Biometric Authentication Systems

The remaining part of this article overviews other biometric systems.

Remaining part

PROF. A. C. SUTHAR & DR. G. R. KULKARNI

Facial Recognition

Looking in the mirror, we can observe certain distinguishable landmarks on our face. These are the peaks and valleys that make up the different facial features. These landmarks are known as nodal points. There are about 80 nodal points on a human face. Here are a few of the nodal points that are measured by the software: Distance between eyes, Width of nose, Depth of eye sockets, Cheekbones, Jaw-line and the Chin.

These nodal points are measured to create a numerical code, a string of numbers, which represents the face in a database. This code is called a faceprint.

Only 14 to 22 nodal points are needed for the FaceIt software to complete the recognition process. Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images. The basic steps followed by the FaceIt system to capture and compare images are:

- Detection - When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale

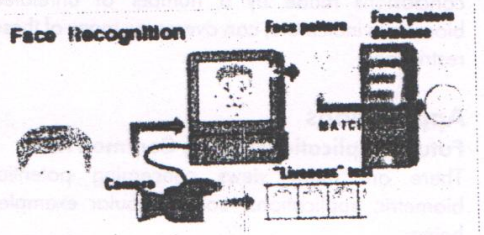

Fig. 12.

algorithm is used to search for faces in low resolution. The system switches to a high-resolution search only after a head-like shape is de ected.

- Alignment - Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it.
- Normalization -The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.
- Representation - The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.
- Matching - The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation.

The heart of the FaceIt facial recognition system shown in fig. 12 is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of face prints stored in a database. Facial recognition, like other forms of biometrics, is considered a technology that will have many uses in the near future.

Understanding Signature Verification

Signature verification is the process used to recognize an individual's hand-written signature. Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. This is done by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. As a replacement for a password or a PIN number, dynamic signature verification is a biometric technology that is used to positively identify a person from their handwritten signature. There is an important distinction between simple signature comparisons and dynamic signature verification. Both can be computerized, but a simple

comparison only takes into account what the signature looks like. Dynamic signature verification takes into account how the signature was made. With dynamic signature verification it is not the shape or look of the signature that is meaningful, it is the changes in speed, pressure and timing that occur during the act of signing. Only the original signer can recreate the changes in timing and X, Y, and Z (pressure). A pasted bitmap, a copy machine or an expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to duplicate the timing changes in X, Y and Z (pressure). There will always be slight variations in a person's handwritten signature, but the consistency created by natural motion and practice over time creates a recognizable pattern that makes the handwritten signature a natural for biometric identification.

Voice Recognition

Voice Recognition is a technology, which allows a user to use his/her voice as an input device. Voice recognition may be used to dictate text into the computer or to give commands to the computer. Voice recognition uses a neural net to "learn" to recognize your voice. As you speak, the voice

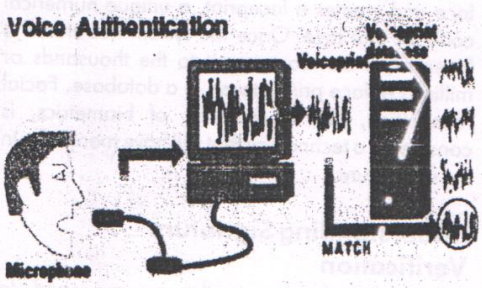

Fig. 13.

recognition software remembers the way you say each word. In addition to learning how you pronounce words voice recognition also uses grammatical context and frequency of use to predict the word you wish to input. These powerful statistical tools allow the software to cut down the massive language database before you even speak the next word. Also it involves identification of the speaker. The technique is shown in fig. 13. However, voice verification is a difficult area of biometrics, especially if one does not have direct control over the transducers, as indeed you wouldn't when dealing with the general public. The variability of telephone handsets coupled to the variability of line quality and the variability of user environments presents a significant challenge to voice verification technology, and that is before you even consider the variability in understanding among users.

Multimodal Biometrics

A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart card or any other combination of biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a speaker verification system.

Fig. 7

This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric. A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one biometric as your verification tool. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions.

Applications

Future Applications: Some Common Ideas

There are many views concerning potential biometric applications, some popular examples being:

- IT/Network Security-As more and more valuable information is made accessible to employees via LAN and WAN, the risks associated with unauthorized access to sensitive data grow larger. Protecting your network with passwords is problematic, as passwords are easily compromised, lost, or inappropriately shared. Whether driven by security, convenience, or cost-

reduction, biometrics are proving to be an effective solution for IT/Network Security. Major challenges in deploying biometrics in this environment include accuracy and performance, integrating biometric match decisions with existing systems, interoperability across proprietary technologies, and secure storage and transmission of biometric data.

- ATM machine use-Potential applications even include ATM and check-cashing security. The software is able to quickly verify a customer's face. After the user consents, the ATM or check-cashing kiosk captures a digital photo of the customer. The FaceIt software then generates a faceprint of the photograph to protect customers against identity theft and fraudulent transactions. By using facial recognition software, there's no need for a picture ID, bankcard or personal identification number (PIN) to verify a customer's identity.
- Workstation and network access-For a long time this was an area often discussed but rarely implemented until recent developments saw the unit price of biometric devices fall dramatically as well as several designs aimed squarely at this application. In addition, with household names such as Sony, Compaq, KeyTronics, Samsung and others entering the market, these devices appear almost as a standard computer peripheral. Many are viewing this as the application which will provide critical mass for the biometric industry and create the transition between sci-fi device to regular systems component, thus raising public awareness and lowering resistance to the use of biometrics in general.
- Access Control - Biometrics have long been used to protect a physical locations. In some cases entry to a facility is protected through a biometric at building entry. More frequently, specific rooms are secured with a biometric, as only certain employees have access to protected areas, and most building have areas considered semi-public.
- PC/LAN Logon - Many vendors have software that allows users to logon to PCs and local area networks, especially Windows NT. This reduces the user's need to remember and change passwords while reducing the administrator's need to frequently reset and manage passwords.
- Travel and tourism:- There are many in this industry who have the vision of a multi application card for travellers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc., all with one convenient token. Technically this is eminently possible, but from a political and commercial point of view there are still many issues to resolve, not the least being who would own the card, be responsible for administration and so on. These may not be insurmountable problems and perhaps we may see something along these lines emerge. A notable challenge in this respect would be packaging such an initiative in a way that would be truly attractive for users.
- Public identity cards-A biometric incorporated into a multi purpose public ID card would be useful in a number of scenarios if one could win public support for such a scheme. Unfortunately, in this country as in others there are huge numbers of individuals who definitely do not want to be identified. This ensures that any such proposal would quickly become a political hot potato and a nightmare for the minister concerned. You may consider this a shame or a good thing, depending on you point of view. From a dispassionate technology perspective it represents something of a lost opportunity, but this is of course nothing new. It's interesting that certain local authorities in the UK have issued 'citizen' cards with which named cardholders can receive various benefits including discounts at local stores and on certain services. These do not seem to have been seriously challenged.

Conclusion

Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening our national borders, in travel documents, visas and in preventing ID theft. Now, more than ever, there is a wide range of interest in biometrics across federal, state, and local governments. Congressional offices and a large number of organizations involved in many markets are addressing the important role that biometrics will play in identifying and verifying the identity of individuals and protecting national assets.

Authors Profile

A. C. Suthar
Asst. Professor, Electronics & Comm. Dept.
C. U. Shah College of Engg. & Tech.
Dr. G. R. Kulkarni, Principal C. U. Shah College of Engg. and Tech., Wadhwah city - Gujarat.

■