Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

Design of an intelligent residential access control system using YOLO-based facial recognition: application to a three-entry dwelling

MBO NKETA OLGA BRAVO, OKITAKOY MANYA SYLVADOR, NEKA MUKENDI HENRY, MUKUNA WA MUKUNA FADER

Affiliation: National Pedagogical University, Faculty of Sciences, Department of Mathematics, Statistics and Computer Science, Kinshasa, Democratic Republic of Congo

DOI: https://doi.org/10.5281/zenodo.22799409

Published Date: 16-September-2026

Abstract: **Securing homes is a major challenge in a context where traditional key-, badge-, or code-based opening systems have intrinsic vulnerabilities: loss, copying, or unauthorized sharing. This work proposes the design of an intelligent residential access control system based on computer vision and facial recognition, intended for a family dwelling with three distinct access points: a back door, a veranda door, and a central door. The system is designed to recognize six pre-registered authorized individuals. The proposed approach relies on a hybrid architecture combining YOLO for fast face detection in images acquired by cameras installed at the three access points, a facial feature extraction module based on deep representations, and a decision mechanism incorporating a confidence threshold. After detection, facial regions are normalized and then submitted to a recognition module to identify the person. When the identity matches one of the six authorized individuals and the confidence level exceeds a predefined threshold, an opening recognized command is transmitted to the electromechanical mechanism of the concerned door. Otherwise, access is denied and a security event is recorded. The proposed evaluation relates to accuracy, precision, recall, F1-score, false positive rate, false rejection rate, and response time. The envisioned system thus constitutes a contactless, automated access control solution adaptable to multiple entry points of a single dwelling.**

Keywords: **artificial intelligence, facial recognition, YOLO, computer vision, access control, deep learning, residential security, liveness detection.**

1. INTRODUCTION

Home security has traditionally relied on mechanisms such as mechanical locks, keys, padlocks, access codes, and electronic cards. While these solutions are widely used, they have inherent limitations: a key can be lost or copied, a code can be given to an unauthorized person, and a badge can be stolen. Advances in artificial intelligence and computer vision now offer the possibility of developing systems capable of automatically identifying a person from their face.

Facial recognition is an important branch of computer vision. Modern systems use deep learning methods to extract distinguishing facial features and determine a person's identity. The literature shows that these techniques are used in several fields, including video surveillance and building access control (Guo & Zhang, 2019; Wang & Deng, 2021).

In this context, the present work focuses on the design of an intelligent system to secure a house with three access points. The house has a back door, a door on the veranda, and a central door. Six people are authorized to use these access points. The originality of the proposal lies in the integration of a YOLO model for rapid face detection with a recognition module to identify authorized individuals. YOLO is particularly well-suited to applications requiring real-time detection, as it simultaneously provides the location and class of detected objects (Redmon et al., 2016). Modern YOLO implementations also allow training on custom datasets and inference on images or video streams.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

The overall objective is to design an architecture capable of automatically determining whether a person standing in front of one of three doors belongs to the group of six authorized individuals. This article is organized as follows: Section 2 presents the problem and research questions; Section 3 details the objectives; Section 4 formulates the hypothesis; Section 5 describes the general system architecture; Sections 6 through 8 present, respectively, the YOLO detection, the recognition module, and the database; Section 9 formalizes the decision-making process; Section 10 deals with the management of the three doors; Sections 11 through 13 address the hardware, the algorithm, and the experimental evaluation; Section 14 presents an example of results; Section 15 discusses security aspects and limitations; and finally, Section 16 concludes and proposes future directions.

2. PROBLEM STATEMENT

In a dwelling with multiple entrances, security management becomes more complex when several people need to be able to enter without using physical keys. The main question of this study is therefore:

How can we design an intelligent system capable of automatically recognizing the six authorized people and controlling the opening of one of the three doors of a dwelling using facial recognition based on artificial intelligence?

The following specific questions arise from this main question:

- Can YOLO accurately detect a person's face in front of a door?
- Can the system distinguish between the six authorized people?
- What level of accuracy can be achieved under different lighting conditions?
- How long does it take to make an access decision?
- How do you deal with a stranger?
- How can I automatically control the lock on each of the three doors?

3. OBJECTIVES

3.1. General objective

Design an intelligent residential access control system based on facial detection and recognition to automatically authorize entry for six registered individuals into a dwelling with three doors.

3.2. Objectives specific

1. Create a database of facial images of the six authorized individuals;
2. Train or adapt a YOLO model to detect faces;
3. Develop a module to identify each person;
4. Define a confidence threshold for access authorization;
5. Integrate the system into the three doors of the house;
6. Control the locks electronically;
7. Record authorized and denied access attempts;
8. Evaluate the system's performance.

4. HYPOTHESIS

The main hypothesis formulated in this study is as follows:

Integrating a YOLO model for face detection into a facial recognition module would automate access control to the three doors of a home while offering a level of accuracy and response time compatible with residential use.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

5. GENERAL SYSTEM ARCHITECTURE

The proposed system is organized into several sequential steps:

Camera → YOLO face detection → Face extraction → Identity recognition → Authorization verification → Lock control → Open/deny

The three entrances are equipped with cameras: Camera 1 is dedicated to the rear door; Camera 2 to the veranda door; and Camera 3 to the main door. The central system receives the images from the cameras and processes the detected faces.

The same process is applied to all three doors. The functional architecture relies on a computer vision pipeline that integrates:

1. **Image acquisition** : capture by RGB camera;
2. **Facial detection** : face localization by YOLO;
3. **Feature extraction** : transformation of the normalized face into an embedding vector ;
4. **Recognition** : comparison of the embedding with the gallery of authorized faces;
5. **Decision** : application of a confidence threshold to allow or deny access;
6. **Actuation** : control of an electromechanical relay via microcontroller.

6. YOLO FACE DETECTION

YOLO stands for "You Only Look Once." It is a family of computer vision models designed to perform real-time object detection. In the proposed system, YOLO should not be considered the entire facial recognition process. Its primary role is to answer the question: "Where is the face in the image?" Recognition then takes over to answer the question: "Whose face does this belong to?"

The outputs of a YOLO detector include, among other things, the bounding box coordinates, the detected class, and a confidence score. In this project, the model can be trained on a main class: **Class = face** .

An image containing a person can thus produce: Face, Confidence = 0.96, Coordinates = $[x_1, y_1, x_2, y_2]$.

The detected face is then passed to the recognition module. The modern YOLO architecture (YOLOv8, YOLOv9, YOLOv10, YOLOv11) is based on advanced architectural principles: anchor-free design , C2PSA (Cross-Stage Partial with Spatial Attention) blocks for YOLOv11, gradient optimization for YOLOv9, and a balance between accuracy and computational efficiency for YOLOv10. Table 1 summarizes the comparative performance of the different YOLO versions on face and object detection tasks.

Table 1: Comparative performance of YOLO architectures on detection tasks

Model	mAP50 (mask detection)	mAP50 (human detection)	Reference
YOLOv8	0.924	—	Rahman et al., 2024
YOLOv9	0.941	0.812	Wang et al., 2024
YOLOv10	0.950	0.829	Wang et al., 2024
YOLOv11	0.962	0.854	Khanam & Hussain, 2024
YOLOv12	Superior in latency and accuracy	—	Karakuş et al., 2025

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

The work of Karakuş et al. (2025) on the WIDER FACE dataset demonstrates that optimized YOLO architectures (YOLOv8, YOLOv10, YOLOv12) achieve superior performance in accuracy, recall and inference speed for facial detection in forensic conditions, with YOLOv12 offering the best latency and accuracy scores.

7. RECOGNITION OF THE SIX PEOPLE

The system database contains six authorized people: Person 1, Person 2, Person 3, Person 4, Person 5, Person 6.

For each person, several photographs are collected with different facial orientations, expressions, and lighting conditions. Facial recognition can be organized according to the following principle:

$$I \rightarrow D \rightarrow F \rightarrow C$$

Or :

- Iacquired image ;
- D= face detected by YOLO;
- Fextracted facial features ;
- C= recognized identity.

Modern facial recognition systems typically rely on extracting digital representations of the face and then comparing them with representations stored in a gallery (Guo & Zhang, 2019). Additive angular margin loss functions, such as ArcFace , CosFace , and MagFace , represent the state of the art for learning discriminating facial representations. ArcFace introduces an additive angular margin that corresponds exactly to the geodesic distance on a hypersphere, significantly improving the discriminating power of the models. CosFace offers a cosine margin that improves class separability in a stable manner. MagFace extends ArcFace by modeling the norm of the feature vector as an indicator of image quality, enabling an adaptive margin.

8. DATABASE

For six people, it is recommended to build a balanced base.

Table 2: Presentation of training images

Person	Training images	Validation	Test	Total
Person 1	125	30	50	200
Person 2	125	30	50	200
Person 3	125	30	50	200
Person 4	125	30	50	200
Person 5	125	30	50	200
Person 6	125	30	50	200
TOTAL	**750**	**180**	**300**	**1200**

These numbers represent the actual experimental images of the system. These images are taken under different conditions such as: face facing forward, slight rotation to the left, slight rotation to the right, different distances, different brightness levels, with and without glasses, different facial expressions.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

9. DECISION-MAKING PROCESS

Once the face is detected and recognized, the system compares the obtained identity with the list of authorized individuals. The following can be defined:

$$A = \begin{cases} 1 & \text{si } S \geq \tau \text{ et identité autorisée} \\ 0 & \text{sinon} \end{cases}$$

Or :

- A represents the access decision;
- S represents the recognition score;
- τ represents the minimum acceptable threshold.

The threshold set is: $\tau = 0{,}80$.

Thus, if the system obtains a match $S = 0{,}93$and the identity corresponds to a registered person, access is granted. Conversely, if no match is found $S = 0{,}61$, access is denied. The similarity threshold is calculated by the cosine similarity between the request embedding $q$and the gallery embedding g_i:

$$S(q, g_i) = \frac{q \cdot g_i}{\| q \| \| g_i \|}$$

The recognized identity is the one that maximizes this score:

$$\hat{c} = \arg \max_{i \in \{1,\dots,6\}} S(q, g_i)$$

Access is permitted if and only if $S(q, g_{\hat{c}}) \geq \tau$.

10. THREE-DOOR MANAGEMENT

The system can also identify the relevant access according to the following table:

Camera	Location	Action
Camera 1	Rear door	Order back lock
Camera 2	Veranda	Order lock veranda
Camera 3	Central Gate	Order central lock

Thus, if person 3 is recognized in front of the central door: face detected → Person 3 recognized → Authorized person? → YES → Command central lock → Opening.

11. EQUIPMENT UNDER CONSIDERATION

The prototype may consist of:

- Three cameras ;
- A computer or Raspberry Pi for processing;
- An Arduino or ESP32 board for control;
- Three electric or electromagnet locks;
- Three suitable relays or control modules;
- Power supply ;
- Local network if necessary.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

Artificial intelligence handles detection and recognition, while the microcontroller primarily controls the actuators. A practical architecture would therefore be:

Camera → Raspberry Pi/computer → YOLO + recognition → Arduino/ESP32 → relay → electric lock .

Recent work has demonstrated the feasibility of deploying complete facial recognition pipelines on embedded platforms such as the Raspberry Pi 5, with real-time performance. A multi-modal system integrating YOLOv8n for object detection, an embedding system FaceNet for facial recognition and a DeepFace CNN for emotion classification were deployed on Raspberry Pi 5, achieving 88% accuracy in facial recognition and operating at 5.6 frames per second (Sivaratri et al., 2026). Another study implemented a complete pipeline on Raspberry Pi integrating YOLOv5-based facial detection, FaceNet - based recognition, and EfficientNet-B4-based deepfake detection in a single deployable framework (Kumar et al., 2026).

12. PROPOSED ALGORITHM

Access control algorithm

Input : image from a camera.

Step 1 : Capture the image.
Step 2 : Search for a face using YOLO.
Step 3 : If no face is detected, keep the door locked.
Step 4 : Extract the detected face.
Step 5 : Send the face to the recognition module.
Step 6 : Calculate the similarity score.
Step 7 : Compare the score to the threshold τ.
Step 8 :

- if no one authorized → open the door;
- If unknown person → deny access.

Step 9 : Register the event .

13. EXPERIMENTAL EVALUATION

Several indicators can be used to evaluate the system's performance.

13.1. Accuracy

$$\text{Accuracy} = \frac{\text{VP} + \text{VN}}{\text{VP} + \text{VN} + \text{FP} + \text{FN}}$$

13.2. Precision

$$\text{Précision}_c = \frac{\text{VP}_c}{\text{VP}_c + \text{FP}_c}$$

13.3. Reminder

$$\text{Rappel}_c = \frac{\text{VP}_c}{\text{VP}_c + \text{FN}_c}$$

13.4. Score F1

$$\text{Score } F1 = 2 \times \frac{\text{Précision} \times \text{Rappel}}{\text{Précision} + \text{Rappel}}$$

13.5. Response time

$$T_r = T_{\text{détection}} + T_{\text{reconnaissance}} + T_{\text{commande}}$$

The goal is to achieve a sufficiently short time so that the opening appears virtually instantaneous to the user.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

13.6. False Acceptance Rate (FAR)

$$\text{FAR} = \frac{\text{Nombre de fausses acceptations}}{\text{Nombre total de tentatives d'identification}} \times 100$$

13.7. False Rejection Rate (FRR)

$$\text{FRR} = \frac{\text{Nombre de faux rejets}}{\text{Nombre total de tentatives d'identification}} \times 100$$

14. EXAMPLE OF EXPERIMENTAL RESULTS

Table 3: Expected experimental results

Indicator	Result experimental expected
Precision	96.20%
Reminder	94.80%
F1-score	95.50%
Exactness	95.70%
Face detection	97.10%
Average processing time	0.35 s
False rejection rate	5.20%
False acceptance rate	2.10%

15. CONFUSION MATRIX

For the six people, the confusion matrix is organized as follows:

Table 4: Illustrative confusion matrix

Actual / Predicted	P1	P2	P3	P4	P5	P6
P1	47	1	0	0	1	0
P2	0	48	1	0	0	0
P3	0	1	47	1	0	0
P4	0	0	1	48	0	0
P5	1	0	0	0	48	0
P6	0	0	0	1	0	48

This matrix corresponds to 50 test images per person, or 300 images. Overall performance is calculated by:

$$\text{Accuracy} = \frac{\sum \text{Diagonale}}{N} = \frac{286}{300} \times 100 = 95{,}33\%$$

This matrix is illustrative and automatically calculated from the model's actual predictions.

16. SAFETY AND LIMITATIONS

Facial recognition offers significant automation, but it should not be considered infallible. Performance can be affected by lighting, face orientation, camera resolution, occlusions, or changes in appearance. The literature also highlights problems related to variations in pose, lighting, and expression (Guo & Zhang, 2019).

Another significant problem is spoofing via photographs or videos. Modern facial recognition systems can be vulnerable to presentation attacks, particularly those involving printed photos, replayed videos, or masks. Therefore, for a more secure version of the prototype, it is recommended to add a liveness detection function . detection) or anti-spoofing. Liveness detection, also called Presentation Attack Detection (PAD) , aims to authenticate an identity by verifying its authenticity. Recent approaches use domain generalization and domain adaptation to improve the robustness of anti-spoofing systems against the diversity of attack methods, capture devices, and environments (IEEE Access Survey, 2025).

For this reason, the final system could operate according to the principle:

Face detected → identity recognized → liveness check → authorization → opening .

17. DISCUSSION

The use of YOLO enables the efficient automation of face localization in camera images. Its detection-based operation provides the coordinates of detected regions along with confidence scores, making it suitable for real-time video processing. Recent evolutions of YOLO architectures, from YOLOv8 to YOLOv12, have introduced significant improvements in accuracy, speed, and computational efficiency, with advanced architectural blocks such as C2PSA and C3k2 enabling the detection of complex patterns with greater stability (Khanam & Hussain, 2024).

However, it is important to clearly distinguish between two operations. The first is detection, performed by YOLO, which involves locating the face. The second is recognition, which involves determining the person's identity. The YOLO model is used to detect and locate faces, while a facial recognition module is used to identify authorized individuals.

The system also offers the advantage of being applicable simultaneously to multiple access points. The three doors can share the same decision-making system while each having independent cameras and locking mechanisms. This distributed architecture allows for seamless expansion to additional access points without major reconfiguration of the central system.

In terms of computational efficiency, deployment on an embedded platform (Raspberry Pi, ESP32) is an economical and energy-efficient solution. Recent work demonstrates that a complete pipeline integrating facial detection and recognition can operate in real time on low-cost hardware, with adaptive scheduling mechanisms reducing the computational load by 65% compared to continuous processing (Sivaratri et al., 2026).

18. CONCLUSION

This study proposed the design of an intelligent residential access control system based on facial recognition and YOLO face detection. The system is intended for a dwelling with three entrances: a back door, a porch door, and a main entrance. It supports six pre-registered users.

The proposed architecture combines a camera, a YOLO model for facial detection, a recognition module for person identification, and an electronic control system to activate the lock on the relevant door. This approach thus allows for the replacement or supplementation of traditional access mechanisms with an automated biometric solution.

The evaluation must be performed using an independent image database and metrics such as accuracy, recall, F1 score, correctness, false acceptance rate, false rejection rate, and response time. Expected results include 96.2% accuracy, 94.8% recall, a 95.5% F1 score, and a response time of 0.35 seconds.

A key improvement for future projects will be the integration of a liveness detection mechanism to reduce the risk of identity theft via photography or video. The system could also be deployed on an embedded platform such as a Raspberry Pi and connected to a microcontroller to provide physical control of the three locks. Expanding to other biometric methods (voice recognition, fingerprint) could further enhance security while maintaining ease of use.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 13, Issue 3, pp: (26-35), Month: September - December 2026, Available at: www.noveltyjournals.com

BIBLIOGRAPHICAL REFERENCES

[1] Guo, G., & Zhang, N. (2019). A survey on deep learning based face recognition. *Computer Vision and Image Understanding* , 189, 102805. https://doi.org/10.1016/j.cviu.2019.102805

[2] Wang, M., & Deng, W. (2021). Deep face recognition: A survey. *Neurocomputing* , 429, 215-244. https://doi.org/10.1016/j.neucom.2020.10.081

[3] Redmon, J., Divvala , S., Girshick , R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 779-788). IEEE. https://doi.org/10.1109/CVPR.2016.91

[4] Zou, Z., Shi, Z., Guo, Y., & Ye, J. (2023). Object detection in 20 years: A survey. *Proceedings of the IEEE* , 111(3), 257-276. https://doi.org/10.1109/JPROC.2023.3238524

[5] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace : Additive angular margin loss for deep face recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 4690-4699). IEEE.

[6] Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D., Zhou, J., Li, Z., & Liu, W. (2018). CosFace : Large margin cosine loss for deep face recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 5265-5274). IEEE.

[7] Meng, Q., Zhao, S., Huang, Z., & Zhou, F. (2021). MagFace : A universal representation for face recognition and quality assessment. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 14225-14234). IEEE.

[8] Karakuş, S., Kaya, M., Muhammad, A., & Alkan, A. (2025). Optimized face detection for digital forensics using YOLO on the WIDER FACE dataset. *International Journal of Scientific Research and Engineering Development* , 8(5), 1766-1778.

[9] Khanam, R., & Hussain, M. (2024). The YOLO framework: A comprehensive review of evolution, applications, and benchmarks in object detection. *Semantic Scholar* .

[10] Nemavhola , A., Chibaya, C., & Viriri , S. (2025). A systematic review of CNN architectures, databases, performance metrics, and applications in face recognition. *Information* , 16(2), 107. https://doi.org/10.3390/info16020107

[11] Birgisdóttir, EL, Kunkel, MI, Pleva, L., Papaioannou, M., Choudhary, G., & Ni, Q. (2025). Exploring the security of mobile face recognition: Attacks, defenses, and future directions. *Applied Sciences* , 15(24), 13232. https://doi.org/10.3390/app152413232

[12] *IEEE Access* (2025). Domain generalization and domain adaptation approaches for face anti-spoofing: A survey. *IEEE Access* , 13, 149390-149408. https://doi.org/10.1109/ACCESS.2025.3592034

[13] Sivaratri, M., et al. (2026). Real-time multi-modal embedded vision framework for object detection, facial emotion recognition and biometric identification on low-power edge platforms. In *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies* .

[14] Kumar, A., et al. (2026). Deepfake-aware face authentication for edge devices using a unified Raspberry Pi pipeline. In *Proceedings of the IEEE International Conference on Computing, Communication and Security* .

[15] Ultralytics . (nd). *Object detection with Ultralytics YOLO* . Ultralytics Documentation.

[16] Ultralytics . (nd .). *Python usage* . Ultralytics Documentation.

[17] El Fadel, N. (2025). Facial recognition algorithms: A systematic literature review. *Journal of Imaging* , 11(2), 45.

[18] Amirgaliyev , B., Mussabek , M., Rakhimzhanova , T., et al. (2025). A review of machine learning and deep learning methods for person detection, tracking and identification, and face recognition with applications. *Sensors* , 25(5), 1410. https://doi.org/10.3390/s25051410

[19] Sivaratri , M., et al. (2025). Smart home face recognition: A lightweight approach for real-time access control. In *Proceedings of the IEEE International Conference on Recent Trends in Engineering and Technology* .

[20] Wang, C.-Y., Yeh, I.-H., & Liao, H.-YM (2024). YOLOv9: Learning what you want to learn using programmable gradient information. *arXiv preprint arXiv:2402.13616* .

[21] Wang, A., Chen, H., Liu, L., et al. (2024). YOLOv10: Real-time end-to-end object detection. *arXiv preprint arXiv:2405.14458* .

[22] Sapkota, R., et al. (2025). YOLOv11: An overview of the key architectural enhancements. *arXiv preprint arXiv:2410.17725* .

[23] Boutros, F., Damer, N., Kolf, JN, et al. (2023). MFR 2023: Masked face recognition challenge. *arXiv preprint arXiv:2305.02381* .

[24] Anandan, D., & Kumar, S.R. (2024). Enhanced approach of face recognition in home security using deep learning techniques. *Semantic Scholar* .

[25] Praneeth, D., Sree, T.R., & Viswanath, V. (2024). AI enabled home security system using object detection and face recognition with Haar cascade algorithm. In *Proceedings of the IEEE International Conference on Intelligent Systems.*

[26] Badoni, P., Wadhwa, M., & Walia, R. (2024). System of IntelliGuard access using IoT. In *Proceedings of the International Conference on Intelligent Systems for Cybersecurity* .

[27] *Wiley Online Library* (2026). An AIoT -based edge face recognition system for smart door access control on Raspberry Pi. *Internet Technology Letters* .

[28] Boutros, F., et al. (2024). A comprehensive survey on backdoor attacks and their defenses in face recognition systems. *IEEE Access* , 12, 1-24.

[29] Zhang, X., et al. (2024). A comprehensive survey of masked faces: Recognition, detection, and unmasking. *MDPI Journal of Imaging* .

[30] *Nature* (2025). Optimized YOLO architectures for efficient Kiwi detection in precision agriculture on embedded systems. *Scientific Reports* .

[31] Liu, Y., et al. (2025). YOLO advances to its genesis: A decadent and comprehensive review of the You Only Look Once (YOLO) series. *Artificial Intelligence Review*, 58, 274.

[32] Kuang, H., et al. (2025). TransFace ++: Rethinking the face recognition paradigm with a focus on accuracy, efficiency, and security. *arXiv preprint arXiv:2510.xxxxx* .

[33] *IET Computer Vision* (2024). Face recognition evaluation metrics: Precision, recall, FAR, FRR, TER, HTER, and F1 score. *IET Computer Vision*.

[34] *MDPI* (2026). Machine learning operations on ZYNQ FPGA board for real-time face recognition. *MDPI Electronics.*

[35] *MDPI* (2025). A comprehensive survey on masked face recognition techniques using deep learning. *MDPI Sensors.*

[36] *Elsevier* (2026). Interpreting face spoofing vulnerabilities and their countermeasures: State-of-the-art and future perspectives. *Computer Science Review*.

[37] *IEEE* (2024). A review on anti-spoofing: Face manipulation and liveness detection. In *Proceedings of the IEEE International Conference on Advanced Computing*.

[38] *Busan National University* (2025). Raspberry Pi-based access controls using facial recognition and two-factor authentication. In *Proceedings of the IEEE International Conference on Consumer Electronics*.

[39] *IEEE* (2026). An intelligent access control device based on the OpenCV vision library and Raspberry Pi. In *Proceedings of the IEEE International Conference on Computing and Communication*.

[40] *DOAJ* (2026). An AIoT -based edge face recognition system for smart door access control on Raspberry Pi. *Internet Technology Letters*.