Advanced Face Recognition System Using dlib

Sahaya Sakila
Department of Computer Science and Engineering
SRM Institute of Scince and Technology
Chennai, Tamil Nadu

Sanyog Acharyya
Department of Computer Science and Engineering
SRM Institute of Scince and Technology
Chennai, Tamil Nadu

***Abstract*— This project designs face recognition system for smart home/office security applications. The design is implemented using webcam and programmed using dlib and openCV. The connection between cam and computer can be both wired and wireless. The approach we are going to use for face recognition is fairly straight forward. The key here is to urge a deep neural network to supply a bunch of numbers that describe a face (known as face encodings). When you pass in two different images of the same person, the network should return similar outputs (i.e.closer numbers) for each pictures, whereas when you pass in images of two different people, the network should return very different outputs for the two images. This means that the neural network must be trained to mechanically establish totally different options of faces and calculate numbers supported that. The output of the neural network may be thought of as associate degree symbol for a selected person's face, if you pass in different images of the same person, the output of the neural network are terribly similar/close, whereas if you pass in pictures of a distinct person, the output are terribly totally different. The additional feature here is that we are going to run this algorithm on database too, to make it more efficient than ever**

Keywords—openCV, dlib, Deep Learning, Neural network

I. INTRODUCTION (*HEADING 1*)

""Face recognition" redirects here. For the human cognitive process, see Face perception. For other uses, see Facial recognition. Swiss European surveillance: face recognition and vehicle make, model, color and license plate reader Close-up of the infrared illuminator. The light is invisible to the human eye, but creates a day-like environment for the surveillance cameras. A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analysing patterns based on the person's facial textures and shape. While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Although the accuracy of facial recognition system as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless and non-invasive process. Recently, it has also become popular as a commercial identification and marketing tool. Other applications include advanced human-computer interaction, video surveillance, automatic indexing of images, and video database, among others.

Dlib may be a general purpose cross-platform software system library written within the artificial language C++.Its style is heavily influenced by concepts from style by contract and component-based software system engineering. Thus it is, 1st and foremost, a collection of freelance software system parts. It is ASCII text file software system free below a lift software system License. Since development began in 2002, Dlib has fully grown to incorporate a large style of tools. As of 2016, it contains software system parts for managing networking, threads, graphical user interfaces, knowledge structures, algebra, machine learning, image process, data processing, XML and text parsing, numerical optimization, Bayesian networks, and many other tasks.In recent years, a lot of of the event has been centered on making a broad set of applied mathematics machine learning tools and in 2009 Dlib was revealed within the Journal of Machine Learning analysis. Since then it's been employed in a large vary of domains..

Deep learning (also known as deep structured learning or hierarchical learning) is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, semi-supervised or unsupervised. Deep learning architectures like deep neural networks, deep belief networks and perennial neural networks are applied to fields together with pc vision, speech recognition, tongue process, audio recognition, social network filtering, MT, bioinformatics, drug style, medical image analysis, material review and parlor game programs, wherever they need created results such as and in some cases superior to human experts. Deep learning models ar mistily impressed by information science and communication patterns in biological nervous systems nonetheless have numerous variations from the structural and useful properties of biological brains (especially human brains), that create them incompatible with neurobiology evidences.

II. LITERATURE SURVEY

In [1], The basic idea here is to to create a secure home environment by making the way to access a home by face detection instead of a key. It makes use of the traditional eigenfaces algorithm. When the person comes to the front gate the camera installed captures the image and feeds to the algorithm which then converts it into greyscale and then into a matrix and then compares the Euclidian distance between this image and dataset images and if that is less than threshold then person is authorized to access home else not. This analysis styles face detection and recognition systems for good home security application. The design is enforced victimization MyRIO 1900 and programmed victimization LabVIEW. The connection between myRIO and computer is Wi-Fi network. The image of an individual is

nonheritable via digital camera connected to MyRIO victimization USB cable. The face detection system is constructed supported the model matching, while the face recognition is based on the principle component analysis. The testing is finished to look at the performance of the face detection in varied modification of distance, light intensity, light position angles, person's accessories and shirt colour. The face detection module has good performance in some conditions as distance between the person and the camera is less than 240 cm, person doesn't use accessories that cover part of face, person doesn't use shirt with colour similar to skin colour, and background colour is difference from skin colour. While the face recognition system has 80% of accuracy when it is tested using real-time image. The combination with positive identification is required so as to extend the protection level because it is applied in real good home security systems.

In [2], The idea here is to achieve effective face recognition using Deep Learning - Linear Discriminant Regression Classification (DL-LDRC) instead of traditional LRC. It is a recently developed method with enhanced accuracy as compared to LRC model. It is run on two, four and six train ORL and YALE datasets and gives better results than LRC. The proposed DL-LRDC method produce better identification and differentiation of biometric facial images than the other algorithms developed earlier. The working performance of the proposed DL-LRDC is compared with the existing systems, which is necessary to provide conclusion that proposed system is better than all the other systems. Linear Regression Classification (LRC) is the earlier method developed to perform classification of images based on their existence of feature vectors, which calculates the distance between the pixels and reduce the error variations in it. An experimental verification is done to reveal the performance of our DL-LRDC, in which it is compared with the other earlier algorithm based on learning, achieved good accuracy. This paper presents the technique of learning strategy in the development of face recognition system using LDRC algorithm. The proposed DL method attempts to learn and analyse all the samples present in the system and also the new incoming face inputs. In addition, it holds the track of information from the face features and makes the LDRC method to perform classification of face in an efficient manner. The experiments are done on ORL and YALE face databases and the resultant values are compared with the early developed LRC method. This study of graph shows that the proposed DLLDRC has more accuracy in all two train, four train, six train and eight train ORL and YALE databases. Thus, the efficiency of traditional LDRC is improved and motivated by the proposed DL method.

In [3], The idea here is to improve the efficiency of a crime investigation process by using a face recognition system to identify the person in the sketch made by artist as depicted by the eye-witness. The system is using deep convolutional network to learn the relationship between photos and sketches and make use of 3-D Morphable model to generate new images based on sketch. It was found that when multiple sketches are fed as dataset the performance is better. This system is one of the few that uses deep learning in hand drawn sketches. Numerous strategies that mechanically establish subjects represented in sketches as delineated by eyewitnesses are enforced, but their performance often degrades when using real-world forensic sketches and extended galleries that mimic law enforcement mug-shot galleries.Moreover, very little work has been done to use deep learning for face photo-sketch recognition despite its success in various application domains together with ancient face recognition robustly train massive networks. This letter aims to tackle these problems with the subsequent contributions: 1) a progressive model pre-trained for face photograph recognition is tuned for face photo-sketch recognition by applying transfer learning, 2) a three-dimensional morphable model is used to synthesise new images and artificially expand the training data, allowing the network to prevent over-fitting and learn better features, 3) multiple synthetic sketches are also used in the testing stage to improve performance, and 4) fusion of the proposed method with a state-of-the-art algorithm is shown to further boost performance. An extensive evaluation of several popular and state-of-the-art algorithms is also performed using publicly available datasets, thereby serving as a benchmark for future algorithms. Compared to a leading method, the proposed framework is shown to reduce the error rate by 80.7% for viewed sketches and lowers the mean retrieval rank by 32.5% for real-world forensic sketches.

In [4], The idea here is to increase security while doing mobile payment by doing the user authentication through face recognition. The idea here is to increase the efficiency of the algorithm by making it work under varied light intensities as the user is on mobile so it can be in a very open space or a very confined space also. The system makes use of Deep Reinforcement Learning approach using python2.7 and Ubuntu on an Intel i7-6700 processor. The drawback still stays that the less the intensity of light, the less accurate the results will be. Numerous crime-related security concerns exist in e-commerce transactions recently. User authentication for mobile payment has numerous approaches including face recognition, iris scan, and fingerprint scan to identify user's true identity by comparing the biometric features of users with patterns in the signature database. Existing studies on the face recognition problem focus mainly on the static analysis to determine the face recognition precision by examining the facial features of images with different facial expressions for users rather than the dynamic aspects where images were often vague affected by lighting changes with different poses. Because the lighting, facial expressions, and facial details varied in the face recognition process. Consequently, it limits the effectiveness of scheme with which to determine the true identity. Accordingly, this study focused on a face recognition process under the situation of vague facial features using deep reinforcement learning (DRL) approach with convolutional neuron networks (CNNs) thru facial feature extraction, transformation, and comparison to determine the user identity for mobile payment. Specifically, the proposed authentication scheme uses back propagation algorithm to effectively improve the accuracy of face recognition using feed-forward network architecture for CNNs. Overall, the proposed scheme provided a higher precision of face recognition (100% at gamma correction located in [0.5, 1.6]) compared with the average precision for face image (approximately 99.5% at normal lighting =1) of the existing CNN schemes with ImageNet 2012

Challenge training data set.

In [5], Here deep convolutional network has been implemented using MATLAB. Then two different synthetic image samples are generated from training set by applying noise. One with less distortion is termed Poisson Noise while the one with higher distortion is termed Gaussian noise. Then these synthetic images are added to previous training set to create augmented training data for CNN. Learning rate of CNN is kept to be 0.001. The major of drawback of this system is that in order to make it work, the batch size and momentum is prefixed. And also the system dropouts are frequent. Deep learning methods, especially convolutional neural networks have achieved significant success within the space of pc vision together with the troublesome face recognition issues. Training of deep models shows exceptional performance with massive datasets, but they are not suitable for learning from few samples. This paper proposes a changed deep learning neural network to find out face illustration from a smaller dataset. The proposed network is composed of a set of elaborately designed CNNs, RELUs and fully connected layers. The training dataset is augmented with synthetically generated samples by applying Gaussian and Poisson noise to each sample of the training set, thus doubling the size of the training set. We through an experiment demonstrate that the increased coaching dataset really improves the generalization power of CNNs. The network is trained victimization the quality AT&T face info. Using the projected approach for restricted coaching knowledge, substantial improvement in recognition rate is achieved. This actually improves the generalization power of CNNs and adds robustness against overfitting to the model. Using the proposed approach for limited training data, 95.21% recognition rate is achieved on the standard AT&T face database for 4 training samples and 99.92% for 5 training samples. This technique can be applied to other face analysis problems in future. The limitation of this approach is that it uses supervised learning with human-annotated data. The deep learning models are often big, so they demand large memory and more computational power which can be fulfilled with the use of GPUs.

III. SYSTEM DESIGN

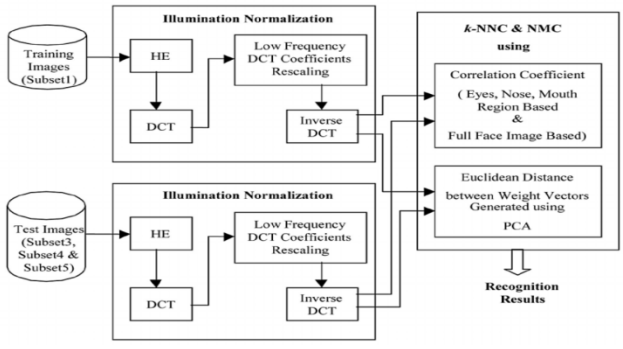

Figure 1. System Architecture

This system is divided in two parts. One is database creation part and other is live time face recognition. For database creation, we have created a simple web form that will be used to upload the image of the people allowed to have access to whatever the security system is for. This form has a background python code written using deep learning library to check whether the uploaded image is compatible with our algorithm or not. It also checks that one single image should not contain more than one person to avoid conflicts. It makes use of get_frontal_face_detector() function of dlib library to detect the faces in image and shape_predictor() of same library to access a shape_predictor_68_face_landmarks.dat a premade data file that contains all the possible human face shapes possible. This file is made available on the web by those whose expertise in the field. Now comes the live time face recognition part. So when the person comes in front of camera, an image of the person is taken cv2.OpenCapture() of OpenCV library. First 30 frames are ignored so as to give time to the person to stay still for a better image. The image captured is made as an image file using .read() function and then temporarily stored in test database using cv2.imwrite(). Now the camera is released using delete(camera) to reduce battery consumption. Now both the images are stored in database, the people who are allowed to have access and the person trying to gain access currently.

The system performs checks as follows. First the allowed people database is accessed and then using for loop face encodings of all the images are created. To get face encodings we have created a function. This function first reads the image using scipy.misc.imread() and then shape of face in that image is taken which is recognised through our premade data file. Now the image is converted into an array using the function np.array (face_recognition _model.compute face_descriptor()) and these arrays of images are referred to as encodings. If, however, there are more than one or no face encodings in one particular image then the system produces an alert and stops. If not, then face encodings are generated for all images in the database.

and live time image can be at max 6% different from each other. General System Architecture is displayed in Figure 1.

IV. RESULTS AND DISCUSSIONS

For testing the mechanism, we are running our web form through xampp server and the database is also managed locally instead of cloud.

So first when we open our web form it will look like this. (Figure 2)

Figure 2. Web form

Now when the image is uploaded, if it is successfully accepted then following alert will be given. (Figure 3)

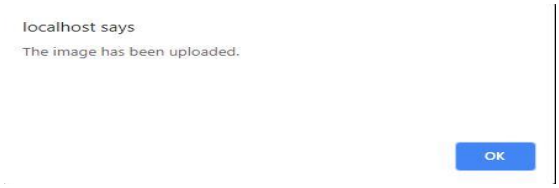

Figure 3. Success

If the image is not accepted, then the following or similar alerts will be shown. (Figure 4)

Figure 4. Fail

Once the database is created, we move onto the demonstration of face recognition part. Since we are doing it locally, we have simply tested the code on Python IDLE. While capturing the image it will display a text letting the person know that the image is being taken now. (Figure 5)

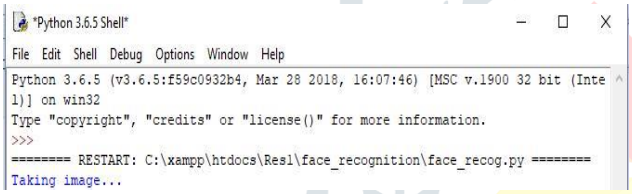

Figure 5. Image being taken

Now if the match is found then the access will be granted and following will appear. (Figure 6)

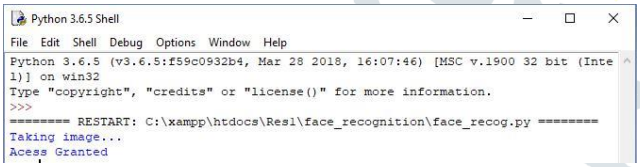

Figure 6. Access Grant

And if the match isn't found then the person is denied access. (Figure 7)

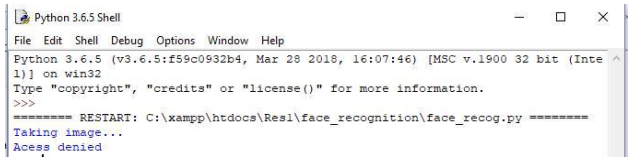

Figure 7. Access Denied

V. CONCLUSION

This system has designed a face recognition system for security purposes. The system performs accurately under normal conditions. In order for system to work properly, the database creation should be done with uttermost care. This is to make sure that all the authorized people are granted access and no outsider has the access.

Few modifications can be done in the system to make it more efficient. What we can do is while taking live time image if suppose there are two people present in the image then instead of showing an alert for that, it checks for both of them individually and grants or denies access accordingly. We can also apply neural regression machine algorithm in the system, then what will happen is that system will observe the pattern and will learn which person comes around which time and at that time instead of comparing with whole database, just compare the encodings with assumed person's encodings and if match is found then great and if isn't then it compares with whole database before displaying final result.

VI. REFERENCES

[1]Dwi Ana Ratna Wati and Dika Abadianto, "Design of Face Detection and Recognition System for Smart Home Security Application" in 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering(ICITISEE).

[2]K. Shailaja and Dr. B. Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification" in 2016 IEEE International Conference on Computational Intelligence and Computing Research.

[3]Christian Galea and Rueben A. Farrugia, "Forensic Face Photo-Sketch Recognition Using a Deep Learning-Based Architecture" in November 2017 IEEE SignalProcessing Letters, Vol. 24, No. 11.

[4]Umme Aiman and Virendra P. Vishwakarma, "Face Recognition using modified Deep Learning Neural Network" in 8th ICCNT 2017, IIT Delhi, India.

[5]Ping Wang, Wen-Hui Lin, Kuo-Ming Chao and Chi-Chun Lo, "A Face- Recognition Approach using Deep Reinforcement Learning Approach for User Authentication" in The Fourteenth IEEE International Conference on e-Business Engineering 2017.

[6]Xi Peng, Nalini Ratha and Sharathchandra Pankanti, "Learning Face Recognition from Limited Training Data using Deep Neural Network" in 2016 23rd International Conference on Pattern Recognition (ICPR), Cancun Center, Cancun, Mexico.