2022 14th International Conference on Computational Intelligence and Communication Networks (CICN) | 978-1-6654-8771-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/CICN56167.2022.10008350

Processing of Images Based on Machine Learning to Avoid Unauthorized Entry

Cesar Peña
Facultad de Ingeniería Electrónica
Universidad Nacional Federico Villarreal
UNFV
Lima, Peru
cpena@unfv.edu.pe

Ciro Rodriguez
Facultad de Ingeniería Electronica
Universidad Nacional Federico Villarreal
UNFV
Lima, Peru
crodriguez@unfv.edu.pe

Israel Arellano Romero
Department of Software Engineering
Universidad Nacional Mayor de San Marcos UNMSM
Lima, Peru
isrrael.arellano@unmm.edu.pe

***Abstract*— The proposal of a facial recognition system to increase security, through facial recognition with multiple utilities such as facilitating the access of people with adequate protection measures in times of Covid-19, as well as security when seeking to hide their identity. The methodology considers the use of tools such as Python and OpenCV, as well as models such as Eigen Faces, Fisher Faces, and LBPH Faces, as units of analysis are considered photographs and portions of the video that capture facial expressions that then their patterns are trained with facial recognition algorithms. The results obtained show that the LBPH Faces obtained confidence values lower than 70, with a 95% certainty of recognition and a shorter recognition time, improving the accuracy of facial recognition, also with the increase of the data was achieved to improve the accuracy of recognition as well as improve confidence regarding the safety of people.**

Keywords*— *Facial recognition, machine learning, COVID-19, image processing, LBPH, unauthorized entry

I. Introduction

For a long time, pandemics have accompanied mankind, causing millions of deaths in the world, such as the bubonic plague during the Middle Ages, which originated in Asia and migrated to the old continent, Europe, and in this 21st century the new ones known as SARS-COV, whose origin is China, are appearing. The pandemic caused many people to wear masks, and the use of masks in some cities increased the way to hide their identity and hide being recognized.

In these times, when technological development is impressive, facial recognition helps us identify people and know who they are individually, thus being able to know the details of the person. It is a technology that identifies and verifies a person from a video, photo, or their face in real time, it is also used as a security element to access your mobile phone, an application, or a service. Facial recognition adds a layer of security to prevent fraud or identity theft, as well as speed up the identification of persons. This technology is booming, and the trend is to increase its application in different places where a person usually goes on a daily basis. In addition, in recent years his research has been increasing. In order to improve security in access to educational institutions we intend to use facial recognition, this technology will help us in the area of security by accurately identifying students whether they are from college, institute or university. The programming used is Python and some of its libraries that will facilitate the coding for facial recognition, using videos from which images will be extracted in a defined quantity, the images obtained will be able to extract are with different expressions on the face, those same images will be used it to train the program and thus improve the accuracy when recognizing the person.

II. Methodology

The functionality of the system to be created is classified into the following steps:

a) *Obtaining data*: The images can be obtained from a video, from a webcam, or from previously obtained photos which will form part of our dataset. When obtaining the images is important to take into account the multiple expressions of the face

b) *Recognizer Training*: The next step is to train the recognizer by adding labels or extra information associated with the image of that person, the more images to obtain of the subject, the better it will be for training and thus improve accuracy.

c) *Recognition:* In this step, is used the algorithms on Python language to recognize people who previously went through steps 1 and 2. People will go through the camera and the created system will be able to identify the person, show their name, and if they belong to the educational institution. Thus, achieving improvement in the security area preventing the entry of people outside the institution. It is necessary to mention that for better recognition is possible to have carried out the training with a good amount of data.

PyCharm was used to be able to carry out the Python coding, and created the facial recognition project for educational institutions as a study case and was consider importing the necessary libraries such as OpenCV, and NumPy, among others; which helped us to create the system. The collected images went through training and then the file generated by the training was used to be able to recognize people.

978-1-6654-8771-9/22/$31.00 ©2022 IEEE
DOI: 10.1109/cicn.2022.135

A. Models

In order for the objective of accurately recognizing people, the system should be trained. Three models for the tests such as EigenFaces, FisherFaces, and LBPH Faces and also other as RaspberryPi [6] will be used to emphasize the methodology.

EigenFaces: [2] The recognition is carried out by projecting an image of a face in the subspace formed by the eigenfaces and comparing its position with that of other known faces. The eigenfaces are a set of graphically represented vectors, becoming a kind of map of the variations between images. These vectors are the result of the application of PCA to the covariance matrix of a set of images of faces which are called eigenvectors, being multidimensional.

FisherFace: The Fisherface is a method that is responsible for face recognition, taking into account how light is reflected and facial expressions [3]. This algorithm maximizes the ratio between the class distribution and the intra-class distribution. Fisherface classifies and reduces the dimension of faces using the Fisher Linear Discriminant (FLD) method and PCA (known as Eigenfaces). This method creates a linear projection that maximizes the different projected face images.

LBPH Face: The local binary pattern method was designed for texture description. The use of local descriptions in some regions of the face provides more information than others, so the texture descriptors tend to average the information they describe, which is not convenient when describing faces since maintaining information on spatial relationships is important. [4]. To form the global description, the face image is divided into different regions, to which a histogram is applied to obtain the LBPH operator that describes independent information by region. These local descriptions are then concatenated to build a global description of the face [5]. The LBPH method assigns labels to each of the pixels in the image taking into account the distribution of neighbors. These are the steps that the LBPH performs for its respective image recognition. As well as these there are also other methodologies that use the RaspberryPi [6].

Facial recognition in this proposal has connected a camera with the real-time application, comparing the records stored in the Raspberry Pi where the name of the person is shown [7].

A multi-scalar and dynamic facial rendering method to improve prediction performance [8]. Multiple time scales are used with convolutional networks CNN in facial regions.

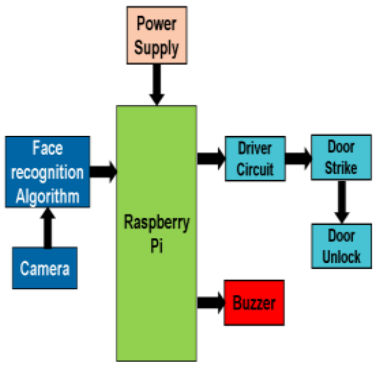

Fig. 1. Design and Implementation of a Door Access Security System Based on Facial Recognition using Raspberry Pi [7].

The proposal considers automatic learning for the recognition of people in situations where their authorization is not authorized, such as in places that require a level of protection without high costs and that allow obtaining additional recognition information, alternatives were explored with the use of low-cost hardware that improves mobility, for which it was evaluated to merge as an alternative Raspberry Pi with infrared cameras Fig 1.

Feeling secure all day is needed [9]. Face recognition is obtained with the system where the face taken from a dataset, matches the name. Facial recognition with OpenCV is combined with Python.

The OpenCV concept has a multitiered framework to recognize faces and XM identifying body parts [10]. OpenCV and detection and recognition work on accepting the input image and giving the best recognition results. The libraries used are dlib and face_recognition with a combination of Python and OpenCV.

The idea is to process the image in real time by processing the feature extraction, which is validated with the stored dataset and then perform the comparison where the slightest difference in the features will be highlighted. Face detection can be performed with Haar classifiers with training to convert to yml for the recognition process with LBPH by checking if it contains the yml in the training, the match or difference is possible to identify as in the process of Fig. 2.

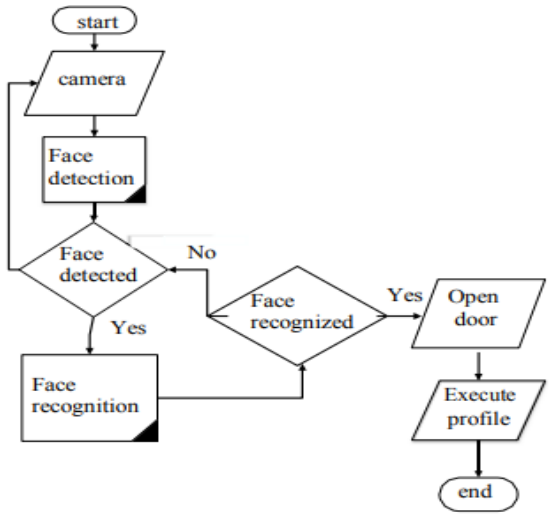

Fig. 2. Operation of the facial recognition system [11].

On the other hand, a classification model for face recognition is considered, for which a proposal is explored with face detection and recognition from the moment the entry is made as shown in Fig. 2.

B. Approach

The system is focused on security, speed, and accuracy when recognizing a person and allowing entry or denying them as the case may be, aimed at educational entities such as schools, institutes, and universities.

Recognition systems have been important during the pandemic for both security and prevention, and the use of masks to prevent contagion was also a means for criminals to hide their identity, requiring individual authentication, which in turn requires more complex and automated methods that can improve the facial recognition process [12]. Improve the performance efficiently in a very short period of time and eliminate the main errors made by humans. A real-time GUI-based face recognition system can facilitate this face detection work and can be achieved in several ways [13].

C. Methods and techniques

The method used is the collection of data through a webcam or surveillance camera from which multiple images will be extracted and stored in our Data folder, previously separated by names for each person if the folder does not exist, the system creates it and within it, the images of each person are stored, these images will go through a recognition training and a file named ModeloLBPHFace.xml will be generated, which will contain all the information in a structured way so that the program can later perform facial recognition

D. Materials:

The Python programming language, the libraries for facial recognition such as OpenCV. A code development IDE for Python such as ' PyCharm ' can also use any code editor such as Visual Studio Code and Sublime Text. Also, a 6th Generation Lenovo i7 Laptop with 8GB RAM, Intel core i7-6500 CPU 2.50Ghz 2.60 GHz, System Type Windows 10 64-bit, a 2GB AMD Radeon Graphics Card, and Webcam.

III. Proposal

The proposal is to create a system based on the Python programming language and the corresponding libraries such as OpenCV that allow us, from the dataset of images obtained from the videos, to be able to train the system and thus recognize the person in question as part of the educational institution, since educational institutions such as colleges, institutes or universities do not have an adequate system to improve security, the system will help quickly and accurately identify a student and allow them to enter, facial recognition helps us improve security by preventing identity theft and preventing the entry of people who could be expelled or are not part of the educational institution, for example in universities they show their ID and the security guard sometimes sees the face of the person on the ID and sees the similarity with the person, but mostly he only sees the card and lets pass, so the security system are not working a and allows people outside the institution to infiltrate. That and other security situations are necessary to improve by using facial recognition.

A. Architecture

The architecture of the system considers three important points of the process such as the generation of Data, training of the recognizer, and recognition. Fig. 3 shows the architecture used to create the system which consists of Generating the data, training the recognizer, and recognize the person.

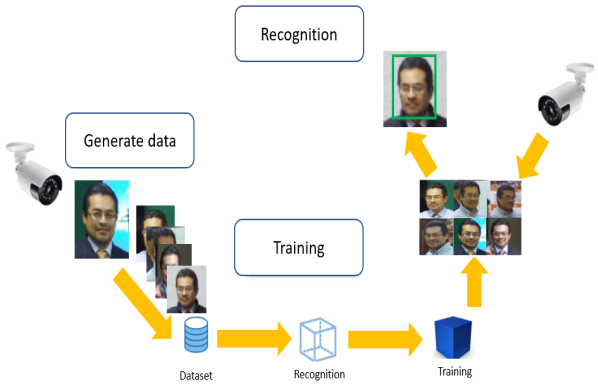

Fig. 3. System Architecture.

Two models for the tests were used, each model has a video of approximately 2 minutes in duration, the people selected for the tests with A and B persons, and each one also has a folder with their name in case they do not have a folder the system creates it, in these folders the images that are captured from the video will be stored[11].

The data obtained, Fig. 4 and 5, was created from a video captured with the webcam from which the capture of video images was programmed, the same ones that were used to carry out the training, the training was done with data of 500

images per person. which are different from each other, but all belong to the same person. In Table I we see some details of the video of both people [14].

B. Capturing and cropping faces from video

For recognition, test images called image A and image B will be used, which have been subjected to different variations of positions, gestures, and light intensities.

Fig. 4. Faces A coded.

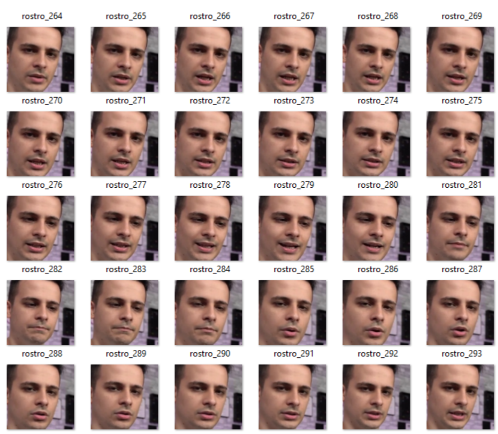

Fig. 5. Faces B coded.

The faces with which they worked were captured from a video for person A and for Person B and the details and time are shown in Tables I and II.

TABLE I. VIDEO DETAILS

Person	Weight	Resolution	Format
A	6 148 KB	804 x 452	.mp4
B	150 663 KB	357 x 636	.mp4

TABLE II. PROCESSING TIME OF FACES IN SECONDS

Number of faces	Time in seconds	
	A	*B*
100	8.9345	7.5175
200	16.5848	14.0279
300	24.4825	19.6772
400	30.3232	26.3127
500	36.4124	32.7463

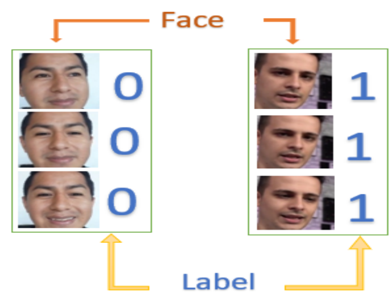

Fig. 6. Image preparation for training.

Preparation of the dataset with image labels showing the classification of the recognition as in Fig. 6.

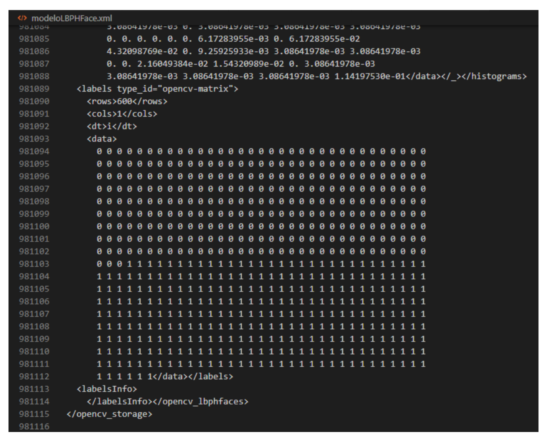

Fig. 7. Data processing.

Data are processed in a matrix with OpenCV

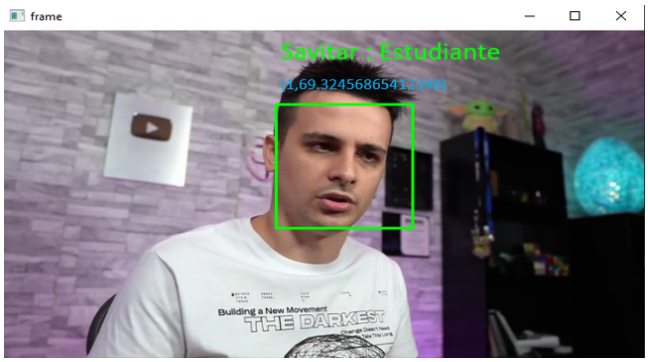

Fig. 8. Recognizing person B and showing their data as a student.

As shown in the proposed architecture of the system shown in Fig. 3, faces were sampled and gradually entered into a dataset, faces with different shapes were identified as shown in Fig. 4 and Fig. 5, images were prepared as shown in Fig. 6, and then the data was processed as shown in Fig. 7, until the recognition with detail identification as shown in Fig. 8 [15],[16].

IV. Results

After the data collection and the respective training, we gave way to the recognition test, which was successful, we did the recognition test with another video of person B and the system was effectively able to recognize the person.

TABLE III. PROCESSING TIME OF FACES IN SECONDS

Number of faces	Training time in seconds		
	Eigen	*Fisher*	*LBPH*
100	8.6015	3.4249	2.4219
200	33.1455	17.1319	7.2557
300	53.1841	33.4474	8.2162
400	92.4477	78.2951	11.2621
500	146.5688	105.9114	10.1478

Person B recognition and the side of the position he occupies. The following information was collected from the tests carried out, which we can see in greater detail in Table IV.

TABLE IV. PROCESSING TIME OF FACES IN SECONDS

Number of images	Recognizer method			Approval
	Eigen	*Fisher*	*LBPH*	
500 images per person	<5700 Student confidence values in the thousands	<500 Student Confidence values less than thousands	<70 Confidence values less than hundreds	95% {Name of individual} {Occupation}

The three tested methods and their confidence values are shown in Table IV, if they exceed the confidence values, the faces will be presented as unknown

V. Discussion

The result expected for facial recognition was one of the most satisfactory, we were able to test the three recognizer methods, and depending on the method we were testing, they gave us confidence values that could be higher or lower, some such as the EignvFace method gave us confidence values of thousands, the Fisherv Face gave us confidence values less than 500 and finally, the LPBH method gave us confidence values less than 70, but according to other authors who used some of the methods, the confidence values varied slightly but did not go too far and were within of the range described for each.

In some places like the UNED [14], biometric identification technologies can impact teaching/learning processes in unexpected ways. They mainly focus on facial recognition to help in exams and avoid identity theft.

Other technologies can be used to implement facial recognition such as RapsberryPI and Python as one of the works we read (Face Detection and Recognition using Raspberry Pi) where they use this technology to perform facial recognition.

VI. Conclusion

In conclusion, the use of the facial recognition system in educational institutions effectively speeds up the authentication process and reinforces the security system, preventing the entry of people outside the institution. The system helps us accurately identify persons, avoid identity theft, as well as prevent the entry of people who do not belong to the institution. The data can be obtained from a video, a webcam in real-time, or previously obtained data.

We can support ourselves with Python and OpenCV as well as other libraries, also from Raspberry PI, and its own benefits that can also be used for facial recognition. The confidence levels that we obtain will depend on the amount of data with which we are going to work and the method that we choose because depending on which one we choose; the confidence level tends to vary.

With the advancement of technology and the increase in security levels, the use of facial recognition will be more common for companies and government organizations, but also to speed up commerce and in university libraries so that just by using facial recognition you can access the loan of books.

Facial recognition has great potential to improve operational security for the best performance of their functions, especially in emerging countries.

In future work, will be interesting to explore the security of the images obtained by the system, and the security expanded to the attack on the system, which recognizes face masks in real-time video.

REFERENCES

[1] J. Vadlapati, SS Velan, and E. Varghese, “Facial Recognition using the OpenCV Libraries of Python for the Pictures of Human Faces Wearing Face Masks during the COVID-19 Pandemic,” IEEE, p. 6, 2021.

[2] JC. Bustamante, C. Rodriguez, D., Esenarro. (2019). Real time facial expression recognition system based on deep learning. International Journal of Recent Technology and Engineering, 2019, 8(2 Special Issue 11), pp. 4047-4051. doi: 10.35940/ijrte.B1591.0982S1119.

[3] C. Rodriguez, D. Luque, D. Rosa, D. Esenarro,. and B. Pandey 2020."Deep Learning Applied to Capacity Control in Commercial Establishments in Times of COVID-19," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, pp. 423-428, doi: 10.1109/CICN49253.2020.9242584..

[4] A. Maier , C. Syben , T. Lasser , C. Riess . “A gentle introduction to deep learning in medical image processing,” Zeitschrift fire Medizinische Physik 2019, Volume 29, pp.86-101. https://doi.org/10.1016/j.zemedi.2018.11.002.

[5] E. Ayan , Ünver , H. (2019).“Diagnosis of Pneumonia from Chest X-Ray Images Using Deep Learning,” Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science, pp. 1-5, doi : 10.1109/EBBT.2019.8741582.

[6] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri , R. Summers, "ChestX-Ray8: Hospital-Scale Chest X-Ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases," 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 3462-3471. doi :10.1109/CVPR.2017.369.

[7] N M. Niu, J. Tao, and B. Liu, “MULTI-SCALE AND MULTI-REGION FACIAL DISCRIMINATIVE REPRESENTATION FOR AUTOMATIC DEPRESSION LEVEL PREDICTION,” IEEE, Biijin, China, 2021.

[8] IM Sayem and M. Sanaullah, “Integrating Face Recognition Security System With the Internet of Things,” IEEE 2018 International Conference on Machine Learning and Data Engineering (iCMLDE), vol. I, no. 2, p. 5, 2018.

[9] T. Dhawle, U. Ukey, and R. Choudante, “Face Detection and Recognition using OpenCV and Python,” International Research Journal of Engineering and Technology (IRJET), vol. 07, no. 10, p. 3, 2020.

[10] A. Munir, SK Ehsan, SMM Raza, and M. Mudassir, “Face and Speech Recognition Based Smart Home,” 2019 International Conference on Engineering and Emerging Technologies (ICEET), pp. pp. 1-5, 2019

[11] T. Dhawle, U. Ukey, and R. Choudante, "Face Detection and Recognition Using OpenCV and Python," International Journal of Research Engineering and Technology (IRJET), India, 2020.

[12] T. Dhawle, U. Ukey, and R. Choudante, "Face Detection and Recognition Using OpenCV and Python," International Journal of Research Engineering and Technology (IRJET), India, 2020.

[13] S. Guha, A. Chakrabarti, S. Biswas, and S. Banerjee, “Implementation of Face Recognition Algorithm on a Mobile Single Board Computer for IoT Applications,” 2020 IEEE 17th India Council International Conference (INDICON), No. 17, p. 5, 2021.

[14] JL Aznarte, MM Pardos and JML López, «On the use of Facial Recognition Technologies in University: the UNED case,» National University of Distance Education, Spain, 2022.

[15] S. Narejo, B. Pandey, D. Esenarro, C. Rodriguez and M. Anjum (2021). Weapon Detection Using YOLO V3 for Smart Surveillance System. Mathematical Problems in Engineering. Hindawi, 1024-123X. https://doi.org/10.1155/2021/9975700.

[16] Adam Schmidt, Andrzej Kasinski, “The Performance of the Haar Cascade Classifiers Applied to the Face and Eyes Detection”, Computer Recognition Systems, 2016.