6th International Conference on "Latest Innovations in Science, Engineering and Management"
(IFUNA) Indian Federation of United Nations Associations, New Delhi (India) ICLISEM - 2017
12th November 2017, www.conferenceworld.in ISBN: 978-93-86171-76-4

A Real Time Face Recognition and authentication System

Mr.Prodipta Bhowmik

Assistant Professor, Department of IT, Techno India, Salt Lake

Kolkata, (India)

ABSTRACT

Human face can be identified by different biometric features, which are genetic properties of a human being. If the biometric features can be extracted from a facial image then they can be used for face recognition. Robust face recognition system has potential application in the area of Surveillance and physical security.

To Design a person authentication system, using Face biometrics that can be used for authentication and recognition in various login systems as well as attendance recording systems. This project describes and implements an effective method for vision-based person identification that can detect and recognize a person by doing a comparison from a specific face from data base and face captured from the camera in front of him. This authentication system is immune to the illumination changes and the biometrics is combined with pin identification number to improve security features. It overcomes the security loop hole associated with traditional ways of identification by tokens or PINs (Personal Identification Number), which are easy to implement, but constantly under the risk of being stolen, or forgotten.

Keywords: Face detection, Authentication, LBP, Haar Like features, Chi-square

I. INTRODUCTION

The current authentication systems are characterized by an increasing interest in biometric techniques. Among these techniques are face, facial thermogram, fingerprint, Hand

geometry, hand vein, iris, retinal pattern, signature and voiceprint. All these methods have different degrees of uniqueness, permanence, measurability, performance, User's acceptability and robustness against circumvention. To identify a person, most of the early works focused on biometrics such as fingerprint, iris, and face recognition. However, fingerprint and iris require the subject to directly interact with the sophisticated sensors. This limits the domain of applications. Face recognition seems to be more feasible in the sense that it uses passive and most common sensor a 'camera'.Biometric identification based on face recognition is particularly useful for security applications and human-machine interfaces. This combined with PIN (person identification number) further improves the security feature of authentication system. Identifying by tokens or PIN only is associated with the risk of being stolen. But the most important biometrics if face cannot be copied and hence have more security features. This system implements the philosophy of how a person identifies another and hence it opens a new door to the interaction between machines and humans by identifying them by their face. The whole system can be divided into three basic phases:

i. Training Phase
ii. Face detection in captured image

iii. Face identification

In this system, at first stage the application is trained with few faces of the person which is to be identified. In the detection phase face of the person is extracted from the image captured from the camera. The face component of the image is then treated to change it in to gray scale image the overall contrast and brightness is adjusted. In addition to it the image is scaled to required size. Then eyes are located in the extracted image. Eye detection is needed in order to align the target face to the model stored in the database before matching. In identification or authentication phase LBP(local binary pattern) histogram of the image thus extracted is compared with that of the image stored in database and then, the face identity is verified by computing histogram intersection distance D(S,M) between the target LBP histogram (S) to the model LBP histogram (M). If D(S,M) is below certain empirically determined threshold Tk, the face is rejected. Otherwise, good match is reported.

II. PRESENT METHODS

2.1 Face and eye detection

Many approaches have been proposed for detecting and recognizing faces. One of them is a color based approach to face detection. Indeed, color is a low-level cue that can be implemented in a computationally fast and effective way for locating objects. When searching for faces, skin color can then greatly reduce the search area by selecting only the skin-like regions. Among the advantages of using color is the computational efficiency and robustness against some geometric changes, when the scene is observed under a uniform illumination field.

However, the main limitation with the use of color lies in its sensitivity to illumination changes. To overcome the limitations of the color based approach, we considered the implementation of the well-known face detection algorithm proposed by ***Paul Viola and Michel J.Jhones*** in 2001[1].It uses Haar like features and AdaBoost learning algorithm. The Haar-like features are extracted using the notion of integral image which allows very fast feature extraction at different scales, while AdaBoost is used to select the most prominent features among a large number of extracted features and construct a strong classifier from boosting a set of weak classifiers. The use of a cascade of classifiers made this approach one of the first real-time frontal-view face detection methods. First, a classifier (namely a cascade of boosted classifiers working with haar-like features) is trained with a few hundreds of sample views of a particular object (i.e., a face or a car), called positive examples, that are scaled to the same size (say, 20x20), and negative examples - arbitrary images of the same size. After a classifier is trained, it can be applied to a region of interest (of the same size as used during the training) in an input image. The classifier gives outputs as "1" if the region is likely to show the object (i.e., face/car), and "0" otherwise. To search for the object in the whole image one can move the search window across the image and check every location using the classifier. The classifier is designed so that it can be easily "resized" in order to be able to find the objects of interest at different sizes, which is more efficient than resizing the image itself. So, to find an object of an unknown size in the image the scan procedure should be done several times at different scales.The word "cascade" in the classifier name means that the resultant classifier consists of several simpler classifiers (stages) that are applied subsequently to a region of interest until at some stage the candidate is rejected or all the stages are passed. The word "boosted" means that the classifiers at every stage of the cascade are complex themselves

and they are built out of basic classifiers using one of four different boosting techniques (weighted voting). Currently Discrete Adaboost, Real Adaboost, Gentle Adaboost and Logitboost are supported. The basic classifiers are decision-tree classifiers with at least 2 leaves. Haar-like features are the input to the basic classifers, and are calculated as described below. The current algorithm uses the following Haar-like features:

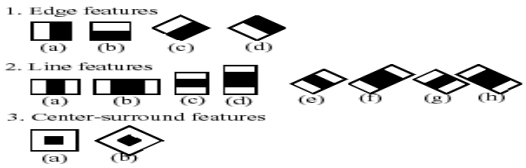


Fig1. Haar-like features

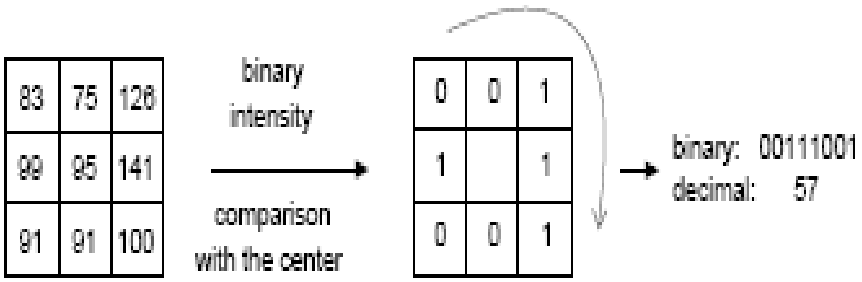
The feature used in a particular classifier is specified by its shape (1a, 2b etc.), position within the region of interest and the scale (this scale is not the same as the scale used at the detection stage, though these two scales are multiplied). For example, in case of the third line feature (2c) the response is calculated as the difference between the sum of image pixels under the rectangle covering the whole feature (including the two white stripes and the black stripe in the middle) and the sum of the image pixels under the black stripe multiplied by 3 in order to compensate for the differences in the size of areas. The sums of pixel values over rectangular regions are calculated rapidly using integral images.

2.2 Face Authentication using LBP Histogram

Local Binary Pattern (LBP) is becoming a popular technique for face representation as well as for image representation in general. Recently, LBP has been applied to the specific problem of face recognition. The LBP is a non-parametric kernel which summarizes the local spatial structure of an image. Moreover, it is invariant to monotonic gray-scale transformations; hence the LBP representation may be less sensitive to changes in illumination. In a realistic scenario, it is very likely that the lighting conditions of the probe image do not correspond to those of the gallery image; hence there is a need to handle such variations. This probably explains the recent success of Local Binary Patterns in the face recognition community.

III. THE LBP

The Local Binary Pattern (LBP) operator is a non-parametric 3x3 kernel which summarizes the local spatial structure of an image. It was first introduced by Ojala et al. who showed the high discriminative power of this operator for texture classification. At a given pixel position (xc, yc), LBP is defined as an ordered set of binary comparisons of pixel intensities between the center pixel and its eight surrounding Pixels. Due to its texture discriminative property and its very low computational cost, LBP is becoming very popular in pattern recognition.



(Calculating the original LBP code)

The decimal form of the resulting 8-bit word (LBP code) can be expressed as follows:

$$LBP(x_c, y_c) = \sum_{n=0}^{7} s(i_n - i_c)2^n$$

Where *i*c corresponds to the grey value of the center pixel (x_c, y_c), in to the grey values of the 8 surrounding pixels, and

function s(x) is defined as:

$$s(x) = \begin{cases} 1 & \text{if} \quad x \geq 0 \\ 0 & \text{if} \quad x < 0 \end{cases}.$$

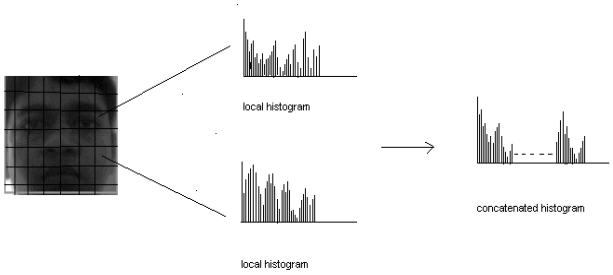
LBP Operation→ 

3.1. Authentication using LBP Histogram:-

The individual sample image is divided into R small non-overlapping blocks (or regions) of same size. Histograms of LBP codes Hr, with r = {1, 2, . . . , R} are calculated over each block and then concatenated into a single histogram representing the face image. Ahonen [2] proposed this face recognition system based on a LBP representation of the face. A block histogram can be defined as:

$$H^r(i) = \sum_{x,y \in block_r} I(f(x,y) = i), \ i = 1, ..., N,$$

Where N is the number of bins (number of different labels produced by the LBP operator), f(x, y) the LBP label 2 at pixel (x, y) and I the indicator function.



This model contains information on three different levels: (1) LBP code labels for the local histograms (pixel level), (2) local histograms (region level) and (3) a concatenated histogram which builds a global description of the face image. For classification, a nearest-neighbor classifier is used with Chi-square dissimilarity measure, defined as follows:

$$\chi^2(\mathrm{S}, \mathrm{M}) = \sum_{r,i} \frac{(S^r(i) - M^r(i))^2}{S^r(i) + M^r(i)},$$

Where S and M correspond to the sample and the model histograms.

Now if this value is calculated below a certain threshold value two faces are considered to be of same person and hence system authenticates him.

IV.EXPERIMENTAL RESULT

The current authentication systems are characterized by an increasing interest in biometric techniques. To identify a person, most of the early works focused on biometrics such as fingerprint, iris, and face recognition. However, fingerprint and iris require the subject to directly interact with the sophisticated sensors. This limits the domain of applications.

The whole system can be divided into three modes:

i. Training Mode
ii. Authentication Mode
iii. Recognition Mode
iv. In training mode 10 faces of user have to be saved.
v. First user have to select training mode by pressing "**Train Face**" button..

vi. After that user has to enter the name.The name should not contain any space in between.

vii. After submitting your name you are in training mode. Now press "**Capture Face From Cam**" button. In the left side of windows you will see your extracted face.

viii. Press "**Accept**" button if eyes are correctly located and if there is a face in rotated face frame. Then press yes button in pop up window. If you are not satisfied with captured face then press "**Reject**" button for rejecting the extracted face and to take new image. If you press the yes button in pop-up window the face will be saved against you

ix. Take 10 acceptable pictures. After taking every picture you will see a pop up window how many more picture you have to take.

x. After completion of training you will see a pop up message that "*That training is completed and you can now authenticate or recognize your face*". Now you are registered in the data base.

If you exit the system while in training mode before completion of training you will not be registered in the data base.

- **Few thing to take care while in training mode :-**
  - **a.** Train system in good lighting condition.
  - **b.** Try to keep your face as normal as possible.
  - **c.** Avoid wearing sunglasses.
  - d. Accept only good quality pictures.

V. AUTHENTICATION MODE

1. Select Authentication mode by pressing "**Authenticate**" button. Before entering the authentication mode ensure that you have already registered in the database.
2. After pressing "**Authentication"** button you will see a window where you have to enter the name.
3. Now capture face and accept if eyes are correctly located and you are satisfied with the quality of picture.If the face matches with the faces stored against that name you will see a popup message "**welcome <name>"**. Otherwise you will see **"access denied**."

VI. RECOGNITION MODE

1. In recognition mode the system matches your face against all the faces stored in database. If successful match occurs name of the person will be displayed.
2. Select RECOGNITION MODE by pressing "**Recognise"** button**.**
3. Capture your face and accept it if eyes are correctly located and quality of picture is good.
4. After accepting you will see a widows with progress bar and message "*processing data".*
5. If match occurs, you will see a message displaying name of the person.
6. For unsuccessful match you will see a message "*cannot recognize face".*

VII. CONCLUSION

The goal of this project is to design a biometric system combined with PIN verification that is independent of any biometric device. An abstraction scheme is proposed that can combine any biometric feature and traditional PIN verification to enhance the security features in any type of authentication system. This scheme of verification can be implemented in system or zones with high security requirement and as well as it can be used in various login systems. With little change it can be used as an attendance recording system. If combined with Infrared Camera, it will enhance security features which will reject an attempt to fool the system using face picture only by mapping thermo gram of face.

Due to its texture discriminative property and its very low computational cost, LBP is becoming very popular in pattern recognition and hence it is used in authentication purpose here. Recently, LBP has been applied for instance to face detection, face localization, face recognition, image retrieval, motion detection or visual inspection. Moreover, it is invariant to monotonic gray-scale transformations; hence the LBP representation may be less sensitive to changes in illumination. This is a very interesting property in face recognition. Indeed, one of the major problems in face recognition systems is to deal with Variations in illumination.

The same philosophy of person authentication can be used in surveillance systems which can identify any unwanted person in any restricted area. It can be also used in the area of robotics if combined with face expression recognition which will enhance the interaction with machines.

REFERENCES

[1.] [1] Pattern recognition used for face , eyes, nose :- Paul Viola and Michel J.Jhones "Rapid Object Detection Using Haar-like Features with Cascade of Boosted Classifiers",IEEE CVPR 2001.

[2.] [2] For Face Authentication system: - T. Ahonen, A. Hadid and M. Pietik¨ainen, "Face recognition with local binary patterns", European Conference on Computer Vision, Prague, 469–481, 2004.

[3.] [3] Image processing library:-"Intel® Open Source Computer Vision Library". http://www.sourceforge.net/projects/opencvlibrary.