IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 1, Ser. II (Jan - Feb 2020), PP 42-48
www.iosrjournals.org

CORDOBA System: Physical Access Management Control System with Face Detection and Face Recognition

Giacomo Abbattista[1], Vito Nicola Convertini[2], Vincenzo Gattulli[3], Lucia Sarcinella[4]

[1](*Department of Computer Science, University of Bari Aldo Moro, Italy)*
[2](*Department of Computer Science, University of Bari Aldo Moro, Italy)*
[3](*Department of Computer Science, University of Bari Aldo Moro, Italy)*
[4](*Department of Computer Science, University of Bari Aldo Moro, Italy)*

Abstract:*This work will address the issue of corporate access security. One of today's problems affecting companies around the world. This study will cover both access to the "main door" and "internal company access". The accesses to the "main door" will be monitored by a Face Recognition system, while the internal accesses will be monitored by the Cloud thanks to the Arduino Beacon technology installed on each internal door of the company.This work will therefore deal with the concepts of Face Detection and Face Recognition, thus creating a system that will perform better in the corporate field. The core of the work is focused on the explanation, implementation and testing of the techniques used with the help of the "CORDOBA dataset" created specifically for the company. This dataset will also contain faces that will be taken from the CASIA-WebFace online public dataset used for unrestricted scientific research of facial recognition. The face images in the dataset are scanned from the Internet by the Institute of Automation, Chinese Academy of Sciences (CASIA). Consequently, thanks to our study, new knowledge and new answers to general problems regarding security in access to companies have been obtained. With the aim of solving the problem and accelerating and predicting facial recognition in the best possible way. The intent will be to show the goodness of the approach proposed with the adjacent experimentation.*

Key Word*:Face Recognition, Face Detection, Company.CORDOBA, Physical Access Management Control System*

Date of Submission: 28-01-2020 Date of Acceptance: 13-02-2020

I. Introduction

In recent years, security has become a potential global problem. Biometrics-based systems have been built to help these issues, which are able to provide biometric security, crime prevention and video surveillance services due to their integrated verification and identification capabilities. In this work we will focus on Facial Biometric Systems, considering the Face Detection phase and the Face Recognition phase. When we talk about Face Recognition, we refer to a technology that allows to recognize or verify the identity of a subject through a digital image of him entered previously in the software. The identities that the software is able to recognize are those provided by service users during a so-called training process, during which they insert their images into the database. Training images usually must be subject to many rules: they must be evenly illuminated and must necessarily be face-centered, to allow the service to detect the face. However, there are several common issues related to this approach: users of a service want to make sure that their sensitive data remains private and the face is definitely one of these. In addition, you must consider the technical limitations of implementations, make a recognition is summarized by assessing the similarity between two faces in the data set, but defining when this distance is within an acceptable limit is extremely complicated. The most important limitation is how this service can withstand the passage of time and the aging of users.

II. System Architecture

The access into the company can be done by many professional figures from maintenance workers up to the company president.There are therefore many issues to manage and monitor. Two types of places mentioned: The first place is the "Main Door" of the company, while the second type of place, equates to all kinds of entrance doors within the company such as offices, meeting or conference rooms, staff-only rooms and so on which we'll call "Secondary Doors".

As for the first type of port, there is two-way authentication: instead of the peephole of the door, a camera will be installed, and the user can be recognized by the camera through an algorithm of made

recognition. If the user has been correctly recognized, a software checks the security policies requesting them to the Cloud to check if the user can actually access the company on that particular day and time.

As for the second type of door (secondary doors), also in this case there is a two-way authentication: every door inside the company prepared for this type of security, is provided by some Arduino, configured as Beacon technologyvia the programmable beacon protocol. These Beacons, which will simulate the internal doors of the company, as soon as they identify another Bluetooth device in their range, will send a message to the device to ask if the user in question wants to enter the room. Therefore, the user who actually wants to enter and who will own his bluetooth device, such as a smartphone, will confirm the message received by the beacon. At this point, a software will check the security policies by requesting them from the Cloud to check if the user can actually access on that particular day and time.

The core of the system will be implemented on Raspberry, developed in the UK by the Raspberry PI Foundation1 with some alternative development boards, considering the technology that concerns access to the company's main door. While the Arduino Technology, developed in 2009 by some members of the Interaction Design Institute in Ivrea, will be useful to be able to simulate the internal doors of the company.The problem of access is a problem open to many technologies and devices; with our procedures we will try to respond in the best possible way with a procedure dictated by our experimentation.In the company it is a significant problem to try to get access to certain doors only to authorized persons at certain pre-established times based on the role covered. After the person has managed to enter through the main door, the role he holds in the company will already be assigned in the database. Based on that role, at the time and date you will be able to access certain locations within the company. Access to the specific Door Inside or Secondary Door the company is facilitated thanks to the Beacon Technology. The Beacon Technology is implemented with Arduino through the Eddystone beacon protocol, so as to be able to easily install these Arduino on the internal doors of the company (Figure 1).

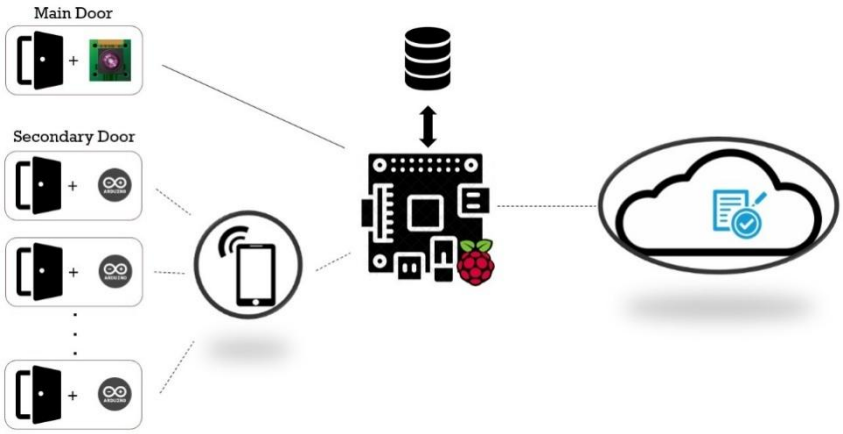

Figure 1. Ideal Scheme Work Project

The Ideal system that characterizes the work project is as follows:

- *MainDoor*: It will be the module that will implement the two Face Recognition programs. On the RaspberryPi the Picamera will be installed which will be located instead of the peephole of the entrance door, which will only accept front faces that will look directly at the room;
- *SecondaryDoor*: The term represents the internal doors of the company, they will be specifically accompanied by an *Arduino nano 33 IoT* device with Eddystone Beacon protocol that will allow the sending of Advertising messages, in broadcast without peering;
- Smartphone Application: The smartphone application will receive the Advertising message of the nearest door, the employee will click on his smartphone the door he wants to go through;
- *RasberryPi*: It will be the core of the system. It will present the Face Recognition Algorithm implemented for the security of the main port, will receive security policies from the cloud, update the internal database with them, check in the database whether the individual can enter the company or not.
- *Database*: The database will be installed on RaspberryPi and will contain information from company employees: roles, entry times, date of access;
- *Cloud*: The cloud will be a real WebServer that will send the policies to the RaspberryPiso as to be able to update the database policies whenever a person accesses the company. The procedure to open the door will start from the RaspberryPi that will send a post request containing a simple string that will contain the credentials of the individual (name, surname and role) that will be received by the Web server.

Thus,creating a real access log. If the acknowledgment is successful, the string will appear in the server log, and it can then send a notification of the physical port opening.

III. State-of-the-Art Algorithm

In this work we will focus on the state of the art of the Face Detection and Face Recognition algorithm,leaving out the other technologies previously mentioned.Over the last ten years, a great deal of work has been done in the detection and recognition [1]. These approaches are constantly evolving with the aim of finding more and more performative and accurate detection and recognition [2]. Thanks to this evolution these techniques have become a very hot theme in biometrics. Why many methods of Detection have been introduced [3] [4] [5] [6] [7] and Face Recognition [5] [8] [9] [10], so much so that they are considered milestones in this topic.

Face Detection:

Face Detection is a specific case of object-class detection, in which principal task is search the position and the dimension of object in an image that belong to a determinate class. However, Face Detection is still a very difficult challenge due to the high variability in the size, shape, color and texture of human faces. Typically, face detection algorithms implement face detection as the Binary Pattern Classification Task. This means that, given an input image, it is divided into blocks and each block is transformed into a function [11].

Facial detection methods can be classified into the following categories:

- *Knowledge-based methods*: these techniques are based on rules that encode Human Knowledge on the relationship between facial features (*Yang [12]*).
- *Feature invariant techniques (e.g. facial features (Yow &Cipolla [13]), texture e multiple features):* find structural features that remain unchanged regardless of changes in face posture and lighting conditions.
- *Template matching methods (E.g. predefined templates e deformable templates (Yuille [14])):* these approaches are based on the use of a standard face pattern that can be manually predefined or parameterized using a function. Then, the face detector is to calculate the correlations between the input image and the pattern.
- *Knowledge-based methods*: these techniques are based on rules that encode Human Knowledge on the relationship between facial features (*Yang [12]*).
- *Feature invariant techniques (e.g. facial features (Yow &Cipolla [13]), texture e multiple features)*: find structural features that remain unchanged regardless of changes in face posture and lighting conditions.
- *Template matching methods (E.g. predefined templates e deformable templates (Yuille [14]))*: these approaches are based on the use of a standard face pattern that can be manually predefined or parameterized using a function. Then, the face detector is to calculate the correlations between the input image and the pattern.

Face Recognition:

Face recognition could be categorized based on many types of algorithms. These include: Classical Face Recognition Approach, Face Representation, holistic approach, statistical approach, model based approach, feature based, artificial intelligence approach, hybrid approach, Gabor wavelets approach, Face descriptor - based methods, 3D - based face recognition and Video- based face recognition (Naeem el, 2015; Wojcik et al, 2016).

- *The classic face recognition approach*: it focuses on the local structure of the manifold. These methods project the face into a linear subspace crossed by eigenface images (Wojcik et al, 2016);
- *Face Representation*: The model with Face Representation [15] will result in a better representation of the face, a better computation speed and a faster detection phase exploiting only the best distance between the features. Thus, the use of ensemble networks leads to stronger representations and better performance to find the best representation of the faces of a certain domain. We then describe the networks together with the respective training details. These networks are based on ResNet-101 [16], Inception ResNet-v2 [17], ResNet-34 [16];
- *Holistic approach*: In the holistic approach, the entire face is considered a feature for detection and recognition. Compare whole faces but ignore individual features such as mouth, eyes and nose, etc. The holistic group can be divided into linear and nonlinear projection methods or grouped as statistical and artificial intelligence methods (Naeem el, 2015; Wojcik et al, 2016). Good examples of holistic method are Eigen faces, PCA, LDA e ICA (Parmar and Mehta, 2013) [18];
- *Artificial Intelligence approach*: this approach uses artificial neural networks to automatically recognize faces. Artificial neural networks are used to solve non-linear problems. A non-convergent chaotic neural

network recognizes human faces. Radial basis function neural is integrated with non-negative matrix factorization (Naeem el, 2015; Wojcik et al, 2016);

- *Statistical approach*: The statistical approach involves calculating the density of the face image and comparing the density values set with the density values of the images in the database (Naeem el, 2015). This approach involves representing patterns as features. The function of recognition is a discriminating function (Marques, 2010). Examples of statistical methods are: PCA, ICA, LDA, Discrete Cosine Transform, Kernel PCA, Gabor Wavelet e Locality Preserving Projections (Marques, 2010) [18];
- *Feature-based approach*: The feature-based approach is of a structural nature and considers individual facial features such as ears, nose, eyes and mouth and matches the similarity between images. This approach could also include hexagonal facial features. Face recognition is performed using heuristic parameters and is stored in a database (Naeem el, 2015; Parmar e Mehta, 2013);
- *Gabor wavelet- based solutions*: Gabor wavelets show desirable features of capturing salient visual properties such as spatial localization, orientation, selectivity and spatial frequency. Several biometric applications use this approach. Gabor wavelets are widely used because Gabor features are recognized as a better representation for face recognition (Wojcik et al, 2016);
- *Face descriptor- based methods*: the face descriptor-based method with local feature-based face image description offers a global description. They are evaluated in neighboring pixels and then aggregated to form the final global description. The purpose of image descriptors is to learn the most discriminating local characteristics that minimize the difference between images of the same person and maximize those between other people's images. These methods are discriminatory and robust for changes in lighting and expression. They provide a compact, easy-to-extract and highly discriminating descriptor (Wojcik et al, 2016) an example would be the LBP, LBPH [18];
- *3D- based face recognition approach*: 3D-based face recognition extends the traditional 2D acquisition process and has more potential for accuracy. The 3D process is getting cheaper and faster. 3D detection has a higher recognition accuracy than 2D. The advantage is that depth information does not depend on laying and lighting, and therefore the representation of the object does not change with these parameters, thus making the whole system even more robust. 3D-based techniques offer more robustness in posing variation problems than 2D-based techniques (Wojcik et al, 2016);
- *Model based approach*: model-based facial recognition approach may be in 3-Dimensional or 2-Dimensional form. Algorithms aim to build a human face. The 3D approach is more complex because it aims to capture the three-dimensional nature of the human face. Examples are elastic bunch graph matching (Marques, 2010; Naeem el, 2015) [18];
- *Video- based face recognition*: Video-based face recognition uses redundancy in the video sequence to improve image systems. The initial phase of Video-Based Face Recognition (VFR) performs re-identification, in which a series of videos is cross-matched to identify all occurrences of the person of interest. Video-based face recognition can be grouped into two categories:
    a. Sequence based;
    b. Set based.

  At a high level, these two approaches are differentiated based on whether they use temporal information. The advantage of using this approach is the use of redundancy in videos to improve image systems (Wojcik et al, 2016);
- *Hybrid approach*: This method uses both holistic and feature based approaches (Naeem el, 2015; Parmar e Mehta, 2013; Zhao et al, 2003). Most of the time, 3D images are used, so you could also observe the curves of the eye sockets [18];

IV. Implementation

The implemented algorithm presents the FaceRecognition and Detection techniques, with attached libraries used to implement it in Python (Table 1):

Python Library	*Face Detection*	*Face Recognition*
Dlib + Face_Recognition	HOG + SVM	Face Embedding Model: ResNet-34

Table 1. Python Design Algorithm

Face Detection and Face Recognition Implementation:

The algorithm uses a Support Vector Machine (SVM) combined with HOG (Histogram of Gradients) to detect faces.While as regards the Face Representation phase, the algorithm will use a Face Representation (ResNet-34) to best represent the faces and immediately after through a similarity control between the feature vectors of the input image and the model of training the most similar image of the training will be chosen.Histogram of Oriented Gradients (HOG) is a feature descriptor used in Artificial Vision. In Artificial Vision, visual descriptors or image descriptors are descriptions of the visual features of content in images, videos, or algorithms or applications that produce such descriptions. Describe elementary features such as shape, color, texture, or movement.

Support Vector Machine (SVM) is a machine learning model proposed by Vladimir N. Vapnik and Alexey Ya. Chervonenkis in 1963. The goal of SVM is to find a hyperplane that best separates the input classes.

For this program, we will use some packages:

- *Dlib*: for detection and recognition;
- *face_recognition*: library that uses Dlib specifically for faces;
- *OpenCV*: Free library to manage images and graphic windows;
- *picamera*: package that will allow us to detect and program the Picamera of the Rasperry.

In this case we need images that contain the faces of people to be recognized (they do not need to be cropped on their faces). Thanks to this type of algorithm, you do not need as many images per person, but you only need to insert into the database only one image per person (Figure 2).

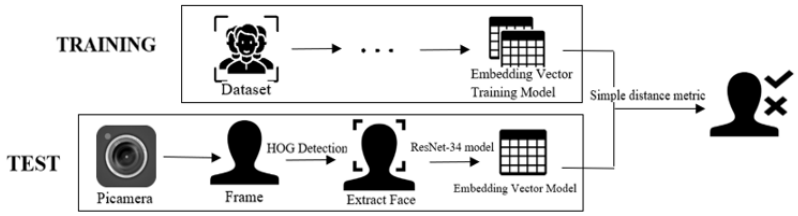

Figure 2 - Program Process Scheme

Now we'll look at the 5 general steps of the algorithm:

- We should capture a stream of images from the camera connected to Raspberry using the appropriate Python picamera library;
- The face detection model will detect the position of the faces in the image;
- You will then create the face model in input or vector of face features: then a vector of size 128;
- Then the input face model will be compared with the total face model in the database and then find the closest one;
- Finally, thanks to a threshold will be the prediction of the algorithm on the genuineness of the face;

For this program, we need two models:

- A face detection model;
- A face embedding model that transforms an image into a specially trained vector (or embedded) on faces.

For both it will be possible to use the models available in the Dlib library:

- A HOG + SVM face detection model (Histogram of Oriented Gradients + linear SVM classifier)
- *And a face embedding model*: a slightly modified ResNet-34 classification model trained on 3 million faces, in which the last classification layers have been removed to transform it into an inclusion model.

V. Experimentation

The experimentation phase provided useful answers to this work, by answering the following question: Does the face recognition system perform well for the company in question?

To answer the question, the concept of confusion matrix will be developed with the various parameters attached (TP, TN, FP, FN, ERR, Accuracy, Precision, Recall, F-score). The Face Recognition program will also be modified because it will have to receive images and no more stream frames, with the addition of a piece of code that will create ad hoc Excel files for the analysis of results and observations.The CORDOBA database created to answer the question at the beginning will be considered. This dataset will also contain the faces that will be taken from the CASIA-WebFace online public dataset used for the scientific research of unrestricted

facial recognition. The face images in the dataset are scanned from the Internet by the Institute of Automation, Chinese Academy of Sciences (CASIA).

CORDOBA Dataset:

The CORDOBA Dataset created will contain a total of 185 images divided into 4 different categories, all four categories have been scaled to 250x250 pixel resolution:

- The first category contains 45 images of generic objects that surround us, of everyday life such as cars, chairs, TVs, plants etc. These images are critical to testing the detection of the system;
- The second category contains 45 images of objects that in looking at them recall the characteristics of a human face with nose, mouth, eyes that could fool the Face Detection phase;
- The third category contains 45 images of "forgers" who are not allowed access to the company. These photos were found at random from the CASIA-WebFace Dataset, a public dataset that portrays the faces of numerous actors sought after on the web;
- The fourth category contains 50 images of "genuine" people who are allowed access to the company. This category was created personally to be able to recreate the real status of the employees who could access the company in question during the work period. 5 individuals were selected and for each of them 10 different photos were taken, with slight variations in brightness, angles and expressions. In such a way as to best simulate the picamera.

The testing phase of these programs implements the10-Cross Fold Validationwith different threshold ranges.

VI. Results

Detection Results:

Detection Expected:Genuine: 95 *Forgery*: 90 on 185 Dataset images

N = 185	Expected: No	Expected: Yes	
Actual: No	TN = 87	FP = 3	90
Actual: Yes	FN = 0	TP = 95	95
	87	98	

Table 2 - Confusion matrix of Detection Program

The values of each parameter are described as an absolute number. Instead, we will show a table containing five other evaluation parameters.

Parameter	*Value*
ERR	0,02
Accuracy	0,98
Precision	0,97
Recall	1
F-Score	0,98

Table 3 - Parameter and Value of Detection Program

Recognition Results:

The results of the Recognition of the second program are as follows:

Threshold	*TP*	*TN*	*FP*	*FN*	*ERR*	*ACC*	*PRE*	*REC*	*F-Score*
40	41	135	0	9	0,04	0,95	1	0,82	0,89
42	44,6	135	0	5,4	0,02	0,97	1	0,89	0,94
44	46,2	135	0	3,8	0,02	0,97	1	0,94	0,96
46	47,8	135	0	2,2	0,01	0,98	1	0,95	0,97
48	48,6	135	0	1,4	0	0,99	1	0,97	0,98
50	49,8	135	0	0,2	0	0,99	1	0,99	0,99
52	50	135	0	0	0	1	1	1	1

54	50	135	0	0	0	1	1	1	1
56	50	134,7	0,3	0	0	0,99	0,99	1	0,99
58	50	134,2	0,8	0	0	0,99	0,98	1	0,99
60	50	134,1	0,9	0	0	0,99	0,98	1	0,99

Table 4 - Table for each threshold of the Recognition program

In the table above, there are 10 columns and 12 rows.Each row in the first column represents a threshold value, while the rows of the other columns represent the parameter values.

VII. Conclusion

It can therefore be concluded that the facial recognition system works well with a possible company. The results obtained with the help of the CORDOBA data set are perfect.The results obtained with the help of the CORDOBA Dataset are perfect. Analyzing both the Face Detection phase (with the HOG-SVM algorithm) where the system errs in the 2% of cases and the Face Representation phase (ResNet-34) with which the system never fails an acknowledgment. The program has only one flaw from the point of view of execution time, because regarding Detection and Recognition, the algorithm in full takes about a second.

References

[1]. W. Zhao, R. chellappa e P. Phillips, «ACM Computing Surveys (CSUR), » Face recognition: A literature survey, December 2003.
[2]. A. Suman, «Automated face recognition: Applications within law enforcement, » Market and technology review, NPIA, 2006.
[3]. S. K. A. T. K. T. Talele, «Efficient Face Detection using Adaboost,» IJCA Proc on International Conference in Computational Intelligence, 2012.
[4]. T. Mita, T. Kaneko e O. Hori, «Joint Haar-like Features for Face Detection,» Proceedings of the Tenth IEEE International Conference on Computer Vision, 2005.
[5]. T. Ahonen, A. Hadid e M. Peitikainen, «Face recognition with local binary patterns,» In Proc. of European Conference of Computer Vision, 2004.
[6]. I. Kukenys e B. McCane, «Support Vector Machines for Human Face Detection,» Proceedings of the New Zealand Computer Science Research Student Conference, 2008.
[7]. M. M. Abdelwahab, S. A. Yousry e I. Aly, «Efficient WebBased Facial Recognition System Employing 2DHOG,» arXiv:1202.2449v1.
[8]. M. A. Pentland e A. Turk, «Face recognition using eigenfaces,» Proceedings of the IEEE, pp. 586-591, 1991.
[9]. J. Lu, K. N. Plataniotis e A. N. Venetsanopoulos, «Face recognition using LDA-based algorithms,» IEEE Neural Networks Transaction, 2003.
[10]. L. Wiskott, M. Fellous, N. Krger e C. Malsburg, «Face recognition by elastic bunch graph matching,» IEEE Trans, p. 775–779, 1997.
[11]. López e Ruiz, «Local Binary Patterns applied to Face Detection and Recognition,» Signal Theory & Communication Department, 2010.
[12]. G. Yang e T. Huang, «Human Face Detection in Complex Backgroun,» Pattern Recognition, vol. 27, pp. 53-63, 1994.
[13]. K. Yow e R. Cipolla, «Feature-based human face detection,» Image and Vision Computing, vol. 15, p. 713 – 735, 1997.
[14]. A. Yuille, P. Hallinan e D. Cohen, «Feature extraction from faces using deformable templates,» International Journal of Computer Vision, vol. 8, p. 99–111, 1992.
[15]. R. Ranjan, A. Bansal, J. Zheng, H. Xu, J. Gleason, B. Lu, A. Nanduri, J.-C. Chen, C. D. Castillo e R. Chellappa, «A Fast and Accurate System for Face Detection, Identification, and Verification,» JOURNAL OF LATEX CLASS FILES, vol. 14, 2015.
[16]. K. He, X. Zhang, S. Ren e J. Sun, «Deep residual learning for image recognition,» IEEE Conference on Computer Vision and Pattern Recognition (CVPR), p. 770–778, 2016.
[17]. C. Szegedy, S. Ioffe, V. Vanhoucke e A. A. Alemi, «Inception-v4, inception-resnet and the impact of residual connections on learning,» AAAI, vol. 4, p. 12, 2017.
[18]. Omoyiola e B. Olushola, «Overview of Biometric and Facial Recognition Techniques,»BayoOlushola, vol. 20, p. 5, 2018.
[19]. F. Ahmad, A. Najam e Z. Ahmed, «Image-based Face Detection and Recognition: "State of the Art",»arXiv, CC BY-NC-ND 4.0, 2013.

Giacomo Abbattista, etal. "CORDOBA System: Physical Access Management Control System with Face Detection and Face Recognition." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22.1 (2020), pp. 42-48.