BIOMETRICS: Selecting the Best Solution

Shirish Joshi
Department of Computer Science & Engineering
Symbiosis Institute of Computer Studies and Research, Symbiosis International University

Abstract— The past few decades have witnessed the rapid progress of technology, engulfing all the aspects of human existence. The assistance of technology in man's mundane as well as specialized activities has rendered it a part & parcel of his life. With the advancement of technology the professional and personal information is now stored digitally in the memory of IC chips. Such vital information cannot be guarded against frauds through lock & key. In order to ensure denial of access to classified data by unauthorized persons, passwords & secret codes were implemented. But the security tools like smart cards, magnetic stripe cards & physical keys can be lost, stolen or duplicated. Passwords can be forgotten, shared or unintentionally observed by a third party. Instead of guaranteeing a foolproof security system these tools become a nuisance for the users. The most rapidly emerging technology for security system is the BIOMETRIC TECHNOLOGY. Biometric user authentication techniques can be used to protect PCs & Networks from unauthorized access by authenticating users based on a physical feature such as fingerprints, retina, iris, hand or face. Biometrics is a means of using parts of human body as a kind of permanent password. Biometrics turns your face, hand or eye into your badge of identity. We attempt to find the best solution in different situations & compare the pros & cons.

Key words: Biometric, Biometric Identification, Biometric Authentication, Fingerprint recognition, Face recognition, Voice Recognition, IRIS recognition, Hardware recognition

I. INTRODUCTION

First of all, an ideal security system has the following listed characteristics:

- It should be foolproof.
- It should be non-evasive.
- It should be fast.
- It should be accurate along with being fast.
- It should be user-friendly.

For example, a particular, company to scrutinize its employees and visitors, buys a security system. The system should be such, that it lets employees inside the company premises without any problems in sign-on.

A. The Underlying Idea

There are qualities that distinguish one person from the other. Personalities differ to some extent but there is a physical uniqueness as well. The statistical use of the characteristic variation in unique elements of living organisms is known as biometrics.

B. Biometric Identification

Biometric identification is a sophisticated variation on a single-factor security scheme. In this case, the factor is some physical attribute of the person--fingerprint, iris, retina face, vein pattern, etc. Biometric identification systems typically follow three high-level processing steps. First, the system must acquire an image of the attribute through an appropriate scanning technique. Once the scanned content is acquired, it must be localized for processing purposes. During this step, extraneous informational content is discarded and minutiae are isolated and turned into a template, a sort of internal canonical form for matching attributes stored in a database. Minutiae are the uniquely differentiating characteristics of the biometric attribute. Finally, templates stored in the database are searched for a match with the one just presented. If a match is found, the identification is a success and the succeeding steps of the security process can begin.

C. Biometric Authentication

The process is similar to biometric identification. First, the requestor presents a token to assert identity. For example, an ATM or credit card is inserted into a reader. Finally, the value of the token is used to look up the template previously stored for this individual. If it matches the template presented on this occasion, the requestor is authenticated.

D. System Quality

The quality of a biometric authentication algorithm is specified in terms of False rejection Rate (FRR) and False Acceptance Rate (FAR). FRR indicates the percentage of instances authorized individual is falsely rejected by the system. FAR states the percentage of instances an unauthorized individual is falsely accepted by the system. FRR and FAR are diametrically opposed, therefore increasing the FAR will lower the FRR and vice versa.

E. Fingerprint Recognition

Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge count.

Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device. The biggest advantage of this method is that an individual's fingerprint is exclusive. Thus, this method is very distinctive. The fingerprint scanner can be built into small devices. But the human mind has discovered loopholes in this method too. A new study from Yokohama National University in Japan shows that phony fingers concocted from gelatin, called "gummy dummies", easily trick fingerprint systems. Some manufacturers claim to guard against such tactics by recording pupil dilation; blood flow in fingers to show that biometric sample is "live". Recent tests by independent research & consulting firm International Biometric Group showed that some systems are unable to collect a finger scan from up to 12% of users as the fingerprint quality can vary with age & occupation. Its applications are in surveillance,

mug shot matching, access control, and casinos. Standard Bank, South Africa, scans he fingerprints of its customers instead of using a PIN when they wish to withdraw cash. The Lower Merion School district near Philadelphia (USA) has installed finger scan devices for school lunch lines.

F. Face Recognition

Acquisition for biometric identification purposes requires the individual's face to be presented to a video camera. The methods used vary. Some systems analyze distances between features like chin, nose and eyes. 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. These systems can be easily fooled by changes in lighting, viewing angle, or sunglasses; they serve merely as a deterrent. "The camera in the ceiling is like the man behind the curtain in the Wizard of Oz. Its all for show," says Smith. Tom Colatosti says, "Crowd scanning can be problematic, if you are talking about an airport, you need a choke point". This technology is easy to use & requires only software. But the shortcoming is significant privacy concerns. It can easily be thrown off by poor lighting. An evident deficiency in some current schemes is the ability to fool or confuse some systems with make-up. The face recognition technique is being successfully used at a handful of airports, including Boston's Logan, Fresno, St. Petersburg – Clearwater, Palm Beach & Dallas Fort Worth in USA. The systems compare passing faces against a database of images from FBI lists of suspected terrorists & wanted felons.

G. Voice Recognition

Using a persons' unique voice patterns, speaker verification compares live speech samples against a stored voice print template or prerecorded sample of the user-selected input using standard signal computing techniques like HMM, speech patterns, tones, inflections, etc. Voice print is a fine series of spectral power density plots that depict how the energy in one's voice at different frequency varies with time as one vocalizes a word or phrase. Voice experts say that sufficient characteristics of one's voice print remain constant under all circumstances, enabling these plots to reliably verify one's identity.

The main attraction for voice identification is telephone applications, where most of the necessary hardware is already in place. If properly implemented it could provide a greater safety tofinancial transactions conducted over the telephone. Mobile manufacturers & wireless operators are incorporating voice -scanning techniques in their devices. Companies that have introduced this include Nuance, Trintech & Dialogic. Voice recognition is a low-cost technique & requires little user training. Sometimes voice may vary over time & is affected by illness & stress.

H. Iris Recognition

Iris recognition is another developed biometric recognition system capable of positively recognizing the identity of individuals without physical contact. The iris is the colored portion of the eye that surrounds the pupil. The boundary of the pupil is defined by the video capture device, eyelid occlusion and specular reflection discounted, and the quality of the image is determined for processing. Iris patterns are processed and encoded, which are stored and used for future recognition transactions. Iris recognition usually takes only a second or two to complete and can accommodate both eyeglass and contact wearers. Iridian Technologies, Inc. of Moorestown, NJ leads the world in research, development and marketing of authentication technologies based on iris recognition -- the most accurate biometric identifier.

Iris scanning is one of the most accurate biometric user authentication techniques. High accuracy results from the fact that iris is very distinctive and rarely changes. The drawback is that the hardware employed is large and expensive. It requires user-training and controlled lighting.

The iris scanning is expected to be used extensively in applications such as user identification for Automated Teller Machines (ATMs) as in Nationwide Building Society, UK and Japan. The New York state Lottery uses iris scanners for employee access to a secured room containing its data system.

I. Handwriting Recognition

Most questioned document cases involve contested handwriting. Initials, signatures, writing or printing contain features, which can attest to their genuine or spurious nature. The slide shows evidence of a guideline, smudging and tremor that indicate this signature was traced from a model.

There are many processes of doing this:

- Electrostatic document imaging – detects indented writings and invisible writing images, useful in the detection of substituted pages, alterations to multi-page documents and clues as to the origin of anonymous notes.
- Video spectral comparison system – detects differences in the infrared reflectance and infrared luminescence of writing inks, useful in the detection of alterations and the decipherment of obliterated entries
- Microscopy - stereo binocular microscope enlarges images 7X - 120X, useful
- in the detection of traced and simulated forgeries
- Differences in the color of inks.

J. Computer Imaging:

color scanner and imaging software useful in the enhancement of faint carbon, NCR or erased entries and in the detection of slight color differences between inks

K. Choosing a Biometric Authentication Solution

Before choosing a biometric user authentication solution, an organization should evaluate its needs carefully. The choice depends upon:

- Level of security required
- Accuracy
- Cost and implementation time
- User acceptance

1) Level of Security

Biometric techniques that identify physical features are more accurate; therefore, they offer a higher level of security. Iris and fingerprint recognition techniques are highly secure.

2) Accuracy

Retinal scanning and iris identification are both highly accurate ways of identifying individuals. This is because iris is very distinctive and rarely changes. However, they are both expensive to implement. Hand, face, and fingerprint authentication techniques offer good accuracy for a smaller investment in scanning hardware.

3) Cost and Implementation Time

When implementing a biometric user authentication system, an organization should work with its PC vendor to evaluate the cost and time associated. Iris scan requires a large and expensive hardware. In contrast, voice recognition offers a low cost alternative.

4) User Acceptance

Users generally find less intrusive biometric techniques, such as fingerprint, voice, or hand identification, most acceptable. Face scan is less acceptable to users as it arouses significant privacy concerns. Iris scan can also sometimes prove to be harmful for the eyes. Thus, it is preferred only where high security is required.

II. Conclusion

A. Multiple Biometrics, Best Option

It is observed from the study of biometric techniques that it is of utmost importance to evaluate one's security requirements before choosing a system. After the evaluation, it may appear that using one technique alone may not cater to the desired needs. A biometric system relying only on a single biometric technique is often unable to meet the desired performance requirements. The best option available then is multiple biometrics. Identification based on multiple biometrics represents on emerging trend. For example, face recognition is fast but not reliable while fingerprint verification is reliable but insufficient. Voice recognition is low cost & user-friendly technique, but it may give inaccurate results when the person is ill or stressed. In order to design a foolproof security system, we need to combine the three techniques. As shown in the block diagram, the user identity is verified by acquiring the images of his face, finger and his voice samples these are then matched against the stored templates through the respective recognition processes. The final acceptance of the user is dependent upon the individual acceptance of each technique. Thus, it can also be named as a three-tier security system. We may indeed reach a time in the not too distant future when biometrics is the norm and passwords are passé. Those who keep an "eye" on emerging authentication strategies will be biometric-ready.

References

[1] Biometrics: Theory, Methods, and Applications (Google eBook) By N. V. Boulgouris, Konstantinos N. Plataniotis, Evangelia Micheli-Tzanakou
[2] Biometric Systems: Technology, Design and Performance Evaluation by James L. Wayman
[3] Biometrics: Identity Assurance in the Information Age by John D. Woodward Jr.
[4] A SURVEY OF BIOMETRIC RECOGNITION METHODS, 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia
[5] The Common Biometric Exchange File Format (CBEFF) development, www.nist.gov/cbeff March 2001.
[6] Biometrics: A Grand Challenge, https://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/biometricsgrandchallenge.pdf
[7] www.fingerprint-it.com

