ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Significant Applications of Biometrics

K.Ramya[1], K.Suganya[2], A.Rethinavelsubramanan[3]

[1]Asst. Professor & Head, Department of Science & Humanities, Kingston Engineering College Katpadi, Vellore, Tamil Nadu.
[2]Assoc. Professor, Department of Software Engineering & IT, A.V.C College of Engineering, Mannampandal, Mayiladuthurai, Tamil Nadu.
[3]Asst.Prof & Head, Department of Mechanical Engineering, K.S.K.College of Engineering & Technology, Kumbakonam, Tamil Nadu

Abstract: Biometric Technology and its applications have existed longer than people believe. Currently the number of applications instituted around the world is increasing. In 1996 approximately 10,000 biometric devices were in use worldwide. Some estimate the number will grow to 50,000 by year 2000. Bimetric vendors feel that time and attendance is the biggest growth area for biometrics in the near future. The applications in the biometric technology are limitless. Four to five years ago biometric technology will still considered too 'fictional' for many.

Keywords: FMR, ROC, DET, FTC, PIN

I. INTRODUCTION

Biometrics (ancient Greek: *bios*= "life", *metron* = "measure") refers to two very different fields of study and application. Biometric in reference to biological sciences has been studied and applied for several generations and is somewhat simply views as "biological statistics".

More recently the term's meaning has been broadened to include the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Overview

Biometrics are used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics.

* Possession-based: using one specific "token" such as a security tag or a card

* Knowledge-based: the use of a code or password.
Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions.

1.1 Common Human biometric characteristics

Classification of some biometric traits Biometric characteristics can be divided in two main classes, as represented in figure on the right: Physiological are related to the shape of the body. The oldest traits that have been used for more than 100 years are fingerprints. Other examples are face recognition, hand geometry and iris recognition.

Behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.

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.

Other biometric strategies are being developed such as those based on gait (way of walking), retina, hand veins, ear canal, facial thermo gram, DNA, odor and scent and palm prints.

1.2 Comparison of various biometric technologies

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- **Uniqueness** is how well the biometric separates individually from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** ease of acquisition for measurement
- **Performance** accuracy, speed and robustness of technology used.
- **Acceptability** degree of approval of a technology
- **Circumvention** ease of use of a substitute

The following table shows a comparison of existing biometric systems in terms of those parameters

Comparison of various biometric technologies, according to A. K. Jain[2] (H=High, M=Medium, L=Low)

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

Biometric systems

The basic block diagram of a biometric system the diagram on right shows a simple block diagram of a biometric system. When such a system is networked together with telecommunications technology, biometric systems become telebiometric systems. The main operations a system can perform are *enrollment* and *test*. During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is be robust. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block features needed are extracted. This step is an important step as the correct features need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identifiability.

If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

II. FUNCTIONS IN BIOMETRIC SYSTEM

A biometric system can provide the following two functions

***Verification** authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card or database for verification.

* **Identification** authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score is returned. The closest match within the allowed threshold is deemed the individual and authenticated

Performance measurement

* *false accept rate (FAR)* or *false match rate (FMR)*: the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

* *false reject rate (FRR)* or *false non-match rate (FNMR)*: the probability that the system incorrectly declares failure of match between the input pattern and the matching

template in the database. It measures the percent of valid inputs being rejected.

* *receiver (or relative) operating characteristic (ROC)*: In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

* *equal error rate (EER)*: the rate at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

* *failure to enroll rate (FTE or FER)*: the percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.

* *failure to capture rate (FTC)*: Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly.

**template capacity*: the maximum number of sets of data which can be input in to the system.

Issues and concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. A theoretical example is a debit card with a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. However, this argument ignores a key operational factor intrinsic to all biometrics-based security solutions: biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a pre-stored, static "match template" created when the user originally enrolled in the security system. Most of the commercially available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (for example, by using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently designed solutions contain anti-hacking routines. For example, the scanned "live" image is virtually never the same from scan to scan owing to the inherent plasticity of biometrics; so, ironically, a "replay" attack using the stored biometric is easily detected because it is too perfect a match.

The television program *MythBusters* attempted to break into a commercial security door equipped with biometric authentication as well as a personal laptop so equipped. While the laptop's system proved more difficult to bypass, the advanced commercial security door with "live" sensing was fooled with a printed scan of a fingerprint after it had been licked. There is no basis to assume that the tested security door is representative of the current typical state of biometric authentication, however. With careful matching of tested biometric technologies to the particular use that is intended, biometrics provide a strong form of authentication that effectively serves a wide range of commercial and government applications.

However, the big concern is when the biometric features of an individual are successfully attacked (compromised) by impostors and the legitimate owner runs out of new biometric feature to replace the old ones since they will not be secure to be used anymore as an identity. Therefore the so called *Cancellation Biometric* came to tackle this limitation

III. Biometrics and Privacy

A concern is how a person’s biometric, once collected, can be protected. Australia has therefore introduced a Biometrics Institute Privacy Code Biometric Institute in order to protect consumer personal data beyond the current protections offered by the Australian Privacy Act.

Marketing of Biometric products

Despite confirmed cases of defeating commercially available biometric products claim the products as replacements, rather than supplements, for passwords.

Consumers and other end users must rely on published test data and other research that demonstrate which products meet certain performance standards and which are likely to work best under operational conditions.

IV. CURRENT APPLICATIONS

Immigration and Naturalization Service's (INS) Passenger Accelerated Service System (INSPASS)[1,2] INSPASS was designed as a means to provide prompt admission for frequent travelers to the US by allowing them to bypass the personal interview/inspection part of the entry process. It uses hand geometry to verify the identity of the traveler at an automated inspection station. INSPASS stations have been installed, for example, at John F. Kennedy Airport in New York and Newark International Airport in New Jersey. INSPASS is available for citizens of 23 countries in the US visa waiver program who visit the US at least 3 times per year. These same 23 countries are planning to participate in the Future Automated Screening for Travelers (FAST) project, which would allow travelers to use automated passport inspection stations in countries participating in FAST.

- CANPASS
  CANPASS is the Canadian version of INSPASS, except that it uses a fingerprint biometric, rather than hand geometry, for traveler verification. The goal of CANPASS is to ease the transfer of goods and people between the US and Canada. CANPASS is in use at the Vancouver International Airport.
- PORTPASS
  PORTPASS is another INS initiative similar to INSPASS except that people in vehicles at borders are being monitored and it uses voice recognition biometric, instead of hand geometry. PORTPASS is used at a US/Canadian vehicle border crossing and is planned for use at US/Mexican border crossings. One version of PORTPASS (the Automated Permit Port) requires the vehicle to stop. It will also have a Video Inspection Service, allowing a driver to conference with an Inspector should the biometric fail. Another version, known as the Dedicated Commuter Lane, uses a radio frequency tag affixed to the vehicle in order to obtain the biometric as the vehicle is moving.
- Federal Bureau of Prisons
  The Federal Bureau of Prisons is using hand geometry units to monitor the movements of prisoners, staff, and visitors within certain Federal prisons. A successful trial with the hand geometry units was conducted at the Federal prison in Jesup, Georgia. Visitors must enroll upon arrival and are given a magnetic stripe card containing information that points to his/her identifying information in a central database. This card must be carried with the visitor at all times. Staff and inmates must also enroll. Staff is enrolled to reduce the possibility of mistakenly identifying them as an inmate or for positive identification in the event of a disturbance. Prisoners are enrolled for access control to places such as the cafeteria, recreation lounges, and the hospital. The system also allows for the tracking of prisoners' movements. By the end of 1995, around 30 Federal prisons were to have the hand geometry monitoring system installed.
- Automated Fingerprint Image Reporting and Match (AFIRM) In July of 1991, Los Angeles County in California installed the first AFIRM system. AFIRM was needed to reduce fraudulent and duplicate welfare benefits. The fingerprints of new applicants for welfare benefits are checked against a central database of prior claimants. Within the first 6 months of use, the county saved $5.4 million dollars, and the savings have been growing ever since. The system has been so successful that San Francisco, Alameda County, and Contra Costa County have installed AFIRM and check new claimants' fingerprints against existing recipients in these locales. AFIRM is expected to be in statewide operation in California by some time in 1997.
- Spanish National Social Security Identification Card (TASS): The TASS program is a smart card initiative employing fingerprint technology to eliminate enrollment duplication and provide secure access to personal information upon retrieval. The program is an ambitious one, in that it will combine pension, unemployment, and health benefits all on one card.
- The Colombian Legislature: The Colombian Legislature uses hand geometry units to confirm the identity of the members of its two assemblies immediately prior to a vote. The voting has been conducted this way since 1992.Many Federal, State, and local government agencies have purchased biometric systems. The Defense Advanced Research Projects Agency, Drug Enforcement Agency, Department of Defense, Department of Energy, Department of Public Safety, Department of State, Federal Bureau of Investigation, Federal Reserve Bank, Hill Air Force Base, the Pentagon, and the US Mint have approximately 250 biometric devices with 13,000 enrolled users for access control applications.

Planned Applications

- California, Colorado, Florida, and Texas Departments of Motor Vehicles [3] Efforts are underway to establish biometric-based screening of drivers. California records thumbprints digitally in its database.* Colorado and Texas record fingerprint images on their drivers' licenses. Florida is considering this idea. The goal is to eliminate the tampering with or faking of licenses by verifying the recorded fingerprint data.
- Government Accounting Office's Electronic Benefits Transfer (EBT) Task Force[11] Plans are underway to disburse many of the Federal Government benefits (e.g., retirement, social security, welfare) electronically through ATMs and point-of-sale terminals. It is estimated that $110 billion in Government benefits could be transferred onto and debited from access cards in this way. Initial plans are to implement fingerprint identification at the benefit enrollment phase. The success of the AFIRM program in Los Angeles County was the inspiration for the EBT plan. Fingerprint identification in the benefit disbursement phase is also under consideration to eliminate what could amount to extensive losses from the abuse of lost or stolen cards.
- FBI's Integrated Automated Fingerprint Identification System (IAFIS) IAFIS is designed to electronically replace the horrendously outdated, mostly manual fingerprint identification system that requires paper-based fingerprint cards, postal submissions of the cards, and labor-intensive searches. IAFIS would replace paper-based fingerprints with electronic ones. Submissions of requests could be made electronically and all searches for fingerprints would be conducted electronically. The goal is to reduce response time to a requesting agency from the current 10 weeks to 24 hours.
- National Crime Information Center 2000 (NCIC 2000)
  NCIC 2000 offers new and improved capabilities for the National Crime Information Center. Biometric information, such as that contained in the signature, face, and fingerprint, will be used in an automated system. Patrol cars will have the capability to capture fingerprints and eventually relay the information to local, State, and/or Federal Automated Fingerprint Identification Systems (AFISs). The goal is to have the new and improved system fully operational by the fall of 1999.

V. Conclusion:

Biometric vendors feel that time and attendance is the biggest growth area for biometrics in the near future. The application of biometric technology is limitless. Using the biometric technology is a way to achieve fast, user-friendly authentication with a high level of accuracy

VI. References

[1]. http://www.cilab.upf.edu/biosecure1/public_docs_Deli/BioSecure_Deliverable_D10-2-3_b3.pdf

[2]. Jain, A. K. (28-30 April 2004), "Biometric recognition: how do I know who you are?", Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE **12th**: 3 - 5

[3]. Jain, A. K.; Ross, A. & Pankanti, S. (June 2006), "Biometrics: A Tool for Information Security", IEEE Transactions On Information Forensics And Security **1st** (2)

[4]. P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, Face Recognition Vendor Test 2002: Overview and Summary (Online) [1]

[5]. C. Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson, Fingerprint vendor technology evaluation 2003: summary of results and analysis report, NIST Internal Rep. 7123, Jun. 2004 [Online] [2]

[6]. R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, Performance evaluation of fingerprint verification systems, IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, Jan. 2006

[7]. E. Kukula, S. Elliott, Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance, IEEE 2005

[8]. International Biometric Group, Independent Testing of Iris Recognition Technology, May 2005 (Online) [3]

[9]. NIST Iris Challenge Evaluation, (Online) [4]

[10]. S. Hocquet, J. Ramel, H. Cardot, Fusion of Methods for Keystroke Dynamic Authentication, Automatic Identification AdvancedTechnologies, 2005. Fourth IEEE Workshop on 17-18 Oct. 2005 Page(s):224 - 229

[11]. D. A. Reynolds, W. Campbell, T. Gleason, C. Quillen, D. Sturim, P. Torres-Carrasquillo, and Adami, The 2004 MIT Lincoln laboratory speaker recognition system, in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, Mar. 2005

[12]. Video of the Mythbusters episode on how to hack fingerprint scanners [5]

[13]. BBC News: Malaysia car thieves steal finger [6] Some other reports, giving more credence to the story: [7][8]

[14]. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy”