International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 5, Sep-Oct 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Application of Machine Learning-Based Face Recognition Methods in Dormitory Access Control Systems

Ran Gong, Wenxi Li, Yueshan Wang

School of Information, Beijing Wuzi University, Beijing, China

ABSTRACT

Against the backdrop of smart campus construction, traditional access control systems in university dormitories are plagued by low efficiency and insufficient security, making face recognition technology a preferred solution for building intelligent access control systems.[1]

Focusing on the pain points of dormitory access control, this study first clarified requirements through research, then designed and implemented an embedded face recognition access control system, completing data collection and preprocessing, model training, development of a liveness detection module, and joint debugging and testing.[2] Tests indicate that the system demonstrates excellent recognition accuracy, real-time performance, and anti-counterfeiting capabilities. It effectively addresses the issues of traditional access control systems, provides a feasible solution for the intelligent management of university dormitories, and contributes to the informatization of education.

KEYWORDS: *face recognition, Dormitory Access Control*

How to cite this paper: Ran Gong | Wenxi Li | Yueshan Wang "Application of Machine Learning-Based Face Recognition Methods in Dormitory Access Control Systems" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-5, October 2025, pp.385-388, URL: www.ijtsrd.com/papers/ijtsrd97495.pdf

IJTSRD97495

1. INTRODUCTION

With the in-depth advancement of smart campus construction, campus security management is rapidly moving toward digitalization and intelligence. As a key area for students' daily life, the security management of dormitory entrances and exits serves as the first line of defense to protect students' personal and property safety. Traditional access control methods such as manual supervision or card-swiping have drawbacks including low efficiency, vulnerability to tailgating, and easy loss or theft of cards, which can hardly meet the comprehensive management needs of modern campuses for efficiency, convenience, and security.[3] Against this background, biometric recognition technology—especially face recognition technology, which features non-contact and high convenience—has become an ideal solution for constructing a new generation of intelligent access control systems.[4]

2. Face Recognition Technologies

Face recognition technology is an intelligent identity verification technology based on computer vision and biometric recognition. It analyzes face images or videos to extract unique biometric features (such as facial contour, texture information, etc.), and compares them with known face data in the database to realize the identification and verification of individual identities.[5] Its core technologies include face detection, feature extraction, feature matching, and other links, and it continuously improves recognition accuracy and efficiency by relying on deep learning algorithms (e.g., Convolutional Neural Network, CNN) and big data training.[6] With the optimization of algorithms and the enhancement of hardware computing capabilities, face recognition has been widely applied in scenarios such as security monitoring, financial payment, access control and attendance, and smart terminal unlocking, significantly improving the intelligence level of social management.

Face Detection: Definition: A technology that locates and extracts face regions from images/videos, serving as a prerequisite for face recognition.

Common methods: Haar feature cascade (strong real-time performance), MTCNN (multi-task cascade,

high positioning accuracy), YOLO series (based on target detection framework, balanced speed and accuracy).

Feature Extraction: Definition: The process of converting detected face images into low-dimensional, distinguishable numerical vectors (feature vectors).

Common methods: Principal Component Analysis (PCA, a classic dimensionality reduction method), Local Binary Pattern (LBP, resistant to light interference), Convolutional Neural Network (CNN, the mainstream in deep learning, capable of extracting high-level features).

Feature Matching: Definition: A technology that calculates the similarity between the feature vector of the face to be recognized and the face feature vectors in the database to determine whether they belong to the same person.

Common methods: Calculate the similarity between the feature vector of the face to be recognized and the face feature vectors in the database to determine whether they belong to the same person.

3. Dormitory Access Control System

The access control system for university dormitories is the first line of defense to ensure the security of the dormitory area. Traditional access control methods include manual management and card-swiping access control, both of which have drawbacks as shown in Table 1. Firstly, students often forget to bring or lose their access cards, and the reissue process is cumbersome. Secondly, the phenomenon of "one person swiping the card while multiple people follow" is difficult to eliminate, leading to serious security loopholes. Thirdly, manual identity verification by dormitory administrators is inefficient, which easily causes congestion at entrances and exits during peak hours, resulting in a poor user experience.

Management Method	Advantages	Disadvantages
Manual Management	Flexible handling of special cases, zero initial hardware cost, strong humanized communication capability	High long-term labor cost, low efficiency and easy congestion during peak hours
Traditional Electronic Access Control (IC Card)	Mature technology with low cost, fast recognition speed and high efficiency, electronic records facilitating management	IC cards are easy to lose and replicate, failing to ensure that the card matches the user

Table 1 Comparison of Advantages and Disadvantages of Current Dormitory Access Control Management Methods

4. Research and Methodology

4.1. Field Research

To accurately identify these pain points, the research team conducted in-depth field research in April 2025.[2] Through on-site visits, interviews with dormitory administrators, and continuous observation during peak hours for several days, we clarified the core requirements and design constraints of the system:

1. High-frequency Concurrent Processing: The absolute peak hours for access are 6:30–8:00 a.m. and 21:00–23:00 p.m. The system must have fast recognition capability to avoid long queues.
2. Adaptability to Complex Environments: It must effectively address issues such as insufficient lighting in corridors at night, dimness on rainy days, partial occlusion caused by students wearing masks/glasses, and image motion blur due to fast walking.
3. High Security: It must integrate an effective liveness detection function to firmly prevent fraudulent behaviors such as using printed photos or mobile phone videos.
4. Privacy Protection and Compliance: All collected face data must be stored in an encrypted manner, its scope of use must be strictly restricted, and students' informed consent must be obtained in advance, with the process complying with ethical standards.
5. Cost and Deployment Feasibility: The hardware cost of the system must be controlled within a reasonable range, and it should be easy to install and deploy without affecting the original structure of the dormitory building and normal access.[4]

4.2. Face Data Collection

Data Collection and Preprocessing Stage: This stage is the cornerstone of model training.[5] In strict accordance with the established plan, the project collected face data of on-campus students from May to July 2025, covering different time periods including morning peak (7:00–8:00), noon off-peak (12:00–13:00), and evening peak

(21:00–22:00). A multi-angle (frontal, side, upward, downward) strategy was adopted to simulate the real scenario of dormitory entrances and exits. After collection, the data was cleaned through a dual-process of "manual annotation + algorithm screening", with low-quality data (such as blurred images, over 50% facial occlusion, and abnormal postures) strictly removed. Finally, a high-quality, multi-scenario training dataset (with approximately 200 photos) was built, laying a solid foundation for subsequent model development.[2]

4.3. Implementation of Face Recognition Access Control System

4.3.1. Development Environment

In the hardware selection for the face-swiping system, the camera, as the core component, must meet requirements such as high resolution, wide dynamic range, and adaptability to low-light environments; the Raspberry Pi Camera Module 3 (wide-angle version) is recommended. For the face recognition processor/edge computing device, an edge computing device is suggested to reduce cloud dependence and improve real-time performance; the recommended model is Raspberry Pi 4B/5 equipped with Intel Movidiu. The storage device is used to store face feature data and recognition records; a hybrid local-cloud storage solution is recommended. For local storage, an ordinary surveillance-grade hard disk (single disk) can be used, with Seagate SkyHawk (1TB/2TB) recommended. The total budget for the above hardware is approximately 1,000 yuan.[2]

4.3.2. System Implementation Process

The face recognition access control system consists of 5 modules: hardware deployment, data collection, model training, system development, and joint debugging and testing. The implementation process of the system is shown in Figure 1. Firstly, the most cost-effective equipment is selected based on functions and budget; then face data is collected, and a face database is established through face image upload. Secondly, a face recognition framework is built: first, face image information is captured through a computer camera and corresponding face features are extracted; then liveness detection is performed on the extracted face images; finally, the extracted face information is compared with the previously built database, and the result is output.[2][3]

Figure 1 Flowchart of Face Recognition Access Control System Implementation

4.3.3. Model Training

The lightweight MobileFaceNet model was used, which adopts a depthwise separable convolution module. The research team initially mastered the methods for optimizing its computational complexity and parameter quantity. MobileFaceNet is a lightweight face recognition network designed for mobile/edge devices. Based on CNN optimization, it uses lightweight structures such as depthwise separable convolution, which can reduce the number of parameters and computational load while retaining the accuracy of face feature extraction, making it suitable for low-computing-power scenarios such as face-swiping access control. The depthwise separable convolution network itself is an efficient convolution structure, often used as a core component of lightweight networks. By splitting standard convolution into depthwise convolution (single-channel convolution) and pointwise convolution (1×1 convolution), it significantly reduces computational costs while maintaining feature extraction capabilities. In addition to MobileFaceNet, it is also widely used in models such as MobileNet.[6]

4.3.3.1. Face Image Acquisition

The system provides two methods for inputting face information. One is dynamic collection: the VideoCapture() function of the OpenCV library is called to capture the user's face video stream in real time through a connected camera, and high-quality frames are intercepted manually or automatically as input. The other is static import: it supports reading compliant face image files stored locally. All images must be bound to user identity information (e.g., student ID, name) and uploaded to the system's temporary database.

4.3.3.2. Data Preprocessing

Standardization: Unify the size (e.g., 112×112 pixels, as required by MobileFaceNet input), perform grayscale normalization, and align (correct posture through key points).

4.3.3.3. Face Feature Extraction

An improved MobileFaceNet model based on ArcFace loss was used as the feature extractor. This lightweight model processes the aligned face images and outputs 128-dimensional face feature vectors with high discriminability.

4.3.3.4. Construction of Face Feature Database

The extracted high-dimensional feature vectors are bound to the corresponding user identity information, encoded and stored using an efficient vector index

library, and finally a localized face feature database is formed.

4.4. Design of Face Recognition Module

The face recognition module is the core of the entire system, responsible for quickly and accurately identifying user identities in real-time video streams. The module is implemented through the following steps:[5][6]

4.4.1. Load the Recognition Model

The system uses the lightweight MobileFaceNet model as the main recognition network. This model has been pre-trained on a large-scale face dataset and fine-tuned on the self-built dataset to achieve the optimal balance between accuracy and speed, meeting the deployment requirements of embedded devices.

4.4.2. Real-time Feature Extraction and Matching

First, the module calls the face detection sub-module to obtain the face region in the current frame. Then, the image of this region is sent to the feature extraction network to obtain a 128-dimensional feature vector. Finally, by calculating the cosine similarity between this vector and all registered vectors in the feature database, the feature with the highest similarity and its corresponding identity information are identified.

4.4.3. Output of Recognition Results

The system presets a similarity threshold (e.g., 0.7). If the highest similarity exceeds this threshold, the recognition is determined to be successful, and the user's identity label is output; otherwise, it is determined to be an unknown person or a recognition failure. The recognition results (including face frame, identity information, and timestamp) will be displayed in real time and written into the database log.

5. Conclusion

This study designed and implemented an embedded face recognition access control system for university dormitories, and fully explored the application of face recognition technology in dormitory access control systems.[1][2][3] The system adopts a "dual cameras + lightweight model" architecture, realizes efficient face recognition through MobileFaceNet, and effectively improves security. Tests show that the system performs well in terms of recognition accuracy, real-time performance, and anti-counterfeiting capabilities, providing a feasible technical solution for the intelligent management of university dormitories. It not only demonstrates the powerful capabilities of Python in the field of computer vision but also shows how AI technology can bring practical changes to daily life. In the future, we look forward to building a more intelligent and secure campus environment through continuous optimization and innovation, contributing to the development of education informatization.

References

[1] Zhang, Y. H. (2025). Analysis of the application of access control systems based on face recognition technology in subways. Transportation Technology and Management, 6(17), 10-12.

[2] Huang, S. F., & Zhou, Q. (2025). Face recognition technology based on Raspberry Pi and its application. Digital Technology and Application, 43(08), 129-131.

[3] Lin, C. N., Zhou, W. X., & Huo, Q. (2024). Design and implementation of a face recognition system for security authentication. Information and Computers, 36(4), 159-162.

[4] Xie, X. H., Li, C. D., & Lai, J. H. (2022). A review of face liveness detection. Journal of Image and Graphics, 27(1), 63-87.

[5] Kaushik, S., Dubey, B. R., & Madan, A. (2025). Study of Face Recognition Techniques. International Journal of Advanced Computer Research (IJACR), 4(17).

[6] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823).