Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 9, No. 2, June 2023, pp. 429-443
ISSN: 2338-3070, DOI: 10.26555/jiteki.v9i2.26162

Design and Implementation of Embedded Biometric-Based Access Control System with Electronic Lock using Raspberry Pi

Youssef Elmir [1,2], Abdeldjalil Abdelaziz [2], Mohammed Haidas [2]
[1] Laboratoire LITAN École supérieure en Sciences et Technologies de l'Informatique et du Numérique RN 75, Amizour 06300, Bejaia, Algérie
[2] SGRE-lab University Tahri Mohammed of Bechar, Bechar, Algeria

ARTICLE INFO

Article history:

Received May 03, 2023
Revised June 08, 2023
Published Juner 10, 2023

Keywords:

Access control system;
Biometric recognition;
Raspberry pi technology;
Multimodal biometrics;
Facial recognition;
Speaker verification;
Personal identification;
Electronic lock

ABSTRACT

This paper presents the design and implementation of an improved access control system based on biometric recognition, utilising Raspberry Pi technology. The proposed system aims to enhance the security of the existing electronic lock-based system at the SGRE-Lab of University Tahri Mohammed of Bechar in Algeria. The proposed system employs multimodal biometrics, integrating facial recognition and speaker verification for personal identification. Following initial verification by the electronic lock, the system captures the user's face through a camera to perform facial recognition. In cases where the user's identity is uncertain, a voice recognition module prompts the user to say a secret word, confirming their identity through the microphone. The combination of these two biometric techniques ensures access is granted, and an access log is recorded, with an accompanying notification sent to the administrator via SMS. As technical contribution, this paper presents the design and implementation of an embedded biometric-based access control system using Raspberry Pi, which includes the integration with an electronic lock and digicode, in the other hand, a second innovation contribution by combining biometric-based authentication with Raspberry Pi technology, this paper introduces an innovative approach to access control systems that provides a more secure and reliable means of access control than traditional methods based on keys or passwords. An overview of the proposed system's architecture is provided, its operation modes, and necessary hardware and software requirements. The promising obtained results of demonstrations show a notable improvement in security levels, characterized by reduction of false acceptances, however, the paper acknowledges that users unfamiliar with the biometric system may face challenges, potentially leading to false rejections. Future work should focus on mitigating these challenges and addressing user familiarity issues.

Corresponding Author:

Youssef Elmir, Laboratoire LITAN, École supérieure en Sciences et Technologies de l'Informatique et du Numérique RN 75, Amizour 06300, Bejaia, Algérie
Email: elmir@estin.dz

1. INTRODUCTION

In recent days, security and safety in places have become a major challenge with the increase in thefts [1]-[4]. Traditional door locking systems can be easily intrusive. Security systems have become a field of research of great importance. The design of a reliable, efficient, and robust identification system is a top priority. Individual identification is essential to ensure the security of systems and organizations. It corresponds to the search for the identity of the person who presents themselves in a database and can be used to authorize the use of services. An example is access control to a highly secure area for which only a limited number of people (registered in a database) have access.

Classic access control techniques such as passwords, identity cards, keys, magnetic cards, personal identification numbers (PINs) ... are proving to be ineffective [5]-[8]. Indeed, these different techniques can be lost or even stolen. In the case of a password, it can easily be forgotten by the user or guessed by someone else. A lost key can create problems if it is misused by unauthorized persons. Owners cannot open the door when the key is lost. Sometimes the user may forget to lock the door. Users do not have the ability to check whether the door is locked or unlocked.

Unlike the use of other forms of authentication, such as passwords or tokens, biometric recognition provides a strong link between an individual and a data record, and these characteristics are unique to each individual and cannot be forgotten or lost and are very difficult to guess, steal, and duplicate.

To meet these needs, biometrics seems to be a practical, efficient, and cost-effective solution. Indeed, this technique is experiencing a rapid development. This trend is leading to the development of a wide variety of biometric methods: from the most traditional, such as fingerprint analysis [9]-[13] or iris recognition [14]-[16], to the more exotic, such as gait recognition [17], [18] and ear shape recognition [19], [20]. Manufacturers are increasingly proposing, for problems requiring a high level of security, to no longer use a single characteristic but to implement a system based on combinations of different biometric means to further increase security [21]-[23].

The field of application of this project is the Smart Grids & Renewable Energy Laboratory (SGRE-Lab) at Tahri Mohammed University of Bechar. The laboratory has an access control system (electronic lock) that works using a PIN code or a RFID card to control access as it is shown in Fig. 1. These traditional authorization methods based on the use of passwords or physical media (keys and electronic cards) do not meet modern requirements for reliability in determining the individual's identity. Furthermore, the password can be forgotten, intercepted for copying, lost, or given to another person. Above all, it does not allow traditional access control systems to ensure an adequate level of reliability. As a result, more effective ways of ensuring security are being sought. One way to solve these problems is biometrics. The idea is to add a new functionality to the existing system that will be based on biometrics. For this, we propose to develop an embedded biometric identification system and integrate it with the existing system as a second access control.

Fig. 1. The entry of SGRE-lab

Among the related works found in the literature related to this study, Crystalynne, et al [24] developed a biometric lock system based on a microcontroller with a short message service (SMS). The system scans the fingerprint, matches it with the registered model, and unlocks the lock. The global system for the mobile module (GSM) was able to send a text message containing the automatically generated access code when an unrecognized fingerprint was encountered. This is a simple and reliable way to protect a system, however it needs a physical contact with the fingerprint sensor.

Dhana Lakshmi, *et al.* [25] proposed a system that works on real-time monitoring and voice command, so that the camera can be controlled and monitored remotely. The proposed result of the project aims to offer multiple benefits in saving home security and keeping users informed about the security of their home with an option of controlling devices using their voice or a simple toggle on their smartphone, and if someone enters the home when the owner is not available, then the owner can see the person from anywhere and can also instruct them via live voice.

Sourav, *et al.* [26] developed a facial recognition door lock system. Facial recognition is a well-established process in which the face is detected and identified. It aims to create a smart door that secures the entry. The development of this system based on Raspberry-pi 3, to make the home accessible only when the face is recognized and the person is authorized to enter by the homeowner, who could monitor the entry remotely. By doing so, the system is less likely to be fooled: since the owner can check every visitor on the remote console.

In the work of Dhiraj [27] a web-controlled door locking system with email alert using Raspberry Pi was proposed. The main objective of the system is to provide security and simple authorized access to a home. The owner is alerted when someone is in front of the door or when someone knocks on the door. The user can check the image of the visitor through the email sent by the system. The door can be locked or unlocked remotely and opened or closed by the user via a secure web page. The owner can also check the status of the door and control it accordingly. This system becomes a desirable component in today's smart home environment and can be used with a conventional door locking system.

Naresh [28] show that a biometric fingerprint and near-Field Communication (NFC) chip can be used as two-factor authentication with another server authentication security for a controlled access door. He gave a brief description of NFC technology and protocols and a P2P communication protocol over NFC and how he used this technology to create a server-based authentication model. The concept is currently being implemented in prototype form, where NFC and biometrics with server authentication are used as a token to open a door.

Regarding the previous works, the main idea of this one is strengthening simple electronic lock with multimodal biometrics and monitoring the access control system through the GSM network. This study is based on capturing the biometric characteristics of faces and voices and processing them on an embedded architecture such as Raspberry Pi to control the access to a private area. The choice of face and voice modalities because of their high acceptability by humans [29] and the all results obtained in the work of Elmir, *et al.* [30]-[38].

A technical contribution in this paper is the design and implementation of an embedded biometric-based access control system using Raspberry Pi, which includes the integration with an electronic lock and digicode. The system leverages the capabilities of Raspberry Pi, such as its processing power and input/output interfaces, to provide a secure and convenient access control solution. The paper provides a detailed description of the hardware and software components used, as well as the installation and configuration processes. This technical contribution could be useful for practitioners and researchers interested in developing similar systems, as it provides a practical example of the technical aspects involved in implementing an access control system using Raspberry Pi.

Furthermore, an innovation contribution introduces an innovative approach to access control systems by combining biometric-based authentication with Raspberry Pi technology. By using biometric data to verify the identity of users, the system provides a more secure and reliable means of access control than traditional methods based on keys, passwords or RFID cards. The use of Raspberry Pi also enables the system to be more versatile and customizable, as it allows for the integration of various sensors and devices. This innovation contribution could have implications for improving the security and convenience of access control systems in various contexts, such as homes, offices, and public buildings.

The rest of this paper is organized as follows: The second section is devoted to the design, implementation of the proposed system. In the third section, the deployment of the embedded system is presented. Section four, presents the released tests, obtained results and evaluation of the whole system. Finally, the general conclusion summarizes the results obtained and presents some perspectives.

2. DESIGN OF THE PROPOSED SYSTEM

The Smart Grids & Renewable Energy Laboratory (SGRE-Lab) is a renowned research facility at the University Tahri Mohammed of Bechar that specializes in the development and scientific research of smart grids and renewable energies. As a significant contributor to the advancement of clean energy, the laboratory is an essential resource for researchers, students, and industry professionals seeking to explore innovative solutions to today's energy challenges.

To ensure the protection and security of the laboratory's valuable equipment, data, and research findings, an electronic lock-based access control system has been installed. This system, as depicted in Fig. 2, utilizes an electronic locking mechanism that requires either a PIN code to be entered on a numeric keypad or an RFID card to be presented for entry. Once the correct code or RFID card is presented, the electric latch will unlock the door, allowing authorized personnel access to the laboratory. Fig. 3 shows the electric latch mechanism that unlocks the door when the correct code or RFID card is presented. The secure access control system

prevents unauthorized entry, ensuring that only authorized personnel with the proper clearance and credentials can gain access to the laboratory's sensitive resources.

Traditional authorization methods based on the use of passwords or physical media (electronic keys and cards) do not meet modern reliability requirements in determining the identity of the user. Passwords can be intercepted for copying or given to another person. In addition, it is impossible to track the history of individuals who have accessed the laboratory, and there is no record of the history of authorized access.

Fig. 2. The electronic lock-based access control system of SGRE-Lab

In this work, a door locking system is proposed to improve and strengthen the security of the existing system based on biometrics using Raspberry PI technology. This system is based on multimodal biometrics, which integrates facial recognition and speaker verification during personal identification. An SMS notification should be sent to the administrator using the GSM network. And a log of authorized access can be accessed by the administrator via a web portal. Fig. 4 shows the overall diagram of the proposed architecture.

The user first must use his RFID card or enter the PIN code on the electronic lock. Once authorization is verified, the system takes snapshots of the user's face through the camera. The Raspberry Pi identifies the facial authorization, if yes, using a speaker it requests him to say a secret word to the microphone. And if the speaker is identified, then the electric lock should be opened. Otherwise, the lock remains closed.

After analysing and studying the existing system mode of operation (Fig. 3), an improved system is proposed as shown in Fig. 5. A facial recognition module is added after the first authentication by the electronic lock. This module consists of a camera that will take pictures and send them to the raspberry pi. Once the face detection is completed and validated, if the system is unsure of the user's identity, a second voice recognition module should ask the user to say a secret word through the microphone to confirm his identity, then it will confirm the authentication or not.

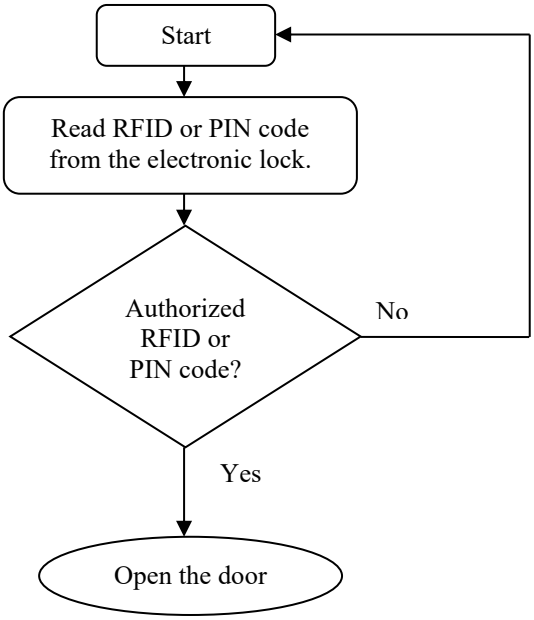


Fig. 3. The operating mode of the existing system at SGRE-Lab

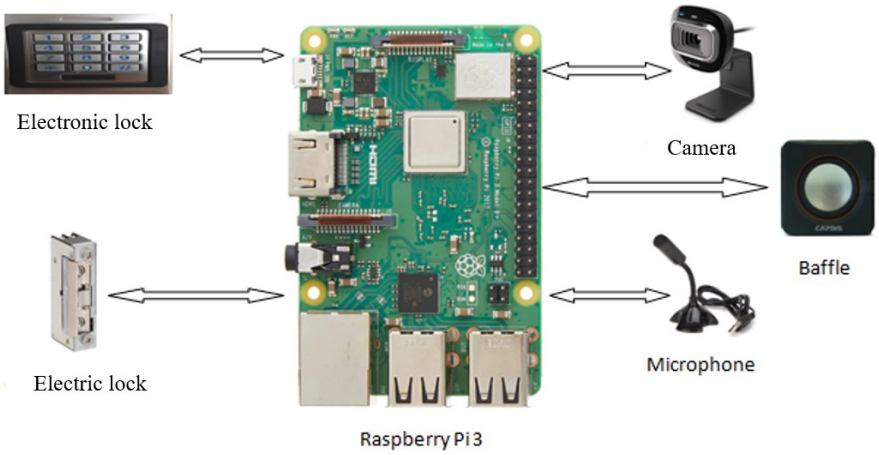


Fig. 4. An overview of the proposed system

As any other biometric system, the proposed algorithm has two modes: one for enrolling users' biometric information and characteristics, and another for biometric authentication that includes face and voice recognition. This second mode is activated when the RFID card is presented, or the PIN code is entered for the usual verification. In this mode, the user's face image is captured via the camera. The system detects the face, and the facial recognition process takes place. The system recognizes a face from the database previously stored using the first mode. If the user's identity is verified with a weak similarity rate, the system activates voice recognition by requesting the user to say the secret word. Once the combination of the two biometric techniques is satisfied, the door must be opened, access recorded, and a notification sent to the administrator via SMS. This algorithm is based on hierarchical fusion of the electronic lock and two biometric modalities as it is shown in the flowchart in Fig. 6. based on the work of Elmir, *et al.* [30], [31].

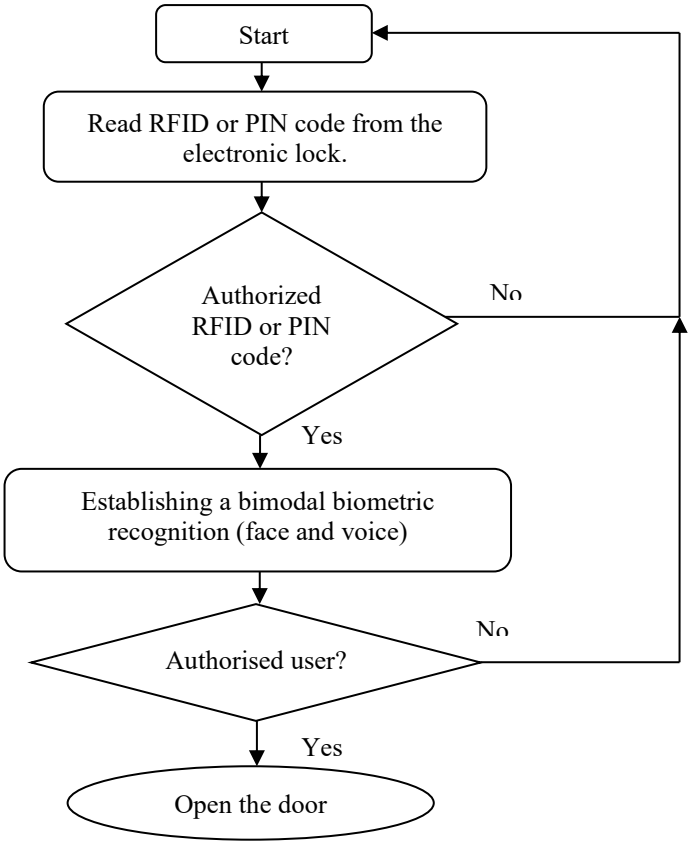


Fig. 5. The operation mode of the proposed system

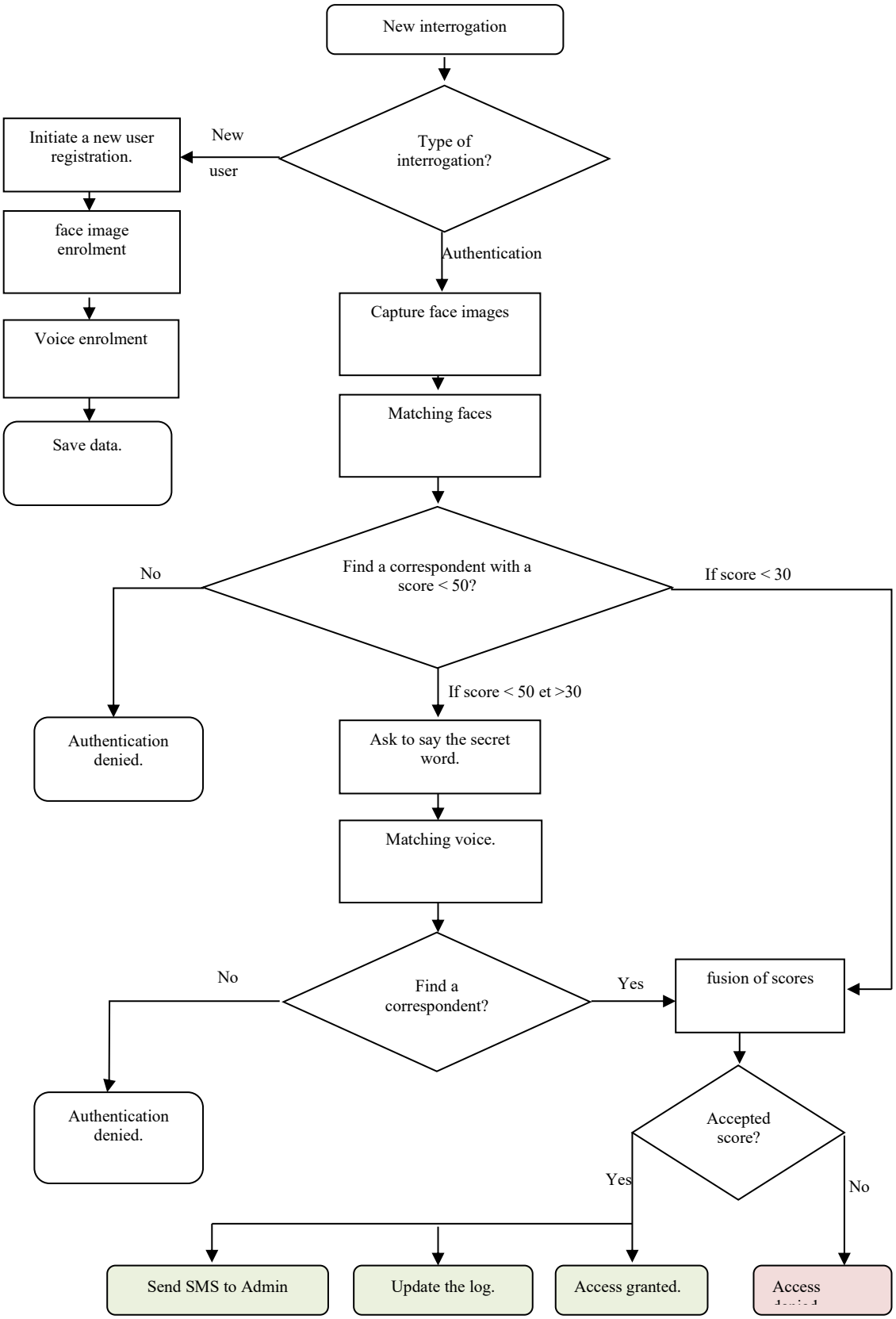
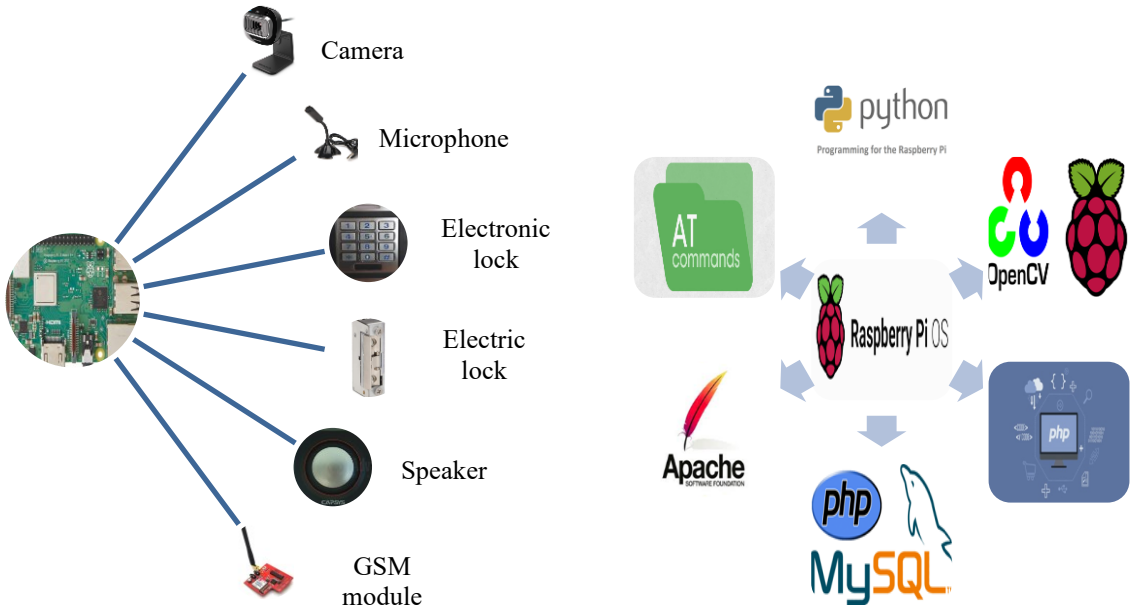


Fig. 6. The flow chart of the proposed system

3. DEPLOYMENT OF THE EMBEDDED SYSTEM

To develop and implement the proposed system, a set of hardware and software shown in Fig. 7, was required:



(a) (b)

Fig. 7. A set of required hardware (a) and software (b)

3.1. The required hardware:

a) The Raspberry Pi 3 is a low-cost basic computer that was originally intended to stimulate interest in computing among school-age children [39]. The Raspberry Pi is contained on a single printed circuit board as it is presented in Fig. 8. and has the following features:
- A 1.2 GHz 64-bit quad-core ARMv8 CPU
- 802.11n Wireless LAN
- Bluetooth 4.1
- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port.

b) Camera: The image is captured using a camera and sent to the Raspberry Pi via USB ports. We can use a standard USB webcam to take photos and videos with the Raspberry Pi.

c) Microphone: The voice sound is captured using a microphone and sent to the Raspberry Pi via the USB port or the jack port.

d) Speaker: it is used by the Raspberry Pi to give instructions, directions, and notifications during communication with him.

Firstly, the various components mentioned earlier are connected as it is shown in Fig. 9. and their schema of connection is presented in Fig. 10.
- Blue LED indicates that the system is turned on and operational.
- Red LED indicates that the authentication mode is in progress.
- Orange LED indicates that the enrolment mode is in progress.
- Green LED indicates that the user is authenticated and authorized.

The relays: are used to conduct electricity to the electric lock to open the door.

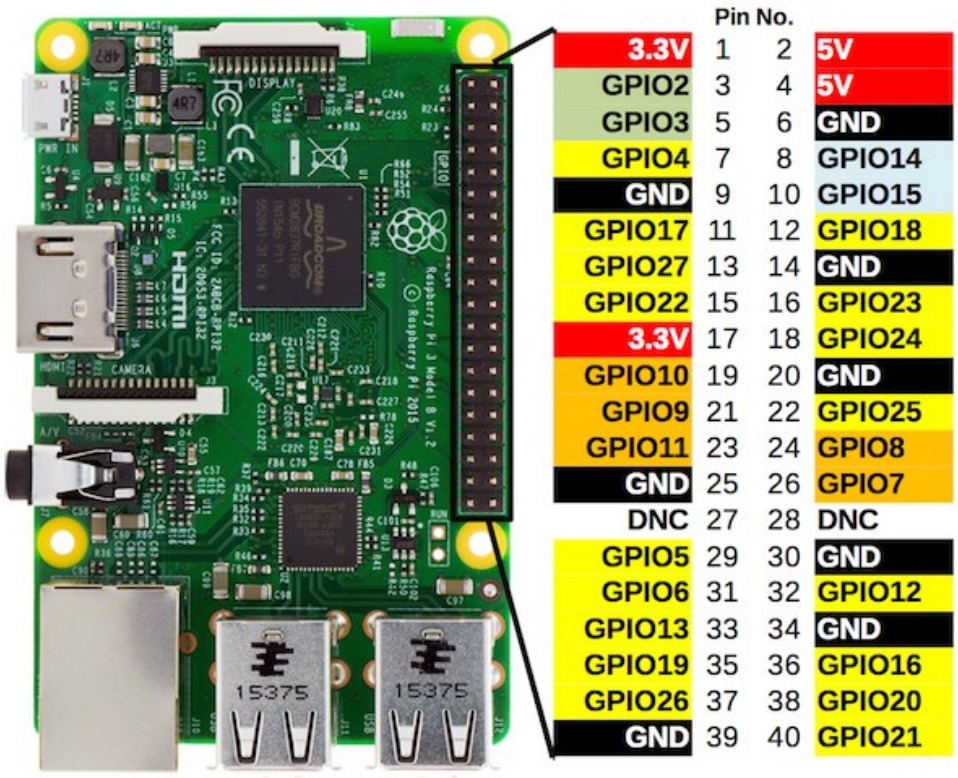


Fig. 8. The Raspberry Pi 3 board with a GPIO port diagram

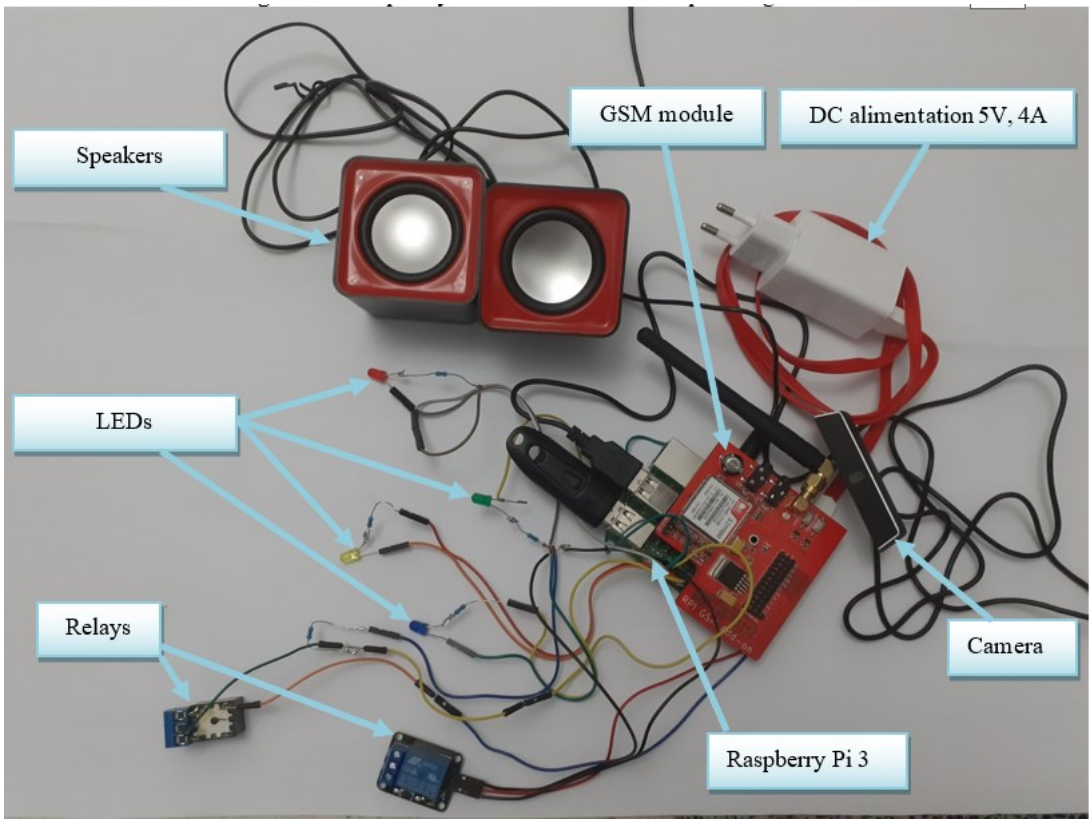


Fig. 9. The connection of the different components of the proposed system

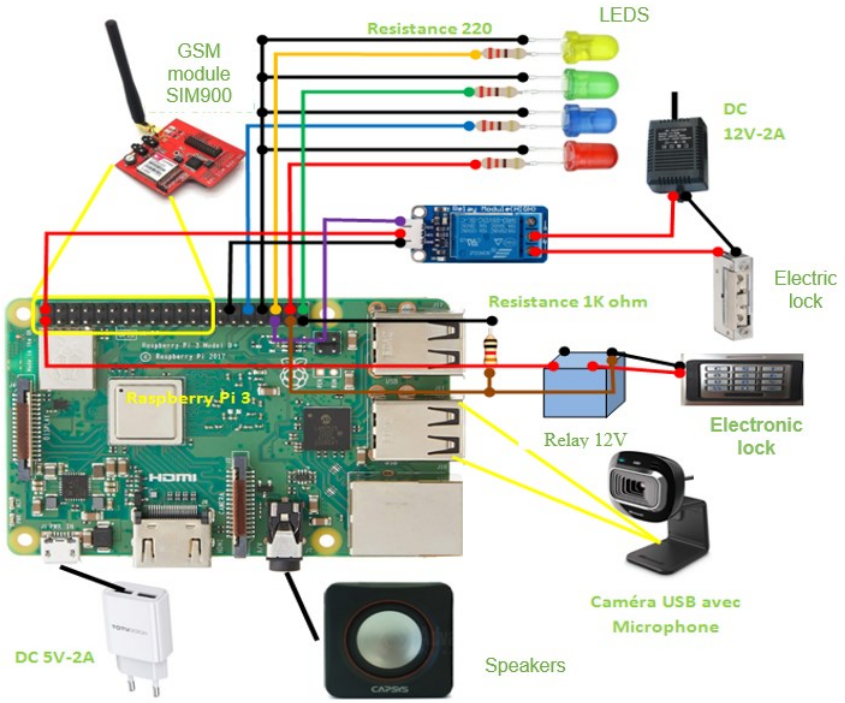


Fig. 10. Components connection schema

3.2. Operating system, softwares, libraries, and development language

a) Raspberry Pi OS: it is a free and open-source operating system based on Debian optimized to run on various Raspberry Pi architectures. The version used in the proposed system is a Raspbian "raspios-buster-armhf".

b) Python Language: it is an interpreted, multi-paradigm, and multi-platform programming language. It favours structured imperative programming, functional programming, and object-oriented programming. It has strong dynamic typing, automatic memory management by garbage collection, and an exception handling system. Python language was used to program facial recognition, cascade classifier Haar, Viola, and Junes suggested a machine learning object detection algorithm known as Haar Cascade to identify objects in videos as well as images built on the principle of features. And for programming voice recognition using the GMM (Gaussian Mixture Model) method and the MFCCs (Mel Frequency Cepstrum Coefficients) method. In this language, we will implement our algorithm that we modelled in section 5 of this chapter. This figure describes the environment called "Thonny Python IDE" used to write instructions in Python. The instructions in this figure will be executed during authentication. The use of the "import cv2" instruction calls the OpenCV library.

c) OpenCV Library: it is a free graphics library originally developed by Intel, specializing in real-time image processing. This library includes many integrated packages for biometric recognition. It contains linear and nonlinear image filtering, geometric image transformation, modification of colour spaces, image smoothing, image thresholding, histograms, etc [40].

d) PHP Language: is a free programming language mainly used to produce dynamic web pages via an HTTP server but can also function as any interpreted language locally. PHP is an imperative object-oriented language. This programming language was used to develop a web administration portal and management of the proposed system. PhpMyAdmin interface is used for creating databases, tables,

e) MySQL: it is a relational database management system (RDBMS). It is distributed under a dual GPL and proprietary license. It is one of the most widely used database management software in the world, both by the public (mainly web applications). It was used to define, store, and manipulate the data of users who are entitled to access system.

f) AT command language: The AT command set consists of a series of short text strings that can be combined to produce commands for operations such as dialling, hanging up, and changing connection parameters. Most dial-up modems use the AT command set in many variations. GSM communication language are a

standard for querying communication modems and even GSM networks, which are used in our system to notify the administrator that a user has accessed the laboratory.
Description of the commands used:

- AT: to test communication between the Raspberry Pi and the GSM modem.
- AT+CMGF=1: to activate the text mode of SMS.
- AT+CMGS="N_tél" "message": to send an SMS to the recipient.

In Fig. 11, we can see samples of some of the AT commands that were used in our study. These commands played a crucial role in facilitating communication between the Raspberry Pi and the GSM module.

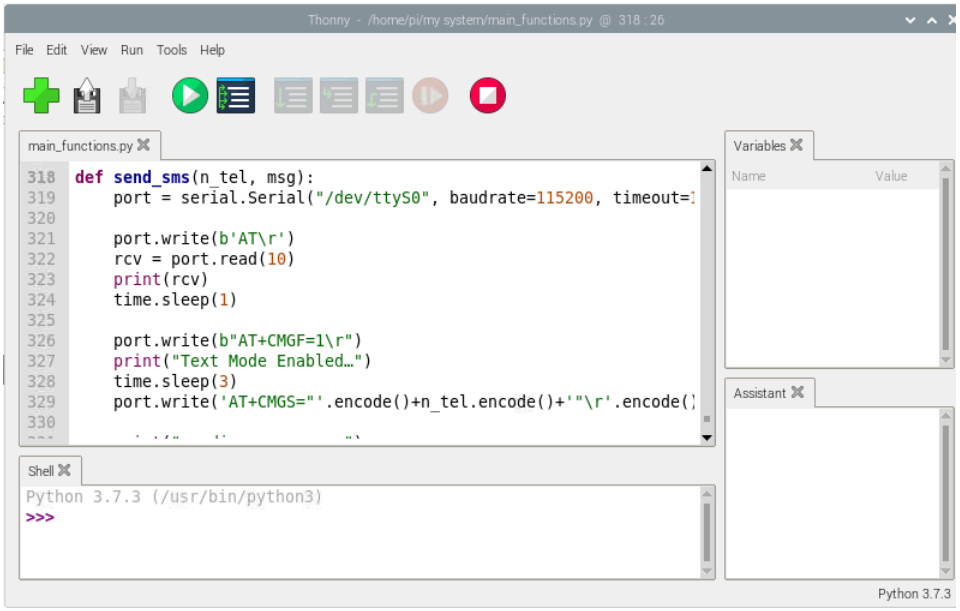


Fig. 11. Samples of some used AT commands

After developing the different software components of the proposed system, the last step is the setup() Fig. 12. This system is composed of two parts, the part written in Python which is the main part of the new access control system, and it is automatically executed every time the Raspberry Pi is power on. The second part, written in PHP which is a web portal intended for the administrator to simplify the administration and management of the system (adding/removing members, enrolments, and updates ...etc.) as shown in Fig. 13. and Fig. 14.

Fig. 12. The electric lock after integration of the proposed system

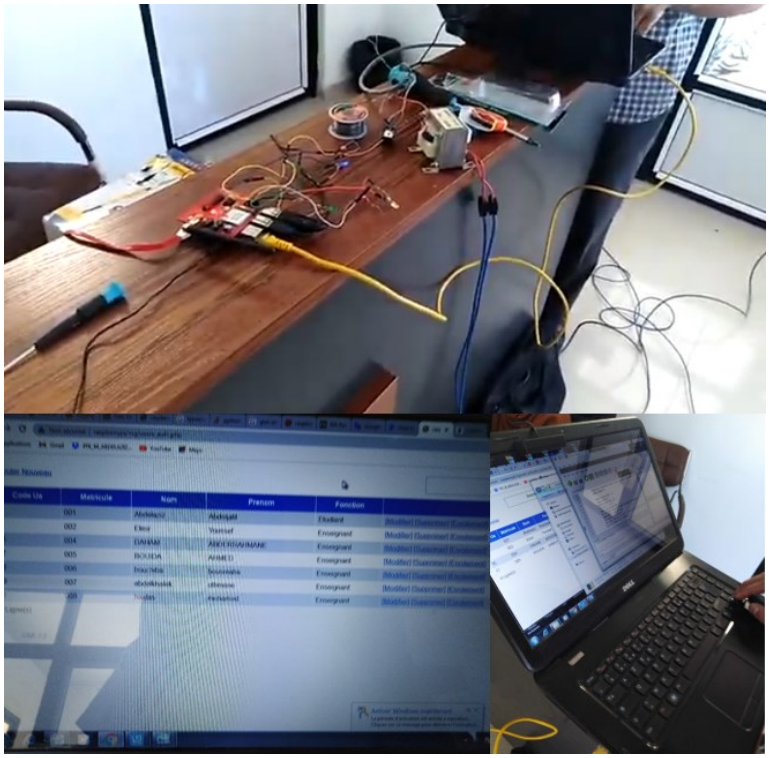


Fig. 13. Administration of the proposed system

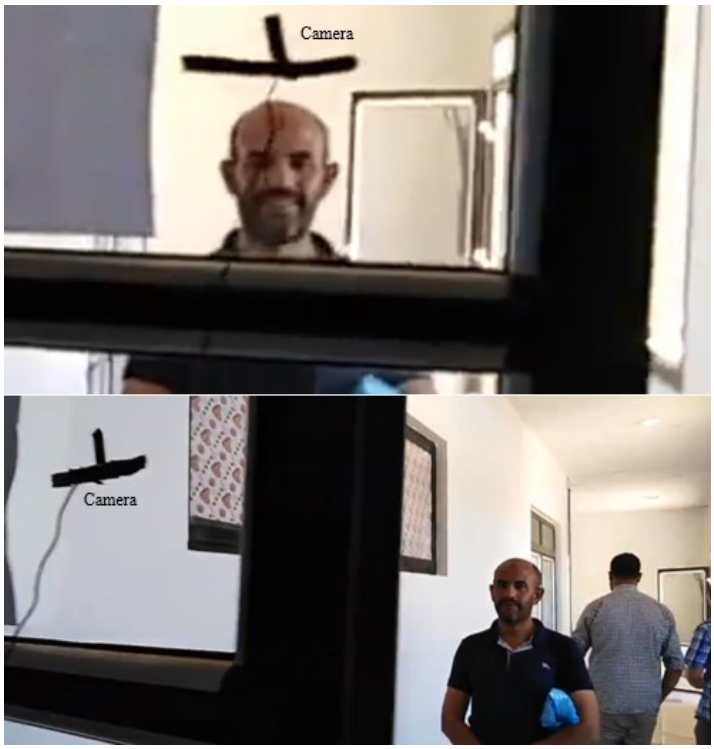
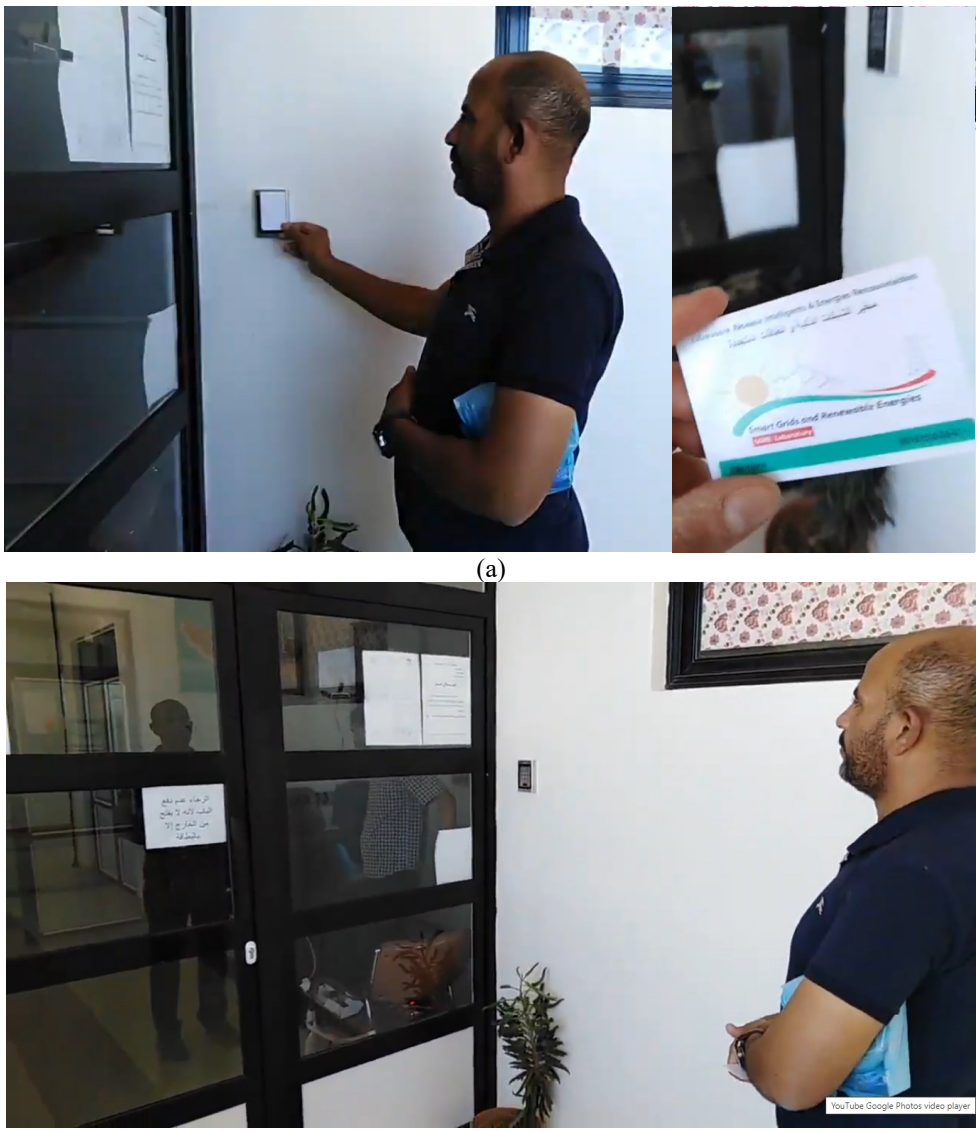


Fig. 14. Adding a new member (enrolment)

4. EXPERIMENTS, OBTAINED RESULTS AND EVALUATION

The final step is testing and evaluating the performance of the proposed system. All the members of the laboratory must use their RFID card or enter the PIN code as usual (Fig. 15. (a)), but now, they have also to

stand in front of the camera then say the secret word enrolled earlier in order to have access to the laboratory (Fig. 15. (b)). A video of demonstration of tests and evaluation is available on YouTube.



(a)

(b)

Fig. 15. (a) Activation of the electronic lock using RFID card, (b) Biometric authentication

The obtained results have shown that this system is capable, to a certain extent, to identify users and determine whether they are authorized or not to access a sensitive area of the laboratory, with a very low number of false acceptances, however, it may increase the false rejection for some genuine users (laboratory members) that are not familiar with this kind of technologies, and by consequence they cannot provide their biometrics correctly even if they enter the PIN code or present their RFID cards the system will not allow them to access to the laboratory.

Furthermore, the proposed access control system exhibits certain other limitations, including potential challenges in varying lighting conditions and vulnerability to spoofing attacks. To address these limitations, future enhancements can include improving the facial recognition algorithm to adapt to different lighting scenarios, incorporating anti-spoofing measures such as liveness detection, and regularly monitoring and evaluating the system's performance. By actively mitigating these limitations, the system can be strengthened to offer improved accuracy, security, and reliability in access control applications.

5. CONCLUSION

In conclusion, this paper aimed to address the problem of enhancing access control systems through the integration of biometric recognition. Traditional methods such as RFID or PIN codes have limitations in ensuring user identification, highlighting the need for more robust and secure solutions.

The significance of biometrics in access control cannot be understated. Biometric recognition offers advantages such as increased security and individual recognition, making it a promising approach for improving access control systems. This paper sought to leverage the benefits of biometrics to develop an advanced access control system.

The proposed solution involved the development of a bimodal biometric process integrating facial recognition and voice recognition. This process was implemented in an embedded system comprising the Raspberry Pi architecture, a camera, a speaker, a microphone, and a GSM module. This integrated system formed the foundation for the successful implementation of the access control system.

The authentication process entailed initial validation through RFID card or PIN code, followed by facial and voice recognition verification. In cases where ambiguity or doubt arose, a second verification was performed to ensure authentication. This multi-modal approach significantly enhanced the security of the access control system.

The achieved results demonstrated the effectiveness of the biometric authentication process in reducing false acceptances. The system showcased improvements in security measures and provided a more reliable means of user identification. However, it is essential to acknowledge that users may encounter difficulties with the biometric authentication process, necessitating user training and education to mitigate any challenges.

Looking forward, there are promising avenues for future work. Recommendations include enhancing the web portal with new functionalities for remote control of the Raspberry Pi, thereby increasing flexibility and convenience for users. Additionally, exploring the use of the GSM network as a transmission support for remote control offers exciting prospects for further research and development.

In conclusion, this research contributes to the advancement of access control systems by leveraging biometric recognition and embedded technology. The findings highlight the potential for improved security, user experience, and convenience in various private places or sensitive areas. The implications of this research extend beyond the scope of this study, offering new possibilities for the development of more sophisticated and effective access control systems.

Acknowledgments

Authors of this work would like to express their sincere gratitude to Prof. Abdelkhalek Othmane head manager of SGRE laboratory for providing valuable materials and resources for this project. They would also like to thank Dr. Abdelmadjid Larbi for his valuable information, advice, and assistance.

REFERENCES

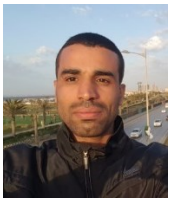
[1] I. Colquhoun, "Design out crime: Creating safe and sustainable communities," *Crime prevention and community safety,* pp. 57-70, 2004, https://doi.org/10.1057/palgrave.cpcs.8140201.
[2] M. Grimaldi, F. Coppola and I. Fasolino, "A crime risk-based approach for urban planning. A methodological proposal," *Land Use Policy,* 2023, https://doi.org/10.1016/j.landusepol.2022.106510.
[3] Y. Z. Lim, "Resident's Satisfaction towards the Gated and Guarded Community in Klang Valley," *Doctoral dissertation, Tunku Abdul Rahman University College*, 2023, https://eprints.tarc.edu.my/id/eprint/23795.
[4] R.-I. Vatasoiu, R.-A. Bratulescu, S.-A. Mitroi, M.-A. Sachian, A.-M. Tudor and A.-G. Vintila, "The Importance of Security and Safety in a Smart City," in *21st International Conference on Informatics in Economy*, 2022, https://doi.org/10.1007/978-981-19-6755-9_2.
[5] M. O. Ahmad, G. Tripathi, F. Siddiqui, M. A. Alam, M. A. Ahad, M. M. Akhtar and G. Casalino, "BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities," *Sensors ,* vol. 23, no. 5, 2023, https://doi.org/10.3390/s23052757.
[6] M. Arif and M. Jawwad, "Physical Security; Logical Security," *Auditing Information System,* vol. 57, 2023. https://books.google.co.id/books?id=Pwv_4mnIRFEC.
[7] J. Vacc. *Biometric technologies and verifiction systems.* Elsevier, 2007, https://books.google.co.id/books?id=Pwv_4mnIRFEC.
[8] N. Clarke. *Transparent user authentication: biometrics, RFID and behavioural profiling*. Springer Science & Business Media, 2011, https://doi.org/10.1007/978-0-85729-805-8.
[9] A. Jain, L. Hong, S. Pankanti and R. Bolle, "An identity authentication system using fingerprints," *Proceedings of the IEEE,* vol. vol 85, no. 9, pp. 1365-1388, 1997, https://doi.org/10.1109/5.628674.
[10] L. Hong, A. Jain, S. Pankanti and R. Bolle. *Identity authentication using fingerprints*. AVBPA, 1997, https://doi.org/10.1007/BFb0015985.

[11] P. Hazarika and D. A. Russell, "Advances in fingerprint analysis," *Angewandte Chemie International Edition,* vol. 51, no. 15, pp. 3524-3531, 2012, https://doi.org/10.1002/anie.201104313.
[12] C. Huynh and J. Halámek, "Trends in fingerprint analysis," *TrAC Trends in Analytical Chemistry,* vol. 82, pp. 328-336, 2016, https://doi.org/10.1111/1556-4029.14313.
[13] M. González, R. P. Gorziza, K. d. C. Mariotti and R. P. Limberger, "Methodologies applied to fingerprint analysis," *Journal of Forensic Sciences,* vol. 65, no. 4, pp. 1040-1048, 2020, https://doi.org/10.1111/1556-4029.14313.
[14] C. L. Tisse, "Contribution à la Vérification Biométrique de Personnes par Reconnaissance de l'Iris," *Montpellier,* 2003, https://www.theses.fr/2003MON20071.
[15] C.-L. Tisse, L. Torres, L. Martin and M. Robert, "Systèmes biométriques pour la vérification d'individu. Un exemple: l'iris," *Traitement du signal,* vol. 22, no. 2, 2005, https://core.ac.uk/download/pdf/15486709.pdf.
[16] J. Daugman, "How iris recognition works," *The essential guide to image processing,* pp. 715-739, 2009, https://doi.org/10.1016/B978-0-12-374457-9.00025-1.
[17] C. Yam, M. Nixon and J. Carter, "On the Relationship of Human Walking and Running: Automatic Person Identification by Gait," *ICPR,* pp. 1051-4651, 2002, https://doi.org/10.1109/ICPR.2002.1044691.
[18] C. Yam, M. S. Nixon and J. N. Carter, "Automated person recognition by walking and running via model-based approaches," *Pattern recognition ,* vol. 37, no. 5, pp. 1057-1072, 2004, https://doi.org/10.1016/j.patcog.2003.09.012.
[19] P. Yan and K. Bowyer, "Empirical Evaluation of Advanced Ear Biometrics," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* p. 41, 2005, https://doi.org/10.1109/CVPR.2005.450.
[20] N. Alay and H. H. Al-Baity, "Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits," Sensors, vol. 20, no. 19, p. 5523, 2020, https://doi.org/10.3390/s20195523.
[21] I. Benchennane, "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus," *Univ USTO Oran,* vol. 20, no. 19, p. 5523, 2016, https://doi.org/10.3390/s20195523
[22] M. Bourezak, S. Chetibi, and A. E. Soukkou, "Conception et réalisation d'un système de pilotage d'une installation domotique à distance (IoT) à base d'Arduino, *Doctoral dissertation, Université de Jijel*, 2019, http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/279.
[23] S. Masmoudi, "Malleable privacy-enhancing-technologies for privacy-preserving identity management systems," *Doctoral dissertation, Institut polytechnique de Paris*, 2022, https://www.theses.fr/2022IPPAS023.
[24] D. C. Crystalynne, S. B. Jaswinder, R. H. Jocelyn, J. C. A. Ditche, S. D. C. Melvie and C. I. Jaira, "Development ofMicrocontroller-Based Biometric Locker System with Short Message Service," *Lecture Notes on Software Engineering,* vol. vol 4, pp. 103-106, 2016, https://doi.org/10.7763/LNSE.2016.V4.233.
[25] R. Dhana Lakshmi, P. Leeela Priya, G. Lokanyaa and J. Sharmila, "Security System using Raspberry Pi With Door Lock Controller," *International Journal of Engineering Science and Computing,* vol. vol 7, no. issue 4, pp. 10090-10094, 2017, https://test.globalinfocloud.com/technodigisoftnew/wp-content/uploads/2019/07/Door-Lock-System.pdf.
[26] R. Sourav, U. Nasir, H. Zahirul and K. Jahidul, "Design and Implementation of the Smart Door Lock System with Face Recognition Method using the Linux Platform Raspberry Pi," *International Journal of Computer Science and Network,* p. 210023, 2018, http://ijcsn.org/articles/0706/Design-and-Implementation-of-the-Smart-Door-Lock-System-with-Face-Recognition-Method-using-the-Linux-Platform-Raspberry-Pi.html.
[27] S. Dhiraj, "Web Controlled Door Lock System with Email Alert using Raspberry Pi," *IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250- 3021,* vol 9, no. 3, pp. 29-38, 2019, https://iosrjen.org/Papers/vol9_issue3/Series-3/D0903032938.pdf.
[28] K. M. Naresh, "Nfc Based Dual Authentication Access Control System With Biometric, IJSRET: International Journal of Scientific Research & Engineering Trends," *International Journal of Scientific Research & Engineering*, vol 6, no. 1, pp. 124-128, 2020, http://ijrar.com/upload_issue/ijrar_issue_20543995.pdf.
[29] S. Hocquet, "Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite," *Thèse de doctorat, Université François Rabelais Tours,* p. 24, 2007, https://www.theses.fr/2007TOUR4028.
[30] Y. Elmir, Z. Elberrichi and R. Adjoudj, "Multimodal biometric using a hierarchical fusion of a person's face, voice, and online signature," *Journal of Information Processing Systems,* vol. 10, no. 4, pp. 555-567, 2014, https://doi.org/10.3745/JIPS.02.0007.
[31] H. Purohit, and P. K. Ajmera, "Optimal feature level fusion for secured human authentication in multimodal biometric system," *Machine Vision and Applications*, vol. 32, pp. 1-12, 2021, https://doi.org/10.1007/s00138-020-01146-6.
[32] Y. Elmir, S. Al-Maadeed, A. Amira and a. A. Hassaine, "Multi-modal biometric authentication system using face and online signature fusion.," in *Qatar Foundation Annual Research Forum Volume*, 2012, https://doi.org/10.5339/qfarf.2012.CSP32.
[33] Y. Elmir and a. N. Khelifi, "Secured biometric identification: hybrid fusion of fingerprint and finger veins," *International Journal of Information Technology and Computer Science ,* vol. 11, no. 5, pp. 30-39, 2019, https://doi.org/10.5815/ijitcs.2019.05.04.
[34] Y. Elmir, "A Hierarchical Fusion Strategy in Multibiometric Authentication Systems," *Sidi Bel Abbes*, 2015, https://www.theses-algerie.com/5075728578124552/these-de-doctorat/universite-djillali-liabes---sidi-bel-abbes/a-hierarchical-fusion-strategy-in-multibiometric-authentication-systems.

[35] A. Khider, "Un système biométrique multimodal basé sur la fusion visage-iris," *Doctoral dissertation,* 2023, http://dspace.univ-guelma.dz/jspui/handle/123456789/14246.
[36] Y. Elmir and S. M., "Model-View-Controller based Online Face Recognition System," *Int J Web Applications,* vol. 11, no. 2, pp. 49–57, 2019, https://doi.org/10.6025/ijwa/2019/11/2/49-57.
[37] Y. Elmir, N. Karour and S. O. Jaafri, "A Reduced Feature Representation based Online Signature Authentication," *Journal of Information Security Research ,* vol. 10, no. 2, 2019, https://doi.org/10.6025/jisr/2019/10/2/39-47.
[38] S. Benkerzaz, E. Youssef and a. D. Abdeslem, "The Contribution of the Neural Network to the Improvement of Speech Recognition," in *International Conference on Information Systems and Advanced Technologies (ICISAT)*, 2021, https://doi.org/10.1109/ICISAT54145.2021.9678470.
[39] M. Kölling, "Educational programming on the Raspberry Pi," *Electronics,* vol. 5, no. 3, 2016, https://doi.org/10.3390/electronics5030033.
[40] A. Hussain, M. Hasnain, M. Faseeh-Ul-Haq, and F. Hussain, "Door Unlock by Face Recognition (DUFR)," *International Journal of Computer Science and Software Engineering*, vol. 8, no. 12, pp. 294-303, 2019, https://ijcsse.org/published/volume8/issue12/p1-V8I12.pdf.

BIOGRAPHY OF AUTHORS

Youssef Elmir, received his BSc in Computer Science from Univ. of Sidi Bel Abbès in Algeria in 2005. He then earned his MSc in Computer Science from Mohamed Boudiaf Univ. of Sciences and Technology in Oran, Algeria in 2007, and his DSc in Computer Science from Univ. of Sidi Bel Abbès in Algeria in 2015. After completing his MSc, he worked as an Assistant Professor at Univ. of Adrar. Following the completion of his DSc, he worked as an Associate Professor at Univ. of Bechar then at ESTIN of Bejaia. elmir@estin.dz, 0000-0003-3499-507X.



Abdeldjalil Abdelaziz, is a dedicated and motivated professional with a strong academic background. He holds an MSc degree from the University of Bechar in Algeria, which he earned in 2021. Prior to that, he obtained an engineering degree from the same university, showcasing his commitment to continuous education and professional development. With his experience as a Technical Inspector Specialist, Abdeldjalil has gained valuable expertise in the field of computer engineering. His academic achievements and practical knowledge make him a valuable asset in the domains of information technology and technical inspection.

Mohammed Haidas, is an accomplished researcher and associate professor of Electrical Engineering at the University of TAHRI Mohammed Bechar. With expertise in artificial intelligence, telecommunications and renewable energies, Dr. Haidas has made significant contributions to the field through his innovative research. He has been involved in optimizing parameters of power quality conditioners, integrating wind energy for electricity production, and developing intelligent systems such as autonomous obstacle-avoiding robots.