Image Analysis for Face Recognition

Xiaoguang Lu
Dept. of Computer Science & Engineering
Michigan State University, East Lansing, MI, 48824
Email: lvxiaogu@cse.msu.edu

Abstract

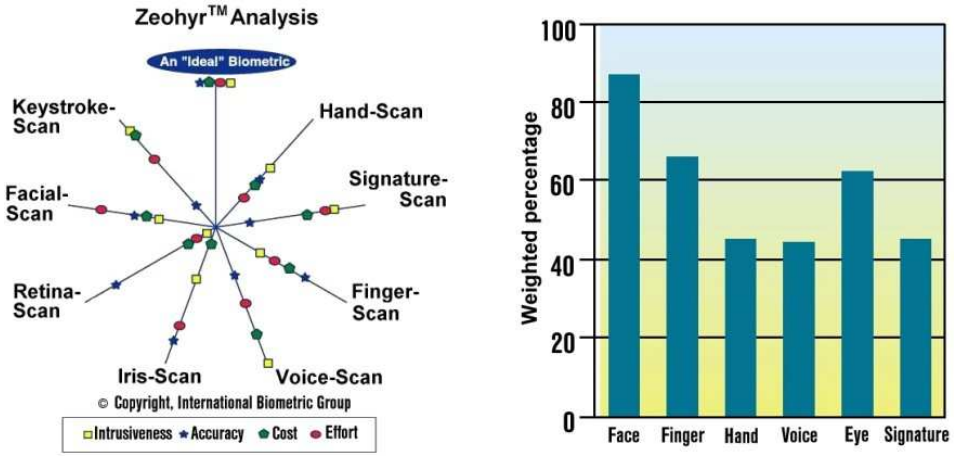
In recent years face recognition has received substantial attention from both research communities and the market, but still remained very challenging in real applications. A lot of face recognition algorithms, along with their modifications, have been developed during the past decades. A number of typical algorithms are presented, being categorized into appearance-based and model-based schemes. For appearance-based methods, three linear subspace analysis schemes are presented, and several non-linear manifold analysis approaches for face recognition are briefly described. The model-based approaches are introduced, including Elastic Bunch Graph matching, Active Appearance Model and 3D Morphable Model methods. A number of face databases available in the public domain and several published performance evaluation results are digested. Future research directions based on the current recognition results are pointed out.

1 Introduction

In recent years face recognition has received substantial attention from researchers in biometrics, pattern recognition, and computer vision communities [1][2][3][4]. The machine learning and computer graphics communities are also increasingly involved in face recognition. This common interest among researchers working in diverse fields is motivated by our remarkable ability to recognize people and the fact that human activity is a primary concern both in everyday life and in cyberspace. Besides, there are a large number of commercial, security, and forensic applications requiring the use of face recognition technologies. These applications include automated crowd surveillance, access control, mugshot identification (e.g., for issuing driver licenses), face reconstruction, design of human computer interface (HCI), multimedia communication (e.g., generation of synthetic faces),

and content-based image database management. A number of commercial face recognition systems have been deployed, such as Cognitec [5], Eyematic [6], Viisage [7], and Identix [8].

Facial scan is an effective biometric attribute/indicator. Different biometric indicators are suited for different kinds of identification applications due to their variations in intrusiveness, accuracy, cost, and ease of sensing [9] (see Fig. 1(a)). Among the six biometric indicators considered in [10], facial features scored the highest compatibility, shown in Fig. 1(b), in a machine readable travel documents (MRTD) system based on a number of evaluation factors [10].



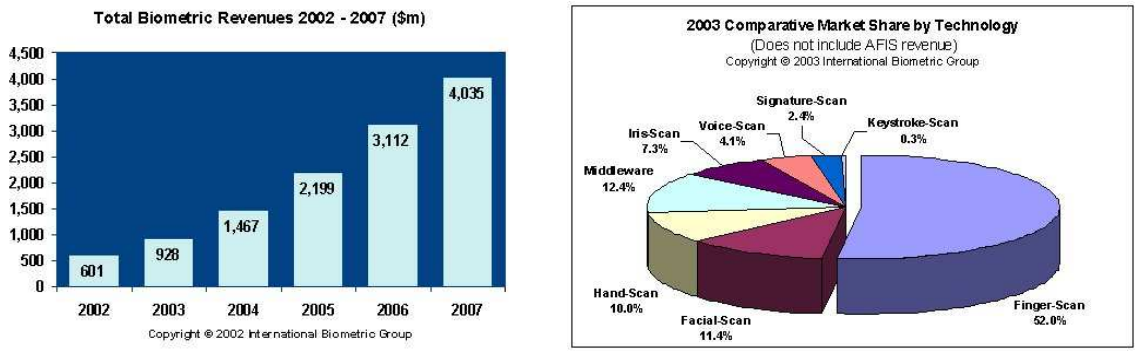
(a) (b)

Figure 1: Comparison of various biometric features: (a) based on zephyr analysis [9]; (b) based on MRTD compatibility [10].

Global 2002 industry revenues of $601million are expected to reach $4.04billion by 2007 [9], driven by large-scale public sector biometric deployments, the emergence of transactional revenue models, and the adoption of standardized biometric infrastructures and data formats. Among emerging biometric technologies, facial recognition and middleware are projected to reach $200million and $215million, respectively, in annual revenues in 2005.

Face recognition scenarios can be classified into two types, (i) face verification (or authentication) and (ii) face identification (or recognition). In the Face Recognition Vendor Test (FRVT) 2002 [11], which was conducted by the National Institute of Standards and Technology (NIST), another scenario is added, called the 'watch list'.

- **Face verification** ("Am I who I say I am?") is a one-to-one match that compares a query



(a) (b)

Figure 2: Face recognition market [9]. (a) Total biometric revenues 2002 - 2007. (b) Comparative market share by technology.

face image against a template face image whose identity is being claimed. To evaluate the verification performance, the verification rate (the rate at which legitimate users are granted access) vs. false accept rate (the rate at which imposters are granted access) is plotted, called ROC curve. A good verification system should balance these two rates based on operational needs.

- **Face identification** ("Who am I?") is a one-to-many matching process that compares a query face image against all the template images in a face database to determine the identity of the query face (see Fig. 3). The identification of the test image is done by locating the image in the database who has the highest similarity with the test image. The identification process is a "closed" test, which means the sensor takes an observation of an individual that is known to be in the database. The test subject's (normalized) features are compared to the other features in the system's database and a similarity score is found for each comparison. These similarity scores are then numerically ranked in a descending order. The percentage of times that the highest similarity score is the correct match for all individuals is referred to as the "top match score." If any of the top r similarity scores corresponds to the test subject, it is considered as a correct match in terms of the cumulative match. The percentage of times one of those r similarity scores is the correct match for all individuals is referred to as the "Cumulative Match Score",. The "Cumulative Match Score" curve is the rank n versus percentage of correct identification, where rank n is the number of top similarity scores reported.

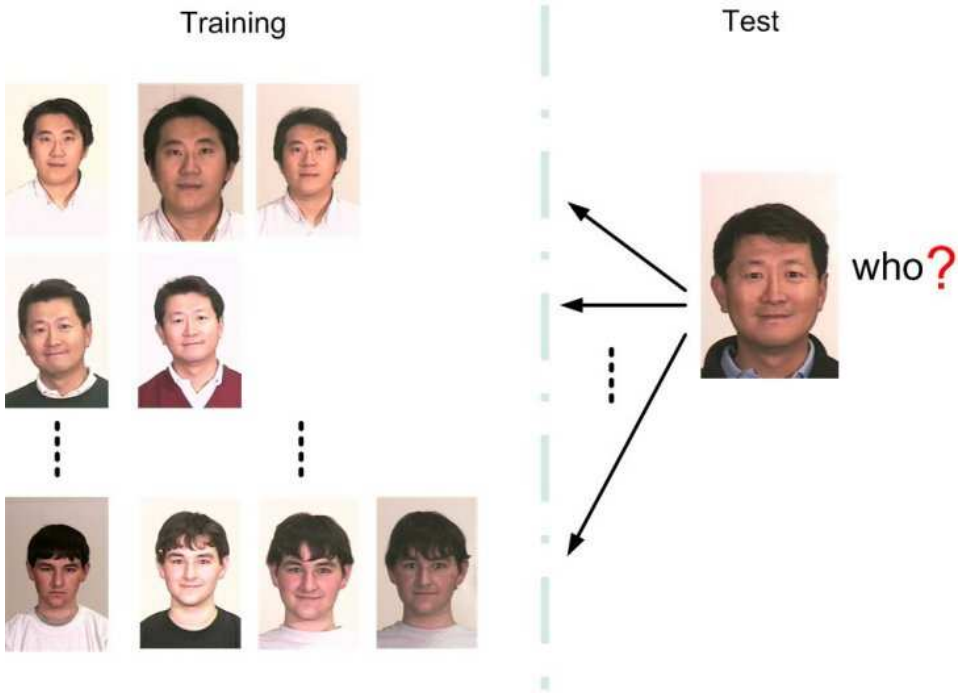


Figure 3: Face identification scenario.

- The **watch list**("Are you looking for me?") method is an open-universe test. The test individual may or may not be in the system database. That person is compared to the others in the system's database and a similarity score is reported for each comparison. These similarity scores are then numerically ranked so that the highest similarity score is first. If a similarity score is higher than a preset threshold, an alarm is raised. If an alarm is raised, the system thinks that the individual is located in the system's database. There are two main items of interest for watch list applications. The first is the percentage of times the system raises the alarm and it correctly identifies a person on the watchlist. This is called the "Detection and Identification Rate." The second item of interest is the percentage of times the system raises the alarm for an individual that is not on the watchlist (database). This is called the "False Alarm Rate."

In this report, all the experiments are conducted in the identification scenario.

Human face image appearance has potentially very large intra-subject variations due to

- 3D head pose

- Illumination (including indoor / outdoor)
- Facial expression
- Occlusion due to other objects or accessories (e.g., sunglasses, scarf, etc.)
- Facial hair
- Aging [12].

On the other hand, the inter-subject variations are small due to the similarity of individual appearances. Fig. 4 gives examples of appearance variations of one subject. And Fig. 5 illustrates examples of appearance variations of different subjects. Currently, image-based face recognition techniques can be mainly categorized into two groups based on the face representation which they use: (i) appearance-based which uses holistic texture features; (ii) model-based which employ shape and texture of the face, along with 3D depth information.

Figure 4: Appearance variations of the same subject under different lighting conditions and different facial expressions [13].

A number of face recognition algorithms, along with their modifications, have been developed during the past several decades (see Fig. 6). In section 2, three leading linear subspace analysis schemes are presented, and several non-linear manifold analysis approaches for face recognition are briefly described. The model-based approaches are introduced in section 3, including Elastic Bunch Graph matching, Active Appearance Model and 3D Morphable Model methods. A number of face databases available in the public domain and several published performance evaluation results are provided in section 4. Concluding remarks and future research directions are summarized in section 5.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.