

Facial Biometric Authenticated Digital Resource Usage

Sameer Sadiq Sofi¹ Dr. Rafi Ahmad Khan²

¹PhD Scholar in Department of Computer Science, Mewar University, Chittorgarh, Rajasthan, India

²Department of Management Studies, University of Kashmir, J&K India, Also affiliated as Faculty of Computer and Information System, Islamic University of Madina, Saudi Arabia

Abstract - Automatic Digital resource comprises of voluminous amounts of data that are stored in digital formats rather than hard/print form and are accessible through different devices like computers, tablets, mobiles, e-readers etc. The digital resources are a type of information retrieval system which can be accessed locally or remotely through different computer networks. The growing availability of the digital resources on World Wide Web and its easy accessibility has caused more concerns about its security due to various types of internet threats that can result in financial losses, loss of digital resources and identity theft. This has resulted in the need to give access to only authorized users to these digital resources. In order to secure, digital resources efficiently and effectively, there is a need of a user identity authentication system. Biometrics is the promising area for research that can be used for authentication of users on a network in order to give access to digital resources.

Among the various biometrics techniques such as iris recognition, signature, fingerprints, face recognition, hand geometry etc., facial biometrics with the help of web cams holds potential of being easy-to-use, fast, reliable, accurate, and less expensive authentication method to access digital resources. In this paper, an attempt has been made to give an overview of different biometric techniques. It also presents a framework of facial biometric authentication method for accessing digital resources and its applications.

Key Words: Facial Biometric System, Digital Resource, Web Cams

1. INTRODUCTION

Main purpose of digital resources is to enable students, academicians and researchers to easily explore vast knowledge stored in digital format. A digital resource can be defined as a networked online information space in which users can locate and access information in the form of books, journals, paper-based archives, videos, films etc. A digital resource offers the services of online catalogs, searching aids, indexing and abstracting services, digitized collections and other e-holdings. It is a networked learning environment that provides access to distance as well as lifelong learning resources. With the advancement of Information and Communication Technology (ICT), many academic libraries are being converted in to digital libraries by digitizing books, theses, papers, journals and other works that are stored in traditional hard copy format.

The growing availability and accessibility of the digital resources through internet by different users of the web has caused great concern about the security of digital resources due to numerous coverage given to Internet threats aimed at causing financial losses and identity theft [1]. Various concerns about digital resources as discussed below [2]:

- The licensing/copyright issues and system requirements to maintain security, registrations, payments.
- The software, hardware, and data communication that are necessary to provide access to digital resources
- The cost and the process involved in migrating data through changing technical regimes with minimum loss of information
- The development of suitable support services for digital resource users
- The costs involved in digital resources system design or modification, metadata creation, and conversion of traditional data resources into digital resources.

2. BIOMETRICS

Biometrics is the method of automatically identifying a person or authenticating the identity of a person based on a physical or behavioral characteristic. Biometric-based techniques have emerged as the most promising option for identifying individuals in the recent years. Instead of authenticating individuals by passwords, pins, smart cards, tokens, keys etc. before giving them access to physical and virtual domains, biometric method examines physical and/or behavioral features of an individual in order to ascertain, determine his identity. As PINs and passwords are difficult to remember and these can be guessed or stolen and (keys, cards, tokens, etc.) can be duplicated, misplaced or forgotten also magnetic card scan become despoiled and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged [3].

Biometric-based technologies comprises of identification based on physical characteristics such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear, voice and behavioral traits such as gait, signature and keystroke dynamics [3]. These systems have high accuracy in recognition.

Almost all biometric technologies require the object to be present in front of the system. As in case of finger print biometric system, one has to put finger prints on device while in other biometric systems, one has to stand in a fixed position in front of a camera for iris or retina identification [4]. However, facial recognition technique does not need the object to actively participate in getting scanned its facial features but it can be passively scanned from a distance. Also mass scanning feature is available only in Facial biometric system and not with any other biometric system.

Biometric recognition identifies a person from the entire registered population by searching the database for a match based solely on the biometric. For example, we can search a full database to authenticate whether an individual is registered user of a digital resource or not.

Face recognition provides us a suitable way to recognize and identify a person in a large database. With face recognition, a captured image of a person can just help us to recognize. In a face recognition system, cameras are installed at a surveillance place, so the system can capture all the objects in real time without being noticed. As a result, face recognition system have received significant attention [5].

3. TYPES OF BIOMETRICS

3.1 Fingerprints:

The pattern of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement agencies have been using fingerprint technique for determining identity of individuals by matching key points of ridge endings and bifurcations. However, this method requires installation of fingerprint recognition devices and active participation of the user. Also this method is time consuming and lacks mass scanning feature.

3.2 Speaker Recognition:

The acoustic features have been found to differ from one individual to another and this property can be used in Speaker recognition for identification purposes. The acoustic patterns of an individual reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice have earned speaker recognition its classification as a "behavioral biometric [6]. However, this method is not flexible and cannot provide much needed security from online threats and thus has information leakage chances.

3.3 Iris Recognition:

In this recognition method iris of the eye is scanned. Iris is the colored area that surrounds the pupil. Iris patterns are thought to be unique. Iris scanning devices have been applied in personal authentication for several years. Systems based on iris recognition have noticeably decreased in price and this trend is expected to continue [7]. However, iris recognition also needs active participation of the users and needs participation of every user and is thus both time consuming and lacks mass scanning facility.

3.4 Hand and Finger Geometry:

The methods hand and finger geometry are well established for personal authentication. To achieve personal authentication, the system may measure either physical characteristics of the fingers or the hands. These characteristics include width, length, thickness and surface area of the hand. Hand geometry has gained acceptance in a range of applications. It is similar to fingerprint biometrics, therefore, has almost same limitations. Also its surveillance in case of larger data resources is hard.

3.5 Signature Verification:

This technology uses the dynamic analysis of a signature to authenticate a person. In this technology, speed, angle and pressure used by the person are measured when a signature is produced. This technology has been used in e-business applications and other applications where signature is an accepted method of personal authentication. But this technology has much larger participation of users and will take very large time for identification of users when access requirement is larger due to larger participation. Also this method needs more robust equipment.

3.6 Face Recognition:

Face Recognition is an application to automatically identify a person after comparing with a database of images [8]. A probe image is taken with the help of a camera from a still source or video frame, and after accounting for various possible face appearance variations, is compared with the database images for identity. The identification can be done by capturing an image of the face in the visible spectrum using a web camera or by using the infrared patterns of facial heat emission. The visible light systems, by using cameras, extract features from the captured image(s) that do not change over time while avoiding superficial features such as hair and other facial expressions. After capturing a facial image, its reduced dimensional feature dataset can be obtained and then comparing these features with the stored images in a database, the user can be identified whether known or unknown.

4. FACIAL BIOMETRIC AUTHENTICATION

Biometric-based authentication applications include workstation and network access, single sign-on, application logon, Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The security of e-government and e-commerce can be attained through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments even for University libraries and other public libraries [9].

5. FACIAL BIOMETRIC AUTHENTICATED DIGITAL RESOURCE USAGE MODEL

In Face Recognition System a person's face is used to identify and verify the person. Every individual face differs in various features based on large number of parameters. These parameters can be extracted using a specific algorithm and then matched with features stored in a database. Based on these results, biometric authentication of a user can be performed using a biometric face recognition system. The modeled digital resource network can also use the facility of face biometric authentication to identify the user over the resource/library network [10]. The given facial biometric authenticated system works through the following processes and performs these intermediate steps:-

- 5.1 User Registration/Login:
- 5.2 Face Capturing:
- 5.3 Preprocessing:
- 5.4 Feature Extraction:
- 5.5 Matching/Comparison:
- 5.6 Classification/Result:

5.1 User Registration/Login:

The system Administrator can set the access rights to each and every individual user. The access rights can be set or modified by the Administrator for change of user or his rights. Using Access rights functionality the following operations can be performed:

5.2 Webcam Sensor:

The user has to get his face scanned with the help of a webcam for further processing and feature extraction operations. The webcam sensor is important component unit in the resource network and can sense/capture the face to get stored as template to be used for verification and identification.

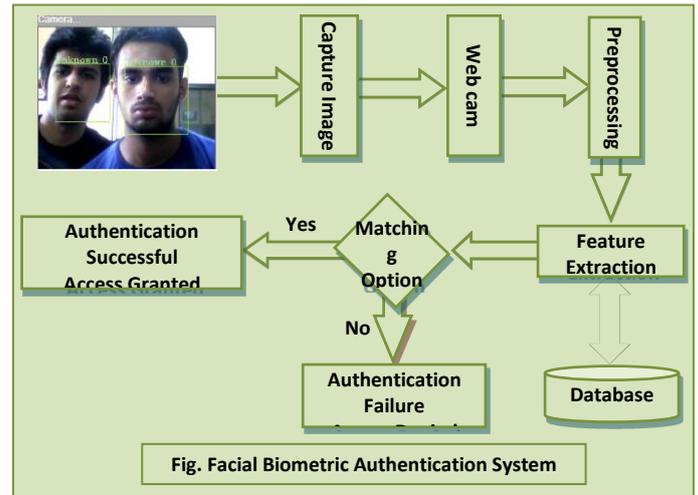


Fig. Facial Biometric Authentication System

5.3 Reprocessing:

In Preprocessing, only specific parameters/features of facial image are taken into account and are stored temporarily as a template in the database. A dedicated circuitry carries out the face verification within the unit itself. Each face registered with the unit is capable of matching facial features internally.

5.4 Feature Extraction & Comparison:

After preprocessing takes place, a pattern-matching algorithm is used to compare a newly retrieved face against the previously stored templates. For this purpose, a reduced dimensional facial feature dataset is obtained by applying the feasible algorithm. The dimension reduction can be performed with various recognition techniques such as Template/Feature based methods, Holistic Based Methods or Neural Network Methods.

5.4.1 Holistic methods:

In holistic approach, the complete face region is taken into account as input data into face catching system [11]. These methods use the whole face region as the raw input to a recognition system. One of the most widely used representations of the face region is Eigen pictures [12], which are based on principal component analysis [12].

5.4.2 Template/Feature Based:

Template based face recognition, where face template has been extracted and used for face recognition [14]. Typically, in these methods, local features such as the eyes, nose, and mouth are first extracted and their locations and local statistics (geometric and/or appearance) are fed into a structural classifier [14]. A template-based approach to detecting the eyes and mouth in real images was presented in [16].

5.4.3 Neural networks:

Artificial neural networks are a popular tool in face recognition [17]. They have been used in pattern recognition and classification. One approach is to use decision-based neural networks, which classifies pre-processed and sub sampled face images [18]. Lawrence et al used self-organizing map neural network and convolutional networks [19]. Self-organization capacity approach is proposed based on SOM which mapped image samples in to a topological space in which input mapping is same for original and output space [20]. So, it encapsulates dimensional reduction as well unvarying to minor changes in image sample. Victor emilNeagoe has presented concurrent SOM for face recognition [21]. Concurrent SOM is assembling of small SOM in which each SOM is developed individually for efficient and good result for one class [22].

The features which are extracted by applying any above facial recognition techniques are then matched with the stored images in the database. If a match occurs, then the user is provided access otherwise an error message is displayed and the user needs first to register himself.

6. BENEFITS & APPLICATIONS OF DIGITAL RESOURCES

- Electronic information can be accessed easily than its counterpart print or hard copy. The electronic warehouse has all files stored with in compatible manner and with flexible equipment.
- Electronic content can be sorted, retrieved and transmitted in an easy and fast manner. Access requests for a document can be met simultaneously by easily creating multiple instances or copies of the requested document. A large number of users can easily meet their requirements by using it.
- Digital texts can be interconnected and made interactive. The information retrieval and exchange by using information exchange protocols and metadata options will help users to enhance access and share information with other digital libraries.
- We can visualize environments that allow skilled professionals to:
- Give information to one another about potentially valuable new tools and technologies;
- share results of different experimentations with one another and assessment of such technologies; and
- Raise shared experimentation and assessment where applicable.

7. CONCLUSION

Biometric technology has come up with more accuracy at reduced costs and is emerging as the groundwork for many highly secure identification and personal verification solutions. Today's biometric solutions provide

a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas benefit from biometric technologies like University libraries and online digital resources by restricting the unauthorized users.

REFERENCES:

- [1] D Gayathri and Uma Rani, "A Prototype for Secure Digital Library Accessing System using Multimodal Biometric System," vol. 2, 2013.
- [2] Daniel Greenstein, "Digital Libraries and Their Challenges," NewYork, 1996.
- [3] Deepali H. Shah, J. S. Shah, and Tejas V. Shah, "The Exploration of Face Recognition Techniques," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 2, 2014. [Online]. www.ijaiem.org
- [4] R. Vinodini, "A Survey on Face Recognition," International Journal of Engineering Science and Technology (IJEST), vol. 6, no. 0975-5462, Feb. 2014.
- [5] Atul M Gonsai and Nilesh N Gonsai, "Biometric Authenticated Library Network Model For Information Sharing," in 5th International CALIBER, Chandigarh, India, 2007.
- [6] Sarbari Gupta, "Identity Authentication Identity Authentication using the using the PIV Token PIV Token," , India, 2004.
- [7] (2006) Biometric Consortium web site. [Online]. <http://www.biometrics.org>
- [8] J Shermina, "Face recognition system using multilinear principal component analysis and locality preserving projection," IEEE GCC Conference and Exhibition, pp. 283-286, Feb 2011.
- [9] (2006) Biometric Fingerprint Security. [Online]. http://www.topazsol.com/bio_door_access.htm
- [10] (2006) Face Identification system. [Online]. <http://www.securitex.com.sg/>
- [11] Li Xianwei and Zhang Haiyang, "A Survey of Face Recognition Methods," in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, 2013.
- [12] I Sirovich and M Kirby, "Low-dimensional procedure for the characterization of human face," J. Opt. Soc. Am. 4, 519-524, 1987.
- [13] Sanjeev Kumar and Harpreet Kaur, "Face Recognition Techniques: Classification And Comparisons," International Journal of Information Technology and Knowledge Management, vol. 5, pp. 361-363, July-December 2012.
- [14] Jigar M. Pandya, Devang Rathod, and Jigna J. Jadav, "A Survey of Face Recognition approach," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 1, pp. 632-635, January-February 2013.
- [15] H. Dibeklioglu, A.A. Salah, and and T. Gevers, "A

- Statistical Method For 2-D Facial Landmarking," Ieee Transactions On Image Processing, vol. 21, pp. 844-858, 2012.
- [16] A L Yuille, D S Cohen, and P W Hallinan, "Feature extraction from faces using deformable templates," Int. J. Comput. Vis. 8, 99-112, 1992.
- [17] J. J. Wong and S. Y. Cho, "'A Face Emotion Tree Structure Representation with Probabilistic Recursive Neural Network Modeling,'" Neural Computing and Applications, vol. 19, pp. 33-54, 2010.
- [18] S Kung and J Taur, "Decision-based neural networks with signal/image classification applications," IEEE Transactions on Neural Networks, 6(1):170-181, 1995.
- [19] S Lawrence, C L Giles, and A C Tsoi, "Face recognition: A convolutional neural network approach," IEEE Transactions on Neural Networks, 8:98-113, 1997.
- [20] QiuChen, Koji Kotani, Lee Feifei, and TadahiroOhmi, "Face Recognition Using Self-Organizing Maps," Tohoku University, Japan.,.
- [21] V E Neagoe, "'Concurrent self-organizing maps for pattern classification," Cognitive Informatics, 2002. Proceedings. First IEEE International Conference on, pp. 304 - 312, 2002.
- [22] A S JosephRaj and Raja, "'neural network based supervised self organizing maps for face recognition'," International Journal on Soft Computing (IJSC), vol. 3, August 2012.

BIOGRAPHY



Rafi Ahmad Khan is working as a faculty member at the Business School, University of Kashmir. He has done MCA from University of Jammu and Ph. D. in Business Intelligence from University of Kashmir. He has published extensively in national and international journal. He is editorial board member /reviewer of several international journals and is member of CSTA, UACEE, IEDRC, IACSIT and IAENG. His current research interests include Information Systems, Business Intelligence, Knowledge Management, Data Mining and Machine learning.

He is also affiliated as a faculty of Computer and Information Systems, Islamic University of Madina, Saudi Arabia.