INCREASING LOG-ACCESS SECURITY SYSTEM BASED ON FACE RECOGNITION

AHMED SOLYMAN
Egyptian Atomic Energy Authority (EAEA)
Cairo, P.O. 11787, Egypt
Email: ahmedesolyman@gmail.com

MAGDY ROMAN
Mechanical Power Engineering Department- Faculty of Engineering, Helwan University
Cairo, P.C. 11718 Egypt

H. I. SALEH
Egyptian Atomic Energy Authority (EAEA)
Cairo, P.O. 11787, Egypt

A. Uzhinskiy
Joint Institute for Nuclear Research (JINR), 6 Joliot-Curie, Dubna
Moscow region, 141980, Russia

Abstract

Today's nuclear institutions are facing major security issues; consequently, therefore, they need several specially trained personnel to attain the desired security. These personnel may make human mistakes that might affect the level of security. The human face plays an important role in social interaction, identifying people. Using the human face as a key to security, face recognition technology has received considerable attention, very popular and it is used more widely because it does not require any form of physical contact between the users and the device. This system is composed of two parts: the hardware part and the software part. The hardware part consists of a camera and a motorized microcontroller system, while the software part consists of face-detection and face-recognition algorithms depends on deep learning neural networks. A special database of colleagues was built consisting of about twenty images each. Different neural network architectures were tried on these data and selected the best one. The architecture and basic principles of the platform and networks are described and compared with other well-known solutions. A camera scans the person's face and matches it to a database for verification. In this research, we propose an algorithm to detect and recognize the face of the person who wants to enter the secured area and verify if he is allowed. The access door will be opened if the user is recognized and an alarm goes off if the user is not recognized. We present an access control entering system to a must highly secured environments like nuclear/radiation environments.

Keywords: Nuclear Security; face recognition; Siamese networks, convolutional neural networks, deep learning

1- INTRODUCTION

Nuclear power should be safe and used solely for peaceful purposes. Over several decades, the international community has established political and legal mechanisms to stem the spread of nuclear weapons. These mechanisms include the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), regional nuclear-weapon-free-zone treaties, export control arrangements, nuclear security measures and the safeguards system of the IAEA [1].

Nuclear security is a state responsibility and establishing an effective national nuclear security infrastructure is a key prerequisite for any country wishing to embark on a nuclear power program. The objective of a country's nuclear security regime is to protect persons, property, society and the environment from the harmful consequences of a nuclear security event (that has potential implications for nuclear security that must be addressed). To achieve the secured facilities objective, countries should establish, maintain and sustain an effective and appropriate nuclear security regime to detect, prevent and respond to such nuclear security events.

The access control system is a very important tool to control access of people or personnel to a facility. It is used primarily to put in place a self-managed (non-human intervention) system to isolate a secure area versus a non-secure or public area. As compared with other biometrics systems, face recognition (FR) has good advantages because of its non-contact process. Face images can be captured from a distance without any direct contact identified from a person, and the identification does not require interacting with the person. We present in this paper, a biometric access control device, which is based on the identification of worker's faces using a camera in order to increase security.

Real-time face recognition is considered part of the field of biometrics. Biometrics is the ability of a computer to recognize a human through facial characteristics. Today, biometrics is one of the fastest-growing fields in advanced technology. Predictions indicate a biometrics development in the next century, to authenticate identities and avoid and unauthorized access to networks and facilities.

A facial recognition device takes an image or a video of a human face and compares it to other image faces in a prepared database. The structure, shape, and proportions of the faces are compared during the face recognition steps. In addition, the distance between the eyes, nose, mouth, and jaw, upper outlines of the eye sockets, the sides of the mouth, location of the nose and eyes, and the area surrounding the check bones are also compared [2].

When using a facial recognition program, several pictures of the person must be taken at different angles and with different facial expressions. At the time of verification and identification, the subject stands in front of the camera for a few seconds, and then the image is compared to those that have been previously recorded. The advantages of facial recognition are that it is not intrusive, can be done from a faraway distance even without the person being aware that he/she is being scanned [2]. Such thing is needed in banks or government offices for example, and this is what makes facial recognition systems better than other biometric techniques in that they can be used for surveillance purposes like searching for wanted criminals, suspected terrorists, or missing children.

Face recognition devices are most beneficial to use for facial authentication than for identification purposes, because it is easy to alter someone’s face, and because the person can disguise using a mask. In order to improve verification and identification results dramatically, facial recognition is preferred to be combined with another biometric method.

2- EXISTING SOLUTIONS

Face Recognition has gained a lot of interest from researchers and it has become one of the most popular areas of research in computer vision and biometrics surveyed [3]. PCA was introduced in 1901 [4] and later in 1965 was proposed for pattern recognition [5]. After a span of thirty four years, Freeman and Tenenbaum proposed a bilinear model with a general framework [6]. It has also been widely considered as a successful application of image processing. Other than FR, there are multiple methods of biometric identification, for example, fingerprints and iris scans as illustrated in Table1 [7].

Table 1. Face recognition applications (marques, 2010)

Domain	Application
Biometric	– Person identification – Automated identity (border control)
Information Security	– Access security – Data privacy
Access Management	– Access authentication – Audit trails – Permission grant
Law Enforcement	– Video surveillance – Suspect identify – Simulated aging
Personal Security	– Home surveillance – Expression detection
Entertainment and Leisure	– Video game – Photo camera

It is widely believed that FR is easier to use and secure as opposed to other forms of identification. As such, fingerprint has some limitations, as it is more difficult to retrieve due to fits orientation. Thorat [8] has identified another weakness in FR which includes many systems are less effective if there are significant differences in facial expressions. Other conditions where FR does not work well include poor lighting, sunglasses, long hair or partially covered face, and low quality image acquisition.

Regardless of the problems and limitations, many researches on FR are still being carried out such as computer vision, optics, pattern recognition, neural networks, machine learning, psychology and so forth. In fact, more techniques are being invented each year such as 3D FR or recognition from video. To overcome such issues mentioned earlier, a Principal Factor Scrutiny method was proposed as an efficient method for face recognition [9].

A facial recognition device enables to view an image or a video of a person and later compares with one in the database's gallery by extracting features from an image of the person's face. Face detection is the first stage in the recognition process where all faces are distinguished from non-faces. It is easy for human being to recognize faces even with different appearances such as different hairstyle, with and without glasses, contact lenses among others.

FR is the second stage after face detection has been done. One way to do this is by feature extractions. There are two approaches for feature extraction; local and global. For local feature, it extracts eyes, nose and mouth information. The coordinates of a set of features from the photographs are extracted and then used by the computer for recognition. For global feature, it extracts features from the whole image that is known as the holistic method. Turk and Pentland [10] discovered the residual error could be used to detect images of faces using eigenfaces. Koch, G., et al. [14] presents Siamese neural networks for one-shot image recognition, that we can use in this research.

3- APPROACHES FOR FACE RECOGNITION

There are many difficulties related to human facial recognition. The fact that human faces are all relatively similar, yet produce varying facial expressions makes it more difficult to generalize an algorithm. The face is arguably a person's most unique physical characteristic except in the case of identical twins. Each face has certain distinguishable facial features. These are the peaks and the valleys that make up the different facial features. Lighting conditions and the angle from which the facial image is taken are other factors to consider. Taking all this into account, it is important to note that humans themselves can distinguish a multitude of different faces quickly and with high accuracy [11]. The facial recognition software is based on the ability to first detect then recognizes faces, which are a technological feat in itself, and then measure the different features of each recognized face [12].

There are many applications that this algorithm could be used for, such as surveillance and security systems. Face recognition is a widespread use technology for Access Control. The task is stated as follows. There is only a group of authorized people, which the recognition system must accept. All the other people are unauthorized or 'alien' and should be rejected. Security identity, whether in the physical or virtual world, has always been a business-critical issue for the world's leading organizations. Whether access to the property, to valuable IP on corporate networks or simply proving your identity-adequate and robust security is essential [12, 13, 14].

Three main tasks of face recognition system may be named as: "data control", "access control", and "database retrieval system". The term "data control" means the verification of a human, by comparison, human actual camera image with a stored photo. Access control is the most scrupulous task in the field. Such systems compare the portrait of a tested person with photos of people who have access permissions. The last arises when it is necessary to determine the stored defined name and other information about a person just based on a person one casual photo. Because of great difference between the tasks, there is not a universal approach or algorithm for face recognition.

4- PROPOSED SOLUTION

The proposed solution is a real-time face recognition system that reads a video from a camera connected to the computer running the software, detects any face present in front of the camera, and then checks if this face is exist in a set of face images in a database using face recognition technique. The proposed algorithm consists of two parts. The software part involves deep-learning preparing the dataset, trainee cascades, face detection, and face recognition. The hardware part involves all hardware components like a camera, Ultrasonic sensor, and Microcontroller.

4.1 Model and Image Database

The most popular way to deal with image classification problems in a vast majority of domains is to use a deep neural network trained on a big dataset with further fine-tuning of the chosen deep classifier on the prepared dataset. The proposed comparative study of transfer learning models was made, which are available in open access and found out that the ResNet50 architecture [14] reached 99.79% classification accuracy on a test subset of YouTube face dataset but was stuck on our self-collected dataset with unsatisfactory 75%. We investigated the problem and discovered that it referred to the type of images used. Their photos were collected and processed under special controlled conditions, so they are rather synthetic and differ from real-life images. It gave us the idea of creating our own database and tests them in reality. At the very beginning, our database had 6 classes of colleagues' faces (Ahmed (Egypt), Dina (Egypt), Delfina (Argentina), Mahmoud Farid (Egypt), Faisal (Egypt) and Diu (Vietnam)). The input face image occupies (p x q) dimensional vector space. For the prepared dataset, it contains 6-classes that was about 115 images total, each image with (256 x 256) pixels has 65536-dimensional image space, see Fig.1. The only way to train a deep neural network on a small dataset is one-shot learning, in particular, Siamese networks [15]. The Siamese network consists of twin networks joined by the similarity layer with the energy function at the top. Weights of twins are tied (the same), thus, the result is invariant and guarantees that very similar images cannot be in very different locations in the feature space. The similarity layer determines some distance metric between so-called embeddings, i.e. high-level feature representations of the input pair of images. Training on pairs is more beneficial since it produces quadratically more possible pairs of images to train the model on, making it hard to overfit. From the trained one-shot model, twin is extracted for further use as a feature extractor. The role of the classifier takes the k-nearest neighbors algorithm, which operates on the feature vectors -outputs of the trained twin. Cosine similarity was applied for the distance metric. The parameter K was set to 1 to be equivalent to the one-shot learning task. The classification accuracy of the model was measured on a test subset of face images and reached 98.8% using all 6 classes [16].

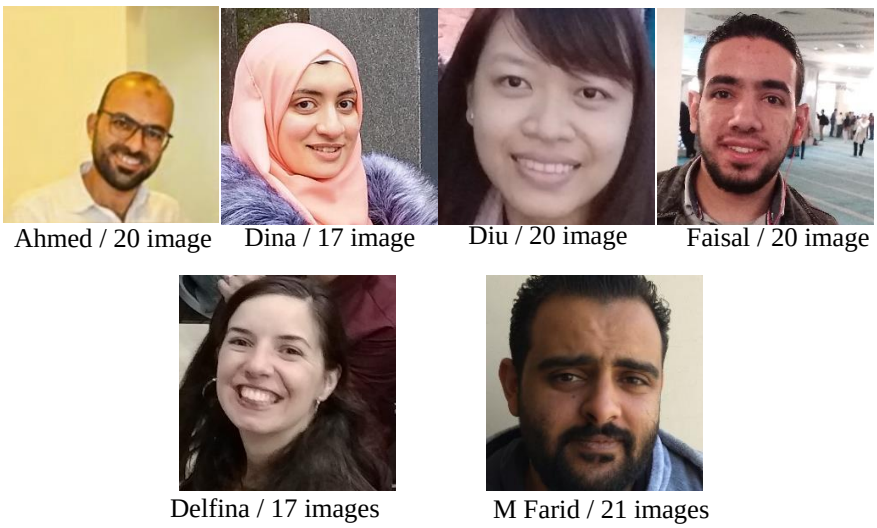


Fig. 1. Colleagues' images of the prepared dataset.

To improve the test classification accuracy we made a special comparative study of different types of estimators including logistic regression, support vector machines with cosine similarity as a kernel, decision tree, random forest, gradient boosting and a simple single-layer perceptron with one input and one output layer ending with softmax activation. The single-layer perceptron being trained for 100 epochs with the Adam optimizer allows us to obtain the classification accuracy equal to 99.71% on a test subset of images. The best architecture we created is presented in Fig. 2.

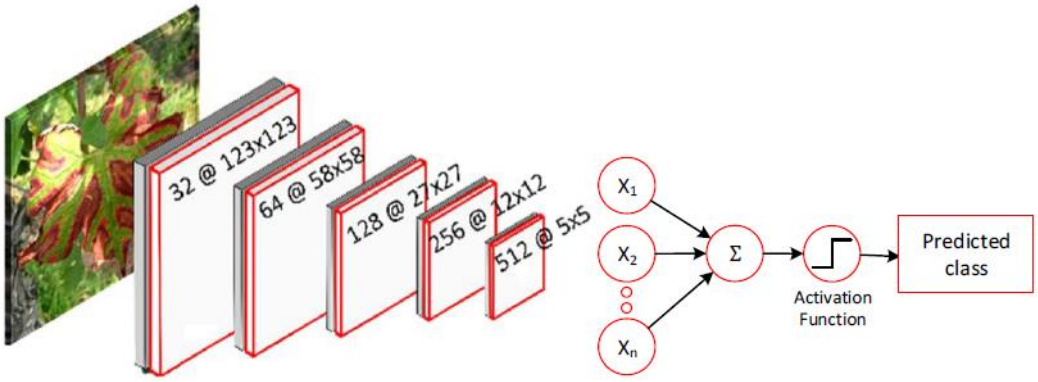


FIG. 2. Best NNA architecture: one of two Siamese twins and single-layer perceptron

4.2 Software Design

Figure 3 shows the flowchart of the proposed face recognition system. First, it reads a signal from the ultrasonic sensor to detect the human presence, which could be set to check every second (configurable). If the human presence is detected, then the camera will capture an image containing the face of a human. The face detection part will localize and segment the face region only. The face image is then fed into the face recognition routine. If the recognized face is detected, the system will unlock the door by turning off the magnetic lock. After 30 seconds (configurable), the system will lock again the door by turning on the magnetic lock. The system will then start from the beginning.

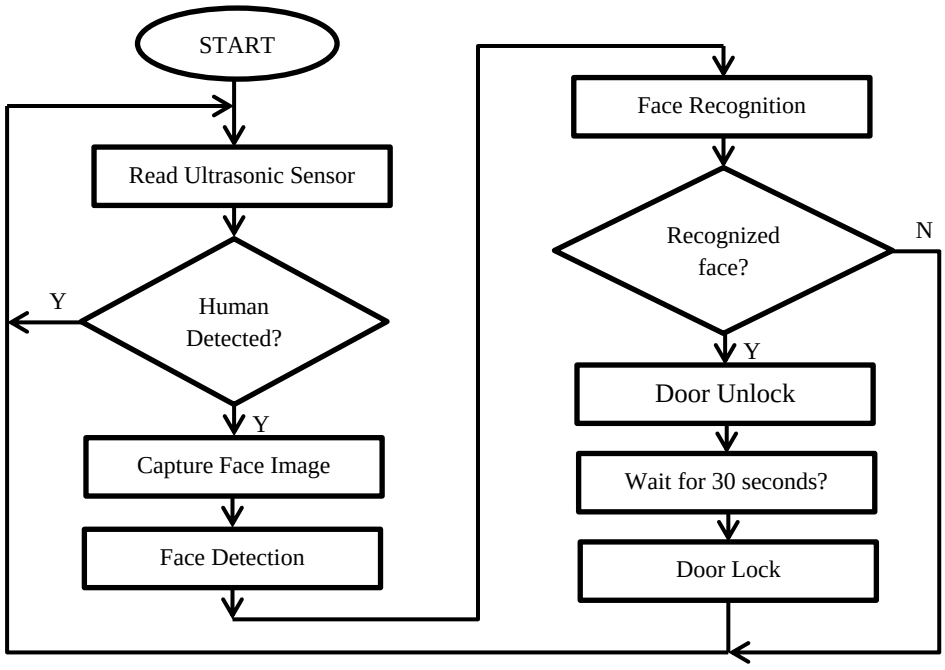


FIG. 3. Flowchart of Face Recognition Security System

4.3 Hardware Design

Figure 4 shows the proposed block diagram of the face recognition system using Raspberry Pi as a microcontroller which connected to the camera module. Raspberry Pi has the same processing capability as a single-core processor with built-in graphics which can support up to 1080p video standard using its High Definition Media Input (HDMI) port. The ultrasonic sensor is used to detect human presence. The relay circuit is connected to Raspberry Pi and provides an interface to the high voltage magnetic lock. The status could be shown using LED indicators and/or further send SMS using the GSM module, or email using an internet connection. Finally, the overall power required is less than 220W, so that a compact power supply can be used.

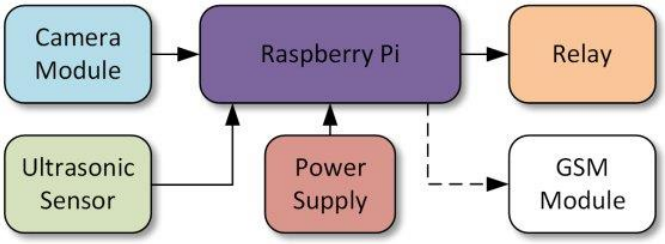


FIG. 4. Block Diagram of Proposed Hardware.

5- IMPLEMENTATION

Figure 5 shows the complete prototype of the face recognition security system. The box contains the Raspberry Pi, ultrasonic sensor, reset button, LEDs and the power input and output. The prototype will be placed beside a door and connected to a magnetic lock as shown in FIG. 6 which is turned off/unlock when the authorized user accesses the system. If unauthorized personnel try to access the door will stay locked and the user image will be stored in the memory. The power supply will be taken from a wall plug and these are the only input and output from the box.

On the software part, the Python and OpenCV library were installed for the algorithm implementation. We build a training Python model to train the faces in order to continue the recognition process. The training data should be loaded into the script. This code will continuously capture images into the training data folder.

The training data given will produce an output named “feature_extractor.h5” file which contains the positive data processed into it. This process can also be done using Google's GPU to shorten the training time. Finally, ports are initialized using the terminal in root mode to access the GPIO pins. The initial set up was done using a servo but this set up can be replaced with a magnetic lock or solenoid lock by simply changing the Pulse Width Modulation (PWM) pin to any other GPIO pins and initialize the pin in the script. To run the code, the terminal window on the Raspberry Pi is opened and the python code is executed. When the red colored light is turned on the system is ready to execute face recognition.

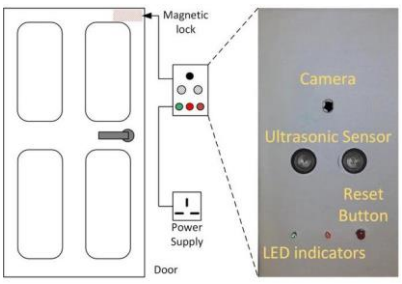
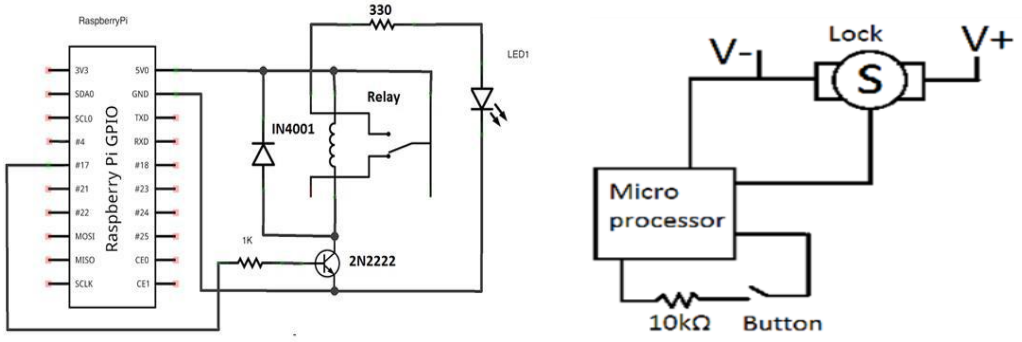


FIG. 5. Complete Prototype of Face Recognition Security System.



(a) (b)

FIG. 6. Circuit diagram of (a) Relay, (b) Magnetic Lock.

6- RESULTS AND CONCLUSION

The database as shown contains a collection of faces of colleagues (training set) from different places where the system is built to recognize. The training database contains 115 images. For testing, 15 images of 6 known and 3 unknown colleagues were used. To test the recognition performances in real environments, test image of the employees are taken using the webcam.

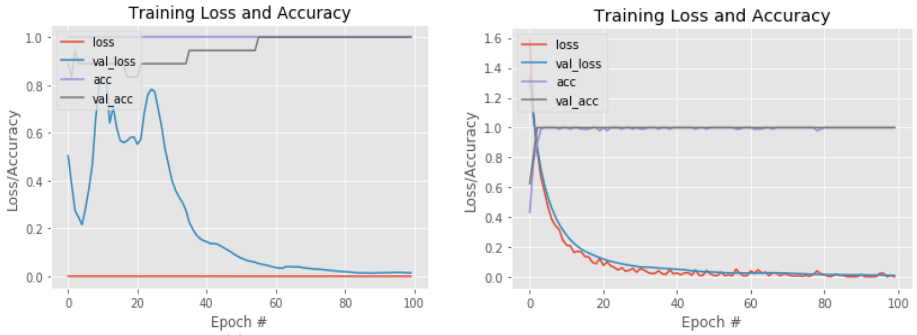
When training Siamese, we have tried many settings and hyper parameters for the model, until finally we settled on the most stable settings:

1- For loss function, we have chosen a contrastive cosine function.

2- For dropout, which is a regularization technique to avoid severe overfitting, we used 0.2

These settings have resulted with a training accuracy of 99.91% and a validation accuracy of 99.9%

As you can see in the graph, (Fig. 7a), the validation accuracy is following the training accuracy with a slack, and it can be also realized in the loss curves.



(a) (b)

FIG. 7. Training loss and accuracy after (a) feature extraction (Siamese network), (b) transfer learning

To visualize the effectiveness of our feature extractor, we reduced the feature space into two dimensions using t-SNE (t-distributed Stochastic Neighbor Embedding) method. As can be seen (Fig. 8), faces are grouped into clusters, and each group almost represent a particular one.

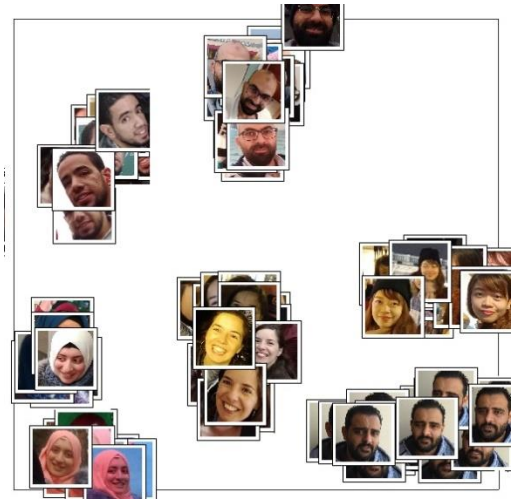


FIG. 8. Dataset are separated into clusters using t-SNE.

Afterwards, we integrated our trained feature extractor with additional layers that will be trained to make multiclass classification. For the additional layers, we used rectified linear activation function (ReLU) for the inner layers and softmax for the last layer to generate probability distribution. For dropout, we used 0.2 also. We achieved a training accuracy of 100% and validation accuracy of 99.9%, see Fig. 7b.

The confusion matrix shows the distribution of the classifications on the validation data. This matrix shows how many Predicted class objects were recognized as True class objects. As you can see in Fig.9, there is a high concentration over the diagonal, which means good accuracy.

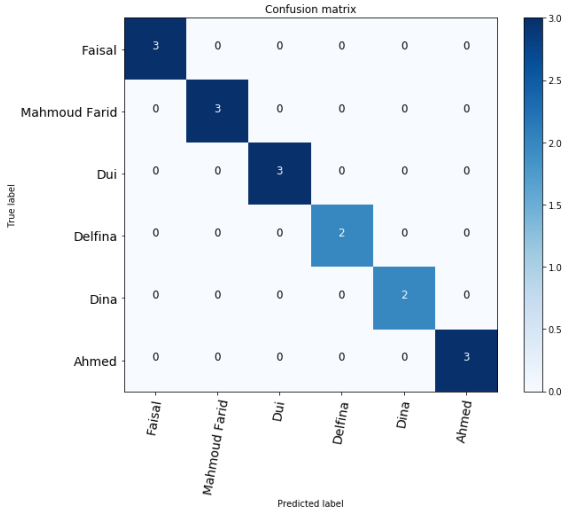


FIG. 9. Metrics of the model using confusion matrix

The model is finally tested on real images different from those included in the dataset. And we found good results, see Fig. 10.

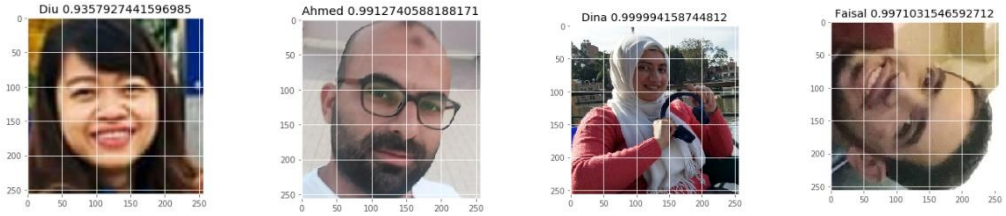


FIG. 10. The FR algorithm results for random samples of the testedface images.

This paper has presented a face recognition security system. Python and OpenCV were used to implement the feature extraction and classifier, in which we used Siamese neural network. The prototype design for real-world implementation has been elaborated, in which the output of the face recognition algorithm will lock or unlock the magnetic lock placed at the door using a relay circuit. The recognition rate was found to be about 99.8% when tested with the dataset images. This proposed system could be connected using the Internet to the smart system for the added security capability. Further research includes optimization of hierarchical image processing, use different features extraction and classifier, or use parallel Raspberry Pi clusters to speed up the computation. Finally, for future work, we will use a multi-modal system using face recognition and fingerprint together to reach to higher security environments.

REFERENCES

[1] BISHOP, Julie, et al. Nuclear security. Australian Year Book of International Law, 2018, 35: 504.

[2] FindBiometrics, Faceial recognition, [Online], Available at: http://findbiometrics.com/solutions/facial-recognition/.

[11] K. Pearson, “On lines and planes of closed fit to systems of points in space,” Philosophical Magazine, vol. 2(6), pp. 559-572, 1901.

[12] W. Chao, R. Chellapa, P.J Phillips and A. Rosenfeld, “Face recognition: A literature survey,” ACM Computing Surveys, vol. 35(4), pp. 399-458, 2003.

[5] S. Watanabe, “Karhunen-Loeve expansion and factor analysis theoretical remarks and applications,” Proc. Of the 4th Prague conference on Information Theory, 1965.

[6] W.T. Freeman and J.B. Tenenbaum, “Learning bilinear models for twofactor problems in vision,” Proc. Of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,”, pp. 554-560, 1997.

[7] I. Marques, “Face Recognition Algorithms,” http://www.ehu.es/ccwintco/uploads/e/eb/PFC-IonMarques.pdf, 2010

[8] S.B. Thorat, “Facial recognition technology: An analysis with scope in India,” Journal of Computer Science and Information Security, vol. 8(1), 2010.

[9] C.V. Arulkumar, G. Selvayinayagam and J. Vasuki, “Enhancement in face recognition using PFS using Matlab,” International Journal of Computer Science & Management Research, vol. 1(1), pp. 282-288, 2012.

[10] M. Turk and A. Pentland, “”Eigenfaces for recognition,” Journal of Cognitive Neuroscience, vol. 3(1), pp. 71-86, 1991.

[11] Steve Mann, “Intelligent Image Processing”, Wiley-Interscience 2002.

[12] Walter G.Kropatsh, “Digital Image Analysis”, Springer 2002.

[13] JALLED, Fares. Face Recognition Machine Vision System Using Eigenfaces. arXiv preprint arXiv:1705.02782, 2017.

[14] Kalita J, Balas VE, Borah S, Pradhan R, editors. Recent Developments in Machine Learning and Data Analytics: IC3 2018. Springer; 2018.

[15] Koch, G., Zemel, R., Salakhutdinov, R. Siamese neural networks for one-shot image recognition. In: ICML Deep Learning Workshop, Vol. 2, 2015

[16] Goncharov, P., Ososkov, G., Nechaevskiy, et al., I. Disease Detection on the Plant Leaves by Deep Learning. International Conference on Neuroinformatics. Springer, Cham, pp. 151-159, 2018