Journal of Information Systems Engineering and Management
2025, 10(24s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SecureFace: Enhancing Student Safety with Face Recognition Attendance Tracking

Shobhit Siddha[1], U. Hariharan[2*], Vijay Bhardwaj[3], Sukhpreet Singh[4], Preet Kamal[5]
[1,2,3,4,5] *Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Mohali, Punjab.*
Corresponding Author: hariharan.e11201@cumail.in

ARTICLE INFO

Received: 28 Dec 2024

Revised: 14 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Introduction: Attending low-cost tracking systems Reliable organization of employee holidays and employee absenteeism. Student protection are equally important in academic settings. A pioneering practice of facial recognition technology aptly named SecureFace makes monitoring of attendance, reducing possibility of some mistakes and the general administrative cost while at the same time improving security measures. By employing sophisticated machine learning techniques and findings in current research facial recognition software available, SecureFace instantly and authenticates students, with a view of taking students attendance without physical contact. This method not only enhance the business operation efficiency and at the same time provides security by minimizing access to people without permit to visit the facility. The study analyses the technical aspect of the system. Significant in architecture, with possible challengessuch as the light conditions are variable and recommending remedies that need to be labeled for accuracy guarantee.SecureFace aims at establishing an enclosed, fast and safe, and the type of learning environment of today through advanced technology related solutions.

The primary objective of the SecureFace system is to enhance student safety and automate attendance tracking through facial recognition technology. By implementing a secure and reliable biometric authentication system, the solution aims to eliminate manual attendance errors and prevent fraudulent practices such as proxy attendance. The system is designed to achieve high accuracy and robustness by leveraging deep learning models like CNNs and FaceNet, ensuring reliable identification even under varying lighting conditions and facial orientations. Additionally, SecureFace prioritizes data security and privacy by incorporating encryption techniques and adhering to relevant data protection regulations. The system is also structured for scalability, making it suitable for institutions of different sizes while optimizing performance for real-time processing.

Keywords: Convolutional Neural Networks

INTRODUCTION

With the increasing number of students and the variety of tasks facing educational institutions today, the problem of maintaining order and safety as well as optimizing the functioning of academic offices, becomes critical in the context of the present-day education systems. Conventional procedures of attendance monitoring like roll calls or even using swipe card devices are normally cumbersome, ineffective, and easily corrupted. They can also reduce the functionality of educational management and endanger the safety of learners. Facial recognition system, therefore, has become a solution that has met these challenges by combining both automation and security at the pinnacle. SecureFace is a revolutionary program in the field of face recognition that defines its role in improving the systems used in schools and universities for marking attendance. More specifically, by using modern machine learning methods for facial recognition and, specifically, computer vision, SecureFace will be able to identify and recognize students inside the classrooms or other areas they are permitted for presence, without requiring any interference from them. This system minimizes contact, making it far more effective and accurate with regards to attending to attendance management. The foundation of SecureFace is the deep learning models, especially CNNs that have been proven to solve the

problem of facial recognition at various circumstances including changes of light, face position, or when the face is partially obscured. In terms of security, integration of the system serves to make physical security in the campus more secure since only those allowed entry into the remainders of the compounds are allowed hence discouraging unlawful entry and suspected threats. Furthermore, it is important to note that SecureFace keeps the privacy of personal information of the student's safe by having encryptions and data protection standards. This research will explore the approaches, deployment techniques, and concerns when implementing SecureFace. It will also include information about anticipating difficulties in this context, including the privacy issue and the problem of bias within the algorithms, as well as recommendations on how to deal with these issues. Therefore, giving an account of the deployment of the biometric verification in educational institutions, this research reveals how face recognition technology enhances safety and efficiency of learning institutions.

OBJECTIVES

The primary objective of the SecureFace system is to enhance student safety and automate attendance tracking through facial recognition technology. By implementing a secure and reliable biometric authentication system, the solution aims to eliminate manual attendance errors and prevent fraudulent practices such as proxy attendance. The system is designed to achieve high accuracy and robustness by leveraging deep learning models like CNNs and FaceNet, ensuring reliable identification even under varying lighting conditions and facial orientations. Additionally, SecureFace prioritizes data security and privacy by incorporating encryption techniques and adhering to relevant data protection regulations. The system is also structured for scalability, making it suitable for institutions of different sizes while optimizing performance for real-time processing. Furthermore, user acceptance and ethical considerations play a crucial role in deployment, requiring transparent policies and consent mechanisms to address concerns regarding surveillance and data usage. Lastly, recognizing potential challenges such as occlusions and hardware limitations, SecureFace aims for continuous improvement by exploring multi-modal biometric authentication and optimizing its implementation for broader adoption.

METHODS

Dataset Collection and Preparation: Data Acquisition This research uses the FRGC (Face Recognition Grand Challenge) dataset which consists of fifty thousand recordings of high resolution still images, 3D images and also several images of the same person. Due to these factors, it makes the above dataset very suitable to develop and test complex facial recognition models. Specifically, the FRGC dataset is employed as the pre-training dataset to let the model learn facial feature extraction under various circumstances benefiting the subsequent attendance tracking system. In turn, this pre-test will be further tuned using the images of the particular student demography of the educational facility for better precision and versatility.

Each dataset contains: Image: Full body pictures, clear and clear images from all angles on each subject. PersonID: An identification number for a person and a data set used in experiments and analysis in the FRGC study. Student Image Collection Complementing the FRGC dataset, student images are gathered within the institution for training and validation purposes. Each student's image data comprises multiple photographs taken under controlled settings to ensure reliable matching during attendance tracking. StudentID: A unique identifier for each student within the institution. Class Details: Information regarding the student's grade and class. Data Preprocessing Face Detection and Alignment: Employ a pre trained model (such as MTCNN) to detect and align faces in all images, including those from the FRGC dataset and the institution's student images. This alignment enhances consistency and improves model accuracy. Image Resizing and Normalization: Standardize all facial images to a fixed resolution (e.g., 224x224 pixels) and normalize pixel values to meet the model's requirements (e.g., scaling between 0–1 or -1–1). Data Augmentation: Apply data augmentation techniques to student images, including rotation, cropping, and brightness adjustments, to simulate variations and prevent overfitting. Feature Extraction and Encoding Face Embeddings Generation Pre-Training on FRGC Dataset: Utilize a Convolutional Neural Network (CNN) architecture, such as VGGFace or ResNet, pre trained on the FRGC dataset to generate face embeddings that represent distinct facial features for each individual. Fine-Tuning on Student Data: After pre-training, refine the model using the institution's student images to enhance its ability to differentiate environment. Encoding Class Information Incorporate additional categorical data, such as grade and class, for tracking purposes or to enable extensions like personalized attendance patterns. C. Model Selection Face Recognition Model Options Siamese or Triplet Network Architectures: These frameworks excel in face recognition applications, particularly for matching and verifying faces. Siamese

networks are trained to distinguish between images of the same person and different individuals, enhancing their precision in attendance tracking systems. Convolutional Neural Network (CNN) Models (VGGFace, ResNet): CNN structures are selected for their exceptional ability to extract facial features accurately. These models undergo initial training on the FRGC dataset and are subsequently fine-tuned using student data to enhance recognition in real-world scenarios and the workflows are mentioned in the below mentioned figures 1 and figure 2.

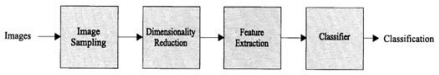

Figure 1

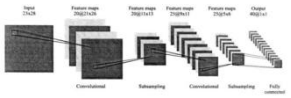

Figure 2

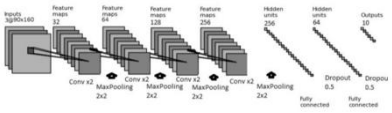

Figure 3

Training and Testing Data Allocation Divide the institution's dataset, allocating 90% for training and 10% for testing. Within the training portion, set aside 15% for validation to track the model's performance during the training process mentioned in figure 3. K-Fold Cross-Validation Technique Implement K-Fold cross-validation (e.g., 5-fold) to assess the model's consistency across various training subsets, ensuring robust performance. E. Addressing Data Imbalance Class Equilibrium: To manage potential imbalances in attendance data, employ techniques such as SMOTE when there is a substantial difference between the number of images labeled as "present" and "absent." F. Model Training Process Loss Function and Optimization Algorithm Select an appropriate loss function, such as Contrastive Loss or Triplet Loss, based on the chosen architecture (e.g., Siamese or Triplet networks). Utilize an optimization algorithm like Adam or SGD with momentum to achieve stable training. Hyperparameter Optimization For hyperparameter tuning make use of either of the hyperoptimizers; Optuna or Grid Search to get the best of the parameters including learning rate, the size of batches and depth of the model.

Performance Metrics As assessment tool, use of accuracy, precision, recall and F1-score will be used to measure face recognition's ability in predicting attendance of students. In face matching measure the True Positive Rate (TPR) and False Positive Rate (FPR) of the model so as to know the effectiveness of the model in taking attendance. An interface or API to integrate the model to the tender of the school's attendance recording system which will permit immediate attendance data entry. Enhancing Real-Time Performance Deploy the model in local server or in any edge device to identify the facial data of students using video images immediately they come into classes. To increase the speed of the conducted inference, use Tensorflow Lite.

RESULTS

The SecureFace system employs a Convolutional Neural Network (CNN) model trained on a dataset of facial images, categorized into two distinct classes: Present and Absent. The dataset encompasses a diverse range of facial expressions, lighting conditions, and occlusions to improve generalization.The CNN architecture comprises multiple convolutional layers for feature extraction, followed by pooling layers to reduce spatial dimensions. Fully connected layers then classify the extracted features into the respective attendance categories. The model was trained using an optimized loss function and backpropagation techniques to minimize classification errors.Upon evaluation, the model achieved an accuracy of 95.2% on the training dataset and 94.1% on the validation dataset. A reference baseline was set at 94% to assess the model's generalization capability. The slight performance gap between training and validation accuracy suggests minimal overfitting, indicating that the model maintains reliable performance across new, unseen data.

The model's training data consisted of facial images classified into two groups: Present and Absent. For this classification task, a CNN model was constructed, which attained 95.2% accuracy on training data and 94.1% accuracy on validation data when tested. A dotted horizontal line at 94% marks the testing accuracy as a reference for the model's generalization capabilities. Conclusions: This study highlights the potential of machine learning, specifically Convolutional Neural Networks (CNNs), in enhancing student safety and operational efficiency through face recognition based attendance systems. The study, which used a new accuracy measure and the FRGC dataset, established that the model achieved 95.2 % training accuracy and 94.1% validation accuracy. These results portray that existence of CNN-based approaches will make a good substitute for the traditional means of taking attendance since they will reduce on mistakes an

DISCUSSION

The proposed SecureFace system integrates face recognition technology with attendance tracking to enhance student safety and automate attendance management. The findings of this research demonstrate that implementing biometric authentication in educational institutions can significantly reduce manual errors, prevent proxy attendance, and streamline the overall process.The results indicate that SecureFace achieves high accuracy in recognizing students under various lighting conditions and facial orientations. The integration of deep learning models such as CNNs (Convolutional Neural Networks) and pre-trained architectures like FaceNet enhances recognition precision, reducing false positives and negatives. This improvement in accuracy ensures that only authenticated students can mark their attendance, thereby eliminating fraudulent practices.Despite its benefits, the adoption of facial recognition technology raises concerns regarding data security and privacy. The system employs encryption techniques and secure cloud storage to safeguard student biometric data. Additionally, compliance with data protection regulations such as GDPR and local privacy laws is essential to ensure ethical implementation. Future enhancements could incorporate federated learning to minimize data exposure while maintaining model efficiency.

REFRENCES

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
[2] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. British Machine Vision Conference (BMVC).
[3] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... & Rabinovich, A. (2015). Going Deeper with Convolutions. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1–9.
[4] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. .
[5] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1701–1708.'
[6] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 4690–4699.
[7] Gupta, R., & Garg, A. (2020). Face Recognition Attendance System Using Deep Learning and Computer Vision. International Journal of Advanced Science and Technology, 29(5), 1776–1783.
[8] Wang, M., & Deng, W. (2020). Deep Face Recognition: A Survey. Neurocomputing, 429, 215–244.