2015 Fifth International Conference on e-Learning

Efficient Method for Face Recognition and Its Role in Supporting E-learning Systems

Walaa M. Abd-Elhafiez[1], Mohamed Heshmat[2], Seham Elaw[3]

[1, 2, 3] *Mathematical and Computer Science Department, Faculty of Science, Sohag University,*
82524, Sohag, Egypt.

[1]*College of Computer Science & Information Systems, Jazan University, Jazan, KSA.*

[1]walaa.hussien@science.sohag.edu.eg
[2]Heshmat@science.sohag.edu.eg
[3]Seham_amer@science.sohag.edu.eg

Abstract— **In this paper, a new technique for face recognition is proposed. This technique has great degree of applications including identification, authentication, psychology, e-learning, security, marketing and human-computer interaction. The important role of the proposed technique with e-learning systems, it will identify users when they first log into a program, also will confirm whether they're the one taking the test. The first step of our technique is detecting the face location in an image. Then the important points of face can be recognized by the proprieties of face such as symmetric location of eyes and different colors of face segments. The experimental results have shown the efficient of the proposed technique. It can be invoked in online system.**

Keywords— **E-learning, color spaces, face detection, face recognition, facial feature, OpenCV.**

I. Introduction

E-Learning is a method of learning which ultimately depends on the Internet in its execution. It shares similar characteristics of many other e-services, such e-commerce, e-banking and e-government. The e-services users' behaviours are different according to their roles and needs. The Internet has become the venue for a new set of illegal activities, and the E-learning environment is now exposed to such threats [1]. Under such a teaching environment, students would watch pre-recorded course contents on the internet. All of the other class activities, such as participation, examinations, class discussion, homework assignment, etc., are also conducted on the internet, i.e., without face to face interactions between the instructor and students [2]. The development of E-learning has a way of learning and, at the same time, has given equal opportunities to everyone to become learners. E-learning method has many advantages, especially commercial values, like many students can be learning at the same time [3], with such methods of learning now available, it is said that information can be reached easily. However, despite the Internet as a place to obtain all necessary information and knowledge, it has also become the venue for a new set of illegal activities. Information on the Internet is continuously exposed to security threats. As a consequence of E-learning having to depend on the Internet via web applications, the E-learning environment has also become affected by security threats [1, 4]. The security (Trust management / user authentication) is one of the most pressing information technology issues that E-education faces today, but it's especially a concern for student.

Trust management like traditional face-to-face education, trust is an important concern in e-learning systems. It is very important that the user is the true student or the learner. In the context of networking and distributed applications, one system needs to be trusted to access another underlying system or service. Trusted interaction forms the underlying requirement between user and providers. For example, a service provider must trust that a learner truly has credentials that are not forged and is authorized to attend the course, or is limited to accessing only some services. On the other hand, the learner must trust the services. More importantly, the learner must believe the service provider will only use his/her private information, such as name, address, credit card details, preferences, and learning behaviour in a manner expressed in the policy provided for the e-learning system user. The most common trust mechanisms are related to digital certificate-based approaches and are found in trust management systems. Recently, there are a lot of researches about e-learning security concerning the user authentication [5-7].

Biometric techniques have advanced over the past years to a reliable means of authentication, which have been deployed in different application domains. Saromporn and Michiko proposed a design of an E-learning system using biological signal that are affective to the learner that closer to learn in the classroom [8]. Many governments have already rolled out electronic passports [9] and IDs [10] that contain biometric information, as face image, fingerprints, and iris scan of their legitimate holders. Unlike other types of data used for authentication purposes (passwords, key material, secure tokens, etc.), biometric data cannot be revoked and replaced with a new value, hence it calls for strict protection of such biometric data. In particular, face recognition systems have become more popular due to its unobtrusiveness and ease of use, no special sensors are necessary and readily available images of good quality can be used for biometric authentication.

Face recognition has a large number of applications, including security, biometric authentication, person verification, Internet communication, and computer entertainment. Although research in automatic face recognition has been conducted since the 1960s, this problem is still largely unsolved. Recent years have seen significant progress in this area owing to advances in face modelling and analysis techniques. Systems have been developed for face detection and tracking [11, 12], but reliable face recognition still offers a great challenge to computer vision and pattern recognition researchers. There are several reasons for recent increased interest in face

978-1-4673-9431-4/15 $31.00 © 2015 IEEE
DOI 10.1109/ECONF.2015.21

recognition, including rising public concern for security, the need for identity verification in the digital world.

This paper proposes a new method for face recognition of faces have facial expressions and rotation, the proposed method have great degree of applications including identification, authentication, psychology, e-learning, security, marketing and human-computer interaction. The proposed method is divided to four parts. The first step in face recognition or facial expression analysis is to detect the face location in an image by using OpenCV's face detection code [13] to detect and extract faces within the input image. Secondly, variance estimation is applied to extract database images which have a close variance value to the test image, then; the important points of face can be recognized faces by the proprieties of face such as symmetric location of eyes and different colors of face segments, where the cut features method is used to extract facial features from the face images. Finally, Euclidean distance of facial features is computed to compare similarity between features.

II. The proposed method

The face and facial feature detection algorithms are applied to detect generic faces from several face images. Most automatic face recognition approaches are based on frontal images. Facial profiles, on the other hand, provide complementary information of the face that is not present in frontal faces. Fusion of frontal and profile views makes the overall personal identification technique fool proof and efficient. The proposed method is based on the average variance estimation of the three components of RGB faces images, and the extraction of the most facial features. The features under consideration are eyes, nose and mouth. The technique used to extract facial features is based on feature location with respect to the dimensions of the face image. Given a face image, which obtained from a camera or pre-processed previously, our goal is to identify this face image using a database of known humans' faces. Therefore, our algorithm is divided into three main steps. First: variance estimation of faces images. Second: facial feature extraction, an effective method to extract facial features like eyes, nose and mouth depending on their locations with respect to the face region is used, which we have developed before in [14]. Third: similar face identification or image searching; the goal of this step is to scan the database of known faces to find the most similar faces to the test face.

1) *Variance estimation*

Variance calculation is a very light calculation and considered as an important constraint to prove similarity between two images. Let x be a vector of dimension n, the variance of x can be calculated as follows:

$$\mathrm{var} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n} \quad , \qquad (1)$$

where $\bar{x}$ is the mean value of x .

However, it is not necessary that the two images which have the same variance to have the same contents. Different images may have the same value of variance because variance estimation is totally depending on the values of image pixels and their mean value. So the variance is used at first to filter the database of faces and extract faces that have the same or close value to variance of the input face image, then another test is required to detect the most similar faces to this test face [14].

When working with RGB color images, there are three values for each pixel in the image, representing the red, green, and blue components. To compute the variance of RGB image, the variance for each color is calculated separately. So there are three values for variance, one for the red values, another for the green values and third for the blue values [14], which are calculated as follows:

$$v_{red} = \frac{\sum_{i=1}^{n}(x_r - \overline{x_r})^2}{n} \ , \ v_{green} = \frac{\sum_{i=1}^{n}(x_g - \overline{x_g})^2}{n} \ , \ v_{blue} = \frac{\sum_{i=1}^{n}(x_b - \overline{x_b})^2}{n} \ , \qquad (2)$$

To simplify the comparison, the average of the three values is computed as follows:

$$v = \frac{(v_{red} + v_{green} + v_{blue})}{3} \quad , \qquad (3)$$

2) *Facial features extraction*

In this part of work, the aim is to compare two color faces to decide whether they both belong to the same person or not and detect the similarity between them using Euclidean distance. RGB (Red, Green and Blue) color space, Fig. 1, which is used here, is an additive color system based on tri-chromatic theory. It is often found in systems that use a Cathode Ray Tube (CRT) to display images. The RGB color system is very common, and is being used in virtually every computer system as well as television, video etc. [15, 16].

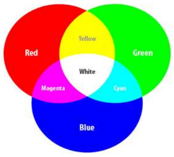


Fig. 1 RGB color model

In RGB color model, any source color (F) can be matched by a linear combination of three color primaries, i.e. Red, Green and Blue, provided that none of those three can be matched by a combination of the other two, see Fig. 1.

Here, F can be represented as:

$$F = rR + gG + bB \quad , \qquad (4)$$

where r, g and b are scalars indicating how much of each of the three primaries (R, G and B) are contained in F. The normalized form of F can be as follows:

$$F = R'R + G'G + B'B \quad , \qquad (5)$$

where

$$R' = r/(r+g+b) \, , \quad G' = g/(r+g+b) \, , \quad B' = b/(r+g+b) \, , \qquad (6)$$

To extract facial features, we used our method proposed in [14], which is based on feature location with respect to the whole face region. By detecting the candidate regions of left eye, right eye, nose and mouth, by training, then applying the obtained dimensions of each region on several other faces with the same size, the results were very good, as shown in Fig. 2.

Given a face image of 200 pixels height and 200 pixel width, after training with a lot of images, we found that the candidate region of eyes is located between rows 60 and 95, columns 25 and 80 for right eye and columns 115 and 170 for left eye. The candidate region for the nose is located between rows 110 and 145 and columns 75 and 125 and the candidate region for the mouth is located between rows 145 and 185 and columns 60 and 135. When applying the dimensions obtained by training on many face images, we found that they there were suitable for any face image with the same width and height even it has expression, as shown in Fig. 2. This feature extraction technique can be generalized and the candidate region for each feature, which is based on height and width of the face image to match any face image size, can be as follows:

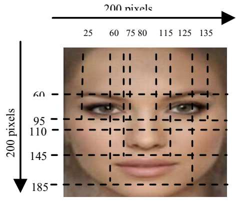


Fig. 2 Examples of features extraction

Right eye: Rows from (height/3.3) to (height /2.1)
Columns from (width/8) to (width/2.5)
Left eye: Rows from (height/3.3) to (height /2.1)
Columns from (width/1.7) to (width/1.17)
Nose: Rows from (height/1.8) to (height /1.38)
Columns from (width/2.67) to (width/1.6)
Mouth: Rows from (height/1.38) to (height /1.08)
Columns from (width/3.33) to (width/1.48)

3) *Method representation*

The proposed algorithm consists of three parts. Firstly, variance estimation is applied to extract database images, which have a close variance value to the test image. Secondly, the features extraction method is used to extract facial features from the face images. Finally, Euclidean distance of facial features is computed by the following equation:

$$\begin{aligned} d = {} & abs\left(test\ feature\left[R\right] - matched\ feature\left[R\right]\right) + \\ & abs\left(test\ feature\left[G\right] - matched\ feature\left[G\right]\right) + \\ & abs\left(test\ feature\left[B\right] - matched\ feature\left[B\right]\right) \end{aligned} \tag{7}$$

By applying eq. (7) to find the distance between the right eye region of the test image and the right eye region of each image, which has variance value close to the variance value of the test image (returned from variance test), then, by applying eq. (7) to left eye, nose and mouth regions and find summation of these four distance values, it can be decided which of the images that have close variance value is the most similar to test image. The steps of the proposed algorithm are shown in the next algorithm.

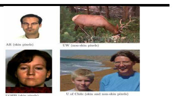
III. Results and Discussion

The experiments using several color images containing faces and a database of six different images with different sizes, as shown in Fig. 3 (middle column). The test images include different images for the same person with different conditions. Some images have expressions, glasses and some rotation, as shown in Fig. 3. The images in the database have been chosen carefully such that they are standard and have no expressions if possible. The proposed algorithm gives good results in recognizing all the test images, which belong to the same person in the database, with different expressions, glasses and rotation. Even if the gaze direction is different, the proposed algorithm succeeds in returning the correct location of the right image in the used database.

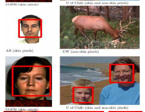
Table 1 shows some of the results obtained using 150 test RGB images of 10 different persons and a database of 10 standard RGB images of those persons, some images from the database are shown in Fig. 3.

Algorithm 1

Step 1: Read input image.

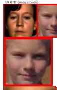


Step 2: Apply face detection code on the input image and detect faces.



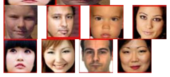
Step 3: Extract faces each in a separate image.

Step 4: Read test face (each face separately from previous step.



Step5: Read codebook array (database of images)

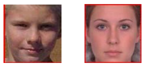
Step 6: Divide codebook into n images.



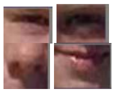
Step 7: Calculate variance to each image in step 6 and put variance values in an array, by using eq. (2), (3).

Step 8: Calculate variance to test image (step 4) using eq. (2), (3).

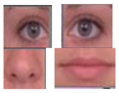
Step 9: Compare variance value of test image and each image in codebook and keep locations of the most similar images to test image in an array.
$(-n \le \text{variance difference} \le n)$



Step 10: For i=1 to number of similar images which extracted from step 9.
a) Extract facial features from each image according to location (right eye – left eye – nose – mouse).



b) Calculate the Euclidean distance between the 3-arrays containing the RGB color values of each feature using eq. (7).



Step 11: Detect minimum distance (d) and location of the image has minimum distance from step 10.

Step 12: Display the best matched image from codebook.

The first column of the table shows the test face. The next columns show the results that were obtained by applying the classical method, variance estimation formula, feature extraction method, the proposed method and the time in each method. The classical method is the general method in comparing two images, by comparing pixel by pixel and computing the summation of the difference of all pixels. The classical method performs on the whole image without partitioning. The variance estimation is applied by using eq. (2) and (3). The results of the variance are displayed separately to show how the variance computation is efficient and important in comparing similarity between images. When variance estimation used as a first test in the proposed method, as seen, it gives the correct image location from the database if the test image and the matched image in the database have similar conditions of illumination and background. Also, the feature extraction method is applied, separately, to study how it is efficient in face recognition. Facial features are extracted and Euclidean distance is computed for each feature then the summation of the difference is obtained. By comparing the difference between the test image and all the images in the database, the matched image is detected as the image has minimum difference. It is noticed from the table that the classical method and variance estimation method have less time than the two other methods. The execution of the proposed method proceeds as follows: the first test (variance test) with variance difference range equals [-n, n], where n is an optional threshold (variance difference range is arbitrary and can be changed), is applied first to detect the images that have close variance values to the test image. The algorithm returns the locations of faces whose variance value close to the variance of the test face. In order to know which one of them is the same or the closest to the test face, the facial features of the test face and the facial features of the obtained face images are extracted then the Euclidean distance of their RGB components is calculated by eq. (7). The face image with the minimum distance (d) is considered as the best-matched image and its location is returned.

The search efficiency is evaluated by how many times the distance (d) computations are performed on average compared to the size of the database. In the proposed method the total number of distance calculations is small, because it uses the variance test to find out the face images that have a close variance value to the input face image, and then the distance computation is performed only on those images where their number is always small compared to the database size. But execution time of the proposed method is high compared to the other methods because the proposed method works in two stages or two tests variance estimation and facial feature extraction where each of these stages take some time. The execution time depends on the database size.

In most cases, the proposed algorithm gives good results. However, in some cases, the results are not good, because the proposed algorithm is affected by illumination conditions in some images, zooming and big rotation in some others.

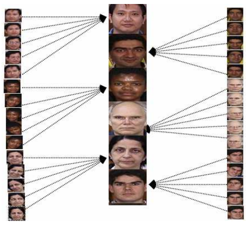


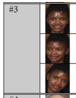
Fig. 3 The used database and some of test images

IV. Conclusion

The integrity of e-learning and online education programs requires that verify the identity of the student. Face recognition technique plays important role with e-learning systems, where it verify of student identities when they log into a program. In this work we presented efficient method to face detection and facial expression. Generally, face detection occurs using the following process. An image is captured by a digital camera in the first. These images are then sent to the proposed method, which determines whether the image contains a face. The robustness of the proposed method has been tested using different images.

Future work: Some integrity to online development programs that are plagued by plagiarism and cheating can be added. Also, E-learning system can be more personal and responsive by giving the administrator a firmer grasp on what students are paying attention to during lecture.

TABLE I SOME RESULTS OF THE PROPOSED ALGORITHM AND THE COMPARISION METHODS

Test image		Classical method		Variance method		Feature extraction method		Proposed method	
		Loc. in database	Time	Loc. in database	Time	Loc. in database	Time	Loc. in database	Time
#1		10	0.58	6	0.05	7	0.33	1	0.43
		10	0.59	6	0.06	1	0.23	1	0.45
		10	0.5	6	0.1	7	0.26	1	0.85
#2		9	0.44	4	0.13	2	0.25	2	1.3
		2	0.63	2	0.07	3	0.15	2	0.62
		10	0.57	2	0.09	2	0.18	2	0.89
#3		5	0.37	2	0.15	3	0.29	3	1
		3	0.59	2	0.12	2	0.22	3	0.85
		7	0.21	2	0.12	3	0.13	3	0.88
#4		4	0.42	4	0.13	4	0.28	4	1.3
		4	0.52	4	0.07	4	0.22	4	0.86
		4	0.52	10	0.12	4	0.32	4	0.92
#5		9	0.47	5	0.04	5	0.25	5	0.24
		10	0.42	5	0.04	7	0.22	5	0.26
		7	0.6	5	0.03	5	0.16	5	0.17
#6		6	0.4	6	0.07	5	0.18	6	0.58
		9	0.42	7	0.16	6	0.17	6	1.36
		3	0.34	6	0.14	5	0.18	6	0.86

Reference

[1] A. Ahmad and M. A. Elhossiny," E-Learning and Security Threats,“ *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 4, pp. 15-18, Apr. 2012.

[2] P. Lii, "The Functions of Distance Learning," in *Proc. The Future of Education Conference 33d Edition,* 13 - 14 June 2013, Florence, Italy.

[3] N. M and B. Ammar M “Agent-based Collaborative Affective e-Learning Framework,” *The Electronic Journal of e-Learning*, vol. 5, no. 2, pp. 123 – 134, 2007.

[4] Z. F. Zamzuri, M. Manaf, A. Ahmad and Y. Yunus, "Computer Security Threats towards the E-Learning System Assets”, in *Proc. Second International Conference, ICSECS*, vol. 180, pp. 335-345, 27-29 June 2011, Kuantan, Pahang, Malaysia.

[5] F. Graf, “Providing security for e-learning”, *Computers & Graphics*, vol. 26, no. 2, pp. 355-365, Apr. 2002.

[6] M. T. Banday, " Ensuring Authentication and Integrity of Open Source Software using Digital Signature,” *International Journal of Computer Applications, IJCA Special Issue on Network Security and Cryptography NSC*, vol. 4, no. 2, pp. 11-14, 2011.

[7] E. Kritzinger, “Information Security in an E-learning Environment “, in *Proc. IFIP International Federation for Information*, vol. 210, pp. 345-349, 21–24 Aug. 2006.

[8] S. Charoenpit and M. Ohkura , A New E-Learning System Design Focusing on Emotional Aspect Using Biological Signals , M. Kurosu (Ed.): Human-Computer Interaction, Part II, HCII 2013, LNCS 8005, pp. 343–350, Berlin, Springer-Verlag, Heidelberg, 2013

[9] Naumann I, Hogben, Machine Readable Travel Documents (MRTD), International Civil Aviation Organization (ICAO). Doc 9303, Part 1, Fifth Edition, 2003.

[10] G. Privacy features of European aid card specifications. Network Security, European Network and Information Security Agency (ENISA), vol. 8, pp. 9-13, 2008.

[11] R.S. Feris, T.E. de Campos, and R.M. Cesar Junior, “Detection and Tracking of Facial Features in Video Sequences,” *Lecture Notes in Artificial Intelligence*, Springer-Verlag press, pp. 197-206, 2000.

[12] Z. Liu and Y. Wang, “Face Detection and Tracking in Video Using Dynamic Programming”, in *Proc.* International Conference of Image Processing, vol. 1, pp. 56-56, Sep. 2000.

[13] (2015) The OpenCV website(Open Source Computer Vision Library.), [Online]. Available: http://opencv.org/

[14] W. Mohamed, M. Heshmat, M. Girgis and S. Elaw, "A new Method for Face Recognition Using Variance Estimation and Feature Extraction," *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, vol. 2, no. 2, pp. 134-141, 2013.

[15] A. Ford and A. Roberts, Colour Space Conversions, Tech. Rep., [Online]. Available: http://www.poynton.com/PDFs/coloureq.pdf, 11 Aug. 1998.

[16] C. Yang and S. Kwok, "Efficient Gamut Clipping for Colour Image, Processing using LHS and YIQ", *Optical Engineering Journal*, vol. 42, no. 3, pp. 701–711, Mar. 2003.