IASET: Journal of Library &
Educational Science (IASET: JLES)
ISSN(P): Applied; ISSN(E): Applied
Vol. 3, Issue 1, Jan-Jun 2017, 45-52

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

SECURITY OF INFORMATION WITH BIOMETRIC APPLICATIONS

PREETI PATEL

Librarian and Head Department. of Library Science IPS Academy, Indore

ABSTRACT

The biometric is a science which relates to measurement of physiological and behavior of human being. The 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. This study cover various tools of biometrics for useful in Library and Information centers. This article also searches the area where biometrics are useful in Library and Information Centers.

KEYWORDS: Biometrics Techniques, Information Security

INTRODUCTION

Information security is the major aspect of today's libraries because the methods of accessing information are in changing face. With the advancements of technology and its increased use in various areas of life, a major aspect that needs to be considered is security. Just how secure are all the systems that are being used to run the high-technology world? How secure is the information that is being transmitted from one end of the world to another across various networks? How secures the information that is stored on the innumerable located across that world? Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. "Biometrics" is the science and technology that consists of methods for unique recognition of an individual by measuring and analyzing biological data based on physiological or behavioral characteristics like fingerprints, hand geometry, handwriting, iris, retinal and vein. Biostatistics deals with the application of statistics to a wide range of topics in biology. The ability to create intelligent machines has intrigued humans since ancient times and today with the advent of the computer and 50 years of research into programming techniques, the dream of smart machines is becoming a reality.

Objectives of the Study

- The goal of this study is to present an outline of the use of biometrics in libraries
- To recognize the areas where Libraries use Biometrics
- To know the various aspects of these techniques

- The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information.

Need of the Present Study

Today's libraries are facing various problems relating to security of information

- Misused of library reading material;
- Vandalism theft books;
- Hacking the passwords of institutional confidential information;
- Problems conduct in housekeeping activities.

REVIEW OF LITERATURE

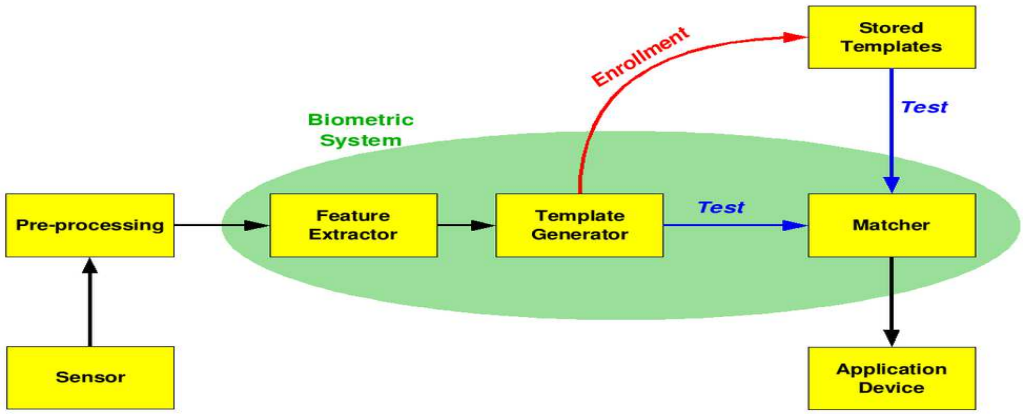
They are widely using computers for various purposes viz. Circulation, cataloguing, information services, collection development and serial control. Somebody either the library users or a mischievous staff may unknowingly or intentionally, conceals (hides or keeps secret), destroy (demolishes or reduces), 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). 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. Mandal and Nandi (2009) had discussed in their paper Biometric authentication approach in an automated and modern library based on the biometric recognition. The person working at the entrance or at the circulation desk of the library needs to either confirm or determine the identity of an individual requesting services in libraries. Biometrics and artificial intelligent combination play a vital role in security of Library and Information Centers (Supriya Indapurkar, 2013).

Concept Of Biometrics

Biometrics are a combination of two subjects, i.e. biology and biostatistic. Biometrics is the science and technology of analyzing biological data and measuring it by statistical methods. In information technology, biometrics refers to technologies that analyze and measure human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. 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 is 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 centers, its prospects and problems as well. 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 is 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. The following are some of the important types of biometric applications useful for the libraries.

Graphical Representation of Functioning of Biometrics



Source: https://en.wikipedia.org/wiki/Biometrics#/media/File:Biometric_system_diagram.png

Figure 1

3.0 Types of Biometric Techniques

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 behavioral biometrics. The coverage of these two types is furnished below.

3.1 Physiological Biometrics

3.2 Behavioral biometrics

3.1 PHYSIOLOGICAL BIOMETRICS

3.1.1 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 sends it back to your brain) provide patterns that can uniquely identify an individual. The pattern of lines and colors on the eye area, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

3.1.2: Fingerprint

A highly familiar and well-established biometric science is fingerprinting. The traditional use of fingerprinting, of course, has been as a forensic 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.

3.1.3: 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.

3.1.4 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 Eigen face comparison. The 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. The ageing face 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

3.2.1 Signature

The most familiar biometrics are 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.

3.2.2 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.

4.0 Applications of Biometrics 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. 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 of 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.

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.

Biometric fingerprint scanners offers 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 to 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 an ID card or ID badge system as the fingerprint can't be lost or stolen. It also reduces overall cost of eliminating portable devices and reducing administrative time as well. Further, there is no need to track down or reprogrammed 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

Most of the libraries are used, electronic environment with the current age. So the security of information is becoming problematic issue for the Libraries. Digital environment makes cyber crime ease and security of information become difficult for the professional. 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. Biometric techniques provide a suitable solution for the libraries. 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. 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.

4.3 Speech Recognition

In the 1990s, computer speech recognition reached a practical level for limited purposes. Thus United Airlines have replaced its keyboard tree for flight information by a system using speech recognition of flight numbers and city names. It is quite convenient. On the other hand, while it is possible to instruct some computers using speech, most users have gone back to the keyboard and the mouse as still more convenient. Speech recognition will be useful in Library and Information Centers.

4.4 Understanding Natural Language

Just getting a sequence of words into a computer is not enough. Parsing sentences is not enough either. The computer has to be provided with an understanding of the domain the text is about, and this is presently possible only for very limited domains. Using AI computer understands the natural language and misused and misplaced books are easily sought.

4.5 Computer Vision

The world is composed of three-dimensional objects, but the inputs to the human eye and computers' TV cameras are two dimensional. Some useful programs can work solely in two dimensions, but full computer vision requires partial three-dimensional information that is not just a set of two-dimensional views. At present there are only limited ways of representing three-dimensional information directly, and they are not as good as what humans evidently use.

5. ADVANTAGES BIOMETRIC FOR LIBRARIES

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

- Biometric traits cannot 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. PROBLEMS WITH BIOMETRIC APPLICATIONS IN LIBRARIES

- 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.
- Noise in sensed data, Intra-Class variation means the data for authentication may be different from the stored template due to the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances, etc.
- 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.

FINDINGS

- A Biometric system can successfully manage to record of the library library users, staff, visitors, vendors, suppliers or others;
- In the case of daily circulation, there is a chance of misusing library membership cards. One member can use another member's card, although there are clear indications that membership Card is not transferable. Biometric based authentication can solve this problem.
- The biometric system can solve the problems of open access related issues. By using a biometrics techniques library automatically prevent from unauthorized access of the library records.
- The day-to-day library operation and managements may easily be covered with the application and use biometric system.
- With the help powerful storage server a biometric system can successfully manage to record of the library
- Attendance of the staff is a most common use of biometric application. The Library also kept their staff attendance update with students when they enter or exit from the library premises

CONCLUSIONS

Biometric application is becoming popular in security of information. The library and Information centers are also using these applications, but due to heavy cost, lack of proper technical support and most important is financial backing these applications are not used in libraries as much as required. The conventional password-based and ID card-based methods do not really provide positive personal recognition because they rely on surrogate representations of the person's identity. It is, thus, obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. Biometric-based systems also have some limitations that can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that foolproof personal recognition systems simply do not exist and perhaps, never will. Biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience. Various techniques of biometrics are the technological developments paved the way for the declining prices and the escalating fraud and security breaches are bringing biometric technology to market.

REFERENCES

1. Indapurkar, Supriya, Patel, Preeti and Naidu, G.H.S.(2013). Indian journal of Information and Society Vol. 26 No. 4.
2. Rathinasabapathy, G. and L. Rajendran.(2007) 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.alpakkam: IGCAR, pp.131-142.
3. Rajendran, L. and G. Rathinasabapathy.(2007) "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, pp. 111-117.

4. Harmon, C. K. (1994)Lines of communication: Bar code and data collection technology for the 90's. Peterborough, Helmens Publishing, Inc. pp.68-71
5. Jain, A.K, Flynn P, & Ross.(2007) " Handbook of Biometrics", S pringer .
6. Jain, A.K, Ross, A.& Prabhakar S.(2004) "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp.4-20.
7. Hong, L., Jain, A. K., & Pankanti, S.(1999)"Can Multibiometrics Improve Performance?" , Proc. AutoID'99, pp. 59-64.
8. Hong, L. & Jain, A. K. (1998)"Integrating Faces and Fingerprints for Personal Identification", IEEE T rans. on Pattern Analysis and Machine Intelligence, Vol.20, No. 12, pp.1295-1307. http://omicsonline.org/jbmbshome.php
9. http://www.springerlink.com/content/l4614x73w8815734/fulltext.pdf
10. http://www.springerlink.com/content/p1715m64424733g3/fulltext.pdf
11. http://www.springerlink.com/content/v853526753863125/fulltext.pdf
12. http://en.wikipedia.org/wiki/Bioinformatics
13. http://searchsecurity.techtarget.com/definition/biometrics