International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Access System Using Facial Recognition and NFC

José Ignacio Vega Luna[1], Gerardo Salgado Guzmán[1], José Francisco Cosme Aceves[1], Francisco Javier Sánchez Rangel[1], Víctor Noé Tapia Vargas[1], Mario Alberto Lagos Acosta[1]
[1]Departmento de Electrónica-Área de Sistemas Digitales, Universidad Autónoma Metropolitana-Azcapotzalco, Ciudad de México, México

***Abstract*—*The security of people, assets and facilities of companies, institutions, homes and offices has become a critical aspect. Currently, different access control systems and devices are used that incorporate biometric technologies. One of them is facial recognition. This paper presents the development of a laboratory access control system using two security mechanisms: face recognition and an NFC card. The system is based on a vision module with Artificial Intelligence and an NFC reader controlled by an Arduino UNO. If the face of the user trying to access is recognized, the system validates the identifier of the assigned card. If both validations are successful, the electric door lock is activated. The tests conducted showed that the face recognition time is 155.875 ms on average, achieving an accuracy of 87.5%.*

Keywords*—*Access control, Arduino, face recognition, NFC, vison module.

I. Introduction

Currently, most installations in industries, buildings, institutions, hospitals and shops, to name a few, have security systems that allow safe access to authorized persons, protection of assets and physical infrastructure and privacy. Recent advances in technology allow for more reliable and effective systems of this type, incorporating different biometric and wireless communication techniques. These techniques have the advantage of uniquely identifying a person by their biometrics. Among the most used biometric identification methods are retina and fingerprint readers, voice recognition systems and facial recognition systems [1]. Facial recognition is a technology based on information extracted from the characteristics of a person's face. It is the most used technology because it is considered the safest, it is low cost and because it does not require physical contact between people and devices [2]. This last aspect is especially important to avoid the risk of contagion in this time of the COVID-19 pandemic.

Facial recognition is also widely used in the automation of home and office processes or in access to computer resources. In general, this technology is based on the capture of an image, where one or more people are, to detect the person's face and try to recognize it by comparing it with a database of known faces [3]. The hardware used in this technology is easy to install since it only requires a video camera. In some security and access systems based on facial recognition, one or more mechanisms are additionally used that allow for a more robust system. Some of these mechanisms include barcode or QR code readers, keyboards to supply passwords, and Near Field Communication (NFC) cards or tags [4]. The latter is one of the most popular mechanisms to control the activation of electric locks, parking pens and turnstiles, among other access devices, since it is a short-range wireless communication technology, based on standards that allows bidirectional information transfer, similar to facial recognition, does not require physical contact between the user and the reader.

The objective of this work was to develop a system for opening an electric lock using two security mechanisms: facial recognition and NFC cards. The system was implemented in an Arduino UNO module, with an NFC card reader and a vision module with Artificial Intelligence (AI). The system was installed in the access door of a laboratory to store in an SD memory card, both the images of the faces of the people registered and authorized to activate the lock, as well as the Non-Unique Identifier (NUID) serial number of the NFC card associated with each user. The lock is activated when the image of the face of the person trying to access the laboratory is recognized and the NFC card code is the one that corresponds to the person. The SD card also stores the image of the faces of the people who tried to access the laboratory unsuccessfully.

When it comes to the algorithms and models used for facial recognition, there are a variety of them. They all perform detection and recognition tasks, differing mainly in the effectiveness and quality of the result as well as in the processing time. Facial recognition algorithms analyze and determine the characteristics of the face from an image or video source, to compare them with the characteristics of images stored in a database of known faces, also called training or learned images. One of the challenges of these algorithms is to conduct the recognition in the shortest time possible in real time [5].

Once the image or video is captured, these algorithms generally perform the following tasks [6]:

1-Detection of the face or faces to obtain the location and scale of the face and the pose.

2-Alignment of the face to determine the components of the face based on geometric transformations located in the nose, the distance between the pupils, the lips, the mouth and the chin. Normally small size grayscale images are obtained that can be easily processed. At this stage, a conditioning and normalization process is conducted to align the face.

3-Feature extraction to generate a unique digital identifier or feature vector for each face, based on the geometric variations resulting from the previous step.

4-Recognition to determine the similarity value by comparing the vector of the unknown face with the vectors of the faces in the database to obtain the result or recognition of the person.

Traditional methods or techniques to implement facial recognition algorithms are classified into two types: geometric and holistic [7]. The geometric methods are based on the

José Ignacio Vega Luna, Gerardo Salgado Guzmán, José Francisco Cosme Aceves, Francisco Javier Sánchez Rangel, Víctor Noé Tapia Vargas and Mario Alberto Lagos Acosta, "Access system using facial recognition and NFC," In*ternational Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 193-198, 2023.

comparison of the geometric characteristics of the faces to obtain the characteristic vectors of the person's front or profile. They have low accuracy percentages and are vulnerable to false positives and negatives. The holistic ones are used more than the geometric ones, they perform the correlation of the characteristics of the unknown face with the characteristics of the faces of the database. They use facial spaces with a lower number of coefficients, discriminating faces that are not similar to the unknown image. Among the most used methods of this type are: Principal Component Analysis (PCA), which uses eigenfaces or eigenvectors, Fisher's Linear Discriminant (FLD) or Linear Discriminant Analysis. (LDA), the latter uses a reduction based on the FLD method [8].

During the last years, methods and models that perform facial recognition in a three-dimensional way and using AI have been proposed and used [9]. The three-dimensional models are used images captured with 3D sensors to train the algorithm [10]. They try to reduce the drawbacks of images captured with lighting problems, person poses, gestures and variations introduced by electronic image capture and processing devices [11]. Those of the second type are based on AI, specifically on computer vision, to make models that make use of deep learning, or deep learning, and achieve facial recognition applications. These models essentially perform the four tasks listed above more effectively. In the first stage, the detection and normalization of faces, they generally use Multitask Cascaded Convolutional Neural Networks (MTCNN). The detector is composed of three neural networks that sequentially debug face detection. In the second stage, the numerical representation of the characteristics of the faces is obtained through vectors called embedding or encoding. The training of the neural networks used in this stage is complex, however, there are different trained models available through APIs and open-source function libraries. In the last stage, the recognition is conducted by determining the similarity between the numerical representation of the unknown face with respect to the representations of known faces stored in the database, generally using the Euclidean distance or the cosine distance [12]. One of the most used programming languages to implement these models is Python and one of the most used libraries is OpenCV whose use allows the development of applications of this type in a faster, simpler and more reliable way.

Open-Source Computer Vision (OpenCV) is a library of computer vision and machine learning functions, free and open source under the BSD license. It is cross-platform, written in C++, and integrates interfaces to programming languages such as Python, C, C++, and Java. OpenCV is composed of thousands of algorithms that allow capturing and processing images from video files or photographs captured with webcams [13]. These algorithms can be used in motion detection applications, face and object recognition, movement tracking, pattern recognition and 3D reconstruction, among other functionalities [14]. All this allows the programmer to focus on the development of the application using the complex algorithms that execute the OpenCV functions [15], [16]. Real-time image processing can be performed using some Arduino and OpenCV modules with certain limitations, since this type of task requires a significant amount of memory. The Arduino modules integrate from 2 to 32 KB of RAM memory and the microcontrollers that they incorporate are not fast and powerful for these tasks. However, Arduinos are cheap, compact and can use external vision modules for image processing such as the AI vision sensor used in this work.

On the other hand, NFC wireless communication is a short-range, high-frequency technology used to exchange information between devices. The communication is conducted using the induction of a magnetic field, where two spiral antennas located in close fields participate [17]. It is made up of a reader, with one or more antennas, and a label. The two devices located a short distance away transmit in the 13.56 MHz band, which has no restrictions and does not require a license to use. The reader receives the electromagnetic signal emitted from the tag. Commonly, the labels are cards that contain an integrated circuit or chip or mobile devices that emit the radio frequency signal. Tags can be active or passive, resulting in NFC using one of two communication protocols: active or passive. In active mode, the devices have an electrical power supply to generate their own electromagnetic field used to send information, implementing peer-to-peer communication to achieve ranges of tens of meters. In the passive mode, the reader or initiator induces the electromagnetic field in the antenna of the second device, or destination, generating the electrical energy used for data exchange [18]. This last device is the label and under this scheme ranges of no more than 15 centimeters are achieved [19].

The protocols and formats of the information transmitted by NFC are based on the ISO 14443 standard established by the NFC Forum. NFC can transmit at speeds of 106, 212, 424 and 848 Kbps, which are small speeds compared to those used by other technologies such as Wi-Fi and Bluetooth [20]. However, NFC was not designed to transmit large amounts of information or files, but rather for purposes of identifying people or synchronizing electronic devices in a simple and fast way, being an alternative to QR codes [21]. It can be summarized by saying that NFC technology allows identifying and contacting devices through the sending and reading of radio signals based on tags in which the devices function as transmitters and receivers of the signals, providing a certain degree of security at a short distance. Currently, NFC is used in a wide variety of applications and different areas of society and industry in which a contactless communication mechanism is required, useful today in the COVID-19 pandemic. Some applications are payments and electronic markets through bank cards, or smart cards, in mobile devices, in storage of personal information, such as passports, in access control systems, in the automation of industrial, domestic and health care processes. health, or to provide information on sites, historical places and museums, among others [22]. NFC tags are also placed on clothing, consumer items, and face masks [23].

Reviewing the state of the art in terms of facial recognition, the results of research carried out in recent years indicate that efforts have been directed at proposing new methods or improving existing ones, with the aim of minimizing or eliminate the problems presented in the variations of face images due to the pose, gesticulation, expressions, occlusion,

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

scene, quality and blurring of the image [24], [25]. This is called Heterogeneous Facial Recognition (HFR) and consists of matching the information of faces captured from different domains such as Visible Light (VIS) and Near Infrared (NIR) [26]. The importance of this task lies in the fact that the images captured with infrared cameras contain more useful information than those captured with visible light deficiencies, which is recently being applied in video surveillance systems and in biometric security systems where there is little lighting [27]. It is about synthesizing VIS images from NIR images. This type of work is being done in an analogous way dealing with faces contained in video files [28] and using other techniques such as Generative Adversarial Neural Networks (GAN), which are machine learning platforms [29], [30].

Other research trying to solve posing problems has explored the use of 3D panoramic models to align the face [31] and dealing with problems caused by geometric distortion [32], [33], as well as the use of classifiers based on overlapping Sparse Parameters (SSP) [34] or based on Local Directional Ternary Patterns (LDTP) [35]. In fact, recent work addresses the problem of having few training images by proposing models of Facial Pose Pre-Recognition (FPPR) and Dual Dictionary Sparse Representation Classification (DDSRC) [36].

The contributions of the work presented here are the following: 1-It is a device that uses a state-of-the-art vision sensor, which makes it more compact in size and with a faster and more reliable response than similar commercial products available today, the latter are based on a much more extensive and complex programming to carry out the tasks performed by the sensor, 2-The cost is a third of the facial recognition products currently in existence, 3-Incorporates two security mechanisms, most current devices only have one and 4-The functionalities provided by the vision sensor make both the use and maintenance of the system easy, since with just one button users can be registered by training the neural network convolutional sensor.

II. Methods

The methodology used to develop this work consisted of dividing it into two functional components: the system hardware and the Arduino UNO programming.

A. System Hardware

The system architecture is composed of the Arduino UNO module, the AI vision module, the NFC reader, and the electrical interface, as shown in the block diagram in Fig. 1. The AI HuskyLens machine vision sensor module was used. This device has seven modes of operation, or functionalities: face, object, color and label recognition, object and line tracking, and object classification. In the first mode, it detects one or several faces, assigns an identifier to each of them, recognizes them and can follow their movements. It is a compact size module that integrates I2C and UART communication interfaces. In this work, the HuskyLens module was connected to Arduino UNO UART interface as indicated in the connection diagram in Fig. 2. The AI HuskyLens machine vision sensor.

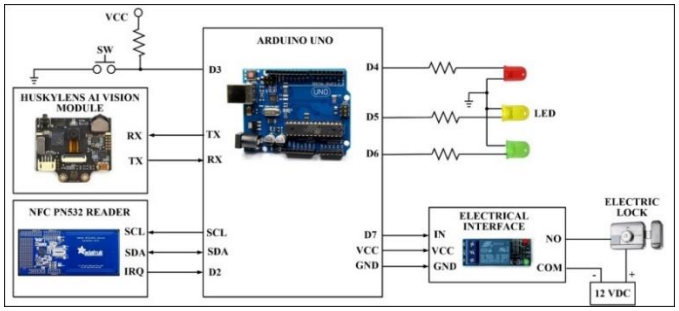

Fig. 1. System architecture.

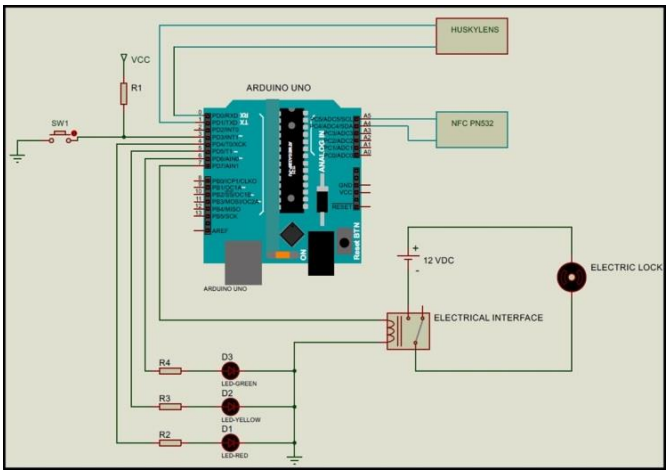

Fig. 2. System connection diagram.

The sensor incorporates the following hardware resources: a Kendryte K210 dual-core 64-bit RISC-V processor, a SEN0305 image sensor composed of an OV2640 2 Megapixel camera, a 2-inch screen with a resolution of 320 x 240 and an SD memory slot. In this work, the HuskyLens module was connected to the Arduino UNO UART interface through the TX and RX terminals using a speed of 9,600 bps. This module has two buttons that allow you to manually perform the following tasks: 1) Capture an image to detect and learn a face, or a group of faces or 2) Select one of the seven functions and set the operating parameters such as brightness of the screen, communication protocol, UART or I2C, serial speed, language and color of the frame drawn on the screen when learning and detecting a face, among others. It is possible to automatically conduct the above tasks from the Arduino UNO using the *HUSKYLENS.h* function library. The HuskyLens module is more than a vision sensor with machine learning technology, because when the new generation processor specialized for AI K210 executes the convolutional neural network algorithm it is 1,000 times faster than the SMT32H743 ARM Cortex-M7 controller, allowing you to capture video of fast-moving objects and continuously learn faces and objects from different angles. The more images you learn or use in training, the more accuracy you achieve. All these features and functionalities were the reasons why the HuskyLens module was used to detect, learn and recognize faces in a simple, agile and fast way, which

José Ignacio Vega Luna, Gerardo Salgado Guzmán, José Francisco Cosme Aceves, Francisco Javier Sánchez Rangel, Víctor Noé Tapia Vargas and Mario Alberto Lagos Acosta, “Access system using facial recognition and NFC,” In*ternational Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 193-198, 2023.

allowed the efficient development of the application presented here.

To implement the NFC reader, the PN532 NFC/RFID v.16 module was used. This device integrates the PN532 circuit, which is one of the most used NFC readers in mobile devices that can read and write NFC tags of types 1 to 4. To communicate with a controller, the PN532 NFC/RFID module has with I2C, UART or SPI interfaces. It incorporates a 13.56 MHz antenna and a 4050-voltage level converter. In this work, the PN532 NFC/RFID module was connected to the Arduino UNO I2C interface to conduct communication through the SCL and SDA terminals. The I2C address 0x48 that the PN532 NFC/RFID has established by default has not been modified. The IRQ output of the PN532 NFC/RFID was connected to Arduino UNO digital input so that the module requests the interruption to the Arduino when it detects the presence of an NFC card in the range of view of the antenna. In the programming conducted on the Arduino UNO for communication with the module, the free access function libraries *Wire.h* were used to access the I2C interface and the Adafruit_PN532.h library. The latter allows the reading of NFC cards of the Mifare type, based on the ISO14443A standard, as well as authenticating the reading and writing of information in their EEPROM. The PN532 NFC/RFID can perform NFC communication in passive or active modes. In the implementation of this application, this module is the initiator and the NFC card the destination, or target, in passive mode.

There are a variety of NFC card vendors that support the ISO14443A standard, including Mifare-type cards from NXP Semiconductor. Within the most used Mifare cards, due to their low cost, are the classic and the ultralight, the classic card contains an EEPROM memory of 1 KB and 4 KB bytes, while the ultralight card contains an EEPROM of 512 bytes and a memory 32-bit OTP. The content of the EEPROM can be read and modified by the initiator in passive mode. The EEPROM organization is divided into sectors and blocks. Sectors have access rights, configurable authentication keys, and are made up of a number of blocks. In 1 KB NFC cards there are 16 sectors, each of 4 blocks and 4 KB cards contain 32 sectors of 4 blocks or 8 sectors of 16 blocks each. Each block contains 16 bytes. Before accessing a block in a sector, the initiator must authenticate with the appropriate key. Communication between the initiator, in this system, the PN532 NFC/RFID, uses the NFC Data Exchange Format (NDEF). The NDEF is made up of messages and records. This format allows information such as plain text or unified resource identifiers (URIs) to be stored on NFC cards. The NDEF includes several record type definitions (RTDs) that specify how this information is stored in memory.

To authenticate the user in this work, through the NFC card, 1 KB ISO classic Mifare cards were used using the NUID assigned to the card. For this purpose, the NUIDs of the cards assigned to users authorized to enter the Laboratory were stored on the SD card of the HuskyLens module.

The electrical interface is constituted by a single channel relay, normally open, input voltage 5 VDC, control voltage 3.3 to 9 VDC and output voltage 250 VAC or 30 VDC/10 A. The terminal digital output D7 of the Arduino UNO controls the relay.

B. Arduino UNO programing

The developed system is executing one of two tasks: recognition or learning of a face. To perform the above tasks, the programming of the Arduino UNO was based on the flow chart shown in Fig. 3.

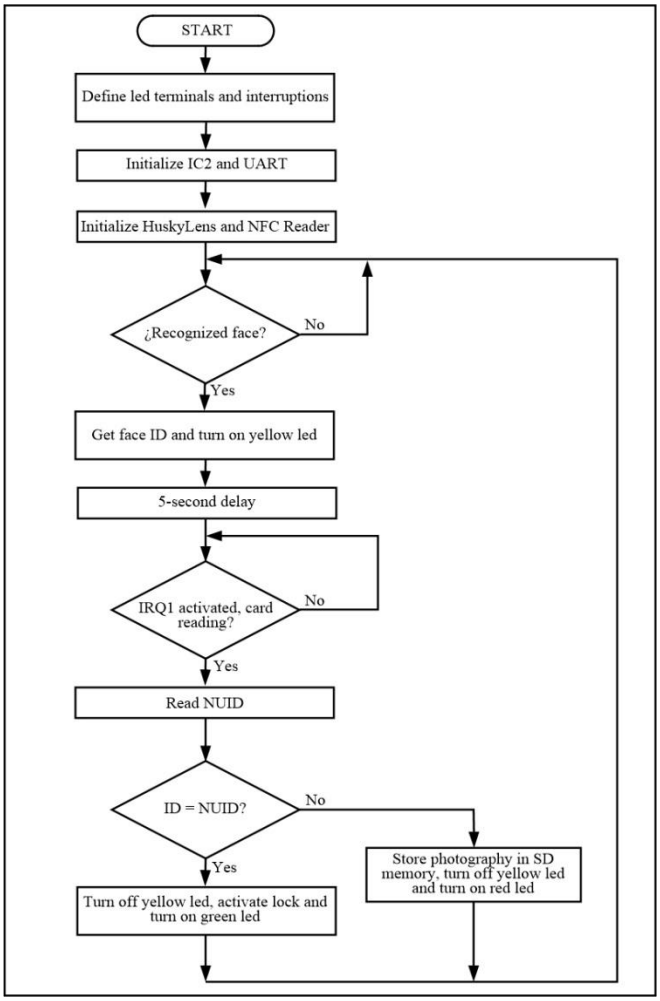

Fig. 3. Main program flowchart.

The main program is responsible for implementing the detection and recognition of the user's face. When starting the program, the terminals used for the indicator LEDs, the interrupts are defined and the I2C and UART interfaces are initialized using the function libraries *Wire.h* and *SoftwareSerial.h*, respectively. Subsequently, the HuskyLens module and NFC reader are initialized and configured through the *huskylens.begin* and *nfc.startPassiveTargetIDDetection* functions, respectively. It then enters a cycle where it continually scans, via the *huskylens.available* function, the HuskyLens module, querying whether a previously learned face has been detected and recognized. If so, it obtains the face identifier or ID through the *huskylens.read* function, then turns on the yellow led and invokes a 5-second delay routine to give the user the opportunity to place the NFC card in the reader. When the user places the card, the reader generates the IRQ1 interrupt through the D2 pin of the Arduino. The service routine

José Ignacio Vega Luna, Gerardo Salgado Guzmán, José Francisco Cosme Aceves, Francisco Javier Sánchez Rangel, Víctor Noé Tapia Vargas and Mario Alberto Lagos Acosta, “Access system using facial recognition and NFC,” In*ternational Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 193-198, 2023.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

of this interruption is in charge of reading the NUID of the card, calling the function *nfc.readDetectedPassiveTargetID* and comparing it with the ID of the recognized face. If the ID and the NUID are the same, the yellow LED turns off, the electric lock is activated and the green LED lights up momentarily. If the NUID does not match the ID associated with the face, it stores the photograph captured by the camera in the SD memory, using the *huskylens.savePictureToSDCard* function, turning off the yellow LED and turning on the red LED momentarily. Finally, the program returns to the beginning of the loop.

The learning task is used by the system administrator and allows training the neural network for face recognition, registering in the SD memory the faces of users authorized to enter. When the administrator needs to tell the system to learn a face, he must press the push-button connected to the Arduino UNO D3 terminal to activate the IRQ2 interrupt. The interrupt handling routine performs the following actions: It asks the HuskyLens to learn a face and set the user ID using the *huskylens.writeLearn* and *huskylens.setCustomName* functions. The ID is the NUID value of the NFC card assigned to the user. Next, it stores the photograph captured by the camera in the SD memory, turns on the green led momentarily and finishes. The SD card was initialized with FAT32 format before use.

III. Results and Discussion

From the point of view of security, the developed system presents, at first sight, the vulnerability that the use of NFC cards represents, since they can be falsified or lost by users. However, this is the second security mechanism of the system, that is, the events indicated above could occur, but it is very difficult to evade the user's authentication through the face. Another aspect to consider is that there was the option of making the system using a module with a more powerful processor than the one contained in the Arduino UNO or a Field Programmable Gate Array (FPGA) to implement facial detection and recognition with OpenCV and C++. This would increase the time and complexity of the system development and the cost is similar to the developed system, since the price of the Arduino UNO plus the HuskyLens module and the NFC reader is almost equal to that of an embedded module with more resources than the Arduino, of in such a way that the cost-benefit ratio was analyzed when deciding the components used in the system. In the system installation, only the video camera of the HuskyLens module and the NFC reader were located on the outside of the Laboratory door, in such a way that only the administrator has access to the configuration and operation buttons of the HuskyLens.

Four sets of tests were performed. The first group aimed to determine the distance at which the user's face should be located with respect to the camera, as well as the orientation angle to achieve recognition. To conduct the tests, a set of 200 users was used and the results showed that the distance should be from 30 to 50 cm and an angle from -20 to +20 degrees. Considering the above, it is recommended that the administrator capture, in the learning process, images of the face of each user from different angles and positions. Using the same number of users, the second group of tests aimed to determine the distance at which the NFC card should be placed from the reader. The results indicated that the distance should be no greater than 14.5 centimeters.

The third group of tests was intended to determine the accuracy of the system. 500 people participated in these tests, of which the HuskyLens learned, or was trained, with the face of 400 of them. Each person tried to access the Laboratory 4 times on average. The results obtained showed that the accuracy of the system is 87.5%. The last set of tests was aimed at determining the response time of face recognition. These tests were divided into eight phases. In the first phase, the system was trained with 50 faces and in each phase 50 images were added until 400 trained faces were achieved. In each phase, the face recognition of 40 users was conducted. The results revealed that the average system recognition time is 115.875 ms, increasing slightly as the number of images used in training stored in the HuskyLens SD memory grows, as shown in the graph in Fig. 4. The SD memory used was 32 GB, enough for system operation, estimating that 400 users is too many for almost any application.

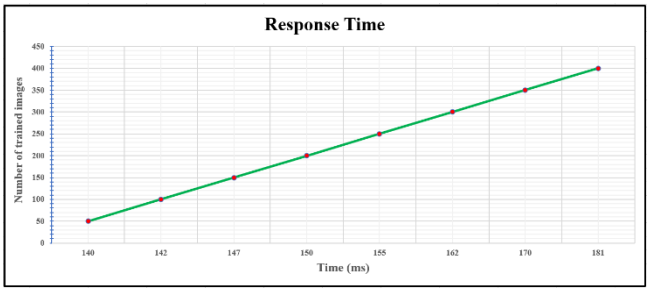

Fig. 4. Recognition response time.

IV. Future Work

Two functionalities are planned to be added to the system software: the first is to incorporate a routine that allows the administrator to remotely request the HuskyLens module to learn a face or delete one, without having to scroll to use the push-button currently used to such end. The second is to add a Wi-Fi interface to the hardware, or replace the Arduino UNO with the Arduino UNO Wi-Fi, so that the administrator can access it from the Internet and have an IoT solution.

V. Conclusion

An access system using facial recognition and an NFC card was developed. Facial recognition was performed using a HuskyLens vision module with AI. The system activates the electric lock of a Laboratory door if it recognizes the user's face, whose trained image is stored in the HuskyLens SD memory and if the serial number of the NFC card is the one assigned to the recognized and trained face. The system records the photographs of users who try to access the Laboratory. The response time of the achieved is 115.875 ms, on average, and the accuracy is 87.5%, which is acceptable for the application conducted, considering that the Laboratory does not have a large number of users and those that do, do not carry it out continuously.

José Ignacio Vega Luna, Gerardo Salgado Guzmán, José Francisco Cosme Aceves, Francisco Javier Sánchez Rangel, Víctor Noé Tapia Vargas and Mario Alberto Lagos Acosta, “Access system using facial recognition and NFC,” In*ternational Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 193-198, 2023.

It is considered that a good cost-benefit ratio was achieved since the components used allowed to build a reliable system, easy to implement and operate. The options presented for implementation are of similar cost, with the disadvantage that both the hardware and the software are more complex. Even whatever the hardware of the system, which fulfills the tasks of the system presented here, must incorporate a video camera similar to the one contained in the HuskyLens. Finally, the functionalities of the vision module not used in this system can be used to incorporate functionalities that require other applications, such as supervision and video surveillance.

REFERENCES

[1] P. Terhörst, D. Fährmann, N. Damer, F. Kirchbuchner and A. Kuijper, "On Soft-Biometric Information Stored in Biometric Face Embeddings", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(4), pp. 519-534, 2021.

[2] IEEE Standard for Biometric Privacy, *IEEE Std 2410-2021 (Revision of IEEE Std 2410-2019)*, pp. 1-37, 2022.

[3] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig and C. Busch, "Feature Fusion Methods for Indexing and Retrieval of Biometric Data: Application to Face Recognition With Privacy Protection", *IEEE Access*, 9(1), pp. 139361-139378, 2021.

[4] E. M. De Lacerda Filho, G. P. Pereira Rocha Filho, R. T. De Sousa and V. P. Gonçalves, "Improving Data Security, Privacy, and Interoperability for the IEEE Biometric Open Protocol Standard", *IEEE Access*, 10(1), pp. 26985-27001, 2021.

[5] Z. Akhtar and A. Rattani, "A Face in any Form: New Challenges and Opportunities for Face Recognition Technology", *Computer*, 50(4), pp. 80-90, 2017.

[6] Y. Zhong et al., "Dynamic Training Data Dropout for Robust Deep Face Recognition", *IEEE Transactions on Multimedia*, 24(1), pp. 1186-1197, 2022.

[7] F. Zhang, T. Zhang, Q. Mao and C. Xu, "Geometry Guided Pose-Invariant Facial Expression Recognition", *IEEE Transactions on Image Processing*, 29(1), pp. 4445-4460, 2020.

[8] S. -I. Choi, S. -S. Lee, S. T. Choi and W. -Y. Shin, "Face Recognition Using Composite Features Based on Discriminant Analysis", *IEEE Access*, 6(1), pp. 13663-13670, 2018.

[9] G. Lou and H. Shi, "Face image recognition based on convolutional neural network", *China Communications*, 17(2), pp. 117-124, 2020.

[10] W. Xu, Y. Shen, N. Bergmann and W. Hu, "Sensor-Assisted Multi-View Face Recognition System on Smart Glass", *IEEE Transactions on Mobile Computing*, 17(1), pp. 197-210, 2018.

[11] S. Kang, J. Lee, K. Bong, C. Kim, Y. Kim and H. -J. Yoo, "Low-Power Scalable 3-D Face Frontalization Processor for CNN-Based Face Recognition in Mobile Devices", *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 8(4), pp. 873-883, 2018.

[12] M. Awais et al., "Novel Framework: Face Feature Selection Algorithm for Neonatal Facial and Related Attributes Recognition", *IEEE Access*, 8(1), pp. 59100-59113, 2020.

[13] J. Sigut, M. Castro, R. Arnay and M. Sigut, "OpenCV Basics: A Mobile Application to Support the Teaching of Computer Vision Concepts", *IEEE Transactions on Education*, 63(4), pp. 328-335, 2020,.

[14] E. Cervera, "GPU-Accelerated Vision for Robots: Improving System Throughput Using OpenCV and CUDA", *IEEE Robotics & Automation Magazine*, 27(2), pp. 151-158, 2020.

[15] J. Huang, A. Huang and L. Wang, "Intelligent Video Surveillance of Tourist Attractions Based on Virtual Reality Technology", *IEEE Access*, 8(1), pp. 159220-159233, 2020.

[16] M. Valdeos, A. S. Vadillo Velazco, M. G. Pérez Paredes and R. M. Arias Velásquez, "Methodology for an automatic license plate recognition system using Convolutional Neural Networks for a Peruvian case study", *IEEE Latin America Transactions*, 20(6), pp. 1032-1039, 2022.

[17] A. Zhao and F. Ai, "Dual-Resonance NFC Antenna System Based on NFC Chip Antenna", *IEEE Antennas and Wireless Propagation Letters*, 16(1), pp. 2856-2860, 2017.

[18] E. U. Calpa, H. F. Pastrana, C. D. Caro, D. S. Becerra and F. E. Segura-Quijano, "NFC-Enabled Passive Sensor for the Quality Control of Ethanol Against SARS-CoV-2", *IEEE Sensors Journal*, 21(20), pp. 23608-23613, 2021.

[19] M. S. Chishti, C. -T. King and A. Banerjee, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication", *IEEE Access*, 9(1), pp. 6344-6357, 2021.

[20] A. Romputtal and C. Phongcharoenpanich, "IoT-Linked Integrated NFC and Dual Band UHF/2.45 GHz RFID Reader Antenna Scheme", *IEEE Access*, 7(1), pp. 177832-177843, 2019.

[21] A. Lazaro, M. Boada, R. Villarino and D. Girbau, "Study on the Reading of Energy-Harvested Implanted NFC Tags Using Mobile Phones", *IEEE Access*, 8(1), pp. 2200-2221, 2020.

[22] J. -Q. Zhu et al., "A Useful Methodology to Convert the Smartphone Metal Cover Into an Antenna Booster for NFC Applications", *IEEE Transactions on Antennas and Propagation*, 67(7), pp. 4463-4473, 2019.

[23] M. Boada, A. Lázaro, R. Villarino and D. Girbau, "Battery-Less Soil Moisture Measurement System Based on a NFC Device With Energy Harvesting Capability", *IEEE Sensors Journal*, 18(13), pp. 5541-5549, 2018.

[24] A. Sepas-Moghaddam, A. Etemad, F. Pereira and P. L. Correia, "CapsField: Light Field-Based Face and Expression Recognition in the Wild Using Capsule Routing", *IEEE Transactions on Image Processing*, 30(1), pp. 2627-2642, 202,.

[25] J. Lu, V. E. Liong and J. Zhou, "Simultaneous Local Binary Feature Learning and Encoding for Homogeneous and Heterogeneous Face Recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(8), pp. 1979-1993, 2018.

[26] R. He, J. Cao, L. Song, Z. Sun and T. Tan, "Adversarial Cross-Spectral Face Completion for NIR-VIS Face Recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 42(5), pp. 1025-1037, 2020.

[27] F. Mokhayeri, E. Granger and G. Bilodeau, "Domain-Specific Face Synthesis for Video Face Recognition From a Single Sample Per Person", *IEEE Transactions on Information Forensics and Security*, 14(3), pp. 757-772, 2019.

[28] J. Zheng, R. Ranjan, C. -H. Chen, J. -C. Chen, C. D. Castillo and R. Chellappa, "An Automatic System for Unconstrained Video-Based Face Recognition", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2(3), pp. 194-209, 2020.

[29] J. Cao, Y. Hu, B. Yu, R. He and Z. Sun, "3D Aided Duet GANs for Multi-View Face Image Synthesis", *IEEE Transactions on Information Forensics and Security*, 14(8), pp. 2028-2042, 2019.

[30] J. Liu, Q. Li, M. Liu and T. Wei, "CP-GAN: A Cross-Pose Profile Face Frontalization Boosting Pose-Invariant Face Recognition", *IEEE Access*, 8(1), pp. 198659-198667, 2020.

[31] Y. Zhong, J. Chen and B. Huang, "Toward End-to-End Face Recognition Through Alignment Learning", *IEEE Signal Processing Letters*, 24(8), pp. 1213-1217, 2017.

[32] Y. -F. Liu, J. -M. Guo, P. -H. Liu, J. -D. Lee and C. -C. Yao, "Panoramic Face Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, 28(8), pp. 1864-1874, 2018.

[33] Z. An, W. Deng, J. Hu, Y. Zhong and Y. Zhao, "APA: Adaptive Pose Alignment for Pose-Invariant Face Recognition!, *IEEE Access*, 7(1), pp. 14653-14670, 2019.

[34] Q. Feng et al., "Superimposed Sparse Parameter Classifiers for Face Recognition", *IEEE Transactions on Cybernetics*, 47(2), pp. 378-390, 2017.

[35] B. Ryu, A. R. Rivera, J. Kim and O. Chae, "Local Directional Ternary Pattern for Facial Expression Recognition", *IEEE Transactions on Image Processing*, 26(12), pp. 6006-6018, 2017.

[36] Z. Jian, Z. Chao, Z. Shunli, L. Tingting, S. Weiwen and J. Jian, "Pre-detection and dual-dictionary sparse representation based face recognition algorithm in non-sufficient training samples", *Journal of Systems Engineering and Electronics*, 29(1), pp. 196-202, 2018.