

# A Model for Face Recognition using OpenCV Framework

**Mr. Ayush Verma**

*Research Scholar*

*Department of Computer Engineering*

*College of Engineering, Bharati Vidyapeeth University, Pune, India*

**Mr. Kunal Tewatia**

*Research Scholar*

*Department of Computer Engineering*

*College of Engineering, Bharati Vidyapeeth University, Pune, India*

## Abstract

Security is the first line of defence for any organization. This research focusses on the importance of security in organizations with emphasis on FACE Biometrics. A system is proposed to recognize faces using the WEBCAM of PC through JAVA programming language and OpenCV framework. When a new employee joins in, his/her image is captured and is stored into a database. When the same employee again attempts to check-in, his/her current image is captured and compared with the earlier image stored in the database. The comparison is done based on the pixel values at every location of the image. If more than 75 percent of the pixels match, the image is considered to be of the same person and he/she can check-in successfully. However, if the percentage similarity is less than 75 percent, the image is considered to be a different one than the one stored in the database and check-in becomes unsuccessful. The percentage similarity criteria has been decided according to the hardware used and may vary from system to system. Overall, this research presents a steady method of biometric security particularly for small-scale organizations.

**Keywords: Biometric Security, Face Recognition, OpenCV framework**

## I. INTRODUCTION

Biometrics refers to metrics which are related to characteristics of human beings. It is used in computer science as a form of identification and access control. Biometric identifiers are then distinctive, measurable characteristics used to describe individuals. Biometric identifiers are often categorized as physiological and behavioral characteristics. Physiological characteristics are related to the shape of the body. Example: - fingerprint, palm veins, face recognition etc. Behavioral characteristics are related to the pattern of behaviour of a person, including typing rhythm, voice etc.

More traditional means of access control include methods such as token-based identification systems, such as an individual's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods.

FACE recognition is a biometric approach that employs automatic methods to verify or recognize the identity of a living person based on his/her physiological characteristics. Because of the prevalent human inherent protectiveness of eyes, some people are reluctant to use eye identification systems. FACE recognition has the benefit of being a passive system to verify personal identity in a natural and friendly way.

FACE recognition is an important research problem spanning numerous fields and disciplines. This is because face recognition, in addition to having numerous practical applications such as bankcard identification, access control, security monitoring, and surveillance system is a fundamental human behaviour that is essential for effective communications and interactions among people.

The rapid development of FACE recognition is due to the following reasons: development of a large number of comparison algorithms, the availability of large databases of facial images, and a method for evaluating the overall performance and efficiency of FACE recognition algorithms.

Many organizations have started using FACE recognition systems as part of their security measure. One of the big benefits of using facial biometric systems is that we don't have to worry about time fraud. Everyone has to go through face scanning biometric devices to check in. Anyone that is not in the system will not be given access.

Any kind of Biometric recognition system is needed by an organization because fraud is increasing day by day in today's modern world and preventive measures need to be taken. Given its simplicity and the advantages FACE recognition brings with it, many organizations have started preferring it.

## II. LITERATURE SURVEY

Security is the first line of defence for any organization. This is the reason why any organization – whether large or small, has one or the other methods of ensuring security in their organization. With the advent of technology, fraud is also increasing and

fraudsters do not leave even a single window of opportunity to harm an organization's assets in some or the other form. This is the reason why organizations have started focussing more and more on security in the last few decades. In today's world, everything is being digitalized and the same should be followed as far as security is concerned. This has been the trend in the last few years and this is the reason why biometric security techniques have increased in importance with passing time. In general, the functionality of biometric devices can be explained in the following three steps: (1) a sensor records an observation. The type of sensor and its observation depend on the type of biometric devices used. This observation gives us a Biometric Signature of the individual concerned. (2) A computer algorithm normalizes the biometric signature so that it is in the same format as the signatures on the system's database. This normalization gives us a Normalized Signature of the individual. (3) A matcher compares the normalized signature with the set of normalized signatures on the system's database and provides a similarity score that compares the individual's normalized signature with each signature in the database set.

FACE recognition research still faces challenge in some specific domains such as an individual's pose and illumination changes. Although numerous techniques have been proposed to solve such problems and have shown significant improvement, the difficulties still remain. Error rates of 2-25% are common. Current systems work very well whenever the test image to be recognized is captured under conditions similar to those of the required conditions. However, problems may arise if there is variation in conditions in which the images are captured. The best facial recognition system is the one in which changes in incident illumination, head pose, facial expression, hairstyle, cosmetics and age, all are considered and does not have an impact on the result.

Despite a large number of available techniques, FACE recognition remains a difficult, unsolved problem in general. While each of the approaches works well for the specific variation being studied, performance degrades rapidly when other variations are present. For instance, a feature invariant to illumination works well as long as pose or facial expression remains constant, but fails to be invariant when pose or expression is changed. This is not a problem for some applications, such as controlling access to a secured room, since both the training and test images may be captured under similar conditions. However, for general, unconstrained recognition, none of these techniques are robust enough. However, FACE recognition systems are still capable enough to operate under basic conditions and they can still be used especially for ensuring security of small-scale organizations.

### **III. PROPOSED SOLUTION**

The ultimate objective of this research is to compare two images: - one which stored in the database and another which is taken to match with the image stored in the database and record the results and based on these results, it is to be determined whether the two images are of the same person or not. In this research, JAVA programming language is used to store the images and compare them at a later stage

For comparing two images, the WEBCAM of the PC is used. To do the actual processing of the image, we use the OpenCV framework. OpenCV is free for both academic and commercial use. It has C++, C, Python and Java interfaces and supports Windows, Linux, Mac OS, iOS and Android platforms. OpenCV is designed for much better computational efficiency and focuses strongly on real-time applications. Written in optimized C/C++, the library can take advantage of multi-core processing. Adopted all around the world, OpenCV has more than 47 thousand people of user community and estimated number of downloads exceeding 9 million. OpenCV framework is slowly increasing in popularity with passing time since it provides better performance when compared to MATLAB.

Before starting any coding, the latest version of OpenCV framework needs to be downloaded and its JAR file needs to be included in the JAVA application. Also, the JAR file of the connector of the database which will be used to store the images needs to be included in the JAVA application. Users can use any database in which they are comfortable for the purpose of storing images and if Netbeans IDE is used for coding, Derby database can be used directly and in that case, no external JAR file needs to be included in the JAVA application.

The first step is checking whether the person under surveillance is a new employee or an existing employee. If he/she is a new employee, the image is captured and directly stored into a database along with his/her other details. If the person under surveillance is an existing employee, his/her image is captured, compared with the earlier image stored in the database and if there is a match, it means that the two images are of the same person. It is to be noted here that only the face of the person is scanned to avoid complexity in comparing at later stages and so that results don't show major deterioration (since WEBCAM is used for capturing images).

However, the most important part of this research is the procedure followed to store the images and the procedure followed to compare them. In JAVA, we have several classes and interfaces which can be used to store and compare images.

In SQL, images are stored in the form of Binary Large Objects (BLOB). BLOB can have a maximum size of 65535 bytes (64 KB). The real problem which may arise is the size of image which is to be stored as the size of the image which is captured may be too large to store in the database or it may even cause difficulty in processing them at a later stage. So, the recommended method is to capture the image, and adjust its width and height before actually storing it into a database. The size by which the image needs to be compressed depends upon the size of the PC monitor as well the quality of the WEBCAM. Good quality WEBCAMs can process a larger-sized image. This compressed image is much easier to process at a later stage. Along with the image, other details of the person can also be stored in the database, if required.

Now, the second part of the research is to retrieve an image from the database and compare with the current image. In JAVA, to work with SQL images, there is an interface named Blob in the package java.sql. Using the method getBlob() of ResultSet

interface, the retrieved image can be directly stored in a reference of type Blob. For comparing two images, we need to convert Blob into a byte array and then convert that byte array to BufferedImage type. These conversions are necessary because in this research, the images are compared according to their pixel values at every location and the results are calculated depending upon the number of similar pixels in the two images.

In order to actually get the pixel values, we have getRGB() method in BufferedImage class. This method accepts two parameters (say a and b) and returns the integer position of that pixel at positions a and b in the RGB colour model space. A counter is defined and incremented by 1 every time the pixel value of the recently captured image is the same as the pixel value of the image stored in the database at a particular position.

Now, the condition for which two images can be considered to be of the same person will depend from system to system and the quality of the biometric hardware used. Since WEBCAM is used in this research and images are compared depending on the number of similar and different pixels, the criteria has been kept 75 %, that is, if the ratio of the number of similar number of pixels (stored in the counter variable at the end of execution of the program) to the total number of pixels (which is equal to the product of width and height of the smaller image among the one captured recently and the one which is stored in the database) is greater than or equal to 0.75, the images are considered to be of the same person.

#### IV. EQUATIONS

Let smw be the width of the smaller of the image which is stored in the database and the image which is recently captured, smh be the height of the smaller of the image which is stored in the database and the image which is recently captured.

$$s = smw * smh.$$
$$x = (p/s) * 100$$

According to the algorithm proposed above, if x is greater than or equal to 75, the images are of the same person and if x is less than 75, the images are of different persons.

#### V. EVALUATION OF PERFORMANCE (OPENCV VS MATLAB)

OpenCV and MATLAB are the two most common frameworks used for image processing. In this research, OpenCV has been used.

Here are some of the advantages of using OpenCV over MATLAB:

- 1) Speed: MATLAB is built on Java, and Java in turn has been built upon C. So when you run a Matlab program, your computer is busy trying to interpret all that Matlab code. Then it turns it into Java, and then finally executes the code.
- 2) OpenCV, on the other hand, is basically a library of functions written in C/C++. You are closer to directly provide machine language code to the computer to get executed. So ultimately you get more image processing done for your computers processing cycles, and not more interpreting. As a result of this, programs written in OpenCV run much faster than similar programs written in Matlab. Statistically speaking, in MATLAB, 3-4 frames are evaluated per second, whereas in OpenCV, up to 30 frames are evaluated per second.
- 3) Resources needed: OpenCV requires just 70 MB of RAM to run. On the other hand, MATLAB consumes a lot of system memory in order to run. MATLAB requires more than 1 GB of RAM to run.
- 4) Cost: OpenCV is absolutely free. On the other hand, the base price for MATLAB is over 2000 US Dollars.
- 5) Portability: Any device that is capable of running C programs can run OpenCV.
- 6) Now, here are some areas in which OpenCV lags behind MATLAB:
- 7) Memory Management in MATLAB is more efficient than in OpenCV.
- 8) MATLAB is easier to use than OpenCV.
- 9) MATLAB has its own development environment unlike OpenCV.

#### VI. CONCLUSION

In this research, we studied about the importance of Biometrics security in any organization. There are many forms of Biometric security among which FACE recognition is one of the techniques. Although FACE recognition has its set of drawbacks over other biometric techniques, it also has its set of advantages over the other techniques and this is the reason why many organizations have started to consider FACE recognition as a reliable security option.

In this research, emphasis has been laid on FACE recognition through the use of OpenCV framework and JAVA programming language. OpenCV framework has been steadily growing in popularity over the years due to its relatively faster rate of image processing as compared to the other popular frameworks such as MATLAB. JAVA programming language is chosen in this research because it is easy to interact with databases using JAVA.

FACE recognition is still a field where research is going on and with time, some more techniques will be developed in this domain. FACE Recognition has the potential to become one of the most capable ways of ensuring security in an organization and the coming years might well prove this statement.

OpenCV framework presents a very efficient set of libraries and interfaces to accomplish the task of image processing and the number of users using this framework has been constantly increasing over the years.

This research can be helpful for ensuring security of small – scale organizations in particular because a very simple and easy method has been followed to compare two images and determine whether they are of the same person or not. The method followed does not involve any additional hardware complexity and is very easy to understand and follow.

Overall, FACE biometrics is a field which will get better, more secure and more efficient with time and organizations must invest their time and effort in this.

#### **REFERENCES**

- [1] Face Recognition: A Literature Survey W. ZHAO Sarnoff Corporation, R. CHELLAPPA University of Maryland, P. J. PHILLIPS National Institute of Standards and Technology and A. ROSENFELD University of Maryland
- [2] Face Recognition: A Literature Review : A. S. Tolba, A.H. El-Baz, and A.A. El-Harby , International Journal of Signal Processing 2;2 2006
- [3] A Literature Survey on Face Recognition Techniques: Riddhi Patel, Shruti B. Yagnik, International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 4 –Nov 2013
- [4] A Literature review on Facial Expression Recognition Techniques: Ms.Aswathy.R, Post Graduate Scholar, Computer Science Department, Nehru college of Engineering , India, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 1 (May. - Jun. 2013), PP 61-64
- [5] Face and Eye Detection Using OpenCV - Step by Step : Mahdi Rezaei , Department of Computer Science, the University of Auckland
- [6] Face Detection and Tracking using OpenCV: S.V. Viraktamath, Mukund Katti, Aditya Khatawkar & Pavan Kulkarni
- [7] <http://www.opencv.org>
- [8] <http://blog.fixational.com/post/19177752599/opencv-vs-matlab>
- [9] <http://www.aishack.in/2010/02/why-opencv/>