Facial Recognition using Biometrics

Heema Bansal
Department of Computer Science and Engineering,
IGET, Abhipur, Mohali, Punjab, India

Upneet Kaur
Department of Computer Science & Engg
CEC Landran Mohali, India

***Abstract*- While humans have had the innate ability to recognize and distinguish different faces for millions of years; computers are just now catching up. Automatic recognition of people is a challenging problem which has received much attention during the recent years due to its many applications in different fields such as law enforcement, security applications or video indexing. Face recognition is a very challenging problem and up to date, there is no technique that provides a robust solution to all situations and different applications that face recognition may encounter. Facial recognition software falls into a larger group of technologies known as biometrics. Biometrics is any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual.**

I. INTRODUCTION

Face recognition refers to a computer application that facilitates the identification and verification of an individual from a video or digital image. It identifies a person by comparing his or her facial features with images from a facial database. Face recognition is most widely used as a security tool in law enforcement departments, custom offices, and casinos. It is a form of biometrics and it is comparable to iris and fingerprint recognition. Identix, a company based in Minnesota, is one of many developers of facial recognition technology. Its software, FaceIt, can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images. In order for this software to work, it has to know how to differentiate between a basic face and the rest of background. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face.

The main aim of this paper is to introduce 2D and 3D facial recognition technologies and also to compare them. The paper is structured as follows. First I introduce the facial recognition technology in section 1. The section 2 describes 2D facial recognition technology. Section 3 presents 3D facial recognition technology. Section 4 illustrates some applications of facial recognition technology and section 5 concludes this paper, followed by references.

II. 2D FACIAL RECOGNITION TECHNOLOGY

Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. It defines these landmarks as nodal points. Each human face has approximately 80 nodal points. Some of these measured by the software are:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These nodal points are measured creating a numerical code, called a face print, representing the face in the database. In the past, facial recognition software has relied on a 2D image to compare or identify another 2D image from the database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. This created quite a problem. In most instances the images were not taken in a controlled environment. Even the smallest changes in light or orientation could reduce the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure.

2.1 Steps to facial recognition

The following are the step to facial recognition:

1. Capture Image
2. Find face in Image
3. Extract features
4. Compare Templates
5. Declare Matches

1. First, an image of the face is acquired. This acquisition can be accomplished by digitally scanning an existing photograph or by using an electro-optical camera to acquire a live picture of a subject. As video is a rapid sequence of individual still images, it can also be used as a source of facial images.
2. Second, software is employed to detect the location of any faces in the acquired image. This task is difficult, and often generalized patterns of what a face “looks like” (two eyes and a mouth set in an oval shape) are employed to pick out the faces.
3. Once the facial detection software has targeted a face, it can be analyzed. Facial recognition analyzes the spatial geometry of distinguishing features of the face.
4. The fourth step is to compare the template generated in step three with those in a database of known faces. In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity.
5. The final step is determining whether any scores produced in step four are high enough to declare a match. The rules governing the declaration of a match are often configurable by the end user, so that he or she can determine how the facial recognition system should behave based on security and operational considerations.

2.2 Difficult scenarios in face recognition

When the scenario departs from the easy scenario, then face recognition approaches experience severe problems. Among the special challenges some are: pose variation, illumination conditions, scale variability, images taken years apart, glasses, moustaches, beards, low quality image acquisition, partially occluded faces etc.

2.3 A possible way out for difficult scenarios

Video-based face recognition- Initially, face recognition systems focused on still images. However, during the last years research on face recognition in image sequences has gained much attention, although nearly all systems apply still image face recognition techniques to individual frames. In addition to its broader number of applications, video-based face recognition provides several advantages over still image based face recognition:

1. Good frames can be selected on which to perform the recognition stage. Video provides temporal continuity which allows reuse of recognition information obtained from high quality images in processing low quality frames.
2. Video allows tracking of images such that facial expressions and pose variations can be compensated for, resulting in improving recognition.
3. Motion, gait and other features can help a video based face recognition system.

III. 3D FACIAL RECOGNITION TECHNOLOGY

A newly-emerging trend in facial recognition software uses a 3D model, which claims to provide more accuracy. Capturing a real-time3D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time. Using depth and an axis of measurement that is not affected by lighting, 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile). Using the 3D software, the system goes through a series of steps to verify the identity of an individual.

1. Detection

Acquiring an image can be accomplished by digitally scanning an existing photograph (2D) or by using a video image to acquire a live picture of a subject (3D).

2. Alignment

Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees, while with 2D, the head must be turned at least 35 degrees toward the camera.

3. Measurement

The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.

4. Representation

The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.

5. Matching

If the image is 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a challenge currently facing databases that are still in 2D images. 3D provides a live, moving variable subject being compared to a flat, stable image. New technology is addressing this challenge. When a 3D image is taken, different points (usually three) are identified. For example, the outside of the eye, the inside of the eye and the tip of the nose will be pulled out and measured. Once those measurements are in place, an algorithm (a step-by-step procedure) will be applied to the image to convert it to a 2D image. After conversion, the software will then compare the image with the 2D images in the database to find a potential match.

6. Verification or Identification

In verification, an image is matched to only one image in the database (1:1). For example, an image taken of a subject may be matched to an image in the Department of Motor Vehicles database to verify the subject is who he says he is. If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match (1: N). In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is.

IV. CONCLUSION

Face recognition has been and will continue to be a very challenging and difficult problem. While facial recognition can be used to protect your private information, it can just as easily be used to invade your privacy by taking your picture when you are entirely unaware of the camera. As with many developing technologies, the incredible potential of facial recognition comes with drawbacks. Facial recognition is by no means a perfect technology and much technical work has to be done before it becomes a truly viable tool to counter terrorism and crime. But the technology is getting better and there is no denying its tremendous potential. In the meantime, we, as a society, have time to decide how we want to use this new technology. By implementing reasonable safeguards, we can harness the power of the technology to maximize its public safety benefits while minimizing the intrusion on individual privacy.

V. REFERENCES

[1] Blackburn, D. M., “Evaluating Technology Properly: Three Easy Steps to Success,” *Corrections Today*, July 2001.

[2] Blackburn, D. M., M. Bone, and P. J. Philips, Ph.D., *Facial Recognition Vendor Test 2000: Evaluation Report,* available at http://www.frvt.org/

[3] Davies, Graham and Sonya Thasen, “Closed-Circuit Television: How Effective an Identification Aid?” *British Journal of Psychology*, 91:3 Aug. 2000.

[4] Hitchcock, E.M., W. N. Dember, J. S. Warm, B. W. Moroney and J.E. See, “Effects of Cueing and Knowledge of Results on Workload and Boredom in Sustained Attention,” *Human Factors,* 41:3 Sep. 1999.

[5] Phillips, P.J., et al, “The FERET Evaluation” in H. Wechsler, et al (eds), *Face Recognition: From Theory to Applications,* Berlin, Springer-Verlag, 1998.

[6] Phillips, P.J, “The FERET Database and Evaluation Procedure for Face-Recognition Algorithms,” *Image and Vision Computing Journal*, 16.5, 1998.

[7] Phillips, P. J., Alvin Martin, C.L. Wilson, and Mark Przybocki, “An Introduction to Evaluating Biometric Systems,” *Computer,* Feb. 2000.

[8] Pike, G., R. Kemp, and N. Brace, “The Psychology of Human Face Recognition,” *IEE Electronics and Communications: Visual Biometrics,* 00/018 (2000).

[9] Ming-Hsuan Yang, D.. Kriegman and N. Ahuja, “Detecting Faces in Images: A Survey”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp. 34-58, January 2002.

[10] W. Zhao, R. Chellappa, A. Rosenfeld and P.J. Phillips. Face Recognition: A literature survey. Technical Report CART-TR-948. University of Maryland, Aug. 2002.

[11] R. Chellappa, C. L. Wilson, S. Sirohey, “Human and Machine Recognition of Faces: a Survey”, Proceedings of the IEEE, Volume 83, No. 5, pp. 705-740, May 1995.