www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 17(1), Jan-April 2026, 166-181. ISSN: 2007-1558. https://doi.org/10.61467/2007.1558.2026.v17i1.1270

Innovation in Biometric Security and Digital Transformation: Redesigning Security Models in Society

María Esmeralda Arreola Marín[1], José Iraic Alcantar Alcantar[1], Mariela Chávez Marcial[1], Edgar Gonzalo Cossio Franco[2]
[1] Tecnológico Nacional de México / ITS de Ciudad Hidalgo, México.
[2] Instituto de Información Estadística y Geográfica de Jalisco, México.
marreola@cdhidalgo.tecnm.mx, jalcantar@cdhidalgo.tecnm.mx, mchavez@cdhidalgo.tecnm.mx & edgar.cossio@iieg.gob.mx

Abstract. This research aimed to generate applied knowledge to support the design, development, and implementation of an intelligent biometric system based on facial recognition, oriented towards strengthening security models in both public and private institutions. A technological solution was developed that integrates hardware, software, and artificial intelligence algorithms to provide access that is precise, rapid, secure, and hygienic, without requiring physical contact or the use of passwords or identification cards. The system supports multiple concurrent functions, including body temperature measurement and real-time logging of entries and exits, which may contribute to reducing risks associated with fraud and human intervention. The system was implemented at the Instituto Tecnológico Superior de Ciudad Hidalgo, where it was used to automate campus access for administrative personnel, academic staff, and students, in accordance with the principles associated with Society 5.0 and the development of intelligent and sustainable environments. Facial recognition is described as offering high levels of accuracy and adaptability, maintaining functionality under varying conditions such as mask usage and changes in lighting. The study adopted a qualitative research approach and employed an evolutionary prototyping development model, using TensorFlow and Python as the primary implementation tools. As a result, an access management system was developed that can be regarded as an innovative contribution to institutional security, while also supporting the integration of disruptive technologies within educational settings. In this context, automation and advanced authentication mechanisms are positioned as relevant components of contemporary infrastructural development.
Keywords: biometrics, facial recognition, TensorFlow, CNN, microcontrollers.

Article Info
Received Aug 26, 2025
Accepted Dec 11, 2025

1 Introduction

Following the global COVID-19 pandemic, traditional models of security and access control were increasingly questioned due to their sanitary and operational vulnerabilities. In this context, many public and private institutions undertook accelerated processes of digital transformation aimed at minimising physical contact and phasing out mechanisms such as manual logs, printed tickets, or easily manipulated identification cards. This transition not only responded to immediate public health concerns but also appears to have facilitated the reconfiguration of security models, contributing to a broader shift towards intelligent automation and enhanced protection of personal identity.

Within this scenario, biometric systems have emerged as advanced technological solutions, integrating methods such as facial recognition, fingerprint analysis, and iris detection. One of the principal advantages associated with their adoption lies in improved identification accuracy, which can reduce impersonation risks, enhance access traceability, and support higher levels of security. In addition, these systems may promote hygiene and operational efficiency by removing the need for physical contact, manual password input, or direct staff involvement in access validation. Even in situations involving face mask usage,

facial recognition technologies have been reported to maintain functional performance through the application of algorithms capable of identifying distinctive biometric features.

An illustrative example of this approach is the project implemented at the Instituto Tecnológico Superior de Ciudad Hidalgo (ITSCH), where an automated access control system based on facial recognition was deployed. The system regulates both vehicular and pedestrian access, providing students and academic staff with rapid, secure, hygienic, and personalised entry. For external visitors, access protocols require prior coordination with authorised personnel, which may assist in managing human traffic and reinforcing institutional security practices.

The operation of the system is based on the integration of artificial intelligence (AI) and Internet of Things (IoT) technologies. A device installed at each access point captures the user's facial image and transmits it to a central server, where identity verification is performed in real time using a trained neural network. This architecture enables autonomous decision-making and a streamlined user experience, characteristics commonly associated with intelligent environments as conceptualised within Society 5.0 [9].

From a development perspective, the evolutionary prototyping model, widely applied in software engineering contexts, was adopted [6]. The process was organised into successive stages, including the definition of general and specific objectives, collection of functional and technical requirements, preliminary design, iterative development, and continuous validation. This methodology allowed progressive refinement of the system through real-world testing and feedback, aligning with continuous improvement practices and the principles of the Deming Cycle (Plan–Do–Check–Act).

Overall, the proposed solution demonstrates precision, security, and operational efficiency, while also exhibiting adaptability across different contexts, including educational, corporate, industrial, and governmental settings. Owing to these characteristics, it can be regarded as a promising exploration for rethinking conventional security models in line with digital transformation initiatives, responsible automation, and human-centred societal frameworks. Figure 1 presents a schematic representation of the prototype architecture.
.

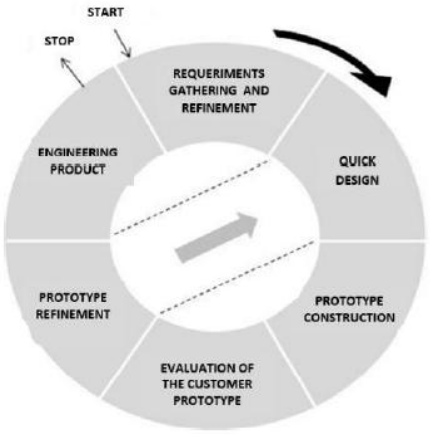

Fig. 1. Prototype Architecture.

The development of a functional prototype in contexts of technological innovation begins with the precise definition of system requirements and the identification of critical variables to be explored. This stage is widely regarded as fundamental, as it establishes the technical, operational, and contextual parameters that guide subsequent design decisions. Accordingly, a detailed analysis of the essential elements required for structuring the prototype is conducted, taking into account not only functional performance but also feasibility in terms of implementation and adaptation to real-world environments.

During the conception phase, the most appropriate type of prototype—conceptual, functional, evolutionary, or validation—is determined through a comprehensive evaluation of factors such as ergonomic design, physical and digital architecture, material selection, structural proportions, and user–device interaction. This approach reflects the view that prototyping extends beyond a purely technical task and also constitutes a design-oriented process centred on user experience, particularly in systems that involve biometric interaction.

Subsequently, empirical validation is undertaken through pilot tests or controlled testing sessions, in which the prototype is exposed to a representative group of end users. During this phase, qualitative observations and quantitative performance indicators are collected in order to assess aspects such as efficiency, usability, stability, and user acceptance. The active involvement of users, who are able to share perceptions, suggestions, and observations, is generally considered a key input for system refinement [15].

Finally, a reflective and systematic evaluation of the results is conducted, not only to verify alignment with the initial objectives but also to identify opportunities for continuous improvement. This feedback-oriented analysis is considered essential for optimising the technological solution, as it integrates practical insights with principles of iterative design, contextual adaptability, and human-centred development, in line with the conceptual framework of Society 5.0. In this way, prototyping can be understood as a strategic instrument not only for validating technical feasibility but also for consolidating innovative, ethical, and sustainable proposals within complex environments [6].

2 Theoretical Framework

The development of this research required the implementation of advanced artificial intelligence tools, particularly those associated with deep learning. In this case, convolutional neural networks (CNNs) were selected due to their well-documented effectiveness in image classification tasks, especially in facial recognition systems. This class of neural network constitutes an algorithmic architecture designed to emulate, to a certain extent, the functioning of the human visual cortex, thereby enabling the hierarchical extraction of visual features, from low-level elements to more complex patterns.

CNNs are a subcategory of machine learning and constitute a central component of deep learning approaches. They are structured as layered architectures comprising an input layer, multiple hidden layers—most notably convolutional, activation, and pooling layers—and an output layer. Each node, or artificial neuron, establishes weighted connections with other neurons and transmits information to subsequent layers only when the activation value exceeds a defined threshold. This mechanism is commonly interpreted as resembling biological synaptic behaviour and enables progressive learning through the iterative adjustment of weights.

Within the domain of computer vision, convolutional networks have demonstrated strong performance due to their capacity to process complex inputs such as images, video sequences, and, in some configurations, audio signals. In this research, their application focuses on the detection, analysis, and classification of facial features to support accurate identification of registered users. This task, situated within the field of computational biometrics, is further supported through the use of specialised development tools.

For the construction of the facial recognition model, TensorFlow was employed. TensorFlow is an open-source platform developed by Google and is widely recognised within the artificial intelligence community for its versatility, scalability, and computational capabilities. It facilitates the design, training, and evaluation of deep learning models through extensive libraries, preconfigured layers, optimisation algorithms, and visualisation utilities. In addition, TensorFlow provides application programming interfaces that enable deployment across mobile devices, web environments (via TensorFlow.js), and embedded systems, thereby expanding the range of potential implementations [6].

Facial image acquisition for system input was carried out using a digital camera connected to a microcontroller programmed on the Arduino platform. This configuration was selected to support a low-cost and adaptable design. Arduino represents a technological solution that integrates three essential components:

1. An open-source electronic board containing a programmable microcontroller,
2. A cross-platform integrated development environment (IDE) for writing, compiling, and uploading code, and
3. A C-based programming language enriched with libraries that simplify the handling of sensors and actuators.

In this system, the microcontroller functions as an autonomous computational unit capable of interacting with devices in the physical environment. On the one hand, sensors such as cameras are employed to capture environmental information, in this case human facial images. On the other hand, actuators are integrated as components capable of executing physical actions in response to electrical signals, such as opening an access point following a successful identification.

The biometric component of the system is based on the statistical analysis of unique and non-transferable physical characteristics, including facial features. In this research, the CNN model was trained to identify these traits and associate them

with an alphanumeric label corresponding to the institutional control number assigned to each user, whether student or staff member. This identifier is linked to a relational database that stores complementary information, such as name, institutional role, and additional metadata relevant for identity validation.

To represent the structure of data storage and management, a relational model was developed to enable a clear visualisation of the relationships among the different tables that constitute the database. This model not only organises and structures the information but also is intended to facilitate efficient interaction between system components, thereby supporting traceability, security, and data integrity.

Taken together, this technological architecture can be characterised as a robust and innovative solution within the domain of biometric security and digital transformation, aligned with principles of precision, automation, and adaptability to real-world settings. The combined use of neural networks, embedded systems, and intelligent databases represents a step towards the development of intelligent and secure environments, in which the integration of hardware and software reshapes conventional access control models in contemporary institutional contexts. Figure 2 presents the relational model.

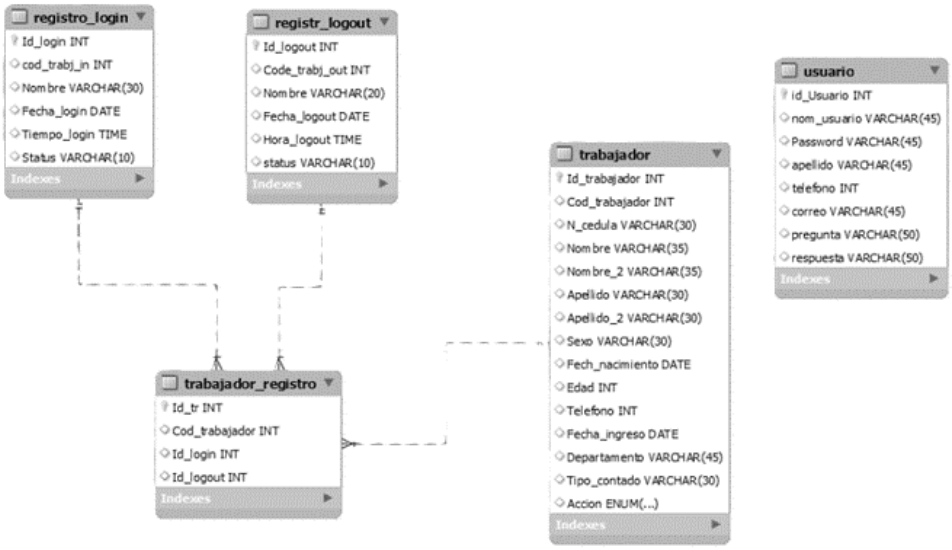

Fig. 2. Relational Model of the Biometric System Database.

The design of the relational model represents a fundamental component in the architecture of intelligent solutions aimed at security, traceability, and efficient management of digital identity. This model, built on principles of normalization, referential integrity, and scalability, ensures a robust and flexible structure for the storage, retrieval, and analysis of biometric data such as facial images, fingerprints, and associated vehicle records.

2.1. Biometric security and digital transformation: a toward society 5.0 approach

Biometric security has increasingly been recognised as a relevant alternative for authentication mechanisms in the context of digital transformation, particularly within the conceptual framework of Society 5.0 [15], where technological development and human-centred objectives are intended to converge in addressing societal challenges. This paradigm seeks to integrate physical and cyber spaces, with an emphasis on human well-being through the use of tools such as artificial intelligence and advanced cyber–physical systems.

Biometric approaches can provide a robust means of strengthening the security and integrity of access processes, as they rely on unique physical characteristics of individuals, thereby reducing susceptibility to impersonation techniques commonly associated with conventional methods, including passwords or physical identification cards. At the same time, issues related to equity, privacy, vulnerability to adversarial attacks, and the ethical management of biometric data require careful consideration.

From a digital transformation perspective, the integration of biometric-based intelligent systems, supported by Internet of Things architectures, extended digital connectivity, and machine learning techniques, may contribute to improved operational

efficiency while also reshaping individual and collective experiences. This integration is often framed as aligning with values of sustainability, inclusion, and resilience that are central to the Society 5.0 vision.

Taken together, the convergence of these elements positions biometrics as a potentially strategic component in the development of secure, human-centred, and intelligent environments. Such an approach can be interpreted as supporting identity protection while reflecting a model of technology that seeks to be sustainable, responsible, and oriented towards societal benefit.

2.2. Society, innovation, and digital transformation

Society 5.0, conceived in Japan in 2016 [6] as part of a national development strategy, represents an evolution of digital transformation paradigms by promoting a more integrated relationship between humans and emerging technologies. Rather than constituting solely a technological advance, this vision is intended to respond to broader societal demands to reconsider the relationship between scientific and technological progress and human well-being. In contrast to Industry 4.0, which prioritises automation and the digitalisation of production processes, Society 5.0 places human beings at the centre of the digital ecosystem, fostering development that is inclusive, sustainable, and ethically responsible.

From this perspective, innovation in biometric security has become a central element in the consolidation of digitally transformed societies. Biometric-based solutions not only address contemporary challenges related to security and authentication but also enable more intelligent management of personal data, supporting secure access, interaction traceability, and identity control while seeking to avoid compromising privacy. Technologies such as facial, fingerprint, and iris recognition—supported by artificial intelligence and machine learning—are no longer viewed merely as technical tools, but rather as integral components in the development of smart urban environments, automated mobility systems, and digital public services.

Within this framework, digital transformation extends beyond simple process digitisation and involves a deeper reconfiguration of social, economic, and cultural structures. The convergence of artificial intelligence (AI), the Internet of Things (IoT), collaborative robotics, augmented reality, and cyber–physical systems has reshaped institutional interactions with users, contributing to improvements in operational efficiency, resource optimisation, and user experience. The strategic objectives commonly associated with this advanced digital society include:

1. Strengthening competitiveness through constant innovation
2. Implementing technological solutions adaptable to different social contexts
3. Democratizing access to disruptive technologies
4. Promoting sustainable models of economic and environmental development
5. Encouraging entrepreneurship and the creation of new business models

Aligned with this integrative vision, an intelligent vehicle recognition system has been proposed that operates through advanced biometric technologies. This development, grounded in applied innovation principles, is based on the collection of vehicle images under varied operational conditions, including changes in viewing angle, lighting, and resolution, in order to build a robust classification and authentication model. The system incorporates automated licence plate recognition, visual pattern detection, and relational data storage within a MySQL database, integrating personal records of vehicle owners, institutional staff, and specific vehicle characteristics.

This approach not only aims to strengthen access protocols for critical infrastructures such as educational or governmental institutions but also reflects the underlying ethos of Society 5.0. In this context, advanced technologies are leveraged to support collective well-being while maintaining humans as active participants rather than passive recipients, positioning them as primary beneficiaries of systems designed to adapt to their needs, respect personal dignity, and enhance quality of life.

Consequently, such innovations can be regarded as contributing to the development of intelligent environments that prioritise security, efficiency, and sustainability—key pillars of a human-centred and technologically advanced society. This contribution is illustrated by a proposed vehicle recognition system based on licence plate analysis, developed through extensive research. For its implementation, a dataset comprising images of vehicles entering the ITSCH facilities was collected, capturing multiple angles and lighting conditions to reinforce model robustness. In parallel, licence plate data, vehicle attributes, and owner information were recorded in a MySQL database, as shown in Figure 3.

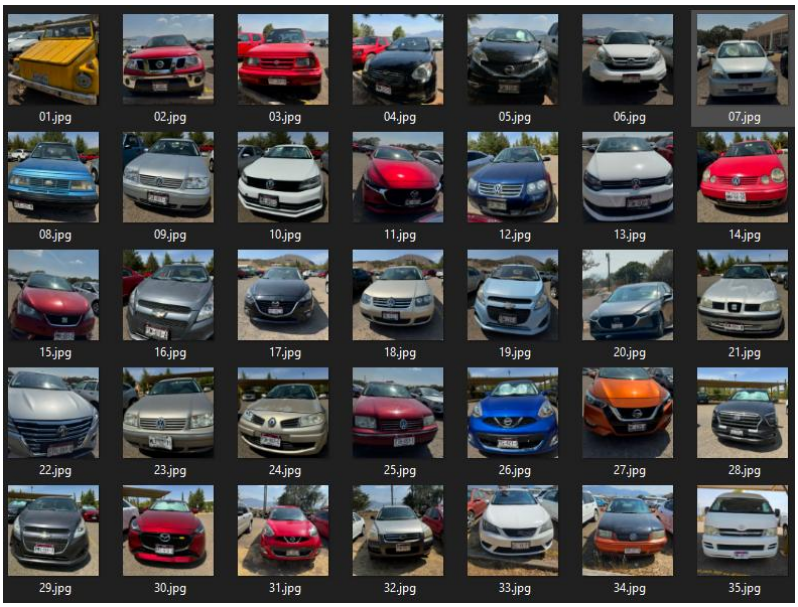

Fig. 3. Training result: accuracy and loss.

Regarding the architecture of the model used for the recognition of vehicles and their occupants at the Instituto Tecnológico Superior de Ciudad Hidalgo (ITSCH), it is based on a Convolutional Neural Network (CNN). This architecture is designed to handle high-resolution images and efficiently extract relevant features, which is fundamental for the accurate recognition of license plates and vehicles (see Figure 4).

Model: "sequential"

Layer (type)	Output Shape	Param #
rescaling (Rescaling)	(None, 512, 512, 3)	0
max_pooling2d (MaxPooling2D)	(None, 256, 256, 3)	0
conv2d (Conv2D)	(None, 254, 254, 64)	1,792
max_pooling2d_1 (MaxPooling2D)	(None, 127, 127, 64)	0
conv2d_1 (Conv2D)	(None, 125, 125, 128)	73,856
max_pooling2d_2 (MaxPooling2D)	(None, 62, 62, 128)	0
flatten (Flatten)	(None, 492032)	0
dense (Dense)	(None, 128)	62,980,224
dense_1 (Dense)	(None, 38)	4,902

Fig. 4. Training Parameters.

The first stage of the model architecture involves preprocessing of the input data. Vehicle images with a resolution of 512 × 512 pixels are scaled to a value range between 0 and 1 through a normalisation process. This is achieved by dividing each pixel value by 255, a procedure that is commonly used to facilitate model training by standardising the input data.

The model comprises multiple convolutional layers interspersed with pooling layers. The convolutional layers are designed to extract both low-level and higher-level features from the images, including edges, textures, and more complex shapes. Each convolutional layer applies filters (kernels) of size 3 × 3 to generate feature maps. The Rectified Linear Unit (ReLU) activation function is employed in these layers, introducing non-linearity into the model and thereby supporting the learning of more complex feature relationships.

The output layer contains a number of neurons corresponding to the number of target classes, such as vehicle types or owner categories, and applies the softmax activation function to produce a probability distribution across these classes. The model was trained for 1000 epochs, a value selected with reference to prior tests conducted in facial recognition experiments (see Figure 5).

Fig. 5. Training Result: Accuracy and Loss.

During the training phase, accuracy is monitored on both the training and validation datasets. This information is used to adjust hyperparameters and to support improvements in overall model performance. Upon completion of training, the model is evaluated using an independent test set in order to assess its generalisation capability and performance on previously unseen data.

The convolutional neural network architecture presented was found to be effective for vehicle recognition and occupant identification within the ITSCH context. Results obtained from both training and field deployment indicate robustness and accuracy, as well as suggest improvements in security and operational efficiency for vehicular access control. Future work could consider the incorporation of additional computer vision and deep learning techniques to further extend the scope of this research.

Recent advances in machine learning research have highlighted transfer learning as an efficient strategy for model optimisation. This approach involves reusing neural networks pretrained on large-scale datasets and adapting them to specific tasks, thereby potentially reducing computational requirements and dependence on extensive task-specific data. As a result, transfer learning has become a widely adopted resource in contemporary research, particularly in scenarios characterised by limited data availability.

Within this framework, the MobileNetV2 architecture is often noted for its lightweight and computationally efficient design, originally conceived for environments with constrained processing resources, such as mobile devices and embedded systems. Its use of depthwise separable convolutions and inverted residual blocks with linear bottlenecks allows for a balance between accuracy and energy efficiency, making it suitable for real-time classification and detection tasks.

Similarly, ArcFace represents a notable development in facial recognition by introducing an additive angular margin loss function designed to enhance inter-class discrimination. This method seeks to cluster facial representations belonging to the same individual while enforcing angular separation between different classes, which may improve robustness under variations in pose, illumination, or facial expression.

In summary, transfer learning, MobileNetV2, and ArcFace can be regarded as important components in the evolution of artificial intelligence applied to image processing, each contributing to improvements in accuracy, efficiency, and scalability of contemporary models.

3 State of the art

Biometric access control to public spaces, supported by emerging technologies, constitutes a rapidly evolving research domain that seeks to balance security requirements with operational convenience. The following overview summarises the state of the art by highlighting contributions from three influential authors in this field.

An early and influential contribution is associated with Giaffreda [12], a recognised researcher in emerging technologies applied to security and intelligent management of public spaces. His work examines how biometric technologies can be integrated into security systems to support efficient and secure access control. In his article “Biometrics for secure access to public spaces:

opportunities and challenges", Giaffreda analyses innovative approaches such as facial recognition, fingerprint recognition, and other biometric modalities for access control. The study reviews multiple biometric techniques, including facial, iris, and fingerprint recognition, and evaluates their effectiveness in public environments. It also discusses their integration with existing security infrastructures to enhance protection and surveillance in contexts such as transportation hubs, government buildings, and large-scale public events [12].

In addition, Giaffreda emphasises the relevance of addressing privacy, ethical considerations, and system reliability when deploying biometric technologies in public spaces. Strategies aimed at compliance with data protection regulations and the safeguarding of individual rights are explored, while still seeking to leverage biometric systems to improve security and operational efficiency in urban settings. His work can be regarded as providing a comprehensive perspective on both the opportunities and the challenges associated with biometric access control.

A second key contributor is Ross, a well-established expert in biometric recognition whose research addresses facial recognition, iris recognition, and other biometric approaches. His studies focus on both the technical and ethical challenges of biometric access control, as well as the application of emerging technologies to strengthen security in public environments.

In the article "Multibiometric systems for access control", Ross examines the use of multimodal biometric systems, which combine multiple biometric traits to enhance accuracy and robustness. Unlike unimodal systems that rely on a single trait, multimodal approaches integrate information from several biometric sources to achieve more reliable identification. The analysis highlights advantages such as increased accuracy, reduced vulnerability to spoofing attacks, and lower error rates. Ross and his collaborators investigate how combinations of biometric traits, including facial and iris recognition, may enhance the reliability of access control systems in complex and demanding environments.

The study also addresses technical and implementation challenges related to multimodal systems, including the integration of heterogeneous biometric technologies, the management of large-scale biometric datasets, and interoperability with existing security infrastructures. Proposed strategies aim to mitigate these challenges and optimise system performance. Overall, Ross's work offers a substantial contribution to understanding the potential of multimodal biometrics for access control applications.

A third seminal contributor is Jain, whose research over several decades has significantly shaped the field of biometric recognition. His work addresses issues such as system accuracy, privacy protection, and the integration of multiple biometric modalities to enhance security in public spaces.

In "Biometric recognition: A review", Jain provides an extensive survey of techniques, algorithms, and applications across a wide range of biometric modalities, including facial, iris, fingerprint, and voice recognition. Each modality is assessed in terms of accuracy, robustness, scalability, and applicability across different use cases, from access control to identity management. The review highlights recent advances and emerging techniques aimed at improving system reliability, while also discussing practical challenges such as intra-class variability, interoperability, and large-scale data management.

The article further addresses security and privacy concerns associated with biometric data collection and use, offering a critical discussion of ethical risks and regulatory considerations. Strategies for mitigating these risks, including robust system design and data protection policies, are also examined.

More recent work [4] situates biometric security within the framework of Society 5.0, which promotes the integration of advanced technologies with human well-being. This contribution analyses how artificial intelligence, the Internet of Things, and advanced biometric systems drive digital transformation in institutional and urban contexts. It examines intelligent biometric systems designed to enable accurate, secure, and contactless identification, while also addressing ethical and technical challenges related to biometric data governance. The study underscores the relevance of inclusive policies and user-centred design in aligning biometric innovation with Society 5.0 principles.

Taken together, this body of literature provides a comprehensive and advanced overview of technologies, applications, and challenges in biometric access control, contextualised within digital transformation processes and the Society 5.0 paradigm. These studies constitute a valuable reference for researchers, practitioners, and policymakers seeking to leverage biometric technologies to enhance security, operational efficiency, and user experience across diverse sectors.

In conclusion, the contributions of these authors represent key reference points in contemporary research on biometric access control in public spaces. Their work not only advances technical understanding but also highlights ethical, regulatory, and

societal considerations associated with deploying biometric systems in real-world contexts. This theoretical foundation supports the development of research that integrates technical innovation with a human-centred and sustainable vision aligned with Society 5.0, positioning biometric security as a strategic component in the creation of secure, inclusive, and resilient environments [15].

4 Methodology

This inquiry focused on the applicability of facial recognition technology to address a challenge that arose at ITSCH, following a qualitative approach to define the fulfillment of the proposed system's operational functionalities and to determine the effectiveness of face recognition using a CNN with a low-resolution generic camera. In this way, the general system structure is as follows (see Figure 6).

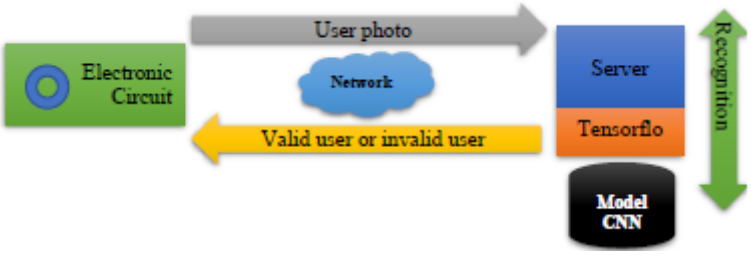

Fig. 6. Functional scheme.

1. An electronic circuit at the input captures an image and sends it through the network to a server via the HTTP protocol.
2. The server receives the image and processes it with the neural network model previously trained with photos and their corresponding identities, allowing it to determine who the person is.
3. The server sends a response, either confirming that the user student or staff member, in this case is valid, or indicating otherwise if the individual is not recognized.
4. The electronic circuit receives the response and, based on it, decides whether to grant access by activating the servo motor.

The requirements gathering was carried out through surveys administered to staff and students who use the institution's current entry and exit systems, as well as through direct and indirect observation of the access control process and document analysis. This provided a solid foundation for development. In this regard, it was determined that the prototype of the electronic circuit would use a Wi-Fi-enabled microcontroller, connected to the aforementioned sensors and actuators (see Figure 7).

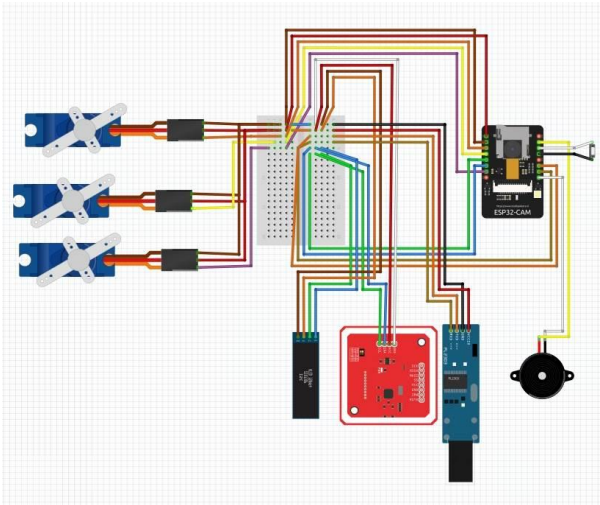

Fig. 7. Arduino Sensor Module.

Microcontroller: Although the microcontroller was programmed using Arduino software and language, no Arduino board was required, as the ESP32 was chosen instead. This microcontroller not only offers advanced features but also perfectly suits the purpose of the prototype, notably providing WiFi wireless communication necessary for server interaction. The selected board is the ESP32-Cam, which includes a connection for the OV2640 camera, as shown in Figure 8.

Fig. 8. Image Capture.

Sensors:

- PN532 NFC: This is an integrated circuit developed by NXP Semiconductors that enables NFC technology for wireless communication between compatible devices via radio frequency. It offers versatile operating modes for applications such as access control using RFID cards, allowing reading and writing to chips of cards that support this technology. In the prototype, it was integrated as an additional access measure.
- OV2640 Camera: This is a CMOS (Complementary Metal-Oxide-Semiconductor) image sensor manufactured by OmniVision Technologies. It is designed to capture still images and video in electronic applications, with a resolution of 2 megapixels. Integrated into the ESP32-Cam board, it was used in the prototype to capture images via the microcontroller.
- PIR Sensor: An infrared sensor that detects the presence of a person, used in this case to determine when to take a photo.
- Button: A simple push button that allows a signal to pass when pressed. It was used as an alternative for a security guard to grant access to visitors or external individuals who cannot be recognized by the system.

Actuators:

- Actuators are components that interact with the physical world outside the board, converting electrical signals into energy that acts directly on the environment. The actuators used are:
- MG90 Servomotors: Compact and low-cost actuators with an internal structure including an electric motor, a gearbox, and a control circuit that receives digital pulse signals to set its position. They can rotate within a specific range of degrees (usually 0–180) in response to control signals from a microcontroller or another device. Although three were included in the circuit, only the first was used to simulate the main access door, as the other two would require a dedicated camera for each.
- 0.91” OLED Display: An OLED (Organic Light Emitting Diode) display measuring 0.91 inches. OLED technology uses organic materials to emit light and create images, known for vibrant colors, deep blacks, and high contrast compared to other display technologies. The small display was used to show simple status messages from the microcontroller.
- Buzzer: A small speaker that vibrates when an electrical pulse (digital or square wave) is applied, emitting a constant sound at a specific frequency, used to provide auditory feedback to users.

The modeling phase allowed the creation of a preliminary system design, laying the foundation for the final design. Subsequently, a 3D prototype was fabricated (Figure 9), and testing began to train the algorithm, progressing toward the development phase and feedback for the final product.

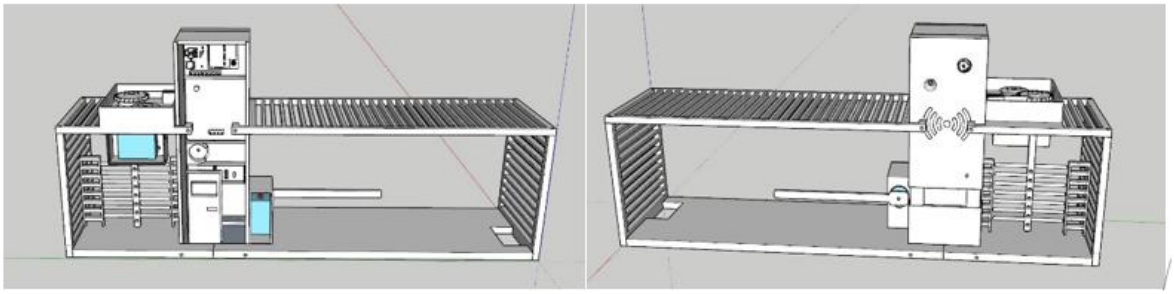

Fig. 9. Input layout.

This prototype allows determining when to take a photo and send it to the server, waiting for the response to decide whether to open the door or not, according to the following logic:

The main functions developed in this study were: the creation of a functional prototype for the institution's main entrance and a recognition system using neural networks. The entity-relationship model represents the relationship between entities and their respective attributes; it determines the data to be managed within the system. Each entity stores important information for the proper functioning of the system. Additionally, an algorithm was implemented that, using comparison techniques, allows the facial recognition of individuals, as shown in Figure 10.

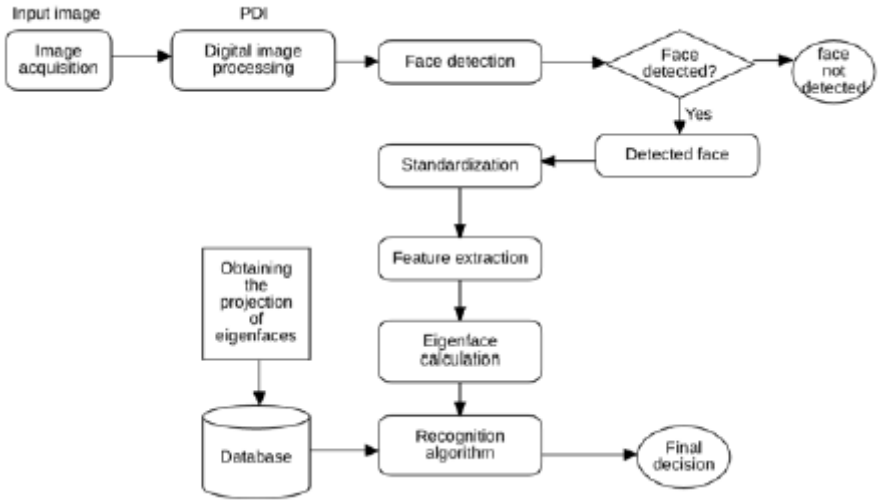

Fig. 10. Facial Recognition System Face Detection Algorithm.

For this recognition algorithm, a CNN was implemented using TensorFlow. Unfortunately, the TensorFlow Lite API for IoT devices was not deployed directly on the microcontroller due to insufficient storage and processing capabilities for this case, as it is intended to handle around 2,000 people, including both students and staff of the institution. Therefore, the main library was used via JavaScript and Python to implement the model on a server.

To train the CNN model, test photos of a group of students were used, all properly labeled with their student ID numbers at a resolution of 512x512 pixels. These images were then sent to the server, which performed the neural network training through a web interface, see Figure 11.

Fig. 11. Training Scheme.

Finally, a facial recognition system was obtained, designed to automate the entry and exit of students and staff at ITSCH. The resulting product features six main functions: registering facial characteristics, identifying and recognizing a student and/or staff member already registered in the system, detecting unregistered faces, recording entry and exit times, maintaining a data log for staff members (administrative or teaching), and generating reports (Figure 12).

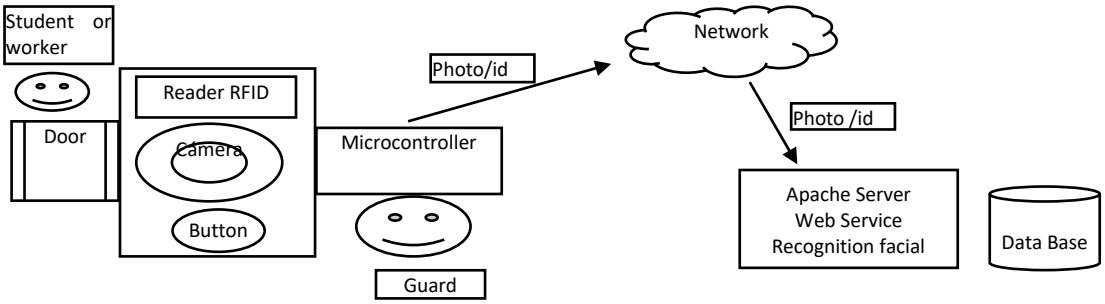

Fig. 12. Final Biometric Process.

The experimental results were satisfactory, and the proposed functionalities were executed correctly. Table 1 shows the resulting evaluation.

Table 1. Fulfillment of functionalities of the facial recognition system.

Functionalities	***Completed***
Facial feature registration	*x*
Face identification	*x*
Entry and exit logging	*x*
Detection of unregistered faces	*x*
Registration control	*x*

This evaluation was conducted with the aim of determining the feasibility of the biometric system and its implementation, as well as the additional services it would provide.

5 Results

The system will be capable of controlling the entry and exit of public and private parking lots. The work team carried out the following:

- Layout: The team created a 3D prototype, which was printed to fulfill the project's objective, and implemented the installation of sensors capable of controlling the processes carried out by the prototype. Tests were conducted, as shown in Figures 13 and 14.

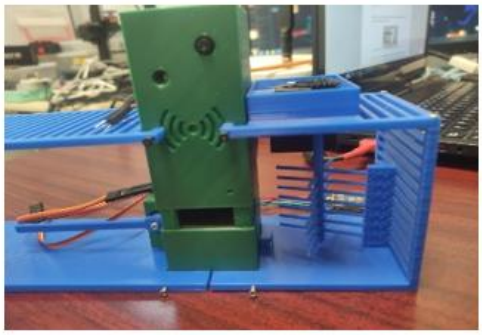

Fig. 13. Installing LED spotlights.

Fig. 14. Camera installation and connection.

Programming. The programming of the Arduino, the servomotors, and the code for the biometric system was developed. For the latter, the training of the Convolutional Neural Network model was carried out for testing under the following parameters:

- A Sequential model was used.
- Photos of 99 students were analyzed at a resolution of 512 × 512 pixels, see Figure 15.
- In this case, each student corresponds to a class, related to their control number.
- Three convolutional layers (with 32, 64, and 128 filters, using 'relu' activation).
- One output layer with 'softmax' activation.
- The optimizer used was 'Adam' and the loss function was 'Sparse Categorical Crossentropy'

Fig. 15. Training result: accuracy and loss – 1.

Training was carried out over 1000 epochs, where it can be observed that the highest accuracy was achieved from epoch 750 with 90% (blue line), while the validation accuracy was lower, approximately 50% (orange line), as shown in the graph in Figure 16.

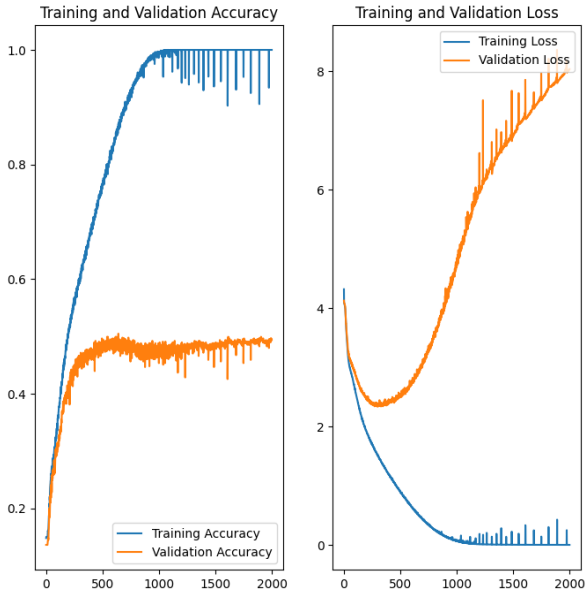

Fig. 16. Training result: accuracy and loss.

Finally, the neural network was able to return the recognized control number based on the validated face or photo, with an average accuracy of 50%.

6 Discussion

The intelligent automation of access in environments such as parking areas and facility entrances is increasingly viewed as a strategic field with potential for high impact in the coming decades. Such developments respond not only to the growing demand for advanced biometric security solutions but also align with principles of digital transformation and the broader vision of Society 5.0, in which technology is intended to integrate harmoniously into everyday life in order to optimise resources, promote energy efficiency, and enhance user comfort.

In this context, the results obtained in the present project suggest that its implementation could address several operational and access control challenges currently experienced by the community of the Instituto Tecnológico Superior de Ciudad Hidalgo (ITSCH), with potential benefits for both institutional management and user experience.

Relevant precedents illustrate the evolution and diversification of biometric access control technologies. For example, [12] developed a facial recognition system for attendance registration within the Cooperativa de Taxis y Camionetas Puyo. Their solution employed the Viola–Jones algorithm, the TensorFlow library in Python, and SQL Server as the database manager, achieving reliable attendance traceability. Similarly, Ghosh and Rai (2020) proposed a facial recognition system based on Local Binary Patterns Histogram (LBPH) integrated with drone platforms, reporting an identification accuracy of approximately 89.1%. This approach represents an innovative extension of biometric systems into dynamic and mobile environments.

In another related contribution, Ross et al. (2018) developed a system focused on intruder detection and identification using a prototyping methodology, a comparative algorithmic approach, PhpMyAdmin (XAMPP), Python, and the OpenCV library. Their work demonstrated the technical feasibility and adaptability of facial recognition technologies within physical security scenarios.

In the present project, the selection of Python as the programming language can be justified by its versatility and compatibility with artificial intelligence libraries such as TensorFlow, which facilitate the training and deployment of computer vision models. Data management is supported through MySQL, enabling structured storage of biometric information and supporting scalability. The graphical user interface was developed using Tkinter, a cross-platform toolkit integrated into Python that meets basic interface design requirements while maintaining computational efficiency.

Overall, this proposal can be situated within the Society 5.0 framework, in which biometric security is conceived not solely as a response to threats but also as a component of intelligent, resilient, and human-centred environments. The convergence of artificial intelligence, big data, the Internet of Things (IoT), and biometric systems has the potential to reshape security practices and redefine interactions and trust in both public and private contexts.

Consequently, the feasibility of implementing this system—subject to approval by the relevant institutional authorities—may contribute to strengthening security at ITSCH while also supporting its positioning as an innovative institution aligned with global digital transformation trends and the human-centric principles of Society 5.0.

7 Conclusions

The proposed technological implementation is based on an advanced biometric access control system centred on facial recognition, developed using a model integrated within the TensorFlow library. The system was trained to support automated control of student and staff entries and exits at the Instituto Tecnológico de Ciudad Hidalgo (ITSCH).

Although experimental results indicated satisfactory performance in relation to the planned functionalities, it is important to note that testing was conducted under controlled conditions, which limits direct extrapolation to real-world environments. Identified constraints include sensitivity to lighting conditions and dependence on the optical quality of the cameras employed. These factors influence recognition accuracy, which tends to improve under uniform illumination and reduced image noise. The use of higher-resolution, low-latency capture devices may therefore enhance system reliability in more variable settings.

The design and deployment of the system represent a step forward in biometric security innovation, integrating mechanisms that support efficient access logging and strengthened control in institutional contexts. Its relevance lies in its alignment with digital transformation principles and with the objectives of Society 5.0, which emphasise the use of technology to address social needs through secure, hygienic, and efficient solutions.

Future work includes plans to improve model accuracy and robustness through expansion of the training dataset, which could enhance generalisation and reduce errors in unforeseen scenarios. The incorporation of transfer learning techniques is also anticipated, leveraging architectures pretrained on large datasets to reduce development time and improve predictive performance under real-world conditions.

The potential applicability of this solution extends beyond academic environments. Institutions and organisations requiring real-time access control with high standards of security, speed, and hygiene may benefit from similar implementations. For ITSCH, adoption of such technologies could support its positioning as a higher education institution committed to institutional modernisation and automation of administrative processes.

Additionally, future integration of an automated vehicle recognition module is envisaged, replacing traditional access mechanisms such as magnetic cards or QR codes with computer vision–based licence plate recognition systems. Such systems could allow rapid identification and automated barrier control without manual intervention, potentially increasing security and operational efficiency while improving user experience.

In summary, the proposed system can be viewed as a practical example of how technological innovation, digital transformation, and the strategic vision of Society 5.0 converge to support the development of safer, smarter, and more human-centred environments.

References

1. Li, J., Shun, C., Duan, J., Gao, P., & Hou, Y. (2015). A Novel Remote Monitoring and Control System Based on GSM for Home Security. International Journal of Online and Biomedical Engineering (Ijoe), 11(4), 34. https://doi.org/10.3991/ijoe.v11i4.4647
2. Alexandre, Luis, (2010). Tecnología NFC, Ecuador, Monografía.
3. Analog Devices. (2014). MP36 data sheet. https://www.analog.com
4. Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. Learning, Media and Technology, 45(2), 115–128. https://doi.org/10.1080/17439884.2020.1686014
5. Banzi, M. (2009). Getting started with Arduino (1st ed.). Make Books.
6. Cabinet Office of Japan. (2016). Society 5.0: A people-centric super-smart society. Gobierno del Japón. https://www8.cao.go.jp/cstp/english/society5_0/index.html

7. Villamar, F. and Rivera, K. (2024). Gestión organizacional y calidad del servicio al cliente en cooperativas de taxis. Revista Científica Arbitrada Multidisciplinaria Pentaciencias, 6(4), 38-45. https://doi.org/10.59169/pentaciencias.v6i4.1175
8. Suárez, J. C. and Paredes, S. S. (2022). El factor humano y su rol en la transición a Industria 5.0: una revisión sistemática y perspectivas futuras . Entreciencias: Diálogos en La Sociedad Del Conocimiento, 10(24). https://doi.org/10.22201/enesl.20078064e.2022.24.81727
9. Mahat, D. (2024). Society 5.0: A Bibliometric Analysis from Management Approach. NPRC J. Multidis. Res., 1(2), 1-19. https://doi.org/10.3126/nprcjmr.v1i2.69237
10. Garduño Santana, M. A., Díaz-Sánchez, L. E., Tabarez Paz, I., & Romero Huertas, M. (2017). Estado del arte en reconocimiento facial. Research in Computing Science, 140(1), 19–27.
11. Rumpak, T., Faturrahman, M., Ramadhan, K., & Agam, Y. (2022). Citizenship Education in Defending Nationalism in the Digital 4.0 Era to Face the Society 5.0 Era. Jurnal Sosial Dan Sains, 2(2), 210-215. https://doi.org/10.36418/sosains.v2i2.345
12. Haddada, L. and Amara, N. (2019). Double watermarking-based biometric access control for radio frequency identification card. International Journal of Rf and Microwave Computer-Aided Engineering, 29(11). https://doi.org/10.1002/mmce.21905
13. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … & Bengio, Y. (2020). Generative adversarial networks. communications of the Acm, 63(11), 139-144. https://doi.org/10.1145/3422622
14. Granado, Emanuel, (2011). Sistemas con Radiofrecuencia, Venezuela.
15. Saunila, M., Nasiri, M., Ukko, J., & Gastaldi, L. (2025). Managing Social Sustainability With IoT Implementation: An Industry 5.0 Perspective. Sustainable Development, 33(4), 5327-5335. https://doi.org/10.1002/sd.3398
16. Benavente, O. and Piccio-Marchetti, R. (2005). Authentication services and biometrics: network security issues., 333-336. https://doi.org/10.1109/ccst.2005.1594871
17. Dantcheva, A., Elia, P., & Ross, A. (2016). What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. ieee transactions on Information Forensics and Security, 11(3), 441-467. https://doi.org/10.1109/tifs.2015.2480381
18. Microchip Technology, (2014). "DSPIC30FXX Data Sheet High-Performance, 16-bit Microcontrollers". Chandler, Arizona: http://www.microchip.com
19. Mikroelektronika, (2014). "GSM Click Manual": www.mikroe.com
20. Torres-Toukoumidis, Á., Picoita, F., & Mendoza, E. (2024). Capítulo 2. Inteligencia Artificial y educomunicación. Espejo de Monografías de Comunicación Social, (23), 37-57. https://doi.org/10.52495/c2.emcs.23.ti12
21. Monroy, F. (2018). Estacionamientos automatizados. Disponible en: https://multiplojp.wordpress.com/2018/07/26/estacionamientos-automatizados/
22. Dheyaa, S. and Sadik, M. (2016). Biometrics System based Human Identification using STR DNA Marker. International Journal of Computer Applications, 138(7), 31-37. https://doi.org/10.5120/ijca2016908931
23. Noble, J. (2009). Programming Interactivity: A Designer's Guide to Proceserjrsing, Arduino, and openFramework (1ª edición). O'Reilly Media. p. 768. ISBN 0596154143.
24. Panasonic, (2014). DN6851 Data Sheet. http://www.semicon.panasonic.co.jp/
25. Portilla Jimenez, J. J. (2018). Análisis y Diseño de un Sistema de Reconocimiento Facial aplicando Machine Learning para detectar e identificar intrusos. En Universidad de Guayaquil.
26. Ross, A., et al. (2018). Multibiometric systems for access control. IEEE Signal Processing Magazine, 35(1)
27. Ruiz, José Manuel, (2007). Manual de Programación Arduino, México.
28. Sánchez, M., & Morales, J. (2022). Transformación digital y tecnologías emergentes en instituciones educativas. Revista Iberoamericana de Tecnología Educativa, 17(1), 45–60.
29. Uber facial recognition. (2016). https://www.techinasia.com/uber-china-facial-recognition
30. Vázquez, L. (2023). La evolución de los sistemas biométricos en entornos inteligentes: un enfoque desde la seguridad digital. Revista de Innovación y Tecnología Aplicada, 12(4), 102–119.
31. Wadham, Rachel, (2003). Radio Frequency Identification. Library Mosaics.
32. Wang, L. and Siddique, A. A. (2020). Facial recognition system using LBPH face recognizer for anti-theft and surveillance application based on drone technology. Measurement and Control, 53(7-8), 1070-1077. https://doi.org/10.1177/0020294020932344
33. Zumba Gamboa, J. P., & León Arreaga, C. A. (2018). Evolución de las Metodologías y Modelos utilizados en el Desarrollo de Software. INNOVA Research Journal, 3(10).