Face Recognition Security System

Conference Paper · December 2013

CITATIONS
16

READS
25,862

6 authors, including:

Michel Owayjan
American University of Science and Technology
61 PUBLICATIONS **205** CITATIONS
SEE PROFILE

Elie Abdo
American University of Science and Technology
9 PUBLICATIONS **39** CITATIONS
SEE PROFILE

Face Recognition Security System

Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo
American University of Science and Technology (AUST)
Departments of Computer and Communications Engineering and Computer Science
{mowayjan, eabdo}@aust.edu.lb

Abstract – Today's institutions are facing major security issues; consequently, they need several specially trained personnel to attain the desired security. These personnel, as human beings, make mistakes that might affect the level of security.
A proposed solution to the aforementioned matter is a Face Recognition Security System, which can detect intruders to restricted or high-security areas, and help in minimizing human error. This system is composed of two parts: hardware part and software part. The hardware part consists of a camera, while the software part consists of face-detection and face-recognition algorithms software. When a person enters to the zone in question, a series of snapshots are taken by the camera and sent to the software to be analyzed and compared with an existing database of trusted people. An alarm goes off if the user is not recognized.

Keywords – Digital Image Processing, Face Detection, Face Recognition, Biometrics

I. INTRODUCTION

Real time face recognition is part of the field of biometrics. Biometrics is the ability for a computer to recognize a human through a unique physical trait. Face recognition provides the capability for the computer to recognize a human by facial characteristics. Today, biometrics is one of the fastest growing fields in advanced technology. Predictions indicate a biometrics explosion in the next century, to authenticate identities and avoid and unauthorized access to networks, database and facilities.

A facial recognition device is a device that takes an image or a video of a human face and compares it to other image faces in a database. The structure, shape and proportions of the faces are compared during the face recognition steps. In addition, 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 [1].

When using a facial recognition program, several pictures of the person must be taken at different angles and with different facial expressions [1]. At 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.

Facial recognition is widely used because of its benefits. 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 [1]. 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. Environment is also a consideration as well as subject motion and focus on the camera [1].

Facial recognition, when used in combination with another biometric method, can improve verification and identification results dramatically.

II. EXISTING SOLUTIONS

Many face recognition software have been implemented during the past decade. Each software uses different methods and different algorithm than other software. Some facial recognition software extracts the face features from the input image to identify the face [1]. Other algorithms normalize a set of face images and then compress the face data, the saves the data in one image that can be used for facial recognition. The input image is compared with the face data [2].

New method for face recognition is being used which is the three-dimensional facial recognition. In this method, a 3-D sensor is used to capture information about the shape of the face so that only distinctive features of the face, such as the contour of eye sockets, nose and chin, are used for face recognition [1]. This new method offers some advantages over other algorithms in that recognition it is not affected by the change of light, and the face can be identified from a variety of angles, including profile view.

Another new technique in facial recognition is called skin texture analysis. This technique uses the visual details of the skin, as captured in standard digital or scanned images and then turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.

Below is an introduction for some of the existing facial recognition programs that were used for security reasons.

A. FaceFirst

FaceFirst is a software that provides a fully automated, user friendly, turnkey mobile and live-video surveillance facial recognition system. This software generates an alert whenever a face is recognized; and this occurs when the match of the input face with a face in the database is above a user defined probability. The advantage of FaceFirst system is the availability to work in low resolution environments enabling real-world performance [1].

B. MorphoTrak

MorphoTrak provides biometric and identity management solutions to a broad array of markets including law enforcement, border control, driver licenses, civil identification, and facility/IT security. MorphoTrak is part of the world's largest biometric company and leading innovator in large fingerprint identification systems, facial and iris recognition, as well as secure credentials [1].

C. Cross Match Technologies

Cross Match Technologies is a leading global provider of biometric identity management systems, applications and enabling technologies to governments, law enforcement agencies and businesses around the world. Offerings include biometric technologies capable of wireless, mobile or stationary use that encompass facial recognition systems and other systems [1].

III. 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. Except in the case of identical twins, the face is arguably a person's most unique physical characteristic. 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 [3]. The facial recognition software is based on the ability to first recognize faces, which are a technological feat in itself, and then measure the various features of each face [2].

The planned testing approach is to have a database of numerous faces that is used to test the recognition algorithm against certain particular faces. The variables that need to be tested for a face against the database include the size and condition variations, illumination changes, different facial expressions, and the angle from which the image is taken. The approach is similar to what may be done in real world applications, where a facial image is acquired, but not necessarily in ideal conditions and needs to be matched against a database of somewhat ideal facial images. There are many applications that this algorithm could be used for, such as surveillance and security systems. Face recognition is a widespread technology used for Access Control. The task is stated as follows. There is a group of authorized people, which a 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 property, to valuable IP on corporate networks or simply proving your identity-adequate and robust security is essential [2].

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

IV. 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 present in a set of face images in a database using face recognition technique. The software is divided into two parts: face detection and face recognition.

A. Algorithm Suggested for Face Detection

First, the image is taken as an input into the software. The program then converts it from its color mode (RGB) into gray-scale then resizes it. An edge detection operation is then applied by calculating the gradient of the image. To calculate the gradient of an image, the Sobel operator is used, which creates a binary mask using a user-specified threshold value. The threshold value is determined by getting the mean of all gray values in the image. The next step is a dilation operation in order to make the borderlines thicker, followed by a filling technique in order to fill the hole in the face. After holes filling, erosions followed by dilations are applied to get rid of other smaller objects in the image and maintain the region of interest intact. Finally, the image is resized back to its original size.

1) Filtering

After taking the initial picture, the median filter technique is applied on the image. The purpose of this technique is to eliminate the noise that will appear during the capturing, and to enhance the edging procedure. So when using other kind of filter it will affect the edging and an error will appear.

2) Resising

After filtering the image, it is resized from 2048 x 1536 x 3 (resolution of the camera) to 512 x 384 x 3, because it easier to MATLAB to deal with small image and the processor will be faster.

3) Color Mode conversion and Skin Detection

The initial image taken from the camera is in RGB color mode which is not good to analyze, because the luminous and the cruminous are mixed together and then the removing of the important parameter will be difficult, so the picture will be converted to (HSV) that facilitate the process of taking the important parameters.

HSV: stand for Hue, Saturation and value and also it is called HSB for brightness [4].

H: It is an angle between (0 and 360) degree in general, in each cylinder the angle around the central vertical axis corresponding for 'Hue', but when there is a skin the range of angle must be satisfied between (0 and 50).

S: The distance from the axis corresponds for ‘Saturation’, for skin must satisfied the interval $0.18 < S < 0.68$.

V: The distance along the axis corresponds to lightness ‘Value’, and also for the skin must satisfied the following interval $0.35 < V < 1$.

Figure 1 shows an image converted from RGB to HSV and Figure 2 shows an image with the skin pixels detected and converted to white pixels while the non-skin pixels are transformed to black pixels.

Figure 1. Image converted from RGB to HSV.

Figure 2. Skin detection.

4) Morphological Operations

After doing all previous procedure, the image will be processed using morphological operations.

a) Dilation

Dilation is the process of converting the black color which has the (value 0) near to the white one (value 1) into white color. Dilation is one of the two basic operators in the area of mathematical morphology (the other being erosion). It is typically applied to binary images, but there are versions that work on grayscale images. The basic effect of the operator on a binary image is to gradually enlarge the boundaries of regions of foreground pixels (*i.e.* white pixels, typically). Thus areas of foreground pixels grow in size while holes within those regions become smaller. The dilation operator takes two pieces of data as inputs. The first is the image which is to be dilated. The second is a (usually small) set of coordinate points known as a structuring element. It is this structuring element that determines the precise effect of the dilation on the input image [5]. In MATLAB, you can use the built-in function imdilate which takes two arguments, the image and a structuring element and return the dilated image. To get the structuring element object, you can use the built-in function strel [6].

Figure 3 shows the result of the image after dilation.

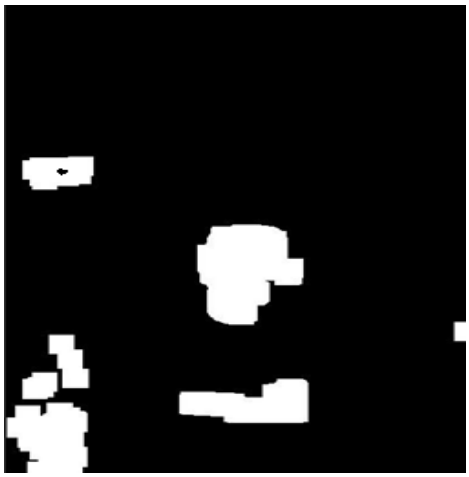

Figure 3. Image dilation.

b) Filling

Filling is the process when a hole surrounded by white color (value 1) will be filled to a white color [7]. In other words, if in a white region there exist some black pixels, those pixels will be transformed to white pixels. This case occurs after the skin detection algorithm because the eyes are not considered skin pixels, and so they are converted to black pixels. In MATLAB, the function imfill takes a binary image as input argument and returns an image with the holes filled.

Figure 4 shows the result of the image after the hole filling operation.

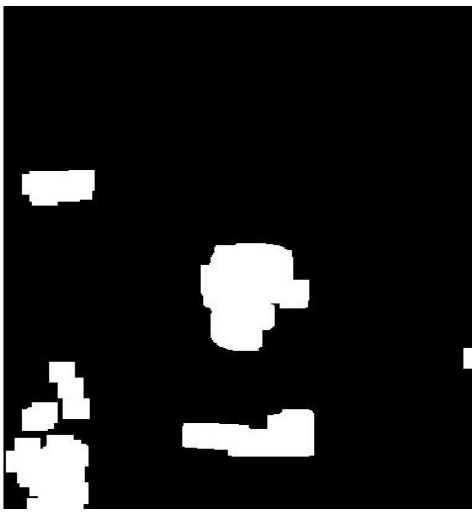

Figure 4. Image filling.

c) Erosion

Erosion is second basic operator in the area of mathematical morphology (the other being dilation as stated before). Again, it is used as the dilation operator, so it is typically applied to binary images, but there are versions that work on grayscale images. The basic effect of the operator on a binary image is to erode away the boundaries of regions of foreground pixels (*i.e.* white pixels, typically). Thus areas of foreground pixels shrink in size, and holes within those areas become larger. The erosion operator, as the dilation operator, takes two pieces of data as inputs. The first is the image which is to be eroded. The second is a (usually small) set of coordinate points known as a structuring element. Again, it is this structuring element that determines the precise effect of the erosion on the input image [8]. In MATLAB, you can use the built-in function imerode which takes two arguments, the image and a structuring element and return the eroded image. To get the structuring element object, you can use the built-in function strel [9].

Figure 5 shows the result of the image after dilation.

Figure 5. Image erosion.

5) Elimination of the non Face Regions

After doing the previous functions, the elimination of the non-face area will be performed using two techniques:

a) Pixels Technique

The correct face has at least 500 pixels, so when we have a skin region with less than 500 pixels, it will be automatically eliminated.

Figure 6 shows the image after the pixels technique operation.

b) Ratio Technique

The correct face has a ratio of height and width between 0.4 and 2.5 respectively, so any skin region that does not fulfill this condition will be eliminated.

Figure 7 shows the image after the ratio technique operation.

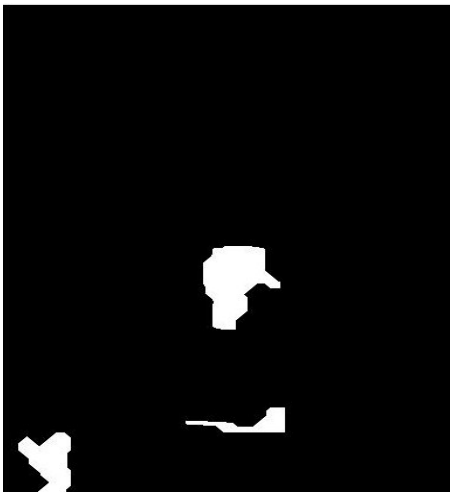

Figure 6. Image after the pixel technique operation.

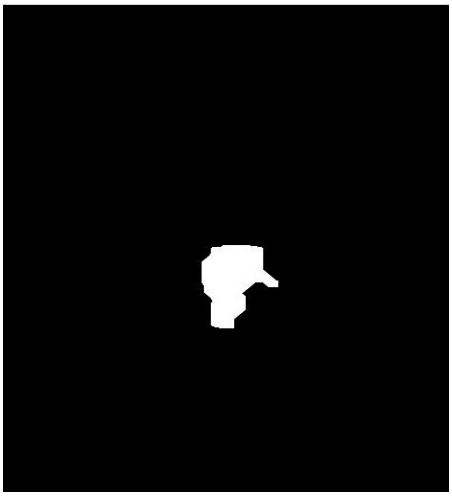

Figure 7. Image after the ration technique operation.

After both techniques, only face region remains and the location of the face will be detected from the image.

B. Algorithm suggested for Face Recognition

In the Recognition procedure, the initial image will be gray scaled to accelerate the processing. After applying the face detection algorithm, only the face part is used now to be compared with the database face images.

First, the face is detected using the face detection algorithm discussed previously. The face is split into three sub-images emphasizing on the special features of the face. Then, a correlation is performed on each sub-image with the database images followed by results averaging to check if the face is recognized or not.

a) Lightining Effect

In this step, the effect of lighting will be reduced to be similar to that of the images in the database. Figure 8 shows the difference between the original image and the image after the reduction of the lightning.

Figure 8. Reducing the light effect.

b) Scaling

All the images in the database should have the same scale. When the face is detected, the image is cropped to the region of the face, and then it is scaled to the same size of the images in the database.

c) Correlation

After scaling the image, the captured face is correlated with each image in the database. If the maximum value of the correlation is greater than 0.9 or less than 0.5, no need for segmentation, otherwise it moves further to the segmentation step.

d) Segmentation

Segmentation is the process of dividing the face into three regions: upper level, middle level and lower level [10]. Then each segment is correlated with each face image in the database. Figure 9 shows the results of the segmentation process.

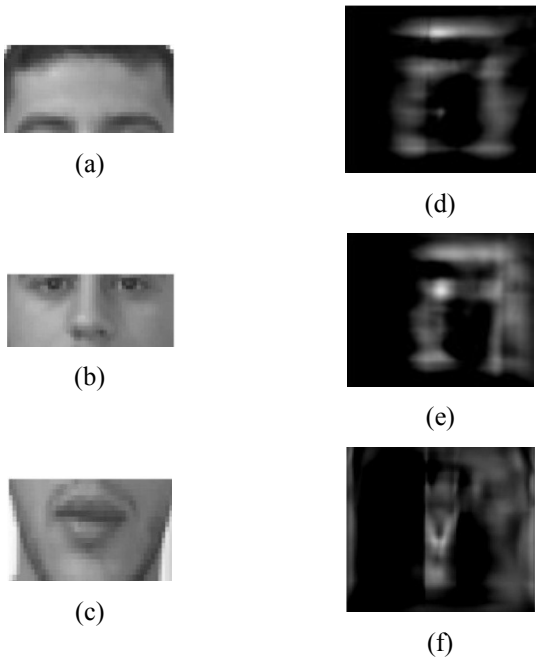

Figure 9. (a) Segment 1 (b) Segment 1 correlation with correct face (c) Segment 2 (d) Segment 2 correlation with correct face (e) Segment 3 (f) Segment 3 correlation with correct face.

V. Results and Testings

In order to test and validate the proposed face recognition security system, a GUI implementation of the algorithm was applied using MATLAB. The database was created and accessed by the software during the processing of the input image.

This system is a real-time face recognition system that reads a real-time video from the camera connected to the computer running the software, takes an image from this video, processes it to detect any human face presented in front of the camera, and then recognizes the face using a set of face images in a database.

This system was tested on several cases, and it achieved a face detection accuracy of 98% and a face recognition accuracy of 90%.

Conclusions and Future Work

Face recognition systems are going to be used more and more in the future for security reasons because they provide better performance over other security systems.

An experimental study face recognition system is presented, which may be applied in identification systems and access control. The proposed face similarity meter was found to perform satisfactorily. The software for the system was coded in MATLAB and was based on face detection and recognition. Although its accuracy is above 90%, this system may be improved by utilization of additional features.

Light normalization and accurate segmentation of face may allow the threshold value to improve. Cruising the warping space more efficiently, e.g. using a corresponded face rotation and gesture geometric model, may speed up the execution time.

Future work may include improvement of the Face recognition using specific characters in the face (distance between eyes) and also analyze the face in 3-D by using the combination of two cameras and by using these two methods, the probability of error will decrease and the system will be more accurate and with a very low cost.

References

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

[2] Steve Mann, "Intelligent Image Processing", Wiley-Interscience 2002.

[3] Walter G.Kropatsh, "Digital Image Analysis", Springer 2002.

[4] Wikipedia, HSL and HSV [Online], Available at: http://en.wikipedia.org/wiki/HSL_and_HSV.

[5] Image Processing Learning Resources, HIPR2, Dilation, [Online], Available at http://homepages.inf.ed.ac.uk/rbf/HIPR2/dilate.htm.

[6] Marc E.Herniter, "Programing in MATLAB" ,Brooks/Cole 2001.

[7] S. Calmer. (1999, June 1). Engineering and Art. (2nd Edition). [Online]. 27(3). Available: www.enggart.com/examples/students.html. [March 21, 2011].

[8] Image Processing Learning Resources, HIPR2, Erosion, [Online], Available at http://homepages.inf.ed.ac.uk/rbf/HIPR2/erode.htm.

[9] Stephen J.chapmon, "MATLAB Programing for Engineers", Brooks/Cole 2002.

[10] Bernd Jahne, "Digital Image Processing", 5th Edition, Springer 2002.