Facial recognition system

Abstract:

Recently face recognition is attracting much attention in the society of network multimedia information access. Areas such as network security, content indexing and retrieval, and video compression benefits from face recognition technology because "people" are the center of attention in a lot of video. Network access control via face recognition not only makes hackers virtually impossible to steal one's "password", but also increases the user-friendliness in human-computer interaction. Indexing and/or retrieving video data based on the appearances of particular persons will be useful for users such as news reporters, political scientists, and moviegoers. For the applications of videophone and teleconferencing, the assistance of face recognition also provides a more efficient coding scheme. In this paper, we give an introductory course of this new information processing technology. The paper shows the readers the generic framework for the face recognition system, and the variants that are frequently encountered by the face recognizer. Several famous face recognition algorithms, such as eigenfaces and neural networks, will also be explained. This project is able to recognize a person’s face by comparing facial structure to that of a known person.

This is achieved by using forward facing photographs of individuals to render a two-dimensional representation of a human head. The system then projects the image onto a “face space” composed of a complete basis of “eigenfaces.” Because of the similarity of face shape and features from person to person, face images fall within a relatively small region of the image space and as such can be reproduced with less than complete knowledge of the image space. When new images are fed into this system it can identify the person with a high rate of success with the robustness to identify correctly even in the presence of some image distortions.
Introduction

In today's networked world, the need to maintain the security of information or physical property is becoming both increasingly important and increasingly difficult. From time to time we hear about the crimes of credit card fraud, computer breakin's by hackers, or security breaches in a company or government building. In the year 1998, sophisticated cyber crooks caused well over US $100 million in losses (Reuters, 1999). In most of these crimes, the criminals were taking advantage of a fundamental flaw in the conventional access control systems: the systems do not grant access by "who we are", but by "what we have", such as ID cards, keys, passwords, PIN numbers, or mother's maiden name. None of these means are really define us. Rather, they merely are means to authenticate us. It goes without saying that if someone steals, duplicates, or acquires these identity means, he or she will be able to access our data or our personal property any time they want. Recently, technology became available to allow verification of "true" individual identity. This technology is based in a field called "biometrics". Biometric access control are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as fingerprints or facial features, or some aspects of the person's behavior, like his/her handwriting style or keystroke patterns.

Since biometric systems identify a person by biological characteristics, they are difficult to forge. Among the various biometric ID methods, the physiological methods (fingerprint, face, DNA) are more stable than methods in behavioral category (keystroke, voice print). The reason is that physiological features are often non-alterable except by severe injury. The behavioral patterns, on the other hand, may fluctuate due to stress, fatigue, or illness. However, behavioral IDs have the advantage of being nonintrusiveness. People are more comfortable signing their names or speaking to a microphone than placing their eyes before a scanner or giving a drop of blood for DNA sequencing. Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. It has the accuracy of a physiological approach without being intrusive.
**Definition of face recognition**

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. The ability to recognize people by their facial characteristics. The most advanced technology is based on the Eigenface algorithm, which maps the characteristics of a person's face into a multidimensional face space. Computers can conduct facial database searches and/or perform live, one-to-one or one-to-many verifications with unprecedented accuracy and split-second processing. Users can be granted secure access to their computer, mobile devices, or for online e-commerce, simply by looking into their Webcam.

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other. Typical sources of images for use in facial recognition include video camera signals and pre-existing photos such as those in driver's license databases.

**Database**

A database management system (DBMS) is computer software that manages databases. DBMSes may use any of a variety of database models, such as the network model or relational model. In large systems, a DBMS allows users and other software to store and retrieve data in a structured way.

**Biometrics**

It refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.
Biometric characteristics can be divided in two main classes:

- **Physiological** are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent.

- **Behavioral** are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term *behaviometrics* for this class of biometrics.

Strictly speaking, voice is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

**History of Face Recognition**

The subject of face recognition is as old as computer vision, both because of the practical importance of the topic and theoretical interest from cognitive scientists. Despite the fact that other methods of identification (such as fingerprints, or iris scans) can be more accurate, face recognition has always remained a major focus of research because of its non-invasive nature and because it is people's primary method of person identification.

Perhaps the most famous early example of a face recognition system is due to Kohonen, who demonstrated that a simple neural net could perform face recognition for aligned and normalized face images. The type of network he employed computed a face description by approximating the eigenvectors of the face image's autocorrelation matrix; these eigenvectors are now known as `eigenfaces.'

Kohonen's system was not a practical success, however, because of the need for precise alignment and normalization. In following years many researchers tried face recognition schemes based on edges, inter-feature distances, and other neural net approaches. While several were successful on small databases of aligned images, none successfully addressed the more realistic problem of large databases where the location and scale of the face is unknown.
Kirby and Sirovich (1989) [6] later introduced an algebraic manipulation which made it easy to directly calculate the eigenfaces, and showed that fewer than 100 were required to accurately code carefully aligned and normalized face images. Turk and Pentland (1991) [7] then demonstrated that the residual error when coding using the eigenfaces could be used both to detect faces in cluttered natural imagery, and to determine the precise location and scale of faces in an image. They then demonstrated that by coupling this method for detecting and localizing faces with the eigenface recognition method, one could achieve reliable, real-time recognition of faces in a minimally constrained environment. This demonstration that simple, real-time pattern recognition techniques could be combined to create a useful system sparked an explosion of interest in the topic of face recognition.

Techniques

➢ Traditional

Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data. Popular recognition algorithms include eigenface, fisherface, the Hidden Markov model, and the neuronal motivated dynamic link matching.

Eigenface

Eigenfaces are a set of eigenvectors used in the computer vision problem of human face recognition. The approach of using eigenfaces for recognition was developed by Sirovich and Kirby (1987) and used by Matthew Turk and Alex Pentland in face classification. It is considered the first successful example of facial recognition technology. These eigenvectors are derived from the covariance matrix of the
probability distribution of the high-dimensional vector space of possible faces of human beings.

Dynamic link matching

Dynamic link matching is a neuronal model for face recognition. It uses wavelet transformations to encode incoming image data. Bunch graph matching is an algorithm based on many ideas found in dynamic link matching.

- **3-D**

A newly emerging trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. This technique uses 3-D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.

One advantage of 3-D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view.

**Three-dimensional face recognition**

Three-dimensional face recognition (3D face recognition) is a modality of facial recognition methods in which the three-dimensional geometry of the human face is used. It has been shown that 3D face recognition methods can achieve significantly higher accuracy than their 2D counterparts, rivaling fingerprint recognition.

3D face recognition has the potential to achieve better accuracy than its 2D counterpart by measuring geometry of rigid features on the face. This avoids such pitfalls of 2D face recognition algorithms as change in lighting, different facial expressions, make-up and head orientation. Another approach is to use the 3D model to improve accuracy of traditional image based recognition by transforming the head into a known view. Additionally, most range scanners acquire both a 3D mesh and the corresponding texture.
The main technological limitation of 3D face recognition methods is the acquisition of 3D images, which usually requires a range camera. This is also a reason why 3D face recognition methods have emerged significantly later (in the late 1980s) than 2D methods. Recently commercial solutions have implemented depth perception by projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. This allows for good recognition accuracy with low cost off-the-shelf components.

Currently, 3D face recognition is still an open research field, though several vendors already offer commercial solutions. The first international workshop to deal specifically with 3D face processing will be held at CVPR 2008.

➢ Skin texture analysis

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person’s skin into a mathematical space. Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent.

➢ Notable users and deployments

The London Borough of Newham, in the UK, previously trialled a facial recognition system built into their borough-wide CCTV system.

The German Federal Police use a facial recognition system to allow voluntary subscribers to pass fully automated border controls at Frankfurt Rhein-Main international airport. Subscribers need to be European Union or Swiss citizens Recognition system are also used by casinos to catch card counters and other blacklisted individuals.
The Australian Customs Service has an automated border processing system called SmartGate that uses facial recognition. The system compares the face of the individual with the image in the e-passport microchip, certifying that the holder of the passport is the rightful owner.

Pennsylvania Justice Network searches crime scene photographs and CCTV footage in the mugshot database of previous arrests. A number of cold cases have been resolved since the system became operational in 2005. Other law enforcement agencies in the USA and abroad use arrest mugshot databases in their forensic investigative work. U.S. Department of State operates one of the largest face recognition systems in the world with over 75 million photographs that is actively used for visa processing. Spaceship Earth in EPCOT uses this for the touch screen part of the ride.

**Card counting**

**Card counting** is a card game strategy used to determine when a player has a probability advantage. The term is used almost exclusively to refer to the tracking of the ratio of high cards to low cards in blackjack and its derivatives such as Spanish 21, although it is sometimes used to refer to obtaining a count of the distribution or remaining high cards in trick-taking games, such as contract bridge or spades. This article deals only with card counting as it applies to blackjack and its derivatives.

➢ **Additional uses**

In addition to being used for security systems, authorities have found a number of other applications for facial recognition systems. While earlier post 9/11 deployments were well publicized trials, more recent deployments are rarely written about due to their covert nature.

At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida, used Identix’s facial recognition software, FaceIt, to search for potential criminals and terrorists in attendance at the event.\(^5\) (it found 19 people with pending arrest warrants)\(^8\)
In the 2000 presidential election, the Mexican government employed facial recognition software to prevent voter fraud. Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new facial images to those already in the voter database, authorities were able to reduce duplicate registrations.\[^9\] Similar technologies are being used in the United States to prevent people from obtaining fake identification cards and driver’s licenses.\[^10\][^11]\]

There are also a number of potential uses for facial recognition that are currently being developed. For example, the technology could be used as a security measure at ATM’s; instead of using a bank card or personal identification number, the ATM would capture an image of your face, and compare it to your photo in the bank database to confirm your identity. This same concept could also be applied to computers; by using a webcam to capture a digital image of yourself, your face could replace your password as a means to log-in.

As part of the investigation of the Disappearance of Madeleine McCann the British police are calling on visitors to the Ocean Club Resort, Praia da Luz in Portugal or the surrounding areas in the two weeks leading up to the child’s disappearance on Thursday 3 May 2007 to provide copies of any photographs of people taken during their stay, in an attempt to identify the abductor using a biometric facial recognition application.

➤ **Comparative study**

Among the different biometric techniques facial recognition may not be the most reliable and efficient but its great advantage is that it does not require aid from the test subject. Properly designed systems installed in airports, multiplexes, and other public places can detect presence of criminals among the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning. However, questions have been raised on the effectiveness of facial recognition software in cases of railway and airport security.
➢ **Criticisms**

   ➢ **Weaknesses**

   Face recognition is not perfect and struggles to perform under certain conditions. Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems.

   Other conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject’s face, and low resolution images.

   ➢ **Effectiveness**

   Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system having been running for several years. "Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target."[14][15] This information seems to conflict with claims that the system was credited with a 34% reduction in crime - which better explains why the system was then rolled out to Birmingham also.[16]

   An experiment by the local police department in Tampa, Florida, had similarly disappointing results."Camera technology designed to spot potential terrorists by their facial characteristics at airports failed its first major test at Boston's Logan Airport"
Privacy concerns

Despite the potential benefits of this technology, many citizens are concerned that their privacy will be invaded. Some fear that it could lead to a “total surveillance society,” with the government and other authorities having the ability to know where you are, and what you are doing, at all times. This is not to be an underestimated concept as history has shown that states have typically abused such access before.

Recent Improvements

In 2006, the performance of the latest face recognition algorithms were evaluated in the Face Recognition Grand Challenge. High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.

Early development

Pioneers of Automated Facial Recognition include: Woody Bledsoe, Helen Chan Wolf, and Charles Bisson. During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces (Bledsoe 1966a, 1966b; Bledsoe and Chan 1965). He was proud of this work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images (in effect, a book of mug shots) and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database. Bledsoe (1966a) described the following difficulties:
This project was labeled man-machine because the human extracted the coordinates of a set of features from the photographs, which were then used by the computer for recognition. Using a graphics tablet (GRAFACON or RAND TABLET), the operator would extract the coordinates of features such as the center of pupils, the inside corner of eyes, the outside corner of eyes, point of widows peak, and so on. From these coordinates, a list of 20 distances, such as width of mouth and width of eyes, pupil to pupil, were computed. These operators could process about 40 pictures an hour. When building the database, the name of the person in the photograph was associated with the list of computed distances and stored in the computer. In the recognition phase, the set of distances was compared with the corresponding distance for each photograph, yielding a distance between the photograph and the database record. The closest records are returned.

This brief description is an oversimplification that fails in general because it is unlikely that any two pictures would match in head rotation, lean, tilt, and scale (distance from the camera). Thus, each set of distances is normalized to represent the face in a frontal orientation. To accomplish this normalization, the program first tries to determine the tilt, the lean, and the rotation. Then, using these angles, the computer undoes the effect of these transformations on the computed distances. To compute these angles, the computer must know the three-dimensional geometry of the head. Because the actual heads were unavailable, Bledsoe (1964) used a standard head derived from measurements on seven heads.

After Bledsoe left PRI in 1966, this work was continued at the Stanford Research Institute, primarily by Peter Hart. In experiments performed on a database of over 2000 photographs, the computer consistently outperformed humans when presented with the same recognition tasks (Bledsoe 1968). Peter Hart (1996) enthusiastically recalled the project with the exclamation, "It really worked!"

By about 1997, the system developed by Christoph von der Malsburg and graduate students of the University of Bochum in Germany and the University of Southern California in the United States outperformed most systems with those of Massachusetts Institute of Technology and the University of Maryland rated next. The
Bochum system was developed through funding by the United States Army Research Laboratory. The software was sold as ZN-Face and used by customers such as Deutsche Bank and operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hair styles and glasses—even sunglasses".

In about January 2007, image searches were "based on the text surrounding a photo," for example, if text nearby mentions the image content. Polar Rose technology can guess from a photograph, in about 1.5 seconds, what any individual may look like in three dimensions, and thought they "will ask users to input the names of people they recognize in photos online" to help build a database. [citation needed]

This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations.

**Future Developments-Retailing**

A possible future application for facial recognition systems lies in retailing. A retail store (for example, a grocery store) may have cash registers equipped with cameras, the cameras would be aimed at the faces of customers, so pictures of customers could be obtained. The camera would be the primary means of identifying the customer, and if visual identification failed, the customer 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 the identity of the customer, and the total amount of the sale would be deducted from the customer's bank account.
Three-dimensional face recognition

Three-dimensional face recognition (3D face recognition) is a modality of facial recognition methods in which the three-dimensional geometry of the human face is used. It has been shown that 3D face recognition methods can achieve significantly higher accuracy than their 2D counterparts, rivaling fingerprint recognition.

3D face recognition has the potential to achieve better accuracy than its 2D counterpart by measuring geometry of rigid features on the face. This avoids such pitfalls of 2D face recognition algorithms as change in lighting, different facial expressions, make-up and head orientation. Another approach is to use the 3D model to improve accuracy of traditional image based recognition by transforming the head into a known view. Additionally, most range scanners acquire both a 3D mesh and the corresponding texture. This allows combining the output of pure 3D matchers with the more traditional 2D face recognition algorithms, thus yielding better performance (as shown in FRVT 2006).

The main technological limitation of 3D face recognition methods is the acquisition of 3D images, which usually requires a range camera. This is also a reason why 3D face recognition methods have emerged significantly later (in the late 1980s) than 2D methods. Recently commercial solutions have implemented depth perception by projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. This allows for good recognition accuracy with low cost off-the-shelf components.

Currently, 3D face recognition is still an open research field, though several vendors already offer commercial solutions. The first international workshop to deal specifically with 3D face processing will be held at CVPR 2008.
Automatic number plate recognition

Automatic number plate recognition (ANPR; see also other names below) is a mass surveillance method that uses optical character recognition on images to read the licence plates on vehicles. As of 2006, systems can scan number plates at around one per second on cars travelling up to 100 mph (160 km/h). They can use existing closed-circuit television or road-rule enforcement cameras, or ones specifically designed for the task. They are used by various police forces and as a method of electronic toll collection on pay-per-use roads, and monitoring traffic activity such as red light adherence in an intersection.

ANPR can be used to store the images captured by the cameras as well as the text from the licence plate, with some configurable to store a photograph of the driver. Systems commonly use infrared lighting to allow the camera to take the picture at any time of day. A powerful flash is included in at least one version of the intersection-monitoring cameras, serving to both illuminate the picture and make the offender aware of his or her mistake. ANPR technology tends to be region specific, owing to plate variation from place to place.

Concerns about these systems have centered on privacy fears of government tracking citizens' movements and media reports of misidentification and high error rates. However, as they have developed, the systems have become much more accurate and reliable.

Eigenface

Eigenfaces are a set of eigenvectors used in the computer vision problem of human face recognition. The approach of using eigenfaces for recognition was developed by Sirovich and Kirby (1987) and used by Matthew Turk and Alex Pentland in face classification. It is considered the first successful example of facial recognition technology. These eigenvectors are derived from the covariance matrix of the probability distribution of the high-dimensional vector space of possible faces of human beings.
To generate a set of eigenfaces, a large set of digitized images of human faces, taken under the same lighting conditions, are normalized to line up the eyes and mouths. They are then all resampled at the same pixel resolution. Eigenfaces can be extracted out of the image data by means of a mathematical tool called principal component analysis (PCA).

The eigenfaces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern is how different features of a face are singled out to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth. Other eigenfaces have patterns that are less simple to identify, and the image of the eigenface may look very little like a face.

The technique used in creating eigenfaces and using them for recognition is also used outside of facial recognition. This technique is also used for handwriting analysis, lip reading, voice recognition, sign language/hand gestures and medical imaging. Therefore, some do not use the term eigenface, but prefer to use 'eigenimage'. Research that applies similar eigen techniques to sign language images has also been made.

Informally, eigenfaces are a set of "standardized face ingredients", derived from statistical analysis of many pictures of faces. Any human face can be considered to be a combination of these standard faces. For example, your face might be composed of the average face plus 10% from eigenface 1, 55% from eigenface 2, and even -3% from eigenface 3. Remarkably, it does not take many eigenfaces summed together to give a fair likeness of most faces. Also, because a person's face is no longer recorded by a digital photograph, but instead as just a list of values (one value for each eigenface in the database used), much less space is taken for each person's face.
Face perception

Face perception is the process by which the brain and mind understand and interpret the face, particularly the human face. The face is an important site for the identification of others and conveys significant social information. Probably because of the importance of its role in social interaction, psychological processes involved in face perception are known to be present from birth, to be complex, and to involve large and widely distributed areas in the brain. These parts of the brain can be damaged to cause a specific impairment in understanding faces known as prosopagnosia.

Mass surveillance

Mass surveillance is the pervasive surveillance of an entire population, or a substantial fraction thereof. Modern governments today commonly perform mass surveillance of their citizens, explaining that they believe that it is necessary to protect them from dangerous groups such as terrorists, criminals, or political subversives and to maintain social control. Mass surveillance has been widely criticized on several grounds such as violations of privacy rights, illegality, and for preventing political and social freedoms, which some fear will ultimately lead to a totalitarian state where political dissent is crushed by COINTELPRO-like programs.

Pattern recognition

Pattern recognition is a sub-topic of machine learning. It is "the act of taking in raw data and taking an action based on the category of the data". Most research in pattern recognition is about methods for supervised learning and unsupervised learning.

Pattern recognition aims to classify data (patterns) based either on a priori knowledge or on statistical information extracted from the patterns. The patterns to be classified are usually groups of measurements or observations, defining points in an appropriate multidimensional space. This is in contrast to pattern matching, where the pattern is rigidly specified.
A complete pattern recognition system consists of a sensor that gathers the observations to be classified or described, a feature extraction mechanism that computes numeric or symbolic information from the observations, and a classification or description scheme that does the actual job of classifying or describing observations, relying on the extracted features.

The classification or description scheme is usually based on the availability of a set of patterns that have already been classified or described. This set of patterns is termed the training set, and the resulting learning strategy is characterized as supervised learning. Learning can also be unsupervised, in the sense that the system is not given an a priori labeling of patterns, instead it itself establishes the classes based on the statistical regularities of the patterns.

Case-based reasoning

Case-based reasoning (CBR), broadly construed, is the process of solving new problems based on the solutions of similar past problems. An auto mechanic who fixes an engine by recalling another car that exhibited similar symptoms is using case-based reasoning. A lawyer who advocates a particular outcome in a trial based on legal precedents or a judge who creates case law is using case-based reasoning. So, too, an engineer copying working elements of nature (practicing biomimicry), is treating nature as a database of solutions to problems. Case-based reasoning is a prominent kind of analogy making.

It has been argued that case-based reasoning is not only a powerful method for computer reasoning, but also a pervasive behavior in everyday human problem solving; or, more radically, that all reasoning is based on past cases personally experienced. This view is related to prototype theory, which is most deeply explored in cognitive science.
Case-based reasoning has been formalized for purposes of computer reasoning as a four-step process:

1. Retrieve: Given a target problem, retrieve cases from memory that are relevant to solving it. A case consists of a problem, its solution, and, typically, annotations about how the solution was derived. For example, suppose Fred wants to prepare blueberry pancakes. Being a novice cook, the most relevant experience he can recall is one in which he successfully made plain pancakes. The procedure he followed for making the plain pancakes, together with justifications for decisions made along the way, constitutes Fred's retrieved case.

2. Reuse: Map the solution from the previous case to the target problem. This may involve adapting the solution as needed to fit the new situation. In the pancake example, Fred must adapt his retrieved solution to include the addition of blueberries.

3. Revise: Having mapped the previous solution to the target situation, test the new solution in the real world (or a simulation) and, if necessary, revise. Suppose Fred adapted his pancake solution by adding blueberries to the batter. After mixing, he discovers that the batter has turned blue – an undesired effect. This suggests the following revision: delay the addition of blueberries until after the batter has been ladled into the pan.

4. Retain: After the solution has been successfully adapted to the target problem, store the resulting experience as a new case in memory. Fred, accordingly, records his newfound procedure for making blueberry pancakes, thereby enriching his set of stored experiences, and better preparing him for future pancake-making demands.
Malintent

MALINTENT is technological system that was developed by the U.S. Department of Homeland Security to be implemented for detection of potential terrorist suspects. The system does various test scanning for elevated blood pressure, rapid heart and breath rate, and non-verbal cues. According to the scientists, the MALINTENT system uses a barrage of non-invasive sensors and imagers to detect and evaluate a person's facial expressions to gauge whether he or she could be planning to commit an attack or crime. In its current development, it can recognize seven primary emotions and emotional clues and will eventually have equipment which can analyze full body movement, an eye scanner and a pheromone-reader. If the sensors pick up anything considered alarming, analysts can decide whether to subject a person to questioning.

Card reader

Memory card reader is a device used for communication with a smart card or a flash memory card. A business card reader is a scanning device used to scan and electronically save business cards. A magnetic card reader is a device used to scan cards containing magnetic data strips. A punched card reader is a device used to read holes in punched cardboard cards.

Smart card readers

A smart card reader is an electronic device that reads smart cards. Some keyboards have a built-in card reader. There are external devices and internal drive bay card reader devices for PC. Some laptops have built-in smart card reader. Some have a flash upgradeable firmware. The card reader supplies the integrated circuit on the smart card with electricity. Communication is done via protocols and you can read and write to a fixed address on the card.
Memory card readers

A USB Card Reader like this one, will typically implement the USB mass storage device class. Generic CompactFlash Card Reader with high-speed storage via USB2.0A memory card reader is a device, typically having a USB interface, for accessing the data on a memory card such as a CompactFlash (CF), Secure Digital (SD) or MultiMediaCard (MMC). Most card readers also offer write capability, and together with the card, this can function as a pen drive.

Template matching

Template matching[^1] is a technique in Digital image processing for finding small parts of an image which match a template image. It can be used in manufacturing as a part of quality control,[^2] a way to navigate a mobile robot,[^3] or as a way to detect edges in images.
Conclusion

Face recognition is a both challenging and important recognition technique. Among all the biometric techniques, face recognition approach possesses one great advantage, which is its user-friendliness (or non-intrusiveness). In this paper, we have given an introductory survey for the face recognition technology. We have covered issues such as the generic framework for face recognition, factors that may affect the performance of the recognizer, and several state-of-the-art face recognition algorithms. We hope this paper can provide the readers a better understanding about face recognition, and we encourage the readers who are interested in this topic to go to the references for more detailed study.
References

2. ^ Smith, Kelly. "Face Recognition" (PDF).
3. ^ Williams, Mark. "Better Face-Recognition Software".
4. ^ McNealy, Scott. "Privacy is ( Virtually) Dead".
5. ^ "Mexican Government Adopts FaceIt Face Recognition Technology to Eliminate Duplicate
   "Oregon DMV is going to start using “facial recognition” software, a new tool in the
   prevention of fraud, required by a new state law. The law is designed to prevent someone
   from obtaining a driver license or ID card under a false name."
7. ^ Schultz, Zac. "Facial Recognition Technology Helps DMV Prevent Identity Theft". WMTV
   technology [to prevent ID theft]"
9. ^ Brown, David. "We will travel anywhere to find Madeleine, say parents" . Times Online.
    http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.htm .

^Krause, Mike (2002-01-14). "Is face recognition just high-tech snake oil?". Enter Stage Right.
http://www.enterstageright.com/archive/articles/0102/0102facerecog.htm