Access Control with Facial Recognition: A Systematic Literature Review

Thalita R. E. da Silva[1], Rogério A. dos S. Antoniassi[1], Alex F. de Araujo[1]

[1]*Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul - Campus Três Lagoas*
R. Ângelo Melão, 790, 79641-162, Três Lagoas - MS, Brazil
thalitaaesser@gmail.com, rogerio.antoniassi@ifms.edu.br, alex.araujo@ifms.edu.br

Abstract. Counting people or even identifying individuals present in a given place is a fundamental task for public and private sectors and/or institutions that need to manage the access and permanence of individuals in certain places. This is not different at the Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul - Campus Três Lagoas (IFMS-TL), which has a large physical space and only a few employees to control and supervise these facilities, which are shared by students requiring more access control. Several tools and methodologies have been proposed to meet this demand, including the use of DeepLearning, convolutional networks and a wide variety of facial recognition algorithms, which show great potential, as they are present in solutions in the literature. The aim of this paper is to carry out a Systematic Literature Review (SLR), broadly investigating best practices and success cases using facial recognition to control people's access to environments. The SLR makes a significant contribution to those who intend to develop or research in this field, as it presents an overview of different applications. And also helps on the development of a montoring system for access control to IFMS-TL facilities**.**

Keywords: Facial Recognition; DeepLearning; Acess Control.

1 Introduction

As technology advances, Artificial Intelligence is becoming more present of society's daily lives. This is no different in security, in which authentication and monitoring of people's access to environments through facial detection has grown exponentially. Facial recognition technologies are being integrated into different applications to ensure a better user experience [1]. In facial recognition, verification and authentication, expression recognition and gender/age recognition algorithms, face detection is a key stage. These different algorithms and methods can be used in various applications that identify facial features such as the nose and eyes [2]. Furthermore, a robust face recognition system must contain three stages, which are sequential: face detection, feature extraction and face recognition [3]. In the first stage of detection, the human face is identified in the image obtained, while the second stage involves vectorization of the face by extracting patterns from the facial features. Finally, the third phase consists of facial recognition, by comparing the data extracted in the previous stages with the dataset. Therefore, this study consists in a Systematic Literature Review (SLR) of different methods and approaches used in latest academic papers of facial recognition, for monitoring people's access to environments. Based on this objective and the results obtained from the research questions, the focus is on replicating the outcomes to solve the current problem affecting the IFMS-TL. Which is to monitor access to the institution's physical spaces, because it has a large area, but few employees to control and supervise these places, that are accessed by many students on a day-to-day basis.

This research is composed by an Abstract, an Introduction, in which the study is contextualized, followed by the Methodology applied to the scientific database searches, the filtering of the papers and the inclusion criteria. Also, the Results obtained from the searches, and Discussions with the most used applications, being

those based on Convolutional Neural Networks (CNN). Finally, the Conclusion, in which the answers to the research questions of this SLR are described.

2 Methodology

This section discusses the methodology applied in the research, as well as the criteria for selecting the studies and the planning applied to the analysis of those that were filtered. A Systematic Literature Review should be based on research questions, a search method, inclusion and exclusion criteria, analysis of the results, and evaluation of the quality of the filtered studies, according to [4]. So, the question that guided the research was: "Which facial recognition techniques are most commonly used to monitor access in environments?" Besides this question, other questions were added to obtain answers on relevant specifications, such as the applications of the selected studies, which are answered in the Conclusion.

2.1 Search Stage

To develop this SLR, the search criteria used were works available on the Scopus and IEEE databases, due to their widespread use in the scientific community. For this purpose, a string was defined and applied to the advanced search in each of the databases. In order to define the terms that make up the string, they were standardized in English and selected according to the research objectives, as follows: (("Facial Recognition") AND ("Access Control" OR "Surveillance" OR "Identification") AND ("Classification" OR "Monitoring") AND ("Deep Learning" OR "Machine Learning" OR "Computer Vision") AND NOT ("Disease" OR "Disorder" OR "Law" OR "Speech" OR "Animals")).

2.2 Inclusion Criteria

In the search phase of the SLR, inclusion criteria were defined for the works found from the search string, to assist in the content analysis stage, which were as follows:

1. **Inclusion Criteria CI1**. The studies must have been published in any of the two scientific databases, Scopus or the Institute of Electrical and Electronic Engineers - IEEE;
2. **Inclusion Criteria CI2.** The period of publication selected must be between January of 2022 and may of 2024. This time frame was chosen so that the study would focus on recent applications using facial recognition. Due to the rapid development of facial recognition technologies, this period is likely to capture the latest refined and innovative applications in a variety of scenarios, with emerging features and effectiveness systems, among other challenges. The constraints of this period guarantee relevance and up-to-date research into the current state of the field;
3. **Inclusion Criteria CI3.** The search considered complete articles written in English and Portuguese, excluding book chapters, SLR and event abstracts;
4. **Inclusion Criteria CI4.** The articles must consist of DeepLearning or Computer Vision applications in the context of Facial Recognition of individuals with the development of access monitoring systems.

2.3 Exclusion Criteria

Criteria for exclusion were also used in the search phase, and the following were defined:

1. **Exclusion Criteria CE1.** Duplicate articles;
2. **Exclusion Criteria CE2.** Non-reproducible articles, considering those that do not contain the implementation of an access monitoring system in environments.

2.4 Search and Analysis

The collection of articles was separated into two stages, the first on Scopus, in which 203 results were found, while the second stage, on the IEEE database, returned 198 articles. During this phase of the search, the

CI1 and CI2 inclusion criterias were applied, in addition to the application of CE1, and the final balance was 95 in Scopus and 121 in IEEE.

When the search results were analyzed, they were merged to form the same database. The abstracts of the articles were analyzed and those that didn't meet the CI3 and CI4 inclusion criteria were rejected. Therefore, after this analysis stage, a total of 192 articles were eliminated because they didn't meet the inclusion criteria, resulting in 24 articles for full reading.

For the exclusion criteria CE1, no article met this restriction.

After reading all 24 articles, the CE2 exclusion criteria was applied on each one. Applying this criterion, some articles were excluded because they did not have a reproducible methodology for the IFMS-TL scenario. Such as articles with a different application system to the IFMS-TL requirement and others with a methodology limited to surveys focused on particular algorithms. So, at the end of the complete reading, there were a total of 17 articles, which will be discussed in more detail in the Results section.

2.5 Quality Assessment

Regarding the quality of the publications, the inclusion criteria CI1 is directly related. In addition to being considered whether the methodology used was able to answer the research questions.

Exclusion criterion CE2 was also considered a quality criterion, since reproducibility makes it possible to assess how the different ways of applying the system can perform in the IFMS-TL scenario. And lastly, the impact of the results presented in the papers were also considered as a quality criteria.

3 Results

Based on the inclusion and exclusion criteria defined, a set of seventeen papers were selected after full reading step, of which nine were from Scopus and eight from IEEE. These are detailed in Table 1, organized by author, year of publication and database. This Results section is made up of the summaries of the selected articles, which have different methods and accuracies, as described below.

Table 1. Articles analyzed after applying the inclusion and exclusion criteria

Authors	Database	Publish Year
[5]	Scopus	2022
[6]	Scopus	2022
[7]	Scopus	2022
[1]	IEEE	2023
[2]	IEEE	2023
[8]	Scopus	2023
[9]	Scopus	2023
[10]	Scopus	2023
[11]	Scopus	2023
[12]	IEEE	2023
[13]	IEEE	2023
[14]	IEEE	2023
[15]	IEEE	2023
[16]	IEEE	2023
[17]	Scopus	2024
[18]	Scopus	2024
[19]	IEEE	2024

In [1] the authors carried out a study aimed at analyzing a dataset made up of images taken from different distances, lighting intensities and face orientations, in order to detect the face using the Haar Cascade Classifier algorithm. The detector chosen had an average accuracy of 80%, which showed consistency in the results, based on the different variations in the images.

The article [2] proposes a comparative study between different models in the context of facial recognition, in which they applied pre-trained models based on CNN, such as VGG16, VGG19, Resnet and Inception. The

Haar Cascade Classifier was used to detect the faces in the dataset, and the models used have pre-trained weights, with the addition of two more layers for the tests. The VGG16, VGG19 and Inception models performed better than Resnet, with Iception being the most efficient with an accuracy of 99.7%.

In [8] the authors developed a model that performs facial recognition of employees, so that with the application of DeepLearning in CNN they obtained a final accuracy of 97%. The authors made a comparison between the number of epochs, in which it was found that a total of 100 allowed this value for accuracy, being the most satisfactory obtained. However, they warn that this number of epochs can lead to a reduction in loss, which was 0.1818.

In [9] proposes an application of FaceNet with MobileNetV2, for a presence system, which aims to monitor people's access to a space, in which it is emphasized that the solution can be used on hardware with low operating capacity. With this method, the author obtained an average accuracy of 95%, with a processing speed of 20-23 FPS.

In recent studies [10] developed a Raspberry-PI robot that, using facial recognition, is able to identify "intruders" in a space. When identified, alerts are sent by email with the individual's photo and a warning in the app developed for the application. The model used relied on the Haar Cascade Classifier for face detection and the Local Binary Pattern Histogram (LBPH) for classification, in which this method generated an accuracy of 93.33%, and the authors point out that the cost of implementation is low compared to other existing monitoring systems.

In their latest study [11] has created a facial recognition system, in which they used the Haar Cascade Classifier to detect faces and Deep CNN to extract and classify facial information. The model was trained with two different public datasets, which resulted in an average accuracy of 99%. The authors pointed out that the application depends on a high computational cost and large datasets for training and testing the model.

Also in [12] the authors developed a study to ensure the security of a university campus and real-time monitoring by means of a monitoring system. In this system, images from different cameras are analyzed and classified as to whether someone has authorized access or not. For this application, the Haar Cascade Classifier algorithm was used, but some challenges were encountered, such as the low brightness of the space and the low quality of the images, which affected the performance and accuracy of the model. In addition, the system has an alert feature, in which in the case of unrecognized individuals, a sound is emitted to the user who is monitoring. However, the authors did not mention the accuracy obtained in the application.

In [13] was implemented DeepLearning for intelligent campus monitoring, which detects offenders who are not wearing their ID badges and recognizes them by face. To train the model, they used a dataset with 6000 images for badge detection, which was processed, treated and normalized. The You Only Look Once V7 (YOLOV7) algorithm and CNN were then used for facial detection and recognition. During the tests, the accuracy of facial recognition was 92%, while badge classification achieved 70.6% Mean Average Precision (mAP) and 91.3% accuracy.

The article [14] propose a study on the application of an automated presence system, with the Haar Cascade classifier algorithm for face detection and SVM applied for face extraction and recognition. The dataset used was obtained from images of students on campus. In addition, the model's input images are photos taken by a webcam at the entrance to the room, and once identified the presence is recorded for the student. With this method, the authors achieved an average accuracy of 90%.

The authors of [15] developed an automated student attendance system, the aim of which was to optimize manual marking time. In addition, as soon as the face is recognized, attendance is marked in a spreadsheet that the teacher has access to, and a report with attendance is sent to parents at the end of each school day, SMSs are also sent with information from each class. CNN is applied to a dataset made up of student images and used in facial recognition, in which the entire process takes place on the AWS Cloud system. The authors did not document the accuracy obtained, but pointed out that the accuracy was higher in smaller datasets, and that the application in the classrooms worked as expected.

In [16] was applied an integrated presence system, which automatically marks the presence in a spreadsheet when a face is detected. This was built using the Haar Cascade Classifier algorithm and LBPH. With this method, the authors reported that recognition also worked for faces in different positions and the possibility of marking attendance simultaneously for several students. Therefore, it is worth noting that the accuracy obtained was 80%, with the face at different angles.

Also, [17] has applied an emotion recognition system based on facial expressions, in which HOG is used to

detect faces, as well as Viola-Jones to extract facial information and classification with recognition using Support Vector Machines (SVM), CNN and a hybrid application of CNN-SVM. The aim of this article is to compare the benchmark between the methods in order to identify the most ideal application, in which the results were very promising. In the SVM application, the final accuracy obtained was 99.46%, while for CNN the accuracy was 97.76%-99.76%, and 99.31%-99.80% for the CNN-SVM hybrid application. The authors describe that the best accuracy obtained was with the CNN and SVM models, separately, from the application of Fusion Deep features.

In [18] propose a smart lock system that can be applied in offices to protect sensitive data, where only authorized people can access the environment. The aim is to optimize facial recognition using CNN techniques, applied to a Raspberry-PI, with a dataset made up of 5 classes. Therefore, the accuracy obtained by the authors was 96%, in which the model was trained from a set of 8800 images, with a split of 80:20, respectively for training and testing.

In the authors [19] applied a lock system with facial recognition, using Raspberry-PI and Haar Cascade Classifier for face detection and Local Binary Pattern (LBPH) for classifying the images obtained. If the face detected at the door entrance is not recognized, access is not granted and an email is sent to the application owner, otherwise the door is opened. The accuracy of the model is not documented by the authors, but they describe a 100% success rate obtained in different tests.

4 Discussion

This SLR has two main research questions, they were essential to the process of analyzing the search results, so this section discusses the selected articles that answered the research questions.

4.1 [Q1] What approaches to the use of facial recognition in access monitoring the selected articles can solve?

The first research question is related to the proposed approaches that can be applied to the facial recognition scenario in access monitoring environments. The main methodologies and applications used in the articles found are detailed below.

Remark 1: ***Presence System with Automatic Filling.*** In [14] a study is proposed on the application of an automated attendance system based on facial recognition. The dataset used was obtained from images of students on campus. In addition, the model's input images are photos taken by a webcam at the entrance to the room. With this method, the authors had an average accuracy of 90%. Also, in [16] an integrated attendance system was applied, which automatically marks attendance in a spreadsheet when it detects the face. With this method, the authors reported that recognition also worked for faces in different positions and the possibility of marking simultaneous attendance for several students. Furthermore in [15] the authors developed an automated student attendance system in which the aim was to optimize manual marking time. In addition, as soon as the face is recognized, attendance is marked in a spreadsheet that the teacher has access to, and a report with attendance is sent to parents at the end of each school day, SMSs are also sent with the information from each class.

Remark 2: ***Smart Lock System.*** In article [18] a smart lock system is proposed, which can be applied in offices to protect sensitive data, where only authorized people can access the environment. The aim is to optimize facial recognition using Raspberry-PI. While in [19] was applied a lock system with facial recognition, also using Raspberry-PI. If the face detected at the door entrance is not recognized, access is not granted and an email is sent to the application owner, otherwise the door is opened.

Remark 3: ***Intelligent Robot.*** In research [10] has developed a Raspberry-PI robot which, using facial recognition, is able to identify "intruders" in a space. When identified, alerts are sent by email with the individual's photo and an alert in the app developed for the application. The authors point out that the cost of implementation is low compared to other existing monitoring systems.

[Q2] Which facial recognition techniques are commonly used for access monitoring in rooms?

To answer this question, it was taken into account that a robust facial recognition system must contain three stages, which are sequential: face detection, feature extraction and face recognition, according to [3].

Based on this premise, an article can have more than one technique that answers the question or a combination of different ones. When analyzing the selected articles, it was possible to see that the authors prioritized the use of specific and appropriate algorithms for each stage, so that in most cases the accuracy was high.

It was possible to observe that the most widely techniques used for face detection was the Haar Cascade Classifier, as well as being the most optimized for the scenarios applied. However, as highlighted in [6], there are some limitations that affect detection, such as low light and variation in the angle of the face.

While, for face extraction and recognition, the most used were CNN and LBPH, as they are the most optimized and scalable. As in [10] who highlighted an accuracy of 93.33%, and a low implementation cost compared to other existing monitoring systems. Therefore, Table 2 compiles the articles and each technique used according to the solution".

Table 2. Techniques used in the analyzed articles

Authors	**Facial Recognition Stages**		
	Detection	***Extraction***	***Recognition***
[8]	CNN	CNN	CNN
[9]	MobileNetV2	FaceNet	FaceNet
[10]	Haar Cascade	LBPH	LBPH
[5]	MobileNet	MobileNet	MobileNet
[6]	HOG	SVM	SVM
[7]	EfficientDET	CASIA-WebFace	EfficientDET
[17]	HOG	Viola-Jones	SVM,CNN
[18]	MobileNetV2	CNN	CNN
[11]	Haar Cascade	Deep CNN	Deep CNN
[19]	Haar Cascade	LBPH	LBPH
[2]	Haar Cascade	VGG16,VGG19	VGG16,VGG19
[1]	Haar Cascade	CNN	CNN
[12]	Haar Cascade	CNN	CNN
[13]	YOLOV7	CNN	SVM
[14]	Haar Cascade	CNN	CNN
[15]	CNN	CNN	CNN
[16]	Haar Cascade	LBPH	LBPH

5 Conclusions

This Systematic Literature Review made it possible to identify the most recent applications used in facial recognition, for monitoring people's access to environments. Always starting from the premise that a robust facial recognition system must contain three steps, detection, extraction and facial recognition itself.

Thus, according to the results analyzed, in this research, it was possible to observe that solutions based on CNN currently are the most used, in the facial extraction and recognition stages. In addition to the LBPH, which also has a high application rate, the combination of this technique with the Haar Cascade Classifier for object detection, resulted in high accuracy and optimized systems.

Furthermore, based on the second research question, it was possible to identify applications with the most

commonly technique used. As a result, it was possible to see how the solutions had a positive impact on the problems the authors had as a starting point.

Therefore, this SLR provides an input to solve the current difficulty of the IFMS-TL, which is monitoring access to the institution's physical spaces. As next steps, the aim is to apply the techniques surveyed in order to use them for an authentication and monitoring system at IFMS-TL.

In addition, it can be used as an input for researchers who want to implement facial recognition solutions or who are interested in the topic of research. Therefore, after analyzing the best practices, it is possible to develop numerous solutions with the technologies surveyed applied in the papers analyzed.

Authorship statement. The authors hereby confirm that they are the sole liable persons responsible for the authorship of this work, and that all material that has been herein included as part of the present paper is either the property (and authorship) of the authors, or has the permission of the owners to be included here.

References

[1] N. Karpiuk and H. Klym, "Identity Verification and Detection System through Facial Recognition Technology". 13th International Conference on Eletronics and Information Technologies (ELIT), pp. 206–209, 2023.
[2] A. Khanfri, H. Benbrahim, A. Amine, "Face Detection Using Artificial Intelligence". 9 th International Conference on Optimization and Applications (ICOA), pp. 1–6, 2023.
[3] Y. Kortli, M. Jridi, A. A. Falou, M. Atri. "Face Recognition Systems: A Survey". Sensors 20, no. 2, 2020.
[4] M.C. B. Galvão and I.L.M. Ricarte. Revisão Sistemática da Literatura: Conceituação, Produção e Publicação. Logeion: Filosofia da Informação, Rio de Janeiro, p. 57-73, 2019.
[5] J.C. Leiva, M.V. Rivillas, J.M. Ordóñez. "Acess Control System based on Voice and Facial Recognition Using Artificial Intelligence". International Journal on Advanced Science Engineering Information Technology. vol. 12, no. 6, 2022.
[6] M.L.E. Hadi, M. Nasri, Y. Farhaoui, A. Ellaoui. "Application of the deep learning approach for identification and face recognition in real-time video". 2022 International Conference on Intelligent Systems and Computer Vision (ISCV). pp. 1-6, 2022.
[7] K. Bouzaachane and E.M.E. Guarmah. "Applying Face Recognition in Video Surveillance for Security Systems". 8 th International Conference on Optimization and Applications (ICOA). pp. 1-5, 2022.
[8] H. Maulana, R. Ferdy, A. Khowarizmi. "Facial Recognition Model as Employee Attendance Using Modern Deep Learning with Convolutional Neural Network Method". Journal of Theoretical and Applied Information Technology. vol. 101, no. 15, 2023.
[9] T. V. Dang. "Smart Attendance System based on Improved Facial Recognition". Journal of Robotics (JRC). vol. 4, 2023.
[10] H. Meddeb, Z. Abdellaoui, F. Houaidi. "Development of surveillance robot based on face recognition using Raspberry-PI and IOT". Microprocessors and Microsystems, vol. 96, 2023.
[11] P.K. Mannepalli, D.S. Kushwaha, S. Kalamdhar, V. Nagrale, V. Rajpoot. "Face Recognition Based on Cascade Classifier Using Deep Learning". 1 St International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP). pp. 63-68, 2023.
[12] N.T. Singh,, A. Kumar, A. Jain and M. Pal. "Student Surveillance System using Face Recognition". Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). pp. 843-847, 2023.
[13] R. Deepalakshmi, M.K.R. Senthil, R.S. Arunnachalam, A.B. Mohamed. "Smart Campus Surveillance: Detecting Rule Breakers with Deep Learning". 4 th International Conference on Communication, Computing and Industry 6.0 (C216). pp. 1-6, 2023.
[14] S. Sharmila, G.K. Nagasai, M. Sowmya, A.S. Prasanna, S.N. Sri, N. Meghana. "Automatic Attendance System based on Face Recognition using Machine Learning". 7 th International Conference on Computing Methodologies and Communication (ICCMC). pp. 170-174, 2023.
[15] K. Vignesh, A.M. Abirami, P. Manideep, K. Vasu, K. Rakesh, S.V. Vardham. "Smart Attendance System using Deep Learning". 7 th International Conference on Trends in Electronics and Informatics (ICOEI). pp. 1081- 1087, 2023.
[16] K. Bhambure, A. Kadam, K. Dabhade, B. Deore, P. Gaikwad. "An Integrated Face Recognition based Attendance Monitoring System". 7 th International Conference On Computing, Communication, Control And Automation (ICCUBEA). pp. 1-6, 2023.
[17] H. Aouani and Y.B. Ayed. "Deep Facial expression detection using Viola-Jones algorithm, CNN-MLP and CNN-SVM". Social Network Analysis and Mining, vol. 14, no. 65, 2024.
[18] D.T. Hazriani and A.L. Arda. "Face Recognition for smart dooor security access with convolutional neural network method". TELKOMNIKA – Telecommunication Computing Eletronics and Control. vol. 22, no. 3, pp.702-710, 2024.
[19] A. Jha, R. Bulbule, N. Nagrale, T. Belambe. "Raspberry PI-Powered Door Lock with Facial Recognition". 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). pp. 1-4, 2024.