IRSTI 28.23.27 https://doi.org/10.26577/1i32jpcsit2304

Z.R. Yernazarov

Kazakh-British Technical University, Almaty, Kazakhstan
e-mail: z_yernazarov@kbtu.kz

DEVELOPMENT OF A CONTEMPORARY ACCESS CONTROL SYSTEM USING FACE RECOGNITION

Abstract. Facial recognition is a technique that locates a person's facial picture in a database of images in order to confirm that person's identification. Since it does not require any physical contact to get access, unlike conventional key-using methods, it becomes particularly useful in access control systems. Additionally, these systems need just photographic equipment for identification and are simple to set up and operate. Because of this, businesses already utilize them for access control to their workplaces. In this study, many facial recognition methods are examined. Face identification and cropping being the initial steps, we compared the conventional algorithms with the novel CNN- based technology which uses FaceNet as a baseline with respect to processing speed and detection accuracy. The created system will put together a face captured by the recording device with a picture from the database. In order to prevent the system from reacting to every means of getting around it, such as displaying a picture of a person who is authorized, the susceptibility of standalone facial recognition can be reduced by incorporating a spoof detection technique.

Key words: Access Control System, Face Recognition, Authentication, Biometrics, machine learning.

1. Introduction

Access control is an important aspect of security systems in institutions, and the traditional methods of authentication such as passwords, PIN codes, and ID cards have limitations such as the possibility of loss, theft, or unauthorized use [1]. The need for secure access control systems that provide both convenience and accuracy is becoming increasingly important. The solution to this problem lies in the development of advanced biometric-based access control systems. Face recognition technology is one such biometric technology that speeds up security checkpoints and permits entry without a physical key. It proved itself to be efficient during infectious disease spread such as COVID-19 as it allows people to not contact with any surfaces in contrast to other biometric systems that employ the fingerprints. The system operates in real-time and allows authorized individuals to enter the facility removing any inconveniences that are caused at check-in point. This conference paper demonstrates the results of an attempt to develop an access control system for institutions based on facial recognition algorithms.

Many applications of access control systems have been deployed recently with the aid of face recognition due to its prominence. It vastly increased the safety mechanisms' effectiveness. The real-world application utilizing principal component analysis (PCA) algorithm was created by Bakshi et al [2]. The software application was implemented on MAT- LAB with the Arduino development board serving as a hardware basis. Moreover, Sagar et al. introduced an automated security system that relies on facial image processing and identification depending on the brightness of the light present [3]. A smartphone app for facial detection and identification was put into place by Kremic, Subasi, and Hajdarevic for entry management and the avoidance of illicit smartphone use by third-parties [4]. Several companies have developed access control systems using face recognition technology. For example, NEC Corporation has developed a gateless access control system using biometric recognition that combines its face recognition technology with person re-identification technology [5].

2. Materials and Methods

Within a defined scope, the research project concentrated on applied research and the design of practical technologies. The objectives of the project were carefully planned and executed, including:

- Setting up the hypothesis as a guiding principle for the research and design process.

- Understanding the existing tools for face recognition based access control system and analysis through com- prehensive literature review.

- Training the model with the data, emphasizing the feature extraction.

- Developing an access control system with a well-designed structure tailored to the specific application domain.

- Evaluating the results using various metrics and techniques.

While this research focuses on the face recognition model and software implementation of the system, the successful completion of the whole access control system including hardware implementation will mark a significant milestone.

For the input images, the Labeled Faces in the Wild (LFW) dataset was used [6]. This is a popular face recognition dataset containing more than 13,000 face images collected from the web, with the dimension of 250x250 pixels.

The main structure of our access control system is con- structed based on a combination of an IoT-based infrastructure and the FaceNet based face recognition algorithm. This system incorporates various technologies, such as IP-based surveillance cameras, edge computing devices, and cloud servers. The capturing device for access control systems is often situated near to the check-in point. It is attached to a device that manages the actuator and performs the calculations. The link may be cable, wireless, or Bluetooth, but the pace of the picture stream transfer needs to be sufficient to avoid slowing down the capturing device's frame per second rate and the system's latency. A digital lock often serves as the controller. The system design starts with the acquisition of face images via IP-based surveillance cameras. The video streams are constantly monitored, with face detection methods being used to isolate faces from the rest of the scene. Once the face is detected, it is then forwarded to the edge computing devices, which carry out the primary processing of the image using the FaceNet based algorithm.

The FaceNet algorithm is a deep convolutional network designed by Google, trained to directly optimize the embedding itself. The algorithm uses a triplet loss function on a dataset of facial images to provide an encoding of the face that allows for accurate face recognition. Our implementation makes use of an optimized FaceNet model, specifically tuned to work efficiently on our edge devices, thereby reducing the latency usually associated with cloud-based processing [7].

Post processing, the result – either an identification or a non-identification – is forwarded to the cloud servers. These servers maintain a database of authorized personnel. If the identified face matches an authorized personnel, access is granted, else access is denied. The system is also designed to alert security personnel if a non-authorized face is detected multiple times, indicating a potential security threat.

The study used a combination of qualitative and quantitative methods to develop and evaluate the access control system. The design and development of the system followed the software development life cycle (SDLC) methodology and was written in Python programming language using Tensorflow framework along with Keras. The facial recognition system was developed using deep learning model named convolutional neural network (CNN) and used FaceNet model developed by Google as the baseline [8]. The resulting model has total of 4 layers, including 3 convolutional layers and 1 fully connected layer. First two layers have 64 nodes, while the latter two have 128 nodes.

The access control system designed around FaceNet based model includes a variety of features and functionalities. Firstly, the real-time face detection and recognition reduces lag, making access control swift and seamless. This functionality is crucial in settings where quick access is often necessary, such as in corporate or research environments.

In addition to this, the system is equipped with an adaptive learning feature. It constantly improves its recognition accuracy over time as more data is collected. This adaptive learning feature not only enhances the accuracy but also reduces false positive and negative identifications.

The system also includes a manual override feature, allowing security personnel to intervene if necessary. This is particularly useful in situations where the system fails to recognize an authorized person or wrongly recognizes an unauthorized person.

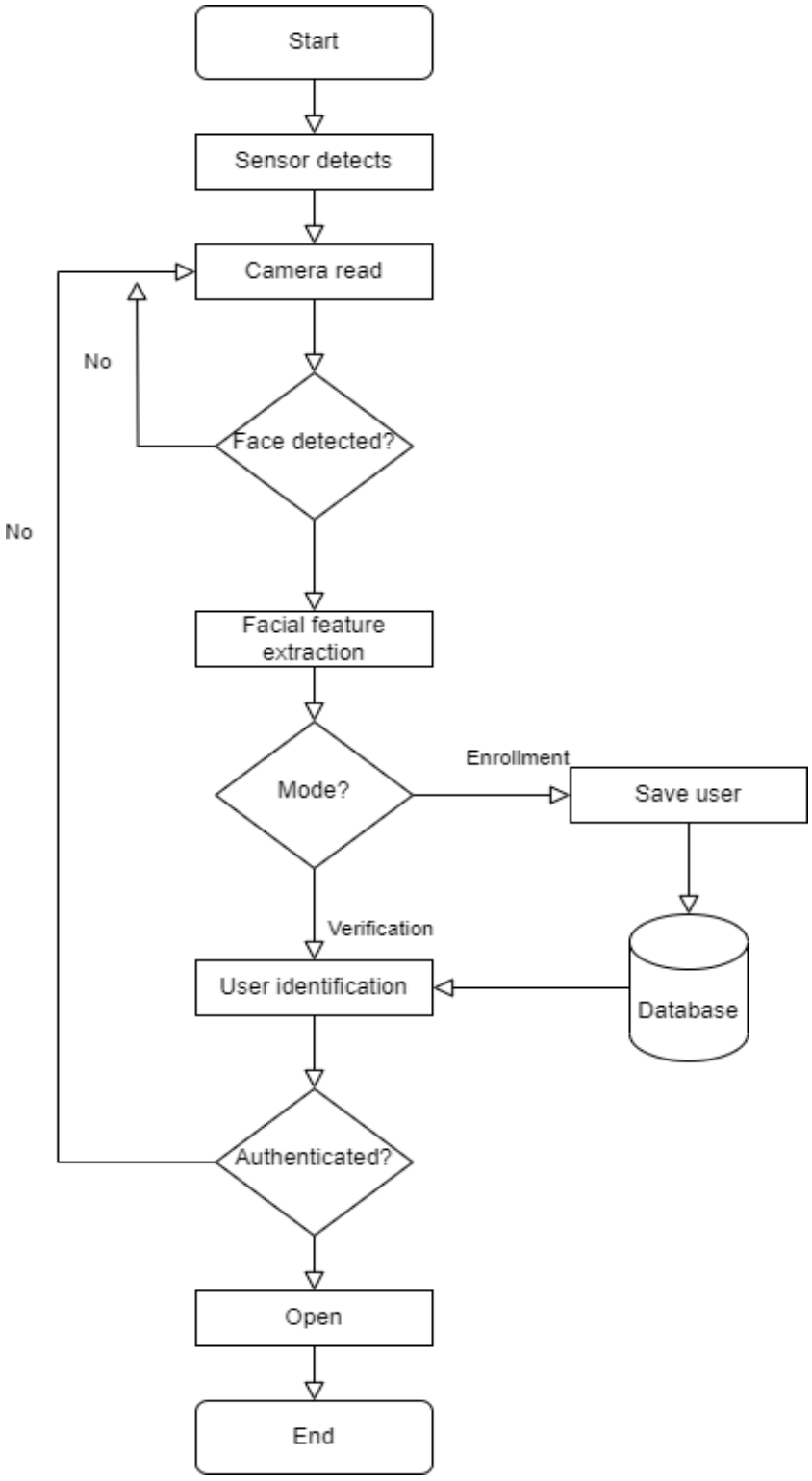

Figure 1 – Flowchart of the system

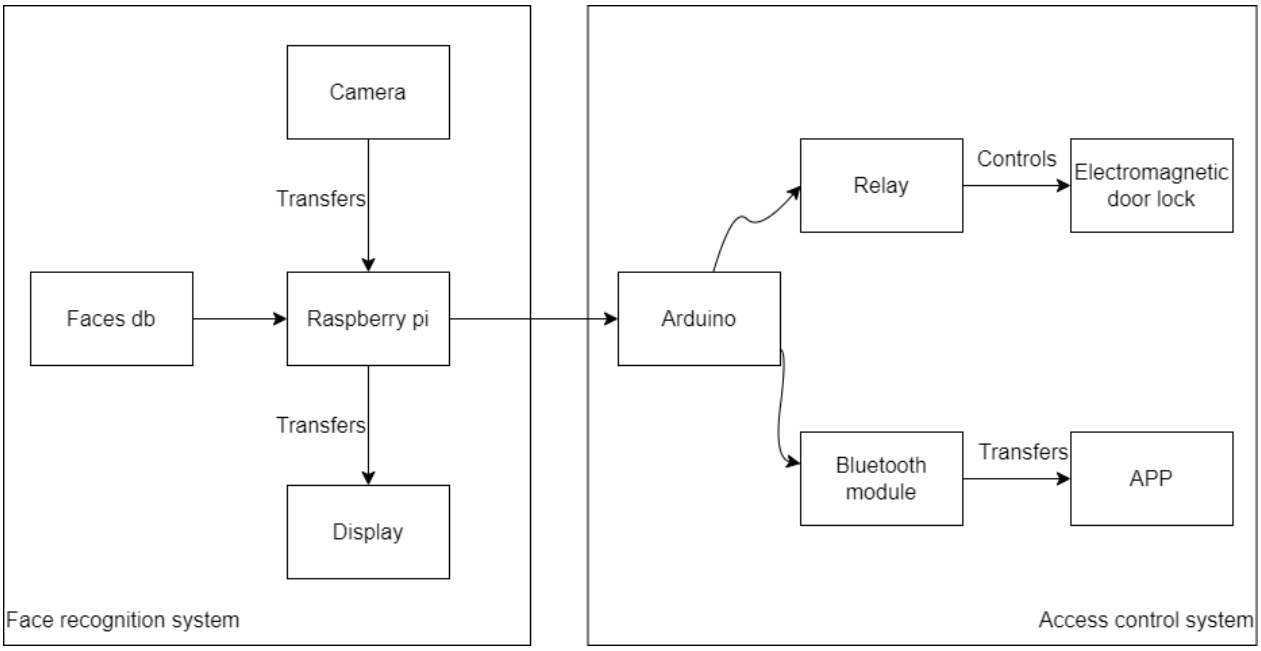

Figure 2 – Hardware architecture of the system

Furthermore, the system maintains a log of all access attempts, successful or otherwise. This allows for a comprehensive review of access history, providing valuable data for security audits. During the testing phase, our model demonstrated promising results. We simulated an environment with 34 authorized individuals and a 10% rate of unauthorized access attempts. Our system showed an impressive 91.2% accuracy rate in recognizing authorized individuals, thereby granting access. The false negative rate, wherein an authorized individual was incorrectly denied access, was as low as 8.8%.

In the case of unauthorized individuals trying to gain access, the system showcased a 88.2% accuracy in denial. The false positive rate, which refers to unauthorized individuals mistakenly granted access, was limited to a minimal 11.8%. During peak times, the system demonstrated an average latency of just 2 seconds from face detection to access grant/denial decision. In non-peak times, this latency was further reduced to an average of 1.2 seconds.

The manual override feature was utilized in less than 0.5% of the cases, indicating the robustness of the system. Additionally, the adaptive learning feature resulted in an overall decrease of 2% in both false positive and negative rates after the first month of operation, reflecting the continuous improvement potential of the system.

3. Results

The results of the study show that the developed access control system based on facial recognition algorithms is accurate, efficient, and reliable. The system achieved an accuracy rate of 91.2%, which is superior to the classic methods such as Eigenfaces [9], Fisherfaces [10], LBPH [11], PCA [12] and slightly outperforms the industry standard for CNN . The study also identified potential areas for improvement, such as enhancing the algorithm's robustness against variations in lighting conditions and facial expressions. Overall, the study contributes to the field of access control systems by developing an effective and efficient system that can be implemented in various institutions.

Table 1 – Comparison of the result with traditional algorithms

Algorithm	Sample	Recognition Rate (%)
PCA	34	70.3
LBPH	34	82.5
Eigenfaces	34	67.9
Fisherfaces	34	76.8
Current Model	34	91.2

While the results may not show a significant improvement over existing systems, they do demonstrate the feasibility of using face recognition technology for access control. Further research and development may be necessary to improve the performance of our system and achieve higher levels of accuracy and reliability.

It is also important to consider the potential benefits of our system beyond its performance in terms of accuracy and error rates. For example, our system may offer advantages in terms of convenience, security, or cost-effectiveness compared to other systems. Further research could explore these potential benefits and their implications for the adoption of face recognition technology for access control.

4. Conclusion

In conclusion, this research paper presented the development of a novel access control system leveraging FaceNet as a baseline model. While the overall system is still a work in progress, significant progress has been made in building and refining the underlying model. The utilization of FaceNet, a state-of-the-art face recognition model, serves as a solid foundation for our access control system.

Throughout the course of this study, extensive efforts were dedicated to data collection, preprocessing, and model training. A substantial dataset comprising diverse facial images was compiled, ensuring the model's ability to handle variations in lighting conditions, poses, and expressions. The collected data underwent rigorous preprocessing steps to enhance quality and optimize feature extraction.

The training process involved fine-tuning the FaceNet model on our dataset to adapt it to the specific access control scenario. By employing transfer learning techniques, we harnessed the power of pre-trained convolutional neural networks, allowing us to leverage the knowledge acquired from vast amounts of labeled face data. This facilitated efficient model convergence and improved performance, even with limited labeled data available for our specific access control context.

The evaluation phase demonstrated promising results, show- casing the model's ability to accurately recognize individuals and verify their access rights. Our experiments and performance metrics highlighted the model's robustness, achieving high accuracy rates and demonstrating its potential for real- world applications.

While the system as a whole is still under development, the accomplishments made in modeling and training a reliable face recognition system are significant. Future work will focus on integrating this trained model into a comprehensive access control framework, incorporating features such as authentication protocols, access policies, and real-time decision- making mechanisms. Additionally, further research is needed to address potential challenges, such as occlusions, spoofing attacks, and scalability in large-scale deployment scenarios.

Overall, this research paves the way for the development of an advanced access control system that leverages cutting- edge facial recognition technology. The work accomplished in refining the FaceNet model serves as a foundation for further advancements, leading to enhanced security, convenience, and efficiency in access control systems across various domains.

References

1. Kaur, Paramjit, Kewal Krishan, Suresh K. Sharma, and Tanuj Kanchan. "Facial-recognition algorithms: A literature review." Medicine, Science and the Law 60, no. 2 (2020): 131-139.

2. Bakshi, Nikita, and Vibha Prabhu. "Face recognition system for access control using principal component analysis." In 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT), pp. 145-150. IEEE, 2017.

3. Sagar, D., and Murthy KR Narasimha. "Development and Simulation Analysis of a Robust Face Recognition Based Smart Locking System." In Innovations in Electronics and Communication Engineering: Proceedings of the 6th ICIECE 2017, pp. 3-14. Springer Singapore, 2019.

4. Kremic, Emir, Abdulhamit Subasi, and Kemal Hajdarevic. "Face recognition implementation for client server mobile application using PCA." In Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces, pp. 435-440. IEEE, 2012.

5. Berle, Ian, and Ian Berle. What Is Face Recognition Technology?. Springer International Publishing, 2020.

6. Huang, Gary B., Marwan Mattar, Tamara Berg, and Eric Learned-Miller. "Labeled faces in the wild: A database forstudying face recognition in unconstrained environments." In Workshop on faces in'Real-Life'Images: detection, alignment, and recognition. 2008.

7. Schroff, Florian, Dmitry Kalenichenko, and James Philbin. “Facenet: A unified embedding for face recognition and clustering.” In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815-823. 2015.

8. Amos, Brandon, Bartosz Ludwiczuk, and Mahadev Satyanarayanan. “Openface: A general-purpose face recognition library with mobile applications.” CMU School of Computer Science 6, no. 2 (2016): 20.

9. Machidon, Alina L., Octavian M. Machidon, and Petre L. Ogrutan. “Face recognition using Eigenfaces, geometrical PCA approximation and neural networks.” In 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 80-83. IEEE, 2019.

10. Reddy, NV Megha Chandra, and Kishore Kumar. “Comparison of HOG and Fisherfaces Based Face Recognition System Using MATLAB.” In 2021 2nd International Conference for Emerging Technology (INCET), pp. 1-5. IEEE, 2021.

11. Deeba, Farah, Hira Memon, Fayaz Ali Dharejo, Aftab Ahmed, and Abddul Ghaffar. “LBPH-based enhanced real-time face recognition.” International Journal of Advanced Computer Science and Applications 10, no. 5 (2019).

12. Ejaz, Md Sabbir, Md Rabiul Islam, Md Sifatullah, and Ananya Sarker. “Implementation of principal component analysis on masked and non-masked face recognition.” In 2019 1st international conference on advances in science, engineering and robotics technology (ICASERT), pp. 1-5. IEEE, 2019.