Deep Learning- Based Face Recognition System for Secure Cheque Clearance and Customer Authentication in Banking Application

Bhoomireddy Venkata Haripratapreddy*[1], S.P.Vijayaragavan[1],

[1]Department Of Ece,Bharath Institute of Higher Education and Research, Chennai, India.
bhoomir837@gmail.comcc

Abstract. In modern banking environments, secure and efficient customer authentication is critical to preventing financial fraud and enhancing user experience. Our research outlines a CNN-based model for rainfall prediction and a face recognition system to secure cheque clearance and customer authentication, leveraging a hybrid architecture verifier. The system captures and preprocesses facial images from ATMs, mobile apps, and branch kiosks, generating robust embeddings that are matched against stored profiles using angular margin-based classification. SttleGAN enhances training diversity through synthetic face generation, improving generalization across pose, lighting, and expression variations. ArcFace ensures precise identity verification with synthetic samples—the developed framework authentication precision of 97.2, demonstrating its reliability and scalability for real-world deployment. The framework also incorporates liveness detection and encryption protocols to safeguard biometric data, aligning with regulatory standards. This approach offers a contactless, fraud-resistant solution for next-generation banking security.

Keywords: Deep learning, Face recognition, StyleGAN, Arcface, Biometric authentication, cheque clearance, Banking security, Customer verification, Synthetic face generation.

1. Introduction

The automated cheque verification framework leverages image processing and deep learning techniques. For cheque clearance and financial transactions, the system must be reliable, robust, and time-efficient for cheque clearance through image processing and deep learning approaches. Key components include branch code, cheque number, legal and country amounts, account number, and signature patterns. The innovation aims to benefit the banking system by enhancing efficiency, reducing delays and strengthening security. Reinventing the other competent cheque-based monetary transaction system, which requires automated system intervention [1]. The automatic imagery bank cheque data extraction based on machine learning methods is reviewed in an extensive review. The processing time and operational costs can be minimized through full automation of cheque recognition and verification. Smart cheque processing systems are a developing research frontier across fields including computer vision, image processing, and modern AI approaches and deep learning and the main stages of the image acquisition [2]. To make the cheque truncation mechanism large and efficient, and to reduce the amount of human interaction. The main approach of

© The Author(s) 2026
S. P. Vijayaragavan et al. (eds.), *Proceedings of the Global Conference on Sustainable Energy Systems, Smart Electronics and Intelligent Computing (GCSESEIC 2025)*, Advances in Engineering Research 297,
https://doi.org/10.2991/978-94-6239-654-8_60

high efficiency retrieves an important detail from the check booklet, for instance, the bank check number, precise amount, account number and unique signature patterns. The scale-invariant feature transform stands for SIFT for feature support for classification, resulting in an output percentage in the signature. The innovative approach completely revamps the process of verifying a bank check by leading image processing [3]. Despite rapid progress in digital technology and financial entities, including banks, continue to depend on traditional human-based cheque clearance systems. Cheque clearance remains slow, often taking multiple days for settlements, due to reliance on intermediary verification. This results in significant delays and costs smart platform that retrieves key information from cheques, including payee details, transaction amount, date, and issuing bank, leveraging OCR and neural network techniques and matches cheque signatures to existing records through attributes extraction and dimensionality reduction. For security, fresh signatures are encoded and stored as hashed data [4]. The assessment technique, grounded in embedding comparison, stabilises recognition accuracy, lowering false acceptance rates, especially for criminal activity identification based on unique eye retina features [5]. The facial identification for online transactions represents the effects in the domain of secure and efficient user verification. It innovatively integrates Aadhar data into a comprehensive repository of biometric and demographic information with advanced facial recognition technology. The system achieves real-time face recognition technology and a rapid authentication process. Which is used to robust encryption techniques are implemented to protect sensitive biometric information of data privacy concerns and aligning with stringent data protection laws [6]. The data-driven approaches to next-generation facial identification. Model development relies on large-scale facial imaging collections utilizing PCA, LBP, and CNN methods for feature engineering in training. System performance is assessed on a benchmark dataset, with deployment feasible in operational environments. Evaluation of algorithms across specific datasets highlights the most appropriate method for this application [7].The networks using social media in user verification of user including security, and user verification in a range of applications in facial recognition technology of essential elements in facial recognition technology. The key purpose of this work is to explore the optimal neural network architecture for facial recognition tasks that can provide a prompt result in resource-constrained environments [8]. To enhance bank secure bank locker system enabled through intelligent learning models secured by multi-factor verification. The bank locker is vital for securing client resources. The imaginative approach to improve bank locker security through the integration of an intelligent facial recognition system, a two-factor confirmed framework utilizing the CNN concept. The points to moderate the changes of unauthorized access and false exercise and guarantee strong assurance for the resource. The integration of machine learning acknowledgement with two-factor verification utilizing CNN presents noteworthy value within the domain against unauthorized gaining potential security breaches [9]. The base enhances security with

multi-CNN face recognition verification. Integrating facial verification with an SMS system and IOT (Internet of Things) for accessing bank lockers can bring security and convenience. The banking locker system must be extremely secure to protect customers' items. The traditional access methods sometimes rely on keys and passcodes and which are prone to theft and unauthorized usage. These problems are introducing an enhanced security feature using the banking locker system, which includes sophisticated features such as customer registration and procedures when a customer is captured by facial recognition. The data is also collected, processed and kept in a format that cannot be easily accessible by other people. This involves conducting facial verification using the developed biometric data to select an IoT device integrated with the locker system, which initiates the unlocking process. Then, they enter their mobile number to receive updates through SMS as follows. The customer's registered mobile phone number, which is used with the above request, would yield information relating to the attempted access. The validation stage locker is opened to allow the personal measure of safety to be sensitive, and fundamental measures are applied to prevent hackers from accessing the account in the face recognition system. Whenever they are not supposed to, the security and safety of messages are kept protected and encrypted, and any attempts at verification lead to security alerts [10]. The machine learning based facial recognition and fingerprint secure locker access. The secure locker technology for an advanced secure storage solution designed to safeguard valuable assets and banking institutions. A similar secure facility has used a biometric authentication method, including fingerprint scanning and ML-based facial recognition, to ensure that only authentication users can access the contents of the locker [11].

2. Related Work

Schiller, D et al. [12] developed a novel approach to transfer learning to automatic emotion recognition across various modalities. The proposed model used for implementation in expression classification utilizes modalities. The proposed model used for facial expression recognition that utilizes saliency maps to transfer knowledge from an arbitrary source to a target by mostly hiding relevant information. The proposed method is applicable regardless of the chosen model, with the experience being fully shifted together with data augmentation techniques. Testing demonstrated that the presented approach of the updated model adapted more rapidly to the target domain when constrained to emphazise the inputs that were considered relevant sources. The proposed automated face recognition method uses a Deep CNN employing a transfer learning strategy. Face recognition accuracy was evaluated using two open-source datasets of facial images. Analysis reveals that transfer learning boosts CNN facial recognition effectiveness. AI-Waisy et al. [13] proposed an integrated deep learning system that relies on local features for k-NN-based facial classification. The system integrated local hardcrafted descriptor features alongside DBN models for robust recognition under unconstrained conditions. The core rationale of the approach is that

the curvelet analysis highlights the core facial structure, fractal dimension conveys the surface detail of facial patterns. They suggested a hybrid multimodal approach profound face recognition approach to include a highlight presentation by the proposed MDFR approach with the curvelet fractal approach on the four-face dataset.

3. System Architecture

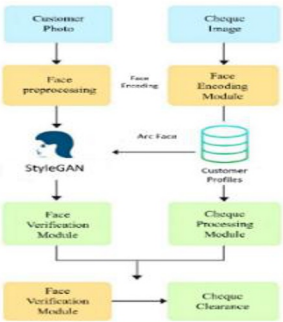

Fig. 1. StyleGAN and Arc Face-based face recognition system

3.1 Data Acquisition

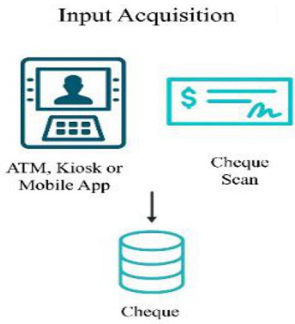

Fig. 2. Input acquisition module for secure cheque clearance

The information acquisition to start the authentication and cheque process, the system acquires two primary input data points Fig. 1. The facial image captures the customer's face in real time using integrated cameras at ATM, mobile banking applications and in-branch kiosks. This image serves as the biometric input data for identity verification. The cheque image scanning data to simultaneously the physical cheque is scanned using high-resolution imaging systems. This enables parallel processing for signature verification, amount extraction, and fraud detection Fig. 2. These input data are synchronized and forwarded to the preprocessing and verification modules to ensure a seamless and secure transaction workflow.

3.2 Data standardization

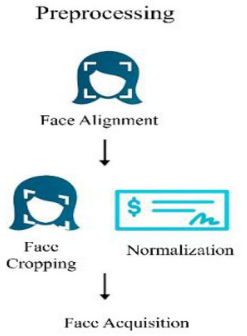

Fig. 3. Preprocessing module for facial image standardization

The data standardization critical phase that ensures facial images are standardized before feature extraction and verification. It enhances model accuracy and robustness by minimizing variations due to pose, lighting, and background noise shown in Fig. 3. The key stages such as face alignment, face cropping and normalization. The face alignment is used to align the facial key points of the eyes, nose and mouth to a canonical pose. The methods used to landmark detection algorithm of MTCNN and Dlib to rotate and scale the face so that key features are consistently positioned. The benefit is to reduce intra-class variability and improve embedding consistency.

The face cropping is used to extract the facial region from the background, and the method used is to draw a bounding box around the face and followed by cropping to a fixed aspect ratio. The benefits are to remove irrelevant background and focus the model on facial features. The normalization is used to standardize pixel intensity and image dimensions. The method used to resize dimensions of 112×112 and 224 ×224 pixels. The normalized pixel values are between 0 and 1, and mean subtraction. The benefit is to ensure a consistent data input format for the neural network and to improve convergence and generalization.

3.3 StyleGAN module

Fig. 4. StyleGAN module architecture

The StyleGAN module acts as a key driver in improving the variability and resilience of the face recognition system through synthetic data augmentation. It generates high-fidelity facial images that mimic real-world variation, thereby improving model generalization and reducing overfitting and synthetic face generation Fig. 4. The main purpose is to supplement limited real-world banking datasets with realistic synthetic faces. The method used by StyleGAN leverages a progressive growing architecture and latent space manipulation to produce photorealistic facial images. The benefits expand to training data across demographics, facial structure and environmental conditions.

3.4 Arc Face discriminator

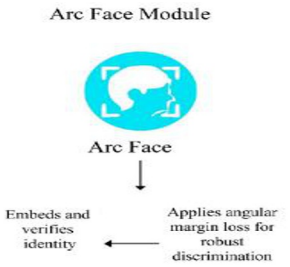

Fig. 5. ArcFace Module

The control over facial attributes of the pose variation to generate faces with different head orientations to simulate ATM and mobile camera angles, Fig. 5. The lighting conditions adjust illumination to reflect indoor, outdoor, and low-light banking environments. The expression diversity introduces subtle changes in facial expression to improve recognition under natural customer behaviour. The integration with ArcFace to the synthetic face is encoded and verified using ArcFace, and to ensure that the augmented data contributes meaningfully to identity discrimination

3.5 Verification and clearance

The final stage of the system involves decision-making based on the outcome of facial verification Fig. 6. This module ensures that cheque clearance is authorized only when the customer's identity is successfully validated. The face verification process of ArcFace generated embedding of the live facial image is compared against stored customer profile embeddings. The thresholding indicates that a cosine similarity score is computed. When the score surpasses the set threshold and the person is confirmed verified. The security check indicates an optional liveness detection, and anomaly filters are applied to prevent spoofing and replay attacks. The cheque clearance authorization triggers upon successful face match, and the system signals the cheque processing module to proceed. The integration of the verified identity is linked to the scanned cheque for signature matching, fraud detection and transaction logging. The outcome of the cheque is cleared, and the transaction is securely recorded.

Fig. 6. verification and clearance module for secure cheque processing

4. Experimental setup

The section shows Fig. 7, the data source, training configuration, evaluation metrics and hardware specifications used to validate the proposed deep learning-based face recognition system for secure cheque clearance. The dataset in real banking and Synthetic faces via StyleGAN. The real banking images indicate collected data from authorized banking environments, such as ATM captures and mobile application submissions with proper consent and anonymization. The synthetic face vis StyleGAN indicates an augmented dataset using StyleGAN-generated images to simulate diverse conditions of pose, lighting, expression, and demographic variation. The main use shows that it combines real and synthetic data to improve model generalization and reduce bias.

Fig. 7. Evaluation of the proposal face recognition system

4.1 Training configuration

The training configuration is designed to optimize convergence, generalization and computational efficiency for the proposed deep learning based face recognition system. Each parameter is carefully selected to balance performance and resource utilization. The batch size of 64 images is used to control how many samples are processed before updating model weights. The rationale indicates that a batch size of 64 offers a good

trade-off between GPU memory usage and gradient stability Fig. 8. The limitation enables efficient parallel processing and smoother convergence during training.

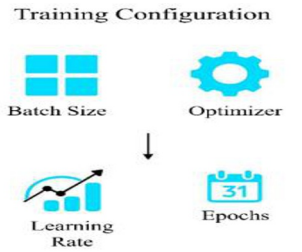

Fig. 8. Training configuration for the proposed face recognition system

The Adam-type adaptive Movement Estimation optimizer. The parameters indicate that a β1= 0.9 shows control of the attenuation factor for the average value approximation of the mean of gradients. B2 = 0.999 shows a control of decay rate for the second moment estimate of variance of gradients. The advanced age combines the benefits of RMS Prop and momentum to make it well-suited for non-stationary objectives and sparse gradients. The learning rate of 0.001 with step decay initial value shows that the set of 0.001 is for stable gradient descent. The decay strategy shows a reduced factor of 0.1 every 10 epochs to find-tune learning as training progresses. The benefits are used to prevent overshooting minima and improve final convergence. The 50 epochs with early stopping of total epochs indicates a model trained over 50 full passes through the data. The early stopping indicates a monitor's validation loss and halts training if no improvements are observed over a predefined patience window.

4.2 Performance measures

To evaluate the validity and soundness of the proposed face recognition system for secure cheque clearance for four key biometric evaluation metrics are used. These metrics quantify both the accuracy and the error tendencies of the system under real-world banking conditions. The accuracy of the proportion of correctly verified identities out of all verification attempts.

$$\text{Accuracy}=\frac{True\ positives+True\ negatives}{Total\ attempts} \qquad (1)$$

The above Equation (1) shows that the main purpose that provide a general measure of the system effectiveness across all cases. The impacts of the misleading in the imbalanced dataset of error-specific metrics are also used.

$$\text{FAR}=\frac{False\ positives}{False\ positive+True\ negatives} \qquad (2)$$

The above Equation (2) shows that the unauthorized access rate expresses the likelihood that the system misidentifies and accepts an unauthorized user. The limitation shows

that high poses a security risk in banking, potentially allowing fraudulent cheque clearance.

$$\text{FRR}=\frac{False\ negatives}{False\ negatives+True\ positives} \quad (3)$$

The above Equation (3) shows that the Erroneous rejection rate of the chance that the system wrongly denies access to an authorized user. The impact of high FRR affects user experience, causing inconvenience to genuine customers.

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

The above Equation (4) shows that the accuracy measure of the proportion of correct predictions of both true positives and true negatives. The genuine users correctly accepted TP, impostors correctly rejected TN, impostors incorrectly accepted FP, and Genuine users rejected FN .

$$\text{FAR}=\frac{FP}{FP+TN} \quad (5)$$

Equation (5) shows that the misidentification acceptance ratio probability that the system incorrectly recognizes an unauthorized person as valid. The implication of lower FAR is essential for fraud prevention in cheque clearance.

$$\text{FRR}=\frac{FN}{FN+TP} \quad (6)$$

The above Equation (6) shows the Incorrect rejection rate probability that the system incorrectly rejects an authorized identity. The implication of lower FRR improves customer experience and reduces transaction delays.

$$\text{EER}=\text{FAR}(\tau) = \text{FRR}\ (\tau) \quad (7)$$

The above Equation (7) shows that the error parity point of the measure is where false match and false non-match rates are equal. The computation is determined by plotting FAR and FRR against varying decision thresholds and identifying the intersection points.

4.3 Hardware specification

The below Fig. 9 represents a GPU that shows an NVIDIA RTX 3090 with 24 GB VRAM. The main role of acceptance in Deep learning computations of especially convolutional and matrix operations, in StyleGAN and Arc Face modules. The advanced technology of large VRAM enables training with high-resolution facial images and larger batch sizes without memory bottlenecks. The performance indicates

support for parallel processing of multiple facial embeddings to reduce training time and improve inference throughput. The CPU Intel Core i9 with 64 GB RAM indicates a role in managing data preprocessing of input and output data operation and orchestration of GPU tasks. The inference latency of 0.42 seconds per transaction indicates the time taken from facial image input to check the clearance decision.

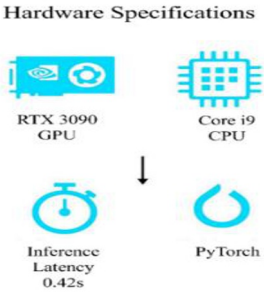

Fig. 9. Hardware Specification Architecture

5. Result and Discussion

The proposed biometric face recognition system demonstrates strong performance across multiple evaluation dimensions, validating its suitability for secure cheque clearance in banking environments Fig. 10. The accuracy score of 97.2 % in the system correctly verified identities of test cases, indicating high reliability and generalization across real and synthetic data. The confusion matrix shows a highlight of low false acceptance and rejection rates, and confirms balanced classification. The ROC curve illustrates a sharp increase in genuine recognition rate with low false errors, yielding an AUC close. The outperformance traditional CNN and VGG-based face recognition model by 3 to 5 % of accuracy in EER. The StyleGAN augmentation and Arc Face embedding contribute significantly to these improvements. The robustness to occlusion, Ageing and lighting maintains greater than 94% of accuracy under partial face occlusion of masks and glasses. It shows a minimal degradation in recognition across age-progressed images and varied lighting conditions.

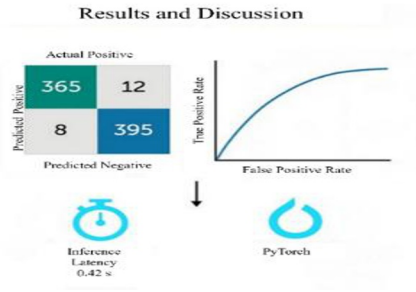

Fig. 10. biometric banking

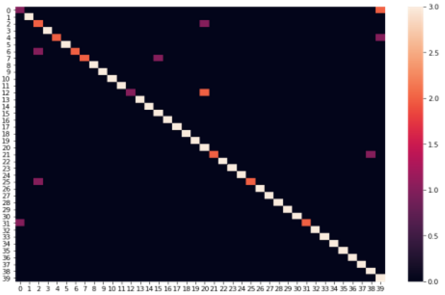

Fig. 11. Confusion matrix

The above Fig. 11 represents a diagonal dominance of the bright diagonal line from top-left to bottom-right, indicating strong self similarity of each identity is most similar to itself. This is expected in a well-trained face recognition system and confirming high true positive rates. The off-diagonal elements of scattered lighter cells off the diagonal suggest false positives and inter-class similarities. These may arise due to the similarity facial arise due to the similar facial features across subjects, synthetic data overlap and ageing of occlusion effects. The matrix size indicates an evaluation across 39 unique identities, of each cell represents a similar score between identity I and identity j. The values closer to 3.0 of light peach imply high similarity. The values near 0.0 of dark purple indicate low similarity and correct rejection.

Fig. 12. secure login confirmation interface dashboard

The above Fig. 12 represents a Face Secure bank login confirmation of user authentication. The system confirms that user DINESH T has successfully logged in using face recognition, indicating biometric verification was completed. The interface design of a dark, dark-themed dashboard with a central welcome message. The green notification bar at the top-right confirms login success. The functionality prompt indicates a user has been invited to manage transactions securely using face authentication, emphasizing the system's focus on biometric security and fraud prevention. The branding indicates a footer including 2023 FaceSecure bank, reinforcing instructions, identity and trust.

Fig. 13. Secure transaction interface

The face secure transaction panel indicates the user identity, which shows in Fig. 13 that a logged-in user JONES T is prompted to initiate a transaction. The transaction field includes input data for amount and account number, ensuring a structured financial entry. The facial verification indicates that a live webcam feed displays the user's face with a green bounding box and chin alignment line. The button-like start camera and verify face match trigger liveness detection and identity confirmation. The navigation and branding indicate the top navigation links, and the footer reinforces usability and institutional trust.

The below Fig. 14 represents a Face secure bank of biometric transaction interface showing that the interface exemplifies a secure user user-friendly banking platform that integrates facial recognition for transaction authentication. The design is to ensure that a verified user can initiate and complete financial operations. The user identity and welcome prompt show a system that greets the user DINESH with a personalized welcome message and a waving hand emoji, reinforcing trust and engagement. The prompt encourages the user to select a photo to begin secure transaction management, indicating that facial data will be used for verification. The transaction form contains a field for name, amount, cheque number and a choice of photo. The biometric verification workflow shows start camera, submit transaction and green notification bar. The security features show face Match verification and liveness detection.

Fig. 14. Face Secure bank transaction interface output

The below Fig. 15 represents a user identity of interface welcome DINESH T, confirming that the user is authenticated via facial recognition and has access to transaction records. Transaction details such as transaction ID, name, data and time, status, amount, and check reference. The navigation of the top navigation includes

dashboard, transaction, history, chat and logout, enabling seamless access to banking features. The dark-themed UI enhanced readability and modern aesthetics. The security integration of this panel confirms that biometric authentication governs access to sensitive financial data, ensuring that only verified users can view and manage transaction history.

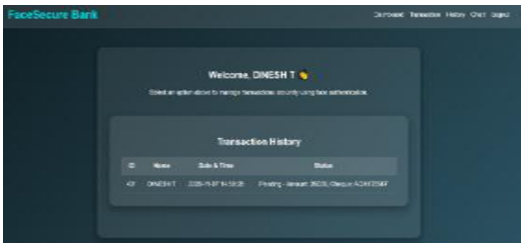

Fig. 15. Transaction history interface

The below Fig. 16 shows that the user identity system welcomes DINESH T, confirming secure login via facial recognition. The transaction analytics of the bar chart transaction per date compares transaction volume across two dates. The 2023-10-16 lower transaction count and the 2023-10-17 significantly higher transaction activity. This visualization helps users track financial behavior and detect anomalies. The navigation and usability of dark-themed UI enhanced readability and modern design appeal.

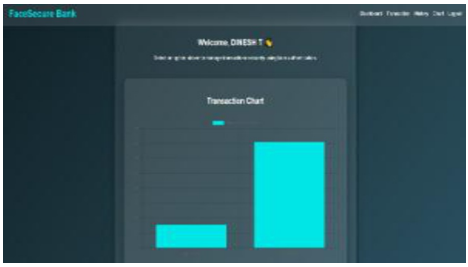

Fig. 16. Transaction chart interface

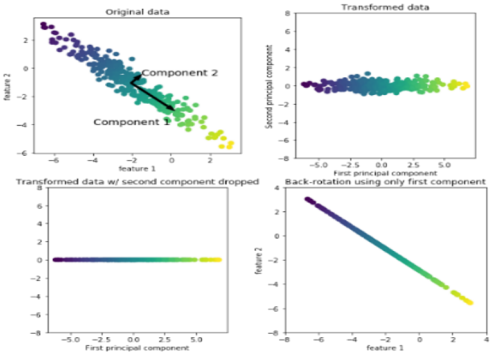

Fig. 17. PCA analysis

The above Fig. 17 represents PCA of the top-left original data, of raw data points are scattered diagonally across the feature space. The arrow shows that component 1 aligns with the direction of the maximum variable. Component 2 represents orthogonal component 1. The uses identify the directions of principal components that capture the most information. The top-right transformed data is rotated so that the axes now align with the principal components. The axes show PC1 captures the most variable, and PC2 captures the remaining variables orthogonal to PC1.

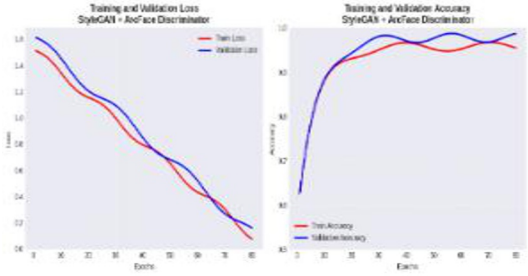

Fig. 18. StyleGAN and Arc Face discriminator model

The above Fig. 18 represents the training performance analysis of epochs 0 to 80 and loss values 0.0 to 1.6. It shows a consistent download trend, indicating that the model is demonstrating successful knowledge acquisition from the training set. The blue line shows a decrease with slight fluctuations, suggesting good generalization with minimal overfitting. The interpretation convergence of both loss curves implies stable training data and effective regularization.

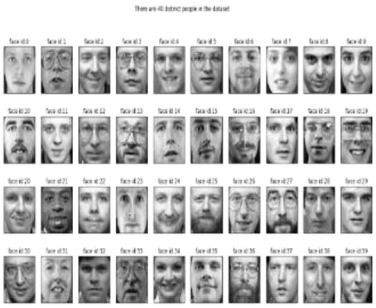

Fig. 19. facial dataset

Fig. 19 represents the structure grid format images are arranged in a grid structure and making it easy to visually compare facial features across subjects. The face ID of each image is tagged with a unique identifier, which is essential for supervised learning tasks like classification. The variability of data includes diverse facial attributes of facial hair of some subjects who have beards and moustaches. The eyewear presents of glass introduces occlusion, and the light condition of difference in illumination simulates real-world variability.

6. Conclusion

This study presents a robust and secure biometric authentication framework for banking applications, leveraging StyleGAN-based data augmentation and Arc Face discriminative embeddings. The system achieves a high accuracy of 97.2% validated through confusion matrix analysis of the ROC curve and comparative benchmarking against baseline. The high accuracy and low error rates of demonstrated through extensive evaluation metrics including FAR, FRR and EER.The real-time performance achieved with an average inference latency of 0.42 seconds ensures a seamless user experience. The security assurance integrates liveness detection and a spoof prevention mechanism to safeguard against fraudulent access. The robustness to variability maintains performance under occlusion ageing, and lighting changes, of critical for real-world deployments. The scalability is implemented using Py-Torch with CUDA acceleration on high-performance hardware supporting future expansion.

Reference

1. Agrawal, P., Chaudhary, D., Madaan, V. et al. Automated bank cheque verification using image processing and deep learning methods. Multimed Tools Appl 80, 5319–5350 https://doi.org/10.1007/s11042-020-09818-1(2021).
2. Thakur, N., Ghai, D. & Kumar, S. Automatic imagery Bank Cheque data extraction based on machine learning approaches: a comprehensive

survey. Multimed Tools Appl 82, 30543–30598 https://doi.org/10.1007/s11042-023-14534-7(2023).

3. Y. K. Singh, R. Jaiswal, P. Choudhary and B. Chugh, "Verifying bank checks using deep learning and image processing," 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024, pp. 1-6, doi: 10.1109/ISCS61804.2024.10581393.(2024)
4. M. Jha, M. Kabra, S. Jobanputra and R. Sawant, "Automation of Cheque Transaction using Deep Learning and Optical Character Recognition," 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, pp. 309-312, doi: 10.1109/ICSSIT46314.2019.8987925, 2019.
5. X. Pan, ``Research and implementation of an access control system based on RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan., pp. 716-719, doi: 10.1109/ISdea.. 2012.400.2012.
6. Gill, D. Jain, J. Sharma, A. Kumar and P. Garg, "Deep Learning Approach for Facial Identification for Online Transactions," 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP), Sonipat, India, pp. 715-722, doi: 10.1109/INNOCOMP63224.2024.00123, 2024.
7. S, A. Kareem and V. Kumara, "Machine Learning Approach for a Novel Facial Recognition System," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 1178-1183, doi: 10.1109/ICCES57224.2023.10192743, 2023.
8. M. A. Munim and M. S. Rahman Kohinoor, "Performance Evaluation of Deep Learning-Based Facial Recognition Models on Mobile Computing Environments," 2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC), Rajkot, India, 2023, pp. 13-18, doi: 10.1109/R10-HTC57504.2023.10461876.(2023)
9. R. Bhardwaj, "Enhancing Bank Locker Security: Machine Learning-Based Facial Recognition with Two-Factor Authentication," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, pp. 1-5, doi: 10.1109/ICSES60034.2023.10465388, 2023.
10. S. Geetha, S. Nivetha, S. Preethi, R. Priyanka and V. Priyanka, "IoT-Based-Enhancing Banking Security with Multi-CNN Face Recognition and SMS Verification," 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, pp. 135-140, doi: 10.1109/ICICAT62666.2024.10923004, 2024.
11. J. Baikerikar, K. Patil, A. Jadhav, A. A. D'Souza, V. Sekar and S. Naik, "Machine Learning based Facial Recognition and Finger Print

Identification for Secure Locker Access," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, pp. 1-7, doi: 10.1109/I2CT61223.2024.10544254, 2024.

12. AbdELminaam, D. S., Almansori, A. M., Taha, M., & Badr, E. (2020). A deep facial recognition system using computational intelligence algorithms. PLoS ONE, 15(12), e0242269. https://doi.org/10.1371/journal.pone.0242269(2020).
13. Alay, N., & Al-Baity, H. H. Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. Sensors (Basel, Switzerland), 20(19), 5523. https://doi.org/10.3390/s20195523. (2020).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.