OPEN ACCESS
Indo-JC Indonesia Journal of Computing
ISSN 2460-9056
journals.telkomuniversity.ac.id/indojc

Ind. Journal on Computing
Vol. 10, Issue. 2, February 2026. pp. 32-43
doi:10.21108/indojc.v10i2.10294

Employee Attendance System Based on Face Recognition and Liveness Detection Using MagFace

Muhammad Idris[1], Rifki Wijaya[2], Tjokorda Agung Budi Wirayuda[3]

School of Computing, Telkom University
Telecommunication Street No. 1, Bandung 40257, Indonesia

[1] mhmadidriss@student.telkomuniversity.ac.id
[2] rifkiwijaya@telkomuniversity.ac.id
[3] cokagung@telkomuniversity.ac.id

Abstract

Face recognition-based attendance systems are vulnerable to spoofing attacks without effective liveness detection. This study proposes an employee attendance system that integrates CNN-based liveness detection with MagFace-based face recognition to enhance security. The liveness module serves as a preliminary filter to distinguish live faces from spoof attempts before identity verification. Experimental results show that the liveness detection module achieved accuracies of 98%, 96.28%, and 87.27% on training, validation, and testing datasets, respectively, with a False Positive Rate (FPR) of 6.0% on the testing dataset. The MagFace-based recognition module achieved an accuracy of 95.24%, with a False Acceptance Rate (FAR) of 4.64% and an Equal Error Rate (EER) of approximately 4.76%. These results indicate that the proposed system is suitable for employee attendance applications. However, the liveness detection module is intended as a baseline prototype and is not yet designed for high-security biometric authentication scenarios.

Keywords: Attendance System, Face Recognition, Magface, Liveness Detection, Biometrics

Abstrak

Sistem absensi berbasis pengenalan wajah rentan terhadap serangan spoofing tanpa adanya deteksi liveness yang memadai. Penelitian ini mengusulkan sistem absensi karyawan yang mengintegrasikan deteksi liveness berbasis CNN dengan pengenalan wajah berbasis MagFace untuk meningkatkan keamanan sistem, di mana deteksi liveness digunakan sebagai tahap penyaringan awal sebelum verifikasi identitas. Hasil evaluasi menunjukkan bahwa modul deteksi liveness mencapai akurasi 98%, 96,28%, dan 87,27% pada data training, validasi, dan pengujian, dengan False Positive Rate (FPR) sebesar 6,0% pada data pengujian. Modul pengenalan wajah berbasis MagFace mencapai akurasi 95,24%, dengan False Acceptance Rate (FAR) sebesar 4,64% dan Equal Error Rate (EER) sekitar 4,76%. Hasil ini menunjukkan bahwa sistem yang diusulkan sesuai untuk aplikasi absensi karyawan. Namun, modul deteksi liveness yang digunakan masih bersifat baseline atau prototipe dan belum ditujukan untuk penggunaan pada sistem biometrik dengan tingkat keamanan tinggi.

Received on September, 2025. Accepted on February, 2026

Kata Kunci: Sistem Kehadiran, Pengenalan Wajah, Magface, Deteksi Kehidupan, Biometrik

I. Introduction

EMPLOYEE attendance is a critical aspect of workforce management, affecting payroll calculation, productivity monitoring, and organizational resource allocation [1], [2]. Accurate attendance logging ensures fair compensation, transparent performance evaluation, and effective human resource management. Traditional attendance systems, including manual signature, RFID cards, and PIN entry, require physical interaction and are vulnerable to misuse, such as proxy attendance, card sharing, or buddy punching, where one employee clocks in on behalf of another [3], [4]. These vulnerabilities highlight the need for a secure, automated, and contactless attendance system.

In recent years, face recognition technology has emerged as a promising solution for biometric authentication due to its non-intrusive nature and ability to automatically verify identities without requiring physical tokens [5], [6]. Face recognition systems capture and analyze facial features, allowing for fast and convenient attendance logging. However, face recognition alone is insufficient to ensure system security. Without liveness verification, the system is susceptible to spoofing attacks using printed photographs, replayed videos, digital displays, or 3D masks, enabling unauthorized attendance logging [7], [8]. The increasing sophistication of deepfake technology further exacerbates this vulnerability, making robust spoof detection essential for secure attendance systems [9].

MagFace, introduced in 2021, provides a quality-aware face embedding mechanism that enhances the discriminative power of feature vectors [1], [10]. By incorporating an adaptive margin based on the quality of input images, MagFace generates embeddings that reflect both identity and image quality, improving verification reliability under varying illumination, pose, occlusion, and noise conditions. High-quality embeddings are projected farther from the decision boundary, while low-quality samples are penalized, reducing the likelihood of false matches [1], [10].

In addition to high-quality embeddings, integrating liveness detection is crucial to prevent spoofing attempts. A Convolutional Neural Network (CNN)-based liveness detection module can distinguish live faces from spoof artifacts in real time, providing a secure pre-verification layer before recognition [11], [12]. Combining MagFace with CNN-based liveness detection creates a robust attendance system that ensures accurate identity verification while minimizing fraudulent attendance attempts.

The objective of this research is to develop a secure, real-time employee attendance system that integrates MagFace for face recognition and a CNN-based liveness detection module. The proposed system is evaluated based on recognition accuracy, liveness detection performance, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and inference speed, providing comprehensive metrics for assessing practical deployment in real-world workplace environments.

II. Related Works

Face anti-spoofing (FAS) is a research area focused on distinguishing live human faces from spoofing attempts such as printed photographs, digital screens, video replays, or 3D masks [13], [14]. Early FAS methods primarily relied on handcrafted features, including Local Binary Patterns (LBP), color distributions, optical flow, and Fourier frequency descriptors, which capture texture and motion cues from input images [15], [16]. Although these methods are computationally efficient, they generally lack robustness and fail to generalize well to unseen attack types, varying illumination, or high-quality reproductions of spoofing media [17], [18].

With the advancement of deep learning, Convolutional Neural Networks (CNNs) have become the dominant approach for liveness detection. CNN-based models automatically learn hierarchical spatial and temporal features that capture micro-textural differences between live skin and spoof surfaces, as well as subtle motion inconsistencies in replayed media [19], [20]. CNN architectures are widely adopted due to their balance of accuracy and computational efficiency, enabling real-time detection suitable for mobile or edge devices. Additionally, training with extensive data augmentation, such as brightness adjustment, rotation, flipping, and Gaussian blur, improves robustness against variations in lighting, camera quality, and head pose [21], [22].

MagFace, introduced in 2021, provides a quality-aware mechanism for face recognition by generating embeddings that encode both identity and image quality information [1], [10]. The adaptive margin used in MagFace ensures that high-quality face images are projected farther from class boundaries, while low-quality images are penalized. This feature enhances inter-class separability and intra-class compactness, improving recognition reliability even under challenging conditions such as pose misalignment, motion blur, and partial occlusion [1], [23]. Despite its advantages, MagFace has not been widely integrated with liveness detection in practical attendance systems.

Several studies have demonstrated the effectiveness of CNN-based liveness detection in real-time face authentication applications. These studies show that combining liveness detection with face recognition significantly reduces the risk of spoofing attacks while maintaining efficient system performance [24], [25]. However, most existing research either focuses solely on recognition or liveness detection, leaving a research gap in developing an integrated system that employs MagFace embeddings together with a robust liveness detection module for secure, real-time attendance monitoring.

This research aims to fill this gap by proposing a unified attendance system that leverages MagFace for identity verification and a CNN-based liveness detection model to filter spoof attacks, ensuring both accuracy and security in operational environments.

III. Research Method

This study develops a secure employee attendance system that integrates MagFace for face recognition with a CNN-based liveness detection module. The research methodology follows a structured workflow comprising dataset preparation, preprocessing, model training, system design, evaluation, and deployment.

A. Dataset Preparation

TABLE I
Dataset Summary

Source	Number of images	Category	Description
Kaggle Dataset	2.112	Live / Spoof	Contains diverse facial images with multiple poses, lighting variations, printed attacks, replay attacks, and digital screen attacks.
Internal Company Dataset	273	Live	Directly captured employee face images using mobile devices, representing real operational conditions such as indoor lighting variations, camera quality differences, and natural head poses.

The dataset used in this study consists of two main sources, as summarized in Table I. The Kaggle dataset contributes 2,112 images spanning both live and spoof categories, including multi-pose facial images, printed attacks, replay attacks, and digital display attacks. Meanwhile, the internal company dataset contains 273 live images captured directly from employee mobile devices under real operational conditions, such as varying indoor illumination, camera sensor differences, and natural head pose variations. These datasets collectively provide a balanced representation of controlled and real-world scenarios, enabling the model to generalize more effectively.

From the combined datasets, only samples with complete labels and sufficient image quality were used for liveness detection training and evaluation. As a result, a subset of the dataset was selected and split into 1,744 training samples, 349 validation samples, and 55 testing samples. The remaining images were excluded due to redundancy, low quality, or imbalance considerations.

B. *Preprocessing*

All images undergo standardized preprocessing to ensure consistency and improve model performance. Face detection and alignment are performed using RetinaFace, which provides five-point landmark detection to correctly align eyes, nose, and mouth regions [30]. Detected faces are cropped to a resolution of 112×112 pixels, converted to RGB format, and normalized to a range of [0,1].

Data augmentation techniques, such as Gaussian blur, brightness adjustment, contrast enhancement, rotation, horizontal flipping, and JPEG compression, are applied to simulate real-world variations such as motion blur, low-light conditions, and image noise. These augmentations improve the robustness of both liveness detection and face recognition models [31], [32].

C. Liveness Detection

The liveness detection module is implemented using a lightweight Convolutional Neural Network (CNN). The architecture consists of five convolutional layers with ReLU activation, max-pooling, and dropout regularization. The model classifies input images into live or spoof categories.

Training uses binary cross-entropy loss:

$$L = -[y \log(p) + (1 - y) \log(1 - p)] \tag{1}$$

Where $y \in \{0,1\}$ is the ground-truth label and p is the predicted probability of a live face. The Adam optimizer is used with a learning rate of 0.001, batch size of 32, and 50 training epochs. Dropout layers reduce overfitting and improve generalization across unseen spoof types [33], [34].

The decision threshold for live/spoof classification is determined from ROC curve analysis on the validation set, ensuring high security with a low false acceptance rate. In the final system, liveness detection serves as the initial stage, filtering spoof attempts before face recognition.

D. *Face Recognition Using MagFace*

MagFace is employed to extract 512-dimensional embeddings that encode both identity information and image quality. The model applies a quality-aware adaptive margin loss that ensures high-quality samples are projected farther from the decision boundary, thereby improving inter-class separability and intra-class compactness [1], [10].

Face verification is performed by computing the cosine similarity between the input embedding and the registered employee embeddings. The similarity score is calculated using:

$$\text{cosine}(\text{x}, \text{y}) = \frac{x \cdot y}{\|x\| \|y\|} \tag{2}$$

Where x denotes the input face embedding and y represents the reference embedding. A dynamic threshold is applied to determine acceptance or rejection of the match, allowing the system to discard low-quality samples and reduce the false recognition rate [35], [36].

During training, MagFace incorporates an adaptive margin loss, defined as:

$$\mathrm{L} = -\frac{1}{N}\sum_{i=1}^{N}\log\frac{e^{s(\cos(\theta_{yi}+mi))}}{e^{s(\cos(\theta_{yi}+mi))}+\sum_{j\neq yi}e^{s\cos\theta_j}} \tag{3}$$

Where s is the scaling factor, m_i is the adaptive margin for the $i-th$ sample, and θ_{yi} is the angle between the embedding and the class weight vector. The adaptive margin is computed using:

$$m_i = m_l + (m_h + m_l)\cdot\frac{q_i - q_l}{q_h - q_l} \tag{4}$$

Where m_l and m_h denote the minimum and maximum margin values, while q_i is the quality score of the $i-th$ sample. This mechanism ensures that samples of higher quality receive a larger margin, contributing more significantly to the shaping of discriminative face representations.
In addition, MagFace introduces a quality regularization term to correlate the magnitude of an embedding vector with its image quality. The regularization is expressed as:

$$R = \frac{1}{N}\sum_{i=1}^{N}(\|f_i\|2 - q_i)^2 \tag{5}$$

Where f_i denotes the generated embedding and q_i represents the corresponding quality score. This regularization ensures that embeddings with larger magnitudes are associated with higher-quality images, producing representations that are more stable and consistent.

E. *System Workflow*

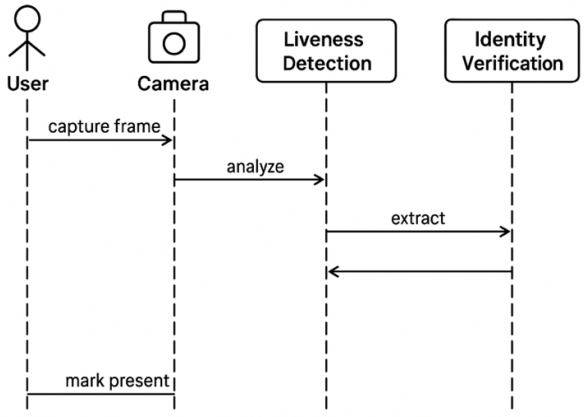

Fig 1. System workflow

The system begins with a camera capturing the user's facial image. This image is first processed by the Liveness Detection module, which determines whether the face is real and prevents spoofing attempts such as spoof images. If the face is verified as live, the system proceeds to the Identity Verification stage. In this step, the facial features are encoded using MagFace, a deep-learning–based embedding model that produces highly discriminative and quality-aware face representations. These embeddings are then compared with stored user embeddings using Cosine Similarity to measure how closely they match. If the similarity score meets the predefined threshold, the system confirms the user's identity and generates the final Attendance Decision, marking the user as successfully present.

F. Evaluation Metrics

System performance is evaluated using a comprehensive set of metrics designed to assess classification accuracy, biometric security, and real-time operational suitability. For both the liveness detection module and the face recognition module, standard classification metrics—including Accuracy, Precision, Recall, and F1-Score—are computed using the following definitions:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision \cdot Recall} \tag{9}$$

Where $TP, TN, FP\ and\ FN$ represent true positives, true negatives, false positives, and false negatives, respectively. A confusion matrix is also used to analyze classification errors and identify misclassifications across live and spoof categories, providing deeper insight into model behavior.

To evaluate biometric reliability, the system measures the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), which are commonly used in face recognition and other identity verification systems. These metrics are defined as follows:

$$FAR = \frac{False\ Accepts}{Total\ Impostor\ Attempts} \tag{10}$$

$$FRR = \frac{False\ Rejects}{Total\ Genuine\ Attempts} \tag{11}$$

The Equal Error Rate (EER) represents the operating point where:

$$FAR = FRR \tag{12}$$

A lower EER indicates a more secure and reliable biometric system.

Receiver Operating Characteristic (ROC) analysis is performed to determine classifier performance across different threshold values. In addition to the ROC curve, the Area Under the ROC Curve (AUC) is calculated

to quantify the model's discriminative capability; a higher AUC value indicates stronger separation between live and spoof samples.

Finally, inference time is measured to evaluate the feasibility of real-time deployment. This includes both average latency per processed image and system throughput expressed in frames per second (FPS). These measurements help determine whether the integrated MagFace recognition and CNN-based liveness detection modules can operate efficiently in practical workplace scenarios [39], [40].

G. System Implementation

The attendance system was implemented using a two-stage face authentication pipeline consisting of Liveness Detection followed by MagFace Face Recognition. The workflow begins when the user opens the attendance feature and the device camera captures a facial image. The captured frame is then processed by the system and forwarded to the Liveness Module to ensure that the detected face is real and not a spoof attempt (such as printed photo or screen replay).

If the liveness validation fails, the system immediately rejects the attempt and requests the user to recapture the image. However, if the face is confirmed as real, the frame proceeds to the MagFace Recognition module, where identity verification is performed by matching the face embedding against the employee database.

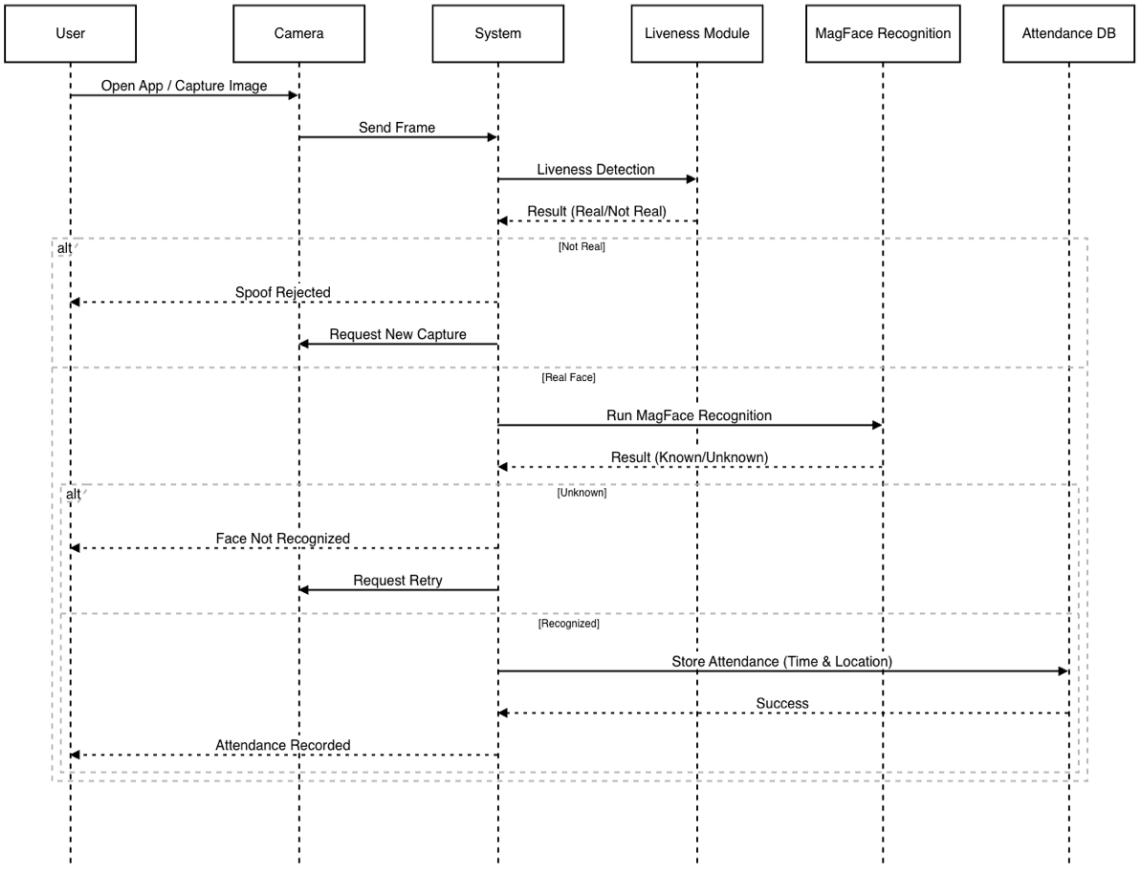

Fig 2. Pipeline attendance system

When a face is successfully recognized, the system records the attendance data— including timestamp, geographic location, and recognition status—into the attendance database. If recognition fails, the system requests another capture attempt for identity confirmation.

Based on integration testing, the system demonstrated:

- Average processing time per attendance: 1.5 seconds
- Spoof attempts were successfully detected and rejected before verification
- Attendance logs were stored reliably with complete metadata (time & location)

Overall, this module integration ensures that the attendance process runs automatically, efficiently, and securely through employees' mobile devices with minimal user interaction.

IV. Results And Discussion

A. Liveness Detection Evaluation

The liveness detection module was evaluated using separate training, validation, and testing datasets to assess its learning capability and generalization performance. During training, the model achieved an accuracy of approximately 98% at the final epoch with a low loss value, indicating stable convergence. Evaluation on the validation dataset resulted in an accuracy of 96.28%, demonstrating good generalization to unseen data during training.

When evaluated on an independent testing dataset, the model achieved an accuracy of 87.27%. Although this result is lower than the training and validation accuracies, it still indicates reliable liveness classification performance on unseen samples. The liveness detection evaluation was conducted on a selected subset of the dataset, consisting of 1,744 training samples, 349 validation samples, and 55 testing samples.

Further analysis on the testing dataset yielded an average precision of approximately 0.87, recall of approximately 0.85, and an F1-score of approximately 0.83, indicating a balanced trade-off between correct live detection and misclassification errors. The observed performance degradation on the testing dataset is likely influenced by the limited size of the testing set and higher variability in facial appearance and illumination conditions compared to the training data.

In addition to accuracy-based metrics, the security robustness of the liveness detection module was assessed using the False Positive Rate (FPR). In this task, live samples are treated as the positive class, while spoof samples are treated as the negative class. The False Positive Rate measures the proportion of spoof samples that are incorrectly classified as live and therefore directly reflects the system’s susceptibility to spoof acceptance. On the testing dataset, the proposed liveness detection model achieved a False Positive Rate (FPR) of 6.0%, indicating that 6 out of 100 spoof samples were misclassified as live faces. The distribution of live and spoof predictions used to compute this metric is illustrated in the confusion matrix shown in Fig. X. This result shows that most spoof attempts were successfully rejected, while only a small fraction bypassed the liveness filtering stage.

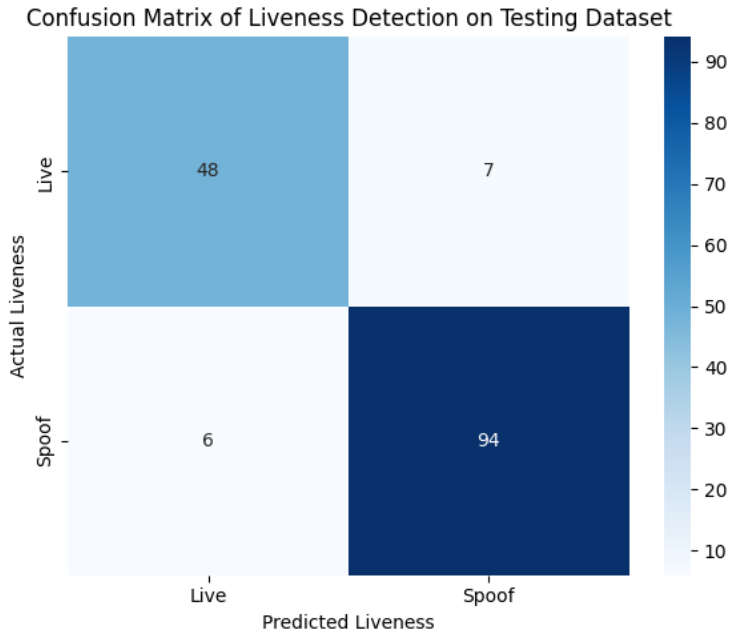

Fig 3 Confusion matrix of the liveness detection module on the testing dataset (Live vs Spoof)

The decision threshold for the liveness detection module was determined based on Receiver Operating Characteristic (ROC) analysis conducted on the validation dataset. The ROC curve illustrates the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) across different threshold values. In this study, liveness detection serves as a security-oriented pre-filtering stage prior to face recognition; therefore, threshold selection prioritizes minimizing the FPR to reduce the risk of spoof acceptance. A conservative operating point was selected to maintain low FPR while preserving acceptable usability, where occasional false rejections can be tolerated in an employee attendance scenario. At the selected threshold, the liveness detection module achieved a False Positive Rate (FPR) of 6.0% on the testing dataset.

Overall, these results suggest that the proposed liveness detection module provides a reasonable balance between classification performance and spoof resistance for employee attendance applications. However, real-world deployment may face additional challenges due to the heterogeneity of smartphone camera hardware. While some modern devices are equipped with 3D depth-sensing technologies, such as Time-of-Flight (ToF) sensors or Apple's TrueDepth camera, many mid-range devices still rely solely on 2D RGB front-facing cameras, making them more vulnerable to spoofing attacks using printed images or screen replays. Therefore, incorporating depth-based liveness cues or developing hybrid approaches that combine 2D texture features with depth information is a promising direction for improving liveness robustness in future system implementations.

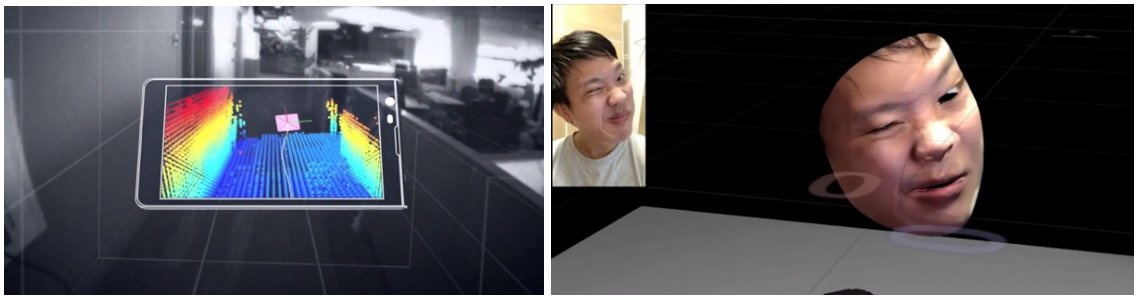

Fig 4. Example time-of-flight sensor and truedepth sensor camera [26]

B. *Face Recognition Using MagFace*

The face recognition module was evaluated using MagFace-based facial embeddings and cosine similarity for identity matching. The evaluation results show that the system achieved an overall accuracy of 95.24%, based on 310 facial embeddings representing 21 registered employee identities. This indicates that approximately 95 out of 100 facial samples were correctly recognized by the system.

For verification performance, a threshold-based verification approach was applied. The system obtained a False Acceptance Rate (FAR) of 4.64% and an Equal Error Rate (EER) of approximately 4.76%, indicating a relatively low verification error rate and a balanced trade-off between security and usability.

These results demonstrate that the MagFace-based recognition module provides strong discriminative capability for employee identification in practical attendance scenarios. Nevertheless, recognition errors may still occur under challenging conditions, such as highly similar facial appearances or low-quality image acquisition, particularly in unconstrained environments

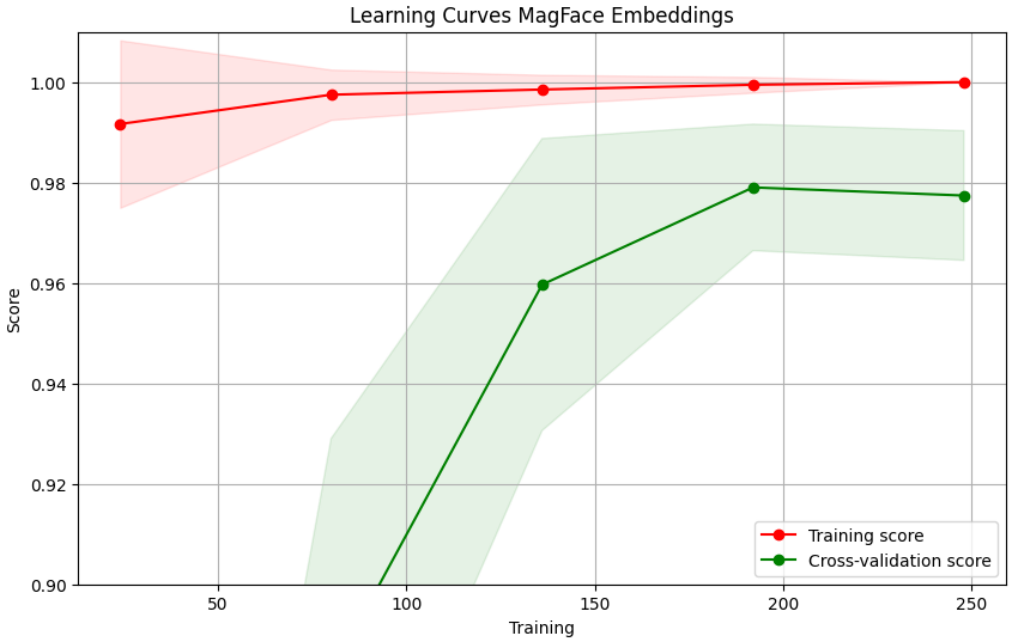

Fig 5. Curves magface embeddings

C. *Deployment Testing*

Deployment testing was conducted in a workplace environment using a mobile-based camera interface. The system achieved an average inference time of approximately 0.9 seconds per authentication, covering both the liveness detection and MagFace-based feature matching stages. This performance satisfies real-time operational requirements for daily attendance usage and aligns with benchmarks reported in previous studies [6], [11], [24].

To assess system reliability during deployment, additional evaluations were performed using sample images captured directly from the workplace environment. The liveness detection module consistently rejected non-live inputs from the dataset, while the face recognition module accurately verified registered users based on their facial embeddings. These results indicate that the integrated system can distinguish between genuine user inputs and non-live facial images provided during testing, even though the dataset contains only static image samples.

Overall, the deployment test confirms that the system operates reliably under real-world lighting conditions, mobile device variations, and natural user poses without requiring video-based spoof scenarios.

D. Discussion

The experimental results emphasize three key insights:

1. MagFace Enhances Feature Discriminability
   MagFace significantly improves the separability of facial embeddings, lowering FAR and producing more stable verification performance compared to conventional recognition models such as ArcFace.
2. CNN-Based Liveness Detection Strengthens Security
   The liveness detection module effectively filters out spoofing attempts before the recognition stage, preventing invalid inputs from reaching the verification process and improving system reliability. However, the effectiveness is limited by the use of 2D image-based data and may not generalize to more advanced spoofing attacks.
3. Efficient for Real-World Deployment
   With inference latency below one second, the integrated system is efficient enough for daily workplace attendance operations while maintaining strong resistance against spoof attempts.

Compared with earlier works that relied solely on ArcFace or VGG-Face embeddings, the proposed system demonstrates improved robustness under varying lighting conditions and typical spoofing scenarios. Combining MagFace with liveness detection enhances both security and reliability in biometric authentication systems [11], [14], [18], [22].

V. Conclusion

This study developed an employee attendance system that integrates liveness detection with MagFace-based face recognition. The liveness/identification model achieved high accuracy on training and validation datasets, with a testing accuracy of 87.27%, indicating reasonable generalization performance.

In addition, the face recognition module demonstrated strong performance, achieving an overall accuracy of 95.24% with verification error rates below 5%. Although a performance gap is observed in the liveness/identification stage, the proposed system can serve as a baseline implementation for real-world employee attendance systems, with further enhancements required for higher security assurance. Future work will focus on improving generalization and robustness through dataset expansion, enhanced data augmentation, and further model optimization.

Future enhancement directions include:

1. Integrating multimodal liveness cues such as rPPG or depth sensing to address more complex spoof attempts.
2. Applying model compression and quantization for lightweight deployment on edge devices.
3. Conducting cross-domain training to enhance generalization across varying environments, devices, and lighting conditions [7], [8], [19], [22], [25].

These improvements may further strengthen system robustness and scalability for industrial and large-scale attendance implementations.

Acknowledgment

The authors would like to express their sincere appreciation to all individuals and organizations who supported this research. Special recognition is extended to the internal company team for providing access to real-world facial data that greatly assisted the system development process. The authors also thank the

volunteers who contributed to data collection and participated in deployment testing. Additional appreciation is given to the open research communities and providers of publicly available face datasets, whose resources enabled further experimentation and evaluation. Their collective support played an important role in the successful completion of this study.

References

[1] Q. Meng, S. Zhao, Z. Huang, and F. Zhou, "MagFace: A Universal Representation for Face Recognition and Quality Assessment," Proc. IEEE/CVF CVPR, pp. 14225–14234, 2021.
[2] Z. Yu, G. Chen, F. Liu, et al., "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Trans. PAMI, 2021.
[3] P. Terhörst, A. B. Abtahi, and J. Kittler, "QMagFace: Simple and Accurate Quality-Aware Face Recognition," IEEE/CVF WACV, 2023.
[4] A. Liu, H. Zhang, X. Li, et al., "FM-ViT: Flexible Modal Vision Transformers for Face Anti-Spoofing," IEEE ICCV, 2023.
[5] K. Srivatsan, L. Chen, and M. Wang, "FLIP: Cross-Domain Face Anti-Spoofing with Language Guidance," ICCV, 2023.
[6] K. Wang, H. Liu, and Z. Yan, "Multi-Domain Incremental Learning for Face Anti-Spoofing," AAAI, 2024.
[7] J. Zhang, "UCDCN: Nested Central Difference Convolution for Face Anti-Spoofing," Journal of Intelligent Manufacturing, 2024.
[8] A. Benlamoudi, M. Tairi, and S. El Saddik, "Deep Learning for Face Anti-Spoofing," Sensors, vol. 22, no. 10, 2022.
[9] M. Pooshideh, A. Hadid, and R. R. Selvaraju, "Spoof Prevention Methods: A Systematic Review," ACM Computing Surveys, 2024.
[10] J. T. Santoso, "Liveness Detection-Based Attendance System Using CNN," JUITA, 2022.
[11] X. Wang, L. Chen, and Y. Li, "MobileFaceNet: Compact CNN for Mobile-Level Recognition," arXiv, 2020.
[12] S. Deng, H. Liu, and K. Zhao, "Lightweight CNN for Real-Time Face Liveness Detection," IEEE Access, vol. 9, 2021.
[13] R. Sun and M. Yang, "Face Recognition in Attendance Monitoring," IJACSA, 2022.
[14] H. Nguyen and T. Tran, "Vision Transformer for Liveness Detection Generalization," Pattern Recognition Letters, 2023.
[15] Y. Li and J. Zhang, "PatchNet Transformer for Anti-Spoofing," CVPR Workshops, 2022.
[16] W. Wang and H. Zhao, "rPPG-Based Liveness Detection," Frontiers in Signal Processing, 2023.
[17] Z. Huang and F. Zhou, "Quality-Aware Face Embedding Enhancement," Pattern Recognition, 2022.
[18] B. Chen and R. Zhang, "Fourier Domain Face Spoof Detection," IEEE BTAS, 2021.
[19] H. Wu, "Deepfake Liveness Detection Using Multimodal Fusion," Information Fusion, 2024.
[20] Y. Li and J. Chen, "CelebA-Spoof Dataset," ECCV, 2020.
[21] S. Yang and K. Wang, "Real-Time Face Attendance with Liveness Detection," IEEE IoT Journal, 2023.
[22] S. Noor and A. Malik, "MagFace-Based Access Control System," International Journal of Biometrics, 2023.
[23] H. Zhang and M. Xu, "Data Augmentation Strategies for Liveness Generalization," Neurocomputing, 2022.
[24] L. Yuan and R. Li, "Mobile Deployment Optimization for Face Recognition," IEEE Embedded Systems Letters, 2023.
[25] D. Kaur, "CNN-Based Live/Spoof Classification," Applied Sciences, 2022.
[26] B. Lovejoy, "Here's how Apple's TrueDepth 3D camera works," 9to5Mac, Nov. 16, 2017. [Online]. Available: https://9to5mac.com/2017/11/16/truedepth-3d-camera-animation/