IJITKM 0973-4414 Volume-9, Number-2 Jan-Jun 2016 pp. 61-63 available online at www.csjournalss.com

Biometrics: A Business Prospective

Anish Soni
HCTM Technical Campus,Kaithal, Haryana,India
soni_anish@yahoo.com

Abstract: Biometric methods are concerned with the measurement and evaluation of human physiological or behavioral characteristics. During the last years, the economic relevance of the biometric industry and market has increased rapidly. Although public security projects have initiated the positive market development, future growth will be also generated by private sector demand such as secure and convenient banking, payment applications, hardware component etc. The Internet security industry is composed of hardware tokens, software tokens, and biometrics. All are used for authentication.
The deployment of biometrics to machine readable travel documents such as passports provides citizens with first experiences in biometric applications, thereby functioning as pioneer projects and market openers for other market segments. For example, biometric passports will redefine the border control process in the future, and in the mid-term, aviation security is another market segment that will contribute to the growth. To prepare for this business, the industry must carefully analyze the market and meet the demand. This paper assesses the relevance roll of biometrics in business and discusses selected market segments.

1. Introduction

Nowadays the need for automated [1] biometrical identification systems is increasing in civil and forensic fields of applications. The fast and accurate identification becomes particularly critical for large-scale applications, such as passport and visa documentation, border crossings, election control systems, credit card transactions control and crime scene investigations. Many countries, including the US, European countries and others incorporate biometrical data into passports, ID cards, visas and other documents for using in large national scale automatic biometrical identification systems. Automated fingerprint identification systems (AFIS) have been widely used in forensics for the past two decades, and recently they became relevant for civil applications. Whereas large-scale biometrical applications require high identification speed and reliability, multi-biometric systems that incorporate both face and fingerprint recognition offer a number of advantages for improving identification quality and usability. Large-scale automatic biometrical identification systems have a number of special requirements, which are different from those for small or middle scale biometrical systems. The system must perform reliable identification with large databases, as biometrical identification systems tend to accumulate False Acceptance Rate with database size increase and using single fingerprint or face image for identification task becomes unreliable for large-scale application. Several biometrical samples should be used to increase identification reliability, and multi-biometrical technologies (i.e. collecting fingerprint and face samples from the same person) are often employed there for additional convenience. The system must show high productivity and efficiency, which correspond its scale. The system must support major biometrical standards. This should allow using the system generated templates or databases with the systems from other vendors and vice versa.

2. Biometrics Business Overview

Fotronics provides [2] cost-effective biometrics security products and solutions designed and manufactured by leading manufacturers in the Asia Pacific region.
Product range includes

- Access Control Systems and Time Attendance Management System.
- Wireless Fingerprint Access Unit.
- Fingerprint Reader
- Fingerprint Door Lock
- RF Key Fob

Many of these products have been deployed in government and commercial applications to enhance security of confidential/financial transactions, protect data and restrict access to private premises.
Fotronics is committed to continue development of innovative security products that combine biometrics, RFID and wireless technology.

Microsoft is announcing today its first hardware products to use fingerprint recognition, a technology that has made inroads in the office environment but is barely existent for home users. Three new company products will use fingerprint readers to log on a user to a computer and store passwords used at Web sites. They were developed by Microsoft's hardware group, a small team in Redmond that focuses on mice and keyboards, not software. The products are a sign of the Microsoft's hardware group's evolution. Years ago, computer hardware meant mice and keyboards in shades of beige, dark beige and light beige, said Tom Gibbons, general manager of the group.

In banking business [3] automatic teller machines (ATMs), phone banking, online services and electronic commerce has changed the nature of financial services, giving people the convenience and the flexibility to do so much more with their time and resources. Now a day all these make secure by biometrics.

To date most of the high profile pilot projects for the use of biometrics [4] have been in two areas - government identity documents and passport control, and financial transactions. Many of these installations have now moved to live use. There is also a well-established but less glamorous use of biometrics for control of access to premises.
Major examples include passenger and staff clearance at airports by iris scan and hand geometry, voter and social security registration by fingerprint, financial transaction authorisation by iris scan and signature verification, police identification of known criminals from CCTV by facial recognition, and many examples of building access control and time & attendance recording using several different technologies.

Smart Cards that include digital credentials required for authentication and decryption are examples of cards that are multifunctional, capable of using multiple applications. The continuing expectation for the next generation is to embed the cards with tamper-proof biometric chips, and consequently, not only reduce fraud, but increase the trust of users.
This technology is advancing rapidly today for several reasons. The first is that the cost of biometric technologies is becoming less to use than not to use, i.e., less than the costs associated with fraud. The second is the improved ease of integrating a high level of security by matching individual attributes such as fingerprints, facial structure, voice patterns, vein systems, eye tissues, signature patterns, and other physical identifiers to database fields. These changes, along with the ever-expanding e-commerce and business-to-business applications on the market today, may effectuate a sea change in the type of cards people will use to access and manipulate their personal information. [5]
Biometric recognition can be used in **Identification** [6]mode, where the biometric system identifies a person from the entire *enrolled* population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters [7] an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user. To understand the above process see the figure 1.

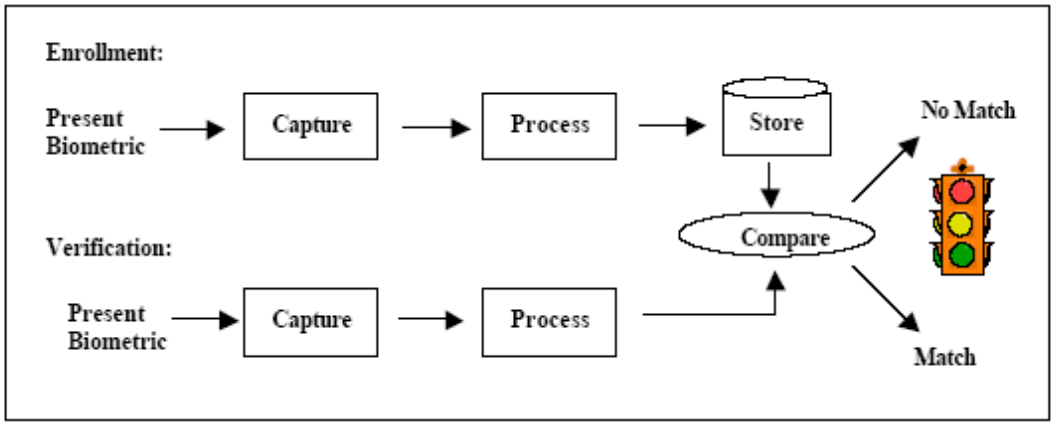

Figure 1: Biometric verification Process.

3. Relevance for Industry

Once one starts thinking of applications [8] it becomes apparent that the only limitations are imagination and, more practically, cost justification.

Business is rightly concerned about physical and logical security, both from internal and external threats. It is important to control who has access to any place or process, and to know which individuals are involved at every stage of the company's business operations.

Since the employees of any business represent an easily defined and influenced closed user group, biometric technology can be readily used not only for verification, but also for identification.

Areas where accuracy, security and simplicity are important include access control to restricted facilities (eg research labs) or systems (eg confidential data), time & attendance monitoring (where biometrics prevent friends from using tokens to falsely record attendance for each other), sign-off authorisation for sensitive process control steps, tracability records of all individuals involved in the production of sensitive items, and the replacement of cash by electronic authorisation in company sales outlets (like canteens).

It was once the stuff of science fiction, but the process of identifying an individual by their biological characteristics is gradually becoming a business reality. Thanks to technology known as biometrics, identity recognition techniques such as fingerprint, retinal and voice scanning are increasingly finding everyday applications in the workplace.

4. Conclusion

As more and more pilot systems turn into live installations, led in particular by highly visible government projects, biometrics has moved from science fiction, through technological novelty, to mainstream business tool.

Increasing volumes of sale are driving prices of hardware and software down, and, although the internal processes of individual technologies remain largely proprietary, standards are now emerging for the usable output from the devices.

The issue of public acceptance of these technologies remains a challenge to large scale open implementations, but within the boundaries of a corporate implementation (including the extended family of sub-contractors, suppliers etc.) they are much easier to manage. But even in the wider public, acceptance is growing too, partly in response to the perceived benefits of easier service through 'fast-track' options, and to a large extent by a willingness to make some sacrifices to protect against identity theft, which has increased six-fold in the UK over the last five years.

With proper planning and consideration for the effect on operational procedures, biometrics are now ready to take their place in the technology kit bag of every organization.

References

[1] http://www.neurotechnologija.com/megamatcher.html.

[2] http://www.fotronics.com/index.php?option=com_content&task=view&id=27 &Itemid=52 - 13k

[3] Scottson & Michaels, Inc. has been in the business of Credit Card Fraud Verification Processing since 1994. http://www.scottson-michaels.com/ccfraudhistory.htm

[4]"Army's New Password: 'Biometrics'", USA Today, Thursday, June 22, 2000, Section "The Nation," page 3A. http://www.scottson-michaels.com/ccfraudhistory.htm

[5] Scottson & Michaels, Inc. has been in the business of Credit Card Fraud Verification Processing since 1994. http://www.scottson-michaels.com/ccfraudhistory.htm

[6] Biometric Consortium web site: http://www.biometrics.org

[7] National Institute of Standards and Technology web site: http://www.nist.gov

[8] http://www.cambashi.com/research/articles/Biometric_Technologies_jan06.htm