Chapter 24
Face Recognition Applications

Thomas Huang, Ziyou Xiong, and Zhenqiu Zhang

24.1 Introduction

One of the reasons face recognition has attracted so much research attention and sustained development over the past 30 years is its great potential in numerous government and commercial applications. In 1995, Chellappa et al. [5] listed a small number of applications of face recognition technology and described their advantages and disadvantages. However, they did not analyze any system deployed in real applications. Even the more recent review [38], where the set of potential applications has been grouped into five categories, did not conduct such an analysis. In 1997, at least 25 face recognition systems from 13 companies were available [3]. Since then, the numbers of face recognition systems and commercial enterprises have greatly increased owing to the emergence of many new application areas, further improvement of the face recognition technologies, and increased affordability of the systems. We have listed 10 of the representative commercial face recognition companies, their techniques for face detection, the face features they extract, and face similarity comparison methods in Table 24.1. These 10 companies are also the participants of the face recognition vendor test (FRVT 2002) [29] carried out independently by the U.S. government to evaluate state-of-the-art face recognition technology. Although some of these techniques are not publicly available for proprietary reasons, one can conclude that many others have been incorporated into commercial systems.

T. Huang (✉) · Z. Zhang
University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
e-mail: huang@ifp.uiuc.edu

Z. Zhang
e-mail: zzhang6@uiuc.edu

Z. Xiong
United Technologies Research Center, East Hartford, CT 06108, USA
e-mail: xiongz@utrc.utc.com

S.Z. Li, A.K. Jain (eds.), *Handbook of Face Recognition*,
DOI 10.1007/978-0-85729-932-1_24,

Table 24.1 Comparison of face recognition algorithms from 10 commercial systems in FRVT 2002. N/A: not available

Company	Method for face detection	Face feature extraction method	Matching method
Acsys	N/A	Biometric templates	Template matching
Cognitec	N/A	Local discriminant analysis (LDA)	N/A
C-VIS	Fuzzy face model and neural net	N/A	Elastic net matching
Dream Mirh	N/A	N/A	N/A
Eyematic	General face model	Gabor wavelet	Elastic graph matching
IConquest	Fractal image comparison algorithm		
Identix	N/A	Local feature analysis (LFA)	Neural network
Imagis	Deformable face model	Spectral analysis	N/A
Viisage	N/A	Eigenface	Euclidean distance
VisionSphere	N/A	Holistic feature code	N/A

As one of the most nonintrusive biometrics, face recognition technology is becoming ever closer to people's daily lives. Evidence of this is that in 2000 the International Civil Aviation Organization endorsed facial recognition as the most suitable biometrics for air travel [12]. To our knowledge, no review papers are available on the newly enlarged application scenarios since then [3, 5, 38]. We hope this chapter will be an extension of the previous studies. We review many face recognition applications that have already used face recognition technologies. This set of applications is a much larger super-set of that reviewed in [3]. We also review some other new scenarios that will potentially utilize face recognition technologies in the near future.

These scenarios are grouped into 10 categories, as shown in Table 24.2. Although we try to cover as many categories as possible, these 10 categories are neither exclusive nor exhaustive. For each category, some of the exemplar applications are also listed. The last category, called "Others," includes future applications and some current applications that we have not looked into. These 10 categories are reviewed from Sects. 24.3 to 24.11. In Sect. 24.12, some of the limitations of the face recognition technologies are reviewed. Concluding remarks are made in Sect. 24.13.

24.2 Face Identification

Face recognition systems identify people by their face images [6]. In contrast to traditional identification systems, face recognition systems establish the presence of an authorized person rather than just checking whether a valid identification (ID) or key

Table 24.2 Application categories

Category	Exemplar application scenarios
Face ID	Driver licenses, entitlement programs, immigration, national ID, passports, voter registration, welfare registration
Access control	Border-crossing control, facility access, vehicle access, smart kiosk and ATM, computer access, computer program access, computer network access, online program access, online transactions access, long distance learning access, online examinations access, online database access
Security	Terrorist alert, secure flight boarding systems, stadium audience scanning, computer security, computer application security, database security, file encryption, intranet security, Internet security, medical records, secure trading terminals
Surveillance	Advanced video surveillance, nuclear plant surveillance, park surveillance, neighborhood watch, power grid surveillance, CCTV control, portal control
Smart cards	Stored value security, user authentication
Law enforcement	Crime stopping and suspect alert, shoplifter recognition, suspect tracking and investigation, suspect background check, identifying cheats and casino undesirables, post-event analysis, welfare fraud, criminal face retrieval and recognition
Face databases	Face indexing and retrieval, automatic face labeling, face classification
Multimedia management	Face-based search, face-based video segmentation and summarization, event detection
Human computer interaction (HCI)	Interactive gaming, proactive computing
Others	Antique photo verification, very low bit-rate image & video transmission, etc.

is being used or whether the user knows the secret personal identification numbers (PINs) or passwords. The security advantages of using biometrics to check identification are as follows. It eliminates the misuse of lost or stolen cards, and in certain applications it allows PINs to be replaced with biometric characteristics, which makes financial and computer access applications more convenient and secure. In addition, in situations where access control to buildings or rooms is automated, operators may also benefit from improved efficiency. Face recognition systems are already in use today, especially in small database applications such as those noted in Sect. 24.3. In the future, however, the targeted face ID applications will be large-scale applications such as e-commerce, student ID, digital driver licenses, or even national ID.

Large-scale applications still face a number of challenges. Some of the trial applications are listed below.

1. In 2000, FaceIt technology was used for the first time to eliminate duplicates in a nationwide voter registration system because there are cases where the same person was assigned more than one identification number [12]. The face recog-

nition system directly compares the face images of the voters and does not use ID numbers to differentiate one from the others. When the top two matched faces are extremely similar to the query face image, manual inspection is required to make sure they are indeed different persons so as to eliminate duplicates.

2. Viisage's faceFinder system [33] has been supplied to numerous state corrections authorities and driver license bureaus. This face recognition technology has also been used by the U.S. Department of State for the Diversity Visa Program, which selects approximately 50 000 individuals to be considered for a permanent U.S. visa from millions of applications submitted each year. Each application includes a facial image. The system compares the image of every applicant against the database to reduce the potential of the same face obtaining multiple entries in the lottery program. Once enrolled in the Viisage system, images can also be used during the diversity visa application process to help identify known individuals who pose specific security threats to the nation.

24.3 Access Control

In many of the access control applications, such as office access or computer log-in, the size of the group of people that need to be recognized is relatively small. The face pictures are also captured under constrained conditions, such as frontal faces and indoor illumination. Face recognition-based systems in these applications can achieve high accuracy without much cooperation from the users; for example, there is no need to touch an object by fingers or palms, no need to present an eye to a detector. When combined with other forms of authentication schemes such as fingerprint or iris recognition, face recognition systems can achieve high accuracy. Thus, the user satisfaction level is high. This area of application has attracted many commercial face recognition systems. The following are several examples.

- In 2000, IBM began to ship FaceIt [11] enabled screen saver with Ultraport camera for A, T, and X series Thinkpad notebook computers. Face recognition technology is used to monitor continuously who is in front of a computer terminal. It allows the user to leave the terminal without closing files and logging off. When the user leaves for a predetermined time, a screen saver covers the work and disables the keyboard and mouse. When the user returns and is recognized, the screen saver clears and the previous session appears as it was left. Any other user who tries to log in without authorization is denied.
- The University of Missouri-Rolla campus has chosen a face recognition system by Omron [28] to secure a nuclear reactor, which is a 200-kilowatt research facility that uses low-enriched uranium to train nuclear engineers. Visitors must pass through a staff-monitored lobby, a second door that is accessed with a key, and a third door that is secured with a keypad before getting to the face scanner, which regulates access to the reactor core.
- Another commercial access control system is called FaceGate [10]. Entering a building using FaceGate simply requires one to enter his entry code or a card and

Fig. 24.1 FaceGate access control system

face a camera on the door entry system. Figure 24.1 is a snapshot of the system. By applying a mathematical model to an image of a face, FaceGate generates a unique biometric "key." Whenever one wishes to access a building, FaceGate verifies the person's entry code or card, then compares his face with its stored "key." It registers him as being authorized and allows him to enter the building. Access is denied to anyone whose face does not match.

- The FaceKey standard biometric access control system combines face recognition and fingerprint recognition to provide a high level of security [13]. There is no need for cards, keys, passwords, or keypads. The combination of the two biometrics makes it possible to have security with a low error rate. The system can operate as a stand-alone, one-door system, or it can be networked to interconnect multiple doors at multiple sites, domestically or internationally.
- "FaceVACS-Entry" [6] adds facial recognition to conventional access control systems. At the access point, the face of each person is captured by a video camera, and the facial features are extracted and compared with the stored features. Only if they match is access permitted. For high security areas, a combination with card terminals is possible, so each card can be used only by its owner. Flexible communication interfaces enable easy integration into existing access control or time and attendance systems. Terminals with FaceVACS-Entry can be networked together, so after central enrollment the face data are distributed automatically to all the terminals. In addition, visual control by security personnel can be supported. All facial images collected at the terminals can be stored in a log for later visual inspection via a standard browser.

In addition to commercial access control systems, many systems are being developed in university research laboratories that are exploring new face recognition algorithms. We give two examples.

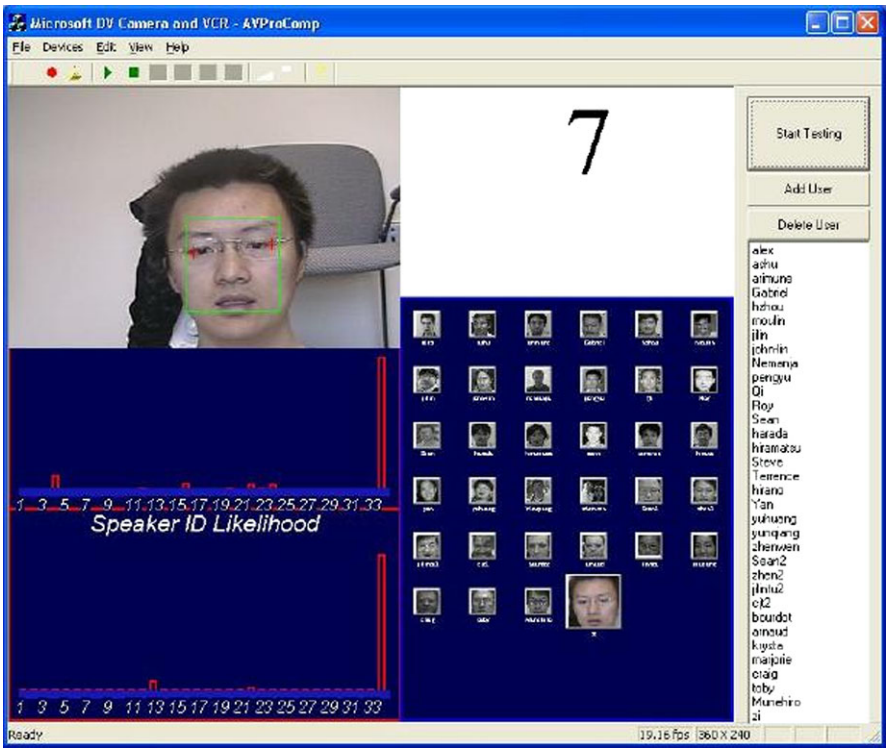

Fig. 24.2 A computer access control system using both face and speaker recognition

1. At the University of Illinois [37], face recognition and speaker identification systems have been integrated to produce high recognition accuracy for a computer login system. Figure 24.2 shows the system interface where the upper-left corner displays the real-time video captured by a digital camcorder. The upper-center displays text or digits for the user to read aloud for speaker identification. At the upper-right corner are three buttons titled "Start Testing," "Add User," "Delete User," indicating three functionalities. Two bar charts in the lower-left corner display the face recognition and speaker identification likelihoods, respectively, for each user. In the lower-center, icon images of users that are currently in the database are shown in black and white and the recognized person has his image enlarged and shown in color. The lower-right of the screen displays all the names of the users currently in the database.
2. The second system [2] uses a multilayer perceptron for access control based on face recognition. The robustness of neural network (NN) classifiers is studied with respect to the false acceptance and false rejection errors. A new thresholding approach for rejection of unauthorized persons is proposed. Ensembles of NN with different architectures were also studied.

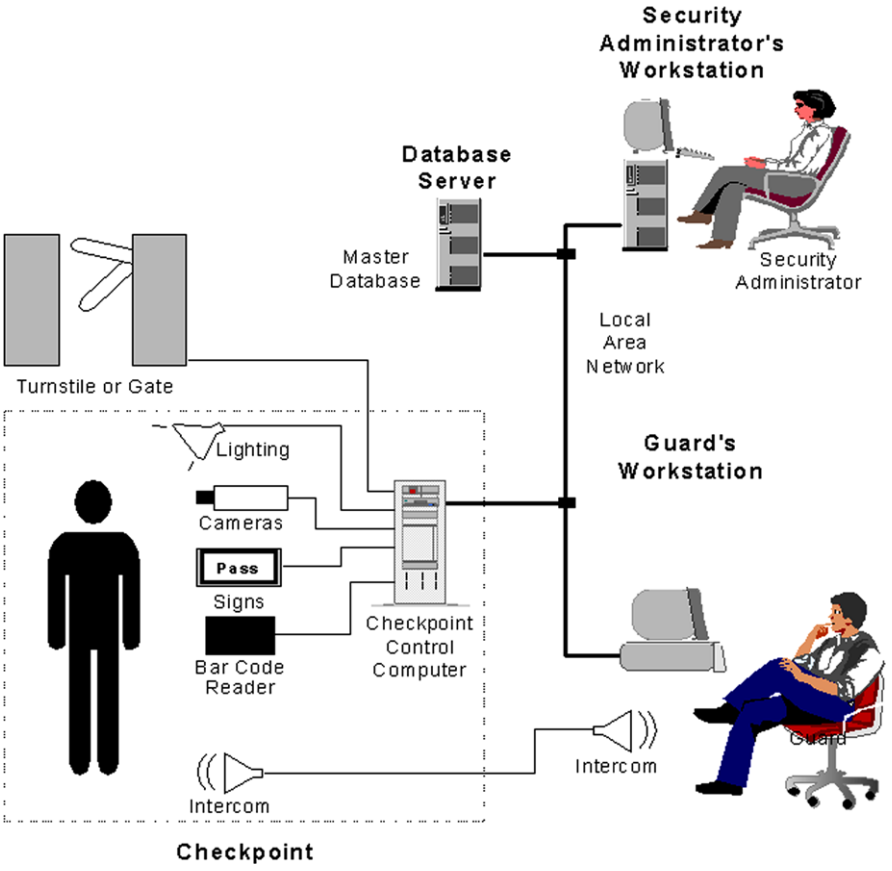

Fig. 24.3 An exemplar airport security system

24.4 Security

Today more than ever, security is a primary concern at airports and for airline personnel and passengers. Airport security systems that use face recognition technology have been implemented at many airports around the globe. Figure 24.3 diagrams a typical airport security system that employs face recognition technology. Although it is possible to control lighting conditions and face orientation in some security applications, (e.g., using a single pedestrian lane with controlled lighting), one of the greatest challenges for face recognition in public places is the large number of faces that need to be examined, resulting in a high false alarm rate. Overall, the performance of most of the recognition systems has not met the very low false rejects goal with low false alarm requirements. The user satisfaction level for this area of application is low.

Some of the exemplar systems at airports, stadiums, and for computer security are listed below.

1. During the 2008 Beijing Olympics games, a face recognition system developed by the Institute of Automation of the Chinese Academy of Sciences (CAS) was introduced into the entrance security checks for the Olympic opening and closing ceremony. According to CAS, it was the first time that such technology was adopted as security measures in the Olympic history.
2. In October, 2001, Fresno Yosemite International (FYI) airport in California deployed Viisage's face recognition technology for airport security purposes. The system is designed to alert FYI's airport public safety officers whenever an individual matching the appearance of a known terrorist suspect enters the airport's security checkpoint. Anyone recognized by the system would undergo further investigative processes by public safety officers.
3. At Sydney airport, Australian authorities are trying out a computerized face-recognition system called SmartFace by Visionics with cameras that have wide-angle lenses. The cameras sweep across the faces of all the arriving passengers and send the images to a computer, which matches the faces with pictures of wanted people stored in its memory. If the computer matches the face with that of a known person, the operator of the surveillance system receives a silent alarm and alerts the officers that the person should be questioned. The technology is also used at Iceland's Keflavik airport to seek out known terrorists.
4. At Oakland airport (San Jose, California), a face recognition system by Imagis Technologies of Vancouver, British Columbia, Canada is used in interrogation rooms behind the scenes to match suspects brought in for questioning to a database of wanted criminals' pictures.
5. Malaysia'a 16 airports use a FaceIt-based security system to enhance passenger and baggage security. A lipstick-size camera at the baggage check-in desk captures a live video of the passengers and embeds the data on a smart-card chip. The chip is embedded on the boarding pass and on the luggage claim checks. The system ensures that only passengers who have checked their luggage can enter the departure lounge and board the aircraft, and that only the luggage from boarding passengers is loaded into the cargo area. During the boarding process, the system automatically checks a real-time image of a passenger's face against that on the boarding pass smart chip. No luggage is loaded unless there is a match.
6. Viisage's faceFINDER equipment and software were used to scan the stadium audience at the Super Bowl 2001 at the Raymond James Stadium in Tampa, Florida in search of criminals. Everyone entering the stadium was scanned by video cameras set up at the entrance turnstiles. These cameras were tied to a temporary law-enforcement command center that digitized their faces and compared them against photographic lists of known malefactors. The system is also used by South Wales Police in Australia to spot soccer hooligans who are banned from attending matches.
7. Computer security has also seen the application of face recognition technology. To prevent someone else from modifying files or transacting with others when the authorized individual leaves the computer terminal momentarily, users are continuously authenticated, ensuring that the individual in front of the computer screen or at a kiosk is the same authorized person who logged in.

24.5 Surveillance

Like security applications in public places, surveillance by face recognition systems has a low user satisfaction level, if not lower. Unconstrained lighting conditions, face orientations and other factors all make the deployment of face recognition systems for large scale surveillance a challenging task. The following are some examples of face-based surveillance.

1. In 1998 Visionics FaceIt technology was deployed for the first time to enhance town center surveillance in Newham Borough of London, which has 300 cameras linked to the closed circuit TV (CCTV) control room. The city council claims that the technology has helped to achieve a 34% drop in crime since its installation. Similar systems are in place in Birmingham, England. In 1999 Visionics was awarded a contract from National Institute of Justice to develop smart CCTV technology [12].
2. Tampa, Florida police use video cameras and face recognition software to scan the streets in search of sex offenders. FaceIt provided by Visionics quickly compares the face of a target against a database of people wanted on active warrants from the Hillsborough Sheriff's Office and a list of sex offenders maintained by the Florida Department of Law Enforcement. When the FaceIt system comes up with a close match, cops using it in a remote location can contact others on the street via radio and instruct them to do further checking.
3. Virginia Beach, Virginia is the second U.S. city to install the FaceIt system on its public streets to scan pedestrian's faces to compare with 2500 images of people with outstanding warrants, missing persons, and runaways.
4. In New York City, the National Park Service deployed a face recognition surveillance system for the security of the Statue of Liberty. The system, including two cameras mounted on tripods, at the ferry dock where visitors leave Manhattan for Liberty Island, takes pictures of visitors and compares them with a database of terror suspects. The cameras are focused on the line of tourists waiting to board the ferry, immediately before they pass through a bank of metal detectors.

24.6 Smart Cards

The Smart Card has an embedded microprocessor or memory chip that provides the processing power to serve many applications. Memory cards simply store data. A microprocessor card, on the other hand, can add, delete, and manipulate information in its memory on the card. A microprocessor card also has built-in security features. Contact-less smart cards contain a small antenna so the card reader detects the card from a distance. The Smart Card's portability and ability to be updated make it a technology well suited for securely connecting the virtual and physical worlds.

The application of face recognition technology in smart cards, in essence, is a combination of the two. This can be seen from the following two examples. Smart

cards store the mathematical characteristics of the faces during the enrollment stage. The characteristics are read out during the verification stage for comparison with the live capture of the person's face. If granted, the person can have his stored facial characteristics updated in the card's memory.

1. Maximus [26] coupled face recognition system with fingerprint technology to construct a smart card designed to help airline passengers quickly clear security. To get a smart card, one needs to submit to a background check and register his or her facial and fingerprint characteristics. Biometric readers, presumably set up in specially designated "fast lanes," then verify his or her identification.
2. The ZN-Face system [19], which combines face recognition and smart card technology, is used for protecting secure areas at Berlin airports. Potential threats posed by criminals who often succeed in entering high security areas by means of a suitable disguise (e.g., pilot uniforms) are ruled out effectively. The individual's face characteristics are stored on a smart card; ZN-Face compares and verifies the card information with the face readings at each access station.

Smart cards are used mainly in a face verification scenario. The accuracy of the similarity calculation between the face characteristics stored in the cards and the live-captured face depends on the elapsed time between the two images. With a timely update of the face characteristics, this elapsed time can be kept short. High user satisfaction level can be achieved for a small database of faces.

24.7 Law Enforcement

With a face recognition and retrieval program, investigators can find a suspect quickly. Face recognition technology empowers the law enforcement agencies with the ability to search and identify suspects quickly even with incomplete information of their identity, sometimes even with a sketch from a witness's recollection. Owing to the difficulty of obtaining good-quality face images of the criminals, the system performance is rather low. However, automatic face recognition is playing increasingly important role in assisting the police departments. Some examples in this category of applications are as follows:

1. A law enforcement system by Imigis provides the Huntington Beach, California's police officers and detectives with current arrest information and photographs, readily available by using laptops, Internet protocols, and secure wireless delivery and communication [18]. The Imagis system includes biometric facial recognition, and image and database management, giving officers invaluable investigative tools in their law enforcement and surveillance work. With this face recognition and retrieval program, investigators no longer have to spend hundreds of hours trying to identify a suspect. Now detectives can take a suspect composite and systematically search any digital database of booking images to identify possible suspects. Similarly, a suspect's image caught on a bank or convenience store surveillance video can be matched against a digital photo database

for possible identification. With a face ID interface on a county booking system, officers are able to utilize this face-recognition technology at the time of booking to immediately identify a criminal with multiple identities or outstanding warrants. Detectives can also use face ID to search for suspects in a database of registered sex offenders. It allows witnesses to identify specific features of various faces as a means to query a large database of images. This function enhances the crime resolution process by eliminating the need for witnesses to search large mug-shot books one image at a time.

2. When deployed in a casino environment, an intelligent surveillance and patron management system supported by Imagis's face recognition technology [17] allows casino operators to identify and exclude certain individuals from specific properties. Using a database of North American undesirable patrons or self-barred gamblers, casinos receive a highly effective security solution that can rapidly identify persons entering or playing in casinos. It not only can conduct face recognition searches from images captured through existing surveillance cameras against an internal database, a casino can also widen the identification search to the national database.

24.8 Face Databases

During the early 1990s, because of the emergence of large image databases, difficulties faced by the text-based image retrieval became more and more acute [32]. Content-based image retrieval tries to solve the difficulties faced by text-based image retrieval. Instead of being manually annotated by text-based keywords, images would be indexed by their own visual content, such as color and texture. Feature vector is the basis of content-based image retrieval, which captures image properties such as color and texture. However, these general features have their own limitations. Recently, researchers have tried to combine it with other image analysis technologies, such as face detection and recognition, to improve the retrieval accuracy. For example, web-based face recognition has been used in social-computer sites such as Facebook, Google's Picasa web album, and Microsoft's Windows Live Gallery. These applications use facial scanning and recognition algorithms to scan through a person's online photos and those public photos belonging to his/her friends in order to identify and suggest tags for the untagged people within them [9]. Although face recognition techniques have been mainly used to retrieve and index faces in face-only databases (e.g., searching mug-shot databases of criminals), recently these techniques have also been used for other databases containing both faces and nonfaces (e.g., personal photo albums).

The performance of these retrieval systems is still low because the size of face database is normally large and the face pictures are captured under unconstrained conditions.

24.8.1 Using Faces to Assist Content-Based Image Retrieval

A personal digital photo album has many images that have either human faces or no human faces. Deciding whether an image contains a face can be a preprocessing step to limit the range of search space for a given image query. FotoFile [20] is one of the systems that tries to support this functionality to make the management of personal photo albums easier. This system also blends human and automatic annotation methods. Fotofile offers a number of techniques that make it easier for a consumer to annotate the content manually and to fit the annotation task more naturally into the flow of activities that consumers find enjoyable. The use of automated feature extraction tools enables FotoFile to generate some of the annotation that would otherwise have to be manually entered. It also provides novel capabilities for content creation and organization.

When presented with photos that contain faces of new people, the face recognition system attempts to match the identity of the face. The user either corrects or confirms the choice; the system then can match faces to their correct identities more accurately in subsequent photos. Once a face is matched to a name, that name is assigned as an annotation to all subsequently presented photos that contain faces that match the original. To handle the false positives and false negatives of the face recognition system, a user must confirm face matches before the annotations associated with these faces are validated.

24.8.2 Using Content-Based Image Retrieval Techniques to Search Faces

The content-based retrieval of faces has multiple applications that exploit existing face databases. One of the most important tasks is the problem of searching a face without its explicit image, only its remembrance. Navarrete and del Solar [27] used the so-called relevance feedback approach. Under this approach, previous human computer interactions are employed to refine subsequent queries, which iteratively approximate the wishes of the user. This idea is implemented using self-organizing maps. In particular, their system uses a tree-structured self-organizing map (TS-SOM) for auto-organizing the face images in the database. Similar face images are located in neighboring positions of the TS-SOM.

To know the location of the requested face in the map, the user is asked to select face images he considers to be similar to the requested one from a given set of face images. The system then shows the new images, which have neighboring positions, with respect to the ones selected by the user. The user and the retrieval system iterate until the interaction process converges (i.e., the requested face image is found). This retrieval system in shown in Fig. 24.4, and a real example of the interactive face-retrieval process is shown in Fig. 24.5.

Eickeler and Birlinghoven [8] explored the face database retrieval capabilities of a face recognition system based on the hidden Markov model. This method is able

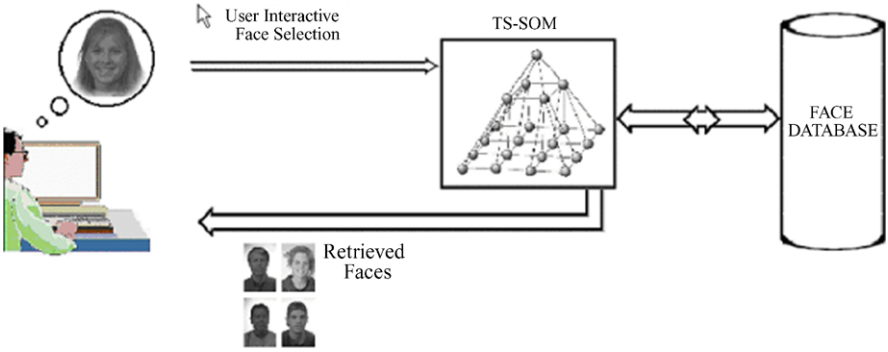

Fig. 24.4 Interface of the SOM system

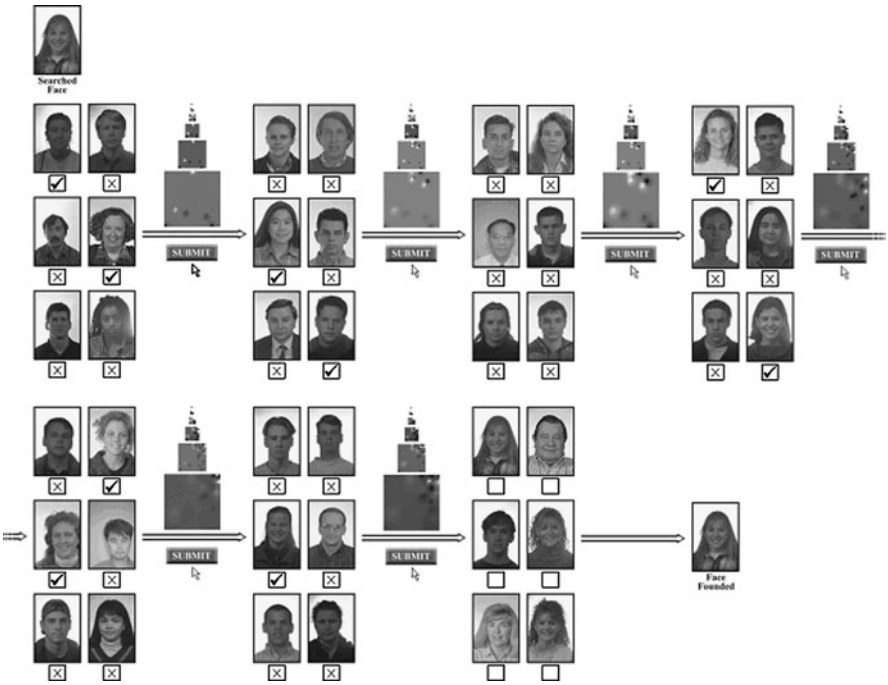

Fig. 24.5 Face retrieval using the SOM system

to work on a large database. Experiments carried out on a database of 25 000 face images show that this method is suitable for retrieval on a large face database. Martinez [25] presented a different approach to indexing face images. This approach is based on identifying frontal faces and allows reasonable variability in facial expressions, illumination conditions, and occlusions caused by eyewear or items of clothing such as scarves. The face recognition system of this approach is also based on the hidden Markov model [8].

24.8.3 Photo Tagging

Face recognition has been used to tag faces found in photographs. Apple's iPhoto and Google's Picasa software allows a user to search and/or tag his/her personal collection of photos based on a tagged photo. Moreover, companies such as face.com specializing in face recognition techniques have introduced software to search and/or tag larger online photo repositories on social networking sites such as Facebook and Twitter. For example, one application of face.com's software is for finding lost photos of a user and his/her friends on Facebook sites [9].

24.9 Multimedia Management

Human faces are frequently seen in news, sports, films, home video, and other multimedia content. Indexing this multimedia content by face detection, face tracking, face recognition, and face change detection is important to generate segments of coherent video content for video browsing, skimming and, summarization. Together with speech recognition, natural language processing, and other image understanding techniques, face processing is a powerful tool for automatic indexing, retrieval, and access to the ever-growing digital multimedia content.

One difficulty of directly using face recognition in multimedia applications is that usually the gallery set is not available. The identity of the person whose face has been detected must be obtained through the multimedia content itself. Houghton [15] developed a "face-naming" method. His method finds names in Web pages associated with the broadcast television stations using three text processing methods and names in images using the optical character recognition (OCR) technique. The names are then linked to the faces detected in the images. The face detector is the FaceIt [11]. In this way, a gallery set is created. Queried about an image without a name, the "face-naming" system compares the faces in the image with the gallery and returns the identity of the face.

Ma and Zhang [24] developed an interactive user interface to let the user annotate a set of video segments that the face recognizer concludes to be belonging to the same nonenrolled person. They have used the face detection algorithm [31] to detect faces to help to extract key frames for indexing and browsing home video. Chan et al. [4] used face recognition techniques to browse video databases to find shots of particular people.

One integrated multimedia management system is the "Infomedia" project at Carnegie Mellon University [34]. This project aims to create an information digital video library to enhance learning for people of all ages. Thousands of hours of video content is indexed and archived for search and retrieval by users via desktop computers through computer networks. One of its indexing schemes is the face detection developed by Rowley et al. [31]. The detected human faces and text are used as a basis for significance during the creation of video segments. A small number of face images can be extracted to represent the entire segment of video containing an

individual for video summarization purposes. It supports queries such as "find video with talking heads" supported by face detection, "find interviews by Tim Russert" supported by face detection and video text recognition, and so on.

Another system is a multilingual, multimodal digital video library system, called iVIEW, developed at the Chinese University of Hong Kong [23]. Its face recognition scheme is similar to the one in Houghton's article [15]. Faces detected are cross-referenced with the names detected by OCR on on-screen words. iVIEW is designed on Web-based architecture with flexible client server interaction. It supports access to both English and Chinese video contents. It also supports access via wired and wireless networks.

Wang and Chang [35] developed a system for real-time detection, tracking, and summarization of human faces in the video compressed domain at Columbia University. Their face detection component uses the MPEG compressed data to detect face objects and refine the results by tracking the movement of faces. The summaries of people appearance in the spatial and temporal dimensions help users to understand the interaction among people.

Because the orientation of faces or lighting conditions in most of the multimedia content is seldom controlled, face recognition accuracy is relatively low.

24.10 Human Computer Interaction

To achieve efficient and user-friendly human computer interaction, human body parts (e.g., the face) could be considered as a natural input "device". This has motivated research on tracking, analyzing, and recognizing human body movements.

24.10.1 Face Tracking

Although the goal of such interfaces is to recognize and understand human body movements, the first step to achieve this goal is to reliably localize and track such human body parts as the face and the hand. Skin color offers a strong cue for efficient localization and tracking of human body parts in video sequences for vision-based human computer interaction. Color-based target localization could be achieved by analyzing segmented skin color regions. Although some work has been done on adaptive color models, this problem still needs further study. Wu and Huang [36] presented their investigation of color-based image segmentation and nonstationary color-based target tracking by studying two representations for color distributions. Based on the so-called D-EM algorithm, they implemented a nonstationary color tracking system. Figure 24.6 shows an example of face localization and tracking in a typical laboratory environment.

Fig. 24.6 Tracking results based on color model

24.10.2 Emotion Recognition

It is argued that for the computer to be able to interact with humans it must have the communication skills of humans, and one of these skills is the ability to understand the emotional state of the person. The most expressive way humans display emotions is through facial expressions. Cohen et al. [7] reported on several advances they have made in building a system for classifying facial expressions from continuous video input. They used Bayesian network classifiers for classifying expressions from video. Figure 24.7 shows four examples of real-time expression recognition. The labels show the recognized emotion of the user.

24.10.3 Face Synthesis and Animation

A realistic three dimensional head model is one of the key factors in natural human computer interaction. A graphics-based human model provides an effective solution for information display, especially in collaborative environments. Examples include 3D model-based very low bit-rate video coding for visual telecommunication, audio/visual speech recognition, and talking head representation of computer agents. In noisy environments, the synthetic talking face can help users understand the associated speech, and it helps people react more positively during interactive sessions. It has been shown that a virtual sales agent inspires confidence in customers in the case of e-commerce, and a synthetic talking face enables students to learn better in computer-aided education [14].

Hong et al. [14] have successfully designed a system, called iFACE, that provides functionalities for face modeling and animation. The 3D geometry of a face is

Fig. 24.7 Emotion recognition results

modeled by a triangular mesh. A few control points are defined on the face mesh. By dragging the control points, the user can construct different facial shapes. Two kinds of media, text stream and speech stream, can be used to drive the face animation. A display of the speech-driven talking head is shown in Fig. 24.8.

24.11 Other Applications

Many of the application scenarios in this section require close collaboration between face recognition systems and domain experts. The face recognition systems assist the domain experts.

- **Antique photo verification.** It is of great value for historians, biographers, and antique collectors to verify whether an antique photo of a person is genuine, given a true photo taken when that person is much older. The age difference and sometimes the low quality of the antique photo pose a great challenge for the face recognition systems.
- **Face images transmission.** Li et al. [21] coded the face images with a compact parameterized model for low bandwidth communication applications, such as videophone and teleconferencing. Instead of sending face images or video,

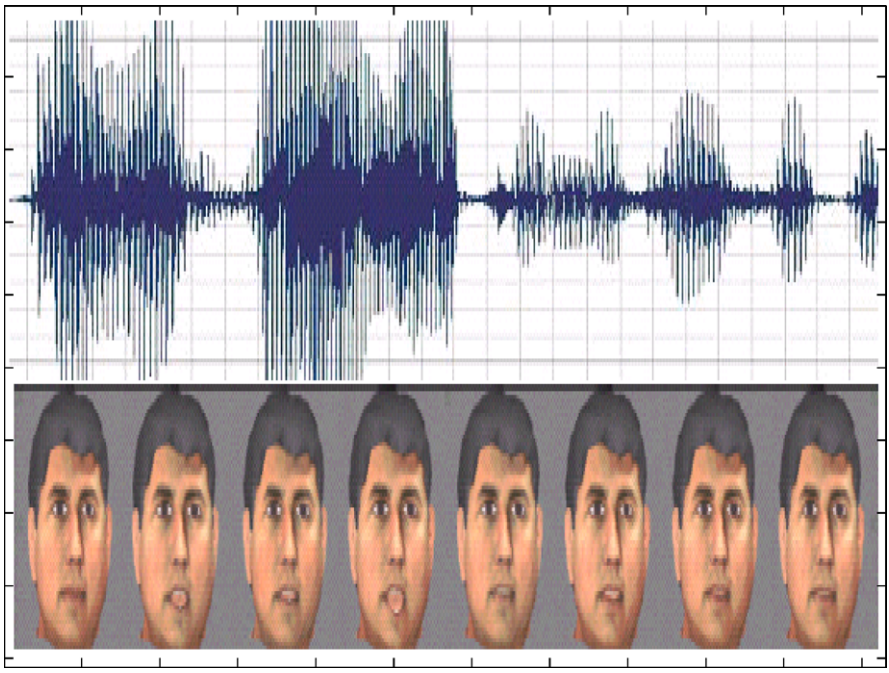

Fig. 24.8 Speech driven face animation

they send robust feature representation of the faces to the other end of the channel so that by fitting a generic face model to the face feature representation a good reconstruction of the original face images can be achieved. Similarly, Lyons et al. [22] developed an algorithm that can automatically extract a face from an image, modify it, characterize it in terms of high-level properties, and apply it to the creation of a personalized avatar in an online Japanese sumo game application. The algorithm has potential applications in educational systems (virtual museums or classrooms) and in entertainment technology (e.g., interactive movies, multiple user role-playing communities).

- Chellappa et al. [5] listed several application scenarios that involve close collaboration between the face recognition system and the user or image domain expert. The interaction between the algorithms and known results in psychophysics and neuroscience studies is needed in these applications. We summarize these applications below; for detailed information see Chellappa et al. [5].

  1. "Expert Identification": An expert confirms that the face in the given image corresponds to the person in question. Typically, in this application a list of similar looking faces is generated using a face identification algorithm. The expert then performs a careful analysis of the listed faces.
  2. "Witness Face Reconstruction": The witness is asked to compose a picture of a culprit using a library of features such as noses, eyes, lips, and so on. The "sketch" by the user is compared with all the images in the database to find the

closest matches. The witness can refine the "sketch" based on these matches. A face recognition algorithm can recompute the closest matches in the hope of finding the real culprit.

3. "Electronic Lineup": A witness identifies a face from a set of face images that include some false candidates. This set of images can be the results from the "Witness Face Reconstruction" application by the face recognition algorithm.
4. "Reconstruction of Face from Remains" and "Computerized Aging": Available face images are transformed to what a face could have been or what the face will be after some time.

24.12 Limitations of Current Face Recognition Systems

Although face recognition technology has great potential in the applications reviewed above, currently the scope of the application is still quite limited. There are at least two challenges that need to be addressed to deploy them in large-scale applications.

1. Face recognition technology is still not robust enough, especially in unconstrained environments, and recognition accuracy is still not acceptable, especially for large-scale applications. Lighting changes, pose changes, and time difference between the probe image and the gallery image(s) further degrade the performance. These factors have been evaluated in FRVT 2002 using some of the best commercial systems [29]. For example, in a verification test with reasonably controlled indoor lighting, when the gallery consisted of 37 437 individuals with one image per person and the probe set consisted of 74 854 probes with two images per person, the best three systems, on average, achieved a verification rate of 90% at a false alarm rate of 1%, 80% at a false alarm rate of 0.1%, and 70% at a false alarm rate of 0.01%. Although good progress has been made to increase the verification rate from 80% to 99% at a false alarm rate of 0.1%, as reported in FRVT 2006 [30], this level of accuracy may be (or may not be) suitable for an access control system with a small database of hundreds of people but not for a security system at airports where the number of passengers is much larger. When evaluating the performance with respect to pose change, with a database of 87 individuals the best system can achieve an identification rate of only 42% for faces with $\pm 45^\circ$ left or right pose differences and 53% with $\pm 45^\circ$ up or down pose differences. The elapsed time between the database and test images degrades performance at a rate of 5% per year of difference. Lighting changes between probe images obtained outdoors and gallery images taken indoors degrades the best systems, from a verification rate of 90% to around 60% at a false accept rate of 1%. The test results in FRVT 2002 can partly explain why several systems installed at airports and other public places have not received positive feedback based on their poor performance. One example is that the crowd surveillance system tested by Tampa, Florida police reported 14 instances of a possible criminal match in a 4-day session, but they were all false alarms. The Tampa police department has abandoned the system.

2. The deployment of face recognition-based surveillance systems has raised concerns of possible privacy violation. For example, the American Civil Liberties Union (ACLU) opposes the use of face recognition software at airports due to ineffectiveness and privacy concern [1]. In addition to listing several factors affecting the face recognition accuracy, such as change of hairstyle, weight gain, or loss, eye glasses or disguise, the ACLU opposes face recognition because "facial recognition technology carries the danger that its use will evolve into a widespread tool for spying on citizens as they move about in public places."

24.13 Conclusions

We reviewed many face recognition systems in various application scenarios. We also pointed out the limitations of the current face recognition technology. The technology has evolved from laboratory research to many small-, medium- or, large-scale commercial deployments. At present, it is most promising for small- or medium-scale applications, such as office access control and computer log in; it still faces great technical challenges for large-scale deployments such as airport security and general surveillance. With more research collaborations worldwide between universities and industrial researchers, the technology will become more reliable and robust.

Another direction for improving recognition accuracy lies in a combination of multiple biometrics and security methods. It can work with other biometrics such as voice-based speaker identification, fingerprint recognition, and iris scan in many applications. For security purpose at airports, face recognition systems can also work together with X-ray luggage scanners, metal detectors, and chemical trace detectors at security checkpoints.

This chapter concludes with the following description of how face recognition could be used in our daily lives in the near future, although some of them are already in place.

If we drive to work, a face recognizer installed in the car will decide whether to authorize our usage of the vehicle before starting the engine. If we choose to take a bus or subway to work, our prepaid boarding pass will be verified by a face recognizer comparing the photo on the pass and live captured pictures of our faces. At the entrance of the office building, we go through a face recognition based access control system that compares our face images with those in its database. We sit down in front of the office computer, a face recognizer in it runs its face recognition algorithm before we log on. when we go to a secure area in the office building, the security check is carried out by another face recognizer. On a business trip, when we use the smart ATM, we are subject to a face recognizer of the bank system. At the airport, our boarding pass and passport or identity card are screened by the airport's face recognizer for passenger security purpose. When we go to a retail store, restaurant, or a movie theater, the cameras equipped with cash registers would be aimed at our faces to compare our pictures with those in a customer database to identify us, if not, we could complete the purchase by using a PIN (personal identification

number). After the cash register had calculated the total sale, the face recognition system would verify us and the total amount of the sales would be deducted from our bank accounts [16]. When we go back home, a face recognition based home security system makes sure we are living in the house before we open the door.

Acknowledgements We sincerely thank Dr. Ying Wu, Northwestern University, Dr. Lawrence Chen, Kodak Research Lab, Dr. Javier Ruiz-del-Solar, Universidad de Chile, Chile, and Dr. Julian L. Center, Jr., Lau Technologies for providing some of the pictures and their permission to use them in the paper. We also want to thank Dr. Anil K. Jain, Michigan State University for giving us helpful suggestions on improving the manuscript.

References

1. ACLU. http://archive.aclu.org/features/f110101a.html
2. Bryliuk, D., Starovoitov, V.: Access control by face recognition using neural networks and negative examples. In: Proceedings of the 2nd International Conference on Artificial Intelligence, pp. 428–436 (2002)
3. Bunney, C.: Survey: face recognition systems. Biom. Technol. Today 8–12 (1997)
4. Chan, Y., Lin, S.-H., Kung, S.: Video indexing and retrieval. In: Sheu, B.J., Ismail, M., Wang, M.Y., Tsai, R.H. (eds.) Multimedia Technology for Applications. Wiley, New York (1998)
5. Chellappa, R., Wilson, C., Sirohey, S.: Human and machine recognition of faces: a survey. Proc. IEEE **83**(5), 704–740 (1995)
6. Cognitec. http://www.cognitec-systems.de/index.html
7. Cohen, I., Sebe, N., Cozman, F.G., Cirelo, M.C., Huang, T.: Learning Bayesian network classifiers for facial expression recognition using both labeled and unlabeled data. In: Proceedings of the IEEE Int. Conf. on Computer Vision and Pattern Recognition (CVPR 2003) (2003)
8. Eickeler, S., Birlinghoven, S.: Face database retrieval using pseudo 2D hidden Markov models. In: Proceeding of IEEE Int. Conf. on Face and Gestures (FG 2002) (2002)
9. Facebook facial-recognition tagger goes live. http://blogs.wsj.com/digits/2009/11/11/facebook-facial-recognition-tagger-goes-live
10. FaceGate. http://www.premierelect.co.uk/faceaccess.html
11. FaceIt. http://www.identix.com
12. FaceIt-Hist. http://www.identix.com/company/comp_history.html
13. FaceKey. http://www.facekey.com
14. Hong, P., Wen, Z., Huang, T.: IFace: a 3D synthetic talking face. Int. J. Image Graph. **1**(1), 19–26 (2001)
15. Houghton, R.: Named faces: putting names to faces. IEEE Intell. Syst. **14**(5), 45–50 (1999)
16. http://en.wikipedia.org/wiki/Facial_recognition_system
17. Imagis. http://www.imagistechnologies.com
18. Imagis-Beach. http://cipherwar.com/news/01/imagis_big_brother.htm
19. Konen, W., Schulze-Krüger, E.: ZN-face: a system for access control using automated face recognition. In: Proceedings of the International Workshop on Automatic Face and Gesture Recognition, pp. 18–23 (1995)
20. Kudhinsky, A., Pering, C., Creech, M.L., Freeze, D., Serra, B., Gvvizdka, J.: FotoFile: a consumer multimedia organization and retrieval system. In: Proceedings of CHI'99, pp. 496–503 (1999)
21. Li, H., Roivainen, P., Forchheimer, R.: 3D motion estimation in model-based facial image coding. IEEE Trans. Pattern Anal. Mach. Intell. **15**(6), 545–555 (1993)
22. Lyons, M., Plante, A., Jehan, S., Inoue, S., Akamatsu, S.: Avatar creation using automatic face recognition. In: Proceedings, ACM Multimedia 98, pp. 427–434 (1998)

23. Lyu, M.R., Yau, E., Sze, S.: A multilingual, multimodal digital video library system. In: ACM/IEEE Joint Conference on Digital Libraries, JCDL 2002, Proceedings, pp. 145–153 (2002)
24. Ma, W.-Y., Zhang, H.: An indexing and browsing system for home video. In: Proc. of 10th European Signal Processing Conference (2000)
25. Martinez, A.: Face image retrieval using HMMs. In: Proceedings of the IEEE Workshop on Content-Based Access of Image and Video Libraries (1999)
26. Maximus. http://www.maximus.com/corporate/pages/smartcardsvs
27. Navarrete, P., del Solar, J.: Interactive face retrieval using self-organizing maps. In: Proceedings, 2002 Int. Joint Conf. on Neural Networks: IJCNN2002 (2002)
28. Omron. http://www.omron.com
29. Phillips, P., Grother, P., Michaels, R., Blackburn, D., Tabassi, E., Bone, M.: Face recognition vendor test 2002: evaluation report. http://www.frvt.org
30. Phillips, P., Scruggs, W., O'Tools, A., Lynn, P., Bowyer, K., Schott, C., Sharpe, M.: FRVT 2006 and ICE 2006 large-scale results. http://www.frvt.org
31. Rowley, H., Baluja, S., Kanade, T.: Neural network-based face detection. IEEE Trans. Pattern Anal. Mach. Intell. **20**, 22–38 (1998)
32. Rui, Y., Huang, T.S., Chang, S.-F.: Image retrieval: current techniques, promising directions and open issues. J. Vis. Commun. Image Represent. **10**(4), 39–62 (1999)
33. Viisage. http://www.viisage.com
34. Wactlar, H., Smith, T.K.M., Stevens, S.: Intelligence access to digital video: informedia project. Computer **29**(5), 46–52 (1996)
35. Wang, H., Chang, S.-F.: A highly efficient system for automatic face region detection in mpeg video sequences. IEEE Trans. Circuits Syst. Video Technol. **7**(4), 615–628 (1997). Special Issue on Multimedia Systems and Technologies
36. Wu, Y., Huang, T.: Nonstationary color tracking for vision-based human computer interaction. IEEE Trans. Neural Netw. **13**(4) (2002)
37. Xiong, Z., Chen, Y., Wang, R., Huang, T.: Improved information maximization based face and facial feature detection from real-time video and application in a multi-modal person identification system. In: Proceedings of the Fourth International Conference on Multimodal Interfaces (ICMI'2002), pp. 511–516 (2002)
38. Zhao, W., Chellappa, R., Rosenfelda, A., Phillips, J.: Face recognition: a literature survey. Technical Report, CS-TR4167R, University of Maryland (2000)