Indian Streams Research Journal
Volume 2, Issue.12,Jan. 2013
ISSN:-2230-7850
Available online at www.isrj.net
ORIGINAL ARTICLE

BIOMETRIC SECURITY TECHNOLOGY FOR LIBRARIES

PRAVEENKUMAR. KUMBARGOUDAR

Assistant Librarian (Sr)
Gulbarga University , GULBARGA: Karnataka

Abstract:

Of the different security systems available for libraries, biometric security technology is proved to be a significant technology for securing the data in libraries. The biometric traits such as finger print, iris, palm, veins, etc are personal and secure the access to the data in libraries.The present paper revealed the biometric security technology applications for libraries along with advantages, characteristics, etc.

INTRODUCTION :

The twenty first century witnessed a rapid growth and advancement in information processing, storage and communication technology. It revolutionized the role of the librarians and libraries in disseminating information service to the users all over the world. Due to the development in technology, library and information systems have re-organized their collection and services, in order to satisfy the user needs. As a result, the libraries are facing new computers, new requirements, new expectations and also new security challenges.

Today, it is essential for every library, Information Centre or Information System connects to the Internet. Further, there is a need for digital collection accessible through online. There is necessity of providing information services through the web. Consequently there is threat from unseen enemies connected to the global computer network. Any form of information that stored digitally may be seriously pilferated.

Referring a circular issued by the office of the Registrar, University of Ilorin, Omoniyi 1inferred the following:

Theft from the university is a reality, rather than a fiction;
Not many arrests have been made in connection with the crimes;
Some individual members of staff play a key role in incidents of theft from their respective faculties, departments, units, and offices;
There is a need for improved security strategies to protect university property against theft or pilfering

Information Security:

The subject of techno-theft in academic libraries is recognized by writers, researchers and library and information professionals as a major problem facing library professionals, users and the institutions in which they are located and the society in general.

In case of libraries, the library professionals must understand that they are legally responsible for the integrity of the information materials that from collection of the library. The professionals must be aware about the data stored in their computers is valuable, and must be careful about its deletion, alteration unauthorized pilferage and distraction. For this purpose libraries must have to frame a security policy and encourage only authorized use of information.

Title : BIOMETRIC SECURITY TECHNOLOGY FOR LIBRARIES
Source:Indian Streams Research Journal [2230-7850] PRAVEENKUMAR. KUMBARGOUDAR yr:2013 vol:2 iss:12

Mutilating library materials is a crime under state and municipal statutes in almost all communities,..Today, global libraries use network security policies to ensure the implementation of their security model, in maintaining network security, protection of information loss, alteration unavailability and the safeguarding of the organization's network form internal and external threats.2

According to Solms3, the growth of networking presents new opportunity for unauthorized access to computer systems and the trend to distributed computing reduces the scope of central, specialist control of IT facilities. As organizations link to the Internet or to the IT networks of business partners, (including libraries) central control over their IT systems and users and thus information security is lost.

The internet is unfortunately, a source for information and tools that can be used by hackers and crackers and has attracted unscrupulous individuals and groups intent to exploiting internet subscribers4. There is conflicting set of objectives between the use of the Internet and securing the Internet. The very success of the Internet has been attributed to the openness and availability of high volumes of information and anonymous access for masses of people5.

Weiss6 listed the areas of possible information abuse, as seven Es as under:

1.error;
2.eavesdropping;
3.espionage;
4.enmity;
5.embezzlement;
6.ego;
7.extortion.

In India due to growing terrorist attacks there is loss of people and also innumerable properties in various places. Following are a few recent major attacks made by terrorists in India.

New Delhi, Sep 13, 2008: Nine people killed in six blasts across the city.
Ahmedabad, July 26, 2008: 57 people killed after 20-odd synchronized bombs went off within less than two hours.
Bangalore, July 25, 2008: One person killed.
Jaipur, May 13, 2008: 68 people killed in serial bombings.
Hyderabad, Aug 25, 2007: 42 people killed in two blasts.
Samjhauta Express, Feb 19, 2007: 66 people killed after two firebombs went off on the India-Pakistan friendship train.
Mumbai, November 26, 2008: about 200 People killed and 400 were injured.

It is noted that the monuments and heritage spots are also the targets of the terrorists. These notable places also include the libraries and educational institutions. Hence, there is need to protect the institutions from the threats from the unauthorized penetrations and users. In this way, to maintain information security and to avoid misuse of the information, technological developments have contributed a few applications. These applications attempts to build up several information systems.

There are various technological applications developed to secure an information system. Skoularidou and Spinellis 7 described about such developments namely, the virtual machine, internet firewalls, the java sandbox, trusted computing systems and smart cards as information security applications.

Many of the Security technologies are developed now to protect the information and data in the networks. They are Radio Frequency Identification Systems (RFID), Visual Systems, Electro-magnetic Systems, Smart Cards, and Biometric Technology etc. the present paper described about the biometric technology developed for information security in digital libraries.

BIOMETRIC TECHNOLOGY:

Biometric technologies are defined as “automated methods of identifying or authenticating the identity of a living person based on a physical or behavioral characteristic”. Unique physical traits, such as fingerprints, iris scans, voice prints, faces, signatures or the geometry of the hand can be used. All of those technologies share a methodology involving enrollment and verification8”.

A biometric is a “measurable physiological and/ or behavioral trait that can be captured and subsequently compared with another instance at the time of verification”. In simplicity, biometric is the

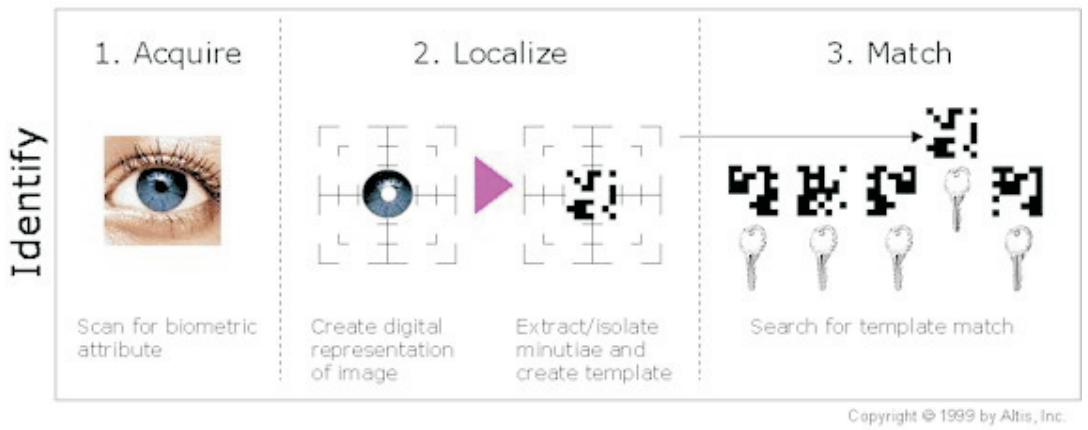
process of automatically recognizing a person using distinguishing traits. Matching of finger prints, voice patterns, hand biometry, iris and retina scans, vein patterns and other such methodologies are more physiological and signature verification, keystroke patterns and other methodologies are weighted towards individual behaviour9.

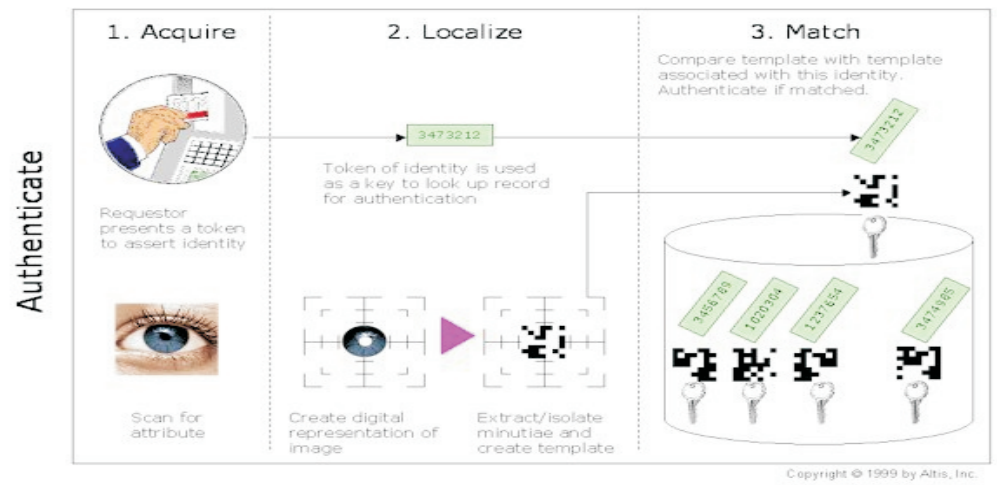
Biometric technologies appear to be the useful tools for identification and verification in security initiatives. In case of digital libraries, there is threat from hackers and crackers that they can misuse alter or delete the information. For this purpose, biometric security technology is useful.

Biometric technology identifies the library users on the basis of finger prints, iris recognition, Palm reading, Voice recognition, facial recognition, retinal scan, Veins and Signature. Good biometric identifiers share several characteristics that make them useful and reliable for recognition and identification applications:10

Characteristic		Description
Universal	---	Every one must have the attribute
Unique	---	The attribute must not change significantly over the time
Permanent	---	The attribute must be inseparable from the individual
Inimitable	---	The attribute must be irreproducible from the individual
Collectible	---	Must be easy to gather the attribute data passively
Tamper Resistant	---	The attribute should be impractical to mask or manipulate
Comparable to others.	---	Must be able to reduce the attribute to a state that makes it digitally comparable

In biometric technology there are two processes, namely, User Identification and User Authentication. This is shown in the following figure considering retinal scan11:





Using biometric technology for user identification and authentication is needed in digital library. As the users are scattered over the world and if there is open access, there is possibility of threats to information stored through networks. Biometric technology is already developed considering following personal attributes of individuals already.

1.Finger Prints:

Finger print recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse…Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image12. For network login use Finger print recognition is a good system of user authentication.

2. Palm/Hand Recognition:

In this kind of recognition, the comparative dimensions of fingers and the location of joints can be recognized through two-dimensional measurement or three dimensional images. A latest digital camera captures the top and side images of the hand. Reference marks on the platen allow calibration of the image to improve the precision of matching.

3. Retinal Scan:

Retinal recognition creates an 'eye signature' the vascular configuration of the retina, an extremely consistent and reliable attribute with the advantage of being protected inside the eye itself.

4.Voice Recognition:

Voice recognition techniques categorized into two approaches – Automatic Speaker Verification, which uses voice as the authenticating attribute. Automatic Speaker Identification attempts to use voice to identify who an individual actually is. Voice recognition differentiates an individual by matching particular voice traits against templates stored in a database.

5.Facial Recognition:

Face recognition technology identifies individuals by analyzing certain facial features such as the upper outlines of the eye sockets or sides of the mouth. Typically, facial recognition compares a live person with a stored template, but it has also been used for comparison between static images and templates. This technology works for both verification and identification13.

6. Iris recognition:

Iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification that the iris presented as a biometric factor is genuine14.

7. Veins recognition:

Like hand and face recognition, Veins recognition relies on the pattern of veins in the hand to build a template with which to attempt matches against templates stored in a database.

8. Signature Recognition:

Signature verification and Interpretation is the process of verifying and interpreting the identity of a person by checking the signature against the samples kept in a database and helping the user to interpret them15. The signature verification system divided into four components. They are (i) Data Capture- which converts signature into digital signals;(ii) Preprocessing- helps to refine the images to enhance the accuracy of the signature image; (iii) Feature Extraction and Segmentation- to obtain the boundaries and partitioning of the signature; (iv) Comparison and interpretation- matches the input signature with the templates consisting of sample signatures.

Zorkadis and Donos16 have compared different biometric technologies as under:

Table No.1. Comparison of several biometric technologies.

Biometric	Fingerprint	Retina	Face	Hand	Iris	Voice
Barriers to Universality	Worn ridges, finger impairments	Retina diseases	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	High	Low	Medium	High	Low
Permanence	High	High	Medium	Medium	High	Low
Collectibility	medium	Low	High	High	medium	Medium
Performance	High	High	Low	Medium	High	Low
Acceptability	medium	Low	High	Medium	Low	High
Potential or Circumvention	Low	Low	High	Medium	Low	High

LIBRARY SECURITY USING BIOMETRIC TECHNOLOGY:

The terrorist attacks around the world have forced all nations to reexamine their national security focus and place a priority on protecting the homeland. They have also forced consideration of a wide array of unconventional threats, especially cyber attacks against the networked information technology systems combining to form a nation's critical infrastructure17.

Biometrics provides security benefits across the spectrum from IT vendors to end users and from security system developers to security system users18. Biometric technologies are relatively inexpensive, requiring little or no new hardware and require nothing more than common place actions. This makes them attractive, especially in situations where remote users must be supported19. There is no risk of forgetting, losing, copying, loaning or getting biometrics stolen, especially if a multi-biometric approach is used for authentication20.

In India, different departments are already using biometric technology for variety of operations. The state of Andhra Pradesh has launched one of the largest programs in the history of iris recognition technology by attempting to enroll at least 20 million citizens- and eventually as many as 80 million- who may be eligible for state-issued food ration cards. The program taken up by LG Electronics ensures a single enrolment in a life time that can be linked for future social benefits. Another shining example is a pilot program taken up by Irirdian Technologies in Andhra Pradesh to employ its iris recognition solution for the allocation of about 9000 affordable homes in the Guntur district. The enrolment process incorporates iris recognition of the applicant couples to prevent duplicate applications. The Andhra Pradesh government is also one of the first to introduce iris-recognition systems in its Secretariat and Chief Minister's Office in Hyderabad21.

The ideal biometric would be easy to use, fast, non-intrusive, convenient and socially acceptable. Most biometric technologies are computationally intensive; and some users see biometrics as an invasion of privacy. Biometric techniques involve trade-offs among several factors, such as accuracy, ease of use, cost and user acceptance.

A digital library is open to all registered users. It operates through networks especially web. Computer networks are always facing the threats from hackers, crackers and cyber-criminals, who may delete, alter or misuse the data. For this purpose, specialized secured system is needed to access the information. Security system using biometric technology is of immensely useful and effective for the digital libraries.

Librarians may be more interested in protecting the privacy of their electronic communications or in protecting the integrity of the content of the resources they provide. Library catalogs and electronic resources are exposed to increasing risks of tampering by the general public. Biometric technologies could

preserve the privacy of electronic communications and transactions.

It is expected that virtual access will provide the critical mass to move biometrics for network and computer access. Physical lock-downs can protect hardware and passwords are currently the most popular way to protect the information stored on a network. Biometric Technology can increase a digital library's Competence to protect its information and information sources by implementing a more secure key than a password. Using biometric technology also allows a hierarchical structure of data protection, making the data even more secure. Biometric technologies further help to enhance security levels of access to network data.

REFERENCES:

1. Omoniyi, Joseph O: The security of computer and other electronic installations in Nigerian University Libraries. Library Management. Vol. 22 No.6 & 7, 2001.P. 272-277.
2. Ramamurthy, CR: Information Security: A source book for librarians. Delhi: Authors press, 2001. P.18
3. Solms, Rossouw von: Driving safely on the information superhighway. Information Management and Computer Security. Vol.5. No.1. 1997. P.20.
4. Trim, Peter RJ: Managing Computer Security issues: preventing and limiting future threats and disasters. Disaster Prevention and Management. Vol. 14. No.4. 2005. P. 493-505.
5. Liddy, Carrie: Commercial Security on the Internet. Internet Research: Electronic Networking Applications and Policy. Vol. 6. No.2/3. 1996. P. 75-78.
6.Weiss, Kenneth P: To Serve and Protect: Reconciling Information protection with LAN Environments. Information Management and Computer Security. Vol. 2. No.3. 1994. P. 19-25.
7. Skoularidou, Victoria and Spinellis, Diomidis : Security architecture network clients. Information Management and Computer Security. Vol.11. No.2. 2003. P. 84-91.
8. Biometric Technology. http://www.voice-security.com/Biomet.html accessed on 27th August 2009.
9. Harris, Austin Jay and Yen, David C: Biometric Authentication: assuring access to information. Information Management and Computer Security. Vol. 10. No.1. 2002. P. 12-19.
10. Biometric Technology Background. http://www.altisinc.com/Biometric/background.html accessed on 27th August 2009.
11.Biometric Identification/Authentication Techniques.
http://www.altisinc.com/Biometric/techniques.html accessed on 27th August 2009.
12.Biometric Identification/ Authentication Techniques.
http://www.altisinc.com/Biometric/techniques.html accessed on 27th August 2009.
13.Rosenzweig, Paul and Others: Biometric Technology: Security, Legal and Policy Implications. http://www.heritage.org/Research/HomelandDefense/lm12.cfm accessed on 27th August 2009.
14. Biometric Identification/Authentication Techniques.
http://www.altisinc.com/Biometric/techniques.html accessed on 27th August 2009.
15. Vivekandan, K and Meena, C: Fuzzy Signature Verification and Interpretation system using stroke comparator. Journal of Computer Science. Vol. 1. No.2. Sept-Oct 2005. P. 95-108.
16. Zorkadis, V and Donos, P: On biometrics based authentication and identification from privacy protection perspective: Deriving privacy-enhancing requirement. Information Management and Computer Security. Vol. 12. No.1. 2004. P. 125- 137.
17. Biometric technology holds the key to system-wide IT security.
http://www.cryptometrics.com/tech_library_security.php accessed on 25th August 2009.
18. Biometric Security Technology.
http://www.peterindia.net/Biometricsview.html#what%20is%a%20Biometric accessed on 27th August 2009.
19. Desmarais, Norman: Body language, security and e-commerce. Library Hi-Tech. Vol. 18. No. 1. 2000. P. 61-74.
20. Heracleous, Loizos and Wirtz, Jochen: Biometrics: the next frontier in service excellence, productivity and security in the service sector. Managing Service Quality. Vol. 16. No. 1. 2006. P. 12-22.
21. Malovika, SV: The Wizardry of Biometrics. i.t. Vol. 15. No.6. April 2006. P. 36-41.