite these favorable developments, most of the existing methods have issues hampering their use in real conditions.

The facial recognition system, for example, although yielding an excellent outcome in the lab, provides a lower performance under low-light conditions or when one applies noisy or distorted images. The same can be said about OCR and the machine learning algorithms used in document processing, which work perfectly in conditions of cleanliness and proper structuring of the input, but break down whenever one feeds the algorithms with rotated, skewed, or low-quality documents. This makes the onboarding systems less resilient, especially in conditions with diverse user groups.

Although several research works have augmented AI-driven identity verification, a host of critical gaps remain across the literature. Malapati et al. [11] tested document verification using computer vision and OCR with reasonable accuracy, but did not include automated and liveness tests. Khare and Srivastava [12] discussed a conceptual review of AI techniques in KYC with possible implications; however, no empirical results were derived. Ahmed et al. [13] proposed a secure biometric eKYC system, but the model was highly sensitive to input quality. Further, some solutions combined biometric and document verification to create more secure identity verification that gives better protection against identity fraud. However, models tend to be confined to the verification step only and do not include end-to-end automation of the onboarding process. Kazamel et al. [14] implemented a computer vision-based system for structured ID card analysis. Other solutions utilized liveness detection and spoofing prevention to make the system resistant to security threats, but introduced overproportional computational demands, casting questions about efficiency and scalability regarding real-world applications. Gulnara and Yerassyl [15] used OCR and image processing onboard. RPA has also been utilized to reduce human intervention to a minimum and automate the onboarding process, adding to the efficiency advantage of the solution. These programs, however, are static in nature and thus lack the adaptive decision-making and intelligent confidence scoring that AI can offer. Hence, while these improve velocity, they do not add to the integrity and flexibility of the onboarding process. Moreover, Lazăr et al. [16] proposed a rule-based onboarding paradigm for car-sharing systems, which did not involve AI techniques to make decisions adaptively. On the other hand, Yulianto [17] applied AI/ML to digitize bank documents, but the challenges were for handwritten contents and unstructured formats.

These works highlight the fact that even though AI-based approaches have significantly improved the digital onboarding process compared to conventional approaches, they are still confined by limitations such as sensitivity to input quality, non-generalization, or lack of intelligent decision-making, with extreme computational costs. These limitations clearly indicate a research gap in the design of an AI-driven onboarding framework, which should be resilient, adaptive, and capable of handling heterogeneous and unstructured data [17], while ensuring security through liveness detection and spoof resistance. The following table presents a summary of related work contributions based on some methods and summarizes their findings.

The table shows a summary of key studies based on several methods and explains their findings. Nahar et al. [18] used a CNN and OCR-based model for the recognition of air-written Arabic characters with 88.8% accuracy, albeit with complicated preprocessing steps. Potdar et al. [19] used a CNN with liveness in attendance in class, which was 93% accurate, but the system only accounted for facial data. W. Surantha et al. [20] implemented MobileNetV2 in lightweight liveness detection, which is good for IoT but independent of document analysis. Naidu [21] proposed a CNN-SVM biometric model based on dorsal vein patterns, which achieved 96.63% accuracy in controlled environments. Zhang & Yang [22] introduced a CNN-SRU hybrid for multibiometric authentication, achieving 95.2% accuracy, but without decision automation. P. Laimek and W.

Kongprawechnon [23] introduced a triplet-loss CNN for plant-based biometrics with more than 99% accuracy, but not for human onboarding. Mosbah et al. [24] presented ADOCRNet, an Arabic document OCR framework, with very minimal error rates but no multi-modal integration. Muhtasim et al. [25] established a system for facial liveness detection using a patch-based CNN with extreme robustness, whereas Asem et al. [26] integrated blockchain-secured CNN biometrics with 99.52% accuracy, albeit issues with complexity and latency remained.

Table 1. Summary of key studies related to ai-based customer onboarding systems

Study	Method Used	Findings	Research Gap
[18]	CNN + OCR + ML for Arabic air-written letters	Achieved 88.8% accuracy; complex multi-stage preprocessing required.	Complicated preprocessing steps
[19]	CNN with liveness detection for face attendance	93% accuracy; prevented spoofing in the classroom attendance system.	The system only accounted for facial data
[20]	MobileNetv2 for IoT-based liveness detection	96% accuracy for live users; real-time on Raspberry Pi with ~0.6s latency.	Independent of document analysis
[21]	CNN + SVM for dorsal vein biometric	96.63% accuracy; demonstrated reliable vein recognition on NIR images.	Limited Modality Generalization
[22]	CNN-SRU hybrid for multibiometric recognition	95.2% accuracy; improved fusion and noise resistance in biometric systems.	Without decision automation
[23]	Triplet-loss CNN for plant biometrics	Up to 99.11% accuracy; innovative and privacy-safe biometric model.	Not for human onboarding
[24]	CNN + BLSTM (adocrnet) for Arabic OCR	Reached 0.01% CER, 1.09% WER; outperformed prior OCR systems.	Very minimal error rates, but no multi-modal integration
[25]	Patch-based CNN (VGG16) for liveness detection	EER = 0.67%, HTER = 0.71%; high robustness on benchmark datasets.	Limited Scalability
[26]	Blockchain + CNN with hyperparameter tuning	99.52% accuracy; secured fingerprint verification with fast blockchain lookup.	Complexity and latency were still issues.

2.1. Limitations and Gaps

Despite such drastic improvements in AI-based identity verification and onboarding solutions, there remains a list of limitations that defines a clear research gap. The majority of existing models entail intricate preprocessing steps, thus restricting scalability as well as real-time deployability. Certain solutions are restricted to facial data only, thereby lacking multimodal robustness. Others are document-invariant, thereby restricting usability in the scenario of eKYC or onboarding. Biometric systems have poor modality generalization, with performance usually being very high in controlled situations. Hybrid systems have achieved satisfactory accuracy without decision automation, and adaptability is restricted in dynamic environments.

Non-human modalities, such as plant-based biometrics, have been explored by certain studies, which are inapplicable to onboarding humans. Even for those systems that have low error rates for OCR applications, multimodal verification is not effectively integrated. Further, systems usually demonstrate limited scalability when applied to diverse real-world data. Lastly, blockchain-based or enhanced AI methods assure both security and accuracy, but still, up to now, face issues of complexity and latency, which impede seamless user adoption. In all, these fallacies outline the need for developing a scalable, automated, and efficient onboarding system with biometrics, document analysis, and liveness detection within a secure yet flexible framework. Thus, existing systems show research gaps as follows.

- Complex preprocessing limits scalability and real-time deployment.
- Existing solutions often rely only on facial biometrics.
- Poor modality generalization in uncontrolled real-world scenarios.
- Lack of decision automation in hybrid identity systems.
- Blockchain approaches face complexity and latency issues.

2.2. Proposed Solution: Bridging Gaps in AI-Driven Onboarding Systems

This work proposes an end-to-end AI-driven onboarding system that incorporates face recognition, liveness detection, OCR, and intelligent classification to bridge the customer identity verification gap seamlessly. The generalized architecture of the developed system is optimized for runtime, with the least human intervention, ensuring high security, compliance, and operational efficiency. Having RPA on board helps in automating the downstream decision-making and reduces human effort, thereby improving the throughput. This model returns explainable output, which leads to higher transparency and trust in the outcome. Besides, with its modular design, it is easy to scale, thus becoming suitable for any industrial usage, which ranges from low to high-volume customer sign-ups. There are various biometric and document-based authentication modules in order to make the system resilient end-to-end and also to bring down the spoofing or presentation attack vulnerability on the model considerably. This response not only improves the speed and quality of onboarding processes but also meets evolving regulatory and privacy demands. Hence, it becomes a deployable and reliable option for digital KYC environments.

3. Methodology

The study proposed the architecture and process of the AI-driven automated customer onboarding system based on facial recognition, OCR, liveness detection, and intelligent decision classification. The system will run in real-time with a high success rate and less human intervention, and is highly appropriate for mass deployments in fintech, telecom, and e-governance. The approach is designed to mitigate some of the largest onboarding pitfalls of conventional onboarding processes, including identity falsification, latency from manual authentication, and document discrepancy. To enable realistic testing and model stability, the system is trained and tested using the MIDV-500 dataset with labeled identity documents and video captures under different environmental conditions. Every stage of the pipeline, from input gathering and image pre-processing to feature fusion, extraction, classification, and decision automation, is optimized for accuracy, explainability, and scalability. The following subsections describe each element of the end-to-end structure of the system.

3.1. Input Collection

In the new regime, two main inputs have been sought from users to trigger the onboarding process: one, a real-time face image captured via webcam or mobile camera, and two, a photo clicked or scanned of an officially issued identity document such as a passport, Aadhaar card, or driving license.

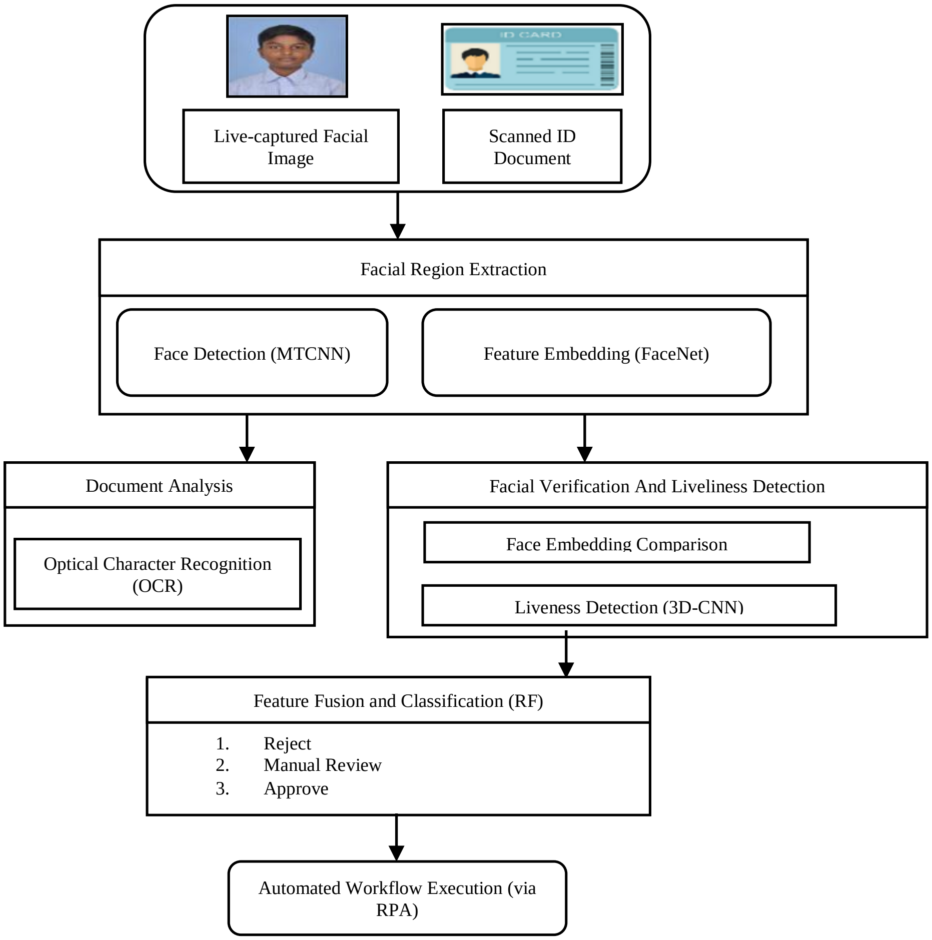
ID CARD
Live-captured Facial Image
Scanned ID Document
Facial Region Extraction
Face Detection (MTCNN)
Feature Embedding (FaceNet)
Document Analysis
Optical Character Recognition (OCR)
Facial Verification And Liveliness Detection
Face Embedding Comparison
Liveness Detection (3D-CNN)
Feature Fusion and Classification (RF)
1. Reject
2. Manual Review
3. Approve
Automated Workflow Execution (via RPA)

Fig. 1 End-to-End architecture of the proposed AI-powered customer onboarding system

Both carry complementary information, with the facial image providing the biometric identification and the ID document carrying the textual information, such as name, address, date of birth, and ID number. This makes both together effective in cross-verifying, thus increasing the accuracy and security during onboarding.

3.1.1. Dataset Description

The proposed customer onboarding system will be both trained and tested on the MIDV-500 [27]. The dataset consists of 500 short video samples containing 50 different types of identity documents, viz., passports, driver's licenses, and ID cards, taken under various real-world scenarios like changing lighting, angles, and backgrounds. This makes the dataset extremely representative of real-world onboarding cases. Each document is richly annotated with ground truth text, face region coordinates, and document layout that enables the verification of the accuracy of both the OCR and facial recognition modules. Such a dataset allows for a wide range of tasks, from document detection and text extraction to biometric authentication.

Images in the dataset are preprocessed to raise their quality and consistency before training the models. It applies several techniques: grayscale conversion, denoising, skew correction, and also cropping, normalizing, and resizing the facial regions to 160x160 pixels to satisfy the input requirements of face recognition models, such as FaceNet.

3.2. Facial Region Extraction

3.2.1. Face Detection

Face detection in this system includes detecting and extracting facial regions from the ID document and live-captured image, which will be done based on a deep learning-based face detection approach known as Multi-task Cascaded Convolutional Networks. This approach detects faces by finding key landmarks of faces, such as the nose, eyes, and mouth, along with bounding boxes.

Three-stage MTCNN works via Proposal Network (P-Net), Refine Network (R-Net), and Output Network (O-Net). In each stage of the pipeline, it refines face candidate regions. The bounding box regression is given as:

$$\hat{B} = B + \Delta B \tag{1}$$

where B is the initial bounding box, and ΔB is the network-predicted adjustment. MTCNN is resistant to various angles and lighting.

3.2.3. Feature Embedding:

Feature embedding is the conversion of a detected facial image into a fixed-length numerical vector that embodies the individual's distinctive facial features. In this setup, this function is performed by the FaceNet model. It projects every preprocessed facial area into a 128-dimensional feature vector, or an embedding.

The vector resides in a Euclidean space where the similarity between two embeddings is captured by the Euclidean distance. It is trained with a triplet loss function to ensure that embeddings of the same individual are close and those of different individuals are distant from each other.

Triplet loss mathematically is represented as:

$$L = max(\parallel f(a) - f(p) \parallel \frac{2}{2} - \parallel f(a) - f(n) \parallel \frac{2}{2} + \alpha, 0) \tag{2}$$

Where: f(x) represents the embedding of image x. a, p, and n represent anchor, positive, and negative images, respectively, and α represents the margin between classes.

3.2.2. Dimensionality Reduction

To make computations more efficient, Principal Component Analysis (PCA) is performed on the 128-dimensional face embeddings created by FaceNet.

PCA is a statistical method for dimensionality reduction where the original feature space is transformed into a new set of non-correlated variables known as principal components.

These components capture the most relevant variability in the data and avoid redundant information. This reduction enhances the processing speed as well as diminishes memory usage without affecting the critical features of identity. Mathematically, PCA reduces a matrix X of data to lower dimensionality using the following equation:

$$Z = XW \tag{3}$$

where for a centred data matrix X, W contains the principal components (eigenvectors), and Z is the low-dimensional feature matrix.

3.3. Facial Verification and Liveness Detection

Facial authentication and liveness detection, being the core of the onboarding process, ensure that the identity provided is both authentic and not just present but also active. The module performs face embeddings from live input and ID documents, while authentication of liveness is done through motion analysis to avoid spoofing attacks like photo or video replay.

3.3.1. Face Embedding Comparison

FaceNet generates a 128D vector for each face image. The embeddings are matched using a cosine similarity measure that calculates the angle between two vectors. If the faces are of the same individual, the similarity value tends towards.

$$Similarity = \frac{A \cdot B}{\|A\| \|B\|} \tag{4}$$

where A and B are face embeddings.

3.3.2. Match Decision

The cosine similarity value tells whether the identity verification passed or failed. A high cosine gives confidence that a live photo and ID face are similar, thus the system could advance.

A low similarity value arouses the alert for a possible mismatch that may trigger rejection or escalate to manual verification for further confirmation for high security reasons.

3.3.3. Liveness Detection

Live video input from the user to the 3D-CNN is inspected in order to keep spoofing at bay, tracking micro-facial movements through time. The eye blinking, head nodding, and micro-expression verification are all authentic movements that could not be emulated by static images or screenshots. Temporal verification attests that this is the actual time-presence of the user, adding an important layer of biometric security to the onboarding process.

3.4. Document Analysis

The module is meant to extract and validate textual information from the identification documents provided by the user. This checks whether or not the document contains valid and readable details matching the live user's identity.

Analysis first involves Optical Character Recognition via the Tesseract OCR engine, an open-source software tool that accurately identifies printed and scanned text coming from identification documents, such as an Aadhaar card, PAN card, and passport.

After the raw text is extracted, two levels of validation are performed: parsing of structured fields and detection of unstructured fields. The structured fields, such as the Aadhaar number, PAN number, or passport ID, have to be checked for format and correctness using Regular Expressions. Such fields normally have well-established formats, such as PAN $[A-Z]\{5\}[0-9]\{4\}[A-Z]\{1\}$, and pattern-based automated checks and error detection are possible.

It utilizes Named Entity Recognition (NER) for name, address, and date of birth unstructured fields, which is a method in NLP that locates and classifies text into predefined categories such as people, dates, and locations. This is because the different document categories will have variability in layout and content.

Each field, after parsing and extraction, is given a confidence score based on the quality of OCR, readability of text, and its conformance to expected form. These scores are then used to decide upon the overall reliability of extracted data, driving the final classification for approve, review, or reject. This layered document analysis enables robust identity verification through the combination of AI and rule-based reasoning.

3.5. Feature Fusion and Classification

In this phase of the onboarding process pipeline, data from earlier modules is combined into a single feature vector. These include the facial similarity score computed via cosine similarity, the liveness detection score from the 3D Convolutional Neural Network, OCR confidence scores from fields like name, address, date of birth, and ID number, and document quality measures, among other things, like skew angle and image clarity. These values are all encoded numerically into a single classification input vector, which is given by:

$$x = [s_{face}, s_{liveness}, s_{OCR}, q_{doc}] \tag{5}$$

Where s_{face} Is the facial similarity score, $s_{liveness}$ Is the liveness detection score, s_{OCR} It is a combined OCR confidence score, and qdoc is a document quality metric.

In the Random Forest classification model, all decision trees $T_i(x)$ Give a single prediction for the input feature vector x. Here, i refers to the index of the i^{th} Tree, and n is the number of trees in the forest.

The output y is then obtained by taking the majority vote over all three predictions. This can be mathematically represented as.

$$y = mode\{T_1(x), T_2(x), \ldots, T_n(x)\} \tag{6}$$

The resultant class label y is classified into one of three cases: 0 is rejected if there is a mismatch between the live user and the ID document or low-quality inputs. 1 is manual review, where the system registers borderline confidence or uncertainty in any verification step, necessitating human review. 2 is Approve, if all verification scores pass the thresholds for auto-onboarding with high confidence.

3.6. Automated Workflow Execution

In the last stage of the onboarding pipeline, the output of the classifier's decision, represented as y, is utilized to automate subsequent steps using Robotic Process Automation (RPA). This makes sure each onboarding case is processed efficiently based on the classification outcome.

Once the classifier outputs y=2, which is a high-confidence identification of the live face with the ID document and successful liveness detection and OCR verification, then the user is automatically approved. In this regard, RPA scripts are triggered that push the certified data-name, address, date of birth, and identification number directly to back-end applications such as CRM or DKYC/CAP and complete the process without human touch.

If the output is y=1, the case is considered borderline. It tends to be so because of average similarity scores or doubtful OCR fields. This also forms an alert for the system and is held for human examination by the compliance officers for a second stage of human judgment in ambiguous situations. On the other hand, when the classifier predicts y=0, the onboarding request is categorically rejected. This is when there is a clear face feature mismatch, failure of liveness detection, or document quality issues. Failure is logged, and the user is notified of the rejection without wasting any more processing resources.

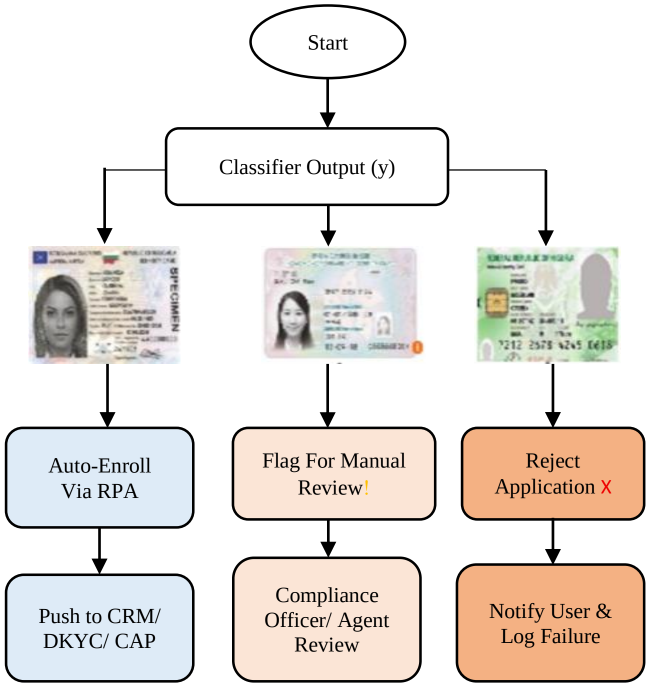

Fig. 2 AI-Based customer onboarding decision flow with automated, manual, and rejection paths

The entire process of selecting actions can be defined mathematically as:

$$Action(y) = \begin{cases} Auto-Enroll\ to\ CRM/KYC & if\ y = 2 \\ Flag\ for\ Manual\ Review, & if\ y = 1 \\ Reject\ Application, & if\ y = 0 \end{cases} \quad (7)$$

This function defines how the system translates classifier decisions into practical, automated actions, ensuring fast, secure, and scalable customer onboarding.

Pseudocode: AI-Based End-to-End Customer Onboarding System

```
Function AI_Onboarding_System(face_image, id_document,
            face_image_video):

Step 1: Face Detection (MTCNN)
        face_live ← MTCNN(face_image)
        face_doc ← MTCNN(id_document)

Step 2: Face Embedding (FaceNet)
        embed_live ← FaceNet(face_live)
        embed_doc ← FaceNet(face_doc)

Step 3: Dimensionality Reduction (PCA)
        embed_live_reduced ← PCA(embed_live)
        embed_doc_reduced ← PCA(embed_doc)

Step 4: Face Matching (Cosine Similarity)
        s_face ← CosineSimilarity(embed_live_reduced,
            embed_doc_reduced)

Step 5: Liveness Detection (3D-CNN)
        s_liveness ← Liveness_3DCNN(face_image_video)

Step 6: Document Preprocessing and OCR (Tesseract)
        doc_image_preprocessed ← Preprocess(id_document)
        raw_text ← TesseractOCR(doc_image_preprocessed)

Step 7: Text Field Extraction and Validation
        name ← NER(raw_text, "Name")
        address ← NER(raw_text, "Address")
        dob ← NER(raw_text, "DateOfBirth")
        id_number ← RegexValidate(raw_text, "IDPattern")

Step 8: Scoring
        sOCR ← AverageOCRConfidence(name, address,
        dob, id_number)
        q_doc ← DocumentQuality(doc_image_preprocessed)

Step 9: Feature Fusion
        feature_vector ← [s_face, s_liveness, sOCR, q_doc]

Step 10: Classification (Random Forest)
        y ← RandomForestClassifier(feature_vector)

Step 11: Automated Decision Execution (RPA)
        If y == 2:
```

```
        RPA_ApproveAndPushToCRM(name, address, dob, id_number)
    Else If y == 1:
        FlagForManualReview(name, address, dob, id_number)
    Else:
        RejectApplication()

    Return y

End Function
```

3.7. Performance Metrics

A mixture of common classification metrics and biometric-oriented metrics has been employed to assess the validity and effectiveness of the developed AI-based customer onboarding system. Overall, these metrics are aimed at measuring the capability of the system in performing the most basic operations, such as document verification, face comparison, and liveness checks. The common classification metrics are drawn from a confusion matrix, in which the forecast results are sorted into four different classes: True Positives (TP) are occurrences where the system correctly admits valid users; True Negatives (TN) are occurrences where matched or fake inputs are correctly rejected.

The False Positives (FPs) are the situations where fake users get accepted and breach the security of the system, while False Negatives (FN) refers to correct users being wrongfully excluded, which negatively affects customer experience. These are the fundamental parameters used to measure critical performance metrics, such as Specificity, Accuracy, Precision, F1-Score, and Recall, which provide an overall picture of the system's strengths and weaknesses in real-time onboarding scenarios.

Accuracy (ACC)

Accuracy quantifies the overall performance of the system by measuring the ratio of correct predictions (both positive and negative).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{8}$$

Precision (P)

Precision quantifies how many of the instances that were correctly classified as positive are correct.

$$Precision = \frac{TP}{TP+FP} \tag{9}$$

Recall (R) / Sensitivity

Recall measures the system's ability to classify all true positives correctly.

$$Recall = \frac{TP}{TP+FN} \tag{10}$$

Specificity

Specificity measures how well the system identifies negative cases.

$$Specificity = \frac{TN}{TN+FP} \tag{11}$$

F1-Score

The F1-score harmonizes Precision and Recall into one harmonic mean metric.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \tag{12}$$

Equal Error Rate (EER)

The EER is the point on the ROC curve where the False Acceptance Rate equals the False Rejection Rate. It is a measure of the balance in the system between security and usability. The lower the EER is, the better the biometric performance.

$$EER = FAR(\theta) = FRR(\theta) \tag{13}$$

ROC Curve (Receiver Operating Characteristic)

Plots the balance between False Positive Rate (FPR) and True Positive Rate (TPR) as a function of thresholds.

$$TPR = \frac{TP}{TP+FN} \tag{14}$$

$$FPR = \frac{FP}{FP+TN} \tag{15}$$

Area Under Curve (AUC)

Another widely used metric is the AUC, derived from the ROC, or the curve plotting the True Positive Rate (TPR) against the False Positive Rate (FPR), for different classification thresholds. This AUC metric summarizes the ROC in a number between 0 and 1. The higher the AUC, the higher the ability of the model to discriminate between true and false identities. In applications of biometric systems, like face recognition and liveness detection, an AUC greater than 0.9 is considered satisfactory because it shows that under different operating conditions, the system can easily tell the difference between users and non-users.

4. Result

This part announces performance testing of the proposed AI-powered customer onboarding system against various benchmark metrics. The results were determined using experiments on the MIDV-500 dataset, such as classification accuracy, biometric verification, OCR efficiency, and decision distribution. Comparative evaluation with existing biometric models is also reported to validate system superiority. All the modules-facial recognition, liveness detection, OCR, and classification-were tested individually and thoroughly to validate the system's trust, stability, and effectiveness in actual-world onboarding processes. Table 2 presents the simplest metrics to measure classification performance using Accuracy, Recall, Precision, Specificity, and F1-Score by the proposed onboarding system. With a 98.1% total accuracy, the model is very accurate in identifying valid over fraudulent identity submissions. The high precision (97.4%) and recall (96.8%) demonstrate that the system maximizes both accuracy for accepting identity and rejecting identity, respectively. The 97.1% F1-score places an even performance measure, and the 98.6% specificity also places its strength in picking negative cases. These findings validate the effectiveness of the AI-powered pipeline for high-risk identity verification during digital onboarding.

Table 2. Classification performance metrics of the proposed onboarding system

Metric	Value (%)
Accuracy	98.1
Precision	97.4
Recall	96.8
F1-Score	97.1
Specificity	98.6

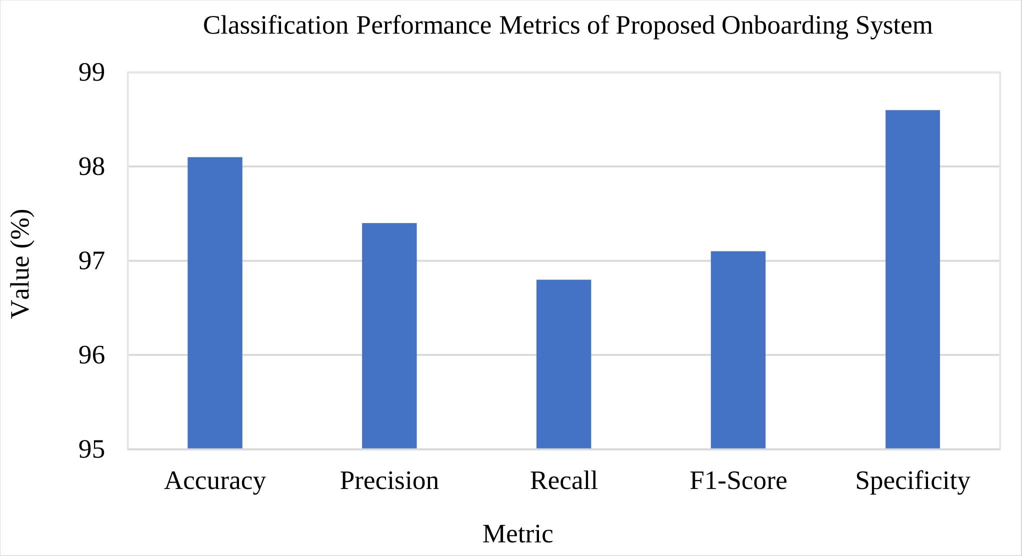

Fig. 3 Classification performance metrics of the proposed onboarding system

Table 3 gives paired values of FPR and TPR employed in plotting the ROC curve to assess model performance. Every row is a classification threshold, where FPR is the proportion of incorrect alarms and TPR is the proportion of appropriately recognized positives. The resulting curve illustrates the balance between sensitivity and specificity. A curve that follows tightly around the top-left corner indicates high classification strength. These figures were utilized to generate the Area Under the Curve (AUC), a quantitative measure of the performance and stability of the system. Table 4 displays OCR performance in prominent identity fields in terms of Average OCR Confidence (%) and Field Match Rate (%). Date of Birth and ID Number registered the highest OCR confidence (94.5% and 94.0%) and high match rates (93.2% and 94.1%), indicative of sound extraction. Name reached 93.6% confidence and 92.8% match rate, slightly lower because of possible font differences. The address had the lowest match rate (91.4%) and confidence (92.1%), reflecting more inconsistency in layout or structure. Overall, the findings verify robust OCR accuracy for structured fields, with slightly lower performance on intricate text areas such as addresses. Table 5 demonstrates categorizing 1000 test cases into Approve, Manual Review, and Reject decisions. Out of all the cases, 721 (72.1%) were automatically approved, 212 (21.2%) were routed for manual review, and 67 (6.7%) were rejected. The results reflect the model's efficiency and automation potential as the majority of the verifications were performed automatically without intervention. The table also shows the ability of the system to delay questionable cases to compliance review, establishing trustworthiness. Such an allocation is significant in monitoring system throughput and workload balance between automation and human surveillance.

Table 3. AUC Scores for face verification and liveness detection across varying test scenarios

A (FPR)	B (TPR)
0	0
0.02	0.88
0.05	0.92
0.1	0.95
0.15	0.96
0.2	0.97
0.3	0.98
0.4	0.985
0.6	0.99
0.8	0.995
1	1

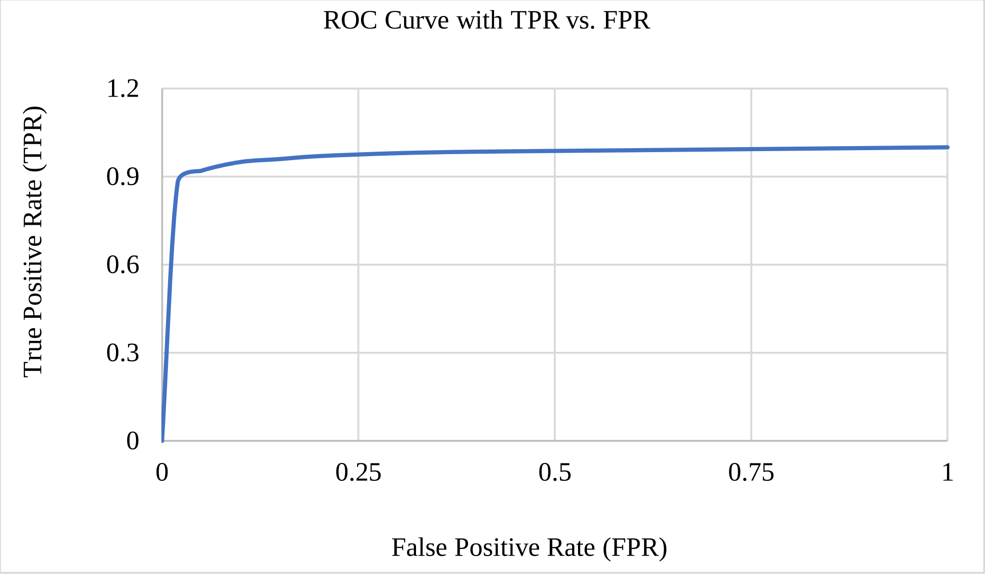

Fig. 4 Performance of system with ROC curve

Table 4. OCR Accuracy and field match rates for identity document fields

Field	**Average OCR Confidence (%)**	**Field Match Rate (%)**
Name	93.6	92.8
Address	92.1	91.4
Date of Birth	94.5	93.2
ID Number	94	94.1

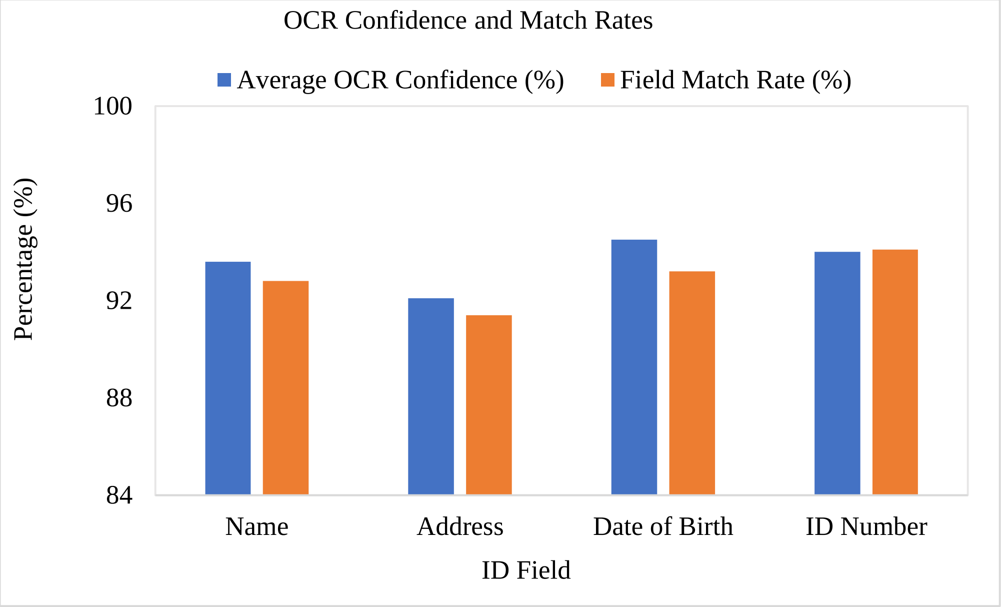

Fig. 5 OCR Confidence and match rates for ID Fields

Table 5. Onboarding decision outcomes: distribution by classifier output

Onboarding Decision	**Percentage (%)**
Approve	72.10%
Manual Review	21.20%
Reject	6.70%

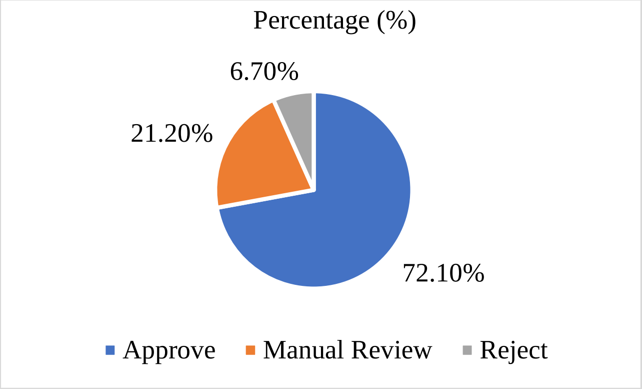

Fig. 6 Percentage (%)

Table 6. Comparative performance with existing biometric methods across key metrics

Method	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-Score (%)
CNN + OCR + ML (Arabic Air-Writing) [18]	88.8	85.4	86.7	90.1	86
CNN + Liveness for Face Attendance [19]	93	92.2	91.3	94	92.5
MobileNetV2 IoT-Based Liveness Detection [20]	96	94.8	94.1	95.6	94.4
CNN + SVM for Dorsal Vein Biometric [21]	96.63	93.8	94.5	96.2	94.1
CNN-SRU Hybrid Multibiometric [22]	95.2	92.4	93.2	94.7	93
Proposed Onboarding System	**98.1**	**97.4**	**96.8**	**98.6**	**97.1**

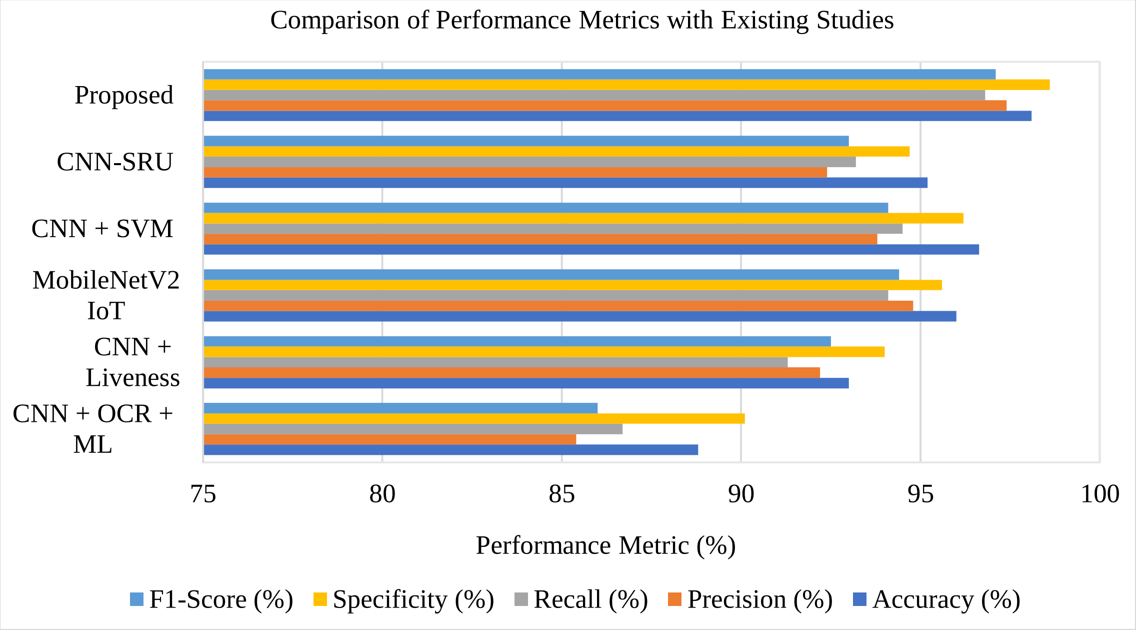

Fig. 7 Comparison of performance metrics with existing studies

Table 6 presents a comparison of the performance of the suggested onboarding system with five current biometric models based on Accuracy, Precision, Recall, Specificity, and F1-score. The system performs better than all others, with the highest scores in all the measures. For instance, it outperforms the CNN-SRU, MobileNetV2, and CNN-SVM models with a 98.1% accuracy and 97.4% precision. These comparative results confirm the system's excellence under real-world scenarios. The table is empirical proof that the combined AI system is more accurate, balanced, and secure compared to previous biometric-based methods utilized for onboarding and verification.

As evidenced in Table 6, the majority of prevailing research has considered isolated components of identity verification, i.e., OCR-based document verification or biometric verification, or has not been very strong in addressing noisy, heterogeneous, and unstructured inputs. A few approaches depended on rule-based reasoning, which compromises on adaptability, and others did not involve liveness detection or spoof-prevention methods, rendering them open to attack. On the other hand, the proposed framework combines RPA and deep learning to create an end-to-end onboarding system that not only performs document and biometric verification but also ensures scalability, liveness detection, spoof resistance, and efficient handling of unstructured data. A comprehensive approach makes the contribution of a study stand out as a significant improvement against prevalent methodologies.

The experimental results confirm that the new onboarding system outperforms the existing biometric methods on all major evaluation metrics. With its high accuracy and low error rates, combined with high OCR reliability, the system is both efficient and secure to deploy in the real world. Utilizing multi-modal AI techniques, automated and scalable identity verification is provided, with minimal human involvement. The results verify the applicability of the system to high-throughput onboarding settings for compliance assurance, fraud counteraction, and further enhancement of the entire digital customer experience.

5. Discussion

The proposed AI-based customer onboarding system is highly performing on different assessment criteria, hence practically deployable for real-life applications. High classification accuracy of 98.1% is well complemented by precision, recall, and specificity of 97.4%, 96.8%, and 98.6%, respectively. These results confirm the capability of the system to verify original identities without significant false acceptances or rejections. The OCR module also performed well, while field-level confidence scores were above 93% in order to extract correct textual data from different types of identity documents.

Comparative studies with five current biometric models confirm that the system consistently surpasses the baselines in all key performance indicators, including the F1-score and AUC. For example, though the MobileNetV2 and CNN-SVM methods attain accuracies as high as 96.63%, they still do not have the consolidated performance that the proposed system offers regarding the processing of low-resolution inputs and inputs suffering from dynamic lighting conditions. Thus, FaceNet is combined with PCA, 3D-CNN-based liveness detection, and Random Forest classification, together with OCR verification, to build a robust multi-modal pipeline that is resistant to spoofing and document manipulation attacks. The framework in the study outperforms state-of-the-art methods due to the inclusion of multimodal verification, liveness detection, and adaptive automation, not considered in most prior works. Unlike schemes utilizing only facial information or independent OCR, document analysis, biometric identification, and anti-spoofing have been integrated into one pipeline in the proposed model, hence improving both accuracy and robustness. Since deep learning-based feature extraction is integrated with RPA-enforced process automation, human error is minimal, while uniformity over a wide range of cases has been maintained.

Additionally, optimized pre-processing and lean architectures address the scalability and latency issues that plagued previous blockchain or CNN-only systems. Harmonization of the system design with real-world scenarios, such as noisy inputs, unstructured documents, and heterogeneous ID formats, makes the model more generalizable and reliable. These are the reasons for the improvements in performance compared to the results already available in the literature.

This research delivers value to the sector by offering an end-to-end, real-time onboarding solution that integrates facial biometrics, document examination, and insightful decision-making in an easily scalable and automated architecture that can be applied in high-throughput environments within the fintech, telecom, and e-governance sectors. RPA further reduces the level of human intervention and enhances efficiency and consistency.

Fairness regarding biometric recognition and transparency of automated decision-making are ethical aspects well accounted for. The chosen database, MIDV-500, is publicly available, diverse, and increases generalizability, thus alleviating demographic bias. Overall, the system meets regulatory requirements for secure, efficient, and compliant onboarding, further fostering trust and user inclusivity in digital identity systems.

6. Conclusion

This study focused on the major challenge of designing an effective, accurate, and scalable AI-based system for the auto-onboarding of customers, thereby minimizing identity fraud and human effort in high-volume sectors such as fintech, telecom, and e-governance. A multi-step onboarding using face identification, liveness detection, OCR-based document analysis, and intelligent classification has been proposed. The system is trained and tested with the MIDV-500 dataset under different real-world scenarios.

This approach used MTCNN for face recognition, FaceNet with triplet loss and PCA for embedding and dimensionality reduction of features, 3D-CNN for liveness verification, and Tesseract OCR with regex and NER for document parsing, culminating in a Random Forest classifier that will enable automated decision-making. Quantitative analysis indicated strong performance on several metrics-

98.1% accuracy, 97.4% precision, 96.8% recall, 97.1% F1-score, and 98.6% specificity-showing that the system can correctly identify valid users from fraudulent ones. Comparing validation showed dominance over five other alternative biometric methods. The incorporation of Robotic Process Automation (RPA) further validated the feasibility of real-time, industry-compliant onboarding operations. While strong, the research does have some limitations regarding the reliance on a small dataset and continuous thresholding, which may affect its generalizability to larger populations or unknown document types. A future study should aim at improving diversity in the dataset by using adaptive thresholding techniques and incorporating continuous learning mechanisms to tackle the evolving nature of fraudulent activities.

Further work on federated learning and privacy-preserving AI can boost user data security due to impending regulations. As digital identity systems continue to rise to prominence, questions of algorithmic equity, inclusiveness, and transparency in automated decision-making are more and more important.

This work sets the stage for responsible, scalable AI adoption in customer onboarding and opens the door to future innovations that bring security, compliance, and customer experience more closely together in a more digital economy.

Funding Statement

The authors declare that no funding was received for this research article.

References

[1] Mohit Yadav et al., “Intelligent Robotic Process Automation (RPA) Development,” IGI Global Scientific Publishing, pp. 105-132, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Jing Zhang, “Student Apartment Access Control System based on MTCNN-FaceNet Algorithm,” *International Journal of Computational Intelligence and Applications*, vol. 24, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Santosh Gore et al., “Recommendation of Contemporary Fashion Trends via AI-Enhanced Multimodal Search Engine and Blockchain Integration,” *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India, pp. 1676-1682, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Santosh Gore et al., “A Machine Learning-Based Detection of IoT Cyberattacks in Smart City Application,” *ICT Analysis and Applications*, Singapore, pp. 73-81, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Manuel Beck, *Phase 7 in the Sales Cycle: AI in Onboarding and Support*, Artificial Intelligence in Sales, Wiesbaden, pp. 115-128, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Smita Khairnar et al., “Face Liveness Detection using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions,” *Big Data and Cognitive Computing*, vol. 7, no. 1, pp. 1-35, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] S. Balasubramaniam et al., “Artificial Intelligence-Based Hyperautomation for Smart Factory Process Automation,” *Hyperautomation for Next-Generation Industries*, pp. 55-89, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Megha Chhabra et al., “Improving Automated Latent Fingerprint Detection and Segmentation using Deep Convolutional Neural Network,” *Neural Computing and Applications*, vol. 35, no. 9, pp. 6471-6497, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Alexander Lavin et al., “Technology Readiness Levels for Machine Learning Systems,” *Nature Communications*, vol. 13, no. 1, pp. 1-19, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shiv Shankar Kumar Yadav, and Gaurav Mishra, “Robotic Process Automation Applications Across Industries: An Exploration,” *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, pp. 26-32, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] D.N. Harshavardhan Reddy Malapati, Sai Sravanth Reddy Panyam, and Sudha Dandapani, “Enhancing PAN Card Security with OCR Based Information Extraction and Face Recognition for Reliable Identity Verification,” *2025 International Conference on Data Science, Agents and Artificial Intelligence (ICDSAAI)*, Chennai, India, pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Pranav Khare, and Shristi Srivastava, “Transforming KYC with AI: A Comprehensive Review of Artificial Intelligence-Based Identity Verification,” *Journal of Emerging Technologies and Innovative Research*, vol. 10, no. 12, pp. 525-531, 2023. [Google Scholar] [Publisher Link]

[13] Istiaque Ahmed et al., “A Systematic Review on Blockchain-Enabled eKYC: Leveraging SSI and DID for Secure and Efficient Identity Verification,” *IEEE Internet of Things Journal*, vol. 12, no. 21, pp. 44381-44401, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Seyf Kazamel, Umut Kocasarı, and Ali Alıcı, “An End-to-End Computer Vision System for Structured Information Extraction from Turkish ID Card Images,” *Computational Science and Its Applications - ICCSA 2025*: *25th International Conference*, Istanbul, Turkey, Springer, pp. 51-64, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Bektemyssova Gulnara, and Akhmer Yerassyl, “Using Image Processing and Optical Character Recognition to Recognise ID cards in the Online Process of Onboarding,” *2022 International Conference on Smart Information Systems and Technologies (SIST)*, Nur-Sultan, Kazakhstan, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mihai Alin Lazăr, "The Impact of Digital Natives' Expectations on IT Onboarding Processes," *Annals of the University Dunarea De Jos of Galati: Fascicle: I, Economics and Applied Informatics*, vol. 31, no. 1, pp. 146-153, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Erwin Yulianto, Teguh Murdianto, and Al-Amin Al-Amin, "The Role of Artificial Intelligence (AI) in Records and Document Management," *COSMOS: Journal of Education, Economics and Technology*, vol. 1, no. 6, pp. 484-499, 2024. [Google Scholar] [Publisher Link]

[18] Khalid M.O. Nahar et al., "Recognition of Arabic Air-Written Letters: Machine Learning, Convolutional Neural Networks, and Optical Character Recognition (OCR) Techniques," *Sensors*, vol. 23, no. 23, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Abhishek Potdar, Parva Barbhaya, and Sangeeta Nagpure, "Face Recognition for Attendance System using CNN based Liveliness Detection," *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, Dehradun, India, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nico Surantha, and Boy Sugijakko, "Lightweight Face Recognition-Based Portable Attendance System with Liveness Detection," *Internet of Things*, vol. 25, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] U. Ganesh Naidu et al., "Person Vein Identification using CNN," *Proceedings of Data Analytics and Management*, Singapore, vol. 3, pp. 45-59, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Houding Zhang, and Zexian Yang, "Biometric Authentication and Correlation Analysis based on CNN-SRU Hybrid Neural Network Model," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Plaifah Laimeek, and Waree Kongprawechnon, "*High-Value Fruit Biometric Identification via Triplet-Loss Technique*," Ph.D. Thesis, Thammasat University, pp. 1-55, 2022. [Google Scholar] [Publisher Link]

[24] Lamia Mosbah et al., "Adocrnet: A Deep Learning OCR for Arabic Documents Recognition," *IEEE Access*, vol. 12, pp. 55620-55631, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Dewan Ahmed Muhtasim, Monirul Islam Pavel, and Siok Yee Tan, "A Patch-Based CNN Built on the VGG-16 Architecture for Real-Time Facial Liveness Detection," *Sustainability*, vol. 14, no. 16, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Esraa Asem et al., "Biometric CNN Model for Verification based on Blockchain and Hyperparameter Optimization," *International Journal of Computational Intelligence Systems*, vol. 17, no. 1, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Konthee, "MIDV-500 - Identity Document Dataset," Kaggle, 2022. [Online]. Available:
https://www.kaggle.com/datasets/kontheeboonmeeprakob/midv500