Biometric Applications in Library and Information Centres: Prospects and Problems

G Rathinasabapathy T Mohana Sundari Thiru L Rajendran

Abstract

Biometric identification refers to a technology that uses scanned graphical information from many sources for personal identification purposes. The biometric technology helps the libraries to ensure safety and security to its invaluable collections, infrastructure and human resources. It is the duty of the librarian to keep the library buildings, shelves and stacks open and free without losing items to make available or putting individuals at unacceptable risk from the malicious, avaricious or senseless acts of others. Further, the LIS professionals are now handling huge database, provide access to online journals and web-enabled online public access catalogues in the networked digital environment where there are a lot of scope for compute /cyber crimes. In this regard, the biometric technology is a boon for the LIS professionals as it provides a single point of control for administrators to manage access to library resources such as computers, buildings, doors, the Internet, and software applications. In this context, this paper attempts to study the various types of biometric applications available for LIS centres, its prospects and problems as well.

Keywords: Biometrics, Library Security, Access Control, Computer Crimes, Cyber Crimes

1. Introduction

A Library is a 'temple of learning' which plays a pivotal role in the overall development of a society. But, it is a known fact that libraries are not always safe and secure places and they are facing a variety of security concerns which includes the theft, mutilation of library materials and other unethical losses. But, it is the duty of the librarian to keep the library buildings, shelves and stacks open and free without losing items to make available or putting individuals at unacceptable risk from the malicious, avaricious or senseless acts of others.

Further, the Library and Information professionals are now handling huge database, provide access to online journals and web-enabled online public access catalogues in the networked digital environment where there are a lot of scope for compute /cyber crimes.

Most of the libraries, especially the academic libraries follow open access system which allows its users directly to the stakes to ensure optimum utilization of the knowledge resources available in the library. Due to the open access system, books are often found on the library shelves with pages torn from the spine. Sometimes books are damaged beyond repair and almost all academic libraries including libraries in advanced countries are suffering from book or document theft by its members. Theft of library materials is not a new problem, not just an Indian problem. It is a universal problem which includes developed countries including USA, UK and European Union.

Therefore, it is important to provide a safe and secure environment for library staff, library resources and equipment, and library users. In this regard, the biometric technology is really a boon for the LIS professionals.

2. Biometric Technology

Biometrics is the science of measuring physiological or behavioural characteristics that verify a person's identity. Biometric identification refers to a technology that uses scanned graphical information from many sources for personal identification purposes viz., facial imaging, retinal and iris scans, fingerprint scans, voice patterns, facial recognition, hand geometry identification, etc. The application of biometric technology is limitless. Four to five years ago biometric technology was still considered too "fictional" for many. Now, these same individuals are asking where and how they can purchase biometric technology.

It is very interesting to know that Biometrics technology is not a very new one and its applications have existed longer than people believe. They have existed in commercially available products since 1968. The oldest ongoing general application of biometrics belongs to the University of Georgia which, in 1973, installed a hand-scanning system to restrict entry into its dining halls. The device measured the lengths of members' fingers by scanning them with photoelectric cells. It is in the last decade that biometric applications have finally caught up with the technology that has been around for nearly 30 years. Biometric vendors feel that time and attendance is the biggest growth area for biometrics in the near future. Beyond time and attendance, computer and electronic commerce security offer the greatest promise for widespread biometric use. During 1990's, fingerprint identification systems were the most popular and widely used from of biometric technology. But, today, a wide variety of biometric devices such as hand scans, voice recognition system, hand-geometry system, eye-scanning system, and face recognition system are available in the market. The technological developments paved the way for the declining prices and the escalating fraud and security breeches are bringing biometric technology to market. For example, the Finance Minister of Government of India recently announced that the Income Tax Department will issue Biometric PAN cards to all Tax payers.

3. Types of Biometric Technologies

A number of discrete biometric technologies are available on the market today such as signature, fingerprint identification, iris identification, retinal identification, hand geometry, hand, palm, and wrist subcutaneous vein pattern identification, signature identification, voice identification, keystroke dynamics identification, facial feature identification, body salinity (salt) identification, body odor identification, and ear identification. In general, biometrics can be classified into two types viz., physiological biometrics and behavioural biometrics. The coverage of these two types is furnished below.

3.1 Physiological Biometrics

- Iris/Retina
- Fingerprint (including nail)
- Hand (including knuckle, palm, vascular)
- Face
- Voice
- DNA
- Odor, Earlobe, Sweat pore, Lips

3.1.1 Physiological Biometrics

(a) Iris/Retina (Eye biometrics)

The iris is the most accurate and invariable of biometrics, and that their system is the most accurate form of biometric technology as the human eye offers two features with excellent properties for identification. Both the iris (the colored part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

(b) Fingerprint

A highly familiar and well-established biometric science is fingerprinting. The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators by the fingerprints they leave behind them at crime scenes. In the context of modern biometrics, these features, called fingerprint minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies. Fingerprints offer tremendous invariability, changing only in size with age, are highly resistant to modification or injury, and very difficult to “forge” in any useful way.

(c) Hand Geometry

Perhaps it is the most ubiquitous electronic biometric system. This system requires the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured. Made of 27 bones and a complex web of interconnected joints, muscles, and tendons, the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication.

(d) Facial Recognition

In the field of biometrics, facial recognition remains one of the more controversial technologies because of its very unobtrusiveness. With good cameras and good lighting, a facial recognition system can sample faces from tremendous distances without the subject's knowledge or consent. The facial recognition technology works by two methods viz., facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces. This technology may be highly useful for the libraries in security point of view.

3.2 Behavioral biometrics

- Signature
- Keystroke
- Voice
- Gait

(a) Signature

The most familiar biometrics is the signature of an individual. Our ability to judge by sight if one signature matches another has made this a time-proven and legally-binding biometric. However, computers can do all these things, and quantify, analyze and compare each of these properties to make signature recognition a viable biometric technology. Being based on things that are not visible (pen pressure and velocity, for example), signature-based biometric technology, offers a distinct advantage over regular signature verification.

(b) Voice Verification :

Voice verification is one among the biometric technology available in these days. Voice verification offers one great advantage, which is that it would allow a remote identification using the phone system, an infrastructure that's already been built and thus has zero client-side cost: no special reader needs to be installed in the library. Even without the phone system, the sampling apparatus, a microphone, remains far cheaper than competing, largely optically-based biometric technologies.

4. Biometric Applications in Libraries

In India, most of the academic libraries use computers, Internet and network based services to extend effective and efficient library and information services to the students, research scholars, faculty members and scientists who form the membership base. They are widely using computers for various purposes viz. circulation, cataloguing, information services, collection development and serial control. Somebody either the library users or a mischievous staff may unknowingly or intentionally, conceal (hides or keeps secret), destroy (demolishes or reduces), alter (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network in the Library. So, the LIS professionals should be very careful in this regard (Rathinasabapathy, 2007).

Further, LIS professionals are handling huge bibliographical databases to cater to the information requirements of their user community. So, they should be aware of the data diddling where somebody may alter the raw data just before a computer processes it and then changing it back after the processing is completed. They should ensure enough safety and security to their databases. To ensure better safety and security to the rich information resource base and human resources in a library, the movement of documents and personnel should be controlled. At present, electronic surveillance and security systems are being used in some academic libraries. (Rajendran, 2007). However, these systems have got their own limitations. In this context, biometrics applications are highly useful for them. The following are some of the important types of biometric applications useful for the libraries.

4.1 Controlled Access to Library Premises

This type of biometric application will not allow any unauthorized person to open the door. In this application, fingerprints of the authorized users will be scanned and stored for verification. This fingerprint identification is really a secure, convenient, and cost-effective alternative to passwords, badges, swipe cards and PINs. The biometric reader mounts on a wall near the library main door.

These biometric fingerprint scanners offer various levels of authorization for an individual. This authorization includes a scheduling mechanism for allowing access for individuals based on the time of day. This can be applied for the whole library or at least for the computer rooms and server/ network stations to avoid unauthorized access.

This system increases security levels more than a ID card or ID badge system as the fingerprint can't be lost or stolen. It also reduces overall cost in eliminating portable devices and reducing administrative time as well. Further, there is no need to track down or reprogramme ex-employee cards and ID badges.

The system is convenient and there are no more fumbling for keys and ID cards. The member need not worry about misplacing their cards. The premises access devices can be networked together so that the system can be controlled and maintained from a central location.

4.2 Controlled Access to Library Network

Nowadays, most of the libraries are working on digital environment where the library is connected with a local area network, wide area network or Intranet of the organization. In a world of cyber crimes, it is the need of the hour for any library to have control over the member access to the library network. Libraries are providing user name and password to the members to make use of the library computer systems and networks. However, too many passwords or inappropriate passwords lead to security lapses in which virtual credentials are lost, forgotten and hacked.

To overcome this problem, advanced biometric solution is available which ensures network authentication and safeguard the library network against unauthorized intrusion.

This kind of biometrics system will protect individual PCs and network access. It also reduces the password reset requests from the users. The library administrator can be able to authenticate who is accessing a PC, network, and application with exceptional accuracy. It associates a single fingerprint with as many as passwords or PINs on a system. Users can log on automatically without having to type in username and password. It eliminates the security risks of written down passwords and PINs.

Further, it protects passwords from most key logging viruses and prevent stolen or borrowed passwords. The system is easy to install, enroll fingerprint profiles and use. Since, most of the intellectual properties of academic and special libraries are residing on personal computers, servers and networks, it is the duty of the librarian to protect them from unauthorized access which may cause serious risks to the invaluable library assets.

5. Biometrics Applications: Prospects

Application of biometric technologies in libraries offers the following major advantages.

- Biometric traits can not be lost or forgotten while passwords can be lost or forgotten.
- Biometric traits are difficult to copy, share and distribute. Passwords can be announced in cracker's websites.
- Biometrics require the person being authenticated to be present at the time and point of authentication.
- The systems are easy to manage and cost efficient
- It is convenient to the users as they no longer responsible for passwords, swipe or proximity cards, PINs or keys.

6. Biometrics Applications in Libraries: Problems

Though the biometrics technology provides a number of advantages, there are some disadvantages too. The following are a select list of problems associated with the system.

- Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.
- Biometric systems are useless without a well-considered threat model.
- Biometrics are no substitute for quality data about potential risks.
- Biometric identification is only as good as the initial ID.
- Some biometric technologies are discriminatory.
- Biometric systems' accuracy is impossible to assess before deployment
- The cost of failure is high.

7. Conclusion

Biometrics technologies are really very useful for the LIS professionals to ensure better safety and security to the valuable collections which consist of various formats of information resource base. Though there are few limitations, the technology could be used in our libraries in a phased manner. The academic libraries can make use of the benefits of the technology to ensure better safety and security to their invaluable information resource base and human resources as well.

References

1. Bateman, S. Biometrics initiatives signal need for digital identification. Computer Shopper (1998), 18. 8. pp.102.
2. Burnell, J. Identifying the biometric opportunity: Biometric technology is now an affordable tool for many users and applications beyond security. Automatic I.D. News. Available at http://www.autoidnews.com (Accessed on 10-12-2007)
3. Cadix.. What is signature verification? Available at http://www.cadix.com/sigver.htm. (Accessed on 12-12-2007)
4. Davis, D. Biometrics. Available at http://cc.weber.edu/~itfm/hottopic/ BIOMETRI/BIOMETRI.HTM (Accessed on 15-12-2007)
5. Green, P. Biometric identification: Coming soon to a system near you. Center Spotlight, (1998) 3, 1.
6. Harmon, C. K. Lines of communication: Bar code and data collection technology for the 90's. Peterborough, Helmens Publishing, Inc., 1994. pp.68-71
7. Markowitz, J. Biometric standards: Why we need them. Speech Technology Magazine. Available at http://www.speechtechmag.com/ st10/jm1097.htm (Accessed on 30-12-2007)
8. O'Sullivan, O. Biometrics comes to life. Available at http://www.banking.com/ aba/cover_0197.htm (Accessed on 03-01-2008).
9. Phillips, K. (1997). Unforgettable biometrics: Your body is your key (just try not to lose it). PC Week OnLine. Available at http://www.zdnet.com/pcweek/reviews/ 1027/27bioapp.html (Accessed on 03-01-2008)
10. Rajendran, L. and G. Rathinasabapathy. Role of Electronic Surveillance and Security Systems in Academic Libraries. In Information to Knowledge: Technology and Professionals. Proceedings of the Conference on Recent Advances in Information Science and Technology (READIT 2007), MALA & IGCAR, Kalpakkam, 12-13th July 2007. Kalpakkam: IGCAR, 2007. pp. 111-117.

11. Rathinasabapathy, G. and L. Rajendran. Cyber Crimes and Information Frauds: Emerging Challenges for LIS Professionals. In Information to Knowledge: Technology and Professionals. Proceedings of the Conference on Recent Advances in Information Science and Technology (READIT 2007), MALA & IGCAR, Kalpakkam, 12-13th July 2007. Kalpakkam: IGCAR, 2007. pp.131-142

About Authors

Dr. G Rathinasabapathy, Assistant Librarian (Senior scale), Tamilnadu Veterinary and Animal Sciences University, Chennai.

Ms. T Mohana Sundari, Information Officer, BTIS & ARIS Cell of Tamilnadu Veterinary and Animal Sciences University. Chennai.

Mr. Thiru L Rajendran, Assistant Librarian, Tamilnadu Veterinary and Animal Sciences University. Chennai.