**ABSTRACT**

The face detection system is a controversial topic right now. This technology has been available for some years now and is used over all the places. A system such as this can be used for various purposes such as authenticate the computer using face, can be used for tracking criminals with the help of face and for keeping the attendance of students/employees through face.

At one of the most successful application of images analysis and understanding, face recognition has recently received significant attention, especially during the past few years. Facial recognition technology (FRT) has emerged as an attractive solution to address many contemporary needs for identification and the verification n of identity claims. It brings together the promise of other biometric systems, which attempt to tie identity to individually distinctive features of the body, and the more familiar functionality of visual surveillance systems. This report develops a socio-political analysis that bridges the technical and social scientific literatures on FRT and addresses the unique challenges and concerns that attend its development, evaluation, and specific operational uses, contents, and goals. It highlights the potential and limitations of the technology, noting those task for which it seems ready for deployment, those areas where performance obstacles may be overcome by future-technological developments or sound operating procedures, and still other issues which appear in tractable. The system can then compare scans to records stored in a central or local database or even on a smart card.

**Introduction:**

Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use. In fact, facial recognition technology has received significant attention as it has potential for a wide range of application related to law enforcement as well as other enterprises. There are different facial recognition techniques in use, such as the generalized matching face detection method and the adaptive regional blend matching method. Most facial recognition systems function based on the different nodal points on a human face. The values measured against the variable associated with points of a person’s face help in uniquely identifying or verifying the person. With this technique, applications can use data captured from faces and can accurately and quickly identify target individuals. Facial recognition techniques are quickly evolving with new approaches such as 3-D modeling, helping to overcome issues with existing techniques.

There are many advantages associated with facial recognition. Compared to other biometric techniques, facial recognition is of a non-contact nature. Face images can be captured from a distance and can be analyzed without ever requiring any interaction with the user/person. As a result, no user can successfully imitate another person. Facial recognition can serve as an excellent security measure for time tracking and attendance. Facial recognition is also cheap technology as there is less processing involved, like in other biometric techniques.

There are certain drawbacks associated with facial recognition. Facial recognition can only identify people when the conditions such as lighting are favorable. The application could be less reliable in case of insufficient light or if the face is partially obscured. Another disadvantage is that facial recognition is less effective when facial expressions vary.

**Technology Used:**

**OpenCV and Python:**

OpenCV is the most popular library for computer vision. Originally written in C/C++, it now provides bindings for Python. OpenCV uses machine learning algorithms to search for faces within a picture. Because faces are so complicated, there isn’t one simple test that will tell you if it found a face or not. Instead, there are thousands of small patterns and features that must be matched. The algorithms break the task of identifying the face into thousands of smaller, bite-sized tasks, each of which is easy to solve. These tasks are also called classifiers. For something like a face, you might have 6,000 or more classifiers, all of which must match for a face to be detected (within error limits, of course). But therein lies the problem: for face detection, the algorithm starts at the top left of a picture and moves down across small blocks of data, looking at each block, constantly asking, “Is this a face? … Is this a face? … Is this a face?” Since there are 6,000 or more tests per block, you might have millions of calculations to do, which will grind your computer to a halt.To get around this, OpenCV uses cascades. What’s a cascade? The best answer can be found in the dictionary: a waterfall or series of waterfalls. Like a series of waterfalls, the OpenCV cascade breaks the problem of detecting faces into multiple stages. For each block, it does a very rough and quick test. If that passes, it does a slightly more detailed test, and so on. The algorithm may have 30 to 50 of these stages or cascades, and it will only detect a face if all stages pass.The advantage is that the majority of the picture will return a negative during the first few stages, which means the algorithm won’t waste time testing all 6,000 features on it. Instead of taking hours, face detection can now be done in real time.

**Feasibility Study:**

**Description:**

Face recognition is very important in many applications such as security verification and people identification in cash machines and employee attendance systems. The existing face recognition designs suffer from many environmental problems such as illumination, pose and expression changes. In order to overcome these problems, some research has outlined the necessity for a pre-processing stage in order to make use of valid facial images which are unadulterated with the use of make-up, wigs, facial hair or glasses. The pre-processing stages of illumination normalization and histogram equalization techniques have been developed to enhance or retrieve the input image. However, these techniques do not solve the problems of pose and expression changes. Other research has focused on improving the feature extraction or classification techniques. These methods, however, require the use of much pre-processing of the input image in order to solve the problems associated with illumination, pose and expression changes. Using a door access control system, however, can produce more robust input data for face recognition. The typical door access control system consists of a camera, an illumination source, an electronic door lock and the system control which connects all components using a human-machine control interface. Door access control systems work on controlling the distance between the camera and the person to control the background, and by fixing the lighting refresh rate and the camera angle (pose) and requiring the person of interest to pose for a frontal view with a neutral expression.

**Need and Significance of Face Recognition:**

Positive identification of individuals is a very basic societal requirement. In small tribes and villages, everyone knew and recognized everyone else. You could easily detect a stranger or identify a potential breach of security. In today's larger, more complex society, it isn't that simple. In fact, as more interactions take place electronically, it becomes even more important to have an electronic verification of a person's identity. Until recently, electronic verification took one of two forms: 1- It was based on something the person had in their possession, like a magnetic swipe card or 2- something they knew, like a password. The problem is, these forms of electronic identification aren't very secure, because they can be given away, taken away, or lost and motivated people have found ways to forge or circumvent these credentials. So, the ultimate form of electronic verification of a person's identity is biometrics; using a physical attribute of the person to make a positive identification. There are many robust biometric techniques like fingerprinting which can be used for human authentication then why go for face recognition?

**Uses for Personal Security**

Theft of personal identity and financial information has become an increasingly real threat. From something like wireless identity theft through RFID scanning, meaning that hackers could potentially steal your credit card information without you realizing from a mere 6 feet away from you, to hacked ATM machines, it makes us all a bit more cautious. Facial recognition technology has already been used as a means to protect your identity; there are ATM machines in China that actually scan your facial and iris features to help prevent an unwanted stranger from using your information.

**Uses for Commercial Security**

Businesses may be able to use facial recognition software to identify criminals or previous offenders. This could be great for the headquarters of a commercial entity: if you have a secure parking lot, you could use something like Gatekeeper’s DriverCam to determine who exactly was coming into your parking lot. The high-resolution images produced by the DriverCam could be matched against a database of criminals to immediately flag anyone who shouldn’t be entering your facility. All this done while the vehicle is moving and the windows shut even through heavy tinted glass and sun glare.

**Uses for National Security**

Facial recognition technology has already been used to identify fraudulent passports or visas. This can be a great aid in combatting terrorist threats, which as we’ve mentioned before, is an absolute necessity in the age we live in. Gatekeeper’s DriverCam can work just as well for the government sector in providing necessary additional security benefits all by matching images up with a database of known terrorists.

**Methodology:**

Over the last several years, numerous projection-based biometric algorithms have been developed including principal component analysis and independent component analysis. The main idea of projection-based approach is to reduce the dimensionality of a data set while retaining most of the variation present in the data set. There is an accepted basic design for the biometric recognition system, however, the details of the basic algorithm require a number of design decisions. These design decisions include preprocessing of acquired biometric information, coefficients selected for representation, and similarity measure for comparing these feature vectors. Each of these system design decisions has an impact on the overall performance of the algorithm. Some of these design decisions have been explicitly stated in the literature; for example, the similarity measure for comparing two biometric feature vectors. There are two main categories of research to advance the state of the art in face recognition. The first category is the design of a system that can provide reliable solutions to face recognition problems. In algorithm development, a number of techniques have been proposed for preprocessing and enhancement, detection of face and facial components in a scene, feature extraction algorithms, and classification techniques. Not one of these procedures should be neglected, since each component is critical and performs as a part of the face recognition system. The second category is the development of an assessment methodology based on different scenarios and categories of images. Recently, empirical evaluation techniques have emerged as a serious research field in pattern recognition and computer vision. An empirical evaluation is defined as the assessment methodology for measuring the ability of algorithms to meet requirements for system level implementation. In this paper, we designed a generic modular projection-based face recognition system and performance evaluation methodology to present the importance of system design and assessment methodology. Our face recognition system consists of preprocessing, representation, and recognition modules. Each module consists of a series of basic steps, where the purpose of each step is fixed. However, we systematically vary the algorithm in each step. Based on modular face recognition system model, we evaluate different implementations. Since we use a generic model, we can change the implementation in an orderly manner and assess the impact on performance of each modification. We report identification and verification performance which is critical for person authentication scenario. In identification model, the input to an algorithm is an unknown face, and the algorithm reports back the estimated identity of an unknown face from a database of known individuals. In verification model, the algorithm either accepts or rejects the claimed identity. We report performance results using top rank score for identification and equal error rate for verification. We performed a detailed evaluation of variations in the implementation. By testing on standard galleries and probe sets, the reader can compare the performance of our implementations. In this experiment, we vary the illumination normalization procedure, the number of feature vectors for representation, and the similarity measure.

**Module and Distribution of work:**

**Coding Face Recognition using Python and OpenCV:**

We are going to divide the Face Recognition process in three steps:

1. **Prepare Training Data:**Read training images for each person/subject along with their labels, detect faces from each image and assign each detected face an **integer label** of the person it belongs.
2. **Train Face Recognizer:** Train OpenCV's LBPH recognizer by feeding it the data we prepared in step 1.
3. **Prediction:** Introduce some test images to face recognizer and see if it predicts them correctly.

To detect faces, I will use the code from my previous article on [face detection](https://www.google.com/url?q=https://www.superdatascience.com/opencv-face-detection/&sa=D&ust=1501261897566000&usg=AFQjCNG1pG5B_lxnukQXZj07kCtmRU1ysA).

Before we start the actual coding, we need to install the **Code Dependencies** and import the **Required Modules**:

**Code Dependencies:**

The following dependencies are required to develop project:

1. [OpenCV 3.2.0](http://opencv.org/releases.html)
2. [Python v3.5](https://www.python.org/downloads/)
3. [NumPy](http://www.numpy.org/) that makes computing in Python easy. It contains a powerful implementation of N-dimensional arrays which we will use for feeding data as input to OpenCV functions.

**Required Modules:**

Import the following modules:

* **cv2:** This is the OpenCV module for Python used for face detection and face recognition.
* **os:** We will use this Python module to read our training directories and file names.
* **numpy:** This module converts Python lists to numpy arrays as OpenCV face recognizer needs them for the face recognition process.

**Software and Hardware Requirements:**

Instruments required for the developments of the project are as per the table below:-

|  |  |
| --- | --- |
| Hardware | Type |
| Processor | Intel Core Processor or better performance |
| Primary Memory | 1 GB or more |
| Secondary Memory | 3 GB or more  Not Specified |
| Graphics | 800 MB or more |
| Printer | Not Required |

|  |  |
| --- | --- |
| Software | Type |
| Operating System | Windows and Linux Operating System |

**Fig:** Software and Hardware Requirements for Project

**Bibliography:**

* <https://www.slideshare.net/gsantosh031/face-recognition-ppt>
* <http://www.researchpublish.com/download.php?file=Scope%20of%20Face%20Recognition%20Techniques-1815.pdf&act=book>
* <http://www.cs.uwc.ac.za/~dwarren/Dmitri%20Warren%20De%20Klerk%20-%202653786%20-%20Thesis.pdf>
* <http://hanzratech.in>
* [http://opencv-pythontutorials.readthedocs.io/en/latest/pytutorials/pyobjdetect/py\_ facedetection/py\_face\_detectio n.html](http://opencv-pythontutorials.readthedocs.io/en/latest/pytutorials/pyobjdetect/py_%20facedetection/py_face_detectio%20n.html)
* <https://www.superdatascience.com/opencv-face-recognition/>
* <http://vismod.media.mit.edu/tech-reports/TR-516/node2.html>
* <https://link.springer.com/chapter/10.1007/978-3-540-30548-4_41>
* https://www.techopedia.com/definition/32071/facial-recognition