IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5251~5259
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5251-5259

Design of an internet of things system with deep learning for facial recognition in security applications

Angel Giordano Marengo Morales, Ricardo Yauri
Department of Electronic Engineering, Faculty of Engineering, Universidad Tecnológica del Perú, Lima, Perú

Article Info

Article history:

Received May 9, 2025
Revised Aug 20, 2026
Accepted Sep 19, 2026

Keywords:

Artificial intelligence
Computer vision
Deep learning
Mask detection
OpenCV
Smart surveillance

ABSTRACT

In recent years, a high crime rate has been observed, threatening the safety of people and private property. As a method of preventing this insecurity, private facilities are opting to install security systems. Furthermore, despite the results found in the literature, a gap has been identified in the design of systems that combine facial cover detection and internet of things (IoT) transmission. Therefore, this research shows the design of a low-cost IoT security system using deep learning for facial recognition. The research adopts a quantitative approach, as a large volume of data is used to train a deep learning model. The system used is divided into three stages: implementation of a facial detection algorithm in Python with a Webcam, training of the recognition model, and transmission of captured images through the Telegram. Unlike previous studies that relied on high-cost hardware or proprietary monitoring platforms, this system demonstrates that it is possible to integrate facial recognition and communication with Telegram as a notification communication medium. Additionally, a face covering detection model was developed as a filter to detect if a suspect is wearing something. The system achieved 97% accuracy in facial recognition model and 82.64% accuracy in face covering detection model.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Ricardo Yauri
Department of Electronic Engineering, Faculty of Engineering, Universidad Tecnológica del Perú
Lima, Perú
Email: c24068@utp.edu.pe.com

1. INTRODUCTION

Society is currently facing incidents that threaten personal safety or private property, which is supported by the number of crimes that put the assets of individuals and businesses at risk. In this context, robberies and thefts are recurring crimes in shopping centers and other public establishments, making it important to have some contingency measures. The most common forms of security systems are closed circuit television (CCTV) systems [1] but this does not recognize people with criminal activities [2]. In addition, the economic factor is important for businesses because they opt for proprietary devices [3], [4] for security, where there might not be an evolution within the area of artificial vision [5]. The analysis of the literature mentions the technological advancement at a global level of artificial intelligence to capture and recognize a person's face, directed to criminal identification centers, surveillance [6], [7], access management to private centers, and intelligent vehicles [1], [8]. On the other hand, there are many problems related to security, theft or entry of unwanted people into private centers, making it important to maintain the safety of people in their daily lives [9], [10].

In the case of identity detections, there is a large presence in security system implementations that use a histogram of oriented gradients (HOG) analysis and local binary pattern histogram (LBPH) algorithm [11], [12]. A comparison is also made of face recognition techniques such as the Haar classifier

cascade technique [13], [14]. These techniques have been applied to face recognition in user registration and access control through a neural network integrated into hardware [4], [15]. Other research makes use of software tools such as the Python language, OpenCV (Python library) [15], [16] to detect the presence of a face in the image or video, using functions such as eigen face, fisher faces, and finally OpenCV [17].

Research papers mention that facial recognition has had a significant impact during the global COVID-19 emergency where it was used to discriminate between a person wearing a mask or not, among other elements related to health care [18], [19]. Likewise, another research proposes the use of online systems with support vector machine (SVM) models for training artificial intelligence and integration with web interfaces [20], [21]. In addition, solutions have also been developed with internet of things (IoT) to detect masks within public transport with deep learning [22] and using a Raspberry Pi 4, with software tools such as TensorFlow [23], [24]. On the other hand, there are papers that focus on the economic impact generated by implementation of surveillance systems through the use of hardware such as the Raspberry Pi, integrating algorithms based on the FaceNet neural network, the Viola-Jones method, and OpenCV for face detection [25]. In another study, an economical video surveillance system was developed, using microcomputers such as the Raspberry Pi 3 and monitoring with the Telegram application [3], [26], using modules for the face detection [27], and facial recognition applying VGGFace2 [28].

For the reasons, the development of a security system with facial recognition generates benefits that contribute to the accessibility and democratization of technology in residential or commercial environments for the prevention of incidents such as theft [8], [14]. The following research question is posed: how is an IoT security system designed with facial recognition? The general objective is to design a low-cost IoT security system using deep learning for facial recognition. The research makes an important contribution related to the proposal of a development methodology for artificial intelligence-based security systems. The motivation lies in the need to offer affordable technological solutions in the face of the high costs of conventional security systems.

2. PROPOSED SYSTEM

The system consists of an IoT module based on a Raspberry Pi 4 model B microcomputer, which processes facial images captured by the camera. These images are processed using the multi-task cascaded convolutional networks (MTCNN) Python library, where each frame is marked with a box. Once this process is completed, the face is identified as belonging to an employee, a frequent customer, or an unwanted person. The image is then evaluated by a neural network model and subsequently sent to a text messaging application. In addition, a face obstruction detection stage was added to the recognition model, which identifies whether the captured face is covered. The algorithm developed with face capture, facial recognition, and the face obstruction model are executed in Python on the Raspberry Pi microcomputer. The proposed IoT security system is illustrated in Figure 1.

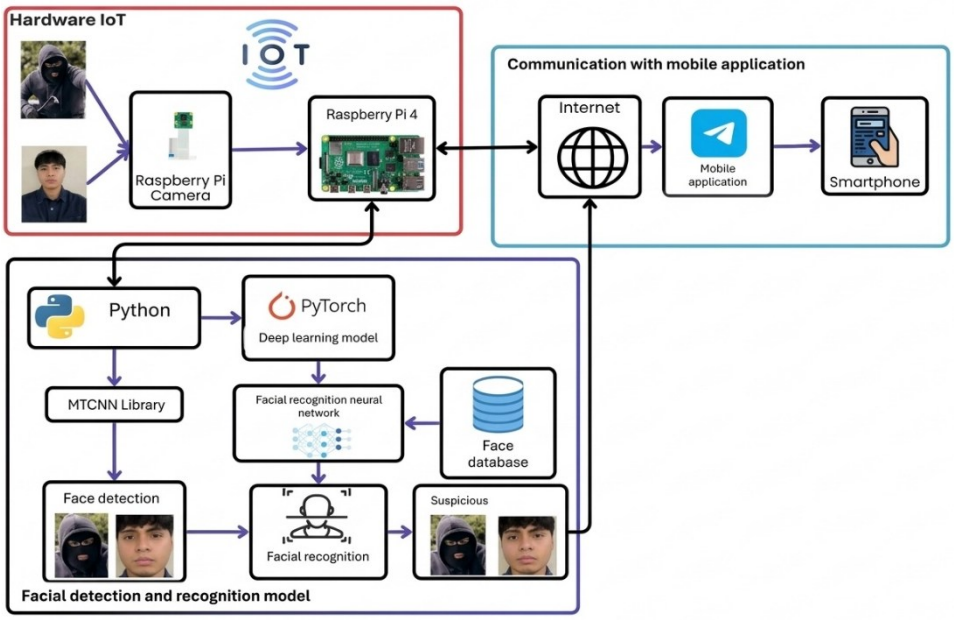

Figure 1. IoT security system diagram

2.1. Internet of things module

It is composed of a 5 megapixel camera connected to the Raspberry module, to take images with a resolution of 2592 × 1944 and for videos in formats of 1080 × 30, 720 × 60. Regarding Raspberry Pi 4 model B, it has an ARM Cortex-A72 processor that has 1.5 GHz. This processor processes the algorithm in the Raspberry Pi OS operating system as shown in Figure 2.

2.2. Facial detection and recognition module

Three types of algorithms were developed. The first is responsible for capturing faces in the frames captured by the camera using the MTCNN library. The second integrates deep learning that uses neural networks to determine if an object interrupts the analysis of a face in front of the camera for recognition, complementing the main model. The MTCNN algorithm is used for this purpose. A third component consists of the hidden face detection algorithm.

2.2.1. Real-time and image face detection

This process consists of image capture, face detection, and face cropping. Embeddings are then extracted from the face image to represent this information vectorially as shown in Figure 3. The information in vector format of the embedding is processed by the facial recognition and face obstruction detection models, for which the data is converted to tensors compatible with the PyTorch software and represented in vector form using the NumPy library as shown in Figure 4.

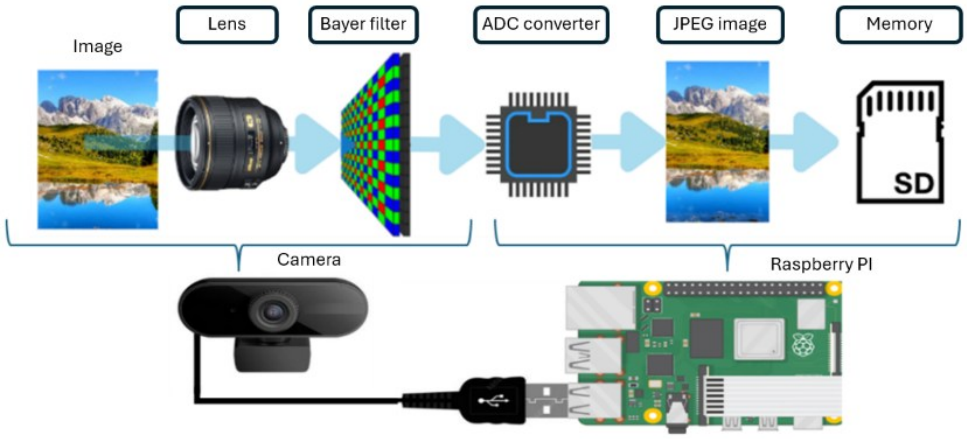

Figure 2. Diagram of the machine vision recognition system

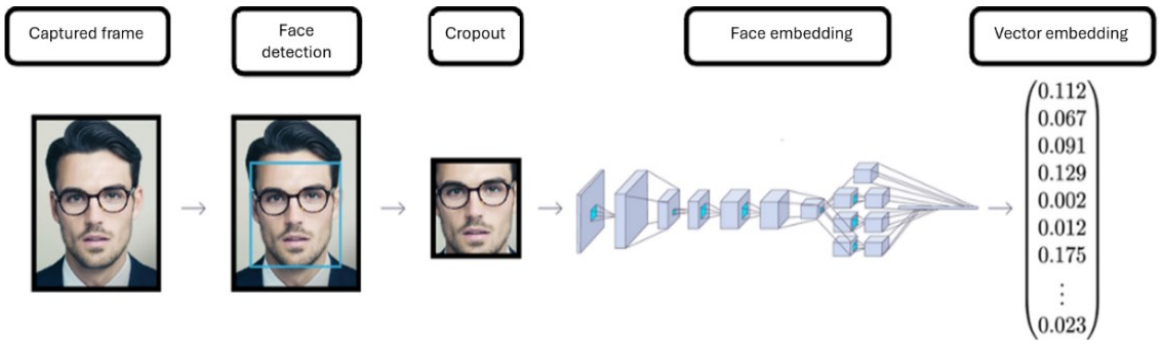

Figure 3. Face detection process

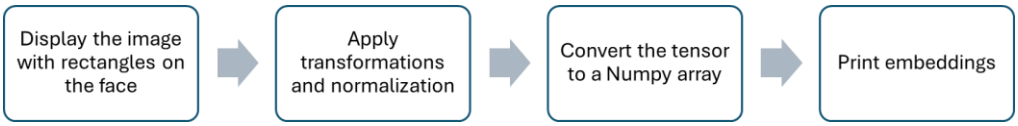

Figure 4. Procedure for extracting embeddings

2.2.2. Facial recognition

A facial recognition learning model was developed using 1,296 images, 54 of which were sourced by the developer. This research followed a series of steps, as shown in Figure 5, using 10 data folders related to different people, along with a proprietary image source to test its performance. This facial recognition model uses a deep learning framework based on convolutional neural networks. For embedding, the FaceNet library was used, which contains tools such as MTCNN and InceptionResnetV1, where the training data is input (extracted embedding). The number of layers in the model is defined using the rectified linear unit (ReLU) activation function and four layers. The first layer consists of 256 neurons, followed by 128, 64, and 11 neurons for the output class.

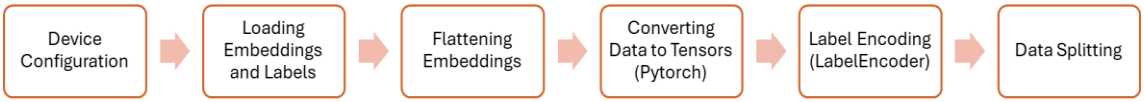

Figure 5. Database routing for facial recognition model

2.2.3. Covered face detection

The neural network model was able to identify the presence of a face in front of the camera that was covered by clothing (sunglasses, a mask, a face covering, or some other object). It also applied a deep learning framework with a convolutional neural network using the PyTorch lightning library. In this case, the labels focused on the captured object that obstructed facial recognition is shown in Figure 6. With the processed data, four layers are established for the convolutional neural network, consisting of 165,454, 120, 84, and 20 neurons in the output layer. To integrate the three generated models, the covered face model and facial recognition model are previously saved in files named "model_covering.cpkt" and "model_recognition.pth". After this, the algorithm module is executed to capture video in real time with a webcam, and the MTCNN tool is used to extract the face in each frame, then highlight the face with a box.

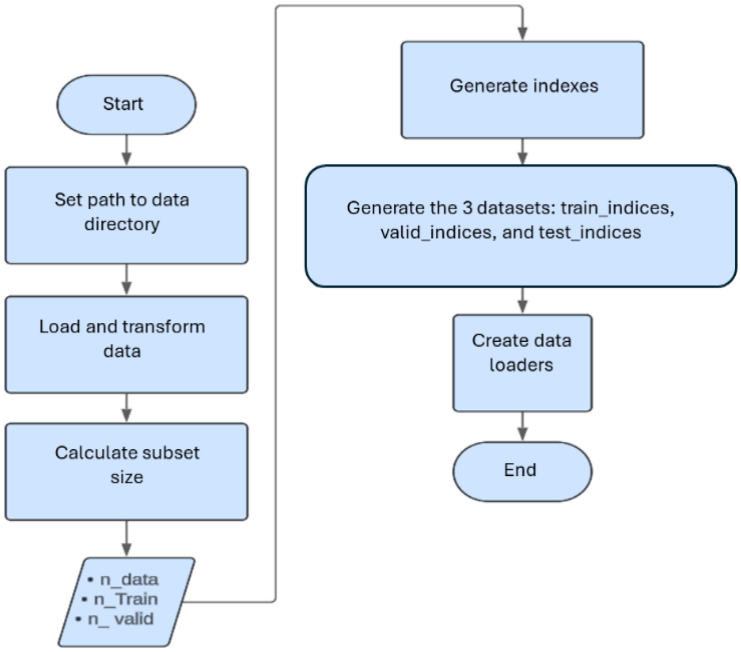

Figure 6. Database processing for a covered face model

2.3. Communication with mobile application

This stage sends alerts to Telegram instant messaging software, in addition to transmitting images. For this purpose, the Telebot library was used, which configures a bot that manages the transmission and

adds a layer of security. In this case, the Telegram tool BotFather, freely accessible within the same application, is specifically used, using identification names such as "SistSeguridad" and "sistseguridadpython_bot" as shown in Figure 7.

The communication algorithm with Telegram is developed in Python, and deployed on the Raspberry Pi microcomputer, using the validation token using the topic "/activar_sistema" which allows sending the detected images. The communication process begins by verifying that the image directory (image_directory) has a new .jpg image, to send it along with a message detailing the characteristics of the photo (caption). The name of the image is configured with respect to the detected parameter ("situation") which can be: "Rec_" (recognized), "Sos_" (suspicious), "Det" (unregistered person). Once the situation is determined, the message is completed in other fields of name, object_used, and time.

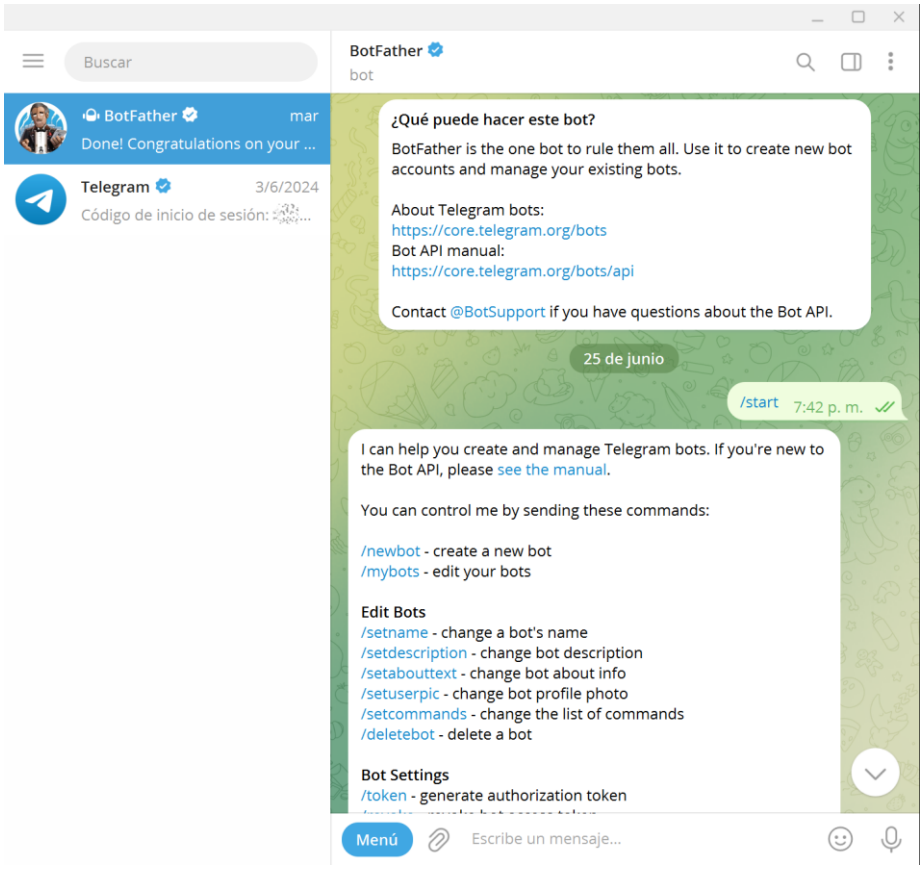

Figure 7. Using and generating bots in Telegram

3. RESULTS AND DISCUSSION

3.1. Facial recognition model using deep learning framework

The three algorithms obtained a face image, assessing whether it was covered ("covering"), storing the image, and indicating whether it was suspicious. The system assessed whether the face was using an object by indicating the object it was using in the image. The face detection process achieved over 90% similarity with any face in the database using the confusion matrix as shown in Figure 8. This result is consistent with other findings on devices using Raspberry Pi with embeddings [25], or surveillance tools featuring edge-based recognition [28]. The classification model, with respect to person identification, obtained an accuracy of 98%, recall (99%), and F1-score (99%).

The covered face model was evaluated during training regarding the identification of "sunglasses" or "sunglasses (imagenet)", obtaining an average accuracy of 82.64% and F1-score of 82.34%. The low performance value of the model is linked to the similarity between different types of occlusions, an issue addressed in other research involving low-cost edge devices [22], [24]. The confusion matrix shows an uncertainty between the values of "sunglasses" and "sunglasses (imagenet)", they are similar by having two different sources of information in the dataset called "sunglasses-imagenet" and "sunglasses" as shown in Table 1. These performance metrics are complemented by the confusion matrix of the covered face model as

in Figure 9, which provides a detailed visualization of how the classifier distinguishes between the five categories of coverage, glasses, none, sunglasses, and sunglasses.

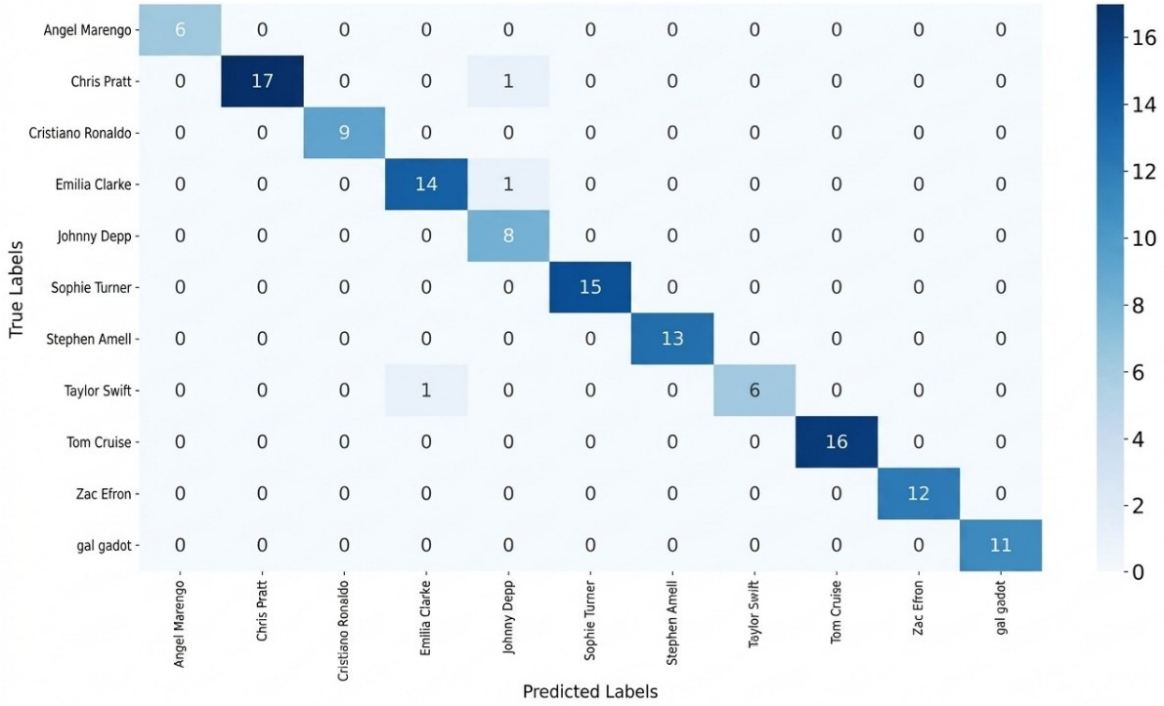

Figure 8. Random forest confusion matrix of the random forest model

Table 1. Covered face model classification report

Name	Precision	Recall	F1-score	Support
Coverage	0.8587	0.7822	0.8187	101
Glasses	0.8981	0.8220	0.8544	118
None (plain)	0.8043	0.8506	0.8268	87
Sunglasses	0.7600	0.8172	0.7876	93
Sunglasses (imagenet) (sunglasses-imagenet)	0.7931	0.8440	0.8178	109
Accuracy			0.8228	508
Macro average	0.8229	0.8232	0.8218	508
Weighted average	0.8264	0.8228	0.8234	508

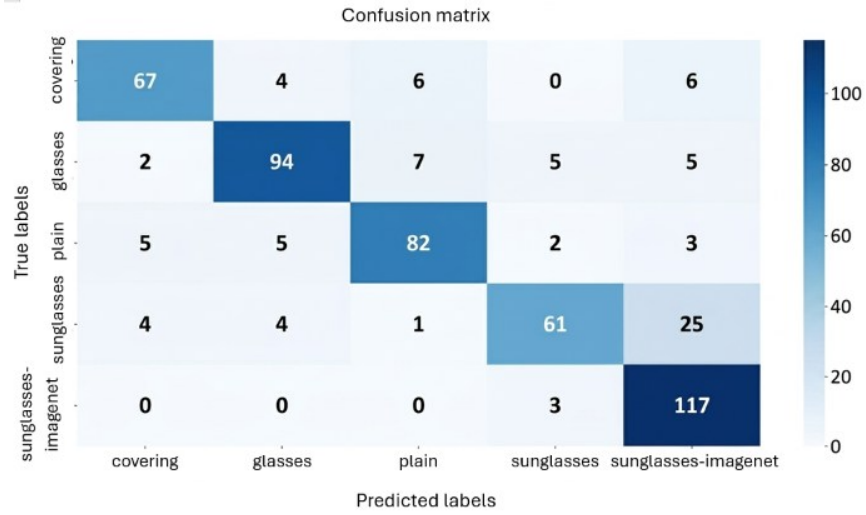

Figure 9. Confusion matrix of the covered face model

3.2. Security system evaluation with the internet of things module

In tests conducted with the IoT hardware, the face was detected and framed even when covered by sunglasses or glasses, and the name of the detected object was entered. Additionally, when a new face was detected, it was logged with a "new person" tag to be stored in the database and sent to Telegram. Facial recognition and covered face models were also applied, displaying the object used, the name of the identified person, and similarity percentage on the screen, with values greater than 90% at different distances as in Figure 10. The model's performance is influenced by distance or lighting [7].

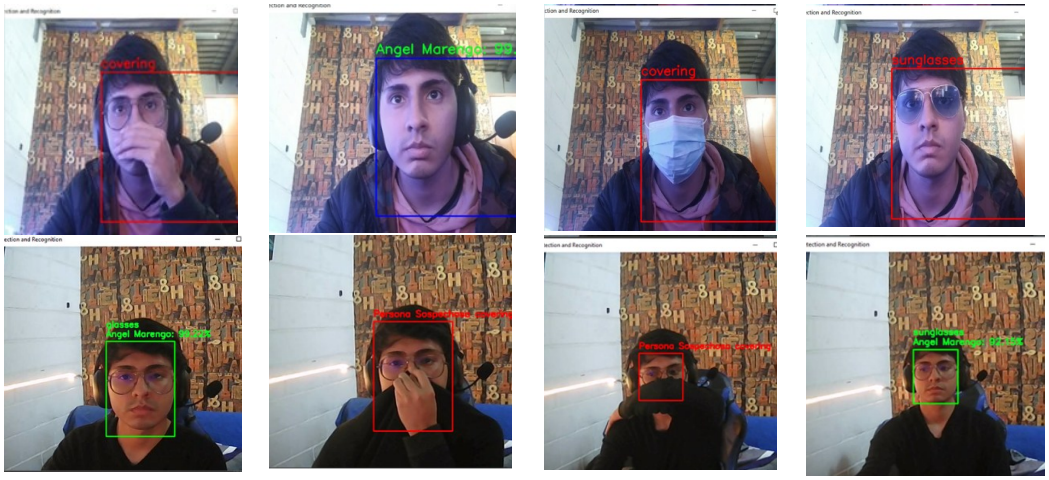

Figure 10. Face detection evaluation

Messages were sent from the Raspberry Pi to the Telegram platform using the bot created by BotFather, as “sistseguridad_bot". The sending of images was activated using the code "/activar_sistema", and then the photos were uploaded to the group chat database. The messages displayed details such as "recognized person:", "is using", and "date and time:". During the tests, when the person was not in the database, a message saying "unregistered person" was displayed. On the other hand, when the person was covered, the message was "Alert! Suspicious person with covered face, please be alert". These messages were sent in Spanish as shown in Figure 11.

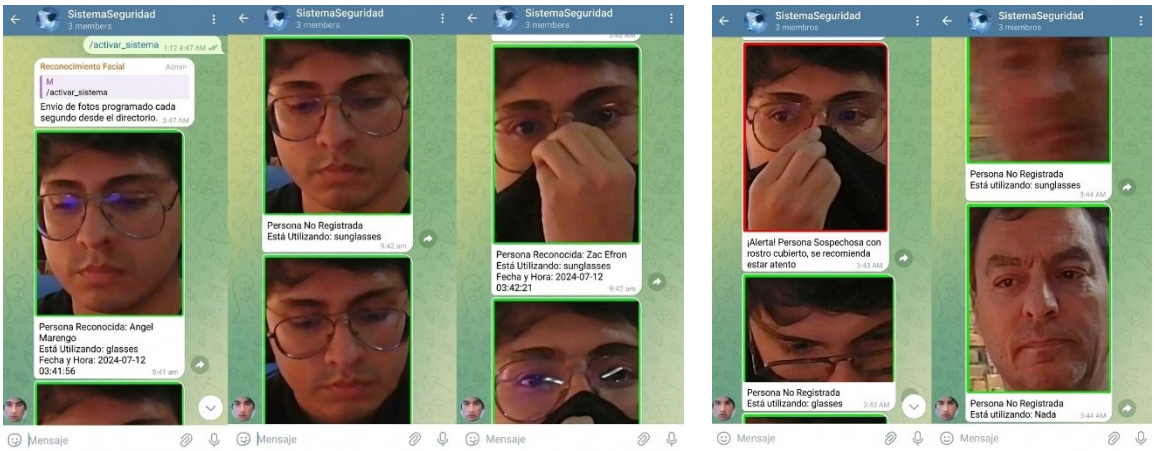

Figure 11. Results on Telegram

4. CONCLUSION

The proposed system successfully integrated a facial recognition model using deep learning with an IoT module, achieving 97% accuracy in identifying individuals and 82.64% accuracy in detecting facial coverings. Experiments validated the system's ability to identify registered users and detect unregistered or suspicious individuals, even those wearing accessories such as sunglasses. These results demonstrate the

feasibility of implementing a low-cost, open-source security solution in environments with limited infrastructure. Furthermore, the research describes the use of facial image datasets. However, it is essential to ensure adequate lighting conditions and consider greater storage and processing capabilities (such as more powerful devices like the Jetson Nano) when deploying the system in high-traffic areas.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Angel Giordano Marengo Morales	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ricardo Yauri		✓			✓	✓			✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [RY], upon reasonable request.

REFERENCES

[1] J. Poměnková and T. Malach, "Optimized classifier learning for face recognition performance boost in security and surveillance applications," *Sensors*, vol. 23, no. 15, Aug. 2023, doi: 10.3390/s23157012.
[2] M. Koca, "Real-time security risk assessment from CCTV using hand gesture recognition," *IEEE Access*, vol. 12, pp. 84548–84555, 2024, doi: 10.1109/ACCESS.2024.3412930.
[3] B. Bhuckory and S. Pudaruth, "A multimodal IoT-based home intrusion detection system," *International Journal of Computer Theory and Engineering*, vol. 15, no. 3, pp. 117–124, 2023, doi: 10.7763/IJCTE.2023.V15.1340.
[4] N. Hiremani *et al.*, "Artificial intelligence-powered contactless face recognition technique for internet of things access for smart mobility," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/8750840.
[5] M. P. -Trigo, E. J. L. -Ortiz, J. L. S. -González, J. A. Á. -García, and J. J. V. Olmos, "Data processing unit for energy saving in computer vision: weapon detection use case," *Electronics*, vol. 12, no. 1, Dec. 2022, doi: 10.3390/electronics12010146.
[6] S. Bethu, M. Trupthi, S. K. Mandala, S. Karimunnisa, and A. Banu, "AI-IoT enabled surveillance security: DeepFake detection and person re-identification strategies," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 7, 2024, doi: 10.14569/IJACSA.2024.0150799.
[7] P. Choudhary, P. Pathak, and P. Gupta, "Assessment of face image quality for improvement of recognition system with machine learning," *AiBi Revista de Investigación, Administración e Ingeniería*, vol. 12, no. 1, pp. 152–162, Jan. 2024, doi: 10.15649/2346030X.3461.
[8] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: a survey," *Sensors*, vol. 20, no. 2, Jan. 2020, doi: 10.3390/s20020342.
[9] A. R. Fathima and A. Saravanan, "An approach to cloud user access control using behavioral biometric-based authentication and continuous monitoring," *International Journal of Advanced Technology and Engineering Exploration*, vol. 11, no. 119, pp. 1469–1496, Oct. 2024, doi: 10.19101/IJATEE.2024.111100516.
[10] P. S. JosephNg, P. S. BrandonChan, and K. Y. Phan, "Implementation of smart NFC door access system for hotel room," *Applied System Innovation*, vol. 6, no. 4, Jul. 2023, doi: 10.3390/asi6040067.
[11] F. J. N. Onana and K. Dimililer, "Smart attendance system by facial recognition," in *16th International Conference on Applications of Fuzzy Systems, Soft Computing and Artificial Intelligence Tools – ICAFS-2023*, Cham, Switzerland: Springer, 2025, pp. 76–85, doi: 10.1007/978-3-031-72506-7_11.
[12] M. Gupta, K. Bisht, A. Sharma, and D. Upadhyay, "HaarCascade and LBPH algorithms in face recognition analysis," in *2023 World Conference on Communication & Computing*, Jul. 2023, pp. 1–4, doi: 10.1109/WCONF58270.2023.10235019.

[13] S. Bose, T. Arjariya, and A. Goswami, "Smart recognition and authentication based on haar cascade classifier and visual cryptography," *International Journal of Computing*, vol. 23, no. 2, pp. 226–239, Jul. 2024, doi: 10.47839/ijc.23.2.3541.
[14] B. S. Vendra, P. R. Dasari, K. Vydehi, and B. S. K. Devi, "Face detection system for smart security application," in *Recent Developments in Electronics and Communication Systems*, Amsterdam, Netherlands: IOS Press, 2023, pp. 651–657, doi: 10.3233/ATDE221327.
[15] R. Shah, S. Punjabi, S. Kamath, Y. Dange, and Y. Bandi, "Biometric-based smart security system," in *2023 IEEE 8th International Conference for Convergence in Technology*, Apr. 2023, pp. 1–6, doi: 10.1109/I2CT57861.2023.10126356.
[16] B. Perumal, S. Rotikadi, H. S. Mv, T. G. Reddy, M. P. Rajasekaran, and S. Velusamy, "JEEVA RAKSHAKA 1.0-AI-driven vision-based drowsiness detection system for driver safety and accident prevention," in *ICT: Applications and Social Interfaces (ICTCS 2025)*, Cham, Switzerland: Springer, 2026, pp. 286–292, doi: 10.1007/978-3-032-19690-3_27.
[17] Ankush, S. Gupta, and M. Singh, "Intelligent defence: enhancing security in smart homes," in *Recent Trends in Intelligent Computing and Communication*, London, United Kingdom: CRC Press, 2025, pp. 3–8, doi: 10.1201/9781003593034-1.
[18] L. A. Morris, D. G. Bazzini, C. J. Holden, and S. J. Lee, "The influence of face mask color on perceptions of African American and white men," *Cognitive Processing*, vol. 25, no. 4, pp. 635–645, Nov. 2024, doi: 10.1007/s10339-024-01196-y.
[19] E. L. Huamaní and L. O. Cunyarachi, "Use of artificial intelligence for face detection with face mask in real time to control the entrance to an entity," *International Journal of Emerging Technology and Advanced Engineering*, vol. 11, no. 11, pp. 68–75, Nov. 2021, doi: 10.46338/ijetae1121_09.
[20] M. Mithun, S. Sundar, and C. D. Ponnan, "College library face detection and management system with anti-spoofing mechanism," in *2024 Asian Conference on Intelligent Technologies*, Sep. 2024, pp. 1–6, doi: 10.1109/ACOIT62457.2024.10941336.
[21] M. H. M. Kamil, N. Zaini, L. Mazalan, and A. H. Ahamad, "Online attendance system based on facial recognition with face mask detection," *Multimedia Tools and Applications*, vol. 82, no. 22, pp. 34437–34457, Sep. 2023, doi: 10.1007/s11042-023-14842-y.
[22] T. A. Kumar, R. Rajmohan, M. Pavithra, S. A. Ajagbe, R. Hodhod, and T. Gaber, "Automatic face mask detection system in public transportation in smart cities using IoT and deep learning," *Electronics*, vol. 11, no. 6, 2022, doi: 10.3390/electronics11060904.
[23] A. A. Abed, A. Al-Ibadi, and I. A. Abed, "Real-time multiple face mask and fever detection using YOLOv3 and TensorFlow lite platforms," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 922–929, Apr. 2023, doi: 10.11591/eei.v12i2.4227.
[24] D. Kolosov, V. Kelefouras, P. Kourtessis, and I. Mporas, "Anatomy of deep learning image classification and object detection on commercial edge devices: a case study on face mask detection," *IEEE Access*, vol. 10, pp. 109167–109186, 2022, doi: 10.1109/ACCESS.2022.3214214.
[25] C. M. Orostegui, A. N. Luna, A. M. García, and C. A. F. Ariza, "A low-cost raspberry pi-based system for facial recognition," *Ingeniería y Ciencia*, vol. 17, no. 34, pp. 77–95, Dec. 2021, doi: 10.17230/ingciencia.17.34.4.
[26] M. F. Wicaksono, M. D. Rahmatya, and Ilham, "IoT implementation for server room security monitoring using Telegram API," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, no. 5, pp. 1931–1937, Oct. 2022, doi: 10.18517/ijaseit.12.5.13922.
[27] Z. Lian, S. Shao, and C. Huang, "A real time face tracking system based on multiple information fusion," *Multimedia Tools and Applications*, vol. 79, no. 23–24, pp. 16751–16769, Jun. 2020, doi: 10.1007/s11042-020-08889-4.
[28] E. A. Haryadi, G. Jati, A. Y. Husodo, and W. Jatmiko, "Low-cost camera-based smart surveillance system for detecting, recognizing, and tracking masked human face," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 23, pp. 104–119, Dec. 2021, doi: 10.3991/ijim.v15i23.22725.

BIOGRAPHIES OF AUTHORS



Angel Giordano Marengo Morales is a graduate of the Electronic Engineering undergraduate program at Faculty of Engineering, Universidad Tecnológica del Perú. His research work focused on the development of intelligent security systems using facial recognition based on deep learning and IoT technologies. He has a strong interest in areas such as computer vision, embedded systems, and neural network optimization for low-power devices. He is particularly motivated by the potential of combining IoT architectures with artificial intelligence to solve real-world problems in security and automation. He can be contacted at email: U18303111@utp.edu.pe.



Ricardo Yauri holds a Master of Science degree in Electronic Engineering with a specialization in Biomedical Engineering. He currently serves as an associate professor at the Universidad Nacional Tecnológica de Lima Sur and is pursuing a Ph.D. in Systems Engineering. In addition, he teaches at the Faculty of Engineering, Universidad Tecnológica del Perú. He has taught courses focused on the IoT, home automation systems, and has been involved with the cisco networking academy for IoT education. As a former researcher at INICTEL-UNI, he was part of the Embedded Systems and Internet of Things Research Group, where he led projects related to the development of low-power IoT devices incorporating. He can be contacted at email: C24068@utp.edu.pe, yauri@untels.edu.pe, or boncer99@gmail.com.