Technological Solutions for Digital Identity:

A Computer Vision-Based Approach to Mitigate Imaging Errors

Harish Kumar, Indian Institute of Management, Kashipur, India*
https://orcid.org/0000-0002-7204-7321

Rameshwar Shivadas Ture, Indian Institute of Management, Kashipur, India

M. P. Gupta, Indian Institute of Technology, Delhi, India

R. S. Sharma, National Health Authority, Government of India, India

ABSTRACT

Digital transformation of enterprises is driving the need for a digital identity to recognize people for delivering services. The implementation of digital identity is complex, requiring several technological solutions and much coordination. Capturing and processing data is challenging because biometric issues may arise due to imaging errors. This article addresses this issue and proposes a computer vision-based framework for contactless recognition process using a focus group discussion approach for inputs from experts. The proposed framework enhances image capturing process, extraction of high-quality features from captured images, image processing, contactless face detection, and authentication. The study also derives lessons for other biometric-based identity projects based on image analysis. The proposed framework can be used as a reference for understanding multidimensional perspectives, scalability, and adoption of technological solutions in other similar projects in developing countries in future.

KEYWORDS

Computer vision, focus group discussion, identity recognition, image detection, technological solutions

1. INTRODUCTION

In the digital transformation era, digital identities are receiving more attention for recognizing people (De Marsico et al., 2019; Liu et al., 2020). National systems for digital identity management have emerged as a vital instrument in the increasingly digitised public services to include citizens (Eke et al., 2022). The use of technology-based services forms the basis for new techno-social realities (Engin et al., 2020) to meet people's ever-changing demand for services (Agarwal et al., 2021). In 2009, the Indian government initiated a unique identification program (UIDAI or Aadhaar) aimed at providing an identity to all Indian residents (Mukhopadhyay, Bouwman, and Jaiswal, 2019).

DOI: 10.4018/JDM.325352

*Corresponding Author

Aadhar, a 12-digit identification number held by every Indian citizen, intends to reduce corruption, intermediation, agency costs, fake identities, and waste of public resources (Mir et al., 2020). Several problems such as fraud and leakage in the public distribution system (PDS) and mismatch of beneficiaries are associated with the nonavailability of a unique identification (Addo and Senyo, 2021). The launch of Aadhaar aims to give the Indian citizen a unique identity, improve the use of government subsidies, and deal with illegal immigrants (Mir et al., 2020). Digital identity helps in simplifying the administrative processes and delivering public and private service efficiently to enhance social inclusion (Madon et al., 2022)

Most service providers use the e-KYC (electronic Know-Your-Customer) process through the Aadhaar platform for quick paperless on-line customer verification. The Aadhaar system makes extensive use of biometrics for identification purposes. The Aadhaar captures a person's demographic, photographic, and biometric details, including 10 fingerprints and iris of both eyes (Mir et al., 2020). However, the Aadhaar system's privacy, security, uniqueness, and scalability have always been a major concern in its development and implementation. The vulnerabilities in the data security of a biometric system may lead to adverse consequences such as leakage of users' privacy, access by unauthorized users, denial-of-service to legitimate users, and repudiation claims by corrupt users (Schlatt et al., 2022; Siau and Wang, 2020).

In developing identification systems, it is crucial that no individual should denied access to services because of false rejections when their fingerprints cannot be recognized. Major difficulties are encountered when just a single feature is used for identifying a user or a device; in particular, it can be easily forged or stolen (Qin et al., 2023). Multiple biometric modalities can be recorded to strengthen increase the accuracy in identification and improve anti-counterfeiting ability to avoid such problems. Therefore, inter-agency coordination and technological innovation are essential for the implementation of digital identity .

Numerous documented errors have been found in Aadhaar, namely, errors in individuals' names, address, gender, date of birth, and even the photographs. Moreover, the implementation of the Aadhaar project faced several challenges, such as the transfer of enrolment data, fewer enrolment stations, issues related to data integrity, printing, and dispatch of letters, seeding of Aadhaar in various domain databases, and verification of duplicate Aadhaar issuance, which directly or indirectly affect the UIDAI's operations and capacity augmentation plans.

In addition, there may be problems with recognition system's design for detecting an individual's biometrics or problems with a specific application that retrieves data from the biometric system (Jain, Nandakumar, and Ross, 2016). One of the most important biometric aspects has often been facial recognition (Qin et al., 2023). Detecting human facial features for identity management is well researched, yet it remains an open challenge because of the different expressions, head pose, aging, and variations in illumination (Leo et al., 2017). The Aadhaar system does not currently use facial recognition as a primary biometric identification method. Earlier research has focused on the challenges associated with implementing block-chain-based identity management solutions in the context of verified claims and self-sovereign identities (Kuperberg, 2019). Moreover, a comprehensive analysis is needed to understand the operational and implementation issues of the identity program. Few studies have so far discussed the analytical and technological models about digital identity management. To address such research gaps, this study proposes the following research objectives:

RO1: To analyze the technological solutions deployed in identity management at various stages of project, such as data enrolment, data processing, identity card generation, and seeding.
RO2: To propose a computer vision-based framework for digital identity to mitigate imaging errors.

This study contributes to ongoing research in three perspectives of digital identity: technology-based solutions for enrolment, identity processing (post-enrolment), identity card generation stage and service accessibility. The study also suggests a computer vision-based framework for contactless digital identity. Computer vision-based face detection is considered better than other existing methods as it can achieve high levels of accuracy when identifying individuals through their facial features. The proposed framework can be used as a reference for adopting technological solutions in future biometric-based identity programs. From a theoretical perspective, it adds significantly to the concentrated knowledge of various solutions implemented in the identity system to address implementation and operational issues. The study also derives lessons for other technology projects, consistent with the overall objectives of this research.

The study is presented as follows. Section 2 reviews the issues associated with Aadhaar. Section 3 provides the details about the focus group discussion approach used in this study. Section 4 discusses the technological solutions adopted in Aadhaar enrolment, processing (post-enrolment), and Aadhaar generation process. Section 5 proposes a computer vision-based framework for digital identity. Section 6 concerns the evaluation of the proposed approach. Section 7 derives the conclusions while Section 8 discusses the theoretical and practical implications. Section 9 presents the limitations and suggestions for further research.

2. REVIEW OF LITERATURE: ISSUES ASSOCIATED WITH AADHAAR

Digital identity refers to a collection of characteristics that are electronically recorded and saved. These characteristics serve to uniquely identify an individual. Throughout the identification life cycle, including collection, verification, storage, transmission, identity authentication, validation, and credential management, digital technology is used in the digital identification system (Eke et al., 2022). Digital technologies make it easier to improve goods and services through innovative transformation (Nambisan et al., 2017). A digital biometric system identifies an individual by determining the authenticity of a particular behavioural characteristic, such as handwritten signature, voice, gait, and keystroke or a physiological pattern such as fingerprints, iris, and retina (Elrefaei and Al-Mohammadi, 2019). Facial recognition technology is also a well-established mechanism for identity programs and has been applied in multiple fields such as identity registration, security, image retrieval, and contactless authentication (Best-Rowden and Jain, 2017; Lv, Su, and Wang, 2021).

Computer vision is a subset of Artificial Intelligence that derives high-level interpretation from digital images, videos, or multi-dimensional visual data (Borji, 2018). Using camera, hardware, software, and sensors, it collects real-time images, converts images into signals, and transmits them to image processing software to accurately identify and classify image objects (Zhang and Li, 2014). Deep learning has accelerated the process of face detection and object recognition (Lv, Su, and Wang, 2021). Computer vision technology has advanced this field (Kakani et al., 2020). A computer vision system includes cameras, illumination source, frame grabber, and image processing software. Fang et al. (2021) used computer vision to match unsafe human behaviour with safety rules.

Typically, a biometric system consists of two stages: enrolment and recognition. In the enrolment stage, biometric traits such as individual's iris, retina, fingerprints, facial features, or voice are captured along with the demographic details. During the recognition stage, the individual's extracted biometric traits are compared with a stored database to verify a claimed identity (Jain, Nandakumar, and Ross, 2016). The identification system should also be integrated with searchable unique IDs, such as name or an assigned number along with biometric details (Storisteanu et al., 2016). The deployment of the biometric system protects an application from unauthorized access. The adoption of block chain technology can be prioritized to increase security in ID cards (Alzahrani, Daim, and Choo, 2022).

Recognizing human facial features is a well-studied problem, but it is still an open challenge with different expressions, head pose, aging, and variations of illumination (Leo et al., 2017). The traditional methods of feature extraction have faced issues about eliminating glare, reducing the influence of light, face angle, and face detection accuracy. Face recognition based on image uses face regions to identify people (Qin et al., 2023). AI uses various algorithms such as Bayesian models, decision trees, k-nearest neighbour, logistic regression, and neural networks (Peng and Bhaskar, 2023). Convolutional neural network (CNN) can overcome issues of image representation and feature extractions due to its high accuracy and scalability. Regarding features extraction and accuracy, the deep learning model outperformed traditional machine learning models (Tian and Han, 2022).

Several reasons led to the delay in the delivery of the Aadhaar letter. Some could be linked to inaccurate address information provided during enrolment. As the volume of Aadhaar enrolment and creation grew, UIDAI began to have issues with the printing of Aadhaar letters. As enrolment, Aadhaar generation, letter printing, and delivering to residents are all sequential processes, bottlenecks in any one of these processes will create bubbles everywhere.

The process of Aadhaar seeding has been complex since the beginning. When the Aadhaar number was used to remove duplicates and fakes, one of the challenges was to first "seed" these databases with Aadhaar numbers, which was also required when Aadhaar authentication was used for any service delivery. There were several approaches to seeding, such as setting up camps in the field and invite all program beneficiaries to bring their eligibility documents such as ration cards and Aadhaar letters to the camp, which would help in the seeding.

Alternative approaches included creating a portal where residents themselves could seed or link their Aadhaar numbers with their records in the domain database. For example, the PDS database could be hosted online and then the residents could be asked to link their Aadhaar numbers. Linking Aadhaar numbers with bank accounts through ATMs is also one such example. However, this suggested "seeding/linking" is only the first step in the seeding process. A third-party verification of the accuracy of this seeding is an essential step. Incorrect seeding of Aadhaar numbers in the database can lead to serious problems such as denial of service to the genuine beneficiaries and conflict of records. Therefore, there is an urgent need for an in-depth analysis of the implementation and operational issues of the Aadhaar system as the system needs to be scaled up.

3. METHODOLOGY: FOCUS GROUP DISCUSSION (FGD)

Qualitative research techniques are essential for gathering detailed background information (Amoah et al., 2023). Focus group discussions (FGDs) were conducting to ascertain individual and group perceptions about digital identity (Ankrah et al., 2023). Through group interaction, focus groups with little facilitation, open-ended questions, and inductive analysis enable a participant-driven, impartial method for gathering data about a subject (Hilditch et al., 2023; Ntali, Lyimo and Dakyaga, 2023). FGD produces diverse information from participants by gathering various insights and opinion regarding the specified research problem. FGD concerns the dynamics between viewpoints on a topic (Siivonen et al., 2019). The approach helps acquire in-depth knowledge that is more than that gathered through personal interviews. As a result of the group setting's emphasis on interaction and group dynamics, issues may be discussed and explored in greater depth. The combination and deviation occurring during focus group discussions demonstrate the robustness of this process. Moreover, a researcher or facilitator can promptly ask the contributors to support or compare their perspectives, rather than just gather individual data.

In this study, the FGD constituted 22 carefully selected subject experts (Appendix 1) They represented a diverse setting to gather all possible dimensions of digital identity systems. The FGD participants had diverse work experience (5–18 years), ranging from policymakers, technology consultants, registrars, section officers, operators, researchers, digital image analysts, service providers, and users. Three FGDs with a maximum of eight experts were conducted in April and May 2022. Anonymity of the FGD participants were protected. The researcher was responsible for presenting the issues related to Aadhaar, facilitating the discussion, and prompting the participants to speak. Conventional qualitative content analysis (CQCA) was used to examine the notes taken. CQCA is the methodical reduction and classification of the gathered information based on inferred content and can be interpreted to develop relevant arguments (Hilditch et al., 2023). The analysis and interpretation of findings involves seeking patterns, relationships, and correlation within the data to draw conclusions and make recommendations.

4. ANALYSIS OF TECHNOLOGICAL SOLUTIONS IMPLEMENTED IN AADHAAR

Based on expert discussion on several aspects of the Aadhaar system, the analysis was categorized into three phases: Aadhaar enrolment, Aadhaar processing, and Aadhaar generation (Figure 1).

4.1 Technological Solutions Implemented in Aadhaar Enrolment

When enrolment started in mid-2010, UIDAI realized that the operators were making various data entry errors. Initially, the enrolment kit contained a computer system or laptop, web camera, fingerprint and iris scanners, and a printer to print the enrolment acknowledgement. UIDAI introduced the dual screen in the enrolment kit, which allowed the data entered by the operator to be simultaneously viewed by the person being enrolled. In general, the operators unknowingly mixed their own biometrics with that of the person registering, entered incomplete address that made it difficult to deliver the Aadhaar letter, provided an improper background for capturing the photograph, used a non-standardized method for photo capture, mismatched the gender, made age-related errors (Figure 1). To resolve such issues, UIDAI decided to train the operators before starting enrolment.

In the enrolment process, the field names, spellings, and pin codes for address entry emerged as a serious issue. To overcome this challenge, the city/village field was converted to a free text field and pin codes were used as the first entry. A software-driven workflow was developed. To reduce the data entry errors, various address components such as habitation, village, district, and state names were standardized, and validation and boundary checks were introduced. In addition, smart enrolment screen, enrolment through certified operators only, standardization and validation of address entries, quality check of biometrics at capture time, collection of meta-data at the time of enrolment, and 48 hours' correction window were also implemented.

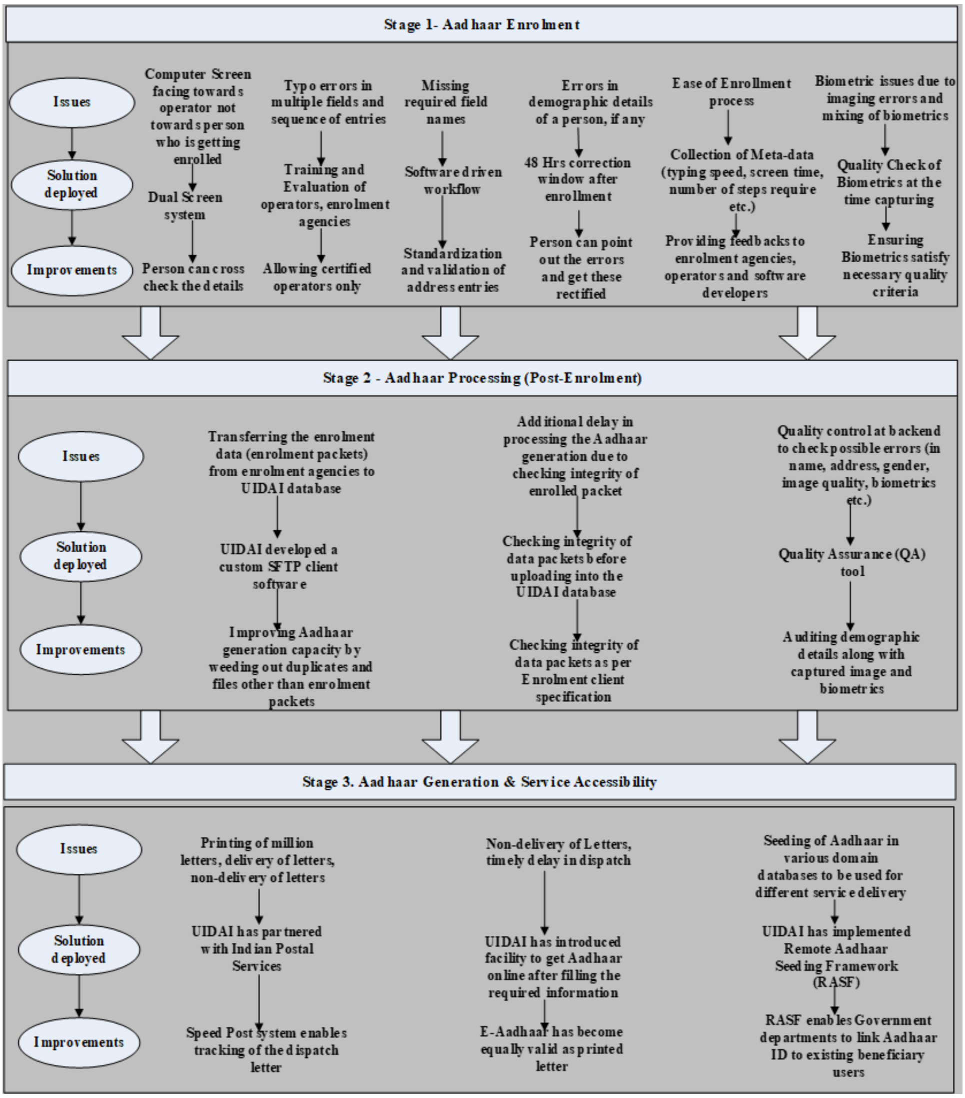
4.2 Technological Solutions Implemented in Aadhaar Processing (Post-Enrolment)

While several steps were introduced at the time of enrolment, several technological solutions were also incorporated at various points at the post-enrolment stage to synchronize enrolment machines and Quality Control at the back end (Figure 1). Enrolment agency operators uploaded each enrolment packets to UIDAI servers for further processing and Aadhaar generation. Such packets were uploaded multiple times knowingly or unknowingly by the enrolment agencies. This resulted in a large number of duplicate files in the process queue and unnecessarily choked the bandwidth. To resolve this issue, a provision was made to disallow the re-uploading of enrolment packets using SFTP client software to prioritize the packets upload to improve Aadhaar generation capacity and system performance by weeding out duplicate enrolments, removing corrupt files, recursive disk queuing for enrolment packets in the upload queue, auto connect feature to help unattended uploads, and checking packet integrity as per enrolment specifications.

An additional step of quality assurance (QA) was introduced. A workflow-based system was devised to check the data quality. The system was developed based on the maker and checker principle. QA tool ensured the quality of resident's data by processing these details and providing the output to the server. Improvements in biometric algorithms such as extracting feature, matching, and fixing security issues enhanced the biometric recognition process. The use of cloud architecture to store data enhanced accessibility and rapid analytics of biometrics across different entities.

As biometrics are the basis of ensuring uniqueness, one could assume that those who did not have biometrics (usable fingerprints or iris, etc.) or young children (who do not have developed biometrics) would be excluded. The enrolment software was so designed that if the age were less than five years, it would not require biometric capture. Similarly, for those adults who fell in the

Figure 1. Issues, technological solutions, and improvements made in Aadhaar
(Source: Authors' elaboration)


Stage 1- Aadhaar Enrolment
Issues
Solution deployed
Improvements
Computer Screen facing towards operator not towards person who is getting enrolled
Dual Screen system
Person can cross check the details
Typo errors in multiple fields and sequence of entries
Training and Evaluation of operators, enrolment agencies
Allowing certified operators only
Missing required field names
Software driven workflow
Standardization and validation of address entries
Errors in demographic details of a person, if any
48 Hrs correction window after enrollment
Person can point out the errors and get these rectified
Ease of Enrollment process
Collection of Meta-data (typing speed, screen time, number of steps require etc.)
Providing feedbacks to enrolment agencies, operators and software developers
Biometric issues due to imaging errors and mixing of biometrics
Quality Check of Biometrics at the time capturing
Ensuring Biometrics satisfy necessary quality criteria
Stage 2 - Aadhaar Processing (Post-Enrolment)
Issues
Solution deployed
Improvements
Transferring the enrolment data (enrolment packets) from enrolment agencies to UIDAI database
UIDAI developed a custom SFTP client software
Improving Aadhaar generation capacity by weeding out duplicates and files other than enrolment packets
Additional delay in processing the Aadhaar generation due to checking integrity of enrolled packet
Checking integrity of data packets before uploading into the UIDAI database
Checking integrity of data packets as per Enrolment client specification
Quality control at backend to check possible errors (in name, address, gender, image quality, biometrics etc.)
Quality Assurance (QA) tool
Auditing demographic details along with captured image and biometrics
Stage 3. Aadhaar Generation & Service Accessibility
Issues
Solution deployed
Improvements
Printing of million letters, delivery of letters, non-delivery of letters
UIDAI has partnered with Indian Postal Services
Speed Post system enables tracking of the dispatch letter
Non-delivery of Letters, timely delay in dispatch
UIDAI has introduced facility to get Aadhaar online after filling the required information
E-Aadhaar has become equally valid as printed letter
Seeding of Aadhaar in various domain databases to be used for different service delivery
UIDAI has implemented Remote Aadhaar Seeding Framework (RASF)
RASF enables Government departments to link Aadhaar ID to existing beneficiary users

category of biometric exceptions (no hands or iris), the software would not capture biometrics but had the provision for taking an additional photograph.

4.3 Technological Solutions in Aadhaar Generation and Service Accessibility

The technological solutions (Figure 1) used to generate Aadhaar can be categorized as follows: (1) online dispatch of enrolment packets; (2) seeding of Aadhaar in various domain databases, and (3) e-Aadhaar.

4.3.1 Online Dispatch of Enrolment Packets

While managing the enrolment eco-system and processing systems at CIDR were quite complex in themselves, post-Aadhaar generation activities were also quite challenging. This included printing letters and ensuring their delivery to recipients. As the Aadhaar generation grew, so did the demand for their letters and UIDAI had to build a system to print millions of letters every day to ensure the Aadhaar cycle of enrolment, generation, and delivery of Aadhaar letters in the shortest time. UIDAI had partnered with India Post for letter printing and delivery. The solution had a robust reconciliation mechanism to reconcile print files with vendors and delivery acknowledgements with India post to ensure each letter was delivered and end-to-end reconciliation was achieved from generation to printing to delivery.

4.3.2 Seeding of Aadhaar in Various Domain Databases

UIDAI simplified the process of initial seeding or linking and verification of this linking in a scalable manner and created an online application "Remote Aadhaar Seeding Framework (RASF)" that enables government departments to link Aadhaar numbers to existing beneficiary identities, such as ration cards, LPG gas connections, job cards, and student roll numbers for scholarships. RASF offers a two-step, reliable, and process-oriented approach to large-scale multichannel seeding. The first stage is seeding request either generated by a resident or on behalf of the resident. The second stage is verification, in which the seeding requests can be verified, thus providing a flag in the seeding record to indicate that it has been verified and can be used for service delivery. RASF application offers several features, including an online multi-channel seeding convergence platform, a prebuilt SMS/online resident self-service channel, user access management, audit trails, and data import/export capabilities to achieve multi-channel seeding.

4.3.3 e-Aadhaar

Non-delivery of letter led to very serious situation, where complaints were received from people who wanted another copy of the letter. Hence, UIDAI introduced the online facility to check the status of Aadhaar enrolment. Furthermore, they introduced a facility for printing Aadhaar letter online after providing some details such as enrolment ID or Aadhaar number and pin code. This letter, termed as e-Aadhaar, became an instantaneous success in solving major problems of letter non-delivery.

Although UIDAI adopted various technological solutions at different stages of the Aadhaar system, the biometrics issues persist in some cases due to imaging errors and the mixing of biometric data. The study focuses on this topic and has developed a computer vision-based approach (section 5) to provide contactless authorization of an individual's identity.

5. PROPOSED COMPUTER VISION-BASED APPROACH FOR AADHAAR

The computer vision technique can resolve biometric issues arising from imaging errors and mixing of biometrics. Based on the earlier discussion and the inputs received from experts (Appendix 1), the proposed framework (Figure 2) consists of three different stages of Aadhaar to improve the existing process while complementing all previous solutions (section 4). The stage 1 (Aadhaar enrolment process) comprises image acquisition to capture an individual's image using a digital camera and a computer vision-based frame grabber for extracting essential features from the captured image. The stage 2 (Aadhaar processing (post-enrolment)) includes image processing for image segmentation, smoothing, restoration, enhancement, and augmentation. Finally, stage 3 (Aadhaar generation (service accessibility)) deals with face detection and contactless authentication.

5.1 Stage 1: Aadhaar Enrolment Process—Image Acquisition and Feature Extractions

Most participants recognized face detecting techniques and extracting the features for further processing to reduce the biometric errors of the image.

5.1.1 Image Acquisition

Participants found two types of cameras used in computer vision techniques to acquire images, namely, “charge coupled device” (CCD) and “complementary metal oxide semiconductor” (CMOS). The light-sensitive semiconductors used in such cameras can convert light into electronic signals using an A/D converter and store these on a hard drive or a flash memory. X-ray tubes, lasers, as well as incandescent, fluorescent, and infrared lamps can be used as light source. The image quality is directly affected by the illumination process during image acquisition in computer vision. The adequate light source, the position of camera, and camera type (either CCD or CMOS) can enhance the quality of the image captured for Aadhaar.

5.1.2 Vision-Based Frame Grabber

The frame grabber is an electronic device that captures and processes images. It transmits the digital image to a computer or graphics memory via bus interface for processing, storing, and displaying. A typical deep convolutional neural network (CNN) has three types of neural layers, such as multiple convolutional layers along with pooling, activation functions, and a fully connected layer (Fang et al., 2020). The CNN model can be used to extract deep features from latent variables to reduce computational and training costs (Ullah et al., 2023). CNN facilitates deep convolutions filtering mechanisms to extract multi-scale feature maps and discriminative features (Feng et al., 2019).

CNNs need a large amount of labelled training data to learn to detect faces. The architecture of a face detection CNN can vary depending on the specific needs of the application. However, some commonly used architectures include VGGNet, ResNet, and InceptionNet. The input layer of CNN architecture receives the image data, which is typically represented as a matrix of pixel values. To extract features such as edges, textures, and shapes, filters can be applied to the input image via convolutional layers. Each filter produces a new feature map by performing a mathematical operation (convolution) on a small section of the input image. Participants mentioned that the convolutional layers extract features from the captured image, followed by an activation function such as rectified linear units (ReLUs). The pooling layers reduce the dimensionality of the visual data. The flattened layers convert the extracted features into neurons and transmit them to the fully connected layers to calibrate the weights and predict the outcome (Ibrahim, Haworth, and Cheng, 2020). Participants explained that the vision-based frame grabber can extract features from captured images during Aadhaar enrolment. It can sharpen the image for detecting edges or specific regions for further processing.

For real-time face detection using computer vision, there are several different face detection algorithms such as the Viola-Jones algorithm. It is a classic approach for detecting faces using Haar features and a cascade of classifiers. This algorithm is fast and efficient but may not be as accurate as others. Histogram of Oriented Gradients (HOG) algorithm works by detecting the local gradients in an image and those gradients are used to construct an image representation. CNNs have shown remarkable success in face detection. They are highly accurate but may be slower than others. Faces are typically detected using machine learning algorithms such as Random Forests or Support Vector Machines (SVMs) . For real-time applications, algorithms such as Viola-Jones and HOG may be more suitable; however, for more accuracy-critical applications, CNNs and feature-based detection may be more appropriate.

5.2 Stage 2: Aadhaar Processing (Post-Enrolment)—Image Processing

After Aadhaar enrolment, the image features and recognition quality should be maintained through image processing while transferring the data packet from enrolment agency to UIDAI database. The participants discussed about image enhancement, segmentation, and classification through an image processing software to enhance contrast and quality of images. The image segmentation process can render meaningful connected components of an acquired image. Different approaches such as threshold, region-based, edge-based, or connectivity-preserving relaxation methods can be used for image segmentation (Zhang, and Li, 2014).

Figure 2. Proposed computer vision-based framework for digital identity (Aadhaar)
(Source: Authors' elaboration)

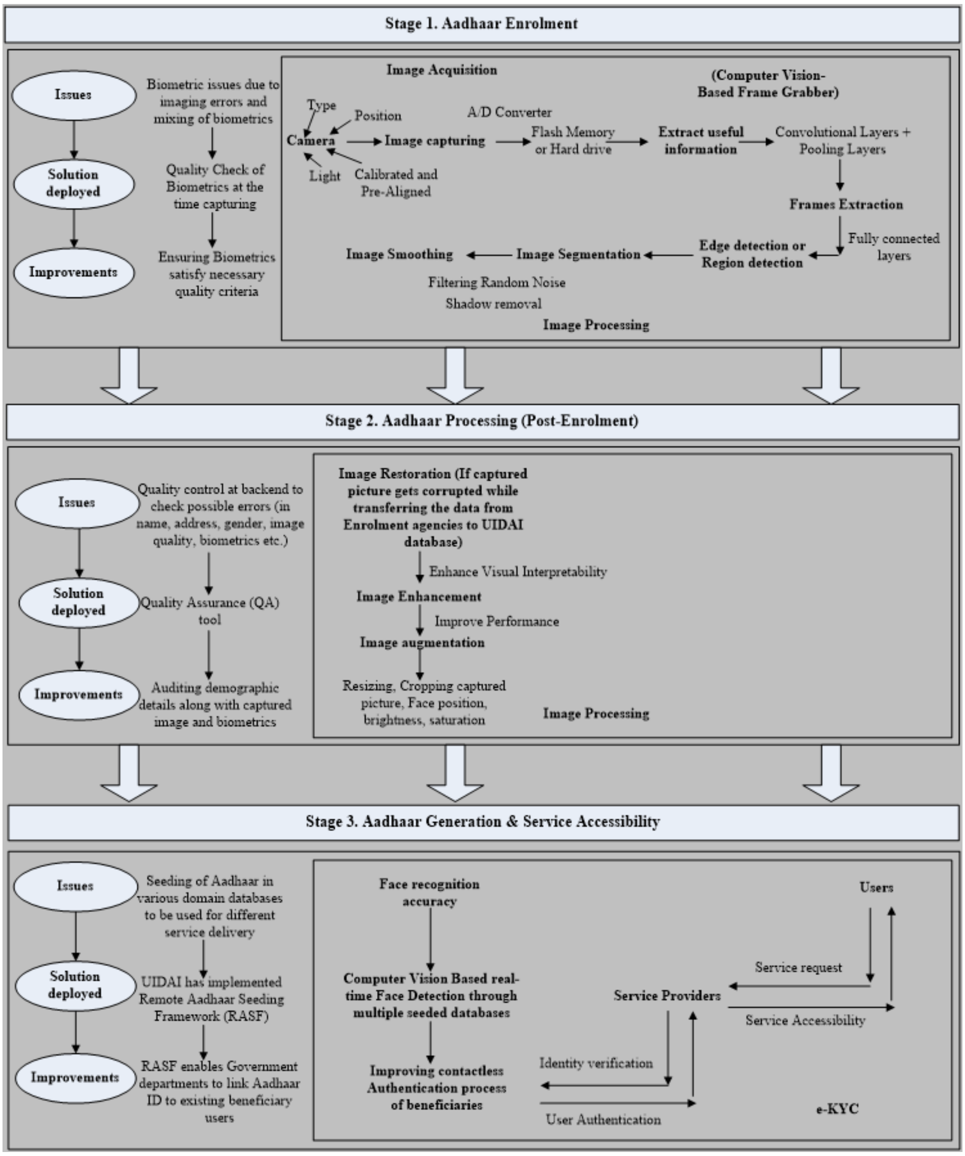

Stage 1. Aadhaar Enrolment
Issues
Biometric issues due to imaging errors and mixing of biometrics
Solution deployed
Quality Check of Biometrics at the time capturing
Improvements
Ensuring Biometrics satisfy necessary quality criteria
Image Acquisition
(Computer Vision-Based Frame Grabber)
Type
Position
A/D Converter
Camera
Image capturing
Flash Memory or Hard drive
Extract useful information
Convolutional Layers + Pooling Layers
Light
Calibrated and Pre-Aligned
Frames Extraction
Fully connected layers
Image Smoothing
Image Segmentation
Edge detection or Region detection
Filtering Random Noise
Shadow removal
Image Processing
Stage 2. Aadhaar Processing (Post-Enrolment)
Issues
Quality control at backend to check possible errors (in name, address, gender, image quality, biometrics etc.)
Solution deployed
Quality Assurance (QA) tool
Improvements
Auditing demographic details along with captured image and biometrics
Image Restoration (If captured picture gets corrupted while transferring the data from Enrolment agencies to UIDAI database)
Enhance Visual Interpretability
Image Enhancement
Improve Performance
Image augmentation
Resizing, Cropping captured picture, Face position, brightness, saturation
Image Processing
Stage 3. Aadhaar Generation & Service Accessibility
Issues
Seeding of Aadhaar in various domain databases to be used for different service delivery
Solution deployed
UIDAI has implemented Remote Aadhaar Seeding Framework (RASF)
Improvements
RASF enables Government departments to link Aadhaar ID to existing beneficiary users
Face recognition accuracy
Computer Vision Based real-time Face Detection through multiple seeded databases
Improving contactless Authentication process of beneficiaries
Users
Service request
Service Providers
Service Accessibility
Identity verification
User Authentication
e-KYC

Image smoothing can filter out random noise from the captured image (Liu, 2020) to reduce the errors due to imaging and mixed biometrics. The image is restored during the image restoration process using suitable processing (Tiwari, Lamba, and Gupta, 2018). Image enhancement increases the contrast of the restored image to provide better visibility and recognizable interpretations. The image augmentation process can be applied to reduce overfitting and improve the model's generalizability. Data augmentation techniques can be divided into two types: (1) position, such as crop, resize, or horizontal flip and (2) Colour, such as brightness, contrast, or saturation (Fang et al., 2020) that enhances the image quality for identity authorization process.

5.3 Stage 3: Aadhaar Generation and Service Accessibility—Face Detection and Contactless Authentication

Participants agreed that identity authorization should be done by comparing an individual's biometric patterns with the captured enrolment data. The identity providers should develop a robust system for authentication (registration, authorization, and management). Augmentation techniques can also be used for better training results (Tian and Han, 2022). The user generally requests service accessibility from service provider. Based on the identity provided by the user, the service provider asks the UIDAI to verify the identity (Figure 2). The UIDAI returns the authentication results. Once the users are successfully authenticated, service providers facilitate services to the users (De Marsico et al., 2019). In the existing Aadhaar authorization process, users are verified through a one-time password (OTP) received on mobile number linked to Aadhaar or the user's registered email id. Some services use finger biometrics to verify an individual's authenticity to provide the services or subsidized benefits. Besides, the platform should be designed to combine identity data with analytics to provide the required social assistance to the beneficiaries (Madon et al., 2022). The proposed computer vision-based framework would help UIDAI and service providers to authenticate an individual through face recognition with higher accuracy to speed up the contactless e-KYC process.

6. EVALUATION OF THE PROPOSED APPROACH

The proposed framework can address the inefficiencies in the existing Aadhaar system. There is no clear assessment path as the best approach depends on the artifact as well as the underlying problem (Schlatt et al., 2022). Qualitative interview method used in our study is often used in IS research as it can generate rich data. Therefore, we conducted seven more interviews in June 2022 for collective evaluation of our proposed framework by presenting it to the interviewees and considering their feedback. The chosen experts included a registrar, UID program (expert A); section officer, UID (expert B); technical consultant, digital services (expert C); analyst—sensor and image data (expert D); manager, service delivery (expert E); professor, technology management (expert F); and developer, AI & computer vision (expert G). The experts held distinct positions; hence, the objectives could be viewed from different perspectives. The proposed framework was designed to assess its utility, functionality, accuracy, reliability.

The relevance of the derived objectives and their corresponding requirements was confirmed by Expert A. He claimed that image acquisition is a critical aspect of digital identity verification and authentication, and it requires careful consideration of quality, consistency, privacy, accessibility, and regulatory issues to ensure its effectiveness, fairness, and reliability. Poor-quality images can result in false positives or false negatives, leading to errors and potential security risks. The images used for digital identity should be consistent over time (experts B, D, and E), which requires standardized image acquisition protocols. Everyone should be able to authenticate, regardless of their physical abilities or technical expertise (expert A, B). Expert C stressed the significance of a positive user experience because the systems' functional details are ignored by many users. Thus, there is a need for user-friendly interfaces to accommodate individuals with disabilities or other special needs.

A computer vision-based frame grabber involves capturing, processing visual data, and analyzing the images for specific features or patterns such as facial features or object recognition and extracting relevant information for further analysis using computer vision algorithms (experts C, D, and F). It requires standardized frames extraction protocols, such as the use of specific cameras or lighting conditions and ensuring that people's poses and facial expressions are consistent across frames (expert G).

An image is divided into multiple segments or regions, each corresponding to a different feature, object, or background. Segmenting the acquired image into different facial features helps in extracting and analyzing the relative positions and dimensions of these features for further analysis (expert D).

The choice of algorithm depends on the particular application and the image characteristics being studied (expert G). Image smoothing involves reducing the noise or irregularities in an image to produce a smoother and more consistent image. Noise reductions helps to extract and analyze the underlying features of an image more accurately and reliably (experts D, G). Over-smoothing can result in the loss of important image details while under-smoothing can result in residual noise and irregularities (experts C, D, and F). Image smoothing can significantly impact downstream analysis, such as feature extraction or classification.

Image restoration is a technique used in image-based digital identity verification and authentication to recover degraded or corrupted images. It involves removing noise, blurring, or other artifacts to produce a clearer and more accurate representation of the image (experts D and G). It involves restoring the image quality that has been degraded because of factors such as poor lighting conditions, sensor noise, or compression artifacts. The choice of an algorithm for image restoration depends on the type of image degradation. For example, different algorithms may be used for removing Gaussian noise, impulse noise, or motion blur. Algorithm selection, type of degradation, and impact on downstream analysis is necessary to ensure its effectiveness and reliability (experts C and F). Image enhancement improves the image quality by adjusting their brightness, contrast, sharpness, and other parameters. Image augmentation increases the diversity and size of image datasets by generating new images from existing ones. This can help in improving the accuracy, reliability, and robustness of facial recognition (experts F and G).

Expert B emphasized that the most crucial factor is process efficiency. Viola-Jones algorithm, HOG algorithm, and CNN algorithm are used for real-time face detection using computer vision. Each algorithm has its own advantages and drawbacks, and algorithm are selected according to the specific needs of the application (experts D and G). Faster algorithms may sacrifice accuracy, while more accurate algorithms may be slower. Techniques such as frame skipping, region of interest selection, and image resizing can be used to reduce the amount of data to be processed (experts F and G).

Contactless authentication in image-based digital identity has several advantages over traditional methods, such as passwords or physical tokens, including convenience, speed, and reduced risk of infectious disease transmission. Face-based digital identity can help improve service accessibility by providing secure, personalized, and interoperable access to various services (experts A, B, and E).

Expert D focused on the possibility of authentication with a high level of assurance and the associated risk reduction. Several experiments such as testing the accuracy, bias, usability, and security can be conducted to show the effectiveness of computer vision-based digital identity systems (experts C and F). The accuracy test includes images of people with different poses, lighting conditions, and facial expressions to simulate real-world scenarios. To test for bias in digital identity, a diverse dataset should be developed to include people of different races, ages, genders, and other demographic factors. The usability test evaluates the ease of use and user experiences. Security testing conducts vulnerability scans to identify potential cyber weaknesses in the digital identity system (experts C, F, and G).

7. CONCLUSION

Implementing Aadhaar identity requires unprecedented coordination of policies, technologies, logistics, and between agencies. Several challenges arose in the implementation of the Aadhaar project. The multidimensional perspectives, technology, and scalability must be understood to resolve the issues associated with Aadhaar.

This study deeply analyses the implementation and operational challenges in Aadhaar in terms of associated issues, technological solutions deployed, and improvements made in Aadhaar enrolment, Aadhaar processing (post-enrolment) and Aadhaar generation and service accessibility process. Dual computer screen, training enrolment agencies, software-driven workflow, collection of metadata, quality check of biometrics, checking the integrity of data transfer, seeding of Aadhaar into multiple databases for linking it with beneficiaries, and e-Aadhaar have been implemented to improve the process. However, in some cases, biometrics issues were reported due to imaging errors and mixing of biometrics.

To resolve this issue, the study has adopted the FGD approach to propose the computer vision-based framework for digital identity. The proposed framework addresses the inefficiencies in the existing Aadhaar system. Computer vision advances the facial recognition process by acquiring an individual's images through digital cameras. It extracts certain features through convolutional, pooling, and fully connected layers. Then it converts images into signals and sends to image processing software for further analysis. The proposed framework deals with enhancing the image capturing process, extracting high-quality features from captured images, image processing, contactless face detection, and authentication. Face detection method using computer vision algorithms can quickly identify the individuals in real-time scenario with higher accuracy. The proposed computer vision approach can be easily scaled to handle large databases of individuals. The computer vision-based face recognition and authorization can improve the service accessibility by the beneficiaries.

8. THEORETICAL AND PRACTICAL CONTRIBUTIONS

Many developing countries have implemented digital identity platforms to improve the administration of social assistance programming and mitigate leakages in the system. Aadhaar has provided the biometric sector with an excellent opportunity to grow. The digital ID opens new markets, such as banking, credit, health, or education, and the perspective of a cashless economy. As a social innovation, the digital identity management system demands responsibility-by-design approaches considering unique values, principles, local contexts, and interests and that can address broader societal concerns. The identity recognition system based on multimodality shows the advantages of high reliability, strong robustness, and wide practicability.

The 2D face detection method uses still images to recognize an individual. The 3D face detection method creates a more detailed analysis of facial features to identify the individuals. 3D methods provide more accurate results than 2D methods by capturing depth and contours of face. Face detection method using computer vision algorithms can quickly identify the individuals in real-time scenario with higher accuracy. CNN is commonly used for facial recognition in computer vision-based approach. Support Vector Machines (SVM) can classify data into different categories and can be used for facial recognition by training model to recognize different facial features and patterns.

The use of CNNs in image-based digital identity improves the accuracy and reliability of digital identity systems and enables more convenient and seamless user experiences. Comparison of face-based digital identity systems must include factors such as accuracy, privacy and security, accessibility, and ease of use. For example, systems such as Face ID (developed by Apple) and Amazon Rekognition have high accuracy rates and are relatively easy to use, while Aadhaar has faced criticism for privacy and security concerns.

The use of facial recognition in Aadhaar is still in the exploratory stage. The findings of this study can be used as a reference for adoption of technological solutions in similar biometric-based identity programs. From a theoretical perspective, it adds significant concentrated knowledge over various solutions implemented in Aadhaar program to resolve implementation and operational issues. This study also advances the theoretical aspects of Aadhaar design to ensure accuracy, security, and privacy of the system. Policymakers, technology consultants, UIDAI officials, enrolment agencies, identity operators, researchers, and service providers can benefit from the proposed framework to explore and implement the visual aspects in digital identity to make contactless authentication of individuals in real time.

From the citizens' perspective, the proposed approach suggests the use of computer vision-based digital identity to authenticate users accessing a system or platform. The proposed approach offers a seamless and convenient user experience, allowing individuals to verify their identity quickly and easily. From the government's perspective, UIDAI should develop the necessary infrastructure, technology, and processes to ensure accuracy, security, and privacy of the Aadhaar system. The Aadhaar system should be supported by a legal framework that defines the rights and responsibilities of individuals and entities involved.

From service providers' perspectives, face-based digital identity can verify the identity of parties involved in accessing services and online transactions. Privacy and security require implementation of strong data protection measures, such as encryption, access controls, and data minimization, to prevent unauthorized access or misuse of images. Using computer vision-based digital identity, retailers can also offer personalized product recommendations and track customers' behavior to improve business strategies. Computer vision-based implementation should be carefully evaluated to ensure its accuracy and security to prevent unauthorized access or misuse of digital identity.

9. LIMITATIONS AND FUTURE RESEARCH

This study has analysed various technological solutions adopted in Aadhaar program at various stages to reduce the operational issues. The study does not discuss the algorithmic issues while proposing the computer-vision based framework for digital identity. Future research can adopt a more robust algorithmic approach to consider the use of computer vision technology for innovating digital identity system. Future research can focus on the development of high energy-efficient hardware engines and massive innovations of computer vision systems for managing digital identity and authentication processes. The future research may also be focused on the measuring of effectiveness of computer-vision based digital identity systems.

COMPETING INTERESTS

The authors of this publication declare there are no competing interests.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, *38*(2), 101568. doi:10.1016/j.giq.2021.101568

Agarwal, R., Mittal, N., Patterson, E., & Giorcelli, M. (2021). Evolution of the Indian LPG industry: Exploring conditions for public sector business model innovation. *Research Policy*, *50*(4), 104196. doi:10.1016/j.respol.2020.104196

Alzahrani, S., Daim, T., & Choo, K. K. R. (2022). Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems. *IEEE Transactions on Engineering Management*. doi:10.1109/TEM.2022.3158185

Amoah, J. O., Britwum, A. O., Essaw, D. W., & Mensah, J. (2023). Solid waste management and gender dynamics: Evidence from rural Ghana. *Research in Globalization*, *6*, 100111. doi:10.1016/j.resglo.2023.100111

Ankrah, D. A., Anum, R., Anaglo, J. N., & Boateng, S. D. (2023). Influence of sustainable livelihood capital on climate variability adaptation strategies. *Environmental and Sustainability Indicators*, *18*, 100233. doi:10.1016/j.indic.2023.100233

Best-Rowden, L., & Jain, A. K. (2017). Longitudinal study of automatic face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *40*(1), 148–162. doi:10.1109/TPAMI.2017.2652466 PMID:28092523

Borji, A. (2018). Negative results in computer vision: A perspective. *Image and Vision Computing*, *69*, 1–8. doi:10.1016/j.imavis.2017.10.001

De Marsico, M., Mecca, A., & Barra, S. (2019). Walking in a smart city: Investigating the gait stabilization effect for biometric recognition via wearable sensors. *Computers & Electrical Engineering*, *80*, 106501. doi:10.1016/j.compeleceng.2019.106501

Eke, D., Oloyede, R., Ochang, P., Borokini, F., Adeyeye, M., Sorbarikor, L., Wale-Oshinowo, B., & Akintoye, S. (2022). Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural concerns. *Journal of Responsible Technology*, *11*, 100039. doi:10.1016/j.jrt.2022.100039

Elrefaei, L. A., & Al-Mohammadi, A. M. (2022). Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme. *Journal of King Saud University-Computer and Information Sciences*, *34*(2), 204–217. doi:10.1016/j.jksuci.2019.10.011

Engin, Z., van Dijk, J., Lan, T., Longley, P. A., Treleaven, P., Batty, M., & Penn, A. (2020). Data-driven urban management: Mapping the landscape. *Journal of Urban Management*, *9*(2), 140–150. doi:10.1016/j.jum.2019.12.001

Fang, W., Love, P. E., Ding, L., Xu, S., Kong, T., & Li, H. (2021). Computer Vision and Deep Learning to Manage Safety in Construction: Matching Images of Unsafe Behaviour and Semantic Rules. *IEEE Transactions on Engineering Management*. Advance online publication. doi:10.1109/TEM.2021.3093166

Fang, W., Love, P. E., Luo, H., & Ding, L. (2020). Computer vision for behaviour-based safety in construction: A review and future directions. *Advanced Engineering Informatics*, *43*, 100980. doi:10.1016/j.aei.2019.100980

Feng, X., Jiang, Y., Yang, X., Du, M., & Li, X. (2019). Computer vision algorithms and hardware implementations: A survey. *Integration (Amsterdam)*, *69*, 309–320. doi:10.1016/j.vlsi.2019.07.005

Hilditch, C. J., Gregory, K. B., Arsintescu, L., Bathurst, N. G., Nesthus, T. E., Baumgartner, H. M., Lamp, A. C. M., Barger, L. K., & Flynn-Evans, E. E. (2023). Perspectives on fatigue in short-haul flight operations from US pilots: A focus group study. *Transport Policy*, *136*, 11–20. doi:10.1016/j.tranpol.2023.03.004

Ibrahim, M. R., Haworth, J., & Cheng, T. (2020). Understanding cities with machine eyes: A review of deep computer vision in urban analytics. *Cities (London, England)*, *96*, 102481. doi:10.1016/j.cities.2019.102481

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, *79*, 80–105. doi:10.1016/j.patrec.2015.12.013

Kakani, V., Nguyen, V. H., Kumar, B. P., Kim, H., & Pasupuleti, V. R. (2020). A critical review on computer vision and artificial intelligence in food industry. *Journal of Agriculture and Food Research*, *2*, 100033. doi:10.1016/j.jafr.2020.100033

Kuperberg, M. (2019). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, *67*(4), 1008–1027. doi:10.1109/TEM.2019.2926471

Leo, M., Medioni, G., Trivedi, M., Kanade, T., & Farinella, G. M. (2017). Computer vision for assistive technologies. *Computer Vision and Image Understanding*, *154*, 1–15. doi:10.1016/j.cviu.2016.09.001

Liu, X. (2020). Research on intelligent visual image feature region acquisition algorithm in Internet of Things framework. *Computer Communications*, *151*, 299–305. doi:10.1016/j.comcom.2020.01.008

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, *166*, 102731. doi:10.1016/j.jnca.2020.102731

Lv, X., Su, M., & Wang, Z. (2021). Application of Face Recognition Method Under Deep Learning Algorithm in Embedded Systems. *Microprocessors and Microsystems*, *104034*, 104034. doi:10.1016/j.micpro.2021.104034

Madon, S., Ranjini, C. R., & Anantha Krishnan, R. K. (2022). Aadhaar and social assistance programming: Local bureaucracies as critical intermediary. *Information Technology for Development*, *28*(4), 705–720. doi:10.1080/02681102.2021.2021130

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly*, *37*(2), 101442. doi:10.1016/j.giq.2019.101442

Mukhopadhyay, S., Bouwman, H., & Jaiswal, M. P. (2019). An open platform centric approach for scalable government service delivery to the poor: The Aadhaar case. *Government Information Quarterly*, *36*(3), 437–448. doi:10.1016/j.giq.2019.05.001

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital Innovation Management: Reinventing innovation management research in a digital world. *Management Information Systems Quarterly*, *41*(1), 223–238. https://www.jstor.org/stable/26629644. doi:10.25300/MISQ/2017/41:1.03

Ntali, Y. M., Lyimo, J. G., & Dakyaga, F. (2023). Trends, impacts, and local responses to drought stress in Diamare Division, Northern Cameroon. *World Development Sustainability*, *2*, 100040. doi:10.1016/j.wds.2022.100040

Peng, G., & Bhaskar, R. (2023). Artificial Intelligence and Machine Learning for Job Automation: A Review and Integration. [JDM]. *Journal of Database Management*, *34*(1), 1–12. doi:10.4018/JDM.318455

Qin, Z., Zhao, P., Zhuang, T., Deng, F., Ding, Y., & Chen, D. (2023). A survey of identity recognition via data fusion and feature learning. *Information Fusion*, *91*, 694–712. doi:10.1016/j.inffus.2022.10.032

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, *59*(7), 103553. doi:10.1016/j.im.2021.103553

Siau, K., & Wang, W. (2020). Artificial intelligence (AI) ethics: Ethics of AI and ethical AI. [JDM]. *Journal of Database Management*, *31*(2), 74–87. doi:10.4018/JDM.2020040105

Siivonen, P. T., Peura, K., Hytti, U., Kasanen, K., & Komulainen, K. (2020). The construction and regulation of collective entrepreneurial identity in student entrepreneurship societies. *International Journal of Entrepreneurial Behaviour & Research*, *26*(3), 521–538. doi:10.1108/IJEBR-09-2018-0615

Storisteanu, D. M., Norman, T. L., Grigore, A., & Labrique, A. B. (2016). Can biometrics beat the developing world's challenges? *Biometric Technology Today*, *2016*(11), 5–9. doi:10.1016/S0969-4765(16)30193-X

Tian, X., & Han, H. (2022). Deep convolutional neural networks with transfer learning for automobile damage image classification. [JDM]. *Journal of Database Management*, *33*(3), 1–16. doi:10.4018/JDM.309738

Tiwari, M., Lamba, S. S., & Gupta, B. (2018). An image processing and computer vision framework for efficient robotic sketching. *Procedia Computer Science*, *133*, 284–289. doi:10.1016/j.procs.2018.07.035

Ullah, F., Cheng, X., Mostarda, L., & Jabbar, S. (2023). Android-IoT Malware Classification and Detection Approach Using Deep URL Features Analysis. [JDM]. *Journal of Database Management*, *34*(2), 1–26. doi:10.4018/JDM.318414

Zhang, H., & Li, D. (2014). Applications of computer vision techniques to cotton foreign matter inspection: A review. *Computers and Electronics in Agriculture*, *109*, 59–70. doi:10.1016/j.compag.2014.09.004

APPENDIX 1

The experts, who have participated in focus group discussion (FGD). The personal information (names, contact and organization details) are kept hidden to follow the data privacy norms

The experts

Experts	Experts / designation	Experience	Country
Expert 1	Technical consultant, IT Services	>10 years	India
Expert 2	Registrar, Aadhaar Enrolment	>13 years	India
Expert 3	Operator, Enrolment agency	>5 years	India
Expert 4	Professor, Public policy	>20 years	India
Expert 5	Solution provider, Digital Services	>13 years	India
Expert 6	Professor, e-governance	>20 years	India
Expert 7	Specialist, ICT	>8 years	India
Expert 8	Officer, Public Distribution System (PDS)	>11 years	India
Expert 9	Professor, Industry 4.0, and competitiveness	>15 years	India
Expert 10	Section Officer, UID	>5 years	India
Expert 11	Technical consultant, digital services	>13 years	India
Expert 12	Analyst, Sensor and image data	> 7 years	India
Expert 13	Assistant Professor, AI, and Computer Vision	>5 years	India
Expert 14	Chief Technical officer, Network, and services	>15 years	India
Expert 15	Associate consultant, Data retrieval	>7 years	India
Expert 16	Supervisor, Aadhaar Operations	>5 years	India
Expert 17	Solution Provider, Database systems	> 10 years	India
Expert 18	Head – IT Digital Transformation	>16 years	India
Expert 19	Senior consultant, Data security	>18 years	India
Expert 20	Senior research fellow, Computer Vision	>5 years	India
Expert 21	Manager, Service development	>12 years	India
Expert 22	Professor, Technology management	>18 years	India

Harish Kumar received his Ph.D. in Information Systems from Department of Management Studies, Indian Institute of Technology (IIT) Delhi, India in 2018. He has completed his M.Tech. from International Institute of Information Technology Hyderabad (IIIT-H), India. His area of research includes artificial intelligence, metaverse, computer vision, digital transformation, technology-oriented businesses, and services. Currently, he is working as an assistant professor in Information Technology and Systems at Indian Institute of Management (IIM) Kashipur, India. He is also involved as a member of assessment teams in esteemed projects such as Digital India Awards – 2016, Web Ratna awards – 2014. He has participated/attended the reputed conferences such as ICEGOV, IEEE, ICEG, Young Scientist's Conclave and Startup India Conclave.

Rameshwar Shivadas Ture is an assistant professor in Organizational Behavior and Human Resource Management at IIM Kashipur. He earned his Ph.D. from Department of Management Studies, Indian Institute of Technology Madras in 2015. He has completed his post graduate degree in Human Resource Development and Management from IIT Kharagpur and Aeronautical Engineering degree from AeSI, New Delhi. His research interests include digitalization, upskilling, and gig economy.

M P Gupta is Modi Foundation Chair Professor at Department of Management studies, IIT Delhi. He is Known for pioneering works in e-governance [that include 30 Doctoral thesis, 22 sponsored projects worth more than 5 crores, co-authored book 'Government Online', two other edited books 'Towards E-government' & 'Promise of E-governance' and 200+ research papers appeared in National and International Journals/Conference Proceedings. He has guided production of 14 edited volumes (large collection of literature on e-gov) via the International Conference on E-governance (ICEG) since 2003. He has been closely following 'Digital India' and 'Smart City' programs of the Government of India (GoI). He is involved in several policy making committees on ICT in the Center and State Governments in India: also, on jury of prestigious awards committees viz. Digital India Awards, National Awards on e-gov, Data Security Council of India (DSCI), and Computer Society of India (CSI) Egov Awards.

Ram Sewak Sharma is an Indian bureaucrat and former civil servant. From February 2021, he is serving as the Chief Executive Officer of the National Health Authority, an Indian governmental organization tasked with managing public health insurance. Previously, He has headed the Telecom Regulatory Authority of India, and the Unique Identification Authority of India. He has served as the Director General in UIDAI (Aadhaar) and was actively involved in leading the ideation, designing, and implementing Aadhaar platform. Previously, he was the Secretary, Department of Electronics, and Information Technology (under Ministry of Communications and Information Technology, Government of India). He has been awarded with Prime Minister's Awards for Excellence in Public Administration in 2008. He earned his PhD from Department of Management studies, IIT Delhi. He has authored various policy documents for the Government of India.