The Importance of a Biometric Authentication System

Sushil Phadke*

*Department of Physics, Government Girls College, Dhar, Madhya Pradesh, INDIA. E-Mail: sushilphadke5@gmail.com

***Abstract*—**A biometric or biometric identifier is an objective measurement of a physical characteristic of an individual which, when captured in a database, can be used to verify the identity or check against other entries in the database. Biometric Identification Systems can be grouped based on the main physical characteristic that lends itself to biometric identification; Fingerprint identification, Hand geometry, Palm Vein Authentication, Retina scan, Iris scan, Face recognition, Signature, Voice analysis. A biometric ID is notably harder to fake. In the long run, biometric identification promises to provide the global citizen with a sound identity management system, which could develop quite independently of nation states. Of course one could argue that this would be a tragedy, and that an ID management solution controlled and operated by governments is absolutely essential in order for government agencies to provide the services citizens expect to receive and to guarantee the survival of the same notion of state. Many private employers also require biometric identification systems to control access to workplaces or as cheat-proof time clocks.

***Keywords*—**Authentication; Biometric; DNA; Fingerprint; Hand Geometry; Hand Vein; Iris Face/Facial Thermo Gram; Physiological; Retinal Scan; Signature; Voice.

***Abbreviations*—** Automated Fingerprint Identification Systems (AFIS); Automatic Speaker Identification (ASI); Automatic Speaker Verification (ASV).

I. INTRODUCTION

OLD, low-tech IDs contain easy-to-forge information: names, addresses and a unique ID number printed on a card along with a picture. A national database that links names to ID numbers exists, but law officers have no way to know if the card and the picture within are authentic. With a low-tech ID system, identity theft is relatively easy, especially in a world full of high-resolution digital cameras, image-manipulation software and home printers. Biometric identification [Jain et al., 2005] is the process by which a person can be identified by his characteristics. Immigration cards holding both passport number and measures of the user's hand [Wing, 1998]; fingerprints taken as a legal requirement for a driver license, but not stored anywhere on the license [Slagle, 1999]; automatic facial recognition systems searching for known card cheats in a casino [Walters, 2001]; season tickets to an amusement park linked to the shape of the purchaser's fingers [Levin, 2002] home incarceration programs supervised by automatic voice recognition systems [Markowitz, 1999] and confidential delivery of health care through iris recognition [Perkins, 2001]: these systems seem completely different in terms of purpose, procedures, and technologies, but each uses "biometric authentication" in some way. "Biometric technologies" are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. There are two key words in this definition: "automated" and "person". The word "automated" differentiates biometrics from the larger field of human identification science. Biometric authentication techniques are done completely by machine, generally (but not always) a digital computer. Forensic laboratory techniques, such as latent fingerprint, DNA, hair and fiber analysis, are not considered part of this field. Although automated identification techniques can be used on animals, fruits and vegetables, manufactured goods and the deceased, the subjects of biometric authentication are living humans. For this reason, the field should perhaps be more accurately called "anthropometric authentication". The second key word is "person". Statistical techniques, particularly using fingerprint patterns, have been used to differentiate or connect groups of people [Jantz, 1987] or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioral components, both of which can vary widely or be quite similar across a population of individuals. No technology is purely one or the other, although some measures seem to be more behaviourally influenced and some more physiologically influenced. The behavioral component of all biometric measures introduces a "human factors" or "psychological"

aspect to biometric authentication as well. In practice, we often Physiological biometrics has to do with the physical traits of a person, and behavioural biometrics have to do with the things that can change with the environment. For example, a fingerprint, a physiological characteristic, does not usually change except for accident or illness, but a signature, a behavioural characteristic [Jhon Chirillo & Scott Blaul, 2003] can change as a person ages. Examples of physiological biometrics include fingerprinting, retinal scans and handprint scans. Behavioural biometrics includes verifying signatures and voice recognition. The most popular methods of keeping information and resources secure are to use password and User ID/PIN protection. These schemes require the user to authenticate [Joseph N. Pato & Lynette I. Millett, 2010] them by entering a "secret" password that they had previously created or were assigned. These systems are prone to hacking from either a brute force attempt to crack the password or from passwords which were not unique or even which were posted near the computer itself. A Biometric Identification system is one in which the user's "body" becomes the password/PIN. Biometric characteristics about the individual are what make that person unique and therefore can be used to authenticate an user's access to various systems.

1.1. Biometric

Systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. Identification [Prabhakar et al., 2003] (also called search) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. It is evident that identification is technically more challenging and costly. Identification accuracy generally decreases as the size of the database grows. For this reason records in large databases are categorized according to a sufficiently discriminating characteristic in the biometric data. Subsequent searches for a particular record are searched within a small subset only. This lowers the number of relevant records per search and increases the accuracy (if the discriminating characteristic was properly chosen). Before the user can be successfully verified or identified by the system, he/she must be registered with the biometric system. User's biometric data is captured, processed and stored. As the quality of this stored biometric data is crucial for further authentications, there are often several (usually 3 or 5) biometric samples used to create user's master template.

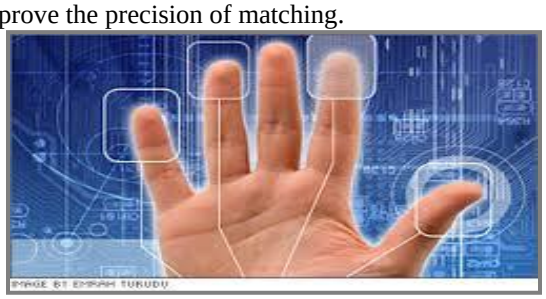
II. TYPES OF BIOMETRIC IDENTIFICATION

2.1. Fingerprint

Fingerprint identification techniques [Maltoni et al., 2003] all into two major categories—Automated Fingerprint Identification Systems (AFIS) and fingerprint recognition systems. AFIS is typically restricted to law-enforcement use. Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical hurdles because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image, so they are less sensitive to dirt and oils. Fingerprint recognition is generally considered reliable enough for commercial use, and some vendors are already actively marketing readers as part of Local Area Network login schemes.

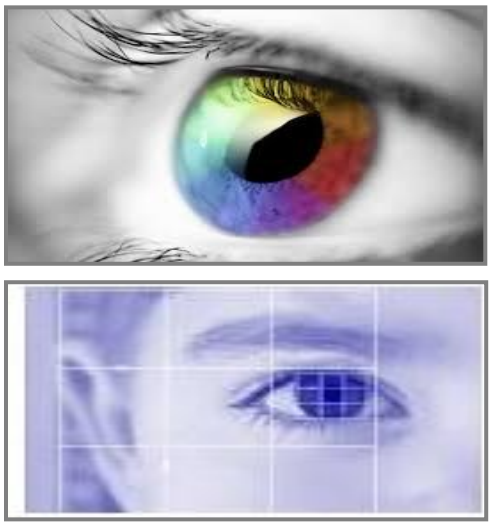
2.2. Hand Geometry

The essence of hand geometry is the comparative dimensions [Wayman, 2001] of fingers and the locations of joints. One of the earliest automated biometric systems, Indentimat, installed at the Shearson-Hamill investment bank on Wall St. during the late 60s, used hand geometry and stayed in production for almost twenty years. Some systems perform simple, two-dimensional measurements of the palm of the hand. Others attempt to construct a simple three-dimensional image from which to extract template characteristics. In one of the most popular descendants of the Identimat, a small digital camera captures top and side images of the hand. Reference marks on the platen allow calibration of the image to improve the precision of matching.



2.3. Retinal Scan

Retinal recognition creates an "eye signature" from the vascular configuration of the retina, an extremely consistent and reliable attribute with the advantage of being protected inside the eye itself. An image of the retina is captured by having the individual look through a lens at an alignment target. Diseases or injuries that would interfere with the retina are comparatively rare in the general population, so the attribute normally remains both consistent and consistently available.

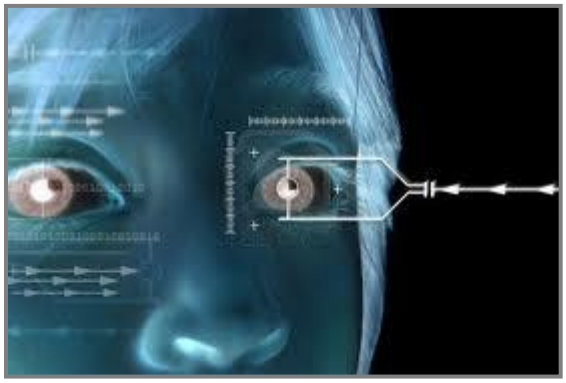


2.4. Voice

Voice recognition techniques are generally categorized according to two approaches—Automatic Speaker Verification (ASV) and Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one enrolment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition.

2.5. Iris

Iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification that the iris presented as a biometric factor is genuine. Though empirical tests with the technology will improve its reliability, it appears quite promising and even practical for many applications, especially two-factor scenarios. While some of the technical issues of iris scanning seem pedestrian, they present implementation challenges. A careful balance of light, focus, resolution, and contrast is necessary to extract the attributes or minutiae from the localized image. While the iris seems to be consistent throughout adulthood, it does vary somewhat up to adolescence.



2.6. Face/Facial Thermo Gram

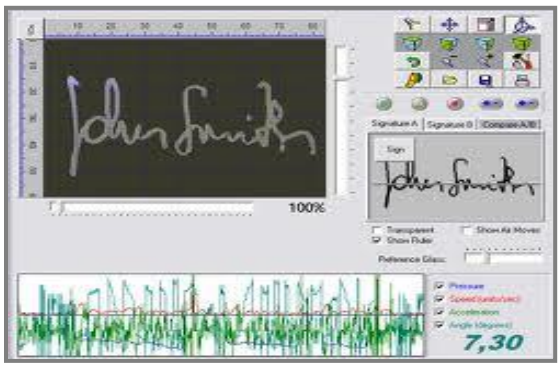
Face recognition technology is still its early stages, and most tests and applications have been run against relatively small databases. The similarity score produced by each comparison determines the match—the highest score wins. Acquisition for biometric identification purposes requires the individual's face to be presented to a video camera. An evident deficiency in some current schemes is the ability to fool or confuse some systems with makeup. A facial thermo gram works much like face recognition except that the image is captured by way of an infrared camera, and the heat signature of the face is used to create the biometric template used for matching. This is more reliable than simple imaging. The U.S. Army Research Laboratory conducted the FERET Database Evaluation Procedure in Sept. of 1996 comparing various technologies and algorithms side by side. While the results are promising and some approaches yielded impressive results, this technology is still considerably less reliable than some alternatives. As is the case with other technologies, practical usefulness increases dramatically in a two-factor scenario.

2.7. Hand Vein

Hand vein recognition attempts to distinguish individuals by measuring the differences in subcutaneous features of the hand using infrared imaging. Like face recognition, it must deal with the extra issues of three-dimensional space and the orientation of the hand. Like retinal scanning, it relies on the pattern of the veins in the hand to build a template with which to attempt matches against templates stored in a database. The use of infrared imaging offers some of the same advantages as hand geometry over fingerprint recognition in manufacturing or shop-floor applications where hands may not be clean enough to scan properly using a conventional video or capacitance technique.

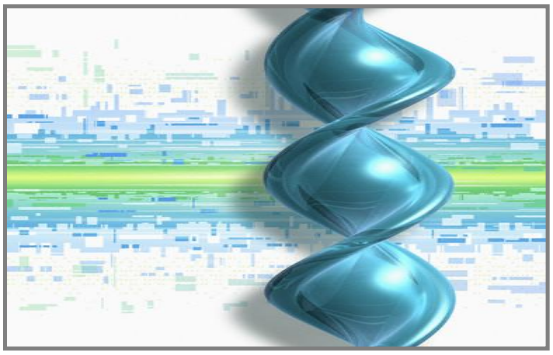
2.8. Signature

While a signature is not strictly biometric, it is a simple, concrete expression of the unique variations in human hand geometry. Forensic experts have developed criteria over the years for verifying the authenticity of a signature. Automating this process allows computer automation to take the place of an expert in looking for unique identifying attributes. In addition to the general shape of the signed name, a signature recognition system can also measure both the pressure and velocity of the point of the stylus across the sensor pad. (Keystroke dynamics is a variation on this technique that measures the typing rates and intervals.) Signatures, however, are difficult to model for variation, as is the reliability of these systems, especially when compared with other simpler alternatives.



2.9. DNA

The DNA is an acronym for deoxyribonucleic acid which is present in nucleus of every cell in human body and therefore a highly stable biometric identifier that represents physiological characteristic. The DNA structure of every human is unique, except from identical twins, and is composed of genes that determine physical characteristics (like eye or hair colour). Human DNA samples can be acquired from a wide variety of sources; from hair, finger nails, saliva and blood samples. Identification based on DNA requires first isolating from source/samples, amplifying it to create multiple copies of target sequence, followed by sequencing that generates a unique DNA profile. The DNA matching is quite popular for forensic and law enforcement applications. However, it requires tangible samples and cannot yet be done in real time. Currently, not all the steps in DNA matching are automated and therefore results can be skewed if the process is not conducted properly or the DNA samples themselves get contaminated. In summary, the DNA matching process is expensive, time consuming and therefore not yet suitable for large scale biometrics applications for civilian usage.



III. BIOMETRIC IDENTIFICATION - ADVANTAGES

There are a number of advantages to this technology:

- Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scans produce absolutely unique data sets when done properly
- Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords)
- Automated biometric identification can be done very rapidly and uniformly, with a minimum of training
- Your identity can be verified without resort to documents that may be stolen, lost or altered.
- the most economical biometric PC user authentication technique
- Easy to use
- Small storage space required for the biometric template
- reducing the size of the database memory required
- There is no known way to replicate a retina standardized
- Verification time is about five seconds

IV. CONCLUSIONS

In the long run, biometric identification promises to provide the global citizen with a sound identity management system, which could develop quite independently of nation states. Of course one could argue that this would be a tragedy, and that an ID management solution controlled and operated by governments is absolutely essential in order for government agencies to provide the services citizens expect to receive and to guarantee the survival of the same notion of state. Discussing this question is well beyond the scope of this paper, but there is no doubt that this is one of the main ethical and political challenges raised by biometric technologies. The endless history of identification systems teaches us that identification has never been a trivial fact but has always involved a web of economic interests, political relations, symbolic networks, narratives and meanings. In ancient Greece, slaves were not considered real persons and were called 'faceless', a prosopon. The word that in Greek designates the face, prosopon, is also at the root of the Latin word persona, person. The person is thus an individual with a face; to use the metaphor, an individual becomes a person when she has a recognizable identity. Biometrics could contribute to give a face to the multitude of faceless people who live in developing countries, contributing to turn these anonymous, dispersed, powerless, crowds into the new global citizens. Certainly, then, there are reasons for the ethical and political concerns surrounding biometrics; but these reasons are fortunately balanced by some reasons for hope.

REFERENCES

[1] R. Jantz (1987), "Anthropological Dermatoglyphic Research", *Annual Review of Anthropology*, Vol. 16, Pp. 161–177.

[2] Wing (1998), "Overview of all INS Biometrics Projects", *Proceedings of CTST'98*, Pp. 543–552.

[3] J. Markowitz (1999), "Voice Biometrics: Speaker Recognition Applications and Markets", *Voice Europe 1999: European Symposium on Voice Technologies*, London.

[4] G. Slagle (1999), "Standards for the Driver's License", Proceedings of CTST'99, Pp. 891–902.

[5] J. Walters (2001), "Casinos Must Tell Customers that Police are Scanning Faces", *Toronto Star*, Edition 1.

[6] J.L. Wayman (2001), "Fundamentals of Biometric Authentication Technologies", *International Journal of Image and Graphics*, Vol. 1, No. 1, Pp. 93-113.

[7] J. Perkins (2001), "FT-IT: New Services will Keep Eye on Security: Biometrics", *Financial Times (London), Wednesday Surveys ITC1*.

[8] G. Levin (2002), "Real World, Most Demanding Biometric System Usage", *Proceedings of Biometrics Consortium*, Crystal City, VA.

[9] S. Prabhakar, S. Pankanti & A.K. Jain (2003), "Biometric Recognition: Security and Privacy Concerns", *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, Pp. 33–42.

[10] D. Maltoni, D. Maio, A.K. Jain & S. Prabhakar (2003), "Handbook of Fingerprint Recognition", *Springer*, NY.

[11] Jhon Chirillo & Scott Blaul (2003), "Implementing Biometric Security", *Wiley*.

[12] A.K. Jain, Ruud M. Bolle & Sharath Pankanti (2005), "Biometrics Personal Identification in Networked Society", *Springer*.

[13] Joseph N. Pato & Lynette I. Millett (2010), "Biometric Recognition: Challenges and Opportunities", Editors: *Whither Biometrics Committee; National Research Council*.