International Journal of Research in Library Science (IJRLS)

ISSN: 2455-104X

DOI: 10.26761/IJRLS.7.1.2021.1368

Volume 7, Issue 1 (January-June) 2021, 57-66, Paper ID: IJRLS-1368

Received: 14 January. 2021 ; Accepted: 26 January. 2021 ; Published: 29 January. 2021

Use of Biometrics and Artificial Intelligence in Libraries

Dr. Preeti Shrivastava

Librarian, Govt. P. G. College, Sendhwa, Dist Barwani, M.P.

preetipatel2407@gmail.com

ABSTRACT

Biometrics and Artificial Intelligence applications are mostly related with Computer Science. Library and Information Centers are suffering the problem of Information Security in digital environment. Use of Biometrics and Artificial Intelligence in Libraries and Information Centers provide accurate solution of this problem. 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. Due to digital impersonation security techniques are predominantly using biometrics. To eliminate identity theft, a measurable physical characteristic or behavioral trait is more reliable. In factual scenario, blend of AI and biometric identification and a keypad code provides virtually unbreakable security. This study elaborates the areas where AI and Biometrics used in Library and Information Centers. It is certain that biometric-based recognition and artificial intelligence will have a profound influence on the security of information in Library and Information Centers.

KEYWORDS: Biometrics, Artificial Intelligence. Information Security

1.0: INTRODUCTION

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 interrelated often 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. Information security is the major aspects of today's libraries because the method of accessing information is in changing face. Security of information is always a major problem for librarians. Information security means to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

"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. To eliminate identity theft, a measurable physical characteristic or behavioral trait is more reliable. In factual scenario, blend of biometric identification and a keypad code provides virtually unbreakable security. The consequential statistical error rates of biometric security systems are calculated for a large population. The choice of biometric is application specific. Biometric is a metric of apparent nontransferable uniqueness provided by user's presence. Biometrics is extremely convenient form of providing identity and cannot be lent to another individual. The main objective of this study to bring together researchers from academia and industry to address current limitations on existing biometric technologies, exchange ideas on the latest theoretical and experimental advances in the present field and explore future directions of AI in biometrics. The number of users, technical implementation and operating environment will influence the selection of distinguishing biometric trait. "Artificial Intelligence" (AI) is the area of computer science focusing on creating machines that can engage on behaviors that humans consider intelligent. 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 AI programming techniques, the dream of smart machines is becoming a reality. Researchers are creating systems which can mimic human thought, understand speech, beat the best human chess player, and countless other feats never before possible. Find out how the military is applying AI logic to its hi-tech systems, and how in the near future Artificial Intelligence may impact our lives. This study will provide an interdisciplinary discussion for researchers, developers and practitioners to present the state of art of artificial intelligence in biometrics focusing on template creation and biometric fusion in Library and Information centers.

2.0 OBJECTIVES OF THE STUDY

- ***The goal of this study is to provide an outline of the use of AI and biometrics in libraries***
- ***To find the areas where Libraries use AI and Biometrics may be apply.***
- ***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.***
- ***To find out the protects against intentional or accidental attempt to deny legitimate users access to information or systems.***

3.0 PROBLEMS WITH DIGITAL ENVIRONMENT

- Vandalism theft books
- Misused of library reading material
- Hacking the passwords of institutional confidential information's
- Problems conduct in housekeeping activities
- Passwords are expensive

4.0 CONCEPT OF BIOMETRICS AND AI

4.1Biometric

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 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 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

4.2Artificial intelligence

Artificial intelligence (AI) is the intelligence of machines and the branch of computer science that aims to create it. John McCarthy, who coined the term in 1956, defines it as "the science and engineering of making intelligent machines." The field was founded on the claim that a central property of humans, intelligence—the sapience of Homo sapiens—can be so precisely described that it can be simulated by a machine. The prospect of creating intelligent computers has fascinated many people for as long as computers have been around. There are various definitions of Artificial Intelligence:-

- An area of study in the field of computer science. Artificial intelligence is concerned with the development of computers able to engage in human-like thought processes such as learning, reasoning and self-correction.
- The concepts of that machine can be improved to assume some capabilities. Normally thought to be like human intelligence such as learning, adapting, and self-correction.
- The extension of human intelligence through the use of computers, as in times past physical power was through the use of mechanical tools.
- In a restricted sense the study of techniques to use computers more effectively by improved programming techniques.

  (The New International Webster's comprehensive dictionary of the English Language, Encyclopedic Edition)

There are so many definitions of Artificial Intelligence, but most of them can be classified it into the following four categories.

- Systems that thinks like humans
- Systems that act like humans
- Systems that think rationally
- Systems that act rationally.

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

5.1 Physiological Biometrics
5.2 Behavioral biometrics

5.1 PHYSIOLOGICAL BIOMETRICS

5.1.1 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 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.

5.1.2: Fingerprint

A highly familiar and well-established biometric science is fingerprinting. The traditional use of fingerprinting, of course, has been as a forensic 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, is highly resistant to modification or injury, and very difficult to “forge” in any useful way.

Fingerprint sensors “read” the finger surface and convert the analog reading into digital form through an analog-to-digital converter (ADC). An RF (Radio Frequency) sensor acquires fingerprint data from the skin’s moist and electrically conductive boundary region where the live cells begin turning into keratinized skin. This live subsurface layer is the source of the fingerprint pattern, and it is rarely affected by damage or wear to the finger surface

5.1.3: 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.

5.1.4: Facial Recognition

FaceSDK is a high-performance, multi-platform face identification and facial feature recognition solution. . The system can work with entire faces or a facial feature, supports face recognition in still images and real-time video streams, and allows creating a wide range of applications from simple automatic red-eye removal tools to biometric login solutions. FaceSDK can help building complex face morphing and animation systems for entertainment portals. FaceSDK can be used in many online and desktop solutions where precise and reliable face identification is required. The face identification library can be used in photo imaging and video processing solutions, Web applications and biometric login automation systems. This technology may be highly useful for the libraries in security point of view.

5.2 BEHAVIORAL BIOMETRICS

5.2.1: 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.

5.2.2: 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.

5.2.3: Keystroke logging

Keystroke logging (often called **key logging**) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. Programmatically capturing the text in a control. The Microsoft Windows API allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks.

5.2.4:Gait analysis

Gait analysis is the systematic study of locomotion, more specific as motion, using the eye and the brain of observers, augmented by instrumentation for measuring body movements, body mechanics, and the activity of the muscles.[1] Gait analysis is used to assess, plan, and treat individuals with conditions affecting their ability to walk. It is also commonly used in sports biomechanics to help athletes run more efficiently and to identify posture-related or movement-related problems in people with injuries.

Minor variations in gait style can be used as a biometric identifier to identify individual people. The parameters are grouped to spatial-temporal (step length, step width, walking speed, cycle time) and kinematic (joint rotation of the hip, knee and ankle, mean joint angles of the hip/knee/ankle, and thigh/trunk/foot angles) classes. There is a high correlation between step length and height of a person

6.0 APPLICATIONS OF BIOMETRICS AND ARTIFICIAL INTELLIGENCE IN LIBRARY AND INFORMATION CENTERS

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 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. There are many reasons to consider this form of personal identification. Applications of Biometrics and AI in Library and Information Centers are given as following:-

6.1: 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.

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 in 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.

6.2: Controlled Access to Library Network

Most of the libraries are used electronic environment in current age. So the security of information is become problematic issue for the Libraries. Digital environment make cyber crime easy and security of information become difficult to 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.

6.3: Speech recognition

In the 1990s, computer speech recognition reached a practical level for limited purposes. Speech recognition make 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. Using this AI techniques unauthorized user will be easily caught by the computer by speech recognition.

6.4: 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 understand the natural language and misused and misplaced books are easily sought.

6.5: 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.

6.6 Gate Checking

Each and every library has a manual gate checking system. At least two persons are engaged for doing this job. If biometric system is introduced in the library, it should be fixed with the entrance gate of the library. The authorized library members and library staff members would be able to open the gate by themselves. Non-members should have the assistance to enter the library.

6.7 Circulation Section

In case of daily circulation, there is a chance of misusing library membership cards. One member can use other member’s card, although there are clear indications that Membership Card is not transferable. AI and Biometric based authentication can solve this problem.

6.8 Stack Entry Record

In Open Access Library System readers are always allowed to enter into the library stacks, but there should be a record in detail about readers along with their identity, time in and time-out. From our daily experience it is observed that the readers are not always maintaining manual records properly. They feel this recording is unnecessary and sometime they avoid it. The biometric system can solve these problems of a library easily if it is fixed with the stack entrance gate of the library. It will automatically take care about the most wanted library records. This concept is equally applicable in entry points of different sections of the library for example reading room, rare section, journal section etc.

6.9. Internet Searching, Using Digital Library

Biometric system can identify automatically the library computer users and welcome them for the purpose of Internet searching, using digital library, OPAC, etc. The day-to-day library operation and managements may easily be covered with the application and use ofbiometric system. Some of the major areas are:

6.9.1: Surveillance

It is the record keeping of library users, staff, visitors, vendors, suppliers or others who come into the library. Biometric system can successfully manage to record of the library with some days back up and for this purpose one powerful storage server is required.

6.9.2: Staff Attendance

It is the essential record for the library and this can easily be maintained with the introduction of biometric system, as this system records the persons’ entrance and entry time at the same time of the users.

6.9.3: Staff movement record

Biometry system can manage to record of the library staff movement of any particular staff in and out of the library for different purposes with few days back up facilities. This record helps librarian to find out the reasons for non-availability of a person in his / her working point.

6.9.4: Staff-Computer Automatic Recognition

Staff working with Desktop PCs for essential routine jobs by using the library management software or other works with computers can be authenticated with this biometric system which welcomes the library staffs after recognizing their identity automatically.

Advantages of the use of AI and Biometrics Applications in Library And Information Centers

- Biometric and AI traits cannot be lost or forgotten while passwords can be lost or forgotten.
- Biometric and Ai traits are difficult to copy, share and distribute. Passwords can be announced in cracker's websites.
- AI and Biometrics requires 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.
- It reduced labor costs
- Libraries, travel and immigration specifically lend themselves to this form of authentication. For example, if library authority plan to use biometric data help police departments check the authenticity of `users. This will increase traceability of unauthorized, nefarious individuals or stolen identities.
- It increases financial accountability
- We are now more sensitive than ever about the need to ensure that physical premises are safeguarded at point of entry. Knowing exactly who is coming into our buildings is indispensable. AI with biometrics can provide ubiquitous building entry identifiers – at least for pre-approved people.
- In many cases, traditional forms of verification generate boatloads of paper. Furthermore, other instances of authentication like notaries often rely solely on paper to document an event. Biometrics combined with other automation can eliminate our sole reliance on a paper trail for a given transaction or event.

Problems with AI and Biometrics Applications in Libraries:

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

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

CONCLUSION

AI and Biometric techniques provide suitable solution to 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. Virtually all biometric techniques are implemented using a sensor, to acquire raw biometric data from an individual; feature extraction, to process the acquired data to develop a feature-set that represents the biometric trait; pattern matching, to compare the extracted feature-set against stored templates residing in a database; and decision-making, whereby a user's claimed identity is authenticated or rejected.

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-

[11] http://omicsonline.org/jbmbshome.php

[12] http://www.springerlink.com/content/l4614x73w8815734/fulltext.pdf

[13] http://www.springerlink.com/content/p1715m64424733g3/fulltext.pdf

[14] http://www.springerlink.com/content/v853526753863125/fulltext.pdf

[15] http://en.wikipedia.org/wiki/Bioinformatics

[16] http://library.thinkquest.org/2705/

[17] http://www.eolss.net/Sample-Chapters/C15/E6-44.pdf

[18]http://searchsecurity.techtarget.com/tip/Biometric-authentication-know-how-Devices-systems-and-implementation

[19] http://searchsecurity.techtarget.com/definition/biometrics

[20] http://cits.curtin.edu.au/global/infosecurity.cfm

[21] Whittle E. Michael, Gait Analysis, An Introduction, preference page, Butterworth Heinnemann, 2007.

[22] http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity.htm

[23] http://usmilitary.about.com/od/glossarytermsi/g/i3094.htm