International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 10 (2013), pp. 1029-1034
© International Research Publications House
http://www. irphouse.com /ijict.htm

Face Recognition Technology

Mittali Rao and Lakshita Parmar

Electrical & Electronics Engineering, Rajasthan Technical University. Jodhpur, India.

Abstract

Wound't you love to replace password based access control to avoid having to reset forgotten password and worry about the integrity of your system? Wouldn't you like to rest secure in comfort that your healthcare system does not merely on your social security number as proof of your identity for granting access to your medical records? Because each of these questions is becoming more and more important, access to a reliable personal identification is becoming increasingly essential .Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost forged or misplaced; passwords can be forgotten or compromised. But a face is undeniably connected to its owner. It cannot be borrowed stolen or easily forged. Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. It a nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

1. Introduction

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences. Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning,

many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have highten the need for methods to prove that someone is truly who he/she claims to be. Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its non transferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

2. What is Biometrics?

A biometric is a unique, measurable characteristic of a human being that can be used to automatically recognize an individual or verify an individual a„¢s identity. Biometrics can measure both physiological and behavioural characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

a. Finger-scan
b. Facial Recognition
c. Iris-scan
d. Retina-scan
e. Hand-scan

Behavioural biometrics (based on measurements and data derived from an action) include:

a. Voice-scan
b. Signature-scan
c. Keystroke-scan

A biometric system refers to the integrated hardware and software used to conduct biometric identification or verification.

Figure 1: Three stages of facial recognition: (a) the range image and texture; (b) the pre-processed surface; (c) the canonical form.

3. Face Recognisation

Face: The face is an important part of who you are and how people identify you. Except in the case of identical twins, the face is arguably a person's most unique physical characteristics. While humans have the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. For face recognition there are two types of comparisons .the first is verification. This is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The second is identification. This is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches. All identification or authentication technologies operate using the following four stages:

a. Capture: A physical or behavioural sample is captured by the system during enrolment and also in identification or verification process
b. Extraction: unique data is extracted from the sample and a template is created.
c. Comparison: the template is then compared with a new sample.
d. Match/non match: the system decides if the features extracted from the new

Samples are a match or a non match Face recognition technology analyze the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with tailored algorithms for each type of biometric device. Face recognition starts with a picture, attempting to find a person in the image.

4. Performance:

False acceptance rate (FAR)

The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate

FAR= NFA/NIIA

Where FAR= false acceptance rate

NFA= number of false acceptance

NIIA= number of imposter identification attempts

Â¢

False rejection rates (FRR)

The probability that a system will fail to identify an enrolee. It is also called type 1 error rate.

FRR= NFR/NEIA

Where FRR= false rejection rates

NFR= number of false rejection rates

NEIA= number of enrolee identification attempt

Response time:

The time period required by a biometric system to return a decision on identification of a sample.

Threshold/ decision Threshold:

The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict; depending on the requirements of any given application.

Enrolment time:

The time period a person must spend to have his/her facial reference template successfully created.

Equal error rate:

When the decision threshold of a system is set so that the proportion of false rejection will be approximately equal to the proportion of false acceptance. This synonym is 'crossover rate'. The facial verification process involves computing the distance between the stored pattern and the live sample. The decision to accept or reject is dependent on a predetermined threshold. (Decision threshold)

5. How Face Recognition Systems Work

An example visionics, company based in a New Jersey is one of the many developers of facial recognition technology. The twist to its particular software, Face it is that it can pick someone's face from the rest of the scene and compare it to a database full of stored images. In order for this software to work, it has to know what a basic face looks like. Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself. If you look at the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features. Visionics defines these landmarks as nodal points. There are about 80 nodal points on a human face. Here are few nodal points that are measured by the software.

- Distance between the eyes
- width of the nose
- depth of the eye socket
- cheekbones
- jaw line
- chin

These nodal points are measured to create a numerical code, a string of numbers that represents a face in the database. This code is called face print. Only 14 to 22 nodal points are needed for face it software to complete the recognition process

Table 1 Applications of Face Recognition Technology

Applications	Advantages	Disadvantages
1a. Credit Card, Driver's License, Passport, and Personal Identification	Controlled image Controlled segmentation Good quality images	No existing database Large potential database Rare search type
1b. Mug shots Matching	Mixed image quality More than one image available	
2. Bank/Store Security	High value Geographically localized search	Uncontrolled segmentation Low image quantity
3. Crowd Surveillance	High value Small file size Availability of video images	Uncontrolled segmentation Low image quality Real-time
4. Expert Identification	High value Enhancement possible	Low image quality Legal certainty required
5. Witness Face Reconstruction	Witness search limits	Unknown similarity
6. Electronic Mug Shots Book	Descriptor search limits	Viewer fatigue
7. Electronic Lineup	Descriptor search limits	Viewer fatigue
8. Reconstruction of Face from Remains	High value	Requires physiological input
9. Computerized Aging	High value	Requires example input

6. Applications

Commercial and law enforcement applications of FRT listed in Table1 static, controlled format photographs to uncontrolled video images posing a wide range of different technical challenges and requiring an equally wide range of techniques from image processing ,analysis, understanding and pattern recognition. One can broadly classify the challenges and techniques into two groups: static (no video) and dynamic (video) matching. Even among these groups, significant differences exist, depending on the specific application. The differences are in terms of image quality, amount of background ,clutter(posing challenges to segmentation algorithms) , the availability of a well defined matching criterion , and the nature , type and amount of input from a human(as in applications 4 and 5). In some applications suggest computerised ageing, one is only concerned with defining a set of transformations so that the new images created by the system are similar to what humans expect based on their recollections.

7. Conclusion:

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the integration and the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment

References

[1] Electronics for You: - Part 1 April 2001 Part 2 May 2001
[2] Electronics World: - December 2002
[3] IEEE Intelligent Systems - May/June 2003
[4] Modern Television Engineering- Galati R.R 5.
[5] Rama Chelleppa, fellow, IEEE, Charles L.,Wilson Senior member, IEEE,and Saad Sirohey, member IEEE.
[6] Danna Voth, IEEE