RESEARCH PAPER | Commerce | Volume : 4 | Issue : 5 | May 2014 | ISSN - 2249-555X

Increasingly Essential Smarter Physical Access to an Account in Near Future

KEYWORDS

Ambika Ramchandra

KUD's Karnatak Science College, Dharwad

ABSTRACT *A biometric is a physical or biological feature or attribute that can be measured and used as an unique identity authentication. In the last couple of years we have seen an enormous growth in electronically available services, such as banking through ATMs, the internet and voice services (phone). Humans are integrated closer to computers every day, and computers are taking over many services that used to be based on face to face contact between humans. This has prompted an active development in the field of biometric systems which is fast growing technique to stop crimes. Biometric identification and verification systems will be increasingly used in the future.*

INTRODUCTION

Undoubtedly, there are significant changes in the living styles of humans, which may be due to the effect of technological growth and modernization or environmental conditions that force the humans to indulge in criminal activities. Law keepers are working rigorously to maintain law and order, but at the same time, the crime activities are increasing enormously leaving the cops difficult to analyze the crime and arrest the criminals. There is an abnormal increase in the crime rate and also the number of criminals is increasing, this leads towards a great concern about the security issues. Crime preventions and criminal identification are the primary issues before the investigators. Identity theft, fraud, hacking, and computer viruses are posing increasingly formidable challenges to individuals, companies, and governments as they seek to protect their data from theft. These concerns have given rise to a multi-billion dollar security industry, whose solutions often require significant resources to implement.

Lot of research is projected in this direction by construction different models by the researchers for effective analysis. However, the main disadvantage is that due to the overload of data regarding the crime activities, together with the increase in the number of criminals makes it difficult in analyzing the data.

In the last couple of years we have seen an enormous growth in electronically available services, such as banking through ATMs, the internet and voice services (phone). Humans are integrated closer to computers every day, and computers are taking over many services that used to be based on face to face contact between humans. This has prompted an active development in the field of biometric systems which is fast growing technique to stop crimes.

BIOMETRICS

A biometric is a physical or biological feature or attribute that can be measured and used as an unique identity authentication.. It can be used as a means of proving that you are who you claim to be, or as a means of proving without revealing your identity that you have a certain right (e.g. access), just like a PIN (personal identification number) or a password. The crucial difference is that the biometric is something that is part of you, rather than something you know or can carry with you.

Following are different types of biometrics which we can use to protect the information.

Some Examples of Different Biometrics

- Face
- Fingerprint
- Voice
- Palmprint
- Hand Geometry
- Iris
- Retina Scan
- Voice
- DNA
- Signatures
- Gait
- Keystroke

Fig 1. Different Biometrics Examples

Biometric characteristics are said to be 'distinctive'. The distinctiveness of a biometric varies by the technique used to measure it and the process through which two similar biometrics are declared as matching. Biometrics identification can be physical or behavioral.

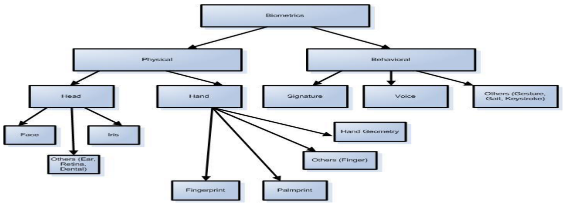


Fig 2: physical and behavioural characteristics used by biometrics

However, there are many reasons to believe that biometrics will change the life of people in near future mostly because its use will be much more convenient than other techniques in use today for individual identity authentication.

BIOMETRICS STAGES

Biometric identification works in four stages:

1) Enrolment
2) Storage
3) Acquisition
4) Matching.

Firstly, individuals are enrolled, i.e. a record associating the identifying features with the individual is created. Secondly, a record of that scan is stored somewhere. Thirdly, when identification is required, a new sample of the feature is acquired. Finally, the newly acquired record is compared to the stored record. If they match, the individual has been identified.

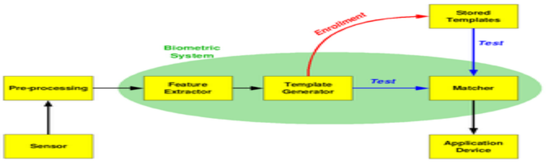


Fig 3: Biometrics Process Diagram.

SEVEN PILLARS OF BIOMETRICS WISDOM

Universality All human beings are endowed with the same physical characteristics - such as fingers, iris, face, DNA – which can be used for identification.

Distinctiveness For each person these characteristics are unique, and thus constitute a distinguishing feature.

Permanence These characteristics remain largely unchanged throughout a person's life.

Collectability A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification.

Performance The degree of accuracy of identification must be quite high before the system can be operational.

Acceptability Applications will not be successful if the public offers strong and continuous resistance to biometrics.

Resistance to Circumvention

In order to provide added security, a system needs to be harder to circumvent than existing identity management systems.

APPLICATION OF BIOMETRCS

Voter ID and Elections - while the biometric national ID card is still in project, in many countries are already used the biometry for the control of voting and voter registration for the national or regional elections. During the registration of voter, the biometric data is captured and stored in the card and in the database for the later use during the voting. The purpose is to prevent the duplicate registration and voting.

Driver's licenses - In many countries the driver license is also used as identification document, therefore it is important to prevent the duplicate emission of the driver license under different name. With the use of biometric this problem can be eliminated.

Benefits Distribution (social service) - the use of biometry in benefits distribution prevents fraud and abuse of the government benefits programs. Ensuring that the legitimate recipients have a quick and convenient access to the benefits such as unemployment, health care and social security benefits.

Employee authentication - The government use of biometric for PC, network, and data access is also important for security of building and protection of information.

Military programs - the military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.

Account access - The use of biometric for the access to the account in the bank allows to keep definitive and auditable records of account access by employees and customers. Using biometry the the customers can access accounts and employees can log into their workstations.

ATMs - the use of biometric in the ATM transaction allows more security. using biometric verification to allow a greater variety of financial transaction than are currently available though standard ATMs.

Online banking - Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.

Telephony transaction - Voice-scan biometric can be used to make more secure the telephone-based transactions. In this type of application, when the costumer calls to make a transaction, a biometric system will authenticate the customer's identity based on his or her voice with no need of any additional device.

PC/Network access - The use of biometric log-in to local PCs or remotely through network increase the security of the overall system keeping more protected the valuable information.

Physical access - the biometric is widely used for controlling the access to building or restricted areas.

E-commerce - biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services

Time and attendance monitoring - In this sector the biometrics is used for controlling the presence of the individuals in a determine area. For example for controlling the time sheet of the employees or the presence of students at the classroom.

BRIEF HISTRY OF BIOMETRIC

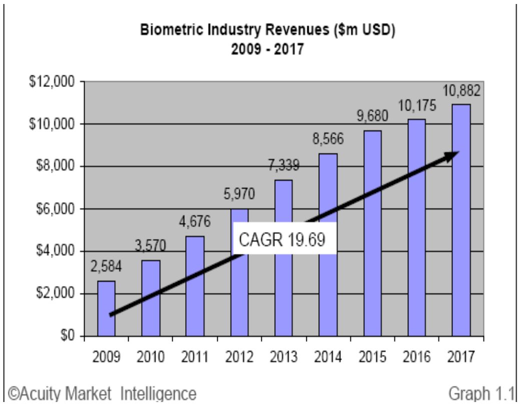
1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individual
1892	Galton develops a classification system for fingerprints
1896	Henry develops a fingerprint classification system
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1974	First commercial hand geometry systems become available
1986	Exchange of fingerprint minutiae data standard is published
1988	First semi-automated facial recognition system is deployed
1992	Biometric Consortium is established within US Government
1997	First commercial, generic biometric interoperability standard is published
1999	FBI's IAFIS major components become operational
2002	M1 Technical Committee on Biometrics is formed
2003	Formal US Government coordination of biometric activities begins
2004	US-VISIT program becomes operational
2004	DOD implements ABIS

BIOMETRICS IN FUTURE

Biometric identification and verification systems will be increasingly used in the future. One reason is that in a society that is increasingly mobile, flexible and digital, there is a need for more efficient identification systems. A second reason is that criminals have acquired great expertise in circumventing the old identification systems. In addition, as biometric technologies become better, cheaper, more reliable and more convenient, they will increasingly be implemented in other environments such the everyday life, in businesses, at home, in schools, and in other public sectors.

Biometrics is gradually gaining ground and pushing out conventional methods of identification and security checking. This emerging technology is growing at a fast rate as it is being rapidly adopted not only in the private sector but in various government projects as well. The size of the biometric readers market was USD 50.2 million in 2011, and is further expected to grow at 48 percent CAGR to touch USD 363 million by 2018.

The market for Automated Fingerprint Identification System (AFIS) and other fingerprint biometric technologies account for the largest share of the global biometrics market and is expected to retain its dominance in the market in the coming future. This sector is valued at USD 2.8 billion in 2010 and is expected to increase at a CAGR of 19.6% to reach nearly USD 6.6 billion by 2015.



Biometrics Industry Revenues 2007—2015

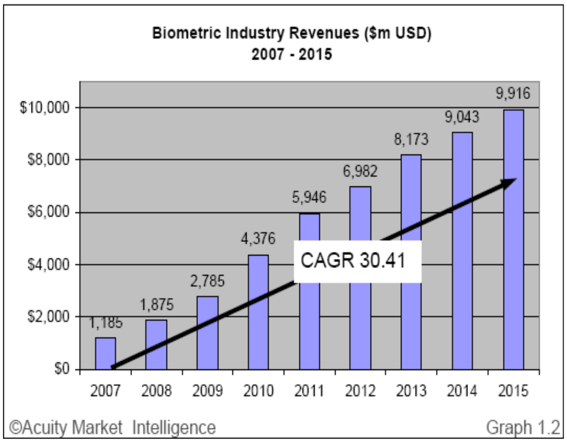
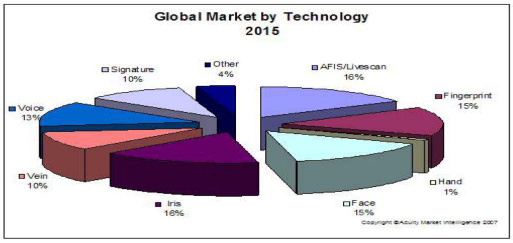


Fig 4: Biometrics Industry Revenue Comparison.

The facial structure, the iris, veins, and voice recognition together constitute the second largest segment. This sector is worth an estimated $1.4 billion in 2010 and is expected to reach $3.5 billion in 2015, at a compound annual growth rate (CAGR) of 19.9%.



The biometrics industry remains on track to experience significant transformation over the next ten years. Technological capabilities will revolutionize ease of use, accuracy, and performance and greatly expand the use of biometrics for personal, commercial, and government applications. Maturing business models will evolve from product to service based offerings with the bulk of revenues generated from transaction based opportunities of that process will play an equal role in determining its effectiveness.

THE LIMITATIONS OF BIOMETRICS

The main reason for introducing biometric systems is to increase overall security. However, biometric identification is not perfect - it is never 100% certain, it is vulnerable to errors and it can be 'spoofed'. Decision-makers need to understand

REFERENCE [1]. Jain, A., Bolle, R., Pankanti, S.: "BIOMETRICS: Personal identification in networked society," 2nd Printing, Kluwer Academic Publishers (1999). | [2]. Dugelay, J.L., et al., Recent Advantages in Biometric Person Authentication, in ICASSP International Conference on Acoustics, Speech and Signal Processing. 2002: Orlando, Florida, USA. | [3]. Ashbourn, J., Biometrics: Advanced Identity Verification: The Complete Guide. Springer-Verlag, London, . . 2000: Springer. 201. | [4]. Biometrics: Advanced Identity Verification, London: Springer-Verlag. | [5]. A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics:Personal Identification in Networked Society. | | [6]. J. L. Wayman, "Fundamentals of biometric authentication technologies," Int. J. Image Graphics, vol. 1, no. 1, pp. 93–113, 2001. |