CNN-Based Cloud System for Student Identification from Incomplete Registration Records

Alyaa Jaber Jalil and Maytham Alabbas*

Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

***Corresponding author E-mail:** ma@uobasrah.edu.iq

https://doi.org/10.29072/basjs.20260111

ARTICLE INFO

Received: 08 October 2025

Accepted: 12 March 2026

Published: 30 March 2026

Keywords:

Cloud Computing,
Deep Learning,
Convolution Neural Networks,
Facial Recognition,
Student Identification.

ABSTRACT

Universities need a decent student identification system to avoid unauthorized attendance. Nonetheless, missing information in registration records creates serious challenges for current recognition schemes. We created a cloud-based facial recognition system using ResNet-based convolutional neural networks to recognize students' faces from video-based images with incomplete enrollment data. The system utilized 270 images taken from nine students under different conditions; using these images, a result of 97% accuracy was achieved at a similarity of 75% to 100%. The approach utilizes notifications when unauthorized access is detected and uses cloud infrastructure for deployment. These results show that identification in these situations can be done using deep-learning models. This can prove fruitful in campus security and other registration management services.

1. Introduction

The use of a cloud-based application has increased since it provides a vast amount of computing power to process and store a lot of data. The blending of cloud computing with AI and computer vision has boosted monitoring systems' performance, facilitated the processing of data promptly while saving storage [1]. Facial recognition systems that rely on biometric approaches are gaining interest in educational institutions for student identification and access control, particularly with high-quality digital cameras now standard on campus [2,3].

However, the most significant issue is that the vast majority of student recognition systems operate on the basis of full and correct registration databases. Colleges and universities also

face challenges with incomplete registration data as a result of late enrolment, misadministration, transfer students, or database mismanagement. Accordingly, conventional methods such as manual attendance-taking, RFID-based systems, or basic biometric scanners malfunction due to incomplete or outdated records, which may lead to unauthorized access or identification errors and escalate administrative overheads [4–6].

In recent years, student identification methods have been grouped into three categories. The first is an attendance system that manually verifies students through their photo IDs and staff visual inspection. This process is time-consuming and prone to error. The second is an RFID or card-based system. This can be easily fooled by cards being shared or stolen. The third is a basic facial recognition system that needs complete databases for enrollment. This fails if the registration data is incomplete [3]. Educational environments with incomplete registration data have not yet seen the application of cloud-based CNN architectures with proven effectiveness, like Residual Network (ResNet), which has demonstrated high accuracy for general face recognition. To our knowledge, no existing work has studied the stability of deep learning systems under non-ideal scenarios where enrollment records are incomplete or where image quality varies dramatically throughout the database.

The existing literature on managing situations of incomplete registration at schools, colleges, and universities is quite scarce. This study tries to fill this gap by developing a cloud-based CNN system to manage incomplete registration. This research was motivated by the observation of issues at the University of Basrah, where the incomplete recording of students has led to students attending classes illegally, the administration mixing up students' exams, and more issues concerning the security of the university. The cloud-based solution is especially well-suited because it provides scalability for growing student populations, allows real-time updates across many campuses, and easily integrates with existing university information systems.

The specific objectives of this research are as follows.

1. Design a cloud system for a facial recognition system with the help of a CNN architecture. Moreover, the registration database is incomplete, but the system should maintain high accuracy.
2. Assess the performance of the system at different image quality and similarity levels (75%–100%).
3. Carry out and verify the functionality of the system in a real university setting.
4. Examine how well the system works to stop unauthorized students from entering academic facilities.

This work presents three major contributions. Firstly, we tackle the issue of incomplete registration data, unlike the past work that assumes complete databases. Secondly, we evaluate the performance of the proposed system for a diverse range of image qualities, which include those arising from campus surveillance datasets. Thirdly, we present an easy-to-use cloud-based implementation of our system, which we tested at an educational institution with a high user satisfaction rate (97% accuracy) using an incomplete registration setup.

The organization of the rest of the present paper is as follows. The second section will review work related to facial recognition systems and cloud-based applications. Section 3 explains the proposed method, system architecture, and the CNN implementation. The experimental results and evaluation are in Section 4. Section 5 highlights the implications and limitations, while Section 6 provides a conclusion and suggestions for future research.

2. Related Work

The cloud system enables the processing and analysis of massive data, which helps in monitoring and detection in multiple sectors, including healthcare, finance, and agriculture. These systems enhance decision-making by automating complex processes and improving operational efficiency.

As it is important to maintain records of births and deaths, national identity databases, and so on, most government services require identification systems. In countries with high populations, it is difficult to maintain such records. Nonetheless, the rise of cloud computing and e-authentication technology has greatly improved efficiency and reduced administrative logjams. Face recognition systems achieve very good system accuracy of 99.9% and 88.13% on the Labeled Faces in the Wild (LFW) and Face Recognition Grand Challenge (FRGC) datasets, respectively [4].

In recent years, metric learning-based approaches, such as FaceNet and ArcFace, have significantly advanced deep face recognition. FaceNet has developed an embedding-based framework that makes use of triplet loss to map images of faces into a discriminative feature space. The use of triplet loss in this design has helped this model to achieve state-of-the-art results on large-scale benchmarks. ArcFace improved recognition performance further by adding an angular margin loss that enforces greater intra-class compactness and inter-class separability. These techniques became primary elements of contemporary face recognition systems and are generally adopted in high-accuracy identification and verification applications [5][6].

Surveillance systems represent another major domain outside of government for which cloud-based identification is vital. Intelligent face recognition systems utilize surveillance camera images, which are transmitted to the cloud to train models that can be used for identification [5]. These systems ensure that the proper individuals are differentiated from those who might tinker [6]. Technologies of such nature allow employers in workplace scenarios to check employees' attendance through smart gadgets without being physically present. Generally, these systems use convolutional neural networks (CNNs) and large databases of registered persons [7][8].

A surveillance system is an important instrument for preserving culture and managing tourism. Organized entry systems are necessary for many archaeological and tourist sites to register the time and date of visits along with visitors' information [9]. Systems intended for security purposes basically focus on regulating access within the systems, preventing theft (property), or preventing system misuse [10].

Technologies for identification based on clouds have also been found capable of addressing public health and agricultural issues [11]. As an illustration, cloud-based surveillance systems have been leveraged to identify infections and track individuals infected with viruses during public health emergencies—or those sought by authorities—by raising alarms so security personnel can obstruct entry when necessary [12]. In the domain of agriculture, methods associated with the cloud allow farmers to protect crops from pests that may lead to major crop losses. Also, voice-based recognition systems have been developed with accuracy rates ranging from 65% to 95% [13].

It is not only related to pest management but also to managing almost everything in farming. Cloud technologies allow for the effective monitoring and management of agricultural tractors and irrigation systems to improve productivity. These technologies also allow early detection of possible issues through continuous data analysis [14].

As one of the most important fields, healthcare is among the many applications of cloud-based voice recognition [15]. Patients who have serious diseases, such as epilepsy, heart attacks, stroke, hypertension, and diabetes, need to be monitored continuously. Voice-activated systems can be used to detect changes in a patient's speech patterns that allow quick intervention and the provision of first aid and treatment [16][17].

In this study, we use deep learning to build a system that prevents uninvited students from entering restricted areas of an educational institute. In particular, the facial recognition system

locks attackers out by identifying their facial images. Although similar technologies can be implemented in various organizations using different biometric modalities, the present work is aimed at the verification and identification of students using facial recognition only.

3. Methodology

A four-stage approach was developed to identify unauthorized students attending classes using cloud computing. Stage I involves photographing registered students and creating their database. Stage II involves identifying students and storing their information in the cloud. Stage III matches the identified student with the database and generates the report. Stage IV manages the alerts. It identifies banned students and sends them emails with complete details. The overall methodology of this work is shown in **Figure 1**.

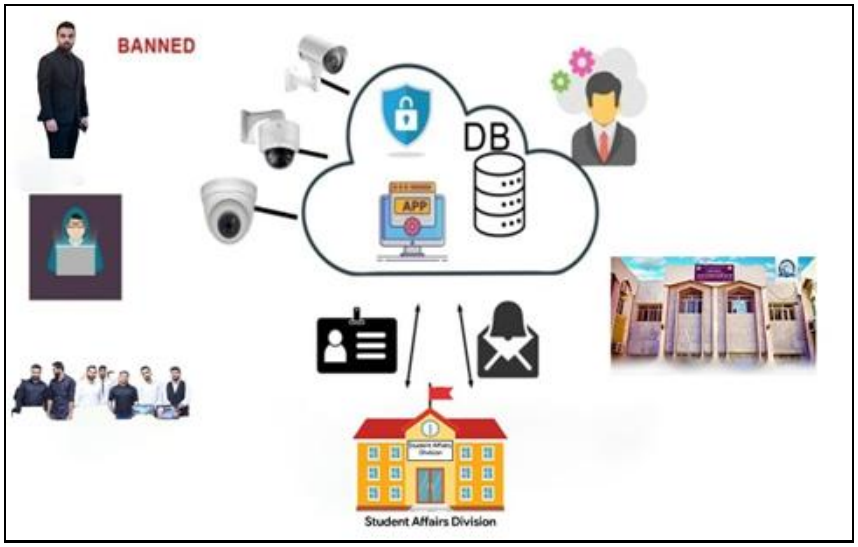

Figure 1. The general diagram of the current methodology.

Stage I: Database construction

The recognition system demands data preparation. For this work (see **Figures 2** and **3**), student videos were recorded, and images were extracted from them for training and verification purposes. This technique makes use of the huge number of frames present in a video, making it efficient and less time-consuming when compared to previous studies, which used to capture thousands of images per person [18]. The steps to create the database are shown in **Figure 4**.

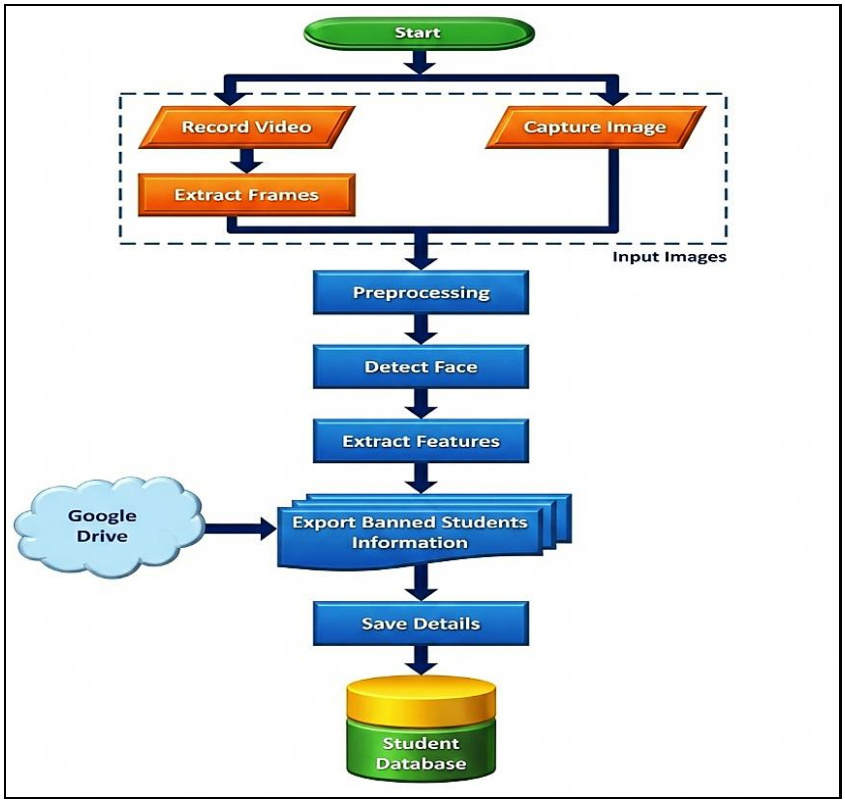

Figure 2: Students' database construction.

Figure 3: The Proposed monitoring system.

Recognition systems depend on feature extraction to differentiate individuals. Deep learning techniques can effectively learn and identify hidden patterns and recognize faces in videos or images. A study collected images of individuals to be recognized with the help of video clips. The above technique was then applied to extract the facial regions, which resulted in a database of registered individuals [19].

Every person entering the system gets a unique ID. Information about banned persons is also stored. The SDB datasets are used to train the system, and the saved model weights are obtained. The cropped faces are obtained from the video frames as well as the captured images. Figure 3 shows examples of cropped faces obtained from both video frames and captured images.

Stage II: Students' recognition

At this stage, the system processes the colored images or video streams of persons passing through the class gate. Deep learning techniques using CNNs have been employed to identify and classify individuals from images [19]. Google Drive, Gmail, and Google Colab are used for storing data, communication, and processing in the cloud.

Stage III: Students' identification

Each image of the student identified in the earlier step is matched against the stored dataset. Further, the access rights are managed. The system matches extracted features, calculates the percentage of similarity, and determines the identity of every individual. As can be seen in **Figures 4** and **5**, the system is adaptable enough to demonstrate the ability to extract human faces from group photos on the university campus.

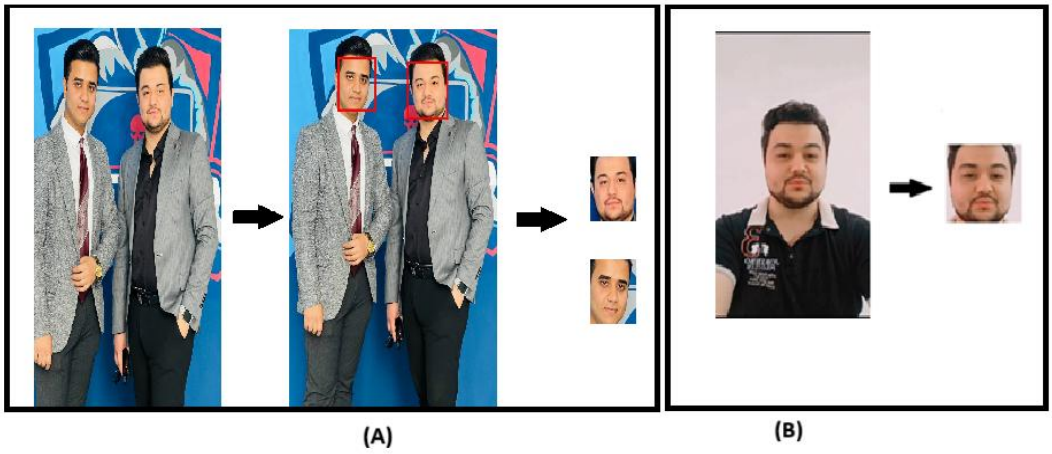

Figure 4: Examples of facial region extraction from (A) a captured image and (B) a video frame.

Figure 5: Sample cropped faces from different campus locations. Examples from (A) indoor group (artificial lighting) and (B) outdoor group (natural lighting), showing the system's ability to detect faces in varied environmental conditions.

Stage IV: Alert management

After recognition has been achieved, the system's final stage occurs. If a student matches a banned (incompletely registered) individual, as shown in Figure 6, the system immediately sends an alert email, as shown in **Figure 7**. The email contains the individual's ID, location, date, and time. The monitoring agent's screen displays all relevant data, including the image of the restricted person, the resemblance ratio, and other details [16].

Figure 6: Student's identification as banned and alert.

Figure 7. The alert management.

4. Implementation

This section describes the implementation process, including the platform and dataset used for the proposed system. It also presents a brief discussion of the experimental findings and outlines the security measures implemented to safeguard information.

1.1 Platform

The process starts with facial capture from audio/video frames or taken pictures. A cloud-based distributed computing system was used for the proposed deep-learning residual neural network model [20][21]. The identification system is designed using Python, where image transfer is done by Gmail, storage is handled in Google Drive, and online training and data processing are performed in Google Colab.

As summarized in **Table 1**, this is the platform configuration used to implement and test the system. The development and preliminary testing were done on an Intel Core i7-7500U CPU (2.70 GHz) with an NVIDIA GeForce 9300MX GPU. The NVIDIA GeForce 9300MX is not really considered a good GPU by present-day deep learning standards. However, it was good enough for our application, as our dataset consisted of only 270 images of 9 students. Moreover, we performed face cropping and resized images to 224 × 224 pixels. Therefore, we did not require a powerful GPU like the NVIDIA GeForce RTX 2080 Ti or similar models. With this dataset size, the available GPU allowed for sufficient training time without expensive high-performance machinery.

Table 1. Configuration of the platform.

Configuration	Parameters
Operating system	Edition: Windows 10 Enterprise
	Version: 22H2
	Experience: Windows Feature Experience Pack 120.2212.4190.0
	System type: 64-bit operating system, x64-based processor
CPU	Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
GPU	NVIDIA GeForce 9300MX
Installed RAM	12.0 GB (11.9) Usable
Python	3.10.12 (main, Sep 11 2024, 15:47:36) [GCC 11.4.0]
Platform processor	x86_64
Tensor flow	2.17.0
Keras	3.4.1
CV2	4.10.0

Nonetheless, we should recognize this hardware limitation. The limited capacity of the GPU restricts the scalability of the system. Deployments with thousands of students and real-time requirements will require more powerful GPUs for institutions, such as NVIDIA Tesla V100, A100, or more modern RTX series. As a proof of concept, the method works in its current form. However, a production implementation would require an increase in computing power.

To reduce local hardware burdens and scale easily, the system utilizes Google Colab. Using this method provides the following benefits: (1) the ability to use a more powerful cloud GPU if needed; (2) scalable storage through Google Drive that grows with the dataset; (3) distributed computing; and (4) cost savings by avoiding expensive local infrastructure. The program, written in Python, is run in the Colab environment for training ResNet on images that were transferred from Gmail to Google Drive folders.

The system is very efficient in performing its task, as it is able to use the strengths of both CPUs and GPUs to perform parallel computation of CNN operations, which is otherwise impossible. This hybrid solution makes better use of resources from existing hardware.

1.2 Dataset

The system was designed to be used in open spaces like schools, banks, and airports, but privacy regulations limit the collection of verification data. Therefore, image acquisition included the collection of images and videos of the students of the college. In order to create a dataset of those students who are banned, it was assumed that certain people were incompletely registered with the student affairs office.

To facilitate the recognition and identification stages, a nine-male student (MSB) database consisting of 270 images was formed, with an extra 18 identification images and 50 additional images, including group images. To prevent unauthorized access and abuse, security measures were implemented, such as sending email alerts that ask for permission to access and take control of documents saved on the drive. The administrator either grants or denies access as per the request.

Even if small, the dataset was designed as a proof of concept with strict privacy and ethical considerations. Because of regulatory limits, it was impossible to conduct large-scale data collection. The dataset reflects a real-world situation where only a limited number of students have incomplete registration records. The quantity of images collected for each student was increased to combat overfitting by altering their conditions. Should the outcomes prove satisfactory, subsequent experimentation will assess the system on larger and more diverse datasets to evaluate generalizability and robustness.

1.3 Parameter Settings

To enhance the application's performance, we established key parameters for CNN training based on prior studies with satisfactory results. An overview of these settings is in **Table 2**.

Table 2. Parameter settings for the proposed work**.**

Parameters	Values
Dropout Rate	0.2
Learning Rate	0.00005
Batch size	32
No. of Hidden	2
No. of Units in Hidden	32768
Act. Fun. in Hidden	Softmax
No. of Conv. Layers	10
No. of kernels	1,2,3,4,5
Kernel size	32,64,128,256,512
Act. Fun. for Conv. Layers	Relu
BatchNormalization	12
No. of pooling layers	5
Max Pooling size	2
Padding	Same
Stride	1
Activ. Fun for the out. Layer	Sofmax
Loss function	Categorical-cross-entropy
Optimizer	Adam
Metrics	Accuracy
Epochs	80
Regularization	L2
Weight decay	0.0001
Early_stopping (patience)	10

5 . Results and Evaluation

The dataset was split into 60% for training, 30% for validation, and 10% for testing. Figure 8 presents the loss and accuracy curves for individual classification. During the execution of the Python program in the cloud environment, all image types were classified.

Similarity thresholds were tested, and recognition rates were calculated by recording the number of correctly recognized images out of a total of 300, as shown in **Table 3**.

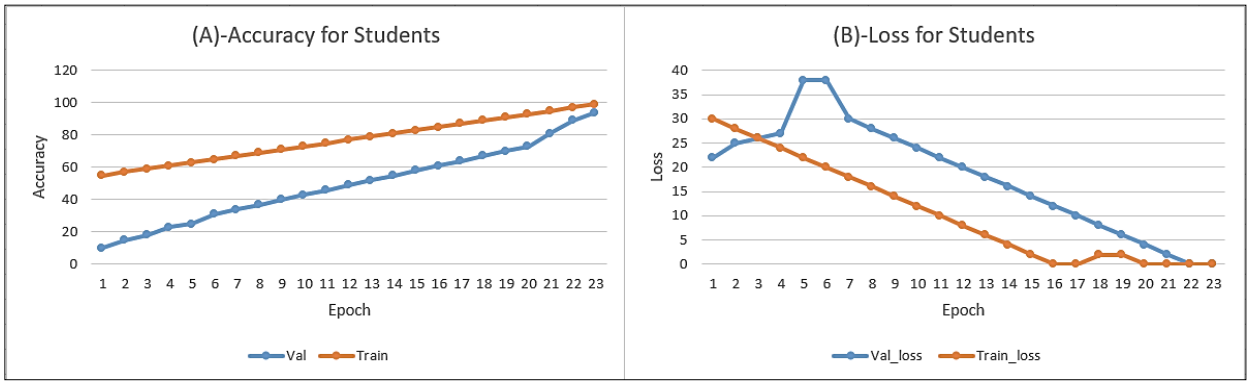

Figure 8. Accuracy and loss during training and validation.

Table 3. Similarity and recognition ratio for students.

Similarity ratio	Recognition ratio	Images
75%	72.5%	145
80%	76.5%	153
85%	83%	166
90%	86.5%	173
95%	92.5%	185
100%	100%	200

As shown in Figure 7 and Table 3, the model achieved improved training and validation accuracy while the loss is on the decline, showing that the model is trained successfully and does not overfit. As the threshold of similarity was raised, recognition ratios also started increasing. The recognition ratio is shown to touch 100% at 100% similarity. This shows the model to be effective on high-quality data. With a 75% similarity value, lower recognition indicates the model is sensitive to lower-quality data on the whole, where improvement in feature extraction or data augmentation could be focused. In general, the results indicate the effectiveness of the model on the current dataset and the possibility of optimizing it further.

As described previously, the framework was tested using different image split ratios, with a primary split of 60% for training and 30% for validation. Performance metrics such as overall

accuracy, recall, precision, F-score, and specificity were calculated based on the proportion of correctly classified samples [20,21,22]:

$$Recall = \frac{\text{True Positive}}{\text{True Positive } + \text{ False Negative}} \quad \textbf{Eq. 1}$$

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{ False Positive}} \quad \textbf{Eq. 2}$$

$$F - Score = 2 * \frac{\text{Precision } * \text{ Recall}}{\text{Precision} + \text{ Recall}} \quad \textbf{Eq. 3}$$

$$Overall\ Accuracy = \frac{\text{True Positive + True Negative}}{\text{True Positive + True Negative + False Positive + False Negative}} \quad \textbf{Eq. 4}$$

$$\text{Specificity } = \frac{\text{True Negative}}{\text{False Positive } + \text{ True Negative}} \quad \textbf{Eq. 5}$$

For students' information in Table 4, they were labeled as ('Hu', 'Za', 'Ha', 'Sa', 'Mo', 'Ab', 'Ms', 'Ja', and 'Aw'). The result of these metrics is shown in **Table 5**.

Table 4. Students' information

IP	Name	Birthday	Stage	Department
1	Hussein Bayan Mohammed	02/11/2003	Second	Information System
2	Zaedon Kasim Alwan	26/06/2005	First	Medicine System
3	Hazim Mahdi Madlom	03/06/2003	Second	Information System
4	Saif Abdul-Motalib Shibeeb	18/10/2000	Fourth	Computer Science
5	Mohamood Sabah Razak	11/03/2001	Second	Information System
6	Ali Basim Zeyara	22/09/2004	First	Computer Science
7	Mostafa Salam Jabber	17/02/2004	First	Computer Science
8	Jaber Saad Abdul_Abbas	25/05/2001	Second	Information System
9	Ali Waleed Waseem	10/04/2003	First	Computer Science

Table 5. The evaluation metrics.

Precision	Recall	F-score	Accuracy	Specificity
98	97	97.4	97	98

As seen in **Table 4**, it can be concluded that the model performs very well on all metrics. The precision of 98% and a recall of 97% show that the model identifies true positives with few false positives and false negatives. These metrics indicate high reliability, which is important for applications where high sensitivity and specificity are required. A score of 97.4% for the F-score indicates excellent precision and recall on the existing dataset. A confusion matrix categorizes the number of samples that were correctly and incorrectly classified. This offers a clearer picture of the false positives and false negatives, thus complementing the overall accuracy and other evaluation metrics reported earlier, as shown in **Figure 9**.

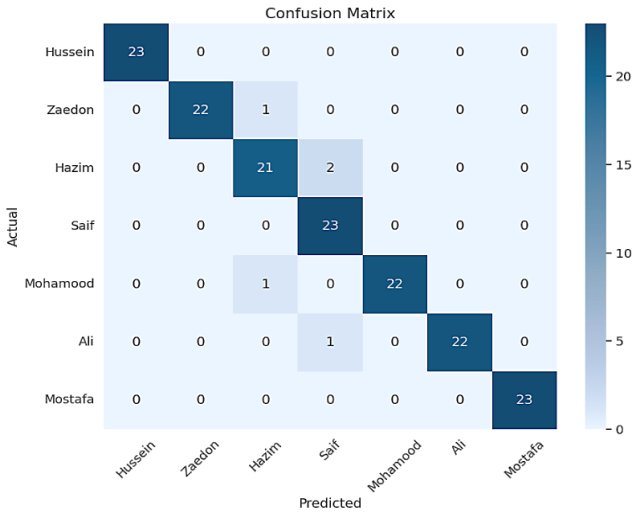

Figure 9. The Confusion Matrix of the classification performance.

The overall accuracy of 97% and specificity of 98% further highlight the model's suitability for the tested student identification scenario. The small difference between precision and recall suggests a minor trade-off between detecting all positive cases and minimizing false positives.

6. Conclusion

In this paper, we present a cloud-based face recognition system designed to prevent unauthorized students from attending classes. Unlike traditional attendance systems that require complete registration databases, our approach leverages deep learning to accurately identify students even with incomplete registration data and variable image quality. Rigorous testing and online implementation in Python achieved 97% accuracy across similarity thresholds from 75% to 100%.

This study has important limitations: testing was conducted on a small dataset (270 images of 9 students) from a single university with homogeneous demographics. While the results are promising for this context, generalization to larger and more diverse populations requires validation with substantially larger datasets covering different ethnicities, age groups, and environmental conditions. Future research should focus on expanding validation to multi-institutional datasets, improving performance under challenging conditions (e.g., varying lighting, facial expressions, occlusions), and incorporating advanced biometric features and real-time video analysis.

For student identification in controlled educational environments, this research demonstrates a practical and effective approach to access control. By addressing unauthorized attendance through cloud-based deep learning, the system provides academic institutions with a scalable

solution for enhancing campus security. However, extension to other domains (such as medical facilities or broader security applications) would require domain-specific validation and cannot be inferred from the current results.

References

[1] L. Wang, R. Ranjan, J. Chen, and B. Benatallah, *Cloud Computing: Methodology, Systems, and Applications*, CRC Press, 2012, https://doi.org/10.1201/b11149.

[2] Ezatullah, "Cloud Computing Principles," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 13, no. 1, Jan. 2024, https://doi.org/10.17148/IJARCCE.2024.13103.

[3] E. Masoud, M. Abuella, A. Aly, and S. Mahmoud, "Cloud Computing and IoT-Based Intelligent Monitoring System for Photovoltaic Plants Using Machine Learning Techniques," *Energies*, vol. 15, no. 9, art. no. 3014, 2022, https://doi.org/10.3390/en15093014.

[4] S. Kumar, D. Sadhya, D. Singh, and S. K. Singh, "Cloud Security Using Face Recognition," in *Web-Based Services: Concepts, Methodologies, Tools and Applications*, pp. 2055–2075, 2016, https://doi.org/10.4018/978-1-4666-9466-8.ch090.

[5] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, https://doi.org/10.1109/CVPR.2015.7298682.

[6] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, https://doi.org/10.1109/CVPR.2019.00482.

[7] Md. A. Bhuiyan, "Towards Face Recognition Using Eigenface," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, 2016, https://doi.org/10.14569/IJACSA.2016.070505.

[8] Chen, J. Zhang, Y. Li, and H. Wang, "A Survey on Facial Image Privacy Preservation in Cloud-Based Services," *arXiv preprint*, arXiv:2501.08665, 2025, https://doi.org/10.48550/arXiv.2501.08665.

[9] Kumar and A. M. Khan, "Face Recognition-Based Attendance Management System," *Zenodo*, July 2024, https://doi.org/10.5281/zenodo.12787806.

[10] Smitha, P. S. Hegde, and Afshin, "Face Recognition-Based Attendance Management System," *International Journal of Engineering Research & Technology*, vol. 9, no. 5, May 2020.

[11] T. Rahman, A. N. Saputra, and E. D. Anggara, "Attendance Monitoring System Based on IoT," *Multitek Indonesia*, vol. 15, no. 2, pp. 33–43, 2022.

[12] Asaduzzaman, A. Mummidi, M. F. Mridha, and F. N. Sibai, "Improving Facial Recognition Accuracy by Applying Liveness Monitoring Technique," in *Proceedings of the 3rd International Conference on Advances in Electrical Engineering*, Dhaka, Bangladesh, Dec. 2015.

[13] M. N. Jacob and M. Y. Wanjala, "A Review of Intrusion Detection Systems," *International Journal of Computer Science and Information Technology Research*, vol. 5, no. 4, pp. 1–5, 2017.

[14] O. Abdulkhaleq and M. F. Akay, "WS-AWRE: Intrusion Detection Using Optimized Whale Sine Feature Selection and ANN-Weighted Random Forest Classifier," *Applied Sciences*, vol. 14, no. 5, p. 2172, 2024, https://doi.org/10.3390/app14052172.

[15] G. A. Robles, "Convolutional Neural Networks for Real-Time Classification of Beehive Acoustic Patterns on Constrained Devices," *Sensors*, vol. 24, no. 19, p. 6384, 2024, https://doi.org/10.3390/s24196384.

[16] S. Liu, L. Guo, H. Webb, X. Ya, and X. Chang, "Internet of Things Monitoring System of Modern Eco-Agriculture Based on Cloud Computing," *IEEE Access*, vol. 7, pp. 37050–37058, 2019.

[17] Lal, S. Aftab, S. Kumar, and M. Shaikh, "Smart SOP's Surveillance System Using Deep Neural Network," vol. 14, no. 7, pp. 6–11, 2022.

[18] O. E. Ojo, M. K. Kareem, O. Samuel, and C. O. Ugwunna, "IoT-Based Real-Time Monitoring System for Smart Classrooms," *Journal of the Nigerian Society of Physical Sciences*, 2022–2023.

[19] J. Jalil, E. A. El-Seidy, S. S. Daoud, and N. M. Reda, "Enhanced Surveillance System: Masked Face Re-Identification Using Cloud Computing and Deep Learning," *International Journal of Technical and Physical Problems of Engineering*, vol. 16, no. 1, pp. 63–72, Mar. 2024.

[20] G. Kasinathan, "Cloud-Based Lung Tumor Detection and Stage Classification Using Deep Learning Techniques," *BioMed Research International*, vol. 2022, art. ID 4185835, pp. 1–17, 2022.

[21] J. Jalil, E. A. El-Seidy, S. S. Daoud, and N. M. Reda, "Modified CNN Model for Classifying Gender of Thermal Images Using Cloud Computing," *Informatica*, vol. 47, no. 10, pp. 123–128, Dec. 2023, https://doi.org/10.31449/inf.v47i10.4924.

[22] J. Jalil, E. A. El-Seidy, S. S. Daoud, and N. M. Reda, "CNN Model for Analyzing Masked Facial RGB Images Using Cloud Computing," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2, pp. 648–654, 2023.

نظام سحابي قائم على الشبكات العصبية الالتفافية للتعرّف على الطلاب في ظل سجلات تسجيل غير مكتملة

علياء جابر جليل وميثم ابوالهيل شهيد

قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة البصرة، البصرة، العراق

المستخلص

تحتاج الجامعات إلى نظام جيد للتعرف على الطلاب لتجنب الحضور غير المصرح به. ومع ذلك، فإن نقص المعلومات في سجلات التسجيل يخلق تحديات كبيرة لخطط التعرف الحالية. قمنا بإنشاء نظام للتعرف على الوجوه قائم على السحابة باستخدام الشبكات العصبية التلافيفية المستندة إلى ResNet للتعرف على وجوه الطلاب من الصور المستخرجة من الفيديو مع بيانات تسجيل غير مكتملة. استخدم النظام 270 صورة مأخوذة من تسعة طلاب تحت ظروف مختلفة؛ وباستخدام هذه الصور، تم تحقيق نتيجة بلغت 97% عند تشابه يتراوح بين 75% و100%. يعتمد النظام على الإشعارات عند اكتشاف وصول غير مصرح به ويستخدم البنية التحتية السحابية للنشر. تظهر هذه النتائج أن التعرف في مثل هذه الحالات يمكن تنفيذه باستخدام نماذج التعلم العميق. ويمكن أن يكون ذلك مفيداً في أمن الحرم الجامعي وخدمات إدارة التسجيل الأخرى.

الكلمات المفتاحية: الحوسبة السحابية، التعلم العميق، الشبكات العصبية التلافيفية، التعرف على الوجوه، التعرف على الطلاب.